A Beginner's Guide To BorderManager 3.x

Understanding and Configuring Novell BorderManager, versions 3.0, 3.5, 3.6, 3.7 and 3.8

Third Edition, Revision 1
June 8, 2004

Craig Johnson
Novell Support Connection Sysop
http://www.craigjconsulting.com/

Table of Contents

TABLE OF CONTENTS **2**

WHAT'S NEW? **18**
Third Edition 18
Third Edition, Revision 1 21

PRINTING THIS BOOK **22**

ACKNOWLEDGEMENTS **23**

ABOUT THE AUTHOR **24**

LICENSING **25**

OFFICIAL DISCLAIMER **26**

CHAPTER 1 - OVERVIEW **27**
What is BorderManager? 27
Filtering 27
Proxies 28
Gateways 28
VPN 28
Differences Between BorderManager 3.8 and Previous Versions 29
How This Book Is Organized 31
What this book covers 32
What this book does not cover 32

CHAPTER 2 - BASICS **33**
Some Important Terminology 33
Prerequisite Knowledge 34
TCP/IP Basics 35
Public & Private Networks 35
The Importance of the Default Route 36
Domain Name Service (DNS) 38
Secondary IP Addresses 39
Proxy Versus Routing and NAT (How Proxies Work) 41
BorderManager Scenarios 43
Scenario 1 - One Public IP Address 43
Scenario 2 - A Cable Modem with DHCP Connection 45
Scenario 3 - Multiple Public IP Addresses 48
Scenario 4 - BorderManager Used Only For HTTP Proxy 50
Scenario 5 - A Single Firewall (3-NIC) DMZ Segment 51
Scenario 6 - A Classic Two-Firewall DMZ 53
Scenario 7 - A Simple Site-to-Site VPN 54
Scenario 8 - A Simple Client-to-Site VPN 55
Scenario 9 - Complex Multiple BorderManager Server Environments 56
Scenario 9A – The Original Network 57
Scenario 9B – The More Current Network 60
Some Rules of Thumb and Words of Wisdom 64

CHAPTER 3 - INSTALLATION **67**
Server Hardware Suggestions 67
NetWare Server Installation Tips 68
Using Caldera DRDOS and NetWare – MultiBoot Menu 68

Using MSDOS 6.22 and NetWare 5.1 ... 71
Don't Let The NetWare Installation Create the Volumes Automatically ... 72
Install BorderManager from the Root of the CD ... 73
Get the Server on the Internet Before Configuring BorderManager ... 73
Setting the Default Route and DNS Servers ... 75
BorderManager Server Configuration Suggestions ... 80
NDS Design Considerations ... 82
Background Information ... 82
Version-Specific NDS Considerations ... 82
How to Install BorderManager Remotely ... 83
Requirements ... 84
Example Scenario ... 85
STARTX.NCF ... 85
REMX.NCF ... 85
DX.NCF ... 85
Procedure ... 86
Recommended Patches and Installation Sequence ... 87
Installing BorderManager 3.8 ... 88
on NetWare 6.5 ... 88
on NetWare 6.0 ... 90
on NetWare 5.1 ... 92
Installing BorderManager 3.7 ... 94
On NetWare 6.0 ... 94
On NetWare 5.1 ... 95
Installing BorderManager 3.6 ... 97
On NetWare 6.0 ... 97
On NetWare 5.1 ... 98
On NetWare 5.0 ... 100
On NetWare 4.11/4.2 ... 101
Installing BorderManager 3.5 ... 102
On NetWare 5.1 ... 102
On NetWare 5.0 ... 104
On NetWare 4.11 ... 106
Installing BorderManager 3.0 ... 108
On NetWare 5.0 ... 108
On NetWare 4.11 / 4.20 ... 108
Upgrade Considerations ... 110
Example Installation of BorderManager 3.8 on NetWare 6.0 ... 112
If You Are Upgrading BorderManager ... 136
NetWare 6.5 – Automatic Cache Volume Selection / Creation ... 137
Example Installation of BorderManager 3.7 on NetWare 6.0 ... 140
If You Are Upgrading BorderManager ... 148
Fresh Install of BorderManager 3.7 ... 149
Installation, Continued (Fresh Install or Upgrade Situation) ... 154
Post-Installation Procedures for BorderManager 3.7 or 3.8 ... 157
Installing BorderManager 3.7 or 3.8 Licenses with iManager ... 157
The FILTSRV MIGRATE Procedure ... 162
Starting BorderManager ... 163
BorderManager 3.0 / NetWare 4.x ... 163
BorderManager 3.7/3.8 / NetWare 5.x/6.x ... 165
General Installation Notes ... 167
Working Around Licensing Startup Delays ... 167
BorderManager 3.0, 3.5 and 3.6 ... 167
BorderManager 3.7 and 3.8 ... 168
NDS –601 Error Messages At Startup ... 168
Loading and Unloading BorderManager Manually ... 169

BMOFF.NCF (BorderManager 3.6 or Earlier) 170
BMON.NCF (BorderManager 3.6 or Earlier) 170
BMON.NCF (BorderManager 3.6 or Earlier) 171
BorderManager Licenses 172
What Are NLS Licenses? 172
NLS Issues 173
MLA Licenses 174
Changing Out A BorderManager Server 176
Concerns 176
Concept 176
Procedure 1 – Primary IP Addresses Used 176
Procedure 2 – Secondary IP Addresses Used 178
Critical BorderManager-Related Files 181
Configuration Tools 181
INETCFG.NLM 181
NIASCFG.NLM 181
VPNCFG.NLM 181
BRDCFG.NLM 181
FILTCFG.NLM 181
INSTALL.NLM 181
NWCONFIG.NLM 181
SYS:\PUBLIC\WIN32\NWADMN32.EXE 182
SYS:\PUBLIC\MGMT\CONSOLEONE\1.2\BIN\CONSOLEONE.EXE 182
iManager 2.0 182
IManager 1.5 182
CRON.NLM 183
Novell Remote Manager (NRM) 183
Data Files 183
SYS:\ETC\HOSTS 183
SYS:\ETC\HOSTNAME 183
SYS:\ETC\GATEWAYS 183
SYS:\ETC\RESOLV.CFG 183
SYS:\ETC\TCPIP.CFG 184
SYS:\ETC\NETINFO.CFG 184
SYS:\ETC\FILTERS.CFG 184
SYS:\ETC\CRONTAB 184
SYS:\ETC\PROXY\PROXY.CFG 184
Startup Files 184
C:\CONFIG.SYS 184
C:\AUTOEXEC.BAT 185
C:\NWSERVER\STARTUP.NCF 185
SYS:\SYSTEM\AUTOEXEC.NCF 185
Troubleshooting Tools 185
TCPCON.NLM 185
CALLMGR.NLM 185
PPPTRACE.NLM 185
Keeping BorderManager Up-to-date 186
Patches 186
PROXY.CFG Settings 186
The BorderManager 3.5 Enhancement Pack 187
Tips For Getting NWADMN32 To Work With BorderManager Servers 188
-601 Errors when Accessing BorderManager Servers 188
Fix NWADMN32 Crash by Renaming the ACNWAUTH.DLL Snapin 188
Get The Latest Version of NWADMN32 188
Fix Invalid BorderManager Snapin Modules Errors 188
Fix “No BorderManager Licenses Available” Messages 189

PC Hangs When Accessing NWADMN32 189
NWADMN32 Fails After BorderManager 3.8 Upgrade 189
What snapins should I have? 189
BorderManager 3.8 / NetWare 6.0 189
BorderManager 3.7 / NetWare 6.0 191
BorderManager 3.6 / NetWare 5.1 192
BorderManager 3.5 / NetWare 5.0 193
BorderManager 3.0 / NetWare 4.11 194

CHAPTER 4 – UNDERSTANDING PACKET FILTERING 195
Default Packet Filters 196
The BorderManager 3.x Default Packet Filters 196
Outgoing RIP Filters: 196
Incoming RIP Filters 197
Outgoing EGP Filters: 197
Incoming EGP Filters 197
OSPF External Route Filters 197
Packet Forwarding Filters 197
Packet Filter Exceptions 198
What are the Default Packet Filter Exceptions? 198
BorderManager 3.0, 3.5 and 3.6 198
BorderManager 3.7 200
BorderManager 3.8 202
Using iManager to View Filtering Information 205

CHAPTER 5 – THE INITIAL CONFIGURATION 211
BorderManager Setup Main Menu 213
BorderManager IP Address Configuration 215
Secondary IP addresses used on BORDER1 217
Authentication Context (Proxy Authentication) 218
Concept 218
Configuration 218
Proxy Authentication Settings 219
40-bit, 56-bit and 128-bit Encryption 224
Using Proxy Authentication on the Client with CLNTRUST 226
CLNTRUST Problem Work-Around 227
Configuring SSL Proxy Authentication 229
Creating a Security Container 230
Creating a Certificate Authority, pre-NetWare 5.1 231
Creating a Certificate Authority, with NetWare 5.1 or 6.x 233
Creating a Key Material Object for BorderManager with NWADMN32 234
Assigning the Key Material Object for SSL Proxy Authentication 243
Using SSL Proxy Authentication 244
Test Conditions 245
The SSL Proxy Authentication Login Screen (HTML) 246
BorderManager 3.8 SSL Proxy Authentication Login Screen (HTML) 248
Cookie-based Proxy Authentication 250
Proxy Authentication For Citrix and Terminal Servers 251
Concept 251
Pros 251
Cons 251
Configuring Terminal Server Authentication 252
PROXY.CFG Configuration 252
DNS Parameters 255
Transport 257

CHAPTER 6 - HTTP PROXY 259

Concepts 259
Pros 259
Cons 260
How BorderManager HTTP Proxy Works With DNS 261
How Browsers Are Configured For HTTP Proxy 265
Internet Explorer 266
Mozilla 1.5 268
Opera 7 270
Netscape 4.7 271
HTTP Proxy Details 273
HTTP 273
Cache Hierarchy Server 275
Cache Hierarchy Client 276
No Cache Hierarchy 276
Cache Hierarchy Client Set 276
Cache Hierarchy Client Set 277
Cache Hierarchy Routing 278
No Cache Hierarchy 278
Cache Hierarchy Configured 279
Logging 280
Common Logging 280
Extended Logging 282
Indexed Logging 283
HTTP Proxy Caching 285
Cache Aging 285
Cache Control 286
Cache Location 288
Cachable Object Control 291
Entering a Non-Cacheable URL Pattern 292
Clearing the Proxy Cache 293
Scheduled Downloads 294
Entering a URL to download on a schedule 295
Set Download Frequency 296
HTTP Proxy - SOCKS Client 297
Concept 297
Pros 297
Cons 297
Setting Up a Cache Hierarchy 300
Concept 300
CERN Configuration, BorderManager Server as a Client 301
ICP Cache Hierarchy 303
Cache Hierarchy Routing Exceptions 304

CHAPTER 7 - TRANSPARENT PROXY 307
Transparent Proxy (HTTP) 307
Concept 307
Pros 307
Cons 307
Configuring Transparent Proxy 309
BorderManager 3.0 Transparent Proxy configuration menu 309
BorderManager 3.5 and Later Transparent Proxy configuration menu 310
Transparent TELNET Proxy 313
Concept 313
Configuring Transparent TELNET Proxy 314
User Authentication 316
Transparent TELNET Proxy Usage 317

Example 1 – No User-based Authentication Required 317
Example 2 – NDS-Based User Authentication 318

CHAPTER 8 - FTP PROXY 321
Concept 321
Pros 321
Cons 321
Alternative For ACTIVE (PORT) FTP 321
Configuring FTP Proxy 322
User Authentication 322
Clear Text User/Password 322
Single Sign On 322
FTP Proxy Usage 323
Example 1 – No User-based Authentication Required, DOS FTP Client 323
Example 2 – User-based Authentication Required, DOS FTP Client 325
Example 3 – User-based Authentication Required, CuteFTP Client 330
Example 4 – User-based Authentication Required, WS_FTP Client 332
All Examples, FTP Proxy Statistics Screen 333

CHAPTER 9 - MAIL PROXY 335
Concept 335
Pros 335
Cons 335
An Alternative 336
A GWIA Alternative 336
Configuring Mail Proxy 337
No Internal Mail Server, Mail Through Proxy 337
Internal Mail Server, All Mail Through Proxy 339
PROXY.CFG Settings for Mail Proxy 342
BorderManager 3.5 through 3.7 342
BorderManager 3.8, With Multiple Domain Support 342
GWIA Example Settings 344
Access Rules to Allow POP3 Through Mail Proxy 345
Inbound POP3 to Internal Mail Server 345
Outbound POP3 to External Mail Server 346
Access Rule To Allow SMTP Through Mail Proxy 347
Access Rules to Control Use of Mail Proxy 348
Internal Mail Server 348
No Internal Mail Server 348
Access Rule Examples 349
Filter Exceptions Required for Mail Proxy with Internal Mail Server 352
Filter Exceptions Required for Mail Proxy with Internal Mail Server 352
SMTP Filter Exceptions 352
POP3 Filter Exceptions 354

CHAPTER 10 - NEWS PROXY 357
Concept 357
Pros 357
Cons 357
Using News Proxy With An External NNTP Server 358
Access Rules Blocking Posting 360
Access Rules Blocking Reading 361

CHAPTER 11 - REAL AUDIO PROXY 363
Concept 363
Pros 363
Cons 363
BorderManager 3.0 Settings 364

BorderManager 3.5 & Later Settings 365
BorderManager 3.0 RealAudio Proxy Access Rule 366
BorderManager 3.5 & Later RealAudio and RTSP Access Rule 367
RealOne (Free) Player Configuration 368
RealPlayer G2 Configuration 372

CHAPTER 12 - DNS PROXY 373
Concept 373
Pros 373
Cons 373
An Alternative 373
Configuring DNS Proxy 375

CHAPTER 13 - GENERIC TCP PROXY 377
Concept 377
Pros 377
Cons 377
Configuring Generic TCP Proxy 379
Example for Novell Remote Manager 381
Generic Proxy Configuration for Novell Remote Manager 381
Access Rule Configuration for Novell Remote Manager 383
Example for iManager 384
Generic Proxy Configuration for iManager 384
Access Rule Configuration for iManager 385
Example for NetWare Web Manager 386
Generic Proxy Configuration for Web Manager 387
Filter Exceptions for Web Manager 388
Browser Configuration for Web Manager 390
Access Rule Configuration for Web Manager 391
Example For NNTP with Port Translation 392
Generic Proxy Configuration for NNTP 393
Access Rule Configuration for NNTP 394
Outlook Express Configuration 395
Agent /Free Agent Configuration 403
Example Generic TCP Proxy for Inbound pcANYWHERE 404
Generic Proxy Configuration for pcANYWHERE 405

CHAPTER 14 - GENERIC UDP PROXY 407
Concept 407
Pros 407
Cons 407
Generic UDP Proxy - Time Server Proxies 409
Configuring A Generic UDP Proxy for NTP 410
Configuring a Generic UDP Proxy for RDATE 411
Example Generic UDP Proxy for Inbound pcANYWHERE 412

CHAPTER 15 – ACCELERATION (REVERSE PROXY) 415
Concept 415
Pros 415
Cons 416
Using The Primary Public IP Address 416
Configuring Reverse Proxy Acceleration 417
Using a Secondary Public IP Address 420
Filter Exceptions Needed for Reverse Proxy Acceleration 420
Access Rule Required for Reverse Proxy Acceleration 424
FTP Acceleration 425
Concept 425
Pros 425

Cons 425
Configuration 425

CHAPTER 16 – THE GATEWAYS 429
IPX/IP Gateway 429
Concept 429
Pros 430
Cons 430
History of IPX/IP Gateway 430
IntranetWare IPX/IP Gateway 430
BorderManager 2.1 IPX/IP Gateway 431
BorderManager 3.x IPX/IP Gateway 432
Client Settings For IP Gateway 435
Use Proxy, No Authentication, No Rules, No Logging 435
Use Proxy, Authentication, Access Rules and Logging 435
Use IP gateway, No Proxy, Access Rules and Logging 436
Installing IP Gateway Service on the PC 437
IP/IP Gateway 440
Concept 440
Pros 440
Cons 440
Access Rules, Proxies and the IP/IP Gateway 441
IP/IP Gateway With Access Rules And Without Proxy 441
IP/IP Gateway Without Access Rules And With Proxy 441
IP/IP Gateway With Proxy and With Access Rules 441
Configuring IP/IP Gateway 442
SOCKS Gateway 444
Concept 444
Pros 444
Cons 444

CHAPTER 17 – LEGACY SITE-TO-SITE VPN 447
Introduction to BorderManager Legacy VPN 447
Concept 447
Filter Exceptions Required 447
Setting Up the Master VPN Server 449
Configuration Tasks at the Server Console 449
VPN IP and IPX Addressing Design Considerations 452
Setting Up The Master VPN Server, Continued 455
Configuring the VPN Master Server in NWADMN32 467
Adding a Site-to-Site Slave VPN Server – Server Console Procedures 474
Adding a VPN Slave Server – NWADMN32 Procedures 488

CHAPTER 18 – LEGACY CLIENT-TO-SITE VPN 497
Concept 497
Setting Up VPN Servers 498
BorderManager Client-to-Site VPN Access Rules 504
Configuring a Client-to-Site VPN Client PC 511
VPN Client Connection Process – A Case Study 512
Step 1 – Try LAN VPN Client Connection to BORDER1 513
Step 2 – Repeat Test With Valid IP Address 516
Step 3 – Install/Reinstall VPN Client Software 520
Step 4 – Try LAN VPN Client Connection to BORDER2 523
Step 5 – Create a Login Policy Object 526
Step 6 – Add Rule for VPN Authentication 529
Step 7 – Try LAN VPN Client Connection to BORDER2 Again 534
Client-to-Site VPN Using Pure IP Login 536

Routing Issues 536
Missing Default Route on Internal Hosts and Routers 536
Incorrect Default Route on Internal Hosts and Routers 537
Missing Encrypted Network on VPN Server 537
Issues with Client-to-Site over Site-to-Site Links 538
Issue with BorderManager 3.5 and 3.6 with Client-to-Site VPN and Dynamic NAT 539
Name Resolution (Service Location) Issues 539
Making Use of SLP 539
Using NWHOST Instead Of (Or In Addition To) SLP (Win9x Only) 540
Using the HOSTS File (All Windows Platforms) 541
The Importance of Client32 Protocol Preferences 542
The Bottom Line 544
Client-to-Site VPN Over NAT 546
Disconnecting a Client-to-Site Connection 546

CHAPTER 19 – BORDERMANAGER 3.8 SITE-TO-SITE VPN 547
Theory 547
Overview 548
Upgrade Considerations 549
Network Diagram 551
Prerequisites 552
Site-to-Site VPN 553
Understanding Certificates and VPN 553
Custom Server Certificates 553
User Certificates (for Client-to-Site VPN) 554
Trusted Root Containers 554
Site-to-Site VPN - Summary of Major Steps 554
Configure JACK as a VPN Server 556
Configure JACK as the Master Site-to-Site VPN Server 567
VPN Server Configuration 567
Configure Site-to-Site VPN Service 569
Configure MOE as a VPN Server 580
Configure MOE as a Site-to-Site VPN Slave Server 588
Prerequisites 588
Configuring MOE 589
Adding MOE as a VPN Slave Server to the VPN 598
Configuring Site-to-Site VPN Parameters 610
General Parameters 611
Traffic Rules 612
3rd Party Traffic Rules 613
Configure MANNY as a VPN Server Behind NAT 614
Configuration Steps Performed 614
Linksys Router Configuration (NAT Configuration) 615
VPN Certificate Details 619
Trusted Root Object in Slave Server NDS Tree 622
Trusted Root Object in Master Server NDS Tree 623
Slave Server MANNY VPN Configuration 624
Configuration of Slave Server MANNY on Master VPN Server 625
Configure a Non-BorderManager Server as a Site-to-Site VPN Link 628
Add the Non-BorderManager VPN Server 628
Configuring 3rd Party Traffic Rules 631
Configure a Linksys Router as a VPN Server 642
Creating VPN Objects with ConsoleOne and iManager 647
Manually Creating A Trusted Root Object (TRO), Using ConsoleOne 647
Exporting JACK's VPN Certificate to a .DER File using ConsoleOne 648
Create MOE's Trusted Root Object from a .DER File Using ConsoleOne 654

Manually Creating A Trusted Root Object (TRO), Using iManager 659
Exporting MOE's VPN Certificate to a .DER File using iManager 660
Create JACK's Trusted Root Object from a .DER File Using iManager 672
Manually Creating a Trusted Root Container (TRC) 681
Using iManager 2.0 681
Using ConsoleOne 684
Manually Creating a VPN Server Certificate 687
Using iManager 687
Using ConsoleOne 703

CHAPTER 20 - BORDERMANAGER 3.8 CLIENT-TO-SITE VPN 717
Quick Summary 717
Limitations 718
NDS Context 718
Traffic Rule Limitations 718
Authentication Rule Limitations 719
LDAP Configuration 719
DNS/SLP Configuration Limitations 719
Configure A Server for Client-to-Site VPN 720
Configure General Parameters 720
Configure Traffic Rules 727
Traffic Rules – Allow Admin User to All Internal Hosts 731
Traffic Rules - Allow VPN Users to All Hosts Except 10.1.1.50 739
Deny All Access to 10.1.1.50 Rule 740
Traffic Rule - Allow VPN Users Group to All Internal Hosts 746
Traffic Rule - Allow All Users in NDS Tree Access to 10.1.1.100 750
Traffic Rule – Allow Any User to iFolder Server 756
Optional Traffic Rule – Do Not Deny Non-VPN Traffic 759
Configure Client-to-Site Authentication Rules 764
LDAP Configuration 770
DNS/SLP Configuration 771
Assign the Client-to-Site VPN Service to VPN Server JACK 777
Novell VPN Client Installation And Configuration 783
Security Considerations – Use A Personal Firewall and Anti-Virus Software 783
Force Novell Client Firewall for VPN Connections 784
Installing the Novell VPN Client 785
Using BorderManager 3.8 VPN Client – Backwards Compatibility Mode 791
Configuring the BorderManager 3.8 VPN Client 792
Connecting to a BorderManager 3.8 Server in Backwards Compatibility Mode 795
Using BorderManager 3.8 VPN Client – NMAS Authentication Mode 796
VPN Client Configuration for NMAS 796
Using BorderManager 3.8 VPN Client – NMAS/LDAP Authentication Mode 803
Prerequisites 803
Configure LDAP Authentication 803
Configure LDAP Traffic Rule 808
Configure VPN Client for NMAS/LDAP 815
Using BorderManager 3.8 VPN Client – Certificate Authentication Mode 820
Create a VPN User Certificate 821
Export a User Certificate to a File 827
VPN Client Option – Get Certificate 833
Configure Certificate Authentication / Traffic Rules 838
Connecting in Certificate Mode 846
Using Client-to-Site VPN in Shared Secret Mode 850
Configure the Server 850
Configure and Use the VPN Client 852

CHAPTER 21 – VIEWING VPN DATA 855

Legacy VPN - Using NWADMN32 To View VPN Log Data and Activity 855
BorderManager 3.8 VPN – Using Novell Remote Manager to View VPN Data 860
Viewing BorderManager 3.8 Audit Log Data 861
VPN Member List Menu 862
VPN View Status (JACK) menu 863
Real Time Monitor 864
Audit Log 865
Current Site-to-Site Activity 866
Current Client-to-Site Activity 867

CHAPTER 22 - ACCESS RULES 869
Concept 869
The Default Deny Rule 870
Rule Inheritance 870
Proxy Authentication and NDS-based Rules 870
Selective Proxy Authentication & Access Rules 871
Enforce Rules 873
Time Restrictions 874
Setting Up Access Rules 875
Explanation of the Effective Rules 876
Checking Effective Rules 879
Rules Applied On BORDER1 883
Allow All users to Access Selected URL's 883
Allow the Admin User to Access a Reverse Proxy 885
Allow Selected Users Access to Any URL 886
Track Usage for a Particular Web Site 888
Track Usage for a Particular Web Site 888
Allow All URL's for Specific IP Addresses 889
Block Selected Downloads 891
Deny Access to URL's with CyberPatrol 894
Deny Access to URL's with SurfControl 896
Deny Access to URL's with LinkWall 900
Allow Admin to Get to Any URL Not Already Blocked 902
Allow Specific Hosts Access to Any URL Not Already Denied 903
Selectively Deny Access to Certain Web Sites 904
Track Specific Users with an Allow URL Rule 906
Allow Authenticated Users to Any URL 909
Allow Admin User to FTP Accelerator (FTP Reverse Proxy) 910
Deny All Users Access To FTP Reverse Proxy 911
Allow All Users Use of the FTP Proxy 912
Allow Generic Proxy Access to Web Manager 913
Allow Access To Generic UDP Proxy for Port 37 (RDATE) 914
Inbound pcANYWHERE Access Rules Using Generic Proxies 915
Inbound Generic Proxy Access To Novell Remote Manager 918
Inbound Generic Proxy Access To iManager 919
Deny Legacy VPN Client Access to the BORDER1 Server 920
Allow Legacy VPN Client Access to the BORDER1 Server 921
Allow Access to RealAudio Proxy (BorderManager 3.0) 923
Allow Access to RealAudio Proxy (BorderManager 3.5 and later) 924
Access Rules Controlling News Proxy 925
Deny a Specific Newsgroup for Reading 925
Allow All Newsgroups to be Read 926
Deny Posting to a Specific Newsgroup 927
Allowing Posting to All Newsgroups 928
Allow Outbound SMTP Through the Mail Proxy 929
Allow Inbound SMTP Mail Through the Mail Proxy 930

Deny All SMTP Mail Through the Mail Proxy 931
Allow Inbound POP3 Through the Mail Proxy 932
Deny All URLs For Troubleshooting Purposes 933
Deny All Ports for Troubleshooting Purposes 934
N2H2 Access Rule Example 935
LinkWall Access Rule Example 938
Example - Setting an Allow All URL Rule 941
Example - Adding a CyberPatrol CyberNOT List Deny Rule 942
CyberNOT List Selection 943
CyberNOT List Definitions in Use 944
The Refresh Server Button 946
Those Additional Rules Fields 947
Backing up Access Rules 948
Selective Proxy Authentication Example Rules 951
Access Rules 952
Allow Admin to Browse Any URL 953
Allow Selected Hosts to Any URL 954
Deny SurfControl URL's to Selected Users 956
Deny SurfControl URL's to NDS Users 957
Allow Selected IP Addresses to Any URL Not Already Denied 958
Allow All NDS Users to Any URL Not Already Denied 959
Effect on Logging with Selective Proxy Authentication 960

CHAPTER 23 – SURFCONTROL, CYBERPATROL, N2H2 AND LINKWALL 961
SurfControl 961
The CSPCONFIG.INI File for Service Pack 2 or 3 966
SurfControl Access Rules (Unregistered): 967
Registering SurfControl 968
Updating SurfControl 972
SurfControl Memory Usage During Updates 972
Reducing SurfControl RAM Requirements 972
SurfControl Disk Space Usage During Updates 973
Updating Through A Cache Hierarchy / Upstream Proxy 973
Scheduling SurfControl Updates 974
Using CRON to Schedule SurfControl Updates 974
Using Scheduled Tasks to Schedule SurfControl Updates 975
Using TaskMaster to Schedule SurfControl Updates 976
CyberPatrol 978
Registering CyberPatrol 979
The CyberPatrol REGISTER.EXE Program 980
Downloading a New CyberNOT List On Demand 981
N2H2 982
How N2H2 Works 982
N2H2 Configuration on Windows 2000 Advanced Server 982
General Menu 983
Updates Menu 984
Windows 2000 Services Configuration 985
BorderManager Configuration for N2H2 985
Configure Category Server Communications 987
N2H2 Sentian Category Server selection list 988
LinkWall 990
Installing LinkWall 991
LinkWall Configuration In NWADMN32 995
SquidGuard Blacklist Example for Filtering Porn Sites 997
LinkWall Startup Options 1000
Registering LinkWall 1001

CHAPTER 24 - CUSTOM ERROR PAGES 1003
Concept 1003
Example 1003

CHAPTER 25 - USING DYNAMIC NAT 1007
Concept 1007
Outbound DNS 1010
DNS from Internal PC's to an ISP's DNS Servers 1010
Outbound NNTP 1013

CHAPTER 26 - USING STATIC NAT 1015
Concept 1015
Static NAT To Internal SMTP Mail Server 1016

CHAPTER 27 -BORDERMANAGER ALERTS 1021
Concept 1021
Configuring Alerts 1022
BorderManager 3.0 1022
BorderManager 3.5 and Later 1023

CHAPTER 28 - LOGGING 1025
Controlling the Size of the Indexed and Access Control Logs 1025
Viewing Common Log Files 1028
Using BRDSTATS 1028
Viewing Extended Logs 1031
Viewing Indexed Logs 1031
Viewing Real-Time Proxy Cache Data in NWADMN32 1039
Viewing Real-Time Browsing Activity with RTMonitor 1040
Discovering Who is Browsing Without Proxy Authentication 1043
Using RTMonitor 1045
RTMonitor Configuration 1046
Viewing Access Control Logs 1048
Usage Trends 1053
Exporting the Access Control Log to Excel 1054
Viewing Legacy VPN Activity 1060
Viewing BorderManager 3.8 VPN Activity 1066

CHAPTER 29 - BORDERMANAGER CONSOLE SCREENS 1067
IP Gateway / SOCKS 1067
Proxy Console 1068
Option 1 - FastCache Current Activity screen 1069
Option 2 – Display Memory Usage 1072
Option 3 – Display ICP Statistics 1073
Option 4 – Display DNS Statistics 1074
Option 5 – Display Cache Statistics 1075
Option 6 – Display Not Cached Statistics 1076
Option 7 – Display HTTP Server Statistics 1077
Option 8 – Display HTTP Client Statistics 1078
Option 9 – Display Connection Statistics 1079
Option 10 – Display FTP Client Statistics 1080
Option 11 – Display GOPHER Statistics 1081
Option 12 – Display DNS Cache Entry Information 1082
Option 13 – Show hosts sorted by most DNS lookup requests 1083
Option 14 – Show Origin Hosts Sorted by Amount of Data Transmitted by the Cache 1084
Option 15 – Show Origin Hosts Sorted by the Amount of Data sent TO the Cache 1085
Option 16 – Show Proxies and Origin Hosts Sorted By Most Data Directly Received 1086
Option 17 – Display Configured Addresses and Services 1087
Option 18 – Display SOCKS Client Statistics 1089

Option 19 – Application Proxies 1090
Mail Proxy Statistics 1091
Real Audio Proxy Statistics 1092
Option 20 – Transparent Proxy Statistics 1093
Option 23 – Virus Pattern Configuration Screen 1094
Option 24 – Terminal Server Authentication Configuration 1095

CHAPTER 30 - PROXY CACHE CONFIGURATION CONSOLE 1097
Option 1 – Display Object Cache Configuration 1098
Option 2 – Display DNS/Miscellaneous Configuration 1099
Option 3 – Display TCP Configuration 1100
Option 4 – Display ICP Configuration 1101
Option 5 – Display FTP/GOPHER Configuration 1102
Option 6 – Display HTTP Configuration 1103
Option 7 – Display Authentication Configuration 1104
Option 8 – Display Generic TCP/UDP Configuration 1105
Option 9 – Display RealAudio Configuration 1106
Option 10 – Display SMTP Configuration 1107
Option 11 – Display POP3 Configuration 1108
Option 12 – Display NNTP Configuration 1109
Option 13 – Display SOCKS Configuration 1110
Option 14 – Display THTTP Configuration 1111
Option 15 – Display Site Download Configuration 1112
Option 16 – Display TTELNET Configuration 1113
Option 17 – Display RTSP Configuration 1114

CHAPTER 31 – TROUBLESHOOTING BORDERMANAGER 1115
Simplify the Configuration 1115
Start at the Server 1115
Isolate the Problem 1116
Look at the IP Packets at the Server 1116
Is it a Filtering Problem? 1116
Is it a NAT or a Routing Problem? 1116
Is it an Access Rule Problem? 1117
How To Search the Novell KnowledgeBase 1118
NWADMN32 Issues 1118
BorderManager 3.7 / 3.8 Issues 1118
Packet Filtering Issues 1118
SurfControl Issues 1119
Printing Problems Due to eDirectory 8.7.1 1119
BorderManager 3.8 Won't Install Over Older Versions 1119
BorderManager 3.8 Installation Fails with Java Error 1120
HTTP Proxy Issues 1120
Transparent Proxy Issues 1121
Mail Proxy Issues 1122
DNS Proxy Issues 1123
IP Gateway Issues 1123
Legacy Site-to-Site VPN Issues 1123
Legacy Client-to-Site VPN Issues 1124
BorderManager 3.8 VPN Issues 1126
Understanding How VPN Gets Configured 1126
Troubleshooting Tools 1127
BorderManager 3.8 Site-to-Site Issues 1130
BorderManager 3.8 Client-to-Site Issues 1132
iManager 2.0 Issues 1136
General Issues 1136
Problems with Unknown System Error in iManager 2.0.1 on Windows 1137

Problems with iManager 2.0.1 on NetWare 6.0 1137
Installing iManager 2.0.1 on NetWare 6.0 1137
Getting iManager 2.0.1 Running on NetWare 6.0 1138
Miscellaneous Issues 1141
BorderManager Does Not Start After NW51SP7, NW6SP4 or NW65SP1 1141
Dial-Up Connection Keeps Coming Up 1141

CHAPTER 32 - PERFORMANCE TUNING 1143
General Recommendations 1143
Use the Following Server Set Parameters 1144
Use The Following NetWare Administrator (NWADMN32) Settings 1145
Watch Your Memory - Memory Considerations 1146
The PROXY.CFG File 1147
Craig's PROXY.CFG File, Revision 12 1148

CHAPTER 33 - ODDS & ENDS 1155
Documenting Your Server 1155
Run TECHWALK.NLM 1155
Run CONFIG.NLM 1155
Save Basic BorderManager Settings to a File with CFGDUMP 1156
Comment Your Filter Exceptions 1157
Screenshot your VPNCFG Screens 1157
Screenshot your INETCFG Settings 1157
Screenshot your NWADMN32 Screens 1158
Back Up Your Access Rules 1158
Miscellaneous Hints 1159
PPTP to BorderManager 3.5 1159
Converting Browser Proxy Settings Automatically 1159
Internet Explorer 1159
VPN & Modems Tip 1161
VPN Client with LAN Connection 1162
VPN with Client 4.7x for NT 1162
Citrix Setting for NAT 1163
HOSTS File Tip 1163
Load Balancing Internal Web Servers 1163
SSL Logout Page Location 1163
St. Bernard Software / Open File Manager – Don't Use On BorderManager 1164
Setting Browser Proxy Settings 1164
Using an Autoconfiguration Program to Set Proxy Settings 1165
Serving up the PROXY.PAC File from BorderManager 1165
Serving up the PROXY.PAC File as a Local File 1165
Simple PROXY.PAC Example 1166
More Complex PROXY.PAC Version 1166
Using PROXY.PAC to Bypass Proxy for Multiple URL's 1167
Round-Robin PROXY.PAC Example 1168
BorderManager and NetWare Cluster Services 1169
Common Log File Format 1172
IP Address 1172
Authenticated User Name 1172
Date 1172
Time 1172
Timezone 1172
HTTP Request 1172
URL 1173
Status Code 1173

CHAPTER 34 - IMANAGER 2.0 1175

Background Information 1175
Install iManager Components 1176
Configuring iManager 2.0 the First Time 1185
Configuring Portal Properties 1187
Unconfigure Option (optional) 1189
Configure Portal 1190
Adding VPN Snapins to iManager 2.0 1197
Adding Filtering Configuration Option to iManager 2.0 on Windows 1205
Resetting the iManager Configuration File 1206

ERRATA & REVISIONS 1209
Beta 2.0 1209
Beta 3.0 1209
First Edition 1209
Version 1.01 1210
Second Edition 1211
Changes from Beta 1 1211
Third Edition 1213
Changes from Beta 1 1213
Third Edition, Revision 1 1215
Changes from Third Edition 1215

INDEX 1217

What's New?

Third Edition

What's new in this version of the book? (As compared to the Second Edition). For starters, all the mentions of BorderManager 3.8 are new. I have also…

- Added entirely new chapters for BorderManager 3.8 Site-to-Site and Client-to-Site, and the old Site-to-Site and Client-to-Site VPN chapters have been relabeled as 'Legacy VPN'.
- Added a new chapter at the end of the book on installing and configuring iManager 2.0 on a Windows PC.
- Updated the installation sequences, and updated the patches there as well. (Of course that is always a losing battle, since the patches may have been updated by the time this book comes out or is purchased).
- Updated a number of the screenshots for the proxies, and access rules. In some cases I corrected either errors or examples that were not clear. In other cases I wanted to update the examples with different URL, names or IP addresses to reflect changes in the test network I used to test the examples and gather screenshots.
- Corrected a number of small typos here and there, and tried to add better wording to some descriptions. I often added another sentence or paragraph to various examples to try to make things more clear than they were previously. The chapter on Client-to-Site VPN is a good case. That chapter was originally written before BorderManager 3.6 was available, and the examples were mostly Windows 95 and IPX-specific. I tried to add more explanation of how that VPN works in more modern environments, with Windows 2000 and XP clients.
- Considerably changed my test network since the First and Second editions of this book. This leads to the dilemma of not having a network that exactly matched all the previous examples, and so required a judgment on leaving in old screenshots or replacing them. I have left in many old screenshots, especially for old systems that I no longer have in place to test with (such as BorderManager 3.0 and IPX/IP Gateway). One big problem was what to do with the Advanced Scenario number 9 that showed the IP addressing

and servers in place when I originally made all the screenshots and examples for the First Edition of this book. I could not completely replicate all of the older systems, yet the examples referred to the advanced scenario for IP addressing information. On the other hand, I have a much different configuration for the current test network used to install and show BorderManager 3.8 servers. I have chosen to show both the old and new advanced scenario diagrams. I hope that the latest diagram will not overwhelm readers! I also have started to use subsets of the diagram for new chapters, such as the BorderManager 3.8 VPN. In that chapter, I show only the relevant parts of the diagram for the VPN examples. Still, some readers might find it both interesting and instructive to see how I have all kinds of subnets and servers interconnected and working.

- Added additional examples to the troubleshooting chapter.
- Added a few new screenshots of features that are new to BorderManager 3.8 (besides the VPN parts), such as option 24 on the Proxy Console screen (added also to BorderManager 3.7 with a later patch, and the 3.8 SSL Proxy Authentication login screen (which can be customized).
- Added a useful note on updating CLNTRUST to newer versions. (I can't believe it took me so long to think of that simple trick).
- Added an example of how to configure BorderManager 3.8 Mail Proxy for multi-domain support.
- Updated my PROXY.CFG example. (My latest version should always be available at my web site).
- Changed all references to my web site from http://nscsysop.hypermart.net to http://www.craigjconsulting.com. As of this writing, both URL's are valid and point to the same server, but registering my own domain name gives me the option of moving my web site if Hypermart should go out of business. I think the new URL will be much easier to remember. Lord knows I had enough problems trying to get people to type in the correct text with the old one!
- Added an example of Terminal Services Authentication, a feature that was added with a late patch to BorderManager 3.7.
- Updated the LinkWall section to reflect a newer version of LinkWall.

- Updated the SurfControl section to reflect Service Pack 2 version of SurfControl (in the beta version of this book) and Service Pack 3 in the final release of this version.
- Updated the RTMonitor section to reflect new features of the current version of that program.
- Updated the section on remote installation of BorderManager somewhat.
- Added a new section showing the installation of BorderManager 3.8 on a NetWare 6.0 server. I also have a short section describing an additional option you might see when installing on a NetWare 6.5 server, involving cache volume creation.
- Added an example of a multiboot menu you can use with Caldera DRDOS before NetWare starts.
- Updated Transparent HTTP Proxy with new features added with later BorderManager 3.7 patches.
- Updated the brief chapter on filtering with information on new default filter exceptions installed with BorderManager 3.8. Note that this book does NOT cover filtering in any depth, but that my book *Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions* does go into filtering with detail.
- Updated methods for configuring browsers with proxy settings.
- Added a couple of new proxy.pac examples.
- Added Generic TCP Proxy examples for iManager and Novell Remote Manager.
- Revised the Mail Proxy chapter extensively.
- Added Pros and Cons to all proxy chapters.
- Removed the (obsolete) example for configuring Webtrends log file analyzer.
- *I have made additional changes since the beta version of this book. Those changes are listed in the Errata & Revisions chapter near the end of this book.*

Third Edition, Revision 1

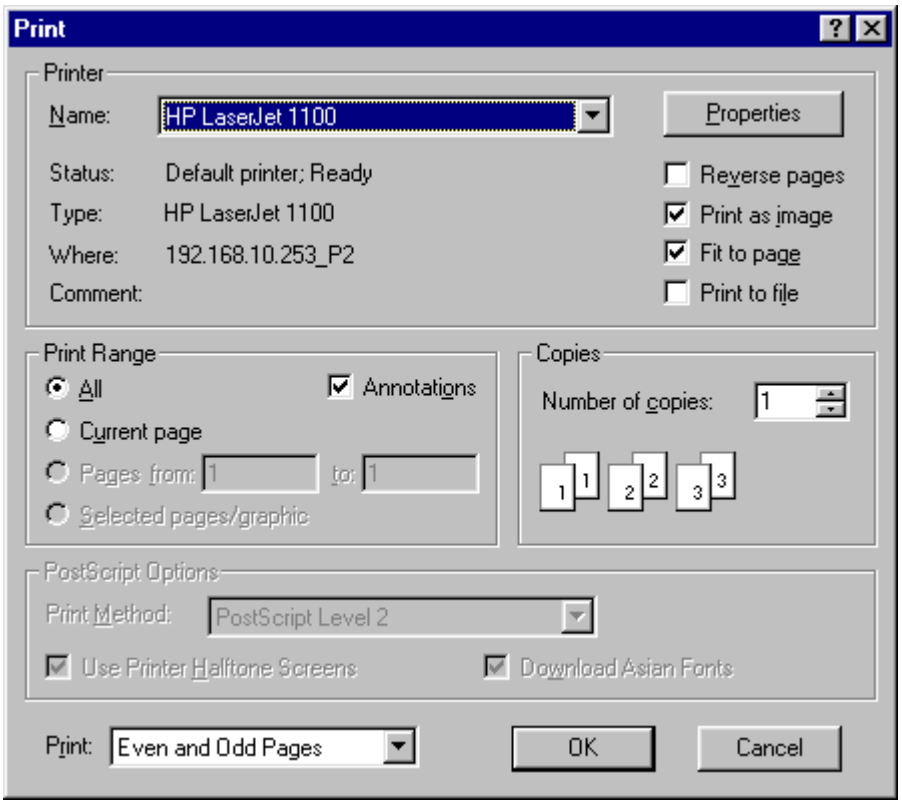
I did not intend to make a revision 1 to the Third Edition, but shortly after I released the Third Edition, I discovered that I had forgotten to include details and screenshots of the Linksys BEFSX41 VPN router used in a Site-to-Site VPN example. In addition, I learned some additional information on various BorderManager features, and was told about some typographical errors, so I have made other corrections, added more information here and there.

- In Revision 1 of the Third Edition, I added a few pages detailing the Linksys router configuration for Site-to-Site VPN.
- Updated the 3rd-Party Traffic Rules for the Linksys router Site-to-Site VPN configuration.
- Added a short section explaining how to require Novell Client Firewall to be running on VPN clients for Client-to-Site VPN.
- Corrected several minor typographical errors pointed out by Jim Michaels.
- Updated patches, including more information on getting newer patches to run on older versions of BorderManager.
- Updated the troubleshooting section with some additional tips for problems installing BorderManager 3.8, snapin issues, and iManager problems.
- Added explanation of using the ACLDUMP.NLM utility
- Added explanation of using the CFGDUMP.NLM utility
- Added explanation of using the VPNRegClean.exe utility
- Updated my proxy.cfg file

Printing This Book

This book is sold in PDF format. It should display well on your monitor, but you may have problems getting the graphics to print well. **If you have problems** printing the graphics, be sure to print as follows:

1. Use Acrobat Reader version 5.0 or later. Acrobat Reader 3.0 does not have the option shown below. The most recent version of Acrobat Reader may not have any issues at all.
2. When you print, be sure to select the option '**Print As Image**' in the print dialog. As shown below. This option made a huge difference for me when printing to a 600 dpi HP LaserJet PCL printer.



3. If the above settings do not help, see this URL:

http://www.adobe.com/support/techdocs/150d6.htm

This book has been written so that the main chapters start on odd-numbered pages, to make it easier to add ring-binder tabs when the book has been printed double-sided.

Acknowledgements

The author would like to acknowledge the following people who have contributed significantly to the creation of this book.

Scott Jones, Novell BorderManager Product Manager, who made it possible for me to participate in the development of BorderManager 3.7 and 3.8, and provide the Lite version of my book on the BorderManager 3.7 and 3.8 product CD's.

The BorderManager Core Team and other Novell employees, who helped answer my questions about many new aspects of BorderManager 3.7 and 3.8 when I was having problems. Very much appreciated was proofreading help from **Ed Sherwood-Smith**, **Meena Guttikar, Jim Short, Scott Jones,** and **Shaun Pond.**

Jim Michaels, Caterina Luppi, Shaun Pond, Terry Rodecker and Marcus Williamson, Novell Support Connection SysOps, who contributed subject matter to this book and proofread it closely. Portions of this document are unpublished copyright (c) 2000 – Marcus Williamson

Neil Cashell, for contributing material for this book.

Evan Mintzer and Michael Prentice, who provided an explanation of how NetWare Cluster Services can be used with BorderManager, and contributed other subject matter to this book as well as proofreading it.

Sue Lange, **Joe Balderson**, **Steven Meier, David Pluke, Jeff Alexander** and **Mark Crosby**, who helped with early beta revisions of this book.

Barbara Myers, **Edward J. Egan**, and **Lee Collar**, who helped with proofreading beta 1 of the Second Edition of this book and pointed out typos to be fixed.

Karim Kronfli and **Cary Stanton**, who helped with proofreading beta 1 of the Third Edition by pointing out typos to be fixed.

Danita Zanrè, Novell Support Connection SysOp and internationally renowned GroupWise consultant, who helped get this book on the market.

The Late John Ryan, whose encouragement convinced me to write a book on the subject of BorderManager in the first place! I am very glad I told him how much his encouragement meant to me before he passed away unexpectedly.

About the Author

Craig Johnson has been working with computers since he wrote his first computer program in college at Purdue University in 1971. Currently Craig is a consultant, owner of Craig Johnson Consulting, and he works on many Novell-related projects, including a sizeable number of BorderManager installations. Craig has been a Novell Support Connection Sysop since 1998, and he specializes in (naturally) the BorderManager forums at support-forums.novell.com (NNTP). Craig has been working with BorderManager since before the official release of BorderManager version 2.1. Through the Novell Support Connection forums, Craig has provided advice on an estimated 3000+ BorderManager installations.

Craig has been a speaker at Novell's BrainShare conference several times.

When not spending 12 hours per day at a computer, Craig likes to work out in Taekwondo, where he holds the rank of Black Belt, fourth degree, and is a certified instructor.

Craig sometimes adds the following letters to his resume / CV:

- Novell MCNE, CNE6, CNE5, CNE 4.11, CNE 4, CNE3
- Novell CLE (Certified Linux Engineer)
- Cisco CCNA
- Compaq ASE
- IBM PSE.
- BSMT, Purdue University
- MBA MGT, Western International University

Licensing

Official Disclaimer

The author and publisher have made their best efforts to prepare this book. The author and the publisher make no representation or warranties of any kind with regard to the completeness or accuracy of the contents herein and accept no liability of any kind including but not limited to performance, merchantability, fitness for any particular purpose, or any losses or damages or any kind caused or alleged to be caused directly or indirectly from this book.

Chapter 1 - Overview

What is BorderManager?

BorderManager is a collection of capable services, designed to allow controlled access to the Internet, while safely preventing unwanted intrusions to your network. Because of the sheer number of different services provided in the BorderManager product, it can be very confusing to the beginner to know what to configure, let alone how to configure it! This book is designed to help with both the concept ("What is this feature used for?"), and the implementation ("How do I set this up?").

BorderManager is a **Firewall**, meaning that it acts as a secure wall between the internal LAN and the Internet, while allowing users on the LAN to access the Internet, subject to control by the system administrator.

BorderManager is a **Proxy Server**, meaning that acts on behalf of the user when connecting with Internet servers.

BorderManager is a **Gateway Server**, allowing internal users to access various Internet services with the BorderManager server acting as a middleman, and even allowing (in the case of the IPX/IP Gateway) workstations on the internal LAN to access the Internet without using TCP/IP packets for communication to the workstations.

BorderManager provides **Virtual Private Network** (VPN) services, to allow, in one case, PC's to safely connect to the internal LAN over the Internet, and, in another case, to allow networks to be securely interconnected over the Internet.

BorderManager also includes RADIUS, a form of authentication for dial-up users, and NIAS dial-in/out services (which unfortunately is not RADIUS-compliant!) BorderManager 3.x dial-in/out services allows up to 250 modems to be hosted on a single server. *Neither of these services is covered in this book.*

The following are major components of BorderManager 3.x.

Filtering

BorderManager 3.x includes sophisticated packet filtering capabilities to secure the internal LAN from unwanted intrusions. Packet filtering is the foundation of any firewall, though it alone is not considered to be adequate security. Both stateful and non-

stateful packet filtering capability is included with BorderManager 3.x.

Proxies

BorderManager 3.x includes built-in proxies for HTTP (web browsing) FTP, DNS, SMTP, POP3, RealAudio, and News (Usenet) traffic. In addition, BorderManager 3.x includes Generic TCP and UDP proxies that allow the systems administrator to create specialized proxies for many other types of traffic. All proxies are controlled with access rules, except the DNS Proxy. (The DNS Proxy works regardless of access rules). The HTTP and FTP proxies can be controlled with access rules based on NDS objects such as user, group or container.

Using a proxy server disconnects the user's computer from actual Internet contact, providing the most secure method of communications possible. The HTTP and FTP Proxy servers also cache data on the BorderManager server, which greatly improves effective performance and leverages the available Internet connection bandwidth.

Gateways

BorderManager 3.x includes IP/IP, IPX/IP and SOCKS Gateway. While these gateways are less used than in previous years, they all have useful purposes, and the IP/IP and IPX/IP Gateways in particular allow an unprecedented level of control through access rules based on NDS users, groups or containers.

VPN

BorderManager 3.x provides two types of Virtual Private Networks. Client-to-Site allows a user to make a local Internet connection, then securely access TCP/IP and IPX resources on the internal LAN from anywhere in the world. Site-to-Site VPN allows up to 254 separate networks to be securely interconnected over the Internet from anywhere in the world. Both types of VPN encrypt the data flowing to and from the internal LAN to secure it from unwanted viewing even if intercepted during the journey through the Internet.

Using a VPN is generally far cheaper and more flexible than providing long-distance dial-in connections, or creating dedicated private WAN links between branch offices.

BorderManager 3.6 and 3.7 also provide the capability of establishing a Client-to-Site VPN connection when the client is behind a Network Address Translation (NAT) hop.

Differences Between BorderManager 3.8 and Previous Versions

BorderManager 3.8 retains almost all of the features of previous versions of BorderManager 3.0, 3.5, 3.6 and 3.7, and adds several enhancements. (NIAS modem sharing has been removed from 3.8).

1. BorderManager 3.8 includes licenses for all components. There is no 'firewall' or 'VPN' version. This is similar to the old Enterprise Edition versions of BorderManager, and is the same as BorderManager 3.7. The licenses for BorderManager 3.8 will not work with other versions. Optional components, such as Novell's NCF (Novell Client Firewall) are only provided with the understanding that you have purchased a BorderManager license for anyone making use of them.
2. BorderManager 3.8 only installs on NetWare 5.1, 6.0 and 6.5. BorderManager 3.8 is the **only** supported version of BorderManager for NetWare 6.5.
3. BorderManager 3.8 includes VPN clients supported on Windows 98, WindowsME, Windows NT, Windows 2000 and Windows XP. As of this writing, the VPN client is not supported on Windows 2003, but a newer version may be available for download in the future with that capability.
4. BorderManager 3.8 VPN has been **extensively enhanced**, and provides far more capabilities than any previous version. BorderManager 3.8 VPN supports IKE-compliant connections, meaning that non-Novell VPN clients and servers that are truly IKE-compliant and industry standard should also be able to make VPN connections to BorderManager 3.8. This includes Linux FreeS/WAN, and clients for Macintosh and even PDA's. (The beta version of this book has examples only of the Novell VPN client. The released version may add more examples).
5. BorderManager 3.7 replaced the old CyberPatrol software with a new SurfControl program, although it still uses the CPFILTER.NLM file name. BorderManager 3.8 also can use SurfControl, though it is no longer supplied on the BorderManager CD. BorderManager 3.7 (with a service pack) and 3.8 can also use N2H2 Sentian Category server and Connectotel's LinkWall, AdWall and FileWall software.
6. BorderManager 3.8 includes **Novell Modular Authentication Services (NMAS)** components. NMAS allows for many sophisticated forms of identification/authorization to the network, including token cards, proximity cards, fingerprint scanners, etc, beyond the usual network ID and password. (This book covers only NDS password authentication with NMAS).

7. BMAS is replaced with NMAS, giving better RADIUS support.
8. BorderManager 3.8 supports multiple internal mail domains with the Mail Proxy. Previous versions supported only one.
9. BorderManager 3.8 includes a **Personal Firewall** called Novell Client Firewall (NCF). A Personal Firewall is bundled so that remote users connecting via VPN have some measure of protection and do not provide an easy method for hackers to penetrate the network via a VPN-connected host. (This book does not cover the installation, configuration or use of the personal firewall).
10. **RAM requirements are higher**, especially if SurfControl is being used. The minimum RAM recommendation for a dedicated BorderManager server is now 512MB, 1GB or more preferred. SurfControl recommends an **ADDITIONAL 512MB of RAM**. In my testing of SurfControl, it used 295MB of RAM, and temporarily doubled that when the update process was running. You should plan for the server to have 1GB or more of RAM.
11. For both BorderManager 3.7 and 3.8, TCP/IP Filters and Filter Exceptions can be managed through a browser interface or by using the old FILTCFG program. IP filters and exceptions are stored in NDS in order to make GUI-based management (through iManager) possible. There are numerous ramifications to this change if you are used to using FILTCFG.NLM and are used to backing up and moving filters and exceptions by moving the FILTERS.CFG file. This book does not cover filtering in any great depth, and you should refer to my book "*Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions*" for a thorough explanation. See http://www.craigjconsulting.com.

How This Book Is Organized

This book has been written to give practical examples and explanations of how to configure the most popular features of Novell's BorderManager, version 3.5, 3.6, 3.7 and 3.8. Almost all of the examples will also apply to BorderManager 3.0. Some of the explanation will be useful in understanding how BorderManager 2.1 functions, but the book is not intended to cover BorderManager 2.1 in any detail.

Each section is intended to stand on its own, though the reader is strongly urged to read the Basics section first if not familiar with the content covered there. Also, Access Rules are closely linked to the use of the Proxies, and it is impossible to understand one without some knowledge of the other.

Two areas of particular concern are not covered *in depth* in this book: Packet Filtering and Virtual Private Networking (VPN). Both of these subjects are left to other books, such as my "*Novell BorderManager: A Beginner's Guide To Configuring Filter Exceptions*", by Craig Johnson, available at http://www.craigjconsulting.com. Other subjects not covered at all include RADIUS / BMAS / NMAS and NIAS Dial-in/out services.

RADIUS services are documented in a Novell AppNote by Marcus Williamson, "Configuring BorderManager Authentication Services for Use with ActivCard Tokens", from http://developer.novell.com/research/appnotes/2000/a0005.htm. This AppNote is based on BorderManager 3.7.

NIAS Dial-in/out services are basically the same as NetWare Connect, and as such the older NetWare Connect documentation should apply. However, NIAS itself includes wide area networking components that must be installed before BorderManager is installed. These components, a subset of NIAS, are installed when you install BorderManager from the root of the BorderManager 3.x installation CD. Prior to BorderManager 3.8, the dial services components are installed as well, but not configured unless you follow options in NIASCFG.NLM. BorderManager 3.8 no longer includes the dial services portions of NIAS.

This book describes much of the configuration procedures and settings used to set up BorderManager 3.0, 3.5, 3.6 Enterprise Edition, 3.7 and 3.8.

It is important to note that numerous services can be allowed through BorderManager **without** going through proxy services by means of packet filter exceptions. A few examples are shown in this book, and many examples are shown in my book on configuring packet filtering exceptions (described above). Refer to the sections in this book on dynamic NAT and Static NAT.

What this book covers

- HTTP Proxy
- Transparent Proxy (HTTP & TELNET)
- ICP / CERN Proxy Hierarchy
- DNS Proxy
- FTP Proxy
- Mail Proxy
- Generic TCP & UDP Proxies
- News Proxy for Internal NNTP Clients
- Reverse Proxy Acceleration of Internal Web Servers
- Reverse FTP Proxy Acceleration of Internal FTP Servers
- BorderManager Access Rules
- Custom Error Pages for HTTP Proxy
- Dynamic NAT
- Static NAT
- BorderManager Alerts
- Troubleshooting
- HTTP logging (Common and Indexed)
- Client-to-Site VPN
- Site-to-Site VPN
- iManager 2.0 installation and configuration

What this book does not cover

- Packet filtering (in any depth, see my other book – http://www.craigjconsulting.com/)
- SOCKS Client or SOCKS Server (in depth)
- News Proxy for Internal NNTP Server
- ActivCard or NMAS authentication other than user ID / password
- RADIUS
- Dial-in/out Services
- Novell's Client Firewall (included with BorderManager 3.8)

Chapter 2 - Basics

Some Important Terminology

In general, **Access Control Rules** (Access Rules) refers to rules set up to restrict or allow access through proxies, VPN or IP Gateway, and, with some exceptions for VPN, they are configured in NWADMN32.EXE. VPN access rules are configured with iManager.

Access Rules may be based on a source or destination equal to Any, NDS Object Name (user, group or container), DNS Hostname, IP address range or IP Subnet Address. Access Rules are stored in NDS and are read and applied by ACLCHECK.NLM.

Note Access Rules based on a source of an NDS user name, group or container generally **only** apply to the HTTP, FTP and Transparent TELNET proxies, and IP Gateway, and require Proxy Authentication to be used.

Filters and **Filter Exceptions** are not the same as Access Rules, and packet filters are set up using FILTCFG.NLM or iManager. Filters do not use any kind of NDS values, but instead apply globally to all traffic passing through the server. Both IP and IPX packet filters and exceptions can be configured. Filters apply regardless of whether a user is configured to use the HTTP proxy cache or not. Packet filters in versions of BorderManager prior to 3.7 are stored in the <servername>\SYS:\ETC\FILTERS.CFG file, so it is a good idea to back up that file before modifying any packet filters. After installing BorderManager 3.7, IP filters are stored in NDS, while IPX and Appletalk filters are stored in FILTERS.CFG. And it is still a good idea to make backup copies of FILTERS.CFG!

Proxy Authentication refers to a method of relating the TCP/IP traffic from a user's workstation to an NDS user ID. Proxy Authentication is necessary to apply NDS-based access rules to control browsing by NDS user ID, and to log usage by NDS user ID.

Reverse Proxy or **Reverse Proxy Acceleration** or just **Acceleration** means to use BorderManager as a proxy between an internal web or FTP server and a user on the Internet. The 'acceleration' term comes in because BorderManager can cache the data being requested from the internal server and provide it more quickly to the requesting user than could be done by going directly to the internal server for the data each time. Reverse Proxy is

basically the same as the forward proxy, except used in an inbound direction.

VPN means Virtual Private Network, and it can refer to a PC or other host connection to a BorderManager server or to two BorderManager or non-BorderManager servers linked together over an encrypted connection.

Prerequisite Knowledge

This book cannot explain everything the user needs to know about setting up a firewall, or every feature and detail about BorderManager. Firewalls and Internet connectivity are not simple to explain (though they can be surprisingly quick to set up, once you get to know your way around the concepts). Do not get too frustrated if you do not understand the concepts the first time you read a section. You will pick up the knowledge you need as you get hands-on experience. You can pick and choose the segments of this book to read as you need them.

If you want to set up a Proxy, you need to be familiar with Access Rules! The two go hand-in-hand.

You should have a basic idea of how services like web browsing work, how DNS works, and it will be very helpful to have some idea about how IP addressing is done. If you have ever taken a basic Novell certification test and been exposed to the OSI 7-layer model of networking, you can make good use of those concepts here, as BorderManager deals a lot with the networking layer, and the application layer of that model. (Remember Application, Presentation, Session, Transport, Network, Data Link and Physical? Well, the proxies are at the Application layer, and packet filtering is at the Network layer.)

You should realize that it is important to prevent unwanted traffic from getting into your LAN when you connect it to the Internet, and that a firewall (like BorderManager) is intended to provide that protection. You should realize that the fundamental building block of firewall protection is provided by packet filtering, and you should begin by enabling packet filters when requested in the installation process.

You should be reasonably familiar with setting up a NetWare server, and applying patches with the INSTALL.NLM (NetWare 4.11) or NWCONFIG.NLM (NetWare 5.x and 6). You should know how to configure network settings in INETCFG.NLM at the server console. You should know how to physically install network cards and cable them to the LAN.

Finally, **you should know how to get help** when you are stuck with a NetWare problem. I highly recommend that all users get familiar

with the Novell Public Forums, and the Novell Knowledgebase as a minimum. The Novell Public Forums can be accessed via a web browser from a link at http://support.novell.com, though performance and ease of use is **much** better if you use a Newsreader pointed at the support-forums.novell.com NNTP server. Real, live, knowledgeable people cover the public forums, and you can often get an answer to a question within hours. The Novell Knowledgebase at http://support.novell.com is one of the best reference databases in the world for finding answers to NetWare-related questions. Both of these resources are **free**. If you need personal help, you can open an incident with Novell to work on a specific problem, or hire me (Craig Johnson Consulting) to work on your network.

TCP/IP Basics

Public & Private Networks

In order to route IP traffic to the proper host on the Internet, each host must be configured with a globally unique IP address that is **registered** with Internic. Such an IP address is called a *public* IP address. A company will normally purchase an IP address range from an Internet Service Provider (ISP) and pay a yearly maintenance fee based partly on the number of IP addresses they are reserving. The ISP will take care of ensuring that all incoming Internet traffic to a host within that IP address range knows how to get there. It is essential to have at least one properly registered public IP address configured on the public interface of your BorderManager server for it to communicate to the Internet (unless using Network Address Translation on an 'upstream' router).

Partly because of the cost involved, and partly because the world is running out of publicly available IP address ranges, not everyone has public IP addresses assigned **inside** their private LANs. In some cases (not recommended, since many restrictions are then placed on BorderManager's operation), an address range registered to some different company is in use on a private LAN. To avoid the situation where registered addresses are being used on different networks, three different IP address networks have been reserved for anyone to use. These special IP networks are called *private* IP addresses**. Internet routers are programmed to drop packets with a private IP destination address**. The three private address ranges set aside for use are:

- 10.x.x.x (a full class A range)
- 172.16.x.x to 172.31.x.x (16 Class B ranges)
- 192.168.x.x (256 Class C ranges)

You can use these IP networks as you wish within your internal network and subnet them as needed, but they MUST be used with either dynamic NAT (**N**etwork **A**ddress **T**ranslation) or proxy services (or both). Most people find the 192.168.x.x network to be the easiest to work with, as it is easier to understand Class C subnetting than other classes. The use of these IP networks is discussed in the following document:

```
RFC 1918 - Address Allocation for Private Internets. Y.
Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot &
E. Lear. February 1996. (Format: TXT=22270 bytes)
(Obsoletes RFC1627, RFC1597) (Also BCP0005) (Status:
BEST CURRENT PRACTICE)
```

Note Use this URL for a link to RFC 1918: ftp://ftp.isi.edu/in-notes/rfc1918.txt

---

Since these ranges cannot 'talk' to the Internet (packets from these addresses will be dropped at some point on an Internet router), some special techniques must be used to let internal hosts using these addresses communicate to the Internet. The two techniques in use are **NAT** (Network Address Translation) and **Proxy**. BorderManager provides both capabilities. Both techniques effectively substitute the public IP address of the BorderManager server for the actual (private) source address of the host originating the traffic.

There is not a problem using NAT and proxy services at the same time. You can easily have some types of traffic using a proxy and other types of traffic using NAT. For the security-conscious, bear in mind that using a proxy is considered to be more secure than using NAT, if you have the option of using either.

Remember – if you use the private IP addresses, you will not get a response back from the Internet to your PC unless you are using a Proxy, a Gateway service or have dynamic NAT enabled! This has nothing to do with packet filtering! The routers on the Internet will drop packets with private addresses.

The Importance of the Default Route

All routers and hosts on both internal and external IP *segments must have a default route set up*! Once you try to communicate with hosts on the Internet, it is not possible to build a routing table in which the location of every subnet is included. Instead, a default route (default gateway) is used to forward any packet with an unknown network address. The default route/gateway is always an IP address on the same network as the host, and points to the next hop to be used to get an unknown packet out to the Internet.

Typically, on a BorderManager server, the default route is set to the external IP segment address (this would be a LAN port, not a WAN port) of a router connected to the Internet. NetWare server default routes are configured in INETCFG.NLM, and stored in the SYS:\ETC\GATEWAYS file. They can be verified using TCPCON.NLM.

The first thing to try when you have a communications issue is to temporarily disable packet filtering. (This is, of course, an obvious security hole, but it is the easiest way to confirm that packet filtering is an issue). If the traffic still doesn't flow, you are likely to be having a routing issue, and experience says that most routing issues involve incorrect or missing default routes.

Here is an analogy of what a default route is. Say you live in a house with several other people, and you want to send one of them a little letter. You write the letter and are ready to deliver it. Since you live in the house, you not only know the address of everyone in the house (master bedroom, kid's bedroom, etc.) but you know how to find the room. So you go to the room and slide the letter under the door. Now, let's say you want to mail a letter to someone else, and that person lives in another city. You have the address, but you have no clue how to deliver the letter yourself! But you DO have a 'default route' - the mailbox. So you drop the letter in the mailbox, and trust the postman to deliver the letter. The postman of course doesn't have any idea how to deliver that letter either, but he/she DOES have another default route - the letter-sorting bin for letters going out of town. Along various steps of the way, the letter keeps getting delivered not directly to the end destination, but instead to the next 'hop' along the way to the destination. Finally, a postman on the final step of the letter's journey gets the mail, and since he/she actually knows where the house is, the letter can be put into a final destination (mailbox). Even then, someone at the house may pick up the letter and forward it onto the intended recipient.

Now suppose that the reader of the letter wants to send a reply. All of the same steps have to occur in the reverse direction, or the reply does not get through.

There is even a measure of packet filtering involved here - if the letter does not have enough postage, it does not get through.

What is the point of all of this? If ANY step in the process IN BOTH DIRECTIONS does not have a default route, the mail (your TCP/IP packets) will not get through, unless the end address is a local address (inside your house = inside your LAN). Remember that the first step a packet takes toward a host outside your LAN is the next router on your LAN, and your own PC needs a default route to it in order to start the packet on its way.

When you install BorderManager 3.7, it will prompt you for the default route on the server, but earlier versions will not.

Domain Name Service (DNS)

Domain Name Services (DNS) is a method used to determine the IP address of a host from the name of the host. Public IP addresses are unique around the world, and it is the IP address, not the name, that routers use to move packets from one point to another. It is impractical to have a network connected to the Internet that does not allow you to resolve names into addresses (although it is theoretically possible). Fortunately, it is not hard to set up BorderManager to use DNS services. However, there are some aspects of DNS services that need to be explained in relation to how BorderManager uses DNS. The BorderManager server itself must be able to resolve DNS queries in order to function normally.

- Public DNS Records – these records are accessed by someone on the Internet, and the records (IP addresses, generally) should always refer to the public IP address of a host, not an internal IP address of a host. (Some hosts will have both a public and an internal – private – IP address). Your ISP will almost always provide public DNS services for you at no extra cost as part of their service.
- Private DNS records – these records are accessed by the users of your internal LAN, and the records should always refer to the private internal IP addresses of the hosts, not the public addresses. You must maintain your own internal DNS server(s) if you want to resolve host names to internal IP addresses, unless you use HOSTS tables. (See below).
- Dual Public/Private DNS System – This is the method recommended in this book (although there are other methods that can be used). In this method, the public records are hosted by the ISP while the internal records are hosted in the LAN (by you). The ISP is officially delegated as Start Of Authority (SOA) for your domain, which means that any time some Internet host tries to resolve a name in your domain to an IP address, the DNS query will come to the ISP and be answered by the ISP's DNS servers. However, when a host on the internal LAN (inside your network) tries to resolve a name in your domain, the query will go first to one of your DNS servers to be resolved. Queries not resolved by your DNS servers will be forwarded on to your ISP's DNS servers. Your DNS server might be a real DNS server, or you may instead rely on HOSTS table entries at one or more computers.
- HOSTS Table – A file on the local computer that contains a qualified domain name and the IP address for that host. The HOSTS file will always be checked for a domain name before a DNS query is sent to a DNS server. On a NetWare server, it is essential that the last entry in the HOSTS file be followed by a carriage return/line feed.

.

Operating System	File Location
NetWare Server	SYS:\ETC\HOSTS
Windows 95, 98, ME	C:\WINDOWS\HOSTS
Windows NT	C:\WINNT\SYSTEM\DRIVERS\ETC\HOSTS
Windows 2000 / XP	C:\WINNT\SYSTEM32\DRIVERS\ETC\HOSTS

- DNS Proxy – BorderManager 3.x comes with a service called DNS Proxy. This service will proxy DNS requests coming to it without having to route DNS through the default packet filters. With DNS Proxy configured, internal PCs (and servers) can be set up to point to the BorderManager private IP address. The DNS Proxy will take outbound DNS requests and proxy them on behalf of the user to whatever DNS servers have been configured in INETCFG.NLM on the BorderManager server. A good alternative to using the DNS proxy is to set up two stateful packet filter exceptions to allow UDP destination port 53 and TCP destination port 53 outbound and have internal users point to the ISP's DNS servers. Normally, only UDP is used for DNS queries, but there are times that DNS queries can fail with UDP and then be (automatically) requested via TCP.

Note Stateful packet filtering is explained in detail in my book "Novell BorderManager: A Beginner's Guide To Configuring Filter Exceptions", available at http://www.craigjconsulting.com. A full discussion of packet filtering concepts and issues is outside the scope of this book.

Secondary IP Addresses

Once you wish to provide a service to users on the Internet (such as a public web server), you will often find that you need to assign more than one IP address to the public network interface card in a firewall, in this case BorderManager.

Note You may need a dedicated IP address for each service, such as a web server or a mail server that you want to host. You will definitely need to have different IP addresses if you want to use static NAT and proxies as you cannot use both of those services on the same public IP address at the same time.

The deciding factor is whether or not you need to allow incoming traffic – traffic going from the internal LAN to the outside (Internet) is usually sent out a single IP address and doesn't require any additional addresses on the BorderManager server.

With NetWare it is possible to assign many IP addresses to each network interface in a server, though it isn't so easy to see more than one assigned address.

Note You can assign addresses in different networks to a single network card, and NetWare will route between them as if they were assigned to two different network cards. Assigning addresses from different networks is done in INETCFG by simply binding a new address to an interface. An example would be to assign 192.168.10.252 and 172.16.31.254 to an interface. This book does not cover such an assignment, as it is not normally needed in a BorderManager configuration. This is NOT the same as a secondary IP address. (See below).

A typical way to assign multiple addresses to a network interface is to add IP addresses from within the same IP network to an interface. An example would be to add 192.168.10.253 to an interface that already has IP address 192.168.10.252 bound (configured with INETCFG under Bindings, TCP/IP). These types of addresses on a NetWare server are called *secondary IP addresses*.

NetWare 6.5 assigns secondary IP addresses in INETCFG in the BINDINGS menu for a particular IP address.

In versions of NetWare prior to 6.5, you must assign a secondary IP address to an interface with the **add secondary ipaddress** command at the server console, as in this example which adds IP address 192.168.10.253 to an existing interface.

```
ADD SECONDARY IPADDRESS 192.168.10.253
```

Note IPADDRESS is all one word!

NetWare will look at the addresses already assigned to the interfaces and add the secondary IP address to the interface that is already configured for that network range. In this example, the current binding is 192.168.10.252, and the secondary IP address 192.168.10.253 is added. You would then have two addresses assigned to the same interface. Once you have executed the ADD command, the IP address is instantly available – you do not have to reinitialize or reboot the server.

Secondary IP addresses do not show up when typing CONFIG at the server, and they do not show up in the Bindings menu of INETCFG. You display the secondary IP addresses with the command

---

```
DISPLAY SECONDARY IPADDRESS
```

If you wish to remove a secondary IP address, use the command **delete secondary ipaddress** as in this example that removes the previously defined secondary address of 192.168.10.253.

```
DELETE SECONDARY IPADDRESS 192.168.10.253
```

*Caution! Prior to NetWare 6.5, secondary IP addresses **are not permanent** – you need to put the ADD SECONDARY IPADDRESS 192.168.10.253 command in AUTOEXEC.NCF (after the primary bindings are made) so that the addresses will be available after a server reboot. NetWare 6.5 has a menu in INETCFG, Bindings, <ip address> for adding Secondary IP Addresses.*

Proxy Versus Routing and NAT (How Proxies Work)

BorderManager provides more than one means of getting to the Internet – using a Gateway service, using a Proxy service (BorderManager 2.1 only has an HTTP Proxy, whereas there are several proxies in BorderManager 3.0 and later), or using simple routing. For the purposes of this book, the difference is that simple routing requires more setup on the part of the administrator in terms of packet filter exceptions, NAT and DNS than when using proxies.

When using a Proxy service on BorderManager, the originating program at the PC (a browser, for example) is normally configured with a special proxy setting that points to the BorderManager private IP address and designated listening port number. When that PC sends out traffic, packets are handed off to the BorderManager proxy, and the proxy then **regenerates** the packets onto its public interface (with the BorderManager server's public IP address as the packet's source address).

A proxy does not route the packet between interfaces, it regenerates it - this is an essential difference between using a proxy and using NAT. When the return traffic comes back to the BorderManager server, the proxy regenerates the reply onto the private interface with the original PC's IP address as the return packet destination address.

Because the proxy is doing all the work for the PC, you will NOT need to

- configure the client with DNS settings (at least not in the case of HTTP proxy),

- have any non-default packet filter exceptions set up on the BorderManager server,
- have dynamic NAT enabled at the BorderManager server,
- have TCP/IP routing enabled at the BorderManager server.

However, the BorderManager server itself must be properly configured to resolve DNS queries.

You control traffic through proxies by setting up access rules in the BorderManager configuration.

If routing (as with NAT) is used instead of Proxy services, you will need to:

- define a DNS server entry on the originating host PC, at least if DNS hostname queries are required for the service (such as HTTP),
- enable Dynamic NAT on the BorderManager server if a private IP network address is used on the internal LAN,
- enable routing for TCP/IP in INETCFG, Protocols, TCP/IP, and
- set up a default gateway on the client PCs,
- configure the PC to make DNS queries.

In addition, some type of packet filter exception must be configured on the BorderManager server to allow the desired traffic to go out and to allow the return traffic to get back in. The only control over outbound traffic is to set up the packet filter exceptions allowing the traffic. You can configure packet filter exceptions to provide access to:

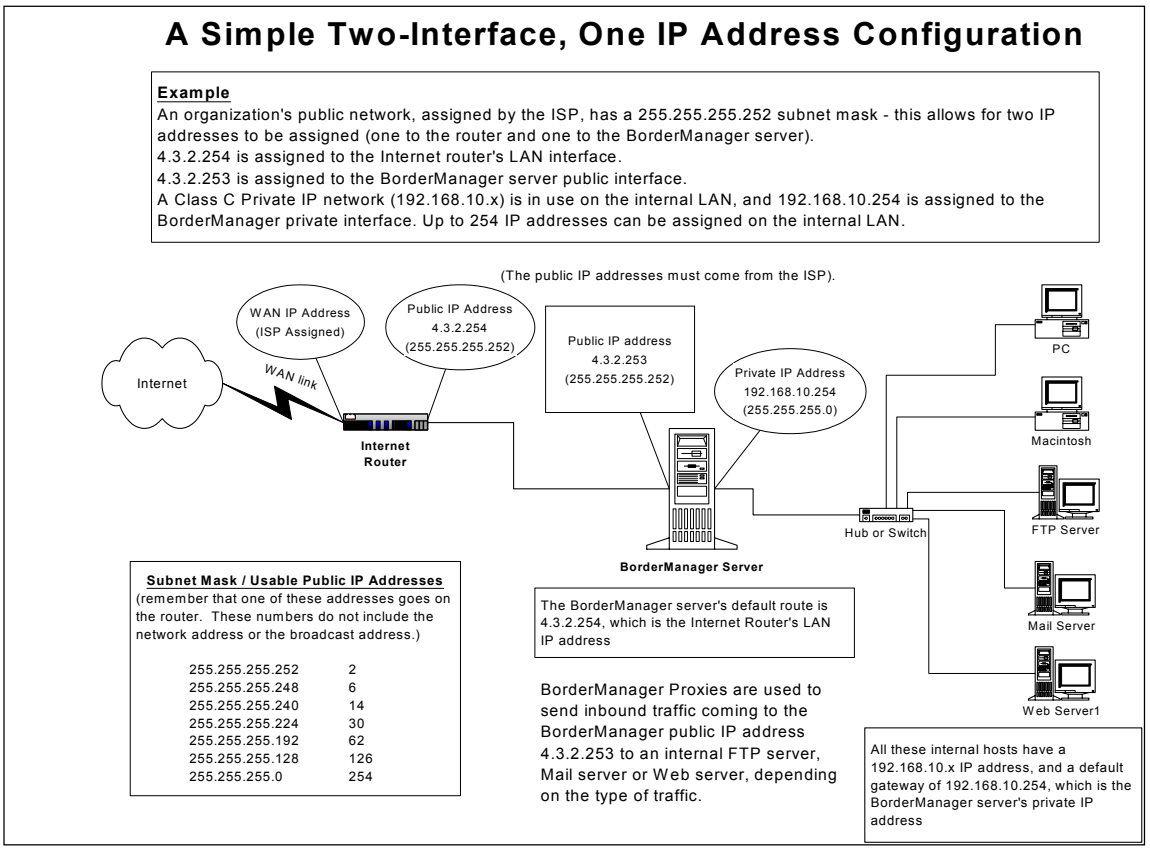
- every host in the internal LAN
- only selected IP networks or subnets. You cannot specify a range of IP addresses within a single packet filter exception, only selected IP addresses (hosts).

BorderManager Scenarios

Note Some of these scenarios are not very basic! Don't get bogged down trying to understand the more complex scenarios until you are familiar with BorderManager. I provide these scenarios in order to show some range of possibilities for implementing BorderManager.

Scenario 1 - One Public IP Address

There are many examples shown throughout this book. Some of the examples, unless otherwise noted, are based on an example configuration similar to the one described here.



The BorderManager server is set up in a two-interface configuration with one interface labeled as Public and the other as Private. The public interface is connected to a router connected to the Internet. The private interface is connected to an internal LAN by way of a 10/100 switch or hub.

In the first sample configuration shown, only a single IP address can be assigned to the BorderManager public interface because of the

public IP address subnet mask (255.255.255.252). A 255.255.255.252 subnet mask only allows two useable IP addresses, with one going on the Internet router's LAN interface and the other going on the BorderManager server's public interface.

The public IP address on the BorderManager server has been configured with BorderManager's reverse proxy acceleration to make both an internal web server and an internal FTP server available to the Internet. (This, and other capabilities, is explained later in this book.) In addition, the BorderManager server has been configured with the Mail Proxy to allow an internal mail server to send and receive mail from the Internet.

The BorderManager server has a default route set up with the IP address of the LAN interface of the Internet router.

The internal IP addresses are the same as in the previous example – up to 254 hosts can be on this subnet without an additional router, including the BorderManager private IP address.

The internal hosts should all have a default gateway configured that is equal to the BorderManager private IP address.

The use of a 255.255.255.252 subnet mask on the public IP subnet is quite limiting in that you can only assign one IP address to the BorderManager public interface. Without having additional IP addresses to assign to the public interface, you cannot make use of static NAT. However, the BorderManager proxies can all share the single primary public IP address.

Not having another public IP address to assign on the public IP subnet also means that you cannot place a PC on the public subnet for testing purposes, at least not without taking the place of the Internet router.

Scenario 2 - A Cable Modem with DHCP Connection

In this scenario, the Internet connection is provided via cable modem with a DHCP-assigned address. The concept would be very similar if a PPPoE connection to the ISP were required. In both cases, a small router is used to make the connection to the ISP instead of a NetWare server. The reasons are:

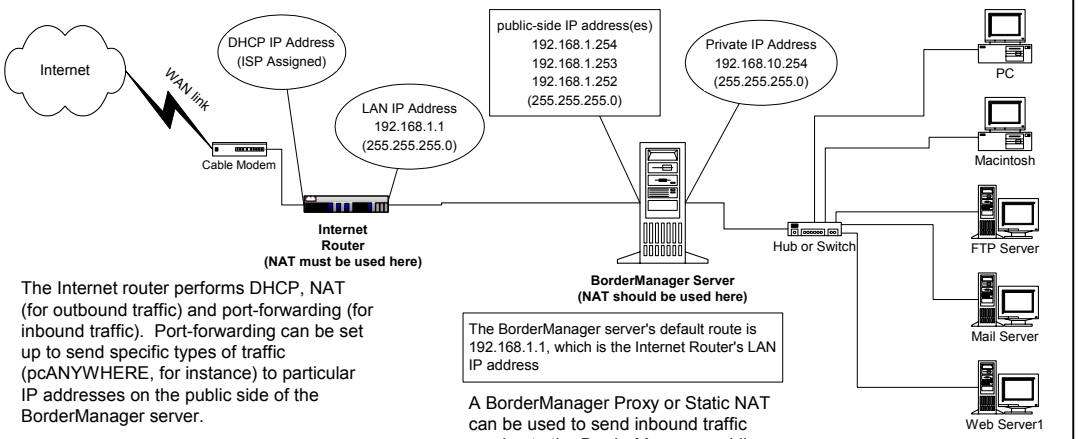
- NetWare used to not do DHCP well, the filter exceptions required for getting DHCP to work can be confusing, and if the IP address changes, the filters also have to change. A separate router is used for DHCP connectivity just to simplify life here.
- NetWare does not support PPPoE, so a separate router is used to provide the WAN link using PPPoE.

A Cable Modem (or PPPoE) Configuration

Example
An organization's public network, assigned by the ISP, has a DHCP-assigned address, and only one public IP address will be allowed by the ISP. This scenario can also apply if PPPoE is used on the Internet router. A small router is used for DHCP/PPPoE connections to the ISP.

A Class C Private IP network (192.168.10.x) is in use on the internal LAN, and 192.168.10.254 is assigned to the BorderManager private interface. Up to 254 IP addresses can be assigned on the internal LAN. Another private IP address (192.168.1.254) is assigned on the Internet side of the BorderManager server, and some secondary IP addressses for use by static NAT or proxies.

NOTE: VPN cannot be used on the BorderManager server in this scenario. (NAT on the Internet router prevents inbound VPN).



The Internet router performs DHCP, NAT (for outbound traffic) and port-forwarding (for inbound traffic). Port-forwarding can be set up to send specific types of traffic (pcANYWHERE, for instance) to particular IP addresses on the public side of the BorderManager server.

The main advantage of this scenario is to allow a cheap router to do DHCP, or PPPoE, which NetWare does not do well, or does not do at all.

The BorderManager server's default route is 192.168.1.1, which is the Internet Router's LAN IP address

A BorderManager Proxy or Static NAT can be used to send inbound traffic coming to the BorderManager public-side IP addresses to an internal FTP server, Mail server or Web server, depending on the type of traffic.

All these internal hosts have a 192.168.10.x IP address, and a default gateway of 192.168.10.254, which is the BorderManager server's private IP address

The BorderManager server is set up in a two-interface configuration with one interface labeled as Public and the other as Private. The public interface is connected to a router connected to the Internet. The private interface is connected to an internal LAN by way of a 10/100 switch or hub.

In the sample configuration shown, any number of IP addresses can be assigned to the BorderManager public interface. However, those

addresses may be of limited use, since inbound connectivity in this scenario is problematical. If DHCP is used on the WAN link, it normally means an IP address could change, affecting inbound connections. DHCP also is typically associated with ISP's that do not allow public servers to be used on that link, such as web servers, mail servers or VPN servers. Nevertheless, it can be useful to have generic proxy or static NAT capability on the BorderManager server if only to support inbound pcANYWHERE connections to an internal PC.

There are two keys to this scenario.

- The Internet router must be performing NAT in order for the BorderManager server or internal LAN to have Internet access.
- If any kind of inbound traffic is desired, the Internet router must be performing some kind of port forwarding. Some routers have a 'DMZ' function, whereby all inbound traffic can be forwarded to one internal IP address, which would be the BorderManager public IP address. Port forwarding allows you to be more specific about the type of traffic allowed in, and where the traffic is forwarded. For instance, pcANYWHERE traffic could be forwarded to one IP address, and static NAT'd to an internal PC. At the same time, VNC could be forwarded to a different internal address, and static NAT'd to a different internal PC.

There is also one limitation to this scenario – the BorderManager server will not be able to host VPN services. VPN on BorderManager up through BorderManager version 3.7 cannot function when the BorderManager server is behind a NAT connection.

In this scenario, both the Internet router and the BorderManager server are doing NAT. The BorderManager server could be using either Dynamic, Static, or Dynamic and Static NAT. If the BorderManager server is NOT using dynamic NAT, then the Internet router would normally have to be set up with a static route for the internal subnet 192.168.10.0, with a next hop of 192.168.1.254.

The public-side IP address on the BorderManager server could be configured with BorderManager's reverse proxy acceleration or generic proxies to make internal hosts available to the Internet. (This, and other capabilities, is explained later in this book.) The BorderManager server could also be set up with static NAT to forward any kind of inbound traffic to particular internal hosts. In general, static NAT is explained in my book "*Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions*", and not in this book.

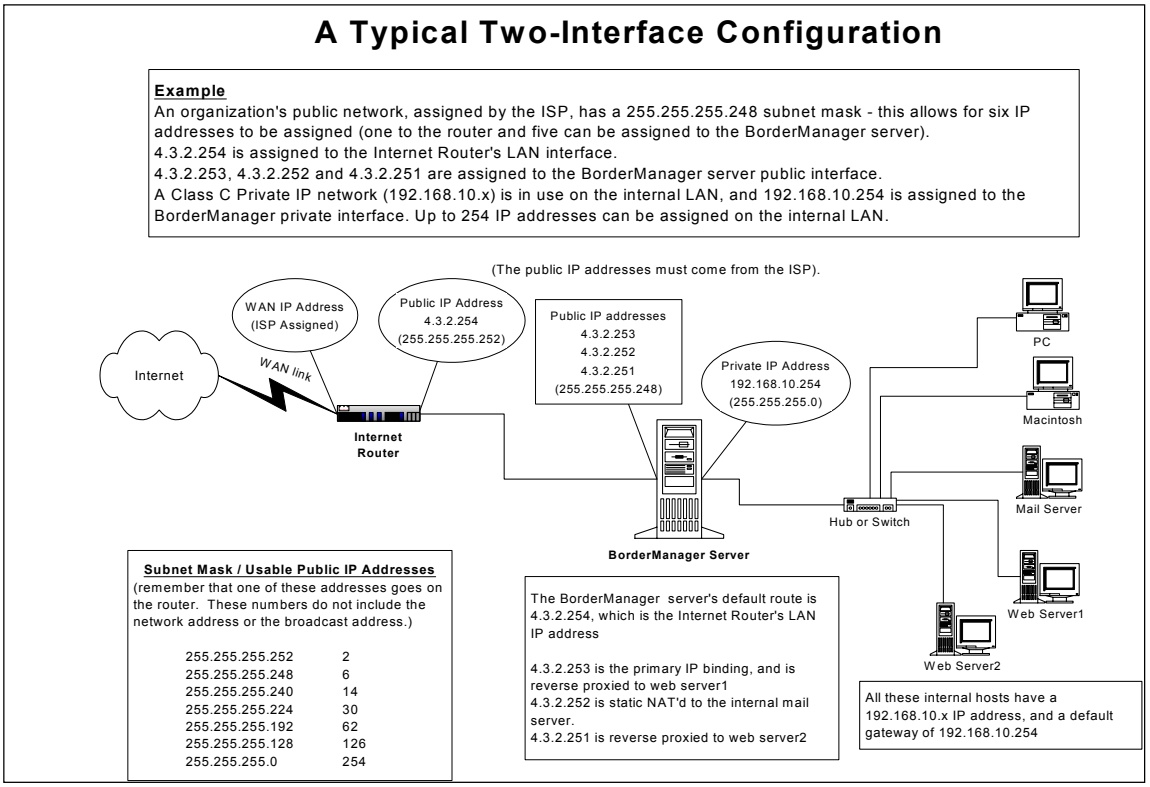
The BorderManager server has a default route set up with the IP address of the LAN interface of the Internet router.

The internal IP addresses are the same as in the previous example – up to 254 hosts can be on this subnet without an additional router, including the BorderManager private IP address.

The internal hosts should all have a default gateway configured that is equal to the BorderManager private IP address.

Scenario 3 - Multiple Public IP Addresses

In this scenario, more than one IP address is assigned to the BorderManager public interface. The public IP address subnet mask is 255.255.255.248, which allows 6 useable IP addresses, 5 of which can be assigned to the BorderManager public interface.



The primary public IP address is configured to reverse proxy accelerate an internal web server to make it available to the Internet. In addition, an internal FTP server could also be reverse proxied to the same public IP address (as in the previous example).

A second public IP address has been assigned to the BorderManager public interface and configured with Static NAT and packet filter exceptions to pass SMTP mail traffic to an internal mail server. (Experience has shown that using Static NAT is more reliable than using the Mail Proxy. Static NAT cannot be configured on the primary public IP address, so this option is not available in the simple scenario shown earlier.)

A third public IP address has been assigned to the BorderManager public interface and configured with BorderManager reverse proxy acceleration to allow another internal web server to make it available to the Internet. This internal web server could not be reverse proxied to the main public IP address because another internal web server has already been reverse proxied to that IP address.

The remaining public IP addresses are available to assign to the BorderManager public interface for additional static NAT or proxy uses.

One excellent use for a public IP address is to put a PC on the public side of the BorderManager server to use for testing.

The BorderManager server has a default route set up with the IP address of the LAN interface of the Internet router.

The internal IP addresses are the same as in the previous example – up to 254 hosts can be on this subnet without an additional router, including the BorderManager private IP address.

The internal hosts should all have a default gateway configured that is equal to the BorderManager private IP address.

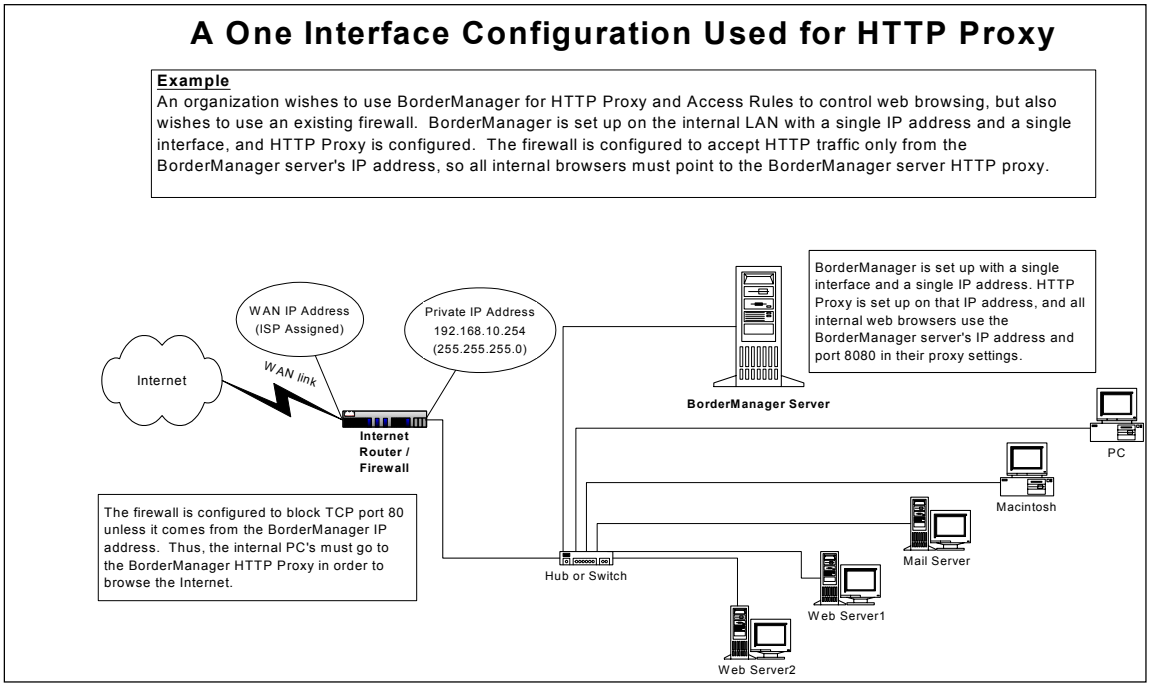
With additional public IP addresses available on the BorderManager server, you can configure more than one reverse web proxy. You cannot have two services (like reverse proxy) listen on the same IP address with the same port number at the same time. For example, if you are reverse proxying an HTTP web server (on TCP port 80) on public IP address 4.3.2.253, you cannot set up a second reverse proxy listening on TCP port 80 on the same IP address. But you can set up a second reverse proxy listening on TCP port 80 on a secondary public IP address 4.3.2.251.

You can reverse proxy two different internal servers to the same public IP address as long as the proxies listen on different port numbers. For example, the same public IP address could reverse FTP Proxy internal server number one for FTP (listens on port 21) and reverse HTTP Proxy internal server number two for HTTP (listens on port 80).

You can have many secondary IP addresses configured on a single interface. I met one person at BrainShare 2000 who had over 200 IP addresses assigned on a single interface without problems.

Scenario 4 - BorderManager Used Only For HTTP Proxy

In this scenario, BorderManager has been installed behind an existing firewall, and is only being used for the HTTP Proxy. In order to prevent users from bypassing the HTTP Proxy, the firewall has been configured to accept HTTP packets only from the BorderManager IP address. In this example, only one network interface is present in the BorderManager server.



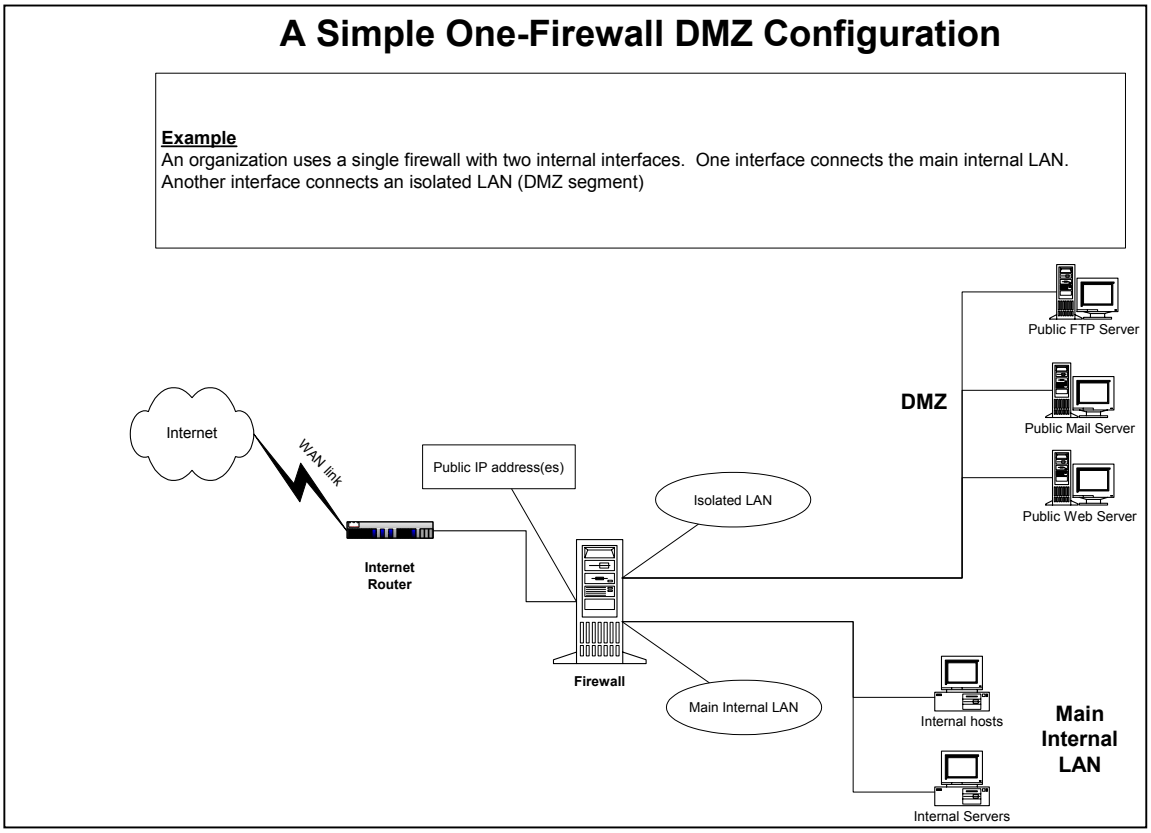
BorderManager can be set up using any internal IP address, and configured with the HTTP Proxy. No IP addressing on the internal side needs to be changed.

The internal hosts must have their browsers configured with the BorderManager server's IP address and HTTP Proxy port (usually 8080).

TCP port 8080 traffic will come to the BorderManager server HTTP proxy, and the BorderManager server will then use standard HTTP (TCP port 80) to access web servers. Because only the BorderManager server's IP address is allowed through the firewall, all internal users have to use the HTTP Proxy (and associated access rules) in order to browse the Internet.

Note that additional port numbers besides TCP port 80 will have to be opened on the firewall in most cases. HTTPS (TCP port 443) will almost certainly have to be allowed, and some web servers are set up to redirect web browsers to non-standard port numbers.

Scenario 5 - A Single Firewall (3-NIC) DMZ Segment



This scenario is shown only to explain some concepts involved – it is not covered in any other segment of this book, or the book "Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions". Setting up a DeMilitarized Zone (DMZ) is out of the scope of this book.

In this scenario, some servers are made available to the Internet from behind a BorderManager server, but are hosted on an isolated private network segment (the DMZ). Should the servers on the isolated segment be compromised in some way, the traffic from that segment must still pass through a firewall in order to get to the main internal LAN segment. This scenario uses only a single firewall.

The isolated (DMZ) segment is essentially the same as in the previous scenarios where a server is made available to the Internet via reverse proxy or static NAT and packet filter exceptions. There are only two differences:

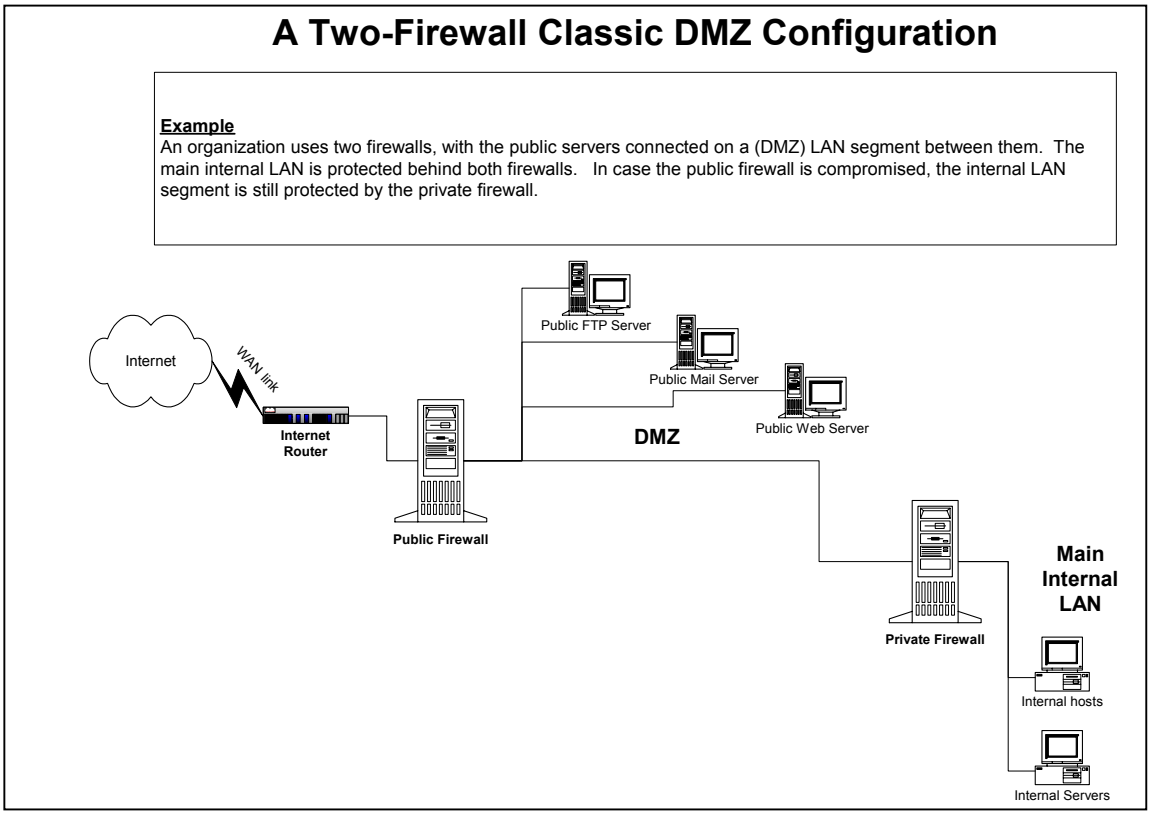
1. The only devices on the isolated segment are servers designed to be available to the Internet, and those servers are (generally) not supposed to be used for internal file & print services.
2. The isolated segment is isolated from the other internal segment(s) by means of packet filters.

The key to this design is to set up custom packet filters to block all traffic between internal segments, and then add custom packet filter exceptions to allow only the desired traffic. In this way, some extra protection can be obtained over putting the publicly-available servers right into the main internal LAN. Should an intruder somehow take control over a server in the isolated segment, very little traffic would be allowed from that server back to the main internal LAN. An example would be to allow only HTTP and FTP traffic to pass from the main internal LAN segment to the isolated LAN segment, and perhaps even then only from selected IP addresses, by using stateful packet filter exceptions.

This book will not attempt to explain the details of accomplishing the packet filtering. However, the concept would be to copy the default packet filters that block traffic to and from the public interface to packet filters that would block traffic to and from the isolated LAN segment. Then add packet filter exceptions as desired to allow only the barest minimum of traffic between the isolated LAN segment and any other internal LAN segment(s).

Scenario 6 - A Classic Two-Firewall DMZ

As with the previous scenario, this book will not attempt to explain how to configure BorderManager to serve as a firewall for a DeMilitarized Zone (DMZ), but instead only explains the concept. Setting up a DMZ is out of the scope of this book.



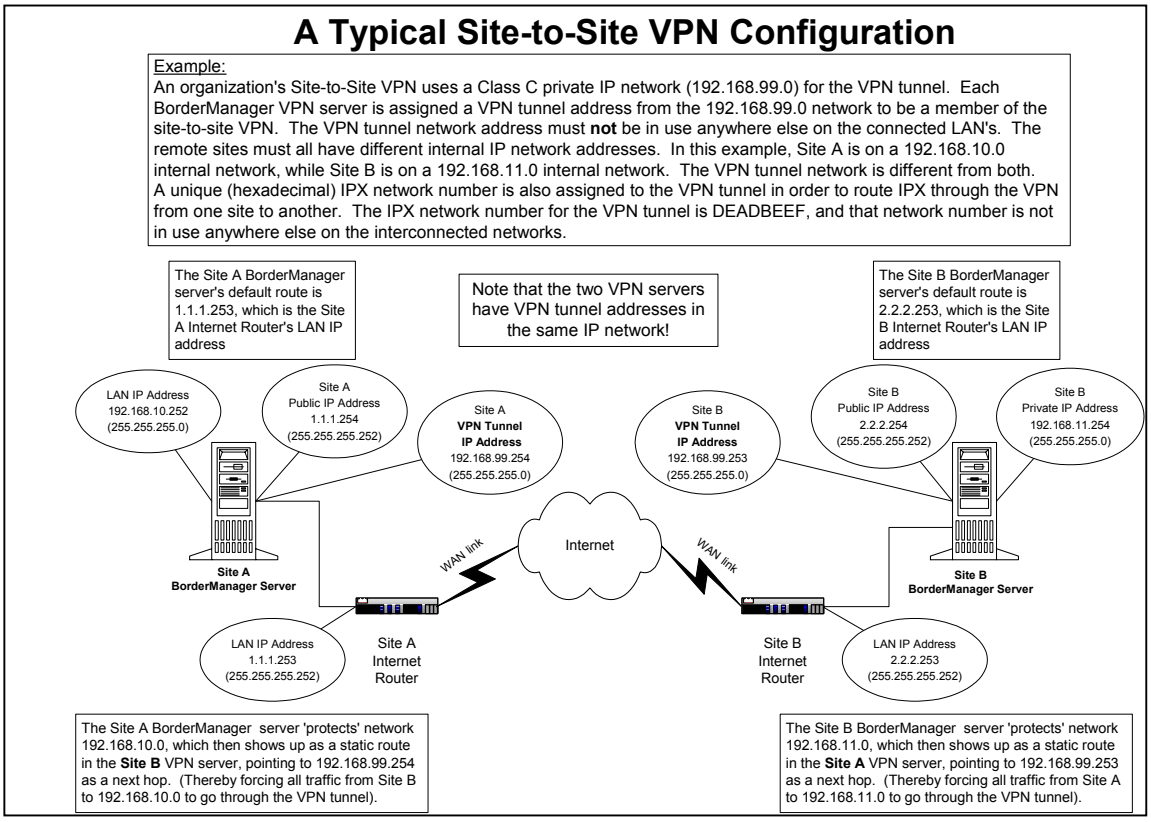
In this scenario, servers designed to be available from the Internet are placed in a segment isolated between two firewalls. This design is much the same as in the previous scenario except that two firewalls are used instead of one. The first (more public) firewall allows only selected inbound traffic from the Internet through packet filter exceptions and proxy services. The second (more internal) firewall allows even less traffic through to the Internal LAN, and it also allows some internal traffic outbound to update the isolated servers.

This scenario provides additional security to the internal LAN in case the public firewall itself is compromised.

Filters and packet filter exceptions would be necessary on each firewall, and proxies might be used at both or either firewall.

Scenario 7 - A Simple Site-to-Site VPN

This scenario shows a very simple site-to-site BorderManager VPN. Two BorderManager 3 servers are connected over the Internet by using a VPN "tunnel". All IP and IPX traffic between the two sites is encrypted and placed inside IP packets when being transmitted over the Internet links so that the data cannot easily be deciphered. Once the data arrives at the other end of the VPN link, the BorderManager server decrypts the data and routes it to the local internal LAN. This scenario can (and often is) combined with one or



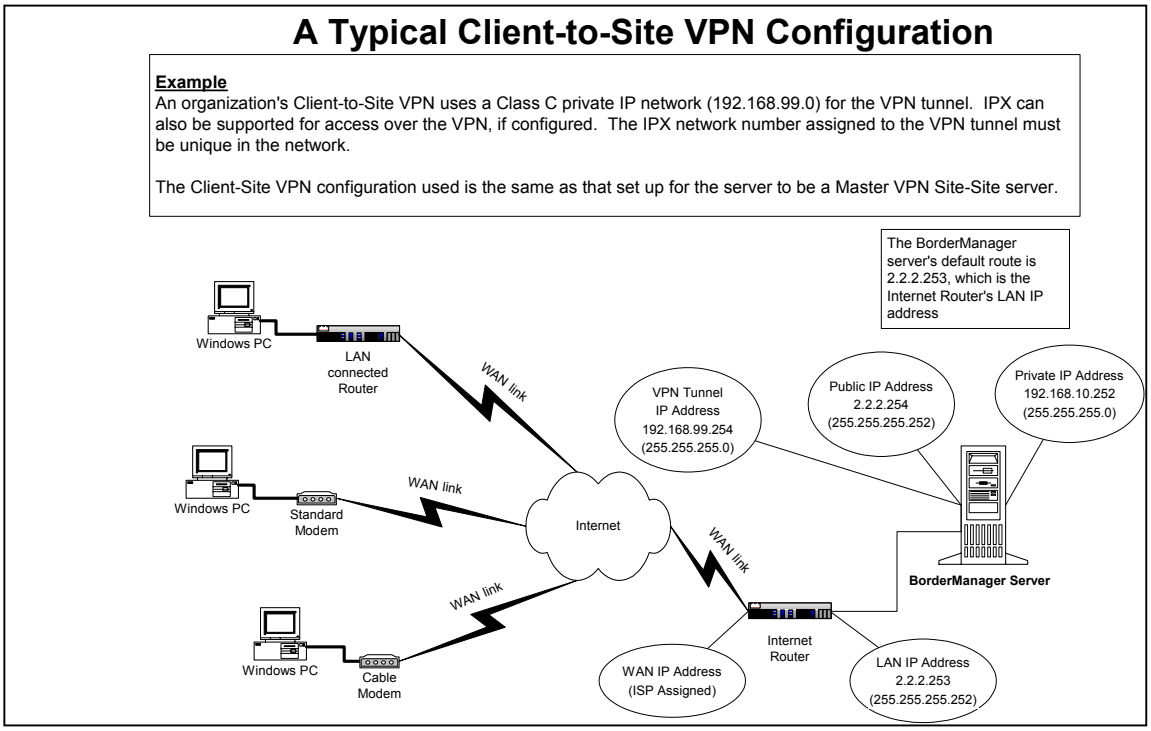
more of the other scenarios.

A VPN tunnel is a routed solution, with the VPN tunnel itself looking like a separate IP and/or IPX network. Because of routing considerations, the VPN tunnel IP network address and IPX network number must be unique and not used anywhere else on either LAN connected to the VPN.

IPX can also be tunneled across a VPN connection, and the same routing rules apply. The VPN tunnel must have an IPX network number that is not in use anywhere on the connected networks, and the connected networks must also have unique IPX network numbers.

Scenario 8 - A Simple Client-to-Site VPN

In this scenario, the BorderManager server has been configured for a client-to-site virtual private network. A windows PC running Novell's VPN client software can make a local Internet connection and then establish a secure, encrypted link to a BorderManager server located virtually anywhere in the world. The remote client can use a dial-up connection, a cable modem, or a LAN connection, though certain restrictions apply. This scenario can (and often is) combined with one or more of the other scenarios.



A Client-to-Site VPN makes it look like the remote hosts are directly connected to the internal LAN, though the speed is generally MUCH slower, especially if the remote host is using a modem connection.

NDS-based access rules control who gets access into the LAN over a VPN connection. Once the user is connected to the LAN through the VPN, the access rules do not apply any more. The user is then free to access any TCP/IP or IPX-based services on the LAN, subject only to controls on those services, such as a login requirement to a NetWare server, or a user ID and password requirement to an FTP server.

Scenario 9 - Complex Multiple BorderManager Server Environments

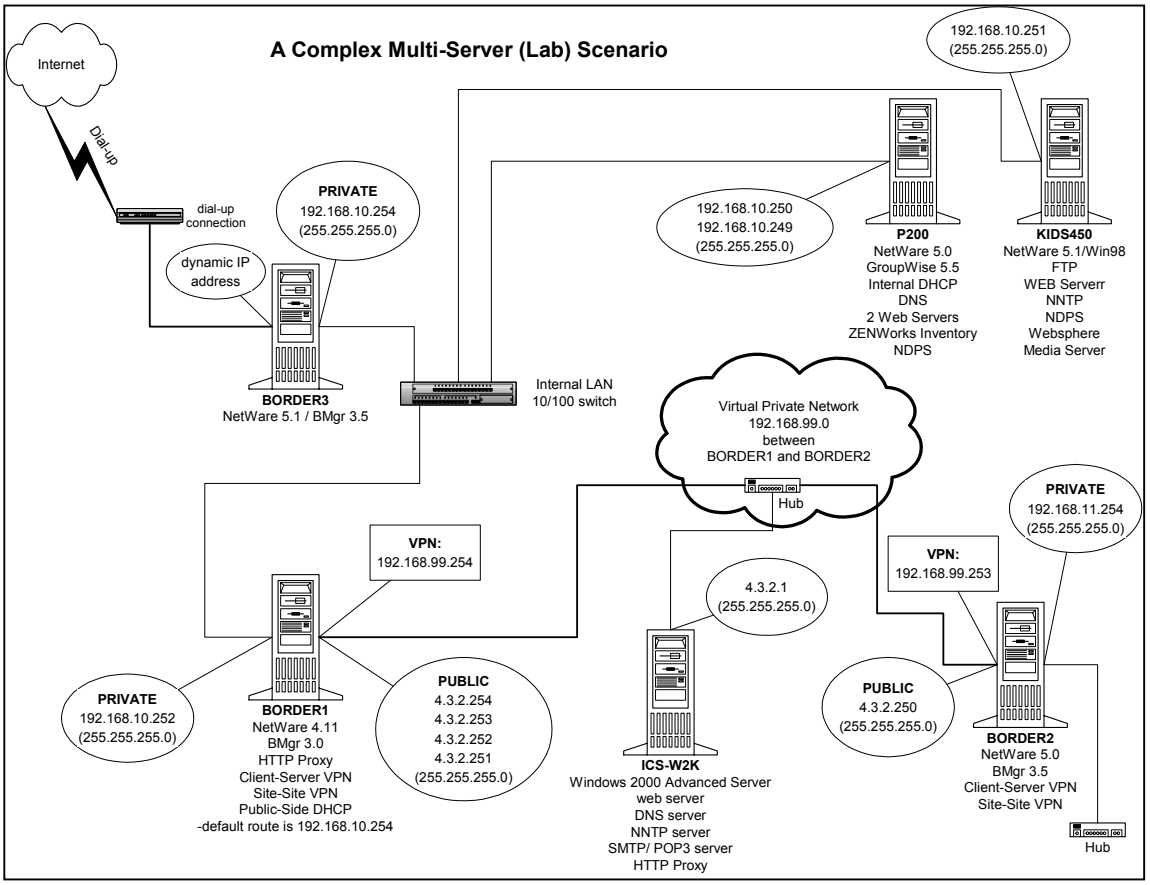
I show two environments here, which are probably too complex for most readers to worry about. The first one shows the test network I used to do most of the screenshots and examples in the first two editions of my book. It was useful for some people to try to trace back through the addressing to see how the servers were interconnected. However, as I added new servers and upgraded old one, the scenario was completely outdated. Nevertheless, some of the examples in the book are still based on these servers and addresses.

I keep the old scenario here for reference. I added a newer version to show how the test network is currently laid out, mostly to show any readers who are interested how things can be interconnected in a fairly complex way. It may be useful for those who want to trace through how I set up the BorderManager 3.8 site-site VPN. It may also be of use for those who wonder how you might set up a test network behind a cable modem – all of the servers and workstation in the test network have internet access.

Please don't worry about these scenarios too much if they seem too complex to follow. They are not essential to understand how BorderManager works, but are only here for completeness. I give descriptions of some of the major features of the scenario that I have used in writing this book after each diagram.

Scenario 9A – The Original Network

This (older) scenario, which is actually how my home network used to be set up, is useful for testing and showing a number of complicated configuration options. Some of the examples in the book are built around this configuration.



The BorderManager server BORDER1 is a two-interface configuration. The public interface is connected to a hub. The private interface is connected to a switch.

The BorderManager server BORDER2 is a two-interface configuration. The public interface is connected to the same hub as the public interface of BORDER1. The private interface is connected to another hub.

The BorderManager server BORDER3 is a two-interface configuration with one interface consisting of an ordinary external analog modem. BORDER3 is configured to dial up to an ISP and make an internet connection on demand.. The private interface is connected to the same switch as the private interface of BORDER1.

In the scenario shown, there is a site-to-site VPN connection between BORDER1 and BORDER2, although that connection is not

actually connected to the Internet. The BORDER1 server is using a default route pointing to the BORDER3 server, which has an Internet connection. A CERN cache hierarchy is being used between BORDER1 and BORDER3. BORDER2 can also reach the Internet by going across the Site-to-Site VPN link to BORDER3.

BORDER1 uses BorderManager 3.0 software installed on a NetWare 4.11 server, while BORDER2 uses BorderManager 3.5 software installed on a NetWare 5.0 server. BORDER3 is using BorderManager 3.5 software running on NetWare 4.11.

All of the NetWare servers except BORDER3 are installed in the same tree. The BORDER3 server acts as a CERN proxy to the rest of the network.

The BORDER1 and BORDER2 servers simulate an Internet connection (4.3.2.0 network) and establish a site-to-site VPN. Workstations and other servers are placed on the 4.3.2.0 network to test inbound and outbound connectivity.

The P200 server at IP address 192.168.10.250 is supplying internal DNS and DHCP services to the 192.168.10.0 network.

Multiple public IP addresses are assigned to the public interfaces of both BORDER1 and BORDER2, with some used in a static NAT configuration, and others used for reverse proxy acceleration.

Internal web servers, an FTP server and a SMTP mail server are shown as they will be used in some examples later in the book.

A server called ICS-W2K exists at IP address 4.3.2.1 (on the 'public' side of BORDER1 and BORDER2). This server runs DNS, FTP, HTTP, NNTP, POP3 and SMTP and is used to test inbound and outbound proxy and static NAT access through BORDER1. This server simulates the Internet for the purposes of testing Proxy services in most of the examples in this book

This scenario shows that you can come up with some creative ways to make things work. The dial-up connection is actually used by BORDER1 and BORDER2 through a cache hierarchy that sends all HTTP requests to BORDER3. BORDER3 is not even in the same NDS tree as BORDER1 and BORDER2, which shows that BorderManager services are not all NDS-dependent.

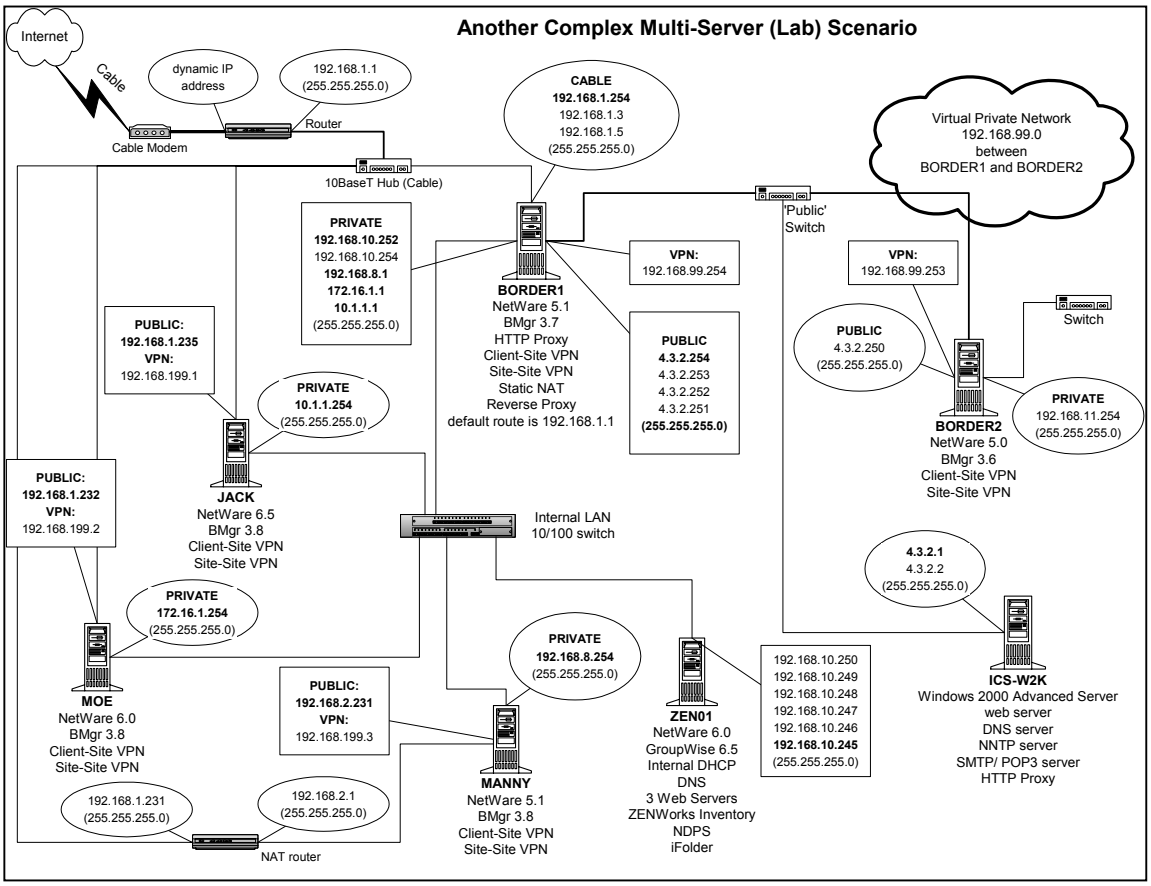
Note This is not a typical BorderManager installation scenario. I use it here for various reasons, one of which is that it allows me to show how an HTTP Caching Hierarchy works.

BorderManager Server IP Addressing

Server	Component	IP Addresses	Functions
BORDER1	PUBLIC Interface	4.3.2.254	Site-to-Site VPN, Client-to-Site VPN
		4.3.2.253	Reverse Proxy
		4.3.2.252	Reverse Proxy
		4.3.2.251	Static NAT
		4.3.2.247	Reverse Proxy
		192.168.99.254	VPN Tunnel IP address
BORDER1	PRIVATE Interface	192.168.10.252	Various proxies, default route for 192.168.10.0 network
BORDER2	PUBLIC Interface	4.3.2.250	Site-to-Site VPN, Client-to-Site VPN
		4.3.2.249	Reverse Proxy
		192.168.99.253	VPN Tunnel IP address
BORDER2	PRIVATE Interface	192.168.11.254	Various proxies, default route for 192.168.11.0 network
BORDER3	PRIVATE Interface	192.168.10.254	CERN Proxy, default route for BORDER1
BORDER3	PUBLIC Interface	Dial-up interface (modem)	Internet connection

Scenario 9B – The More Current Network

This scenario, which closely describes my current test network, consists of a lot of servers and networks in a very confined space. In fact, I have all of the servers on or under a single table in my office. Even better, the network diagram doesn't show the Linux servers that are also in place!



This network started out from the previous one, but the dial-up connection was replaced by a cable modem, the BorderManager and NetWare servers were upgraded (and one was retired), and three new BorderManager 3.8 servers were added for site-site VPN testing.

The network here connects to the switch shown in the center of the diagram, and consists of the 192.168.10.0 network. Not shown are several workstations that connect to that network with either fixed IP addresses or DHCP. Also not shown are two Linux servers.

The only network access is via a cable modem with a single public IP address, and that address is assigned via DHCP from the ISP. When the cable modem was first installed, I was unable to get NetWare to reliably renew the address, resulting in address changes, resulting in me having to redo my filter exceptions five times in two weeks. I soon tired of that and inserted a small router between the

cable modem and the rest of the network. This router (a Linksys) has been very reliable. I have heard that Novell has fixed the problems with DHCP assignments to a NetWare server, but I find a number of advantages to using the Linksys router between the cable modem and my network. For one thing, my BorderManager server addresses never change anymore, and I don't have to worry about changing filter exceptions. I have found that I can do everything I need to do with this configuration, except legacy VPN from the Internet. The Linksys router does dynamic NAT for outbound traffic. (Linksys calls this 'Gateway mode').

Behind the Linksys router connected to the cable modem is a 'public' subnet that I actually call the Cable subnet. This subnet uses the 192.168.1.0 network address, and I have up to four BorderManager and two Linux firewalls connected to it. My primary firewall is BORDER1, which has IP address 192.168.1.254 assigned as the primary IP address on an interface called CABLE.

BORDER1 has three interfaces, called CABLE, PUBLIC and PRIVATE. CABLE connects to the Internet via Linksys router to the cable modem. The PRIVATE interface connects to my main internal switch, where my ZENWorks/GroupWise/etc. server and workstations reside. The PUBLIC interface actually doesn't connect to the Internet at all, but it used for simulating an Internet connection for testing and filtering screenshots. The PUBLIC network is 4.3.2.0 (class C subnet of 255.255.255.0 – all my subnets are class C). The PUBLIC primary IP address is 4.3.2.254. BORDER1 has a VPN tunnel address of 192.168.99.254. BORDER1 is a BorderManager 3.7 server running on NetWare 5.1. BORDER1 is a VPN master server. BORDER1 also has three additional primary IP bindings on the private interface, which are only used for convenience in configure BorderManager 3.8 VPN servers. The addressing and routing concepts are explained in more detail below, when I describe the MANNY, MOE and JACK VPN servers.

On the PUBLIC subnet, I have a permanent Windows 2000 server called ICS-W2K (which simulates Internet servers for various tests), and the public interface of the BORDER2 server. Most of the time this server does nothing but crunch SETI@HOME data…

BORDER2 exists primarily for legacy Site-to-Site VPN testing, and it consists of BorderManager 3.6 running on NetWare 5.0. BORDER2 is a VPN slave server. I have a small 4-port switch attached to the private interface of BORDER2, to test end-end connectivity across the Site-to-Site VPN. BORDER2 has a public primary IP address of 4.3.2.250, and a private IP address of 192.168.11.254. BORDER2 has a VPN tunnel IP address of 192.168.99.253. BORDER2 can only access the Internet via a cache hierarchy, with the parent cache on BORDER1, and suitable access rules to allow HTTP Proxy access.

ZEN01 is a NetWare 6.0 server with only one interface located in the private LAN subnet, and it runs just about every Novell product except BorderManager. In this book, it is hosts web sites accessed by reverse proxy, and some other features, such as internal DNS. It has a primary IP address of 192.168.10.245, and several secondary IP addresses used for web sites and iFolder.

BORDER1, BORDER2 and ZEN01 are all in the same NDS tree.

That brings us to the three BorderManager 3.8 test servers, and the odd IP addresses in use. These servers are named MANNY (NetWare 5.1), MOE (NetWare 6.0) and JACK (NetWare 6.5). All three run BorderManager 3.8, in a Site-to-Site VPN, and all three were used extensively in BorderManager 3.8 beta testing.

MANNY, MOE and JACK are each in their own NDS trees.

JACK is the VPN Master for the BorderManager 3.8 Site-to-Site VPN. MANNY and MOE are each slave VPN servers.

JACK has a primary 'public' IP address of 192.168.1.235. (The 192.168.1.0 subnet can connect directly to the Internet by going out through the Linksys router at 192.168.1.1). JACK has a primary private IP address of 10.1.1.254. The private interface is connected to the main private LAN switch.

MOE has a primary 'public' IP address of 192.168.1.232. MOE has a primary private IP address of 172.16.1254. The private interface is connected to the main private LAN switch.

MANNY is a bit different. MANNY actually started out on the 192.168.1.0 network, but I inserted a small router between the 192.168.1.0 network and MANNY's 'public' IP address in order to test BorderManager 3.8 VPN with the server behind a NAT connection. (Which works fine, by the way). MANNY has a primary 'public' IP address of 192.168.2.231. MANNY has a primary private IP address of 192.168.8.254. The private interface is connected to the main private LAN switch. MANNY's default route points to the small router at IP address 192.168.2.1. That small router has a 'public' IP address of 192.168.1.231. The other BorderManager 3.8 servers connect to MANNY by pointing their VPN connections at 192.168.1.231, and the small router does port forwarding here to forward the data to MANNY. The configuration for this is shown in the BorderManager 3.8 VPN chapter.

The IP addressing on the private side needs explanation. In order to configure a VPN server, you must of course be able to communicate with the server. Generally this means communicating on the private interface. I could have set up three more private switches or hubs, and moved a laptop or PC back and forth to do the configuration, but that was quite inconvenient. Instead, I chose to do some creative routing. My goal was to be able to use one of the PC's on my private (192.168.10.0) network to configure iManager settings on all

three servers. At the same time, I could not have the servers communicating to each other over TCP/IP on the private interfaces. I needed to ensure that the Site-to-Site VPN I was configuring was the only possible communication link between private interfaces of each of these servers. (That is, if I could ping 172.16.1.254 from JACK, I had to know that the traffic only got there by way of a successful VPN connection). To achieve these goals, I added the network addresses 192.168.8.1, 172.16.1.1, and 10.1.1.1 to BORDER1 on the private interface. Next, I disabled RIP on MANNY, MOE and JACK. Then I added a static route on JACK, for network 192.168.10.0, with a next hop of 10.1.1.1. This allowed JACK to communicate with any host on the 192.168.10.0 network, but not to communicate with 172.16.1.0 or 192.168.8.0 networks (MANNY and MOE). On MOE, I added a static route to 192.168.10.0 with a next hop of 172.16.1.1, and on MANNY, I added a static route to 192.168.10.0 with a next hop of 192.168.8.1.

Thus, my PC, which has a default gateway pointing to BORDER1, can route packets to the private interfaces of MANNY, MOE and JACK, while those servers cannot directly contact each other's private IP address. This made it very easy for me to go back and forth between each VPN server and do the required iManager configuration.

Once I got Site-to-Site VPN, MANNY, MOE and JACK could ping each other's private IP addresses, via the VPN link.

It may comfort you to know that the network is complicated enough for me that I have resorted to labeling the IP addresses on all the servers, creating diagrams for the network, network jacks and switch ports, and attempting to color code the patch cables to know what is connected where.

If you've read this far, you must be a geek like me…

Some Rules of Thumb and Words of Wisdom

I wanted to put this section in to start clearing up some confusion and misconceptions that people often have about BorderManager. These are just miscellaneous comments that should be investigated closely by the reader if any of them seem to be surprising.

- Do NOT use all available space on the NetWare server for NSS pools when configuring NetWare. ALWAYS leave some free space for a traditional NetWare partition so that you can configure a traditional volume dedicated for HTTP Proxy caching. If you have no idea how much space to leave available, use 4GB.
- Basic routing to the Internet should be working before installing BorderManager.
- You need to have a default route set up.
- You do not need to use IP/IP or IPX/IP Gateway in order to control user access with Access Rules. In fact, those gateways are not supported, don't work with the newest versions of Client32, and should not be used.
- You do not have to use the Mail Proxy to send outbound email. You can use dynamic NAT and filter exceptions instead.
- If you want to make use of the Mail Proxy to receive mail and proxy it to an internal mail server, BorderManager 3.8 can now accept mail to multiple domains, but you must configure the domains to accept in the PROXY.CFG file.
- The NNTP Proxy will only proxy traffic to a single external NNTP server.
- The NNTP Proxy does not cache NNTP traffic. (In fact, only the HTTP and FTP Proxies cache any traffic).
- There are very few practical differences between BorderManager 3.0 and 3.5. There are almost zero differences between BorderManager 3.5 and 3.6. The biggest difference between BorderManager 3.5 and 3.6 is the ability to use Client-to-Site VPN over NAT. BorderManager 3.6 also contains a more robust version of RADIUS.NLM. BorderManager 3.7 adds a web-enabled capability to configure filter exceptions, and saves IP packet filters and exceptions in NDS. BorderManager 3.7 also can use a new SurfControl content-filtering solution, which replaces the CyberPatrol product used in previous versions. BorderManager 3.8 adds to the capability of 3.7 and includes tremendous differences in VPN capability.

- BorderManager licenses do not enforce a user count. All BorderManager licenses, except MLA licenses, will show 'Installed Units: 1', but this does not limit the number of users.
- BorderManager Alerts, at least up through version 3.8, are not very extensive. However, they should be configured as this is the primary means for BorderManager to notify someone of problems.
- The Indexed and Access Control log file is only stored on the SYS volume, and can become quite large. Be judicious in using this logging capability.
- Access Rules are read from the top to the bottom, and the first one which 'matches' is the only one that is used.
- Access Rules based on a source of NDS user, group or container are ignored if proxy authentication is not enabled, or if the user is not proxy authenticated by some means. The user will instead be affected by some other access rule NOT based on an NDS user, group or container, including the default rule. (Does not apply to legacy VPN).
- Access rules based on group memberships are not dynamic. If a member is added or subtracted from a group, the access rule may not 'refresh itself' for up to an hour. If you want a group membership change to be immediate, click on the Refresh Server button in the Access Rules menu.
- With the exception of the IP/IP and IPX/IP Gateways, you can really only use NDS-based sources in Access Rules for HTTP Proxy, Transparent (HTTP) Proxy, FTP Proxy, and Transparent TELNET Proxy.
- You must have packet filter exceptions to allow the Proxies to work. The default packet filter exceptions are designed to allow some of the proxies, and the VPN, to work.
- Site-to-Site VPN requires RIP filters to be working in order to function properly. This has to do with packet filtering of routing protocols. Site-to-Site VPN will eventually fail if filtering is disabled, unless RIP is also disabled.
- BorderManager default packet filters block ICMP (including PING) packets at the public interface.
- You can get BorderManager to work with a dial-up interface, including a simple analog modem with dynamically assigned IP address, though this is mostly useful only in a lab situation.
- You cannot set up a BorderManager server to split traffic out through two public WAN links. Inbound traffic can come in from multiple WAN public links, but all of the

outbound traffic must use the same (default) route. Actually, I lied a bit there. Site-to-Site VPN can fairly easily make use of a particular public WAN link, as can BorderManager 3.8 client-site VPN, but those are special cases.

- You cannot set up more than one default route. However, there are versions of TCPIP.NLM that provide Dead Gateway Detection, which can allow some limited ability to detect a failed default route and switch to a backup.
- You can use Proxies and dynamic NAT on the same server AND on the same IP address just fine. You cannot use Proxies and Static NAT on the same public IP address at the same time.
- Don't try to set up Static NAT on the primary public IP binding as it will kill BorderManager communications.
- Static NAT is essentially only used for inbound connections to devices on the LAN to be accessed from the Internet. My book on configuring BorderManager filter exceptions includes many examples of static NAT.
- Don't try to set up NAT on a single interface server as it will quickly result in ARP table issues and communications will stop.
- Expect NLS licensing problems at some point. But don't give up, because those problems can always be overcome.
- A properly configured BorderManager server is very fast, assuming you have adequate RAM and have tuned it for performance. If the server seems slow, something is wrong. See Novell TID 10018669 or tip number 23 at http://www.craigjconsulting.com/.
- Don't just 'make up' IP addresses for your internal LAN. If you don't know what you are doing, pick one of the following network addresses, and use a 255.255.255.0 subnet mask: 10.x.x.x, or 172.16.x.x through 172.31.x.x, or 192.168.x.x. These are private IP networks that anyone is allowed to use. But avoid using 192.168.0.0, 192.168.1.0, 172.16.0.0 or 10.0.0.0, because it is likely those addresses will be used in other networks, and it will make VPN connections more difficult to achieve if there is address duplication.

Chapter 3 - Installation

Server Hardware Suggestions

The hardware needed to install BorderManager 3.x can vary widely depending on what else you might want to install on the server, the number of users going through it, the speed of the Internet connection, the amount of disk cache required, and other factors.

Here are some guidelines and a starting point for a typical BorderManager server, running proxies and VPN, with T1 (1.5Mbps) Internet connection speed, servicing 250-500 users. These are my recommendations, and not Novell's recommendations. You can certainly install and run a BorderManager server on much less hardware than I list below, but I would recommend doing that only for a test environment.

1. **Minimum Recommended RAM**: For versions prior to BorderManager 3.7, 384MB, but 512MB or more is preferred. You can run a server on less, but it will not perform well. 256MB is a good minimum for even small installations, with less than 100 users. For BorderManager 3.8: 512MB minimum. For BorderManager 3.7 or 3.8 with SurfControl: 1GB absolute minimum. More is better, but over 2GB is probably not very useful except in the most extremely busy servers.
2. **CPU**: Pentium-II 350 or faster CPU. Not a problem with modern hardware. Older servers may benefit from even more RAM if using slower processors. Multiple processors are not used with BorderManager 3.x, and not supported at all if using NetWare 4.11 with BorderManager. CPU power becomes much more significant when using VPN connections. If you plan on having a lot of VPN clients, you should get the fastest CPU you can in the server.
3. **Network Card**: 100Mbps or faster Ethernet card for the private interface. You want a fast connection on the private side, even with a slow WAN link on the public side, because much of the data will be pulled from cache instead of coming over the WAN link. Be absolutely sure that any network card is set up as either full-duplex or half-duplex on both the card and the switch the card is plugged into (if using a switch). Whether the card and switch are set for manual or automatic duplex sensing, they need to match. The public side network card generally doesn't need to be any faster than the WAN interface speed.

NetWare Server Installation Tips

This book is not intended to be a guide on installing NetWare. The reader is expected to know how to do that already, or to figure that out by him/herself. However, there are some tips here that may be useful for even those people who have set up many NetWare servers, if they were not for Internet access, or did not have BorderManager.

Using Caldera DRDOS and NetWare – MultiBoot Menu

If you install NetWare from a CD (or format the drive from the NetWare license disk), Caldera DRDOS will format the drive. It can be very useful to have a multiboot menu to allow you the option of easily boot to DOS with a CDROM driver loaded, or start NetWare automatically after a short delay. I use the following CONFIG.SYS and AUTOEXEC.BAT files to do this.

Note I provide all the files needed in this example at my web site http://www.craigjconsulting.com/

CONFIG.SYS

```
Rem You will need the Caldera DOS 7.01, 7.02 or 7.03, and the
programs XCOPY.EXE (from FreeDOS, or from
rem Caldera DR DOS 2) and NWCDEX.EXE (from the Novell license
disk, or Caldera DR DOS 7.0x Disk5).
rem Caldera DRDOS 7.03 can be downloaded from the Internet from
various sources.
rem You will have to use the makedisk or diskcopy commands to
create the DRDOS diskettes,
rem and then copy the appropriate files to your server.
rem You will also need some CDROM driver for your system.  The
OAKCDROM.SYS driver shown
rem here can be used on many systems, but any driver that works
on your CDROM should be
rem fine (or better).  Just edit the load line in CONFIG.SYS for
your driver name.

rem Caldera DRDOS multiboot menu for CONFIG.SYS

timeout=15
echo=1. Server
echo=2. DR-DOS
echo=3. XCopy all files on C: to D:
switch server, drdos, xcpy
exit

:server
set config=server
Files=60
Buffers=60
return

:drdos
set config=drdos
Files=60
Buffers=60
Device=c:\OAKCDROMDRV.SYS /D:CD001
return

:xcpy
set config=xcpy
Files=60
Buffers=60
return

[novell]
```

AUTOEXEC.BAT

```
rem Autoexec.bat
IF "%config%"=="server" goto NOVELL
IF "%config%"=="dos" goto DOS
IF "%config%"=="xcpy" goto XCPY

:DOS
nwcdex.exe /d:CD001
goto DONE

:XCPY
cls
@echo Copying all files on C: to D:
xcopy c:\*.* d: /h /k /r /f /v /e /s
goto DONE

:NOVELL
cd c:\nwserver
server -nl

:DONE
```

These files allow me to boot the server automatically, or choose to load the DOS-mode CDROM drivers in case I need to install software (like NetWare). The CPQIDECD.SYS file is just a standard IDE ATAPI CDROM driver, and it works on standard CDROM controllers. You would need something different for a SCSI CDROM.

CAUTION *Never use "CDROM" as a CPQIDECD or MSCDEX command line option. CDROM is a reserved word in DOS and will not work to identify the CDROM. Use something like CDROM1 or CPQCDROM instead.*

Using MSDOS 6.22 and NetWare 5.1

I found that the installation process would simply quit copying files at some point when using my standard config.sys file that had been working for years on many NetWare server installations. It appears that I was short on the FILES and BUFFERS required for installation on NetWare 5.1, because once I increased the values, my installation proceeded without problems. If you boot from the Novell CD and allow the automated installation to format your hard drive (using Caldera DOS) for you, you should not have a problem.

I use the following dual-boot CONFIG.SYS and AUTOEXEC.BAT files, generally:

CONFIG.SYS

```
[menu]
menuitem=NOVELL,Boot as Novell server (default)
menuitem=DOS,Boot to DOS with CDROM TSR's loaded
menudefault,novell,15

[common]
FILES=50
BUFFERS=50

[dos]
DEVICE=\DOS\CPQIDECD.SYS /D:CDROM1
LASTDRIVE=G
```

AUTOEXEC.BAT

```
@echo off
cls
rem Written by Craig Johnson, Jan. 9, 1998
goto  %config%

:NOVELL
cd c:\nwserver
server
goto END

:DOS
path c:\dos;c:\nc
C:\DOS\MSCDEX /l:D /m:40 /d:CDROM1

:END
```

These files allow me to boot the server automatically, or choose to load the DOS-mode CDROM drivers in case I need to install software (like NetWare). The CPQIDECD.SYS file is just a

standard IDE ATAPI CDROM driver, and it works on standard CDROM controllers. You would need something different for a SCSI CDROM.

CAUTION *Never use "CDROM" as a CPQIDECD or MSCDEX command line option. CDROM is a reserved word in DOS and will not work to identify the CDROM. Use something like CDROM1 or CPQCDROM instead.*

Don't Let The NetWare Installation Create the Volumes Automatically

During the installation process for NetWare, you will be asked if you want the NetWare partition to be created for you automatically. This is fine, as long as you don't want to make use of NSS volumes later. (NSS volumes are not created inside a NetWare partition). In NetWare 5.1, the NetWare partition will try to be created using all available free space. However, the installation will also try to create one large SYS volume on that partition, and you do not want that. You need to stop at the point where you first see a SYS volume created, and reduce the volume size to leave room for other volumes, such as LOG, CACHE1, CACHE2, etc. A 4GB SYS volume is a good size to use these days. NetWare 6.0 and 6.5 will try to use about 4GB for a dedicated NSS partition with only a SYS volume on it, and leave the rest of the disk space unconfigured.

CAUTION *ABSOLUTELY NEVER CREATE A PROXY CACHE VOLUME ON AN NSS VOLUME! Note that this is the default setting if you have only a SYS volume on NetWare 6.0 and later.*

The BorderManager 3.8 installation routine will offer you a choice of creating one or more cache volumes as long as it sees free (unpartitioned) space on NetWare 6.5 servers. This is a good thing, as the 3.8 installation will automatically create those volumes with the correct settings. But it will not create volumes in free space on existing partitions. If the installation routine creates the cache volumes for you, it will also automatically configure the HTTP proxy to use them.

On NetWare 6.0, at the point where it suggests you create the SYS volume, pressing F5 should toggle to a screen giving you the choice to make the SYS volume's partition a traditional NetWare file system instead of NSS. This can be desirable, but is not essential.

Once you have created a SYS volume of adequate size (no less than 2GB, 4GB preferred after NetWare 4.11), you can allow the installation to continue. You could also at this point add additional volumes, but you can create them later using INSTALL.NLM

(NetWare 4.x), NWCONFIG.NLM (NetWare 5.x) or ConsoleOne (NetWare 6.x). Just be sure that you have enough free space left to create these additional volumes, or you may have to repeat the installation and choose a smaller SYS volume.

A custom (not 'Express') NetWare 6.x installation will default to creating a 4GB NSS SYS volume, which is fine. You should have a larger physical drive installed than that, and if so, you will see a lot of unconfigured free space. I suggest configuring a legacy CACHE volume at this point in the NetWare 6.x installation, so that you do not have to go back and do that later. I also suggest you create a LOG volume (probably about 2-4GB) to hold the proxy common log files. If you are planning on using the Mail Proxy, also create a MAIL volume of 1-2GB to hold the spool files.

Install BorderManager from the Root of the CD

Versions of BorderManager prior to 3.8 contain a directory for BorderManager and another for NIAS on the product CD. A common mistake is to try to launch the product installation when pointing into the BorderManager directory because there is an installation script there. The proper procedure is to point the installation routine to the root of the BorderManager CD to pick up the main installation script. The main installation script will install NIAS components (which are required), and then install the BorderManager components.

If you install the BorderManager components only, BorderManager will not start because required NIAS files are missing.

Get the Server on the Internet Before Configuring BorderManager

You do not have to have BorderManager configured in NWADMN32 before you can connect to the Internet. In fact, you really should have Internet connectivity itself set up BEFORE you configure BorderManager services. Basically, this means that you should have configured a default route and DNS services, and possibly enabled Dynamic NAT on the public IP address before worrying about whether your BorderManager proxy is configured, and certainly long before you need to worry about how your access rules are set up!

My advice: Install NetWare, and then install BorderManager. Go through the initial configuration process up through the point where the server has been rebooted after the BorderManager installation. If you have installed BorderManager 3.x, you will probably also have RADIUS.NLM loaded. (You will see a console screen about a Dial Access System Name. If you don't use RADIUS, comment out the LOAD RADIUS line in AUTOEXEC.NCF or STARTBRD.NCF).

LOAD INETCFG, and go into Protocols, TCP/IP and set up a default route under LAN Static Routing. Next, specify a domain name and at least one public DNS server IP address in DNS Resolver Configuration. Exit INETCFG, and Reinitialize System. In case you have filters configured, UNLOAD IPFLT to disable filtering. Now, if things are configured correctly, you should be able to LOAD PING WWW.NOVELL.COM, have that URL translated to an IP address, and start receiving PING responses. I would not bother to set up anything else for BorderManager until you can PING an Internet URL from the server console itself. You should not enable filtering for the PING tests.

BorderManager relies on the underlying routing capabilities of NetWare to be working. If you have not gotten Internet access capability working before BorderManager, you may waste a lot of time trying to figure out what is going wrong.

In summary, you will generally need to do all of the following to ping an Internet URL from the server once BorderManager has been installed:

- Disable packet filtering (Unload IPFLT.NLM)
- Set up a default route. (Use INETCFG, Protocols, TCP/IP, LAN Static Routing Table, Route Type=Default Route, <enter your Internet router's LAN IP address).
- Set up your ISP's DNS server addresses on the NetWare server. (Use INETCFG, Protocols, TCP/IP, DNS Resolver Configuration).

If you find that routing is not working, **check the default route**. If you can PING only by IP address and not by URL, check the DNS resolver configuration.

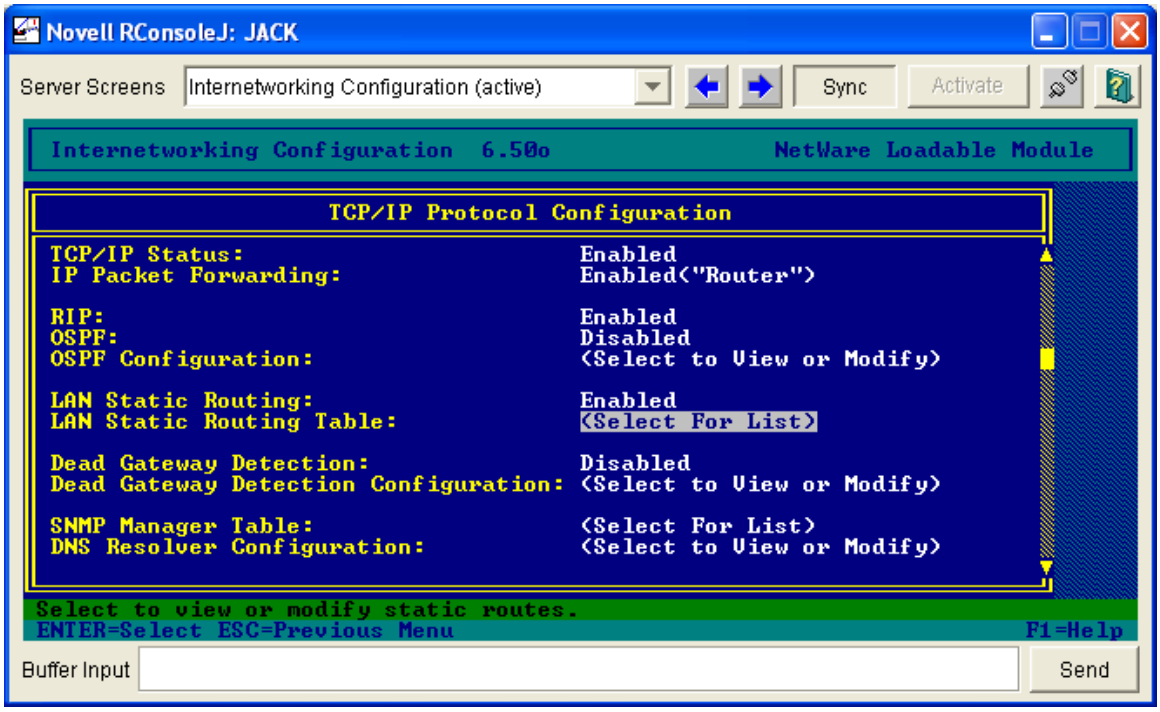
Other extremely useful debugging tools at the server include SET TCP IP DEBUG=1 to see the IP packets at the server (=0 turns off the display), and LOAD IPTRACE x.x.x.x to do a trace route to an IP address.

Load TCPCON is useful for checking the presence of IP routes, though it should NOT be used to enter a route. TCPCON is also useful to see the interface numbers, which show up in FILTER DEBUG output

Setting the Default Route and DNS Servers

Installing BorderManager versions prior to 3.7 does not automatically set up a default route, even though you will not be able to communicate to the Internet without one. Use the following procedure to set a default route, using INETCFG.NLM at the BorderManager server console. I recommend that you do this before installing BorderManager.

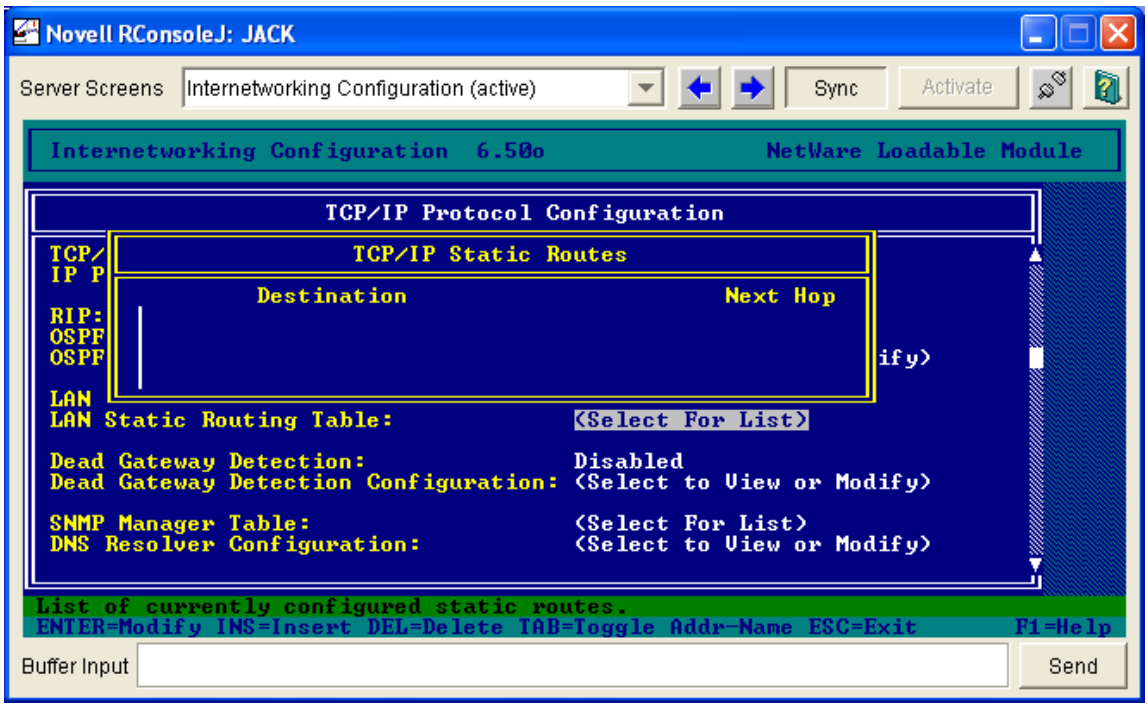
The following example shows a NetWare 6.5 server configured to use a default route of 192.168.1.1.



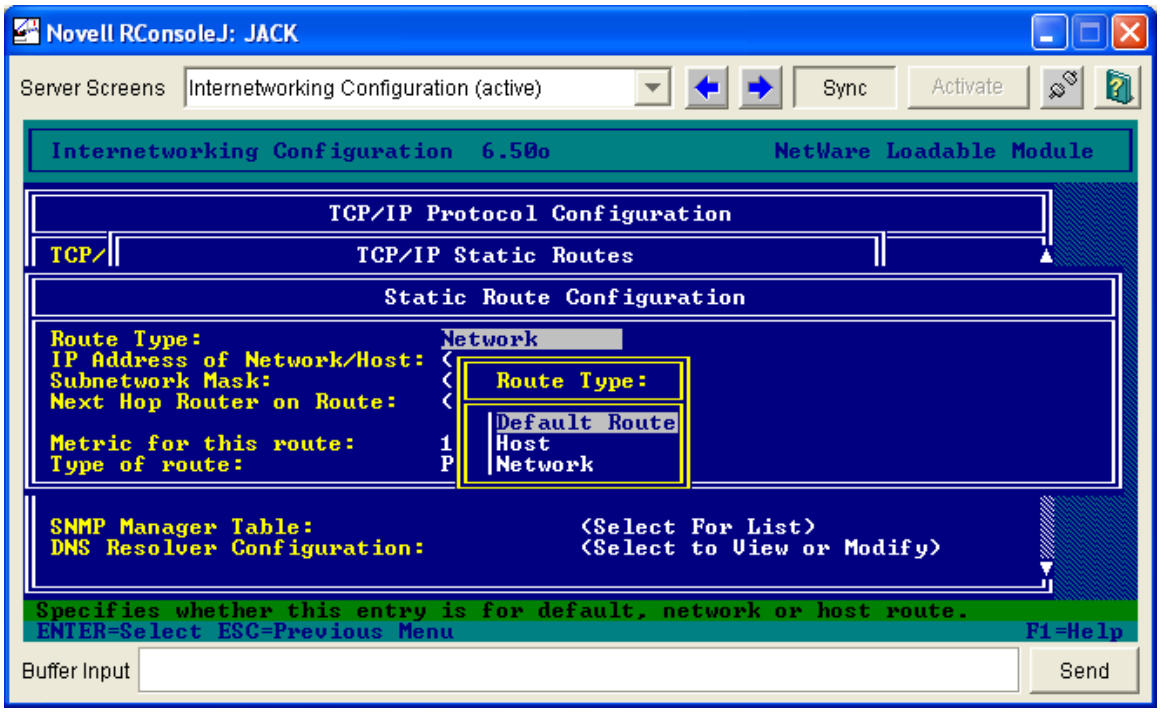
LOAD INETCFG, and select menu option **Protocol**, **TCP/IP**, as shown in the example above.

Note If you intend to use packet filter exceptions to bypass the proxies or IP Gateway for selected traffic, you also will need to **Enable IP Packet Forwarding**. However, the BorderManager services themselves (proxies, IP Gateway, VPN) do not require the BorderManager server to act as a router. In most cases, you will want to enable IP routing.

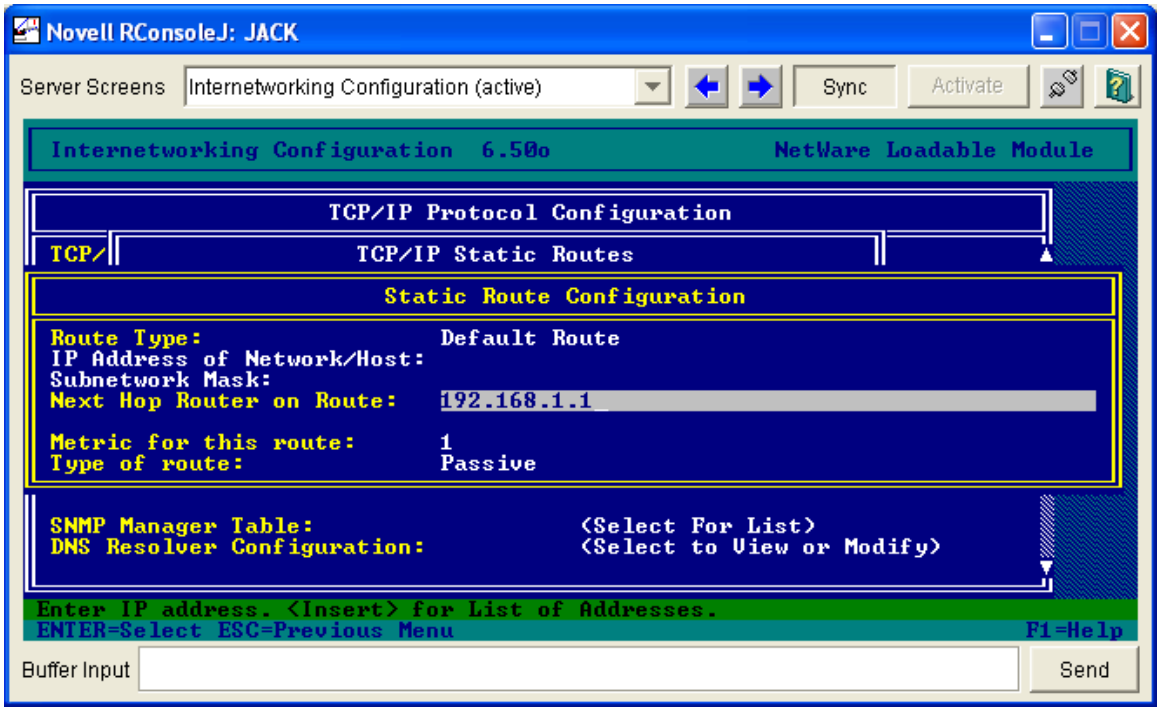
Enable LAN Static Routing, and then select **LAN Static Routing Table**.



The initial entry may be blank. Press the **Insert** key to add a value.

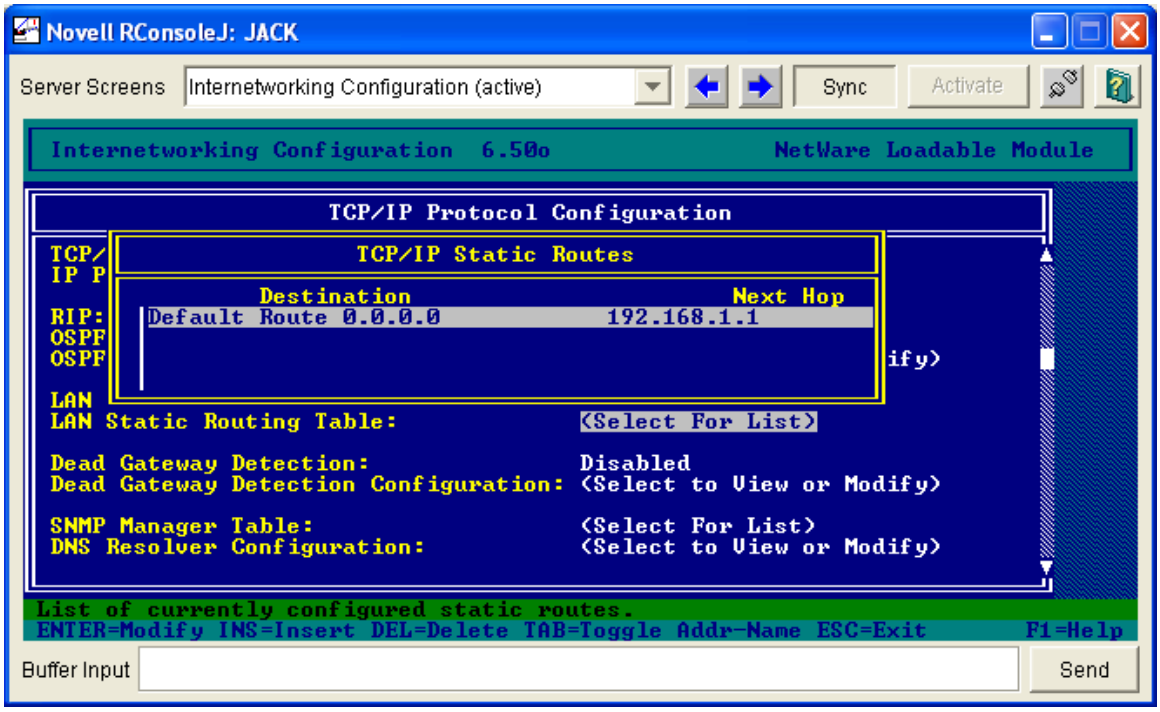


Press **Enter**, and select the option for **Default Route**.



Fill in the IP address of the next hop from the BorderManager server to the Internet. This will generally be the LAN IP address of the Internet router, and it must be an address on a network to which the public interface of the BorderManager server is connected. (A dummy address is shown here).

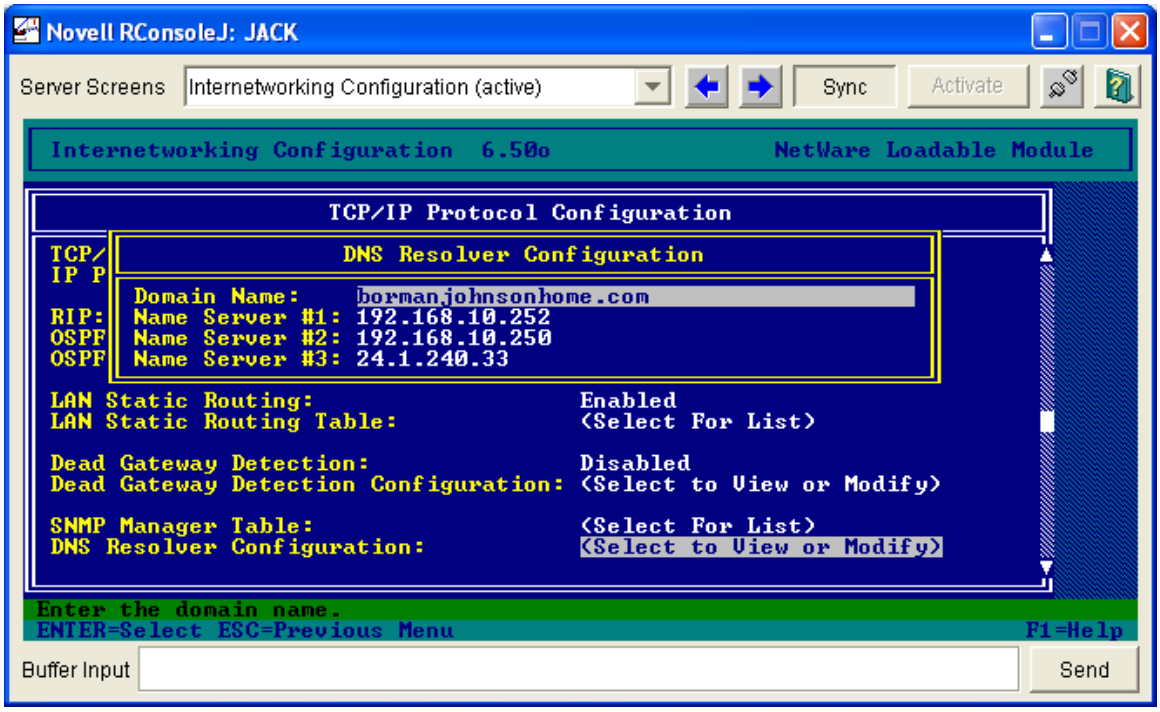
Press **Escape**.



You should now see the default route entry as one of the static routes listed for the BorderManager server.

Press **Escape** again and select **Yes** when asked to **Update Database**.

Now move the cursor down to **DNS Resolver Configuration** and press **Enter** to add DNS server IP addresses.



The example shown above shows two IP addresses configured for DNS resolution.

The **Domain Name** is set to the internal DNS domain I used for my test network. While you do not have to enter a value here, it may be used in outgoing NNTP messages and SMTP mail by the appropriate proxies.

The **Name Server #1** IP address shown is the IP address of an internal DNS server. If you have an internal DNS server, list it first. If you have no internal DNS server, add the IP address of one of your ISP's DNS servers.

The **Name Server #2** IP address shown is the IP address of a public DNS server. List your ISP's DNS server IP addresses here. (You should have a least two public DNS servers configured for fault tolerance. The entries shown above are useful only in my test network).

Escape back to the INETCFG main menu, and select **Reinitialize System** to update the values entered. Then toggle through the console screens until you come back to the INETCFG main menu, and press **Escape** to unload INETCFG.

If you have entered the correct values, and your routers are configured, connected and operating properly, you should now have Internet connectivity.

BorderManager Server Configuration Suggestions

To go along with the above suggestions on hardware, I suggest the following BorderManager configuration options:

1. **Cache Volumes**: Use dedicated cache volume(s)! You **MUST** have the HTTP Proxy cache set up to use a volume **other** than SYS. (The default is to use SYS, but that is the first thing to change when you configure the BorderManager server using NWADMN32. If installing BorderManager 3.8 on NetWare 6.5, the installation may give you the option of creating and/or using a traditional cache volume under certain circumstances). I recommend one or more dedicated 4-5GB legacy (non-NSS) cache volumes, using 16K block size, no suballocation and no compression. It is best to not use compression at all on a BorderManager server for performance reasons, but essential not to use compression on cache volumes. The total cache volume space allotted should be approximately equal to the amount of data from web pages (and downloaded files) browsed in one week during a busy time. Cached web pages default to becoming stale after one week anyway, so holding data in cache longer than that just makes the volumes slower to index when you load BorderManager. If you want 20GB of cache space, use four 5-GB cache volumes. The best performance results from using multiple cache volumes will only come when dedicating a separate disk to each volume, in order to split the disk requests across multiple spindles

---

Note In order to configure cache volumes, you need to select an advanced option during a NetWare 5.x installation. Otherwise you will end up with the default – a SYS volume that uses up the entire NetWare partition. You can either re-install the server, add another drive, or get a copy of a utility like PowerQuest's ServerMagic 3 or Volume Resize from Portlock. ServerMagic or Volume Resize can be used to resize the partitions and volumes, including resizing a SYS volume down to a reasonable 4GB so that you can then use NWCONFIG to create cache and log volumes. As of this writing, Portlock software cannot reduce the size of an NSS volume.

---

2. **Log Volumes**: I recommend a dedicated log volume, though it is not essential. Log files can get extremely large, and you do not want them to take up space on the SYS volume. I recommend a 2GB LOG volume to hold Common Log files, more if you want to keep a lot of log history with a lot of users.
3. **SYS Volume Size**: I strongly recommend configuring (**at least**) a 4GB SYS volume. The Indexed and Access Control rule logs

are both contained in Btrieve files under the SYS:\SYSTEM\CSLIB directory, and you have little control over how large those log files get, or how often they roll old data over. Running out of space on a SYS volume is a serious problem for any NetWare server running NDS as you can get NDS corruption. See Novell TID 10051681 for a method of controlling log files with the CSAUDIT module. There is also a section on using CSAUDIT in this book in the chapter "Logging". Note that simply applying the NetWare 5.1 service packs can require over 500MB of free space on the SYS volume, and more space is required for NetWare 6.x.

4. **General Server Performance Tuning**: Refer to the chapter later in the book entitled "Performance Tuning" for some guidelines on tuning a BorderManager server aggressively for very fast performance.

NDS Design Considerations

Background Information

BorderManager will store much of its configuration as NDS attributes to a server object. In addition, the best way to set up access rules is to save the rules as part of the BorderManager server object attributes. This means that it is best to have a read/write replica on the BorderManager server that at least holds the BorderManager server object. The BorderManager server can be placed at any point in the NDS tree and still allow all users in the tree access through it to the Internet.

If you have more than one BorderManager server, installing them in the same container can reduce the work needed to maintain rules, as they can be applied at the container level; BorderManager will read rules up the tree, i.e. rules applied to the server first, then its immediate container and so on, up to the root. However, this method does not really allow you to customize the rules for particular containers through inheritance.

In NDS6 and NDS7, subordinate references can be a problem. For this reason, I recommend not putting BorderManager in a Root partition if you have more than about 7 servers. Generally speaking, having a server in the Root replica will tend to generate a lot of subordinate references to other servers, though this depends on the NDS design and placement of replicas. Creating a partition just for the BorderManager server(s) can help to minimize subordinate references, as can placing the BorderManager server(s) at containers lower than the Organization container.

Version-Specific NDS Considerations

BorderManager 3.8 has relatively severe NDS requirements, especially as compared to previous versions.

BorderManager 3.6 and earlier would work with any version of NDS. BorderManager 3.7 and 3.8 require auxiliary classes in NDS to support filtering, and therefore require eDirectory version 8 or above. (DS versions 8.82 or higher. 85.12a or higher, or 10xxx). The server holding the master replica of the Root partition also needs to be running NDS 8.6 or later, preferably the latest version of NDS that is being used in the tree. NetWare 5.1 service pack 5 will update NDS to version 8.82 (if using NDS 8), and this should be considered as the minimum NDS version to use with BorderManager 3.7. Failure to have the minimum NDS version in place on the master of Root and the BorderManager 3.7 or 3.8 server will result in NDS errors when trying to migrate filters into NDS.

BorderManager 3.8 requires eDirectory 8.6.2 or 8.7 or higher. (This is not the same as DS version 8.82 – these DS versions are numbered something along the lines of 10411.02. The eDirectory requirement for BorderManager 3.8 is for VPN support.

BorderManager 3.7 and 3.8 store filters in a special container in NDS called NBMRuleContainer. You will have less trouble managing filtering if there is only one BorderManager 3.7 or 3.8 server in the same OU, as sharing the same NBMRuleContainer can cause issues.

BorderManager 3.7 & 3.8 require replicas on the server for filtering to work correctly.

BorderManager reads licenses out of NDS initially only from the Master server of the replica that holds the licenses. Particularly for Site-to-Site VPN, this means that the Master server of that replica should be on the BorderManager server itself.

For the reasons just given, my recommendation is the following:

- Make an OU called BMGR1 (or BORDER1 or similar) in the container where you were thinking of putting the BorderManager server.
- Put only one BorderManager server in that BMGR1 OU.
- Partition the BMGR1 OU from the tree.
- Have at least three replicas of the BMGR1 OU, and have the Master replica on the BorderManager server.

Now you will have a small replica, holding the licenses and filtering objects for the server, on the BorderManager server itself, with the BorderManager server being the master of that replica ring.

How to Install BorderManager Remotely

Because BorderManager installation requires the Java GUI-based method to be used (for BorderManager 3.x on any server after NetWare 4.x), you cannot use RCONSOLE, RCONJ or 3rd-party utilities like Adremsoft's Adrem Free Remote Console. None of those utilities can view the GUI screens, which are XFree86 windows sessions. However, there is a way that you can redirect the Xwindows display to your local desktop. It is relatively easy to switch back and forth between a local (server console) GUI screen and your PC, using some customized NCF files. You use RCONSOLE, RCONJ, etc, to get things started.

Requirements

- An Xwindows server program running on your PC. (You could use Linux as well). I used a program called WinaXe that I downloaded from http://www.tucows.com.
- An NCF file which redirects the XWindows display from the server console to your PC's IP address.
- An NCF file which redirects the XWindows display back to your server console. (You simply modify the existing STARTX.NCF file for this).
- An NCF file which kills any existing XWindows display that is running so that you can redirect it where you want.
- NetWare 5.0 or later.
- For Netware 5.x & 6.0, I put my files in the SYS:JAVA\NWGFX directory, where STARTX is located. For NetWare 6.5, use the SYS: JAVA\NWGFX\BIN directory.

Note I provide sample NCF files at my web site http://www.craigjconsulting.com/.

Example Scenario

In the example shown, I have a NetWare 5.1 or 6.0 server at IP address 192.168.10.250. My PC is at IP address 192.168.10.254. I am running WinaXe 6.2, listening on console port '0'. WinaXe is set up in Single Window Mode.

STARTX.NCF

This is the standard STARTX.NCF file, modified to ensure that the XWindows display goes to the server console. This file is normally located in the SYS:\JAVA\NWGFX directory. Note that the :0 is required here, and the spaces around the '=' signs is significant.

```
env display = 127.0.0.1:0
envset display=127.0.0.1:0
load xinit
```

REMX.NCF

This NCF file redirects the XWindows display to 192.168.10.254, console number '0'. This file is normally located in the SYS:\JAVA\NWGFX directory. Note that the :0 is required here, and the spaces around the '=' signs is significant.

```
env display = 192.168.10.254:0
envset display=192.168.10.254:0
load xinit
```

DX.NCF

This NCF file kills any running XWindows display, so that you can launch it again and direct it where needed. You would use this if the display was already launched on the GUI was running on the server console. Without this NCF file, you would have to be at the server console, in the GUI, to unload it. This file can be located in the same directory as the STARTX and REMOTEX files, or put into the SYS:\SYSTEM directory.

```
unload xfvga16
unload xfsvga
unload xaccel
```

Procedure

1. Start your XWindows session on your PC.
2. Be sure you have your PC's IP address in the REMX.NCF file.
3. Using RCONSOLE, RCONJ, etc, to make a remote console connection to the server, run the DX.NCF file. This should kill any XWindows session running.
4. At the server console, type JAVA –SHOWALL. If you see a 'Taskbar or 'bg' session running, you will probably need to kill it. Look at the session ID number, then type JAVA –kill<id>, where <id> is the session number of the bg session. (The bg session is, I believe, the GUI background). **If killing the session does not work, you may have to stop and restart java, with a JAVA –EXIT command.**
5. Run the REMX.NCF file. The XWindows session should show up on your PC.
6. Now you can install BorderManager remotely. The BorderManager files themselves need to be available on a mounted volume (CDROM or copied to one of the server volumes).

CAUTION *The demo version of WinAXE only works for 30 minutes – do not launch WinAXE until you are ready to install BorderManager, and immediately begin the installation process. If you have to cancel out of the installation, be sure to completely stop and restart WinAXE before repeating the installation.*

Recommended Patches and Installation Sequence

BorderManager 3.x requires certain software to be installed before you can install BorderManager. Check the readme files on the installation CD before installing the software. Install required service packs first, if you don't already have them installed on the server.

BorderManager 3.8 includes a prerequisite check at the beginning of the installation sequence to see if you have all required or optional components installed. This check includes NDS version, LDAP requirements, NICI encryption requirements, TCPIP requirements and iManager requirements. Some of the required components, such as TCPIP or NICI, are supplied on the BorderManager Companion CD.

Check the Novell Public Forums for advice on the latest listed and unlisted patches to apply to the server for BorderManager, as well as the installation sequence that is recommended. This subject can get quite complex, to the point that Novell TID's have been written, and web sites (mine, for one, at http://www.craigjconsulting.com/) have been put up with recommended patch sequences. The following section may be well out of date by the time you read this.

I highly recommend you start by looking at **Novell's Minimum Patch List** at http://support.novell.com/misc/patlst.htm. The minimum patch list contains released (non-beta) patches that are recommended by Novell. Next, check tip #1 at http://www.craigjconsulting.com for the latest available patch sequence and warnings. This list will often contain beta patches, and other patches that may not be on the minimum patch list.

Installing BorderManager 3.8

Note If you have an older version of BorderManager installed on the server before installing BorderManager 3.8 in an in-place upgrade scenario, you may not be able to install 3.8 without first removing the old BorderManager entries from the PRODUCTS.DAT file. This is most easily done with the UINSTALL command. UINSTALL, followed by the exact text in the Configured Products List (in NWCONFIG), simply removes the text from the Configured Products list, and that will allow BorderManager 3.8 to be installed. See Novell TID 10022635.

on NetWare 6.5

Note You cannot start the installation procedure for BorderManager using NWCONFIG. You must first launch the GUI installation program (STARTX), and point to the BorderManager 3.8 PRODUCT.NI file, on the root of the BorderManager CD.

1. Install NetWare 6.5. NetWare 6.5 includes the required version of NDS eDirectory, NICI, and iManager 2.0, which makes it well-suited for BorderManager 3.8. It is best to install NetWare 6.5 with only iManager 2.0 (and requirements for iManager – the installation routine will take care of that for you).
2. Install NW65SP1a.EXE (or the most recent NetWare 6.5 support pack).
3. If you did NOT install NW65SP1a.EXE first, then, from the BorderManager 3.8 Companion CD, install the NetWare 6.5 version of TCPIP. Use the Domestic version if you want to configure VPN. Use the Null version otherwise. (Requires a reboot). The correct version for VPN will say (Domestic) NICI with a MODULES TCPIP command.
4. If you DID install NW65SP1.EXE, there is a post-NW65SP1 TCP patch available. At the time of this writing, the latest version was TCP654REV2.EXE. TCP patches come out often, and you should be checking for them.
5. Load INETCFG at least once, to transfer critical networking information into their final destination files in SYS:ETC.
6. Reboot the server, and begin the BorderManager 3.8 installation.
7. Install various other patches such as new versions of NAT or packet filtering modules that may have been released since BorderManager 3.8. Check the Novell Support Connection public forums (news://support-forums.novell.com) and

http://www.craigjconsulting.com for current information, as *not all available patches will show up on the minimum patch lis*t.

8. If you are upgrading a BorderManager installation from a version prior to 3.7, you must migrate the TCP/IP-related filter exceptions into NDS using the FILTSRV MIGRATE procedure at the server console. Afterwards, I recommend using FILTCFG.NLM to modify any IP filters, simply because it writes changes to both NDS and filters.cfg. (That way, you always have an up-to-date filters.cfg file as a backup). You can use iManager to manage filtering for BorderManager 3.8. (You still must use FILTCFG.NLM to modify IPX or Appletalk filters). This subject is discussed in great detail in the Third Edition of my "*Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions*" book.

9. Update SYS:\ETC\PROXY\PROXY.CFG. You can use the example file maintained at my web site (http://www.craigjconsulting.com). The file provided by default has a bare minimum of entries, and many bug fixes and enhancements have been added to the PROXY.CFG file with each BorderManager patch. An example file is shown later in this book.

10. If you will be using SurfControl, get the latest version of SurfControl from http://www.surfcontrol.com. As of this writing, Service Pack 3 is available. Service pack 3 is a complete installation of SurfControl, including a recent database, and is much newer than the version supplied on the BorderManager 3.7 product CD. Service Pack 3 adds 8 more categories not present in earlier versions.

on NetWare 6.0

Note You cannot start the installation procedure for BorderManager using NWCONFIG. You must first launch the GUI installation program (STARTX), and point to the BorderManager 3.8 PRODUCT.NI file, on the root of the BorderManager CD.

1. Install NetWare 6.0.
2. Install NW6SP4.EXE or later NetWare support pack. (NW6SP3 is the minimum requirement to install BorderManager 3.8).
3. If you installed NW6SP3, you will need to update TCP files. (NW6SP4 includes a version of TCPIP that meets BorderManager 3.8 VPN requirements, but does not install it automatically unless you are upgrading an existing BorderManager server.) From the BorderManager 3.8 Companion CD, install the NetWare 6.0 version of TCPIP. (Requires a reboot). If NW6SP4 is installed, you can find the Domestic (NICI) version of TCPIP in the PRODUCTS\TCP\TCPD folder. However, read the next paragraph.
4. There is a post-NW6SP4 TCPIP patch available called TCP608VREV2.EXE. TCP patches come out often, and you should check for them.
5. If you installed NW6SP3, you will need to update NICI. (NW6SP4 installs a version of NICI that meets BorderManager 3.8 requirements). From the BorderManager 3.8 Companion CD, install NICI 2.6 on the server. (Explode the NICI file somewhere on the server, and then use NWCONFIG to point to the .IPS installation subdirectory).
6. (Optional) From the BorderManager 3.8 Companion CD, install eDirectory 8.7.1. The minimum requirement of NDS is version 8.82, but the latest version is definitely recommended. (Requires a reboot). Run DSREPAIR.
7. Load INETCFG at least once, to transfer critical networking information into their final destination files in SYS:ETC.
8. Install BorderManager 3.8.
9. Install various other patches such as new versions of NAT or packet filtering modules that may have been released since BorderManager 3.8. Check the Novell Support Connection public forums (news://support-forums.novell.com) and http://www.craigjconsulting.com for current information, as *not all available patches will show up on the minimum patch lis*t.

10. If you are upgrading a previous BorderManager installation (prior to 3.7), and you have customized the filter exceptions, you must migrate the TCP/IP-related filter exceptions into NDS using the FILTSRV MIGRATE procedure. Afterwards, you can use FILTCFG or iManager to modify IP filters. (You still must use FILTCFG.NLM to modify IPX or Appletalk filters). This subject is discussed in great detail in the Third Edition of my "*Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions*" book.

11. Update SYS:\ETC\PROXY\PROXY.CFG. You can use the example file maintained at my web site (http://www.craigjconsulting.com). The file provided by default has a bare minimum of entries, and many bug fixes and enhancements have been added to the PROXY.CFG file with each BorderManager patch. An example file is shown later in this book.

12. In order to configure the new VPN services for BorderManager 3.8, you must have access to iManager 2.0. If you have a NetWare 6.5 server available, you can use iManager 2.0 from that server (even if it is in a different tree). Alternatively, you can install iManager 2.0 from the Companion CD to a NetWare 6.0 server, or a Windows 2000 or XP PC, add the VPN snapins, and use that to configure BorderManager 3.8 VPN. Note that if you try to install iManager 2 from the Companion CD to a NetWare 6.0 server, that you will very probably need to modify a number of configuration files to get it to work. The required steps are given in the Troubleshooting chapter.

13. If you will be using SurfControl, get the latest version of SurfControl from http://www.surfcontrol.com. As of this writing, Service Pack 3 is available. Service pack 3 is a complete installation of SurfControl, including a recent database, and is much newer than the version supplied on the BorderManager 3.7 product CD. Service Pack 3 adds 8 more categories not present in earlier versions.

on NetWare 5.1

Note You cannot start the installation procedure for BorderManager using NWCONFIG. You must first launch the GUI installation program (STARTX), and point to the BorderManager 3.8 PRODUCT.NI file, on the root of the BorderManager CD.

1. Install NetWare 5.1
2. Install NW51SP6.EXE or later NetWare 5.1 support pack. NW51SP7 is preferred.
3. From the BorderManager 3.8 Companion CD, install the NetWare 5.1 version of TCPIP. (Requires a reboot)
4. From the BorderManager 3.8 Companion CD, install NICI 2.6 on the server. (Explode the NICI file somewhere on the server, and then use NWCONFIG to point to the .IPS installation subdirectory).
5. From the BorderManager 3.8 Companion CD, install eDirectory 8.7.1, or download a later version from Novell and install that. 8.7.3 is preferred. (Requires a reboot). Run DSREPAIR.
6. Load INETCFG at least once, to transfer critical networking information into their final destination files in SYS:ETC.
7. Reboot the server, and begin the BorderManager 3.8 installation.
8. Install the latest TCPIP.NLM, if one has been released separately from the NetWare service pack. Any newer version needs to explicitly state that it supports BorderManager 3.8. As of this writing, the latest post-NW51SP7 TCP patch is TCP518VREV2.EXE. You want the NICI (Domestic) version to show up when you type MODULES TCPIP at the server console.
9. Install various other interim patches such as new versions of NAT or packet filtering modules. Check the Novell Support Connection public forums (news://support-forums.novell.com) and http://www.craigjconsulting.com for current information, as *not all available patches will show up on the minimum patch list*.
10. If you are upgrading a previous BorderManager installation (prior to 3.7), and you have customized the filter exceptions, you must migrate the TCP/IP-related filter exceptions into NDS using the FILTSRV MIGRATE procedure. Afterwards, you can use FILTCFG or iManager to modify IP filters. (You still must use FILTCFG.NLM to modify IPX or Appletalk filters). This subject is discussed in great detail in the Third Edition of my "*Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions*" book.

11. Update SYS:\ETC\PROXY\PROXY.CFG. You can use the example file maintained at my web site (http://www.craigjconsulting.com). The file provided by default has a bare minimum of entries, and many bug fixes and enhancements have been added to the PROXY.CFG file with each BorderManager patch. An example file is shown later in this book.

12. In order to configure the new VPN services for BorderManager 3.8, you must have access to iManager 2.0. If you have a NetWare 6.5 server available, you can use iManager 2.0 from that server (even if it is in a different tree). Alternatively, you can install iManager 2.0 from the Companion CD to a NetWare 6.0 server, or a Windows 2000 or XP PC, add the VPN snapins, and use that to configure BorderManager 3.8 VPN. Note that if you try to install iManager 2 from the Companion CD to a NetWare 6.0 server, that you will very probably need to modify a number of configuration files to get it to work. The required steps are given in the Troubleshooting chapter.

13. If you will be using SurfControl, get the latest version of SurfControl from http://www.surfcontrol.com. As of this writing, Service Pack 3 is available. Service pack 3 is a complete installation of SurfControl, including a recent database, and is much newer than the version supplied on the BorderManager 3.7 product CD. Service Pack 3 adds 8 more categories not present in earlier versions.

Installing BorderManager 3.7

On NetWare 6.0

Unlike previous versions of NetWare, you cannot start the installation procedure for BorderManager using NWCONFIG. You must first launch the GUI installation program (STARTX), and point to the BorderManager 3.7 PRODUCT.NI file, on the root of the BorderManager CD.

1. Install NetWare 6.0.
2. Install NW6SP4.EXE (or later) NetWare support pack
3. If you installed only NW6SP3, install PURGE_NW.EXE (fixes NW6SP3 bug)
4. If you installed only NW6SP3, install NW56UP3.EXE (post-NW6SP3 patch)
5. If you installed only NW6SP3, install NLS603FT.EXE (and run SETUPNLS afterwards)
6. Install the latest TCPIP.NLM, if one has been released separately from the NetWare service pack. As of this writing, TCP608VREV2EXE was the latest version, but it should only be installed with NW6SP4 installed first.
7. Install BorderManager 3.7.
8. Install BM37SP3.EXE (or later)
11. Install BM37FP4B.EXE (this is a post-BM37SP3 patch).
12. Install various other interim patches such as new versions of NAT or packet filtering modules. Check the Novell Support Connection public forums (news://support-forums.novell.com) and http://www.craigjconsulting.com for current information, as *not all available patches will show up on the minimum patch lis*t.
13. If you are upgrading a previous BorderManager installation, and you have customized the filter exceptions, you need to migrate the TCP/IP-related filter exceptions into NDS using LOAD FILTSRV MIGRATE at the server console. You must not see any NDS errors in the Logger screen when migrating filters, or there will be filtering issues. Afterwards, you can use either FILTCFG or iManager to manipulate filters and exceptions, but I have found FILTCFG to be both easier and more reliable. You must use FILTCFG.NLM to modify IPX or Appletalk filters. This subject is discussed in great detail in the Third Edition of my "*Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions*" book.

14. Update SYS:\ETC\PROXY\PROXY.CFG. You can use the example file maintained at my web site (http://www.craigjconsulting.com). The file provided by default has a bare minimum of entries, and many bug fixes and enhancements have been added to the PROXY.CFG file with each BorderManager patch. An example file is shown later in this book.
15. If you will be using SurfControl, get the latest version of SurfControl from http://www.surfcontrol.com. As of this writing, Service Pack 3 is available. Service pack 3 is a complete installation of SurfControl, including a recent database, and is much newer than the version supplied on the BorderManager 3.7 product CD. Service Pack 3 adds 8 more categories not present in earlier versions.

On NetWare 5.1

Note BorderManager 3.7 is not supported on versions of NetWare prior to 5.1.

Unlike previous versions of NetWare, you cannot start the installation procedure for BorderManager using NWCONFIG. You must first launch the GUI installation program (STARTX), and point to the BorderManager 3.7 PRODUCT.NI file, on the root of the BorderManager CD.

1. Install NetWare 5.1
2. Install NW51SP7.EXE or later NetWare 5.1 support pack. (BorderManager 3.7 will not install without at least NW51SP4 installed first).
3. If you did install only NW51SP6, install PURGE_NW.EXE (fixes NW5SP6 bug)
4. If you did install only NW51SP6, install NW56UP3.EXE (post-NW5SP6 patch)
5. Install the latest TCPIP.NLM, if one has been released separately from the NetWare service pack. As of this writing, TCP585VREV2.EXE was the latest version (post-NW51SP7 patch). New TCP patches are common, and you should keep looking for them.
6. Install BorderManager 3.7.
7. Install BM37SP3.EXE (or later)
8. Install BM37FP4B.EXE (this is a post-BM37SP3 patch).
9. Install various other interim patches such as new versions of NAT or packet filtering modules. Check the Novell Support

Connection public forums (news://support-forums.novell.com) and http://www.craigjconsulting.com for current information, as *not all available patches will show up on the minimum patch lis*t.

10. If you are upgrading a previous BorderManager installation, and you have customized the filter exceptions, you need to migrate the TCP/IP-related filter exceptions into NDS using LOAD FILTSRV MIGRATE at the server console. You must not see any NDS errors one the server console when migrating filters, or there will be filtering issues. Afterwards, you can use FILTCFG to manipulate filters and exceptions. This subject is discussed in great detail in the Third Edition of my "*Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions*" book, available at http://www.craigjconsulting.com.

11. Update SYS:\ETC\PROXY\PROXY.CFG. You can use the example file maintained at my web site (http://www.craigjconsulting.com). The file provided by default has a bare minimum of entries, and many bug fixes and enhancements have been added to the PROXY.CFG file with each BorderManager patch. An example file is shown later in this book.

12. If you will be using SurfControl, get the latest version of SurfControl from http://www.surfcontrol.com. As of this writing, Service Pack 3 is available. Service pack 3 is a complete installation of SurfControl, including a recent database, and is much newer than the version supplied on the BorderManager 3.7 product CD. Service Pack 3 adds 8 more categories not present in earlier versions.

Installing BorderManager 3.6

CAUTION *The BorderManager 3.6 installation has a problem in the install script that causes it to copy all the files in the NIAS directory from the CD on the server, even if they are older than the versions on the server! You **MUST** reapply the latest service pack for NetWare after installing BorderManager 3.6 to correct this issue. (This is regardless of whether you plan on using NIAS features or not).*

On NetWare 6.0

Note If you are upgrading from NW 5.x, see the BM36SP1A.EXE readme.

1. Install NetWare 6.0. You can also install NW6SP4.EXE now, but you must reinstall it after installing BorderManager 3.6 to be sure you do not have back-revved files.
2. Install NW6SP4.EXE.
3. If you have not installed NW6SP4, then install ADMATTRS.EXE - This patch creates NDS attributes for BorderManager relating to a Login Policy Object. NMAS may be installed by default, and installing BorderManager after NMAS can create problems! Before proceeding, see http://support.novell.com/servlet/tidfinder/2959071
4. Install BorderManager 3.6 - When prompted to reboot do NOT reboot. Go on to the next step. If you cannot install BorderManager at all, see the other tips at http://www.craigjconsulting.com.
5. Install BM36SP2A.EXE - Addresses install bug for NetWare 6 and BorderManager 3.6. Do NOT reboot.
6. Install BM36NSP1.EXE - Replaces outdated NIAS files in BorderManager 3. This patch requires BM36SP1A to be installed first, which is the only reason to install BM36SP1A at this point. (You can reboot after this patch if you like).
7. PROXY.NLM – You can use the latest proxy for BorderManager 3.7 on 3.5 and 3.6 servers. Get it from whatever the latest BorderManager 3.7 patch is. (You cannot use the BorderManager 3.8 version of proxy on earlier versions of BorderManager). Starting with the BM37FP4B.EXE patch, you may also have to copy in the AUTHCHK.NLM file to get proxy to load.
8. Optional - Install the CSATPXY.NLM from the latest BorderManager 3.7 patch to fix a logging bug in BorderManager.

9. Install / reinstall NW6SP4.EXE – (Or latest support pack for NetWare).
10. If you only installed NW6SP3, install PURGE_NW.EXE (fixes NW5SP6 bug)
11. If you only installed NW6SP3, install NW56UP3.EXE (post-NW5SP6 patch)
12. If you only installed NW6SP3, install NLS603FT.EXE (and run SETUPNLS afterwards)
13. Install the latest TCPIP.NLM, if one has been released separately from the NetWare service pack. As of this writing, TCP608VREV2K.EXE was the latest version. New TCP patches are common, and you should keep looking for them.
14. Install various other interim patches such as new versions of NAT or packet filtering modules. Check the Novell Support Connection public forums (news://support-forums.novell.com) and http://www.craigjconsulting.com for current information, as *not all available patches will show up on the minimum patch lis*t.
15. Update SYS:\ETC\PROXY\PROXY.CFG. You can use the example file maintained at my web site (http://www.craigjconsulting.com). The file provided by default has a bare minimum of entries, and many bug fixes and enhancements have been added to the PROXY.CFG file with each BorderManager patch. An example file is shown later in this book.

On NetWare 5.1

1. Install NetWare 5.1
2. Install NW51NI1.EXE - Only needed if you installed NW51SP3 before installing BorderManager. See http://support.novell.com/servlet/tidfinder/2960217.
3. Install ADMATTRS.EXE - Should only be needed if you have NMAS installed in your NDS tree. This patch creates NDS attributes for BorderManager relating to a Login Policy Object. Before proceeding, see http://support.novell.com/servlet/tidfinder/2959071
4. Install BorderManager 3.6. Don't install NW51SP3 first! If you installed NW51SP3 first, and have trouble here, see the other tips at http://www.craigjconsulting.com.
5. Install NW51SP7.EXE (or later) - Reinstall this patch even if it was previously installed due to the older NIAS files being installed by BorderManager 3.6. See the note above about the installation of older files problem

6. If you only installed NW51SP6, install NLS603FT.EXE and run SETUPNLS.NLM. This is a post NW51SP6 patch. Run SETUPNLS afterwards.
7. If you only installed NW51SP6, install PURGE_NW.EXE. This is a post NW51SP6 patch to fix a problem in the NW51SP6 patch itself.
8. If you only installed NW51SP6, install NW56UP3.EXE. This is a post NW51SP6 / NW51SP5 patch.
9. PROXY.NLM – You can use the latest proxy for BorderManager 3.7 on 3.5 and 3.6 servers. Get it from whatever the latest BorderManager 3.7 patch is. Starting with the BM37FP4B.EXE patch, you may also have to copy in the AUTHCHK.NLM file to get proxy to load.
10. Optional - Install the CSATPXY.NLM from the latest BorderManager 3.7 patch to fix a logging issue.
11. TCP585VK.EXE, or later. This is a post-NW51SP7 patch.

CAUTION *Do NOT try to run TCPIP.NLM 5.5x after installing NW51SP4. SP4 puts on TCPIP 5.90j. If you feel that you need 5.53 (any version) for some reason, you need to uninstall SP$ and stay at SP3.*

---

12. Remove the Minimum and Maximum Packet Receive buffer limits that NW51SP3 (and later) patches put in AUTOEXEC.NCF, and run the TUNEUP.NCF file from tip #23 at http://www.craigjconsulting.com, or use your own settings. The limits from NW51SP3 are too low. Other support packs may hard-code this or similar settings into AUTOEXEC.NCF, so beware.
13. Install various other interim patches such as new versions of NAT or packet filtering modules. Check the Novell Support Connection public forums (news://support-forums.novell.com) and http://www.craigjconsulting.com for current information, as *not all available patches will show up on the minimum patch lis*t.
14. Update SYS:\ETC\PROXY\PROXY.CFG. You can use the example file maintained at my web site (http://www.craigjconsulting.com). The file provided by default has a bare minimum of entries, and many bug fixes and enhancements have been added to the PROXY.CFG file with each BorderManager patch. An example file is shown later in this book.

On NetWare 5.0

1. Install NetWare 5.0
2. Install a previous support pack, then NW50SP6A.EXE (Installing NW50SP6A, with DS 8 running on NetWare, can cause a serious problem IF a previous NetWare support pack has not been installed).
3. Install BorderManager 3.6. If you cannot install BorderManager at all, see the other tips at http://www.craigjconsulting.com.
4. Reinstall NW50SP6A.EXE - Reinstall this patch due to the older NIAS files being installed by BorderManager 3.6. See the cautionary note above at the beginning of the BorderManager 3.6 installation section about the installation of older files problem.
5. Install BM36SP2A.EXE or BM36SP1A.EXE (if you have it) - Addresses install bug for NetWare 6 and BorderManager 3.6. Do NOT reboot.
6. Install BM36NSP1.EXE - Replaces outdated NIAS files in BorderManager 3. This patch requires BM36SP1A to be installed first, which is the only reason to install BM36SP1A or BM36SP2A at this point. (You can reboot after this patch if you like).
7. Install BM36SP2A.EXE. You will need a customized install script from my web site in order to install this patch, since the patch came out after Novell dropped support for BorderManager on NetWare 5.0. See tip #1 at http://www.craigjconsulting.com for a link to the file.
8. PROXY.NLM – You can use the latest proxy for BorderManager 3.7 on 3.5 and 3.6 servers. Get it from whatever the latest BorderManager 3.7 patch is. Starting with the BM37FP4B.EXE patch, you may also have to copy in the AUTHCHK.NLM file to get proxy to load.
9. Optional - Install the CSATPXY.NLM from the latest BorderManager 3.7 patch to fix a logging issue.
10. Install TCP553V.EXE. You will not be able to install a later version of TCPIP on NetWare 5.0.
11. Install various other interim patches such as new versions of NAT or packet filtering modules. Check the Novell Support Connection public forums (news://support-forums.novell.com) and http://www.craigjconsulting.com for current information, as *not all available patches will show up on the minimum patch lis*t.

12. Update SYS:\ETC\PROXY\PROXY.CFG. You can use the example file maintained at my web site (http://www.craigjconsulting.com). The file provided by default has a bare minimum of entries, and many bug fixes and enhancements have been added to the PROXY.CFG file with each BorderManager patch. An example file is shown later in this book.

On NetWare 4.11/4.2

1. Install NetWare 4.11/4.2
2. Install NW4SP9.EXE
3. Install BorderManager 3.6 - (Install it from the root of the CD!!!)
4. Install BM36SP2A.EXE
5. PROXY.NLM – You can use the latest proxy for BorderManager 3.7 on 3.5 and 3.6 servers. Get it from whatever the latest BorderManager 3.7 patch is. Starting with the BM37FP4B.EXE patch, you may also have to copy in the AUTHCHK.NLM file to get proxy to load.
6. Optional - Install the CSATPXY.NLM from the latest BorderManager 3.7 patch to fix a logging issue.
7. Reinstall NW4SP9.EXE - Reinstall this patch due to the older NIAS files being installed by BorderManager 3.6. See the note above about the installation of older files problem.
8. Run the TUNEUP.NCF file from tip #23 at http://www.craigjconsulting.com, or use your own settings. (The limits from NW51SP3 (and later) are too low. Other patches may insert these or similar limits in AUTOEXE.NCF, so beware!
9. Install various other interim patches such as new versions of NAT or packet filtering modules. Check the Novell Support Connection public forums (news://support-forums.novell.com) and http://www.craigjconsulting.com for current information, as *not all available patches will show up on the minimum patch lis*t.
10. Update SYS:\ETC\PROXY\PROXY.CFG. You can use the example file maintained at my web site (http://www.craigjconsulting.com). The file provided by default has a bare minimum of entries, and many bug fixes and enhancements have been added to the PROXY.CFG file with each BorderManager patch. An example file is shown later in this book.

Installing BorderManager 3.5

If you had ever installed the old 3.5 Enhancement Pack, the problems in updating it are over. The BorderManager 3.5 Service Pack 2 and later is compatible with newer proxy/ACL patch code (as in the BM35C09.EXE patch) and includes the Enhancement Pack features. The BM35SP2 or BM35SP3 patches can be installed over servers running either the BM35C0x or Enhancement Pack patches.

On NetWare 5.1

1. Install NetWare 5.1
2. Install BorderManager 3.5 (Install it from the root of the CD!!!) If you cannot install BorderManager at all, see the other tips at http://www.craigjconsulting.com.
3. Install RADCLNT1.EXE - A RADIUS patch, if you are using RADIUS.
4. Install NW51SP6.EXE.

Note Mar. 1, 2002: There is a bug in TCPCFG.NLM in NW51SP4.EXE. The result is that NAT Implicit Filtering gets enabled every time you start INETCFG. This will cause inbound traffic to reverse proxies, and (probably) to static NAT to fail. There is also a bug in NW51SP5 that causes issues with IPX over Site-Site VPN. The VPTFIX.EXE patch should take care of both issues.

CAUTION *Do NOT try to run TCPIP.NLM 5.5x after installing NW51SP4. SP4 puts on TCPIP 5.90j. If you feel that you need 5.53 (any version) for some reason, you need to uninstall SP4 and stay at SP3.*

---

5. NOTE: Do NOT try to run TCPIP.NLM 5.5x after installing NW51SP4. SP4, and later, puts on TCPIP 5.90j. If you feel that you need 5.53 (any version) for some reason, you need to uninstall SP4 and stay at SP3. You can use TCP553V.EXE for NW 5.1 SP3 servers.
6. Install PURGE_NW.EXE. This is a post NW51SP6 patch to fix a problem in the NW51SP6 patch itself.
7. Install NW56UP3.EXE. This is a post NW51SP6 / NW51SP5 patch.
8. PROXY.NLM – You can use the latest proxy for BorderManager 3.7 on 3.5 and 3.6 servers. Get it from whatever the latest BorderManager 3.7 patch is. Starting with the BM37FP4B.EXE patch, you may also have to copy in the AUTHCHK.NLM file to get proxy to load.

---

9. Optional - Install the CSATPXY.NLM from the latest BorderManager 3.7 patch to fix a logging issue.
10. BM35SP3.EXE Requires at least NW51SP2. If you install the NW51 service pack after this patch, reinstall this patch. See also a discussion of BorderManager filtering modules!) Has Code Red and RealAudio/RTSP fixes.
11. BM35ADM7.EXE Addresses interoperability issues between the Login Policy Object created by NMAS / NetWare 6 install when BorderManager or RADIUS already exists in the tree.
12. RADATR4.EXE If you are using RADIUS, install this update.
13. VPTFIX.EXE Fixes problem with VPN losing IPX capability. Applies to NW51SP4 and NW51SP5 servers, but not NW51SP3 or NW51SP6. Has a later version of INETLIB.NLM than included in NW51SP5.
14. IPFLT1.EXE IP filter module patch. (If still available for download. The IPFLT.NLM and IPFLT31.NLM files were updated in BM37SP1.EXE and BM36SP2A.EXE.)
15. TCP583K.EXE Post-NW51SP6 patch for TCPIP. Do NOT try to run TCPIP.NLM 5.5x after installing NW51SP4 or later. If you feel that you need 5.53 (any version) for some reason, you need to uninstall SP4/SP5/SP6 and stay at SP3. See tip #6 at my web site.
16. NAT600D.EXE (Only needed if running NW51SP4. NW51SP5 and later has this, or newer, version.) Newer version of NAT which (usually) fixes an issue with Client-Site VPN pinging private IP address of the BorderManager Server.
17. FLSYSFT7.EXE (Only needed if running NW51SP4. NW51SP5and NW51SP6 has a later version.) Check the readme..
18. Remove the Minimum and Maximum Packet Receive buffer limits if the support pack puts that in AUTOEXEC.NCF, and run the TUNEUP.NCF file from tip #23 at http://www.craigjconsulting.com, or use your own settings. (The limits from NW51SP3 (and later) are too low. Other patches may insert these or similar limits in AUTOEXE.NCF, so beware!

Note Running the SYS:PUBLIC\BRDRMGR\SNAPINS\SETUP.EXE program to update the NWADMN32 snapin files after installing the BM35SP2 patch does NOT help to copy snapins to another server, because the patch doesn't update that directory. (The BorderManager server itself is correctly updated by installing the patch. Instead, manually copy the updated snapins from the BM35SP2 \public\win32\snapins directory to the BM server's \public\brdrmgr\snapins\data\border\win32\snapins directory. Then rerun the snapin setup against the desired servers.

19. Run the CyberPatrol CP_SETUP.EXE program to extract the new files and apply them.
20. Install various other interim patches such as new versions of NAT or packet filtering modules. Check the Novell Support Connection public forums (news://support-forums.novell.com) and http://www.craigjconsulting.com for current information, as *not all available patches will show up on the minimum patch lis*t.
21. Update SYS:\ETC\PROXY\PROXY.CFG. You can use the example file maintained at my web site (http://www.craigjconsulting.com). The file provided by default has a bare minimum of entries, and many bug fixes and enhancements have been added to the PROXY.CFG file with each BorderManager patch. An example file is shown later in this book.

On NetWare 5.0

1. Install NetWare 5.0
2. Install NW5SP2A.EXE - This patch is present on the BorderManager installation CD under the CSP directory. Installing NW50SP6A.EXE, with DS 8 running on NetWare, can cause a serious problem IF a previous NetWare support pack has not been installed).
3. Install BorderManager 3.5 - Install it from the root of the CD! If you cannot install BorderManager at all, see the other tips at http://www.craigjconsulting.com.
4. Install NW50SP6A.EXE - Includes newer BorderManager filtering modules - Do NOT reboot yet!)
5. Install NICID157.EXE - Install the NICI 1.5.7 update, and reboot. See service pack issues mentioned at http://www.craigjconsulting.com in tip #1.
6. Install BM35SP3.EXE - Requires NW50SP6 or later. If you install the NW5 service pack after this patch, reinstall this patch. You REALLY NEED TO read the discussion of BorderManager filtering modules at http://www.craigjconsulting.com if you choose to apply

NW5SP5 and have not applied BM35SP1 before!) Has Code Red and RealAudio/RTSP fixes.

7. PROXY.NLM – You can use the latest proxy for BorderManager 3.7 on 3.5 and 3.6 servers. Get it from whatever the latest BorderManager 3.7 patch is. Starting with the BM37FP4B.EXE patch, you may also have to copy in the AUTHCHK.NLM file to get proxy to load.
8. Optional - Install the CSATPXY.NLM from the latest BorderManager 3.7 patch to fix a logging issue.
9. Install BM35ADM6.EXE - Addresses interoperability issues between the Login Policy Object created by NMAS / NetWare 6 install when BorderManager or RADIUS already exists in the tree. If you installed BM36C01A.EXE, you don't need this patch.
10. RADAT4.EXE - If you are using RADIUS, install this update.
11. NAT600D.EXE (or later) - If using Client-Site VPN, check that you can ping the BorderManager internal IP address with this version of NAT. If there is a problem, try back-revving NAT.NLM.
12. Install ADMN519F.EXE – A NWADMN32 update that helps with snapin issues somewhat.

Note Running the SYS:PUBLIC\BRDRMGR\SNAPINS\SETUP.EXE program to update the NWADMN32 snapin files after installing the BM35SP2 patch does NOT help to copy snapins to another server, because the patch doesn't update that directory. (The BorderManager server itself is correctly updated by installing the patch. Instead, manually copy the updated snapins from the BM35SP2 \public\win32\snapins directory to the BorderManager server's sys:\public\brdrmgr\snapins\data\border\win32\snapins directory. Then rerun the snapin setup against the desired servers.

---

13. Run the CyberPatrol CP_SETUP.EXE program to extract the new files and apply them. (Note: As of 2004, SurfControl has quit supporting or updating CyberPatrol. In order to run a content filtering program, your only choice now is LinkWall).
14. Install the latest TCPIP.NLM, if one has been released separate from the NetWare service pack.
15. Install various other interim patches such as new versions of NAT or packet filtering modules. Check the Novell Support Connection public forums (news://support-forums.novell.com) and http://www.craigjconsulting.com for current information, as *not all available patches will show up on the minimum patch list*.

16. Update SYS:\ETC\PROXY\PROXY.CFG. You can use the example file maintained at my web site (http://www.craigjconsulting.com). The file provided by default has a bare minimum of entries, and many bug fixes and enhancements have been added to the PROXY.CFG file with each BorderManager patch. An example file is shown later in this book.

On NetWare 4.11

1. Install NetWare 4.11
2. Install IWSP6A.EXE – As a minimum. You can also install NW4SP9. This patch is provided on the BorderManager 3.5 CD under the CSP directory. If you start with NW4SP9, you should re-install it after BorderManager 3.5 is installed.)
3. Install BorderManager 3.5 - Install it from the root of the CD!
4. Install NW4SP9.EXE - Includes newer BorderManager filtering modules.)
5. Install BM35SP3.EXE - Requires NW4SP9.EXe. If you install the NW4 service pack after this patch, reinstall this patch. You REALLY NEED TO read the discussion of BorderManager filtering modules at http://www.craigjconsulting.com if you choose to apply NW4SP8A and have not applied BM35SP1 before!). Has Code Red and RealAudio/RTSP fixes.
6. PROXY.NLM – You can use the latest proxy for BorderManager 3.7 on 3.5 and 3.6 servers. Get it from whatever the latest BorderManager 3.7 patch is. Starting with the BM37FP4B.EXE patch, you may also have to copy in the AUTHCHK.NLM file to get proxy to load.
7. Optional - Install the CSATPXY.NLM from the latest BorderManager 3.7 patch to fix a logging issue.
8. BM35ADM6.EXE - Addresses interoperability issues between the Login Policy Object created by NMAS / NetWare 6 install when BorderManager or RADIUS already exists in the tree. If you installed BM36C01A.EXE, you don't need this patch.
9. RADAT4.EXE - If you are using RADIUS, install this update.
10. NAT600D.EXE (or later) - If using Client-Site VPN, check that you can ping the BorderManager internal IP address with this version of NAT. If there is a problem, try back-revving NAT.NLM.

Note Running the SYS:PUBLIC\BRDRMGR\SNAPINS\SETUP.EXE program to update the NWADMN32 snapin files after installing the BM35SP2 patch does NOT help to copy snapins to another server, because the patch doesn't update that directory. (The BorderManager server itself is correctly updated by installing the patch. Instead, manually copy the updated snapins from the BM35SP2 \public\win32\snapins directory to the BorderManager server's sys:\public\brdrmgr\snapins\data\border\win32\snapins directory. Then rerun the snapin setup against the desired servers.

11. Run the CyberPatrol CP_SETUP.EXE program to extract the new files and apply them. (Note: As of 2004, SurfControl has quit supporting or updating CyberPatrol. In order to run a content filtering program, your only choice now is LinkWall).
12. Install the latest TCPIP.NLM, if one has been released separate from the NetWare service pack.
13. Install various other interim patches such as new versions of NAT or packet filtering modules. Check the Novell Support Connection public forums (news://support-forums.novell.com) and http://www.craigjconsulting.com for current information, as *not all available patches will show up on the minimum patch lis*t.
14. Update SYS:\ETC\PROXY\PROXY.CFG. You can use the example file maintained at my web site (http://www.craigjconsulting.com). The file provided by default has a bare minimum of entries, and many bug fixes and enhancements have been added to the PROXY.CFG file with each BorderManager patch. An example file is shown later in this book.

Installing BorderManager 3.0

BorderManager 3.0 is not supported on NetWare 5.1 BorderManager 3.0 is also EOL (End Of Life), and no new patches are being created for it. If you have abends with BorderManager 3.0 and you have the patches listed below, upgrade to the latest released version of BorderManager.

On NetWare 5.0

1. Install NetWare 5.0
2. Install BorderManager 3.0 - If you cannot install BorderManager at all, see the other tips at http://www.craigjconsulting.com.
3. Install NW50SP6A.EXE - Do NOT reboot yet!) - OR, install an earlier NetWare support pack BEFORE trying to install NW50SP6A.
4. Install NICID157.EXE - Install the NICI 1.5.7 update, and reboot. See service pack issues discussed in tip #1 at http://www.craigjconsulting.com.
5. Install BM30SP3.EXE - Requires at least NW 5.0 Support Pack 4 to be installed. It also includes a new VPN client.)
6. Install BM3LICFX.EXE – Fixes some licensing issues.
7. Install BM3CP3.EXE - This is a CyberPatrol 6/16/2000 update.
8. Install ADMN519F.EXE – This is a NWADMN32 update that helps with snapin issues somewhat.
9. Install BM3SS02.EXE – Contains newer CLNTRUST.EXE.
10. RADAT4.EXE - If you are using RADIUS, install this update.
11. Install NAT600D.EXE - If using Client-Site VPN, check that you can ping the BorderManager internal IP address with this version of NAT. If there is a problem, try back-revving NAT.NLM.
12. Install the latest TCPIP.NLM, if one has been released separate from the NetWare service pack.
13. Install various other interim patches such as new versions of NAT or packet filtering modules. Check the Novell Support Connection public forums (news://support-forums.novell.com) and http://www.craigjconsulting.com for current information, as *not all available patches will show up on the minimum patch list*.

On NetWare 4.11 / 4.20

1. NetWare 4.11

2. Install BorderManager 3.0
3. Install NW4SP9.EXE
4. Install BM30SP3.EXE - Requires NW 4.11/4.2 Support Pack 8A to be installed. This is a 56-bit version patch. It also includes a new VPN client.
5. Install BM3CP3.EXE - This is a CyberPatrol 6/16/2000 update)
6. Install BM3SS02.EXE – Contains a newer CLNTRUST.EXE.
7. Install RADAT4.EXE - If you are using RADIUS, install this update.
8. Install NAT600D.EXE - If using Client-Site VPN, check that you can ping the BorderManager internal IP address with this version of NAT. If there is a problem, try back-revving NAT.NLM.
9. Install the latest TCPIP.NLM, if one has been released separate from the NetWare service pack.
10. Install various other interim patches such as new versions of NAT or packet filtering modules. Check the Novell Support Connection public forums (news://support-forums.novell.com) and http://www.craigjconsulting.com for current information, as *not all available patches will show up on the minimum patch lis*t.

Upgrade Considerations

If you are upgrading an older version of BorderManager, there are a few precautions you should take:

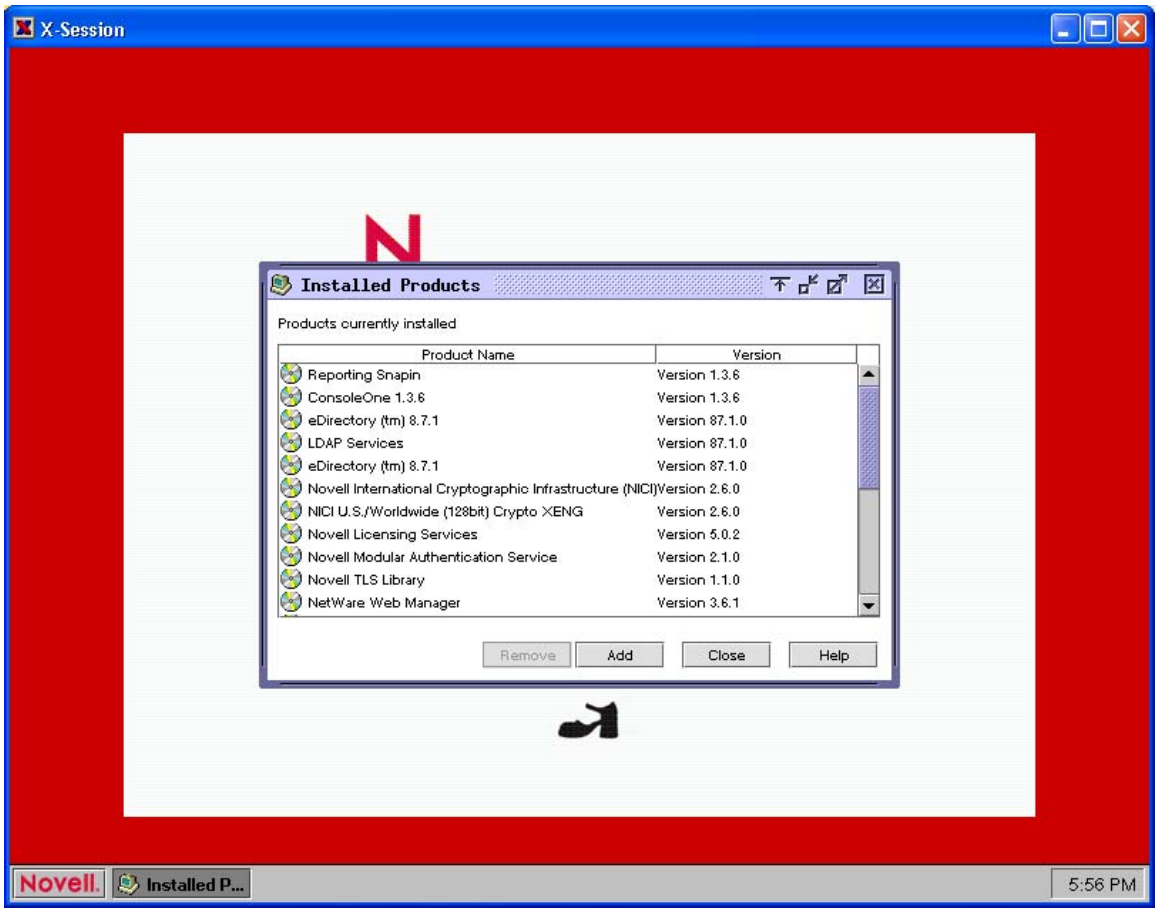
1. **Back up all the files in the SYS:\ETC directory!** This will give you a backup of your filters, static routes, static NAT assignments, and several other useful files. If you are already at BorderManager 3.7, the file holding filters may not be current, if you did used iManager instead of FILTCFG to configure filtering.
2. LOAD CONFIG /S at the server console. This will generate a file called CONFIG.TXT in SYS:SYSTEM. This file is VERY useful for documenting many critical server settings. If you do not have CONFIG.NLM, you can get it from the Minimum Patch List at http://support.novell.com.
3. Be sure you have installed the Microsoft Clipboard Viewer on your PC. (It should be in the Accessories folder, on Win9x. In Windows XP, you can use the CLIPBRD.EXE file in SYSTEM32.) In NWADMN32, BorderManager Access Rules, highlight all the access rules and copy them to the clipboard. Use Clipboard Viewer to save the contents of the clipboard to a .CLP file. You will not be able to view the contents, just save/retrieve them. This backs up all your access rules to a file.
4. Install BorderManager 3.x over the top of your existing BorderManager configuration. In general, old settings should be retained.
5. For BorderManager 3.7 or 3.8 upgrades from 3.6 or earlier versions, **you will need to migrate any existing IP filter exceptions into NDS**. UNLOAD IPFLT, then UNLOAD FILTSRV. Now LOAD FILTSRV MIGRATE, and afterwards LOAD IPFLT again. Unless you know thoroughly what you are doing with BorderManager 3.7 or 3.8 and how it handles filtering changes, use only iManager to administer filters and exceptions. (I cover filtering administration in much depth in my book "*Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions*". The Third Edition or later of that book covers the BorderManager 3.7 and 3.8 filtering system.
6. If you are going to use the new SurfControl content management system, your old CyberPatrol Access Rule will need to be deleted and replaced with a new one for SurfControl, after you have installed SurfControl. There is no way to automatically 'map' the old CyberPatrol Categories to the new SurfControl categories.

7. If you are upgrading from BorderManager 2.1, you would be well advised to install from fresh. In-place upgrades sometimes work, and sometimes fail.
8. The packet filtering capabilities of BorderManager 3.x are far more sophisticated than BorderManager 2.1. You would be well advised to review every custom packet filter exception with an eye to redoing any outbound exception to take advantage of stateful packet filtering.
9. If you are planning on migrating to NetWare 5.1 or 6.0 concurrently with your BorderManager 3.5, 3.6, 3.7 or 3.8 upgrade, perform the BorderManager upgrade first. BorderManager 3.0 is not supported on NetWare 5.1 or later.
10. BorderManager 3.8 is the **only** version of BorderManager that will run on NetWare 6.5. If you are planning on upgrading to NetWare 6.5, be sure that you are also planning on using BorderManager 3.8.
11. Be careful that you do not accidentally try to assign the old BorderManager licenses to BorderManager as the old licenses will not work. An exception is that BorderManager 3.6 will use BorderManager 3.5 licenses.

Example Installation of BorderManager 3.8 on NetWare 6.0

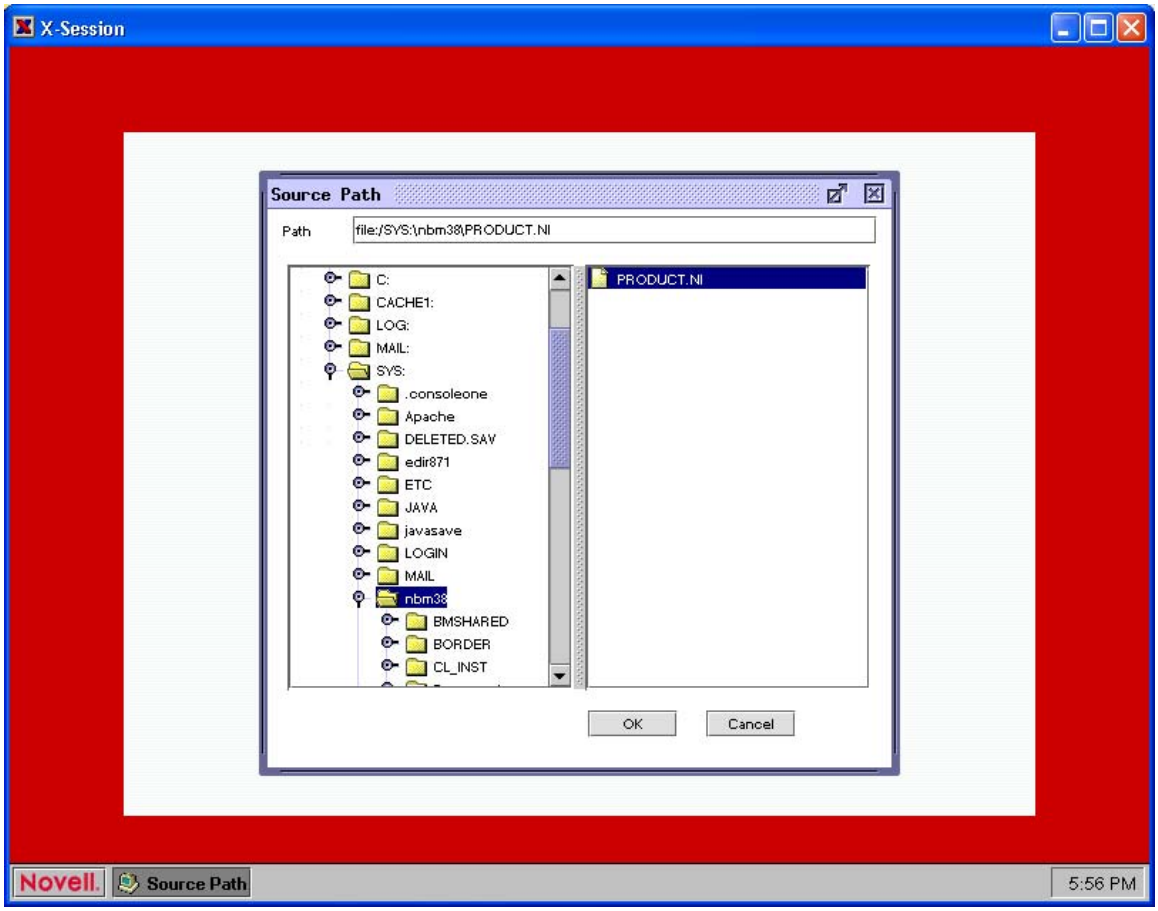
The following section shows how I installed BorderManager 3.8 on a NetWare 6.0, server, after first patching it with NW6SP3.EXE, installing eDirectory 8.71, NICI 2.6.0 and the BorderManager 3.8 version of TCP/IP (domestic).

I also ran INETCFG at least once before installing BorderManager as the installation will prompt you to do that otherwise.



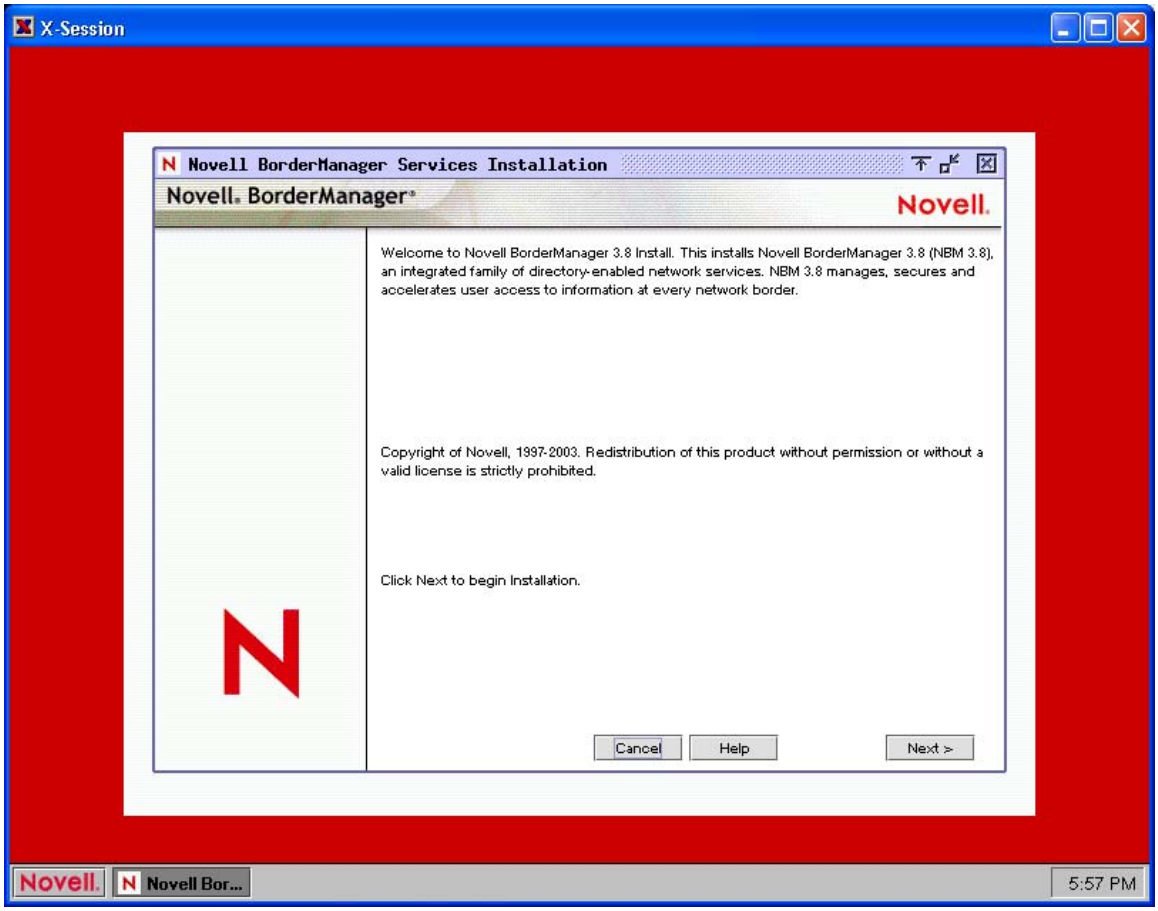
This installation was done by copying files to the local server, and upgrading over an existing BorderManager 3.6 server.

Start the graphical user interface on NetWare (run STARTX). Launch the Install dialog from the pop up menu in the lower left.

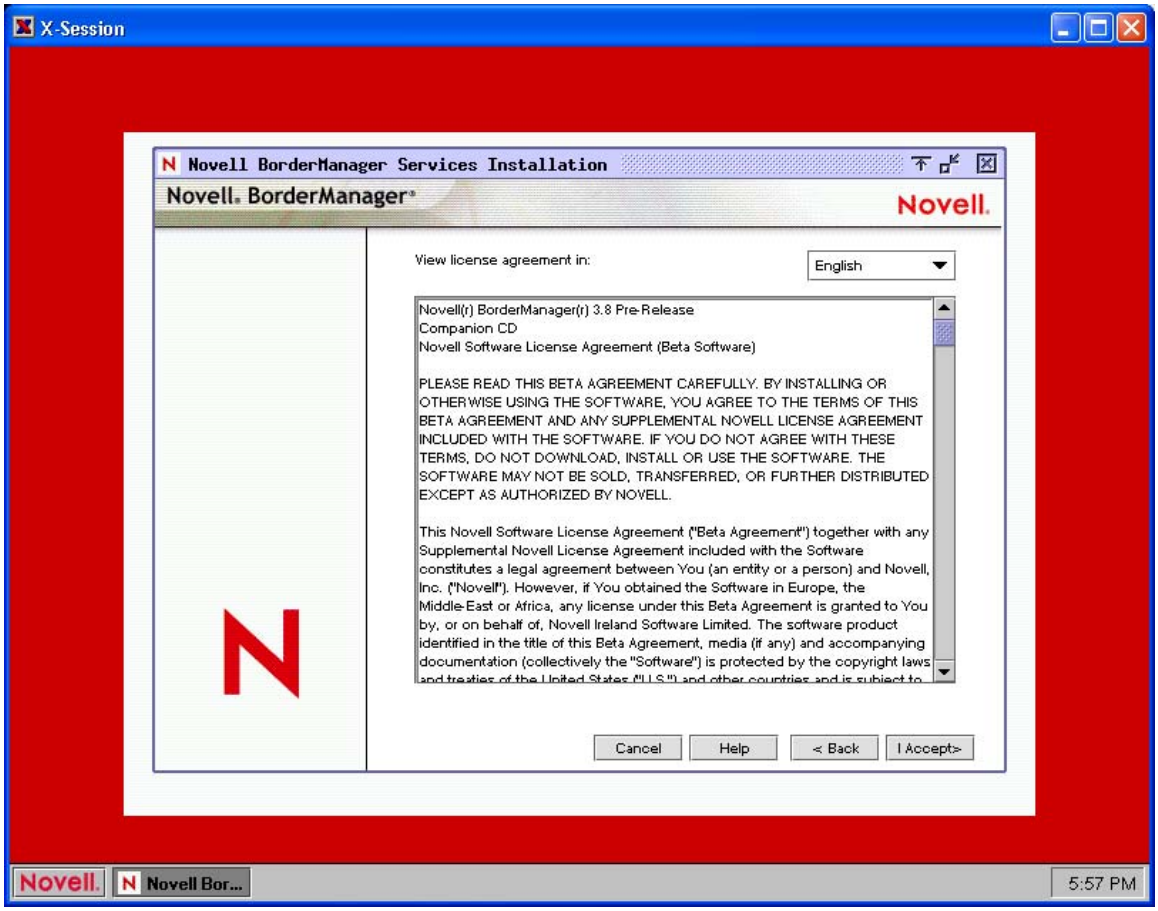


Browse to the location of the PRODUCT.NI file on the BorderManager CD, and click on **OK**

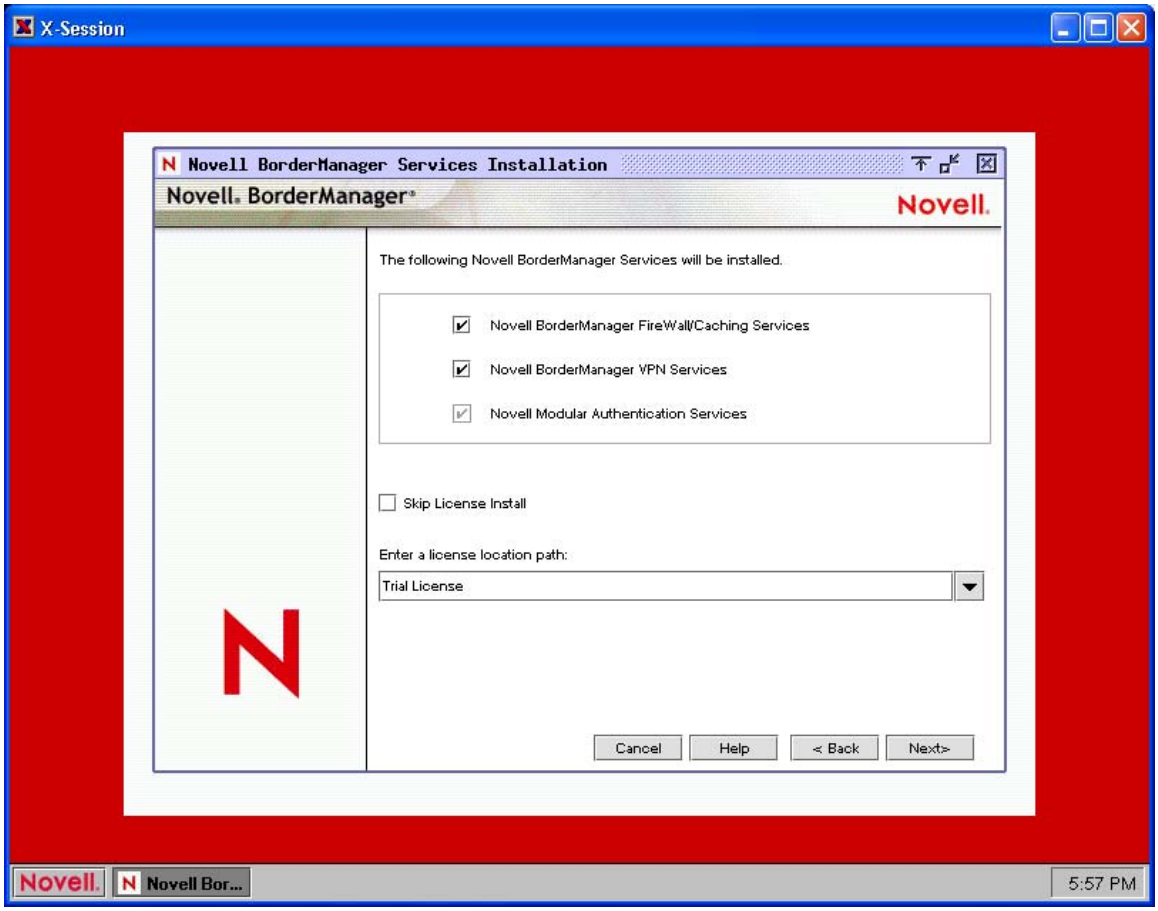
File copying should start.



You should get to a screen that tells you that BorderManager 3.8 is about to be installed. Click **Next** to continue.



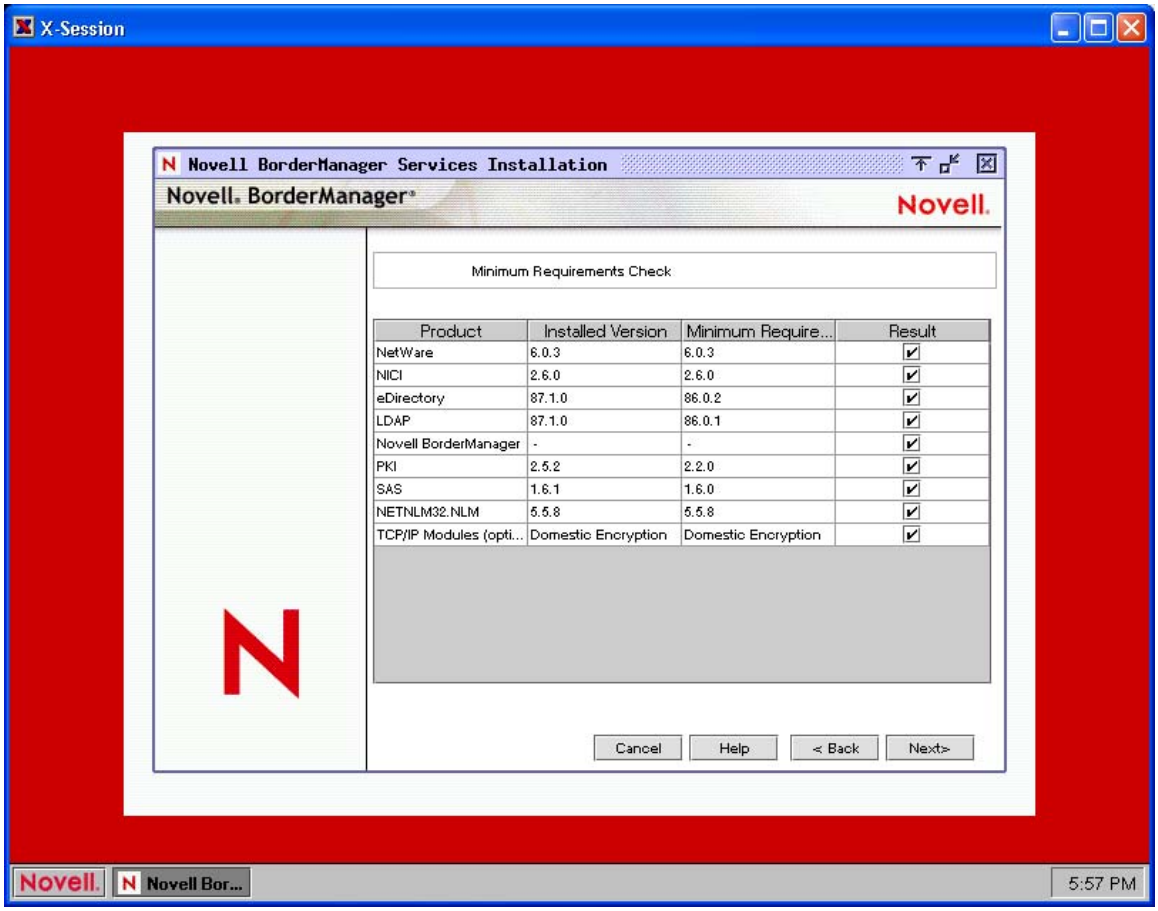
If the proper patches have been installed on NetWare before you begin installing BorderManager, you should reach the License Agreement screen. Click on '**I Accep**t' to continue.



Depending on your needs, you can install some or all of the BorderManager 3.8 components. Essentially, all component files will be installed, and the check boxes simply indicate which LICENSES will be installed for you. I recommend installing all features, even if you do not use them at first.

You can point to a file location holding the licenses now, or add the licenses later. In the example above, I skipped the license install at this point, and added them later using iManager.

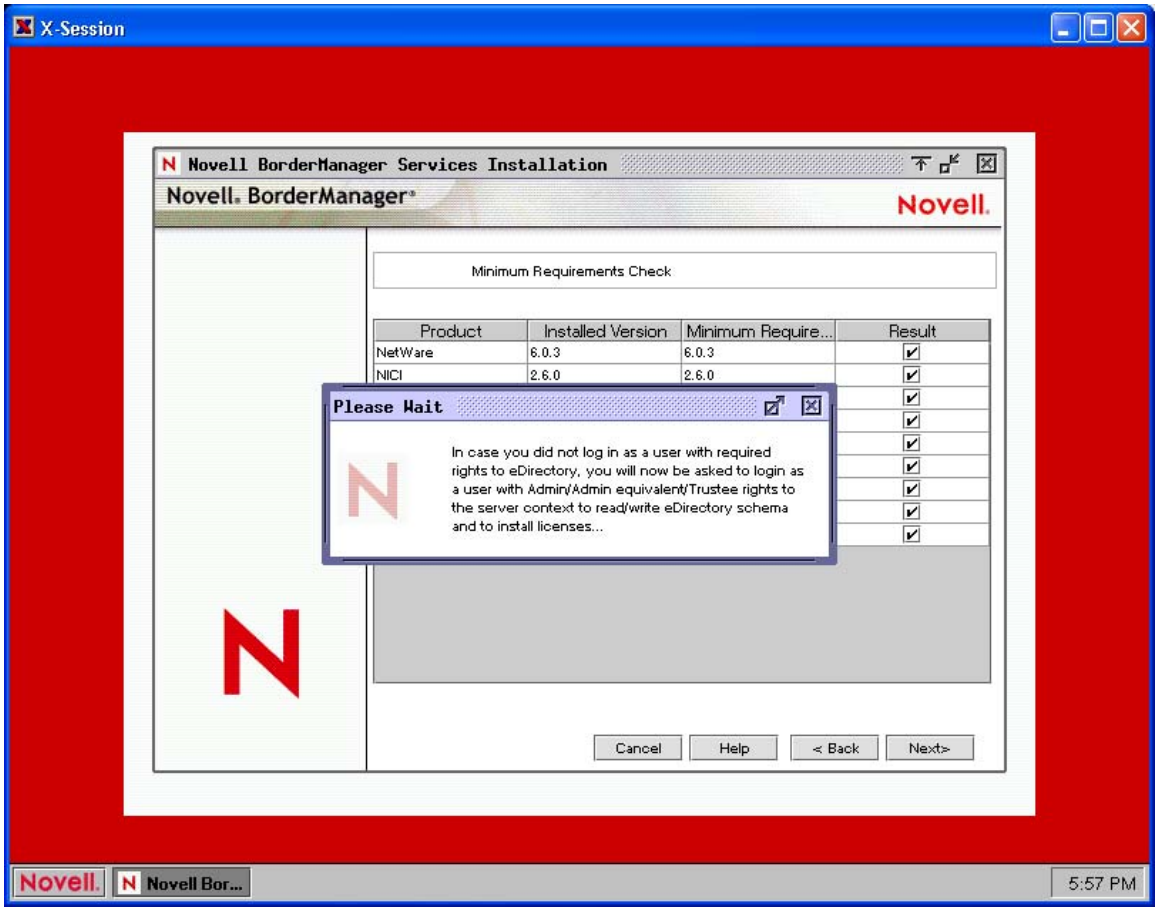
Click **Next** to continue.



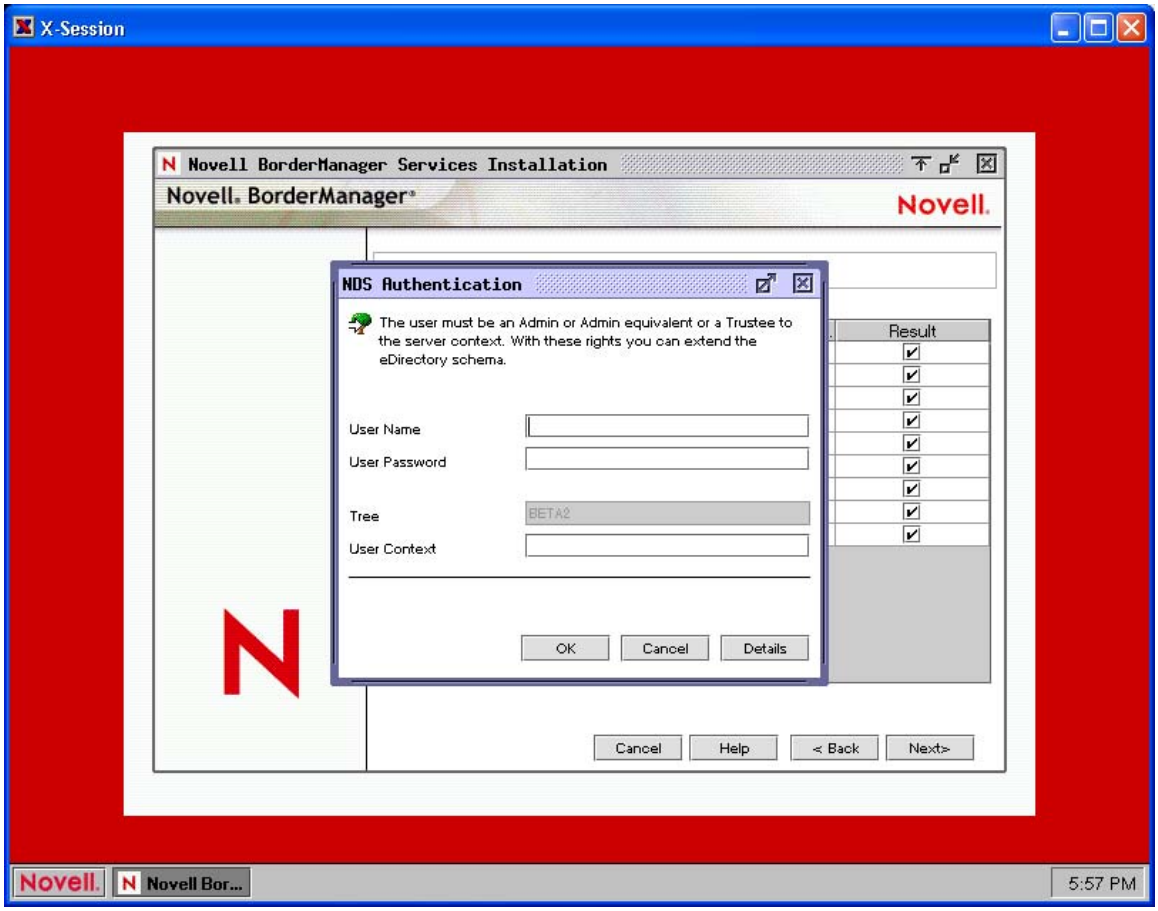
You should now see the BorderManager 3.8 requirements check screen.

If you have not met the basic requirements, you will have to cancel the installation, install the required products or patches, and begin the installation again.

Click **Next** to continue only if all requirements have been met.

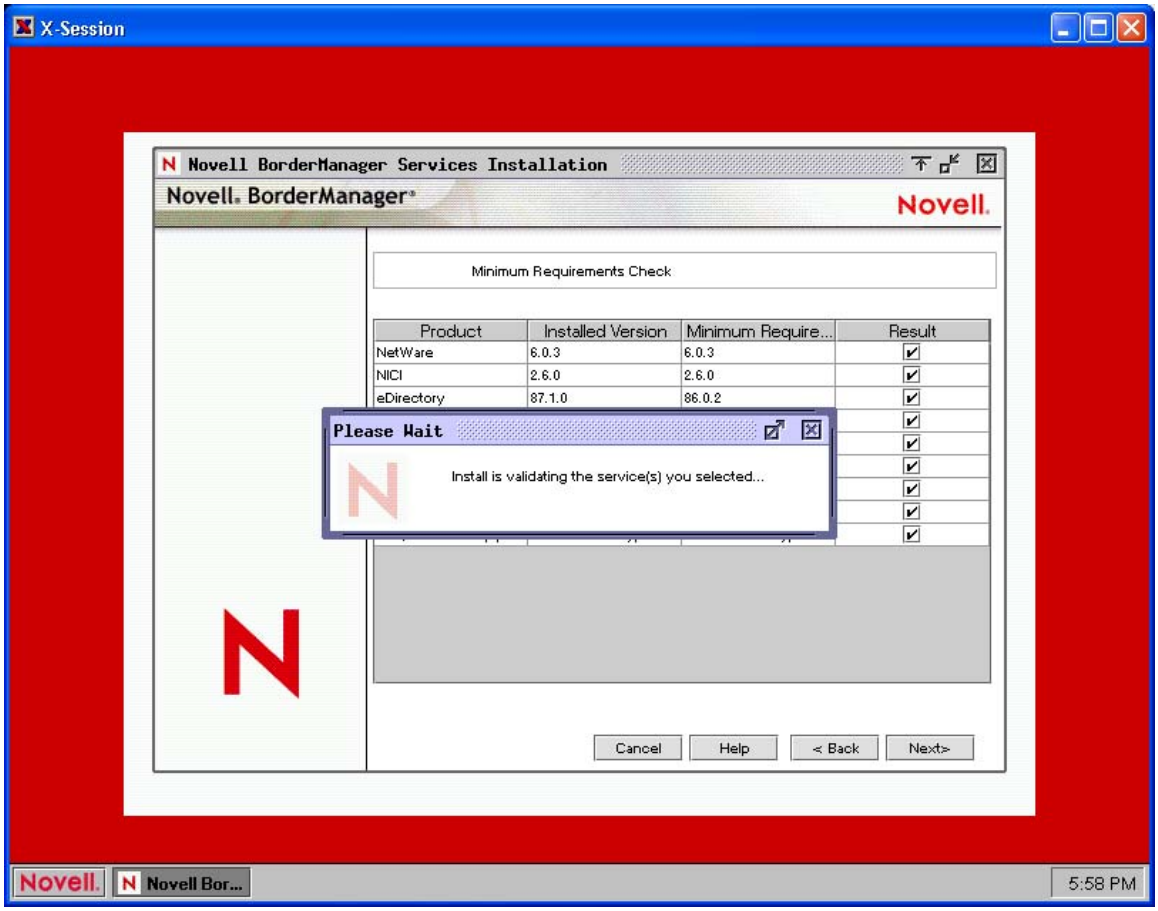


You will be required to log in as an admin-equivalent user next.

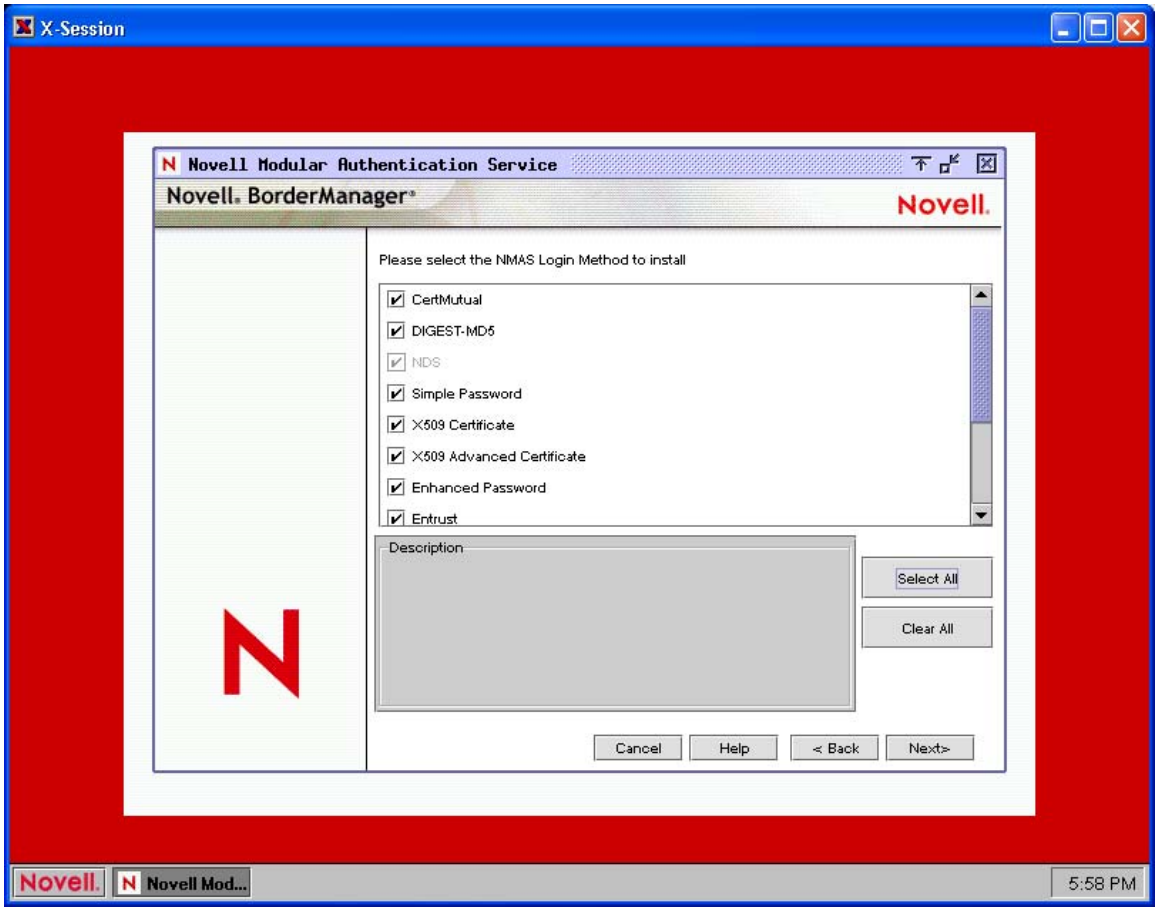


Log in as Admin, or an admin-equivalent user with the necessary NDS rights to extend the schema for the NDS tree.

Click **OK** to continue.

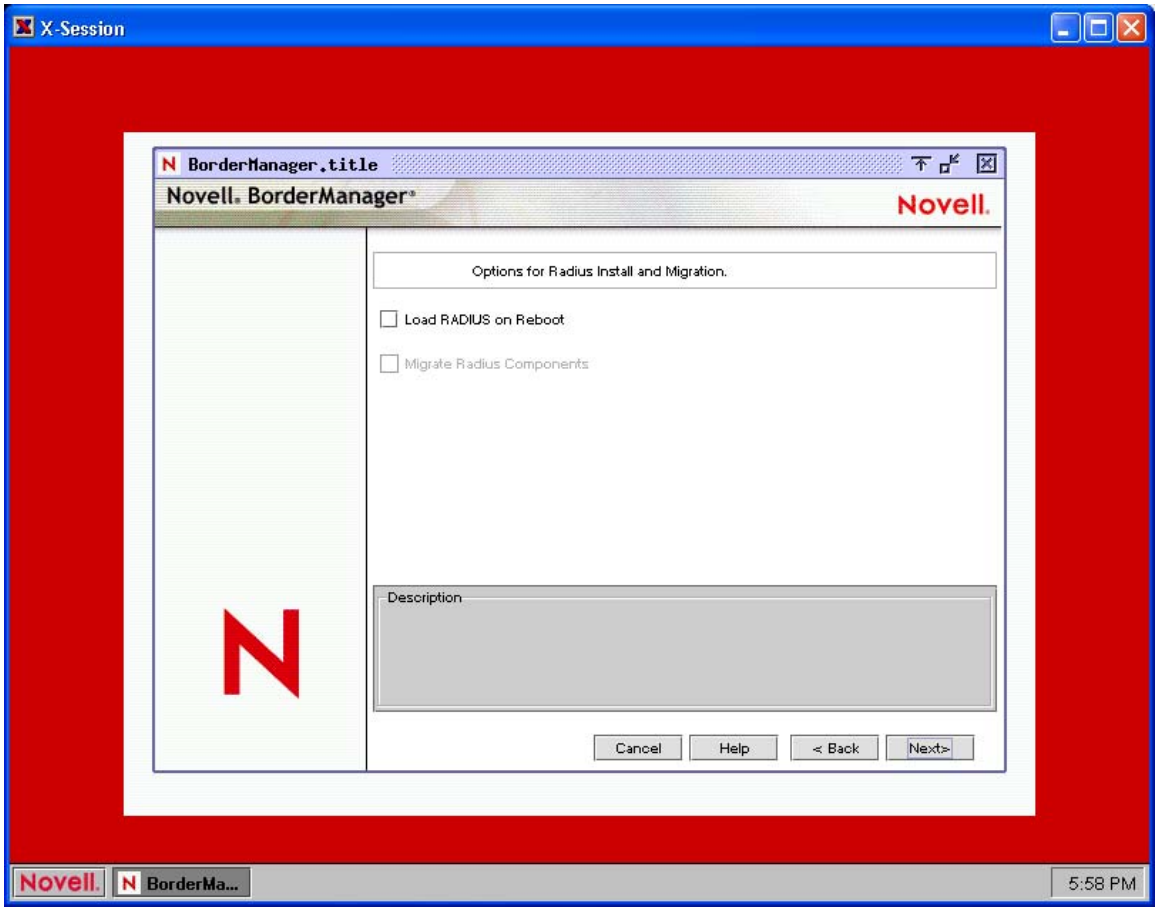


The services you selected will be validated, and you will experience a short delay.



Next, you will be given the option to install NMAS methods. I recommend installing them all.

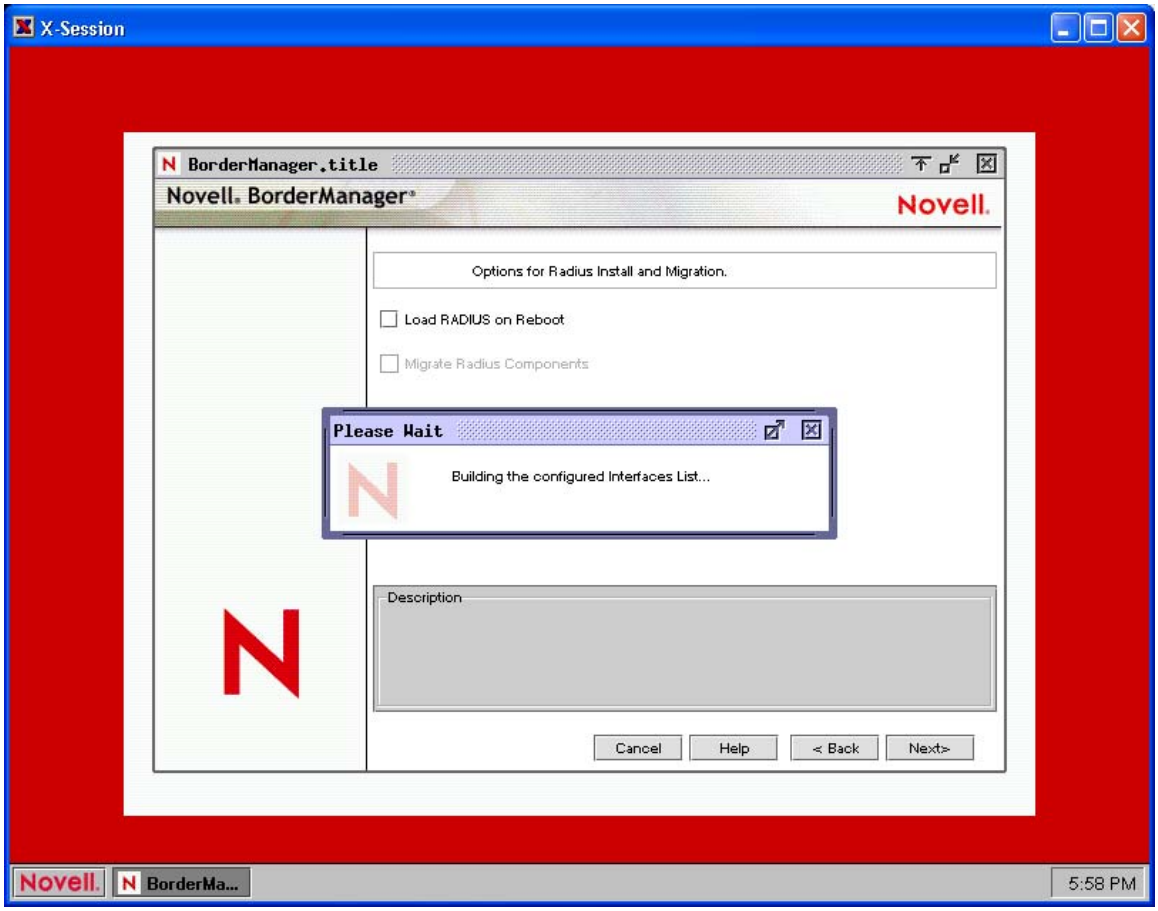
Click **Select All**, then click **Next** to continue.



You should get an option to load or not load RADIUS on reboot at this point. The effect of this option is to put a LOAD RADIUS statement in the STARTBRD.NCF file.

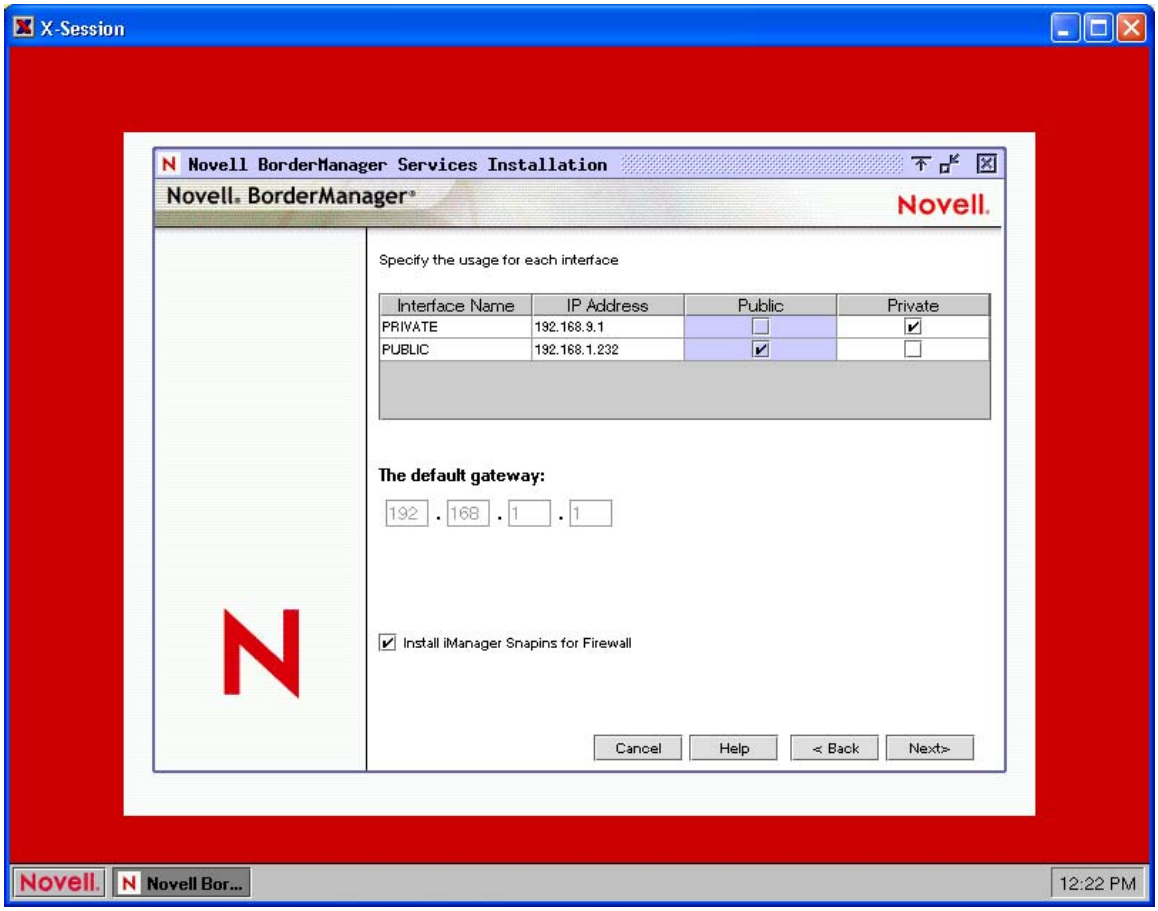
I rarely use RADIUS on a BorderManager server, but if you want it loaded automatically when the server reboots, select it here. However, you will still need to go in to the STARTBRD.NCF file and add command line options for the Dial Access System to be used if you want RADIUS to actually load and work with no further intervention.

Click **Next** to continue.



BorderManager will now build a list of interfaces that are already configured.

You may be prompted to run INETCFG.NLM on the server at least once before this step can succeed.



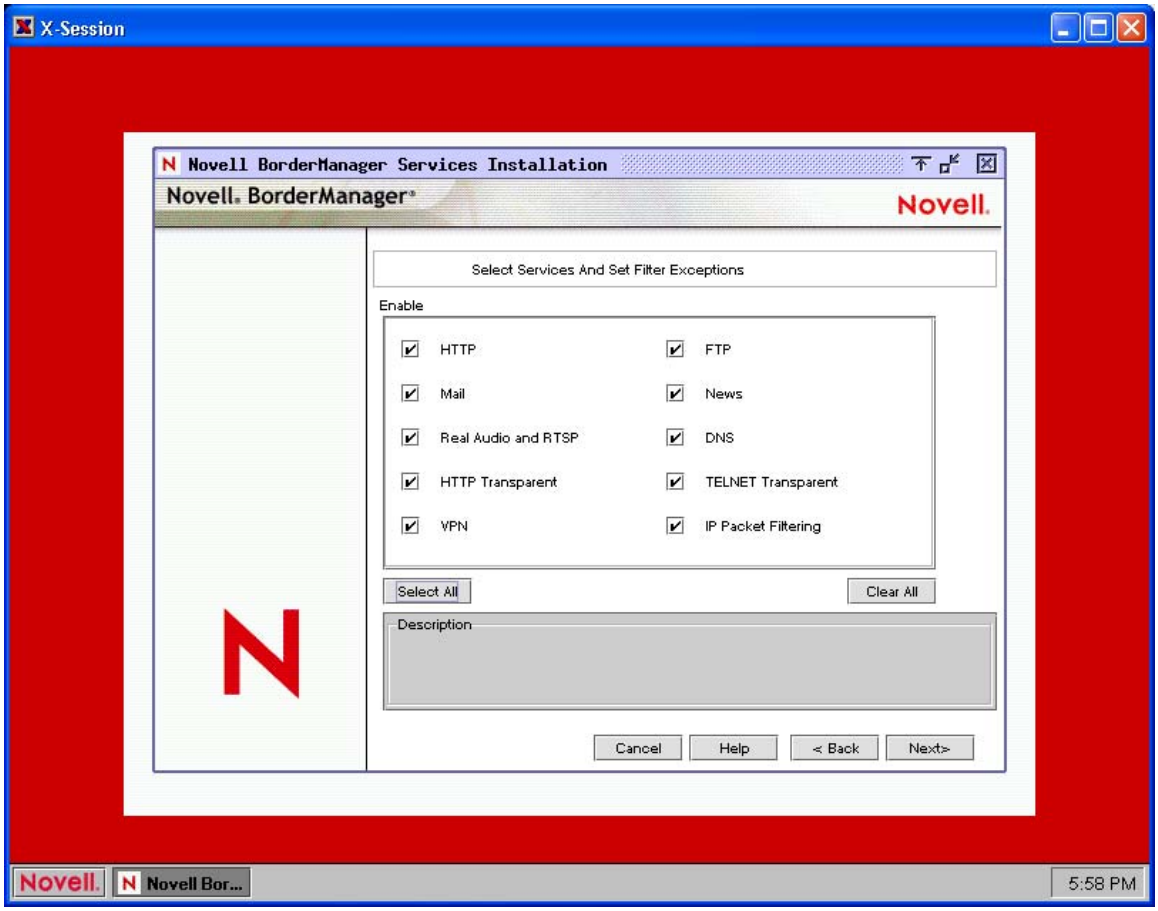
The interfaces configured in INETCFG will be shown next, and you can choose which interfaces are to be PUBLIC and PRIVATE, for filtering and proxies.

The Default Gateway is read from the SYS:ETC\GATEWAYS file (and is configured in INETCFG, Protocols, LAN Static Routing).

Install iManager Snapins for Firewall should copy the filtering snapins, but only for iManager 2.0 on NetWare 6.5 servers. See the chapter on iManager later in this book for information on configuring iManager with filtering and VPN snapins.

Note BorderManager 3.8 does not ship with snapins that work with versions of iManager before version 2.0, meaning that managing BorderManager 3.8 VPN on NetWare 6.0 or 5.1 requires either a NetWare 6.5 server to be present, or iManager 2.0 installed on a Windows PC.

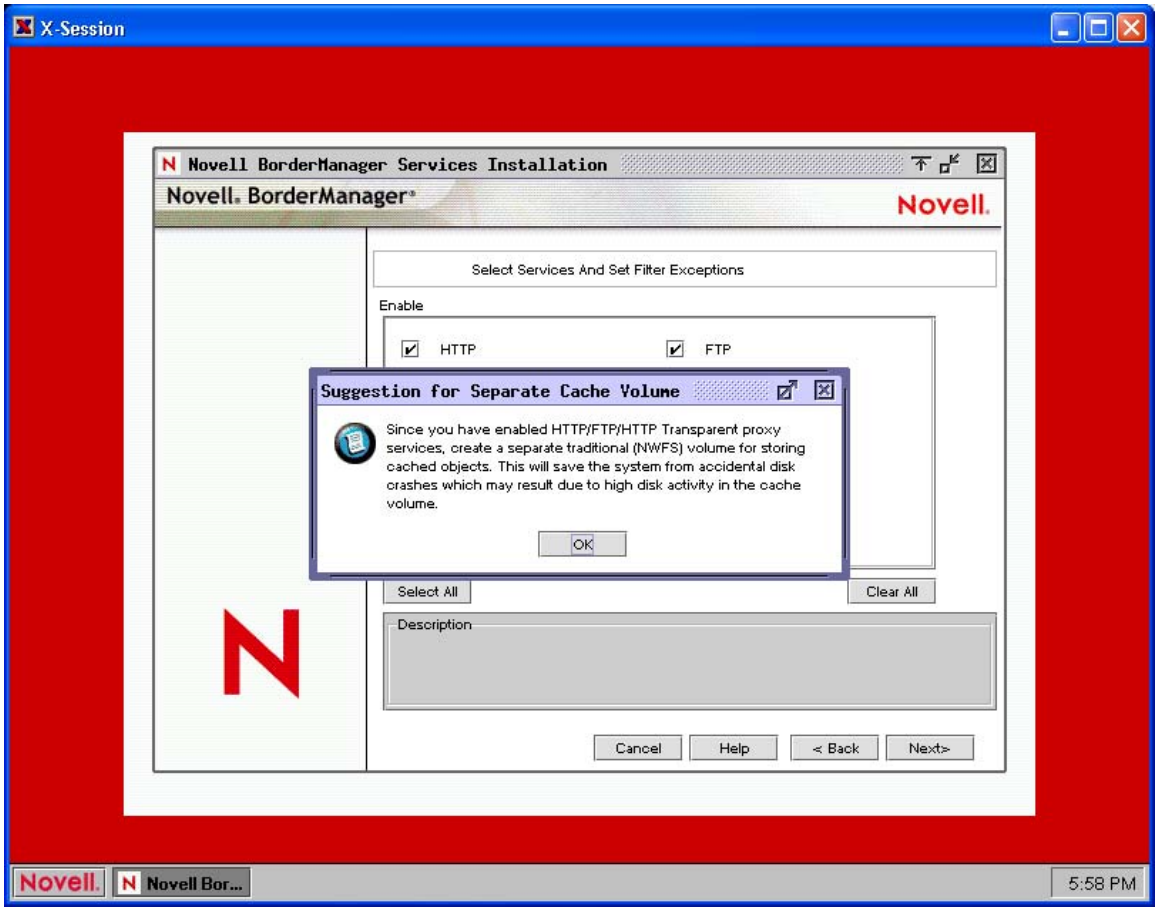
Click **Next** to continue.



You will next be asked to select proxies to be used later. Choosing proxies at this point results in filter exceptions being added to allow the proxies to function, and also will result in some of the proxies being enabled in NWADMN32.

Click on **Select All** (you can always turn off the selections you do not want later), and then click **Next** to continue.

Note The filter exceptions configured by any of these selections do not allow internal hosts to make connections to the Internet. The filter exceptions are configured only for use by the proxies.



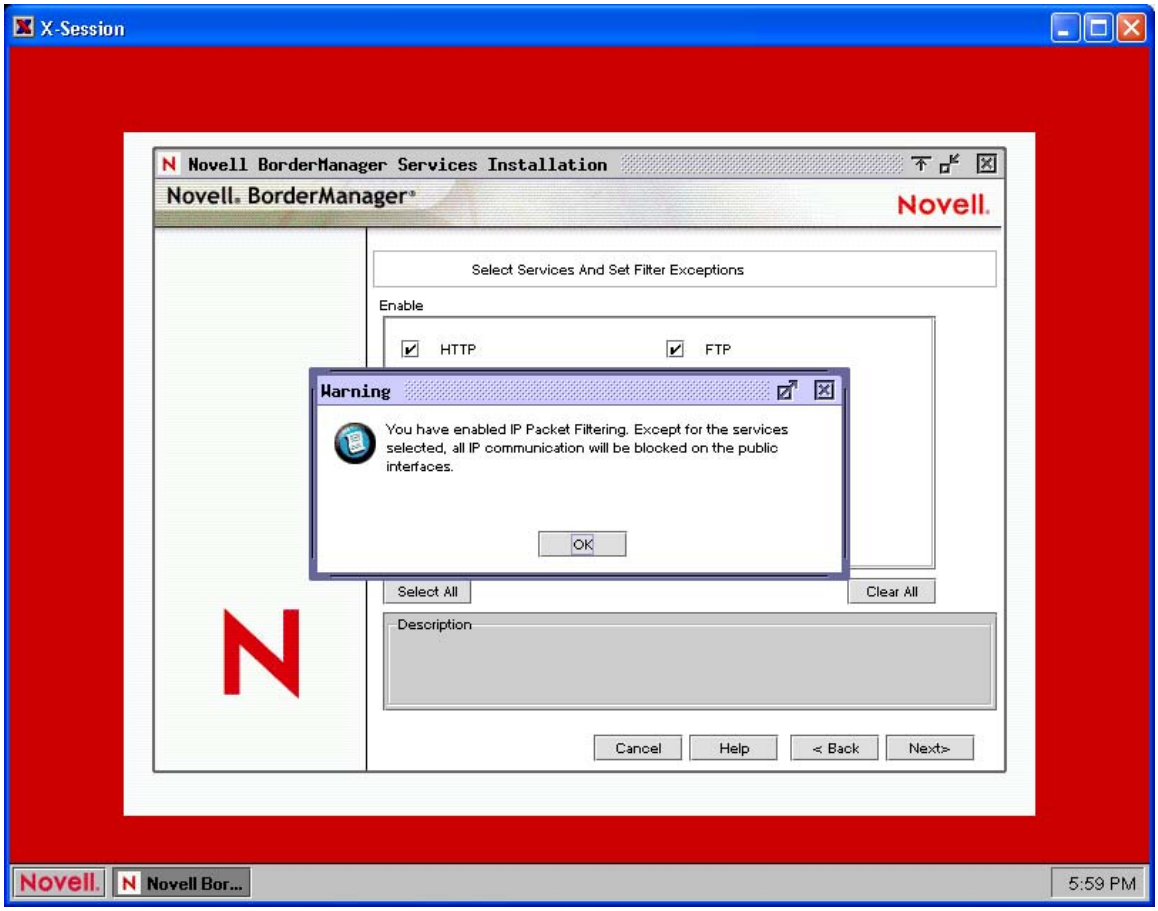
If you enabled HTTP, FTP or Transparent HTTP Proxy, you will get a warning message that you should have a dedicated traditional CACHE volume.

USING DEDICATED LEGACY (TRADITIONAL) CACHE VOLUMES IS ESSENTIAL! It is also very important that the HTTP Proxy not use SYS as a cache volume whether or not the cache volume is NSS or legacy. The HTTP Proxy will not delete old files in cache until its cache volume gets full, at which point you would be having major NDS and suballocation issues on a SYS volume.

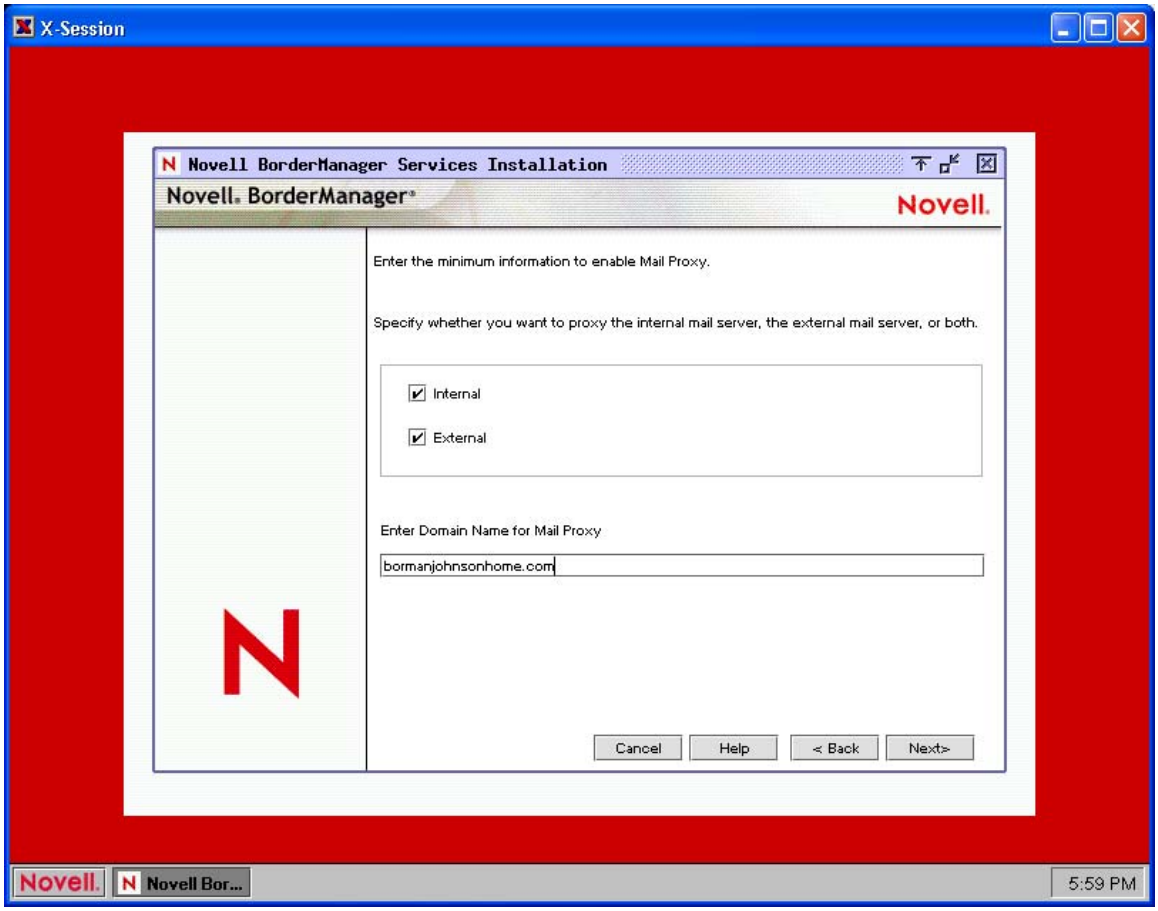
If you do not have the space to create a legacy cache volume because you have only one large NSS partition, I recommend starting over and reinstalling NetWare, or adding another drive.

Note If you are installing on NetWare 6.5, see the following section titled "**NetWare 6.5 – Automatic Cache Volume Selection / Creation**" at this point.

Click **OK**.



You may now see a reminder that IP filtering was selected. Click **OK**.



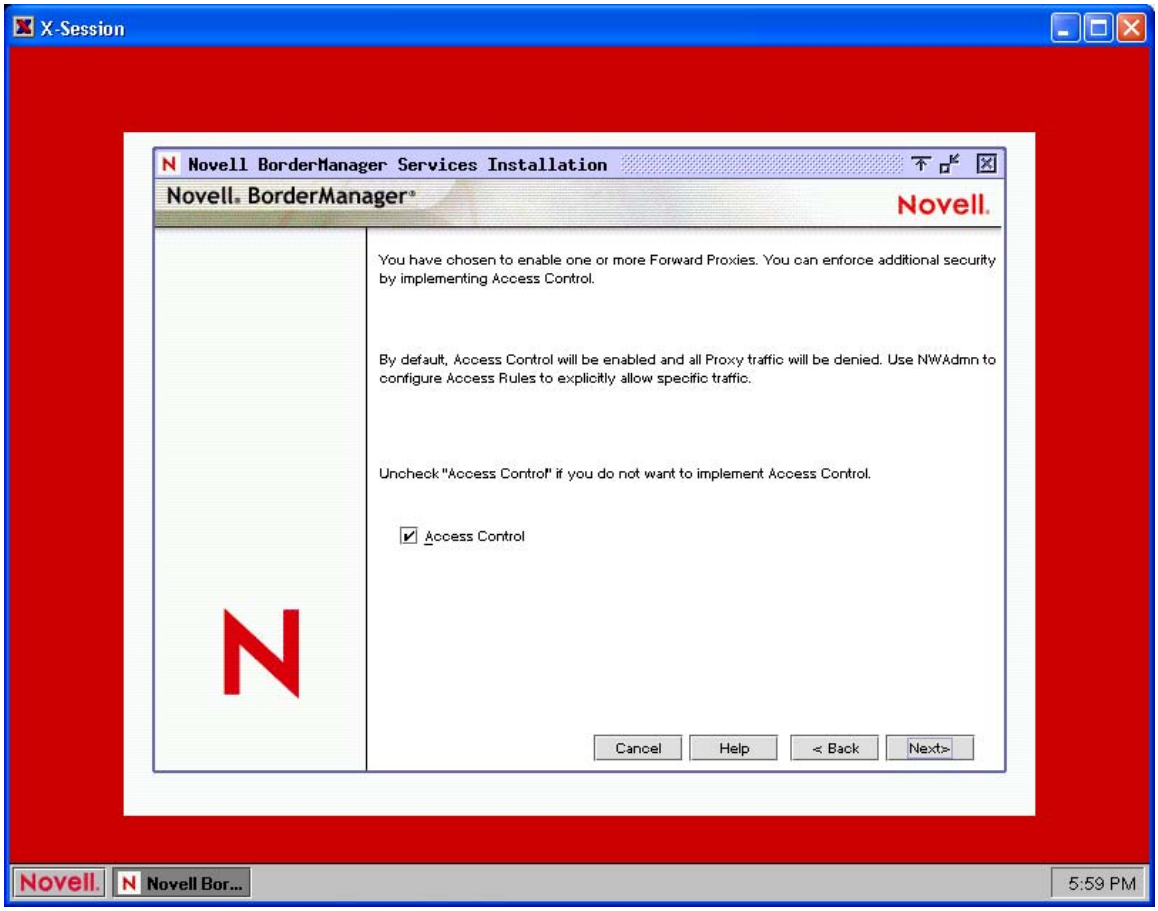
If you selected Mail Proxy, you will be asked to enter a domain name and specify whether you want to proxy mail in the internal or external direction.

Mail Proxy will still require you to make further configuration settings both NWADMN32 and the PROXY.CFG file later in order to function. The main point of this menu entry is to have the BorderManager installation create POP3 and SMTP filter exceptions for inbound or outbound directions.

I recommend selecting both options and entering at least a dummy domain name. You can always change the Mail Proxy configuration later.

Note You also will have to manually configure settings in the SYS:ETC\PROXY\PROXY.CFG file as well.

Click **Next** to continue.

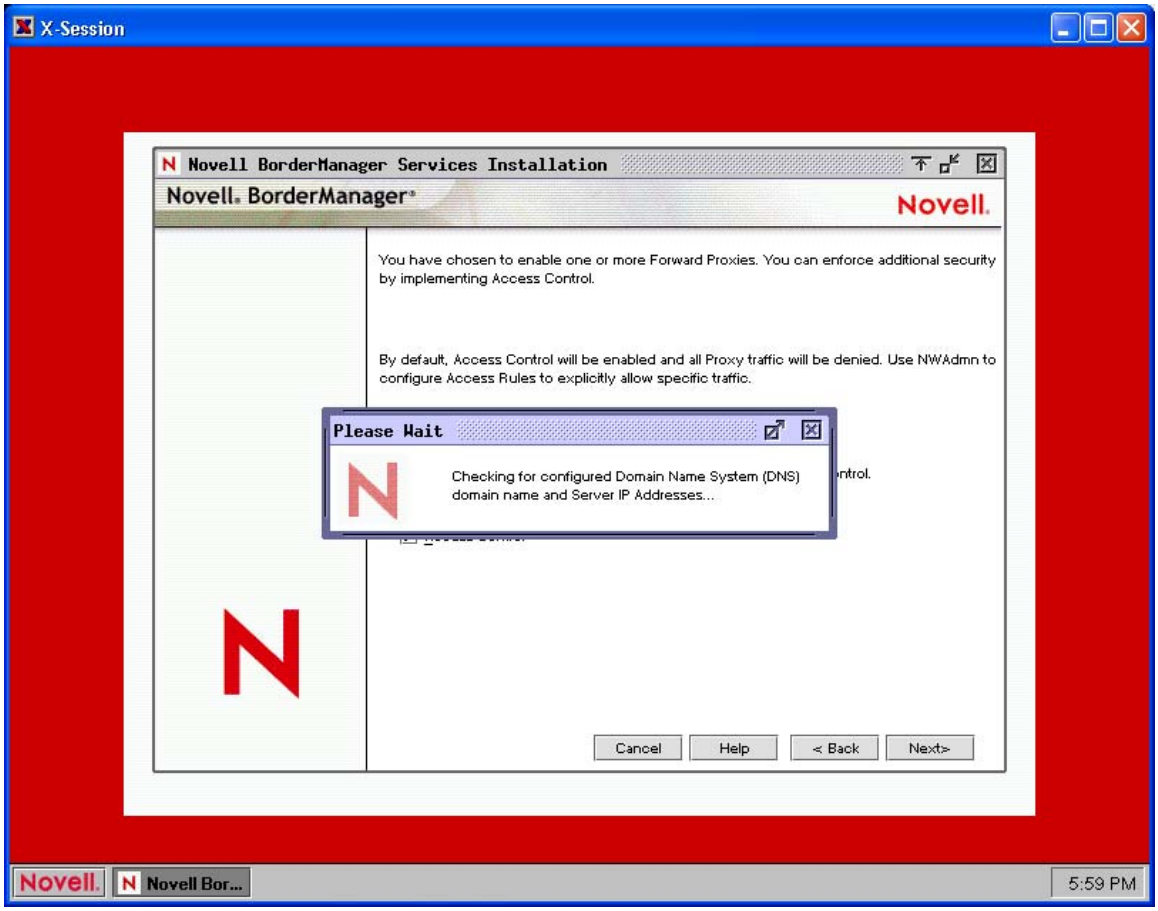


You will now be given the option of enabling or not enabling Access Control. This choice has the effect of enabling or not enabling Access Rule Enforcement in NWADMN32.

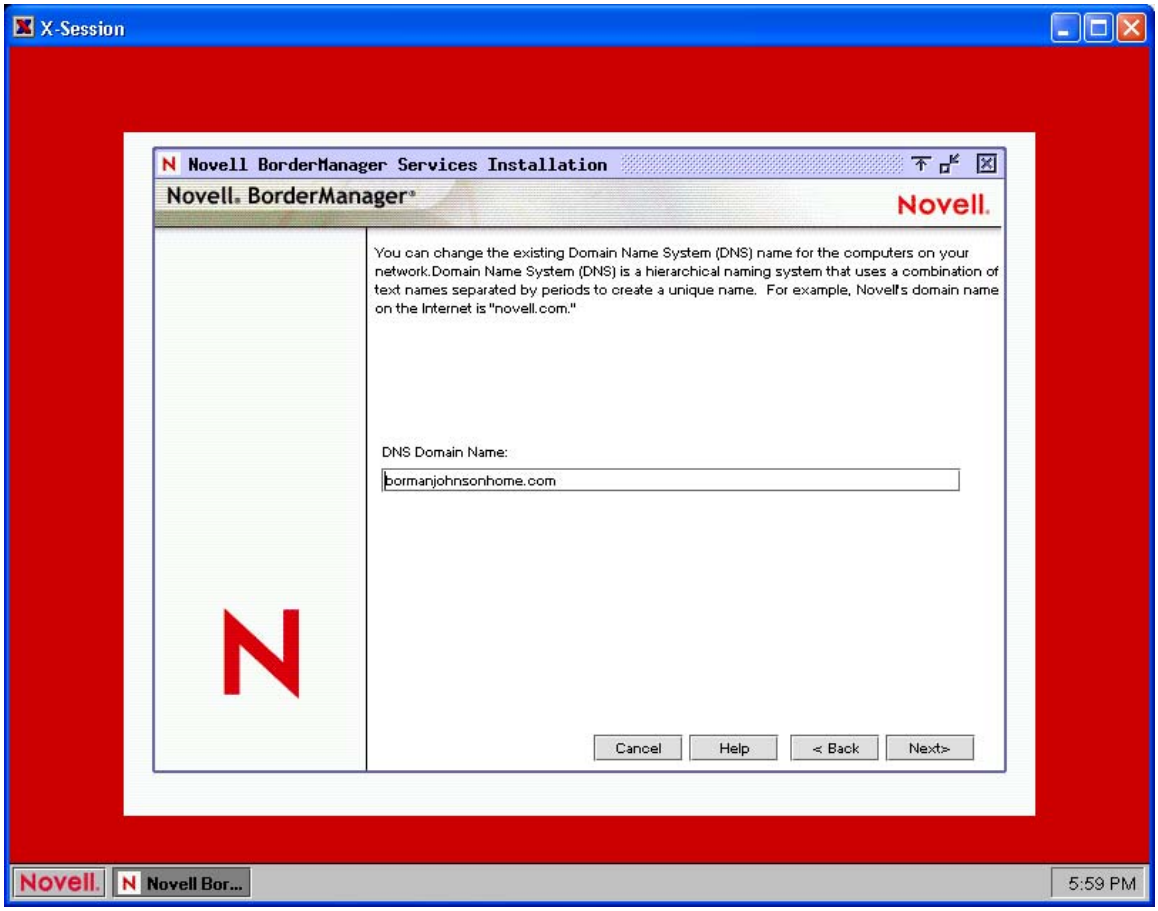
I recommend enabling access control.

You will have to add access rules in NWADMN32 later to allow use of the proxies, but you will, of course, be doing that anyway!

Click **Next** to continue.



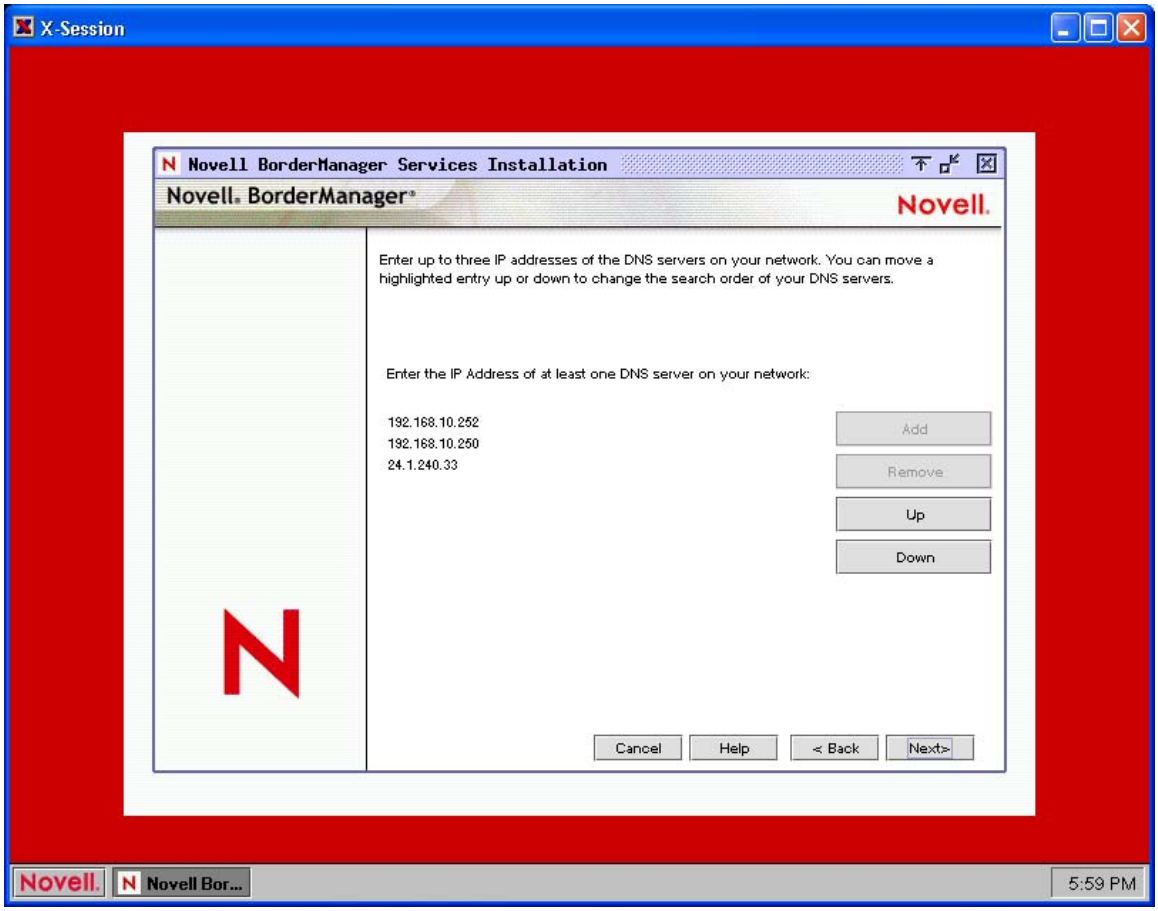
The BorderManager server will now check DNS settings already configured in INETCFG.



Enter your registered domain name when prompted. The installation will pick up a domain name previously configured in INETCFG.

If you have no registered domain name, you can actually enter whatever you like, but it would be a good idea not to choose a name in use by someone on the Internet.

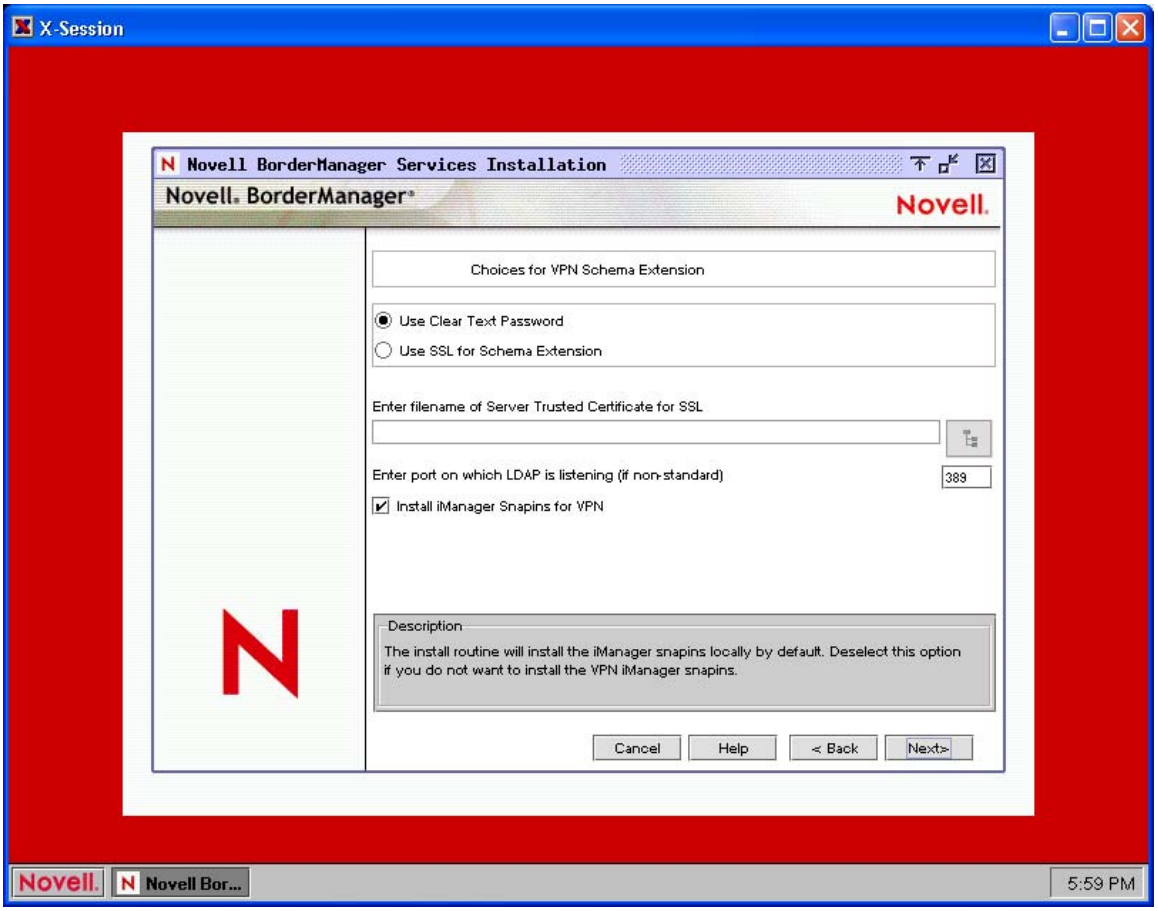
Click **Next** to continue.



The installation will show any configured DNS server IP addresses already entered previously, or allow you to enter new ones.

In the example show, two internal DNS servers were entered for the first two choices, and a DNS server at the ISP was entered as the 'last chance' 3rd choice.

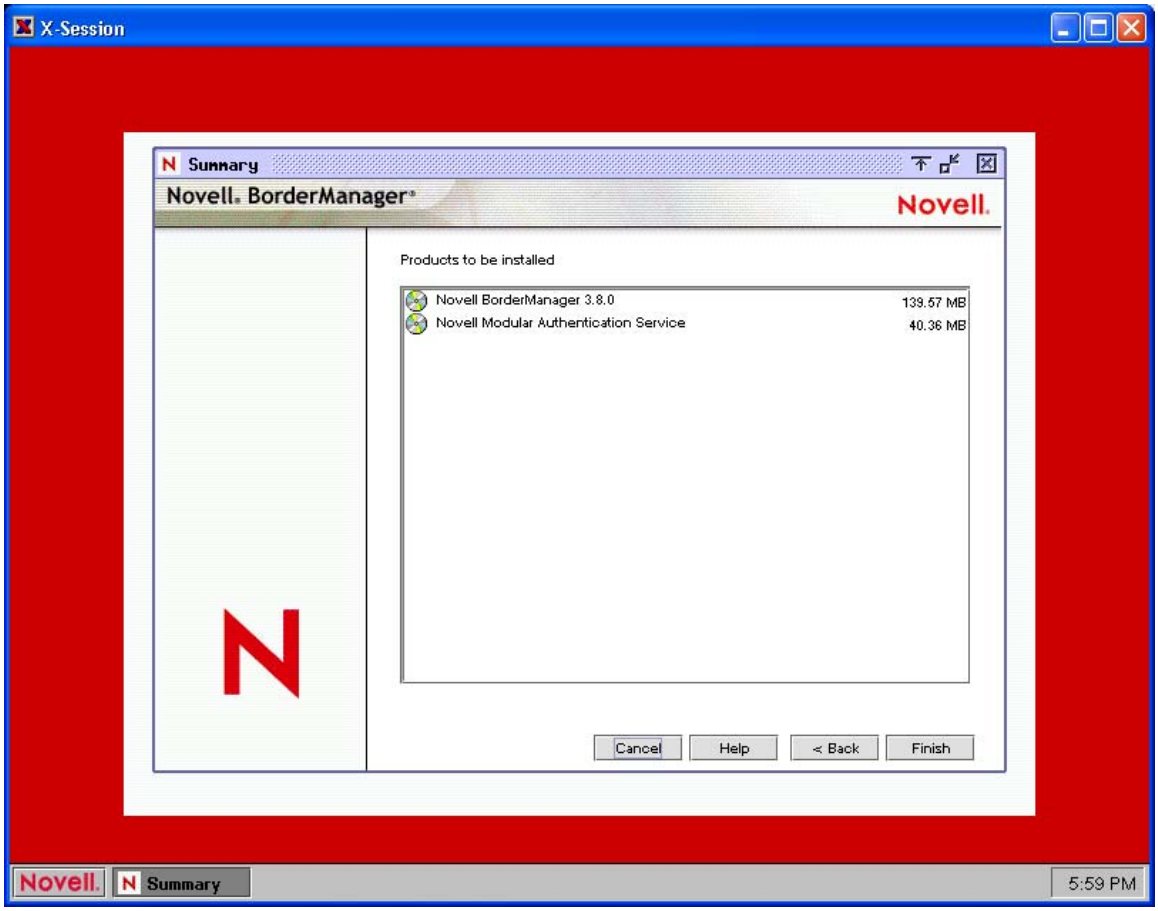
Click **Next** to continue.



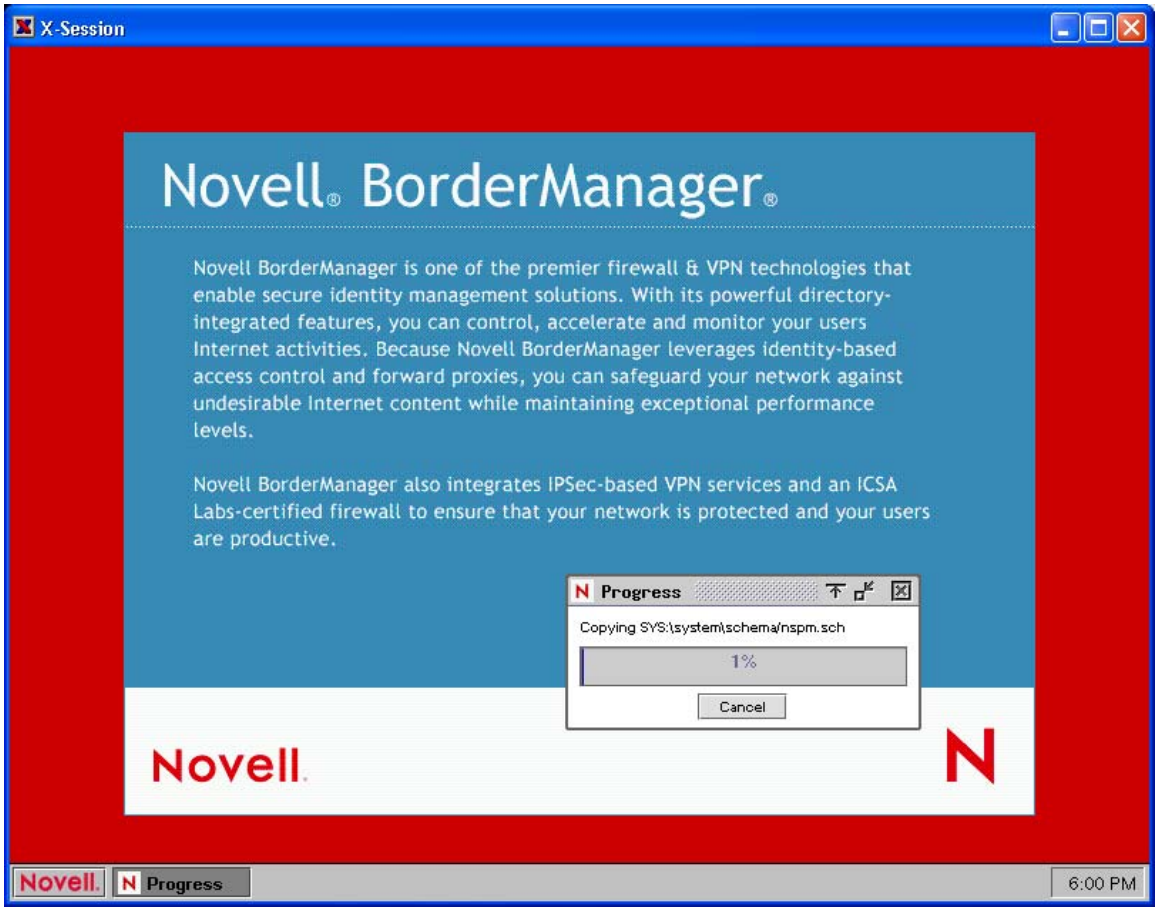
Next, you should have an option for extending the schema for the new BorderManager 3.8 VPN capability, and to add VPN snapins for iManager.

The schema extension installation routine uses LDAP to log in to the NDS tree and apply the changes. If you want to use Clear Text Password, the LDAP Group object for the server must already be set to allow clear text passwords. Otherwise you will have to use SSL, and point to the location of the ROOTCERT.DER file for the NetWare server.

Note The iManager snapin installation primarily applies to NetWare 6.5 with iManager 2.0 installed.



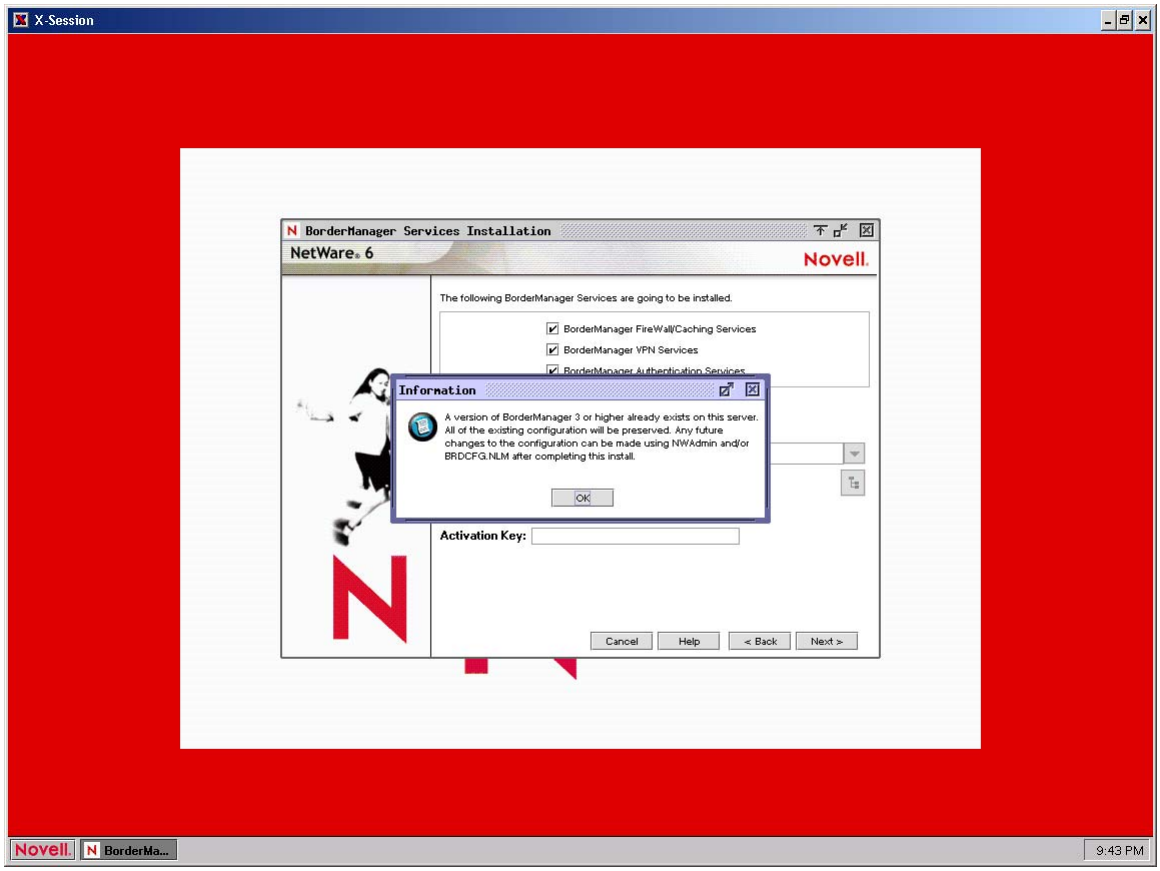
After a short delay while BorderManager gathers configuration data, you should see a summary screen.



Finally, the file copy process should begin, and copy all necessary files to the server.

Following the file copy process, various settings will be configured, and eventually you will be asked to remove any installation CD's and reboot the server.

If You Are Upgrading BorderManager



If you had a previous version of BorderManager 3.x installed on the server, most of the configuration information should be automatically preserved and used with BorderManager 3.8.

Note Existing CyberPatrol rules are not upgraded automatically by a SurfControl installation.

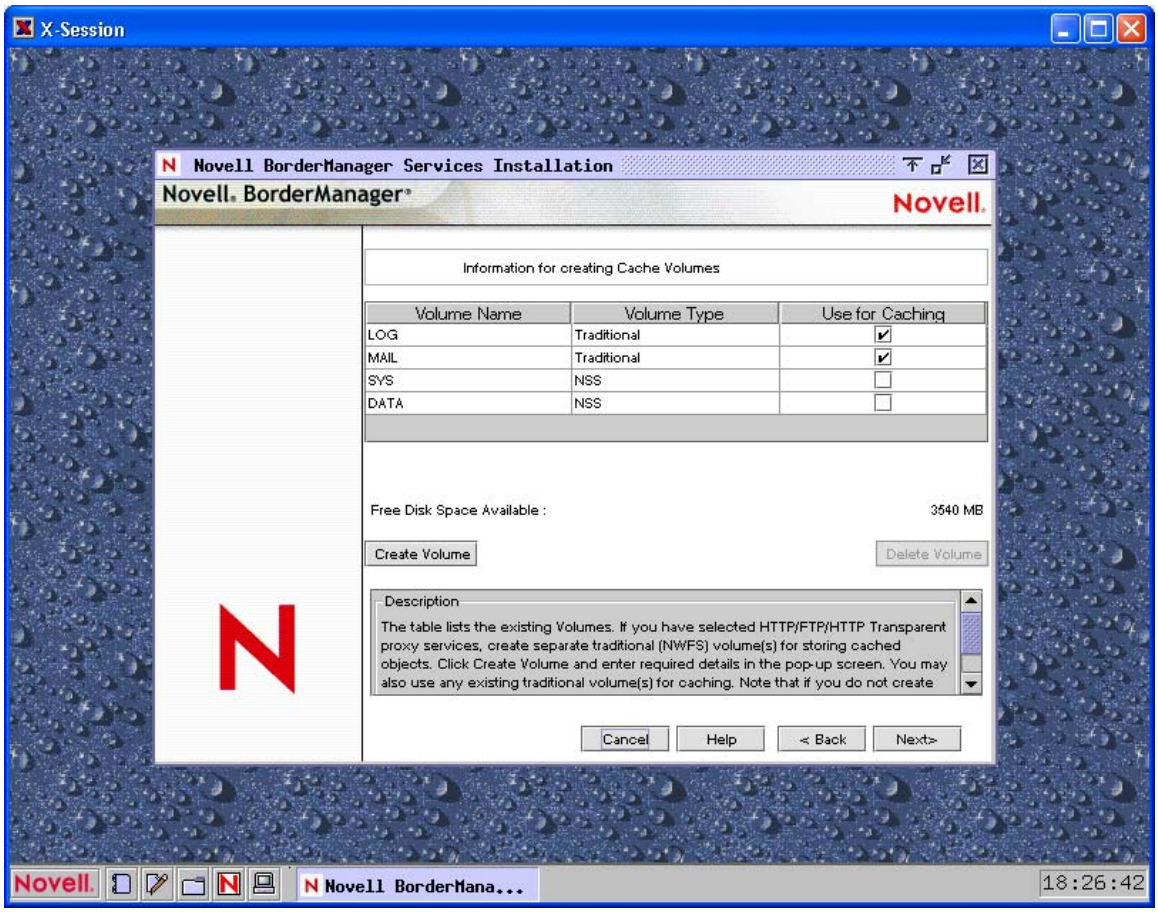
The installation routine skips many of the steps shown previously if an existing BorderManager server installation was found in the Configured Products list in NWCONFIG.NLM.

Click **OK** to continue, if you see this screen.

NetWare 6.5 – Automatic Cache Volume Selection / Creation

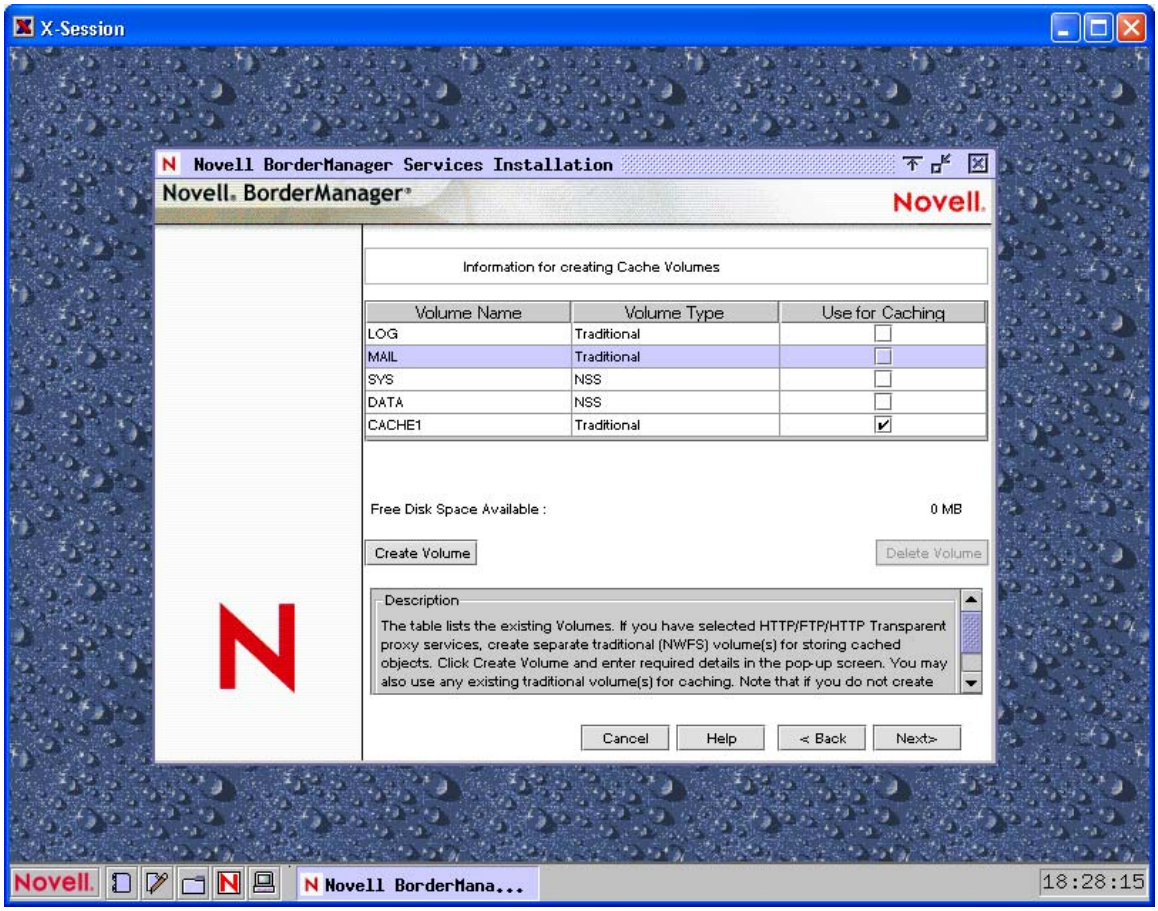
Note This section does **not** apply to NetWare 5.1 or 6.0 servers.

If you are installing BorderManager 3.8 on a NetWare 6.5 server, at the point you select to use the HTTP proxy you may see a dialog directing you to create or designate traditional (non-NSS) cache volumes for use by the HTTP Proxy. Whether or not you see the dialog depends on whether or not you have traditional volumes or unpartitioned free space on the server.



1. If you have any existing traditional volumes on the server, they will automatically be selected for use as caching volumes. In the example shown, I had created traditional volumes for LOG and MAIL before installing BorderManager 3.8. *Notice that the installation routine automatically flagged them for caching, simply because they were traditional volumes and not NSS volumes.*

2. If you have any free, unpartitioned space, you will be given the option to create one or more traditional volumes to be used as cache volumes. (Notice the Create Volume button). The installation routine will automatically create traditional volumes with no suballocation, no compression and 8K block size. (Long name space will be added, but you can remove long name space later with VREPAIR). If you allow the installation routine to create volumes for you, you must designate the size, and provide a 'seed name' for the volumes. Numbers will automatically be added to the volume name, for the possibility that you may want to create more than one cache volume. If you enter a volume name of CACHE, you will end up with a volume called CACHE1. (If you enter a name of CACHE1, you will end up with a volume called CACHE11). If you create two volumes



with a name of CACHE, you will end up with volumes CACHE1 and CACHE2.

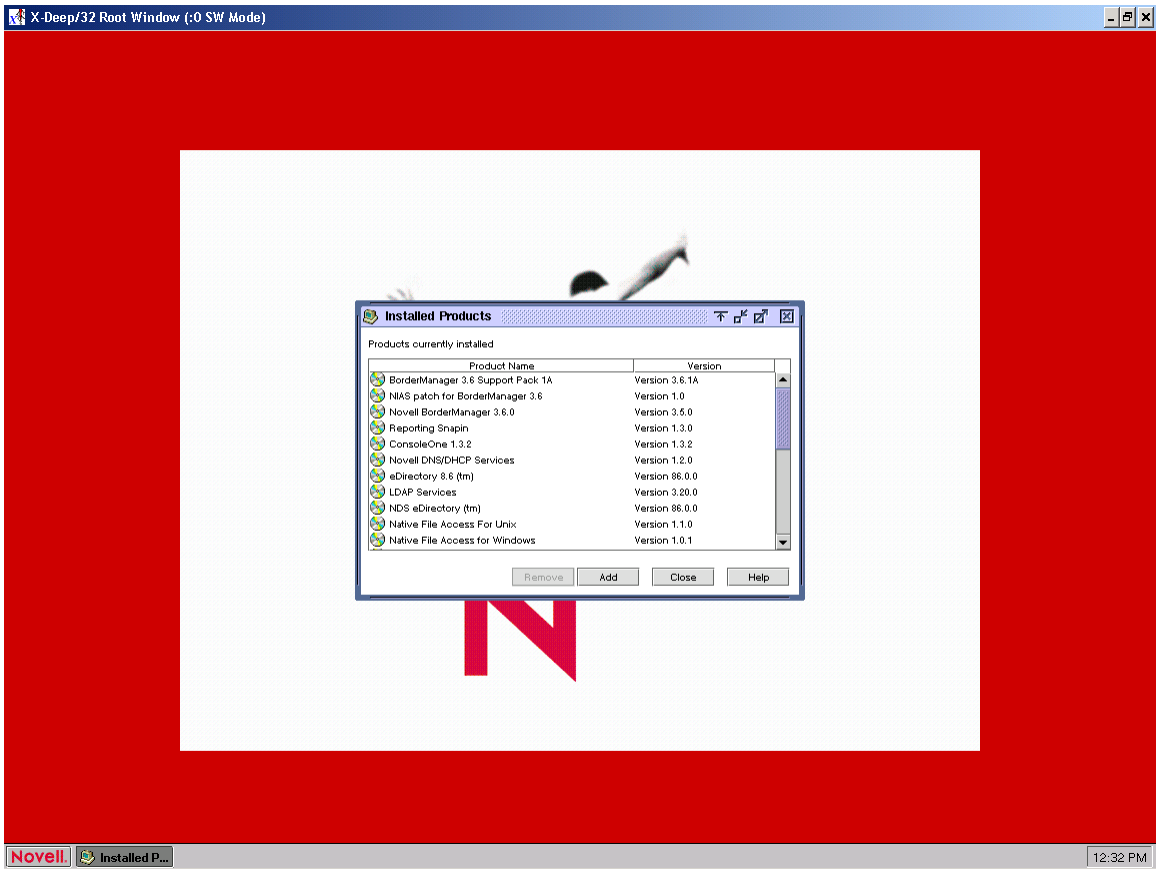
If you created traditional volumes for CACHE before the installation, they will automatically be selected here. However, if you also have other traditional volumes created that are not supposed to be used for caching, you should uncheck those selections before continuing.

The volume selections made here can be modified after the installation using NWADMN32, BorderManager Setup, HTTP Proxy Caching, Cache Location.

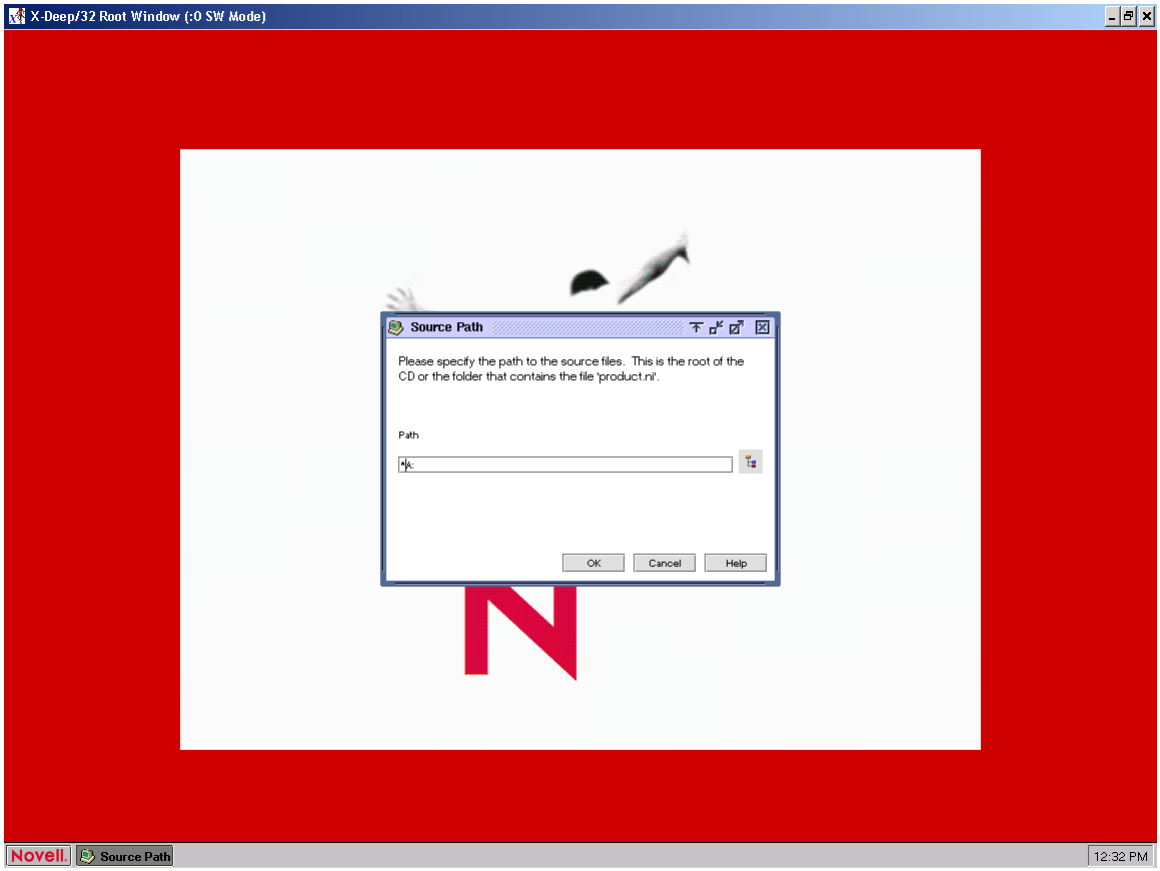
Create, select and/or deselect cache volumes as needed, and click **Next** to continue.

Example Installation of BorderManager 3.7 on NetWare 6.0

The following section shows how I installed BorderManager 3.7 on a NetWare 6.0, server, after first patching it with NW6SP1.EXE.

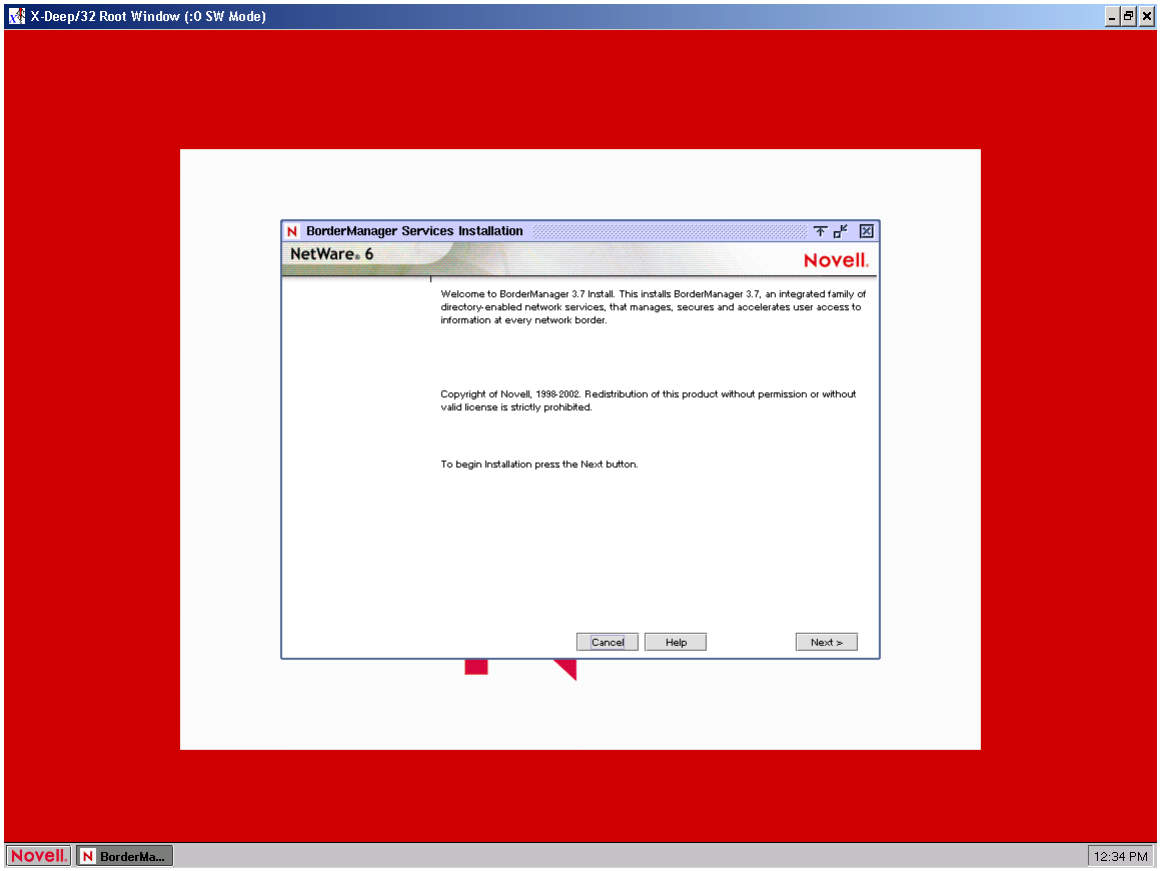


Run STARTX, and launch the Install dialog from the pop up menu in the lower left.

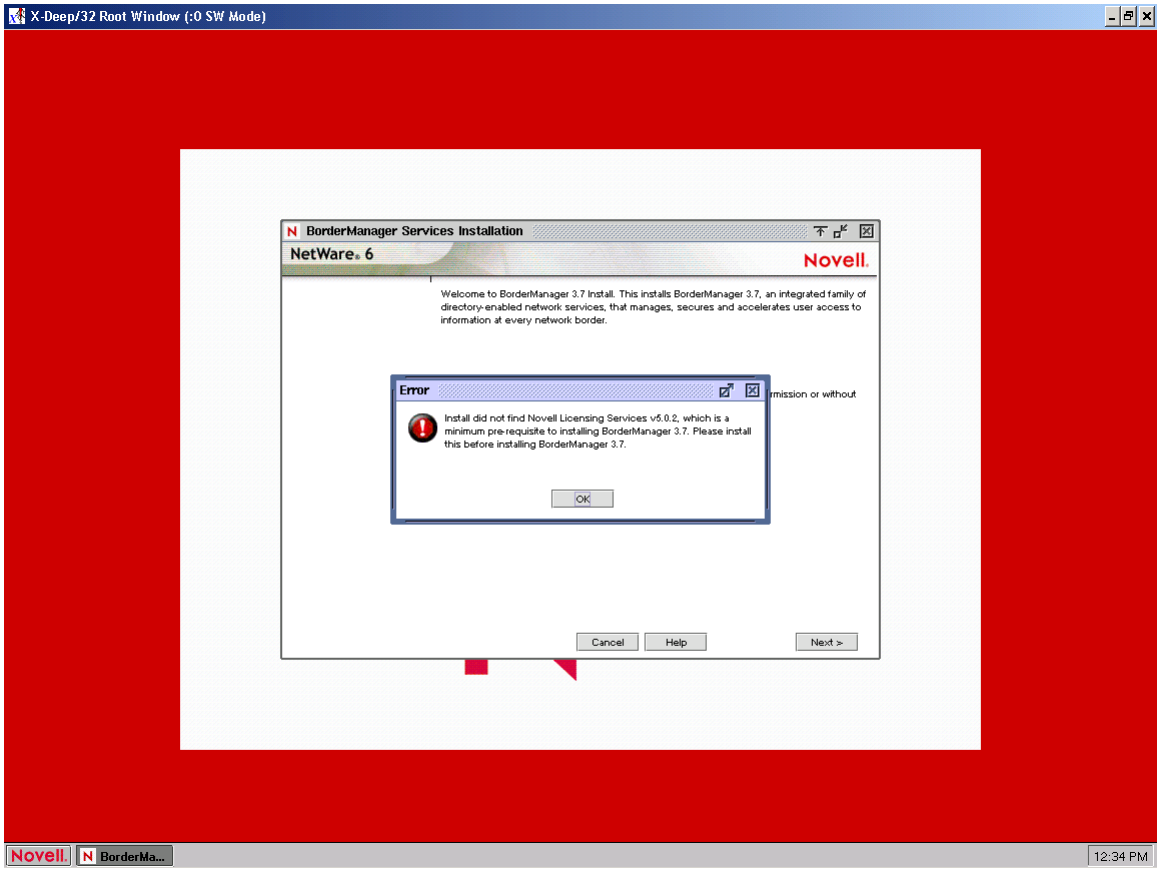


Browse to the location of the PRODUCT.NI file on the BorderManager CD, and click on **OK**

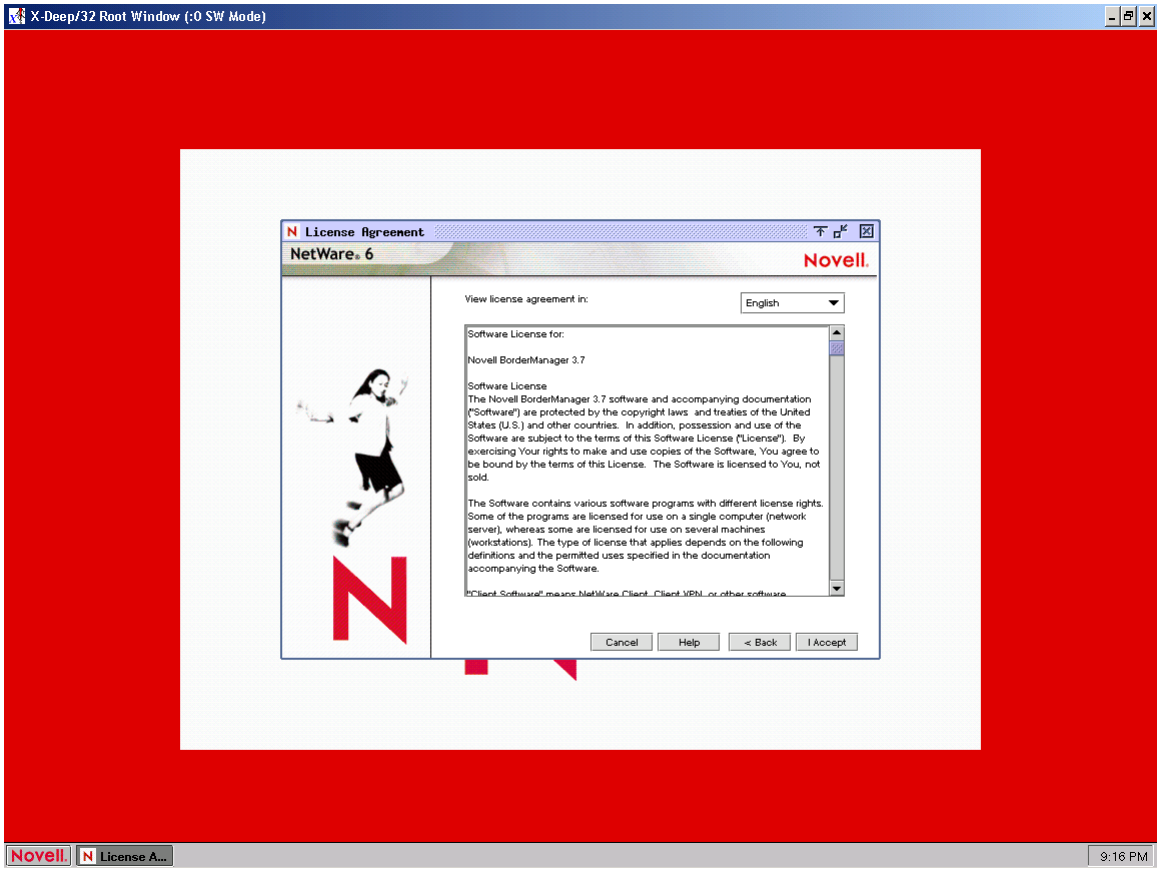
File copying should start.



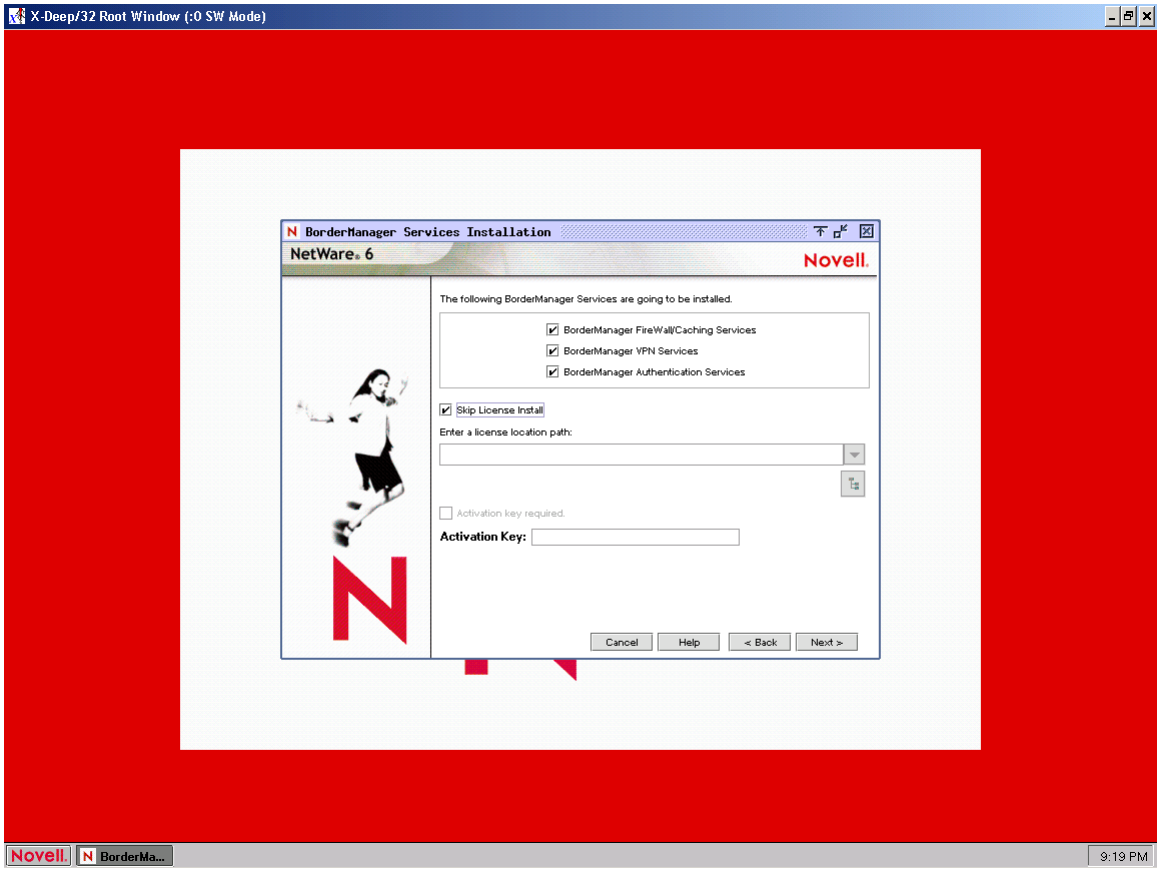
You should get to a screen that tells you that BorderManager 3.7 is about to be installed.



If you should get an error message indicating that you need to have NLS version 5.0.2 installed before you can continue, it is an indication that you need to install the NW6SP1.EXE patch on NetWare 6.0.



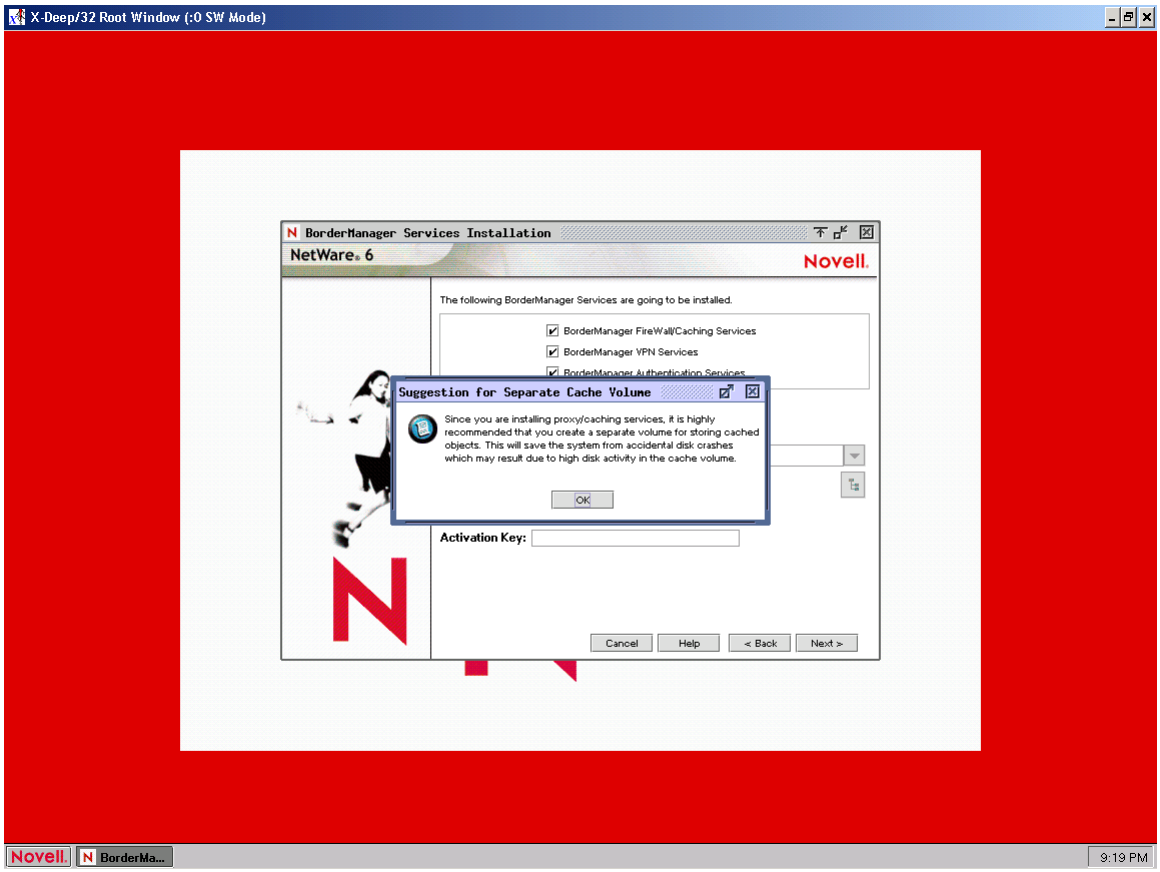
If the proper patches have been installed on NetWare before you begin installing BorderManager, you should reach the License Agreement screen. Click on '**I Accept'** to continue.



Depending on your needs, you can install some or all of the BorderManager 3.7 components. Essentially, all component files will be installed, and the check boxes simply indicate which LICENSES will be installed for you. I recommend installing all features, even if you do not use them at first.

You can point to a file location holding the licenses now, or add the licenses later. In the example above, I skipped the license install at this point, and added them later using iManager.

Click **Next** to continue.

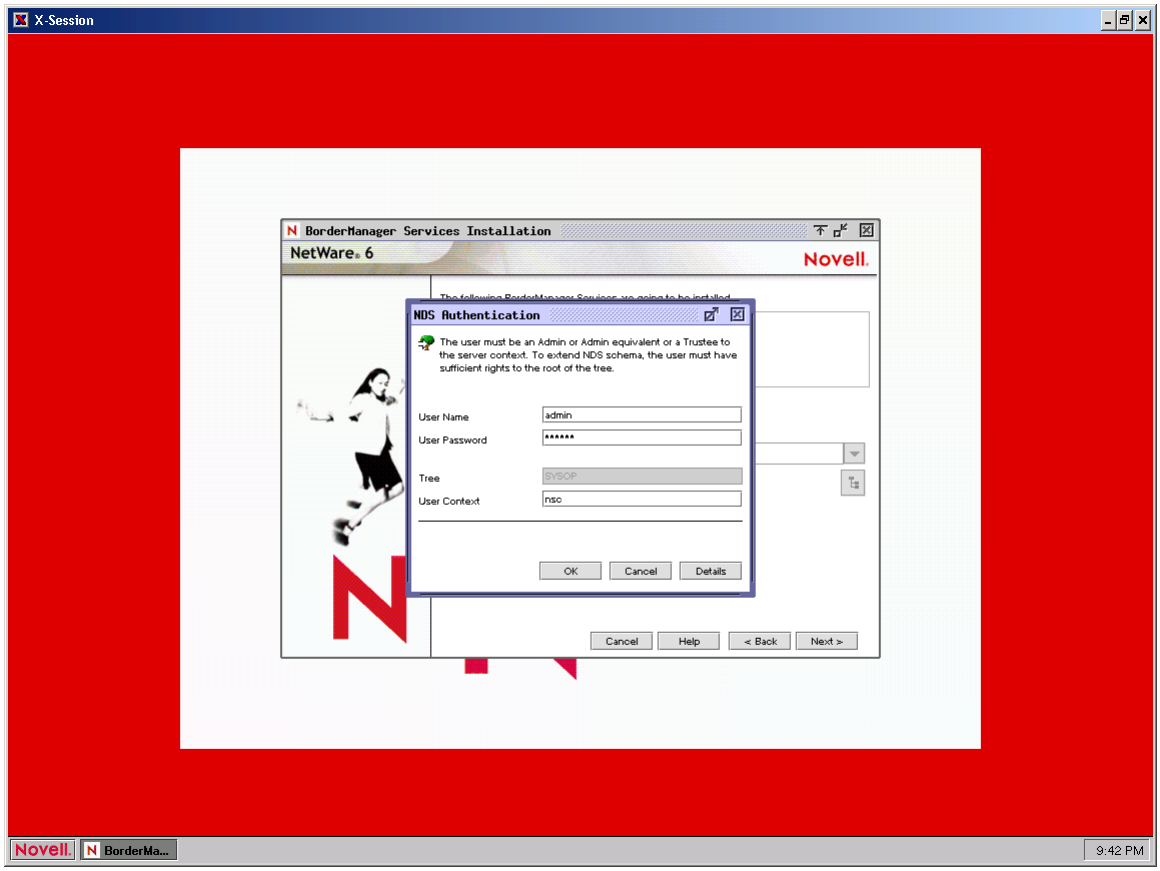


If you enabled HTTP, FTP or Transparent HTTP Proxy, you will get a warning message that you should have a dedicated traditional CACHE volume.

USING DEDICATED LEGACY (TRADITIONAL) CACHE VOLUMES IS ESSENTIAL! It is also very important that the HTTP Proxy not use SYS as a cache volume whether or not the cache volume is NSS or legacy. The HTTP Proxy will not delete old files in cache until its cache volume gets full, at which point you would be having major NDS and suballocation issues on a SYS volume.

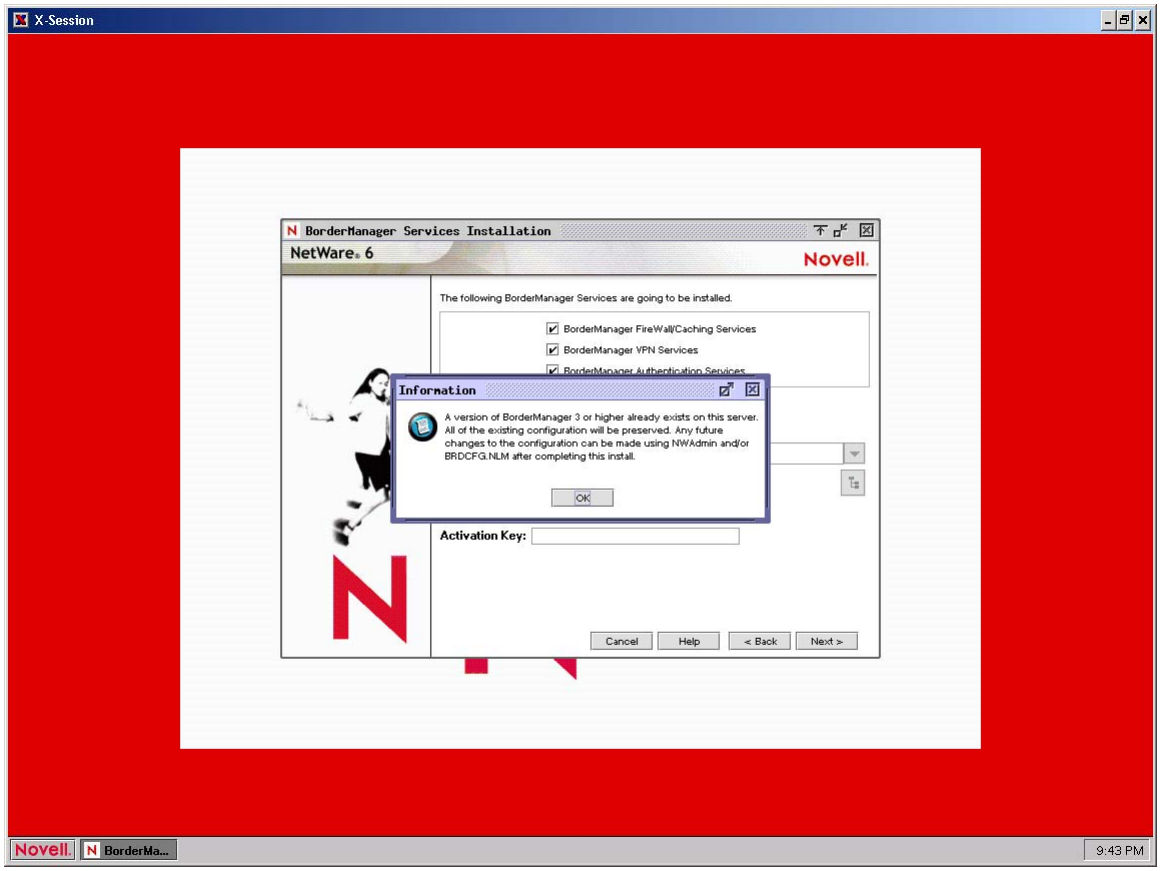
If you do not have the space to create a legacy cache volume because you have only one large NSS partition, I recommend starting over and reinstalling NetWare, or adding another drive.

Click **OK** to continue, then click **Next**.



You will need to be Admin-equivalent if this is the first BorderManager 3.7 server in the tree in order to extend the schema attributes. Unlike previous versions, BorderManager 3.7 stores IP filtering information in NDS.

If You Are Upgrading BorderManager

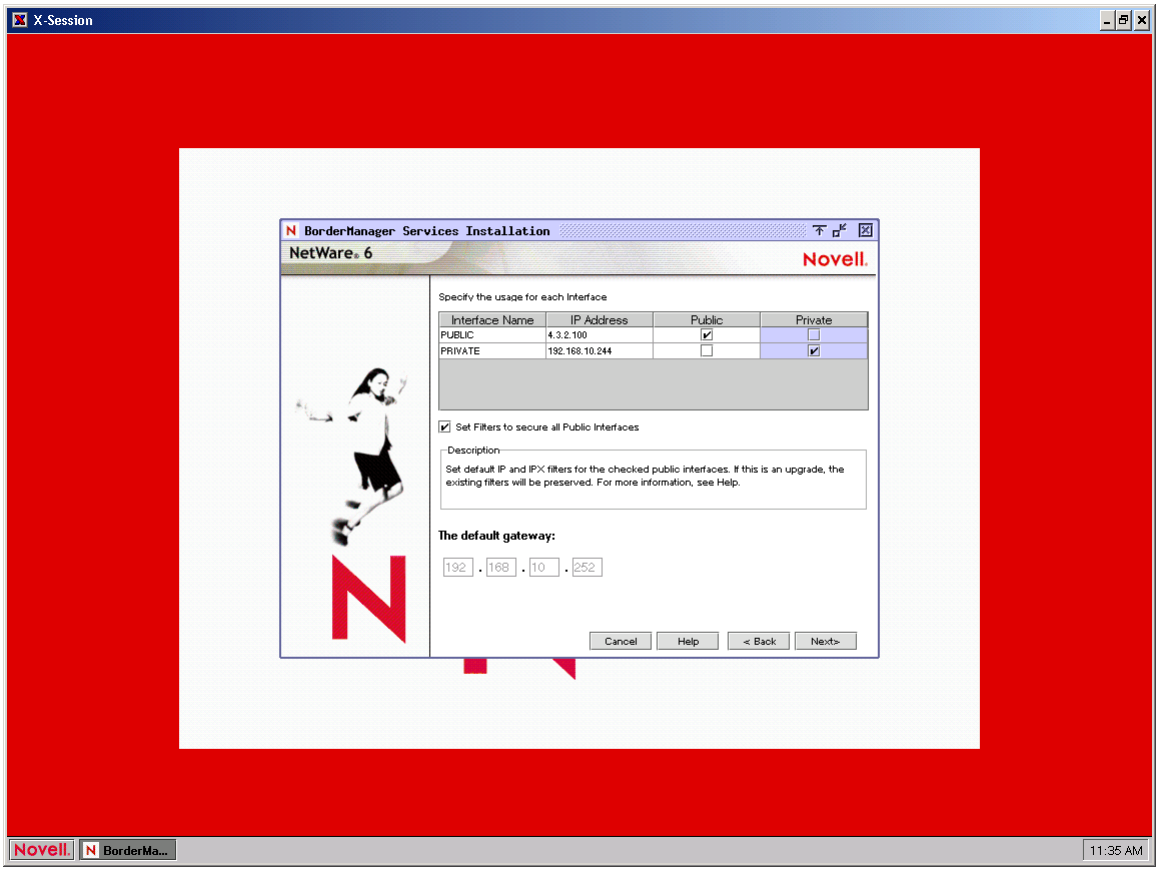


If you have a previous version of BorderManager 3.x installed on the server, the configuration information should be automatically preserved and used with BorderManager 3.7.

Note Existing CyberPatrol rules are not upgraded automatically by a SurfControl installation.

Skip ahead to Installation, Continued, a few pages later in this book.

Fresh Install of BorderManager 3.7



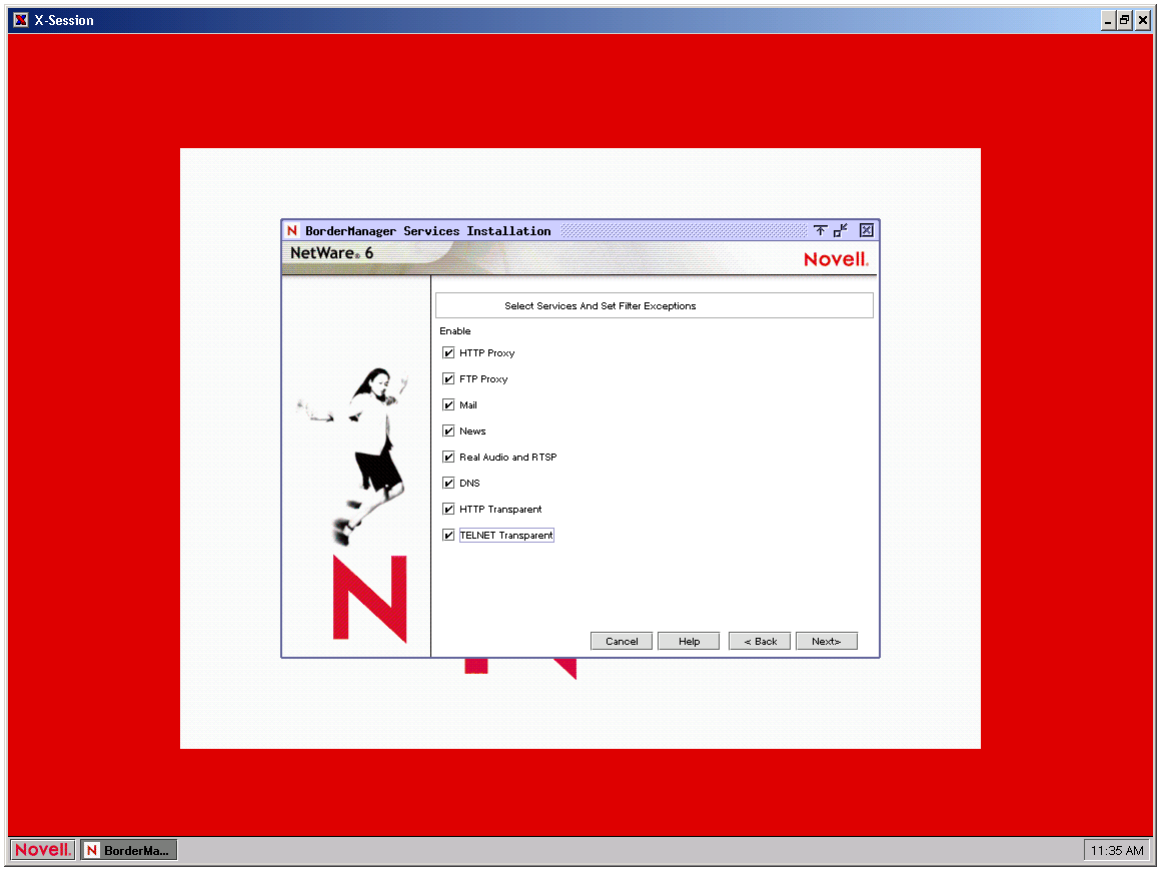
If you have never installed BorderManager on this server before, you will have additional configuration screens not seen on an in-place upgrade installation.

Select the public and private interfaces and define them appropriately. I made sure my interfaces were named PUBLIC and PRIVATE **before** I started the BorderManager installation.

Select the option to set the filters on the public interface.

Note The default gateway shown in the screenshot above was configured using INETCFG.NLM prior to installing BorderManager.

Click **Next** to continue. I told BorderManager to set the filters on the public interface.



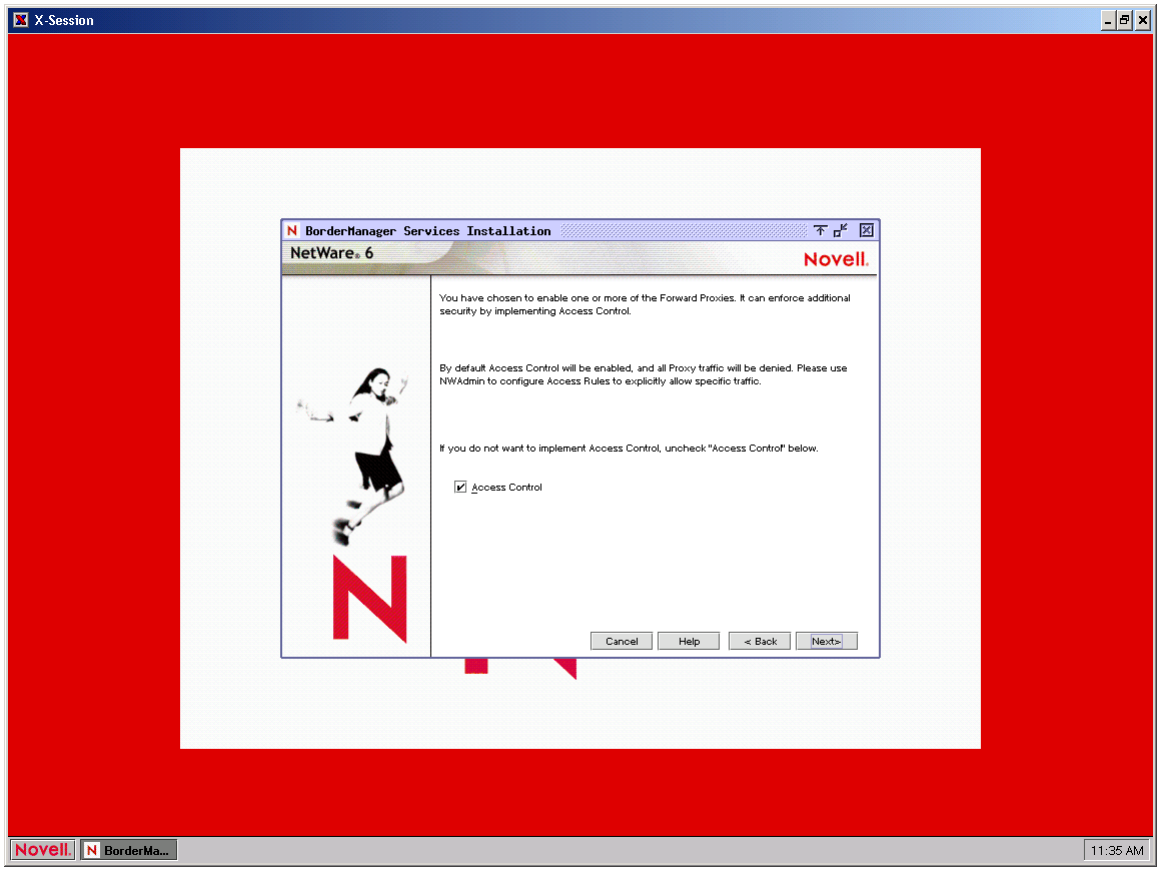
Select the proxy services you wish to use at this point. (You can also select them later in NWADMN32).

The installation routine will:

- configure stateful filter exceptions for each type of proxy selected so that you will not have to do that manually later, and
- enable most of the selected proxies.

Not all of the proxies will show up in NWADMN32 as being enabled. Specifically, the Mail Proxy and News Proxy will not be enabled, because there is additional configuration that must be done for each in NWADMN32. However, filter exceptions will already be enabled to allow those proxies to work in the outbound direction.

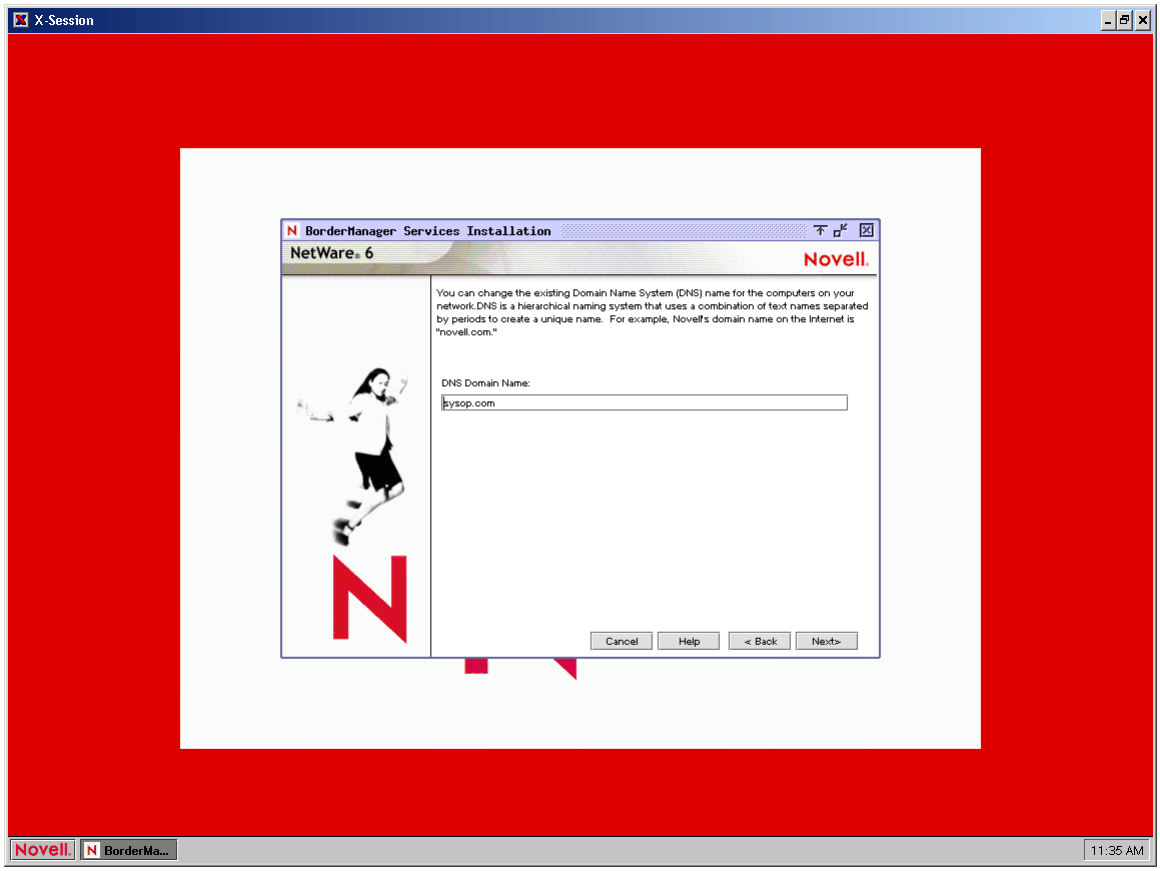
CAUTION *Prior to the BM37SP2.EXE patch, the stateful filter exceptions put in place by a fresh install of BorderManager did not include sufficient exceptions for the VPN to function. BM37SP2.EXE includes a newer version of BRDCFG that addresses the issue. BRDCFG in an unpatched BorderManager 3.7 installation also includes sufficient exceptions, but they are completely different than a fresh installation OR from BM37SP2. This situation is covered in depth in my BorderManager filtering book.*



You may now choose to enforce access controls. This option determines whether or not access rules start out being enforced.

If you choose this option, all outbound traffic through the proxies will be denied, because no Allow access rules will be set up at first. You need to add the appropriate access rules in NWADMN32 to allow particular proxies. (Refer to the chapter on Access Rules later in this book).

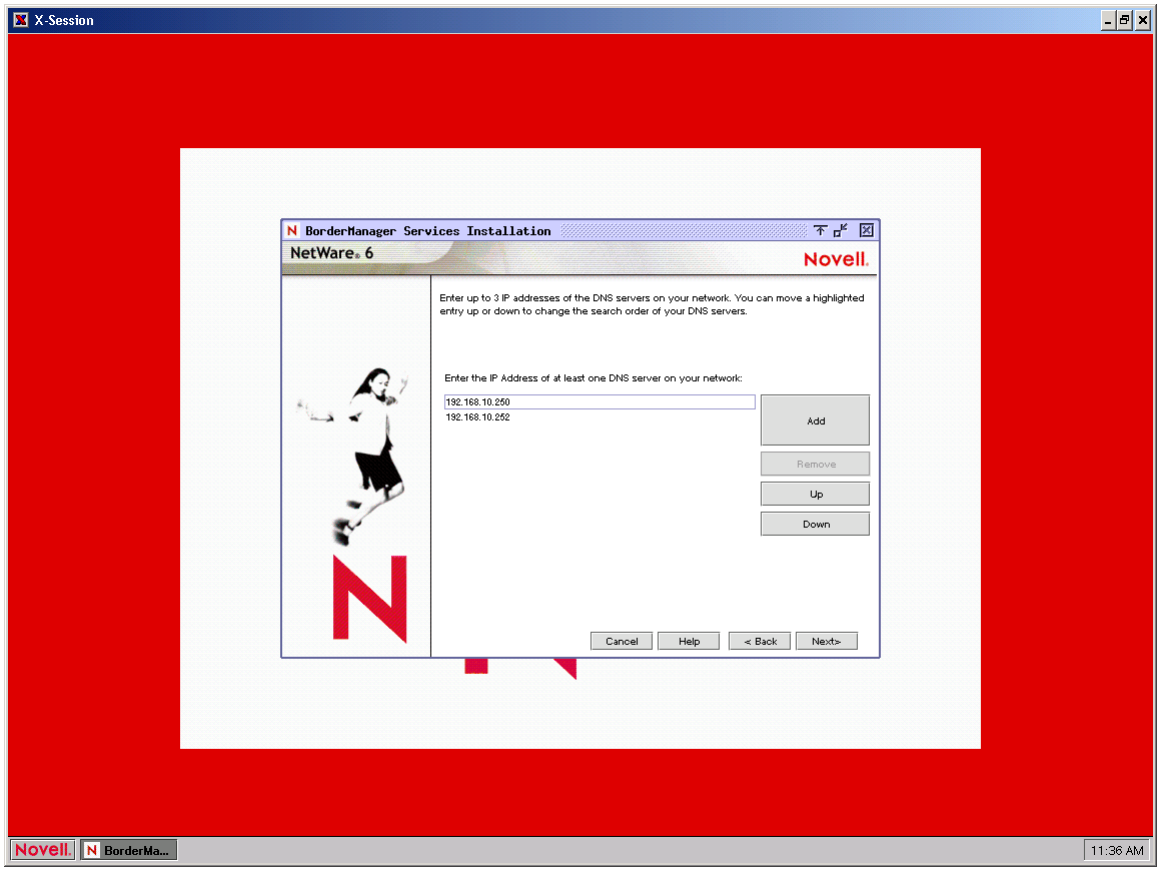
Click **Next** to continue.



Next, you should configure your DNS domain name.

If you do not have a registered domain name, you can make one up, but you should not use one that is already in use on the Internet, or you could get some unexpected results.

Click **Next** to continue.



Enter the IP addresses of any internal or external DNS servers for your network.

If you have an internal DNS server, I recommend configuring it as the first DNS entry in the list.

Be sure to allow any internal DNS servers to bypass the BorderManager server proxy with a stateful filter exception and dynamic NAT. (Do not point an internal DNS server to a BorderManager DNS proxy, and then point BorderManager back to the internal DNS server!)

After any internal DNS servers are added, put in the addresses of your ISP's DNS servers.

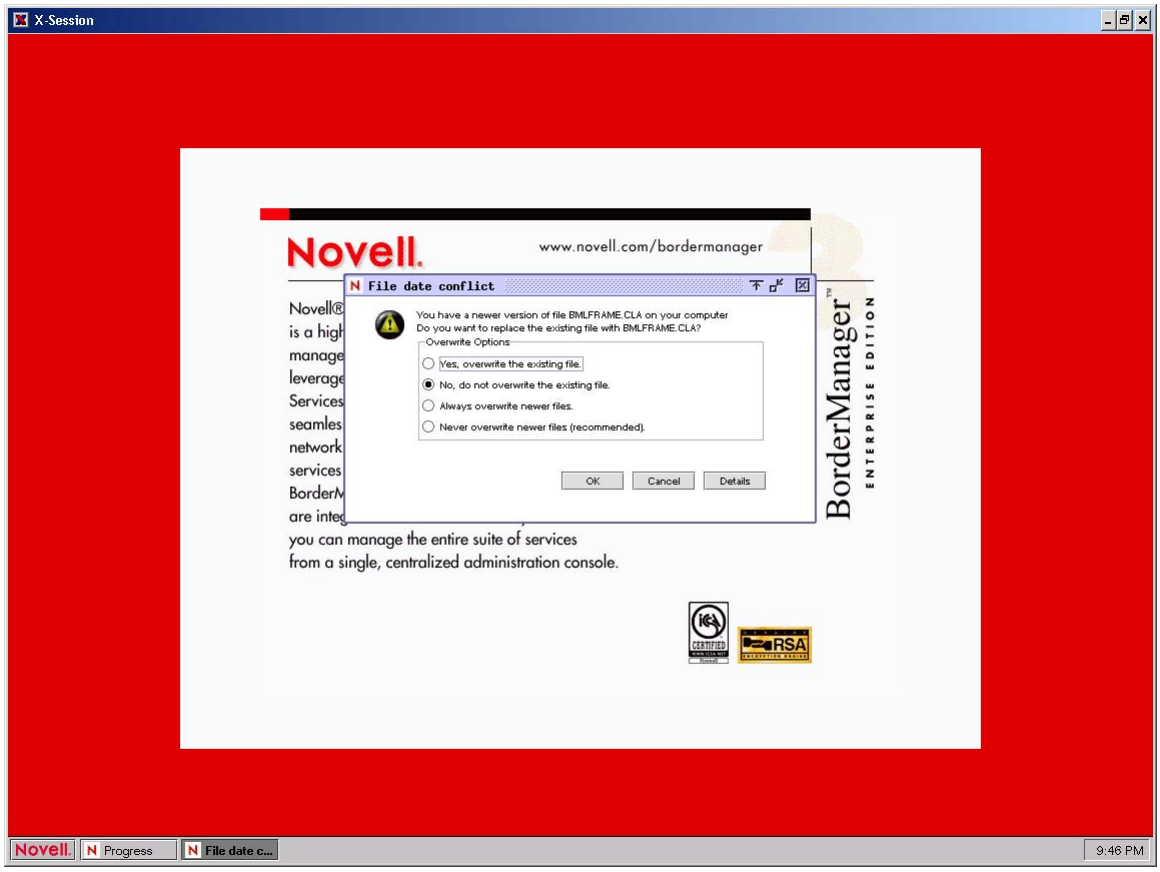
Click **Next** to continue.

Installation, Continued (Fresh Install or Upgrade Situation)

The installation routine for either an upgrade or a fresh installation of BorderManager should be the same from this point forward.

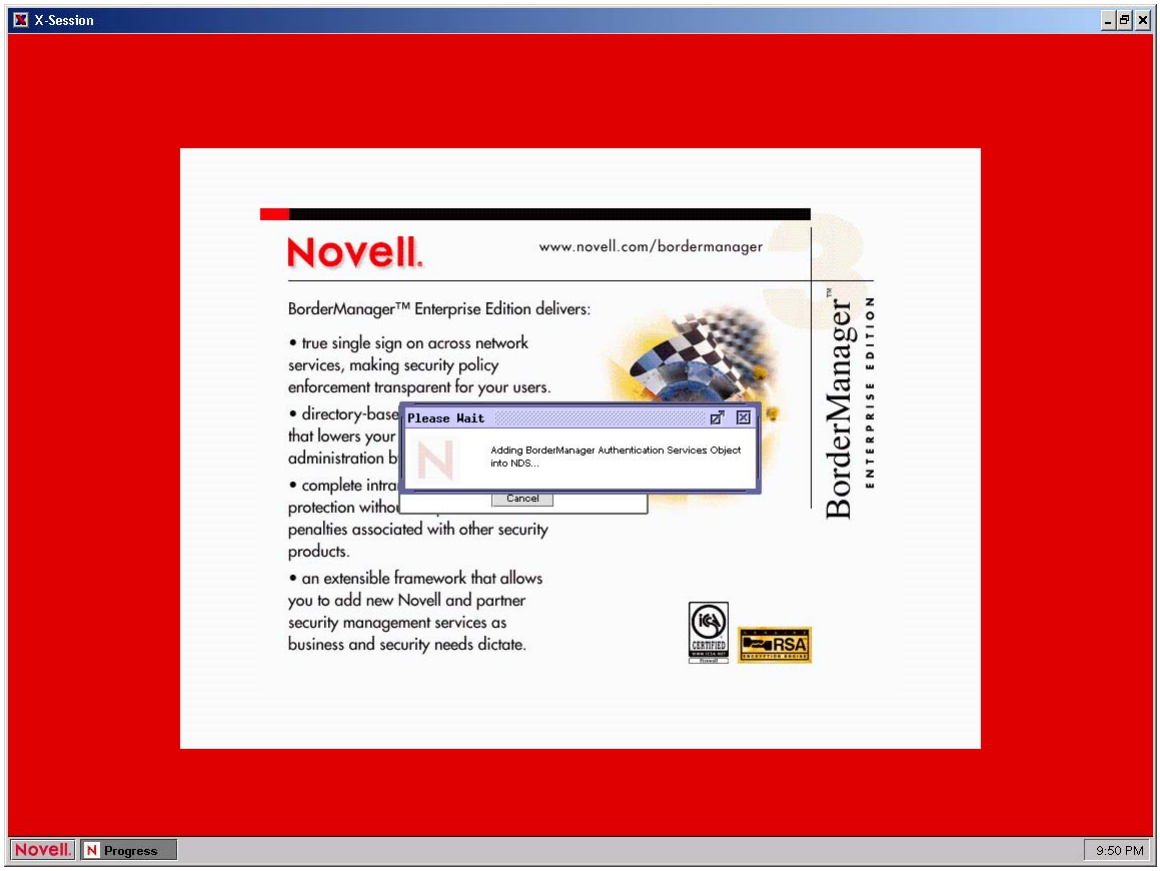
After this point, you will see a few more installation windows, including one that shows files being copied.

You will also see a screen telling you that the NDS schema is being extended. It is critical that all servers in the root and local BorderManager server replica rings are up and synchronizing.



If you see a warning about overwriting newer files, I recommend that you do NOT overwrite them.

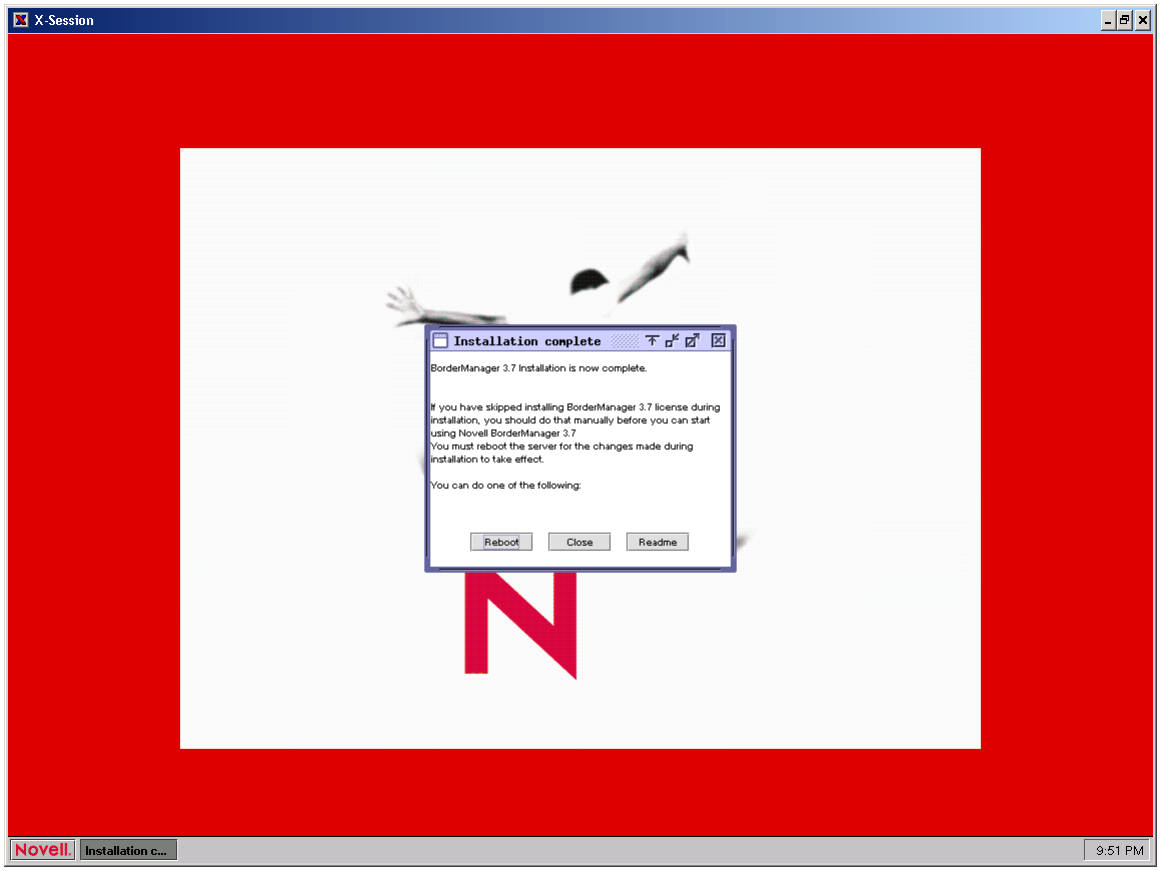
Click **OK** to continue as needed.



You will see a screen telling you that a BorderManager Authentication Services object is being added to NDS. This object has to do with storing IP filter information in NDS.

Afterwards, you will see a screen telling you that the AUTOEXEC.NCF file is being updated. The AUTOEXEC.NCF file will have a STARTBRD line added to launch BorderManager services.

The STARTBRD.NCF file may contain a LOAD RADIUS line. If you do not wish to run RADIUS, manually edit the BRDSTART.NCF file and comment or remove the RADIUS load command.



Finally, you will reach the end of the installation process, and see a screen telling you to reboot the server. Reboot at this time.

Post-Installation Procedures for BorderManager 3.7 or 3.8

Installing BorderManager 3.7 or 3.8 Licenses with iManager

If you installed BorderManager 3.7 or 3.8 without licenses, you will need to use iManager or NWADMN32 to install the licenses.

Note You must have at least one NetWare 6.x server in your NDS tree in order to use iManager, unless you install iManager 2.0 on Windows. IManager 2.0 is provided on the BorderManager 3.8 Companion CD. See the chapter on iManager later in this book.

---

iManager 1.x example:

Open Internet Explorer or Netscape, and use the following URL:

HTTPS://<server IP address>:2200

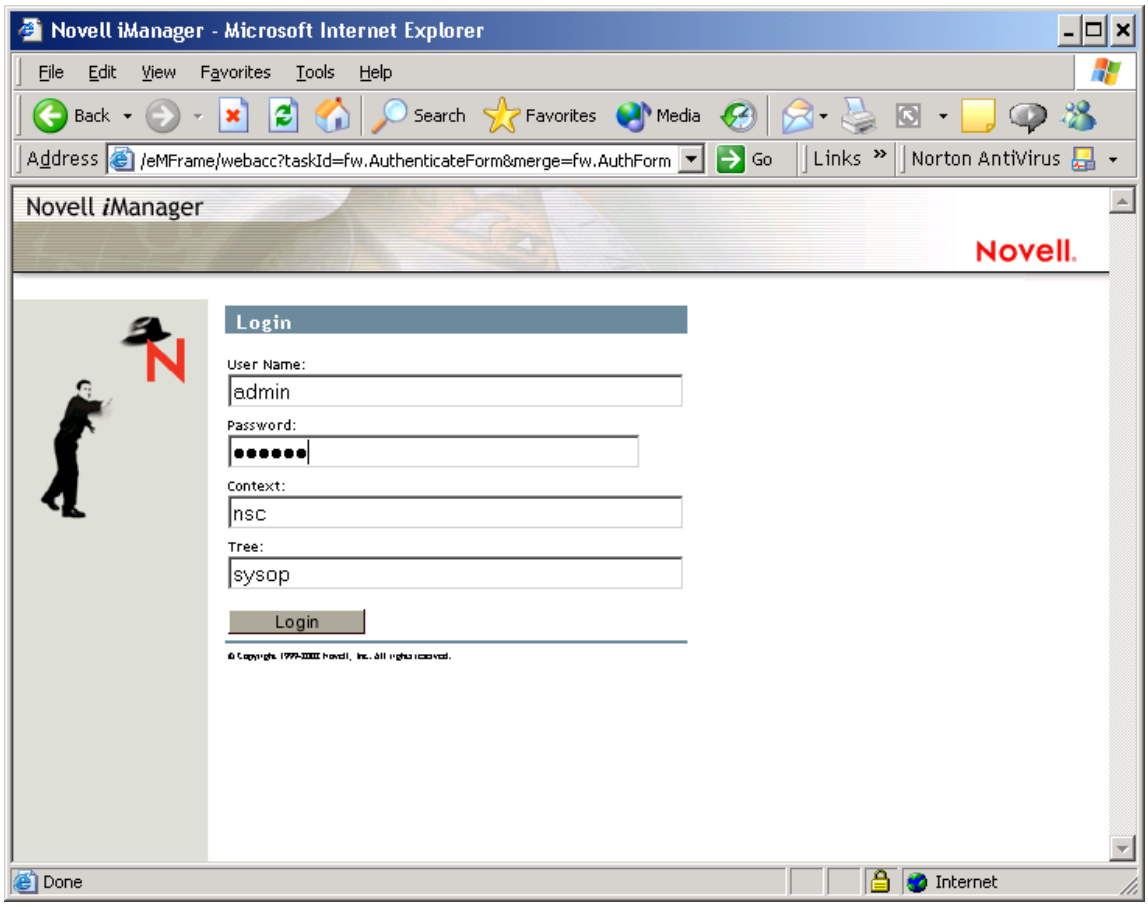
Notice that this is HTTPS, not HTTP.

The IP address is for any server (or Windows PC) running iManager, and does not have to be the BorderManager server.

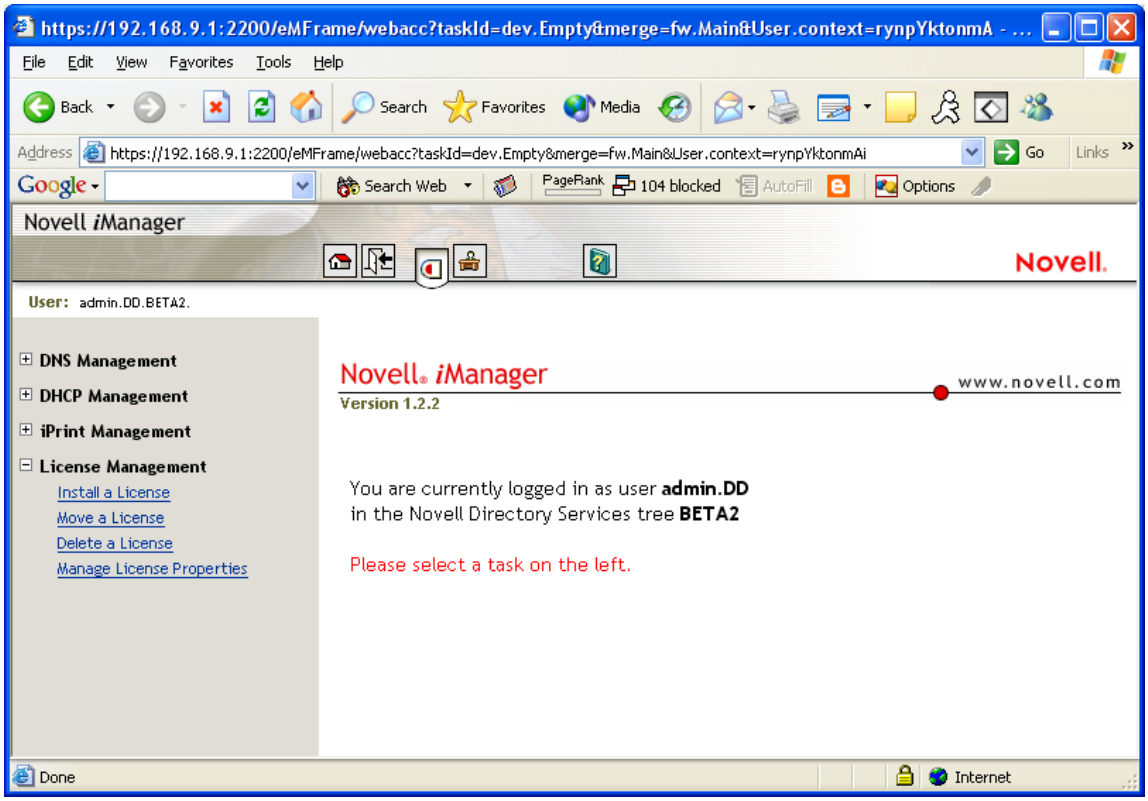
Substitute the private IP address of your iManager server for <server IP address>. The port (:2200) is the default iManager port number.

You will see an iManager link, which takes you to a login prompt. Log in as admin or admin-equivalent. The example shown is for NetWare 6.0. (If you have any problems at this point, it is far simpler to use NWADMN32 to add a license!)

You will see an iManager link, which takes you to a login prompt. Log in as admin or admin-equivalent.

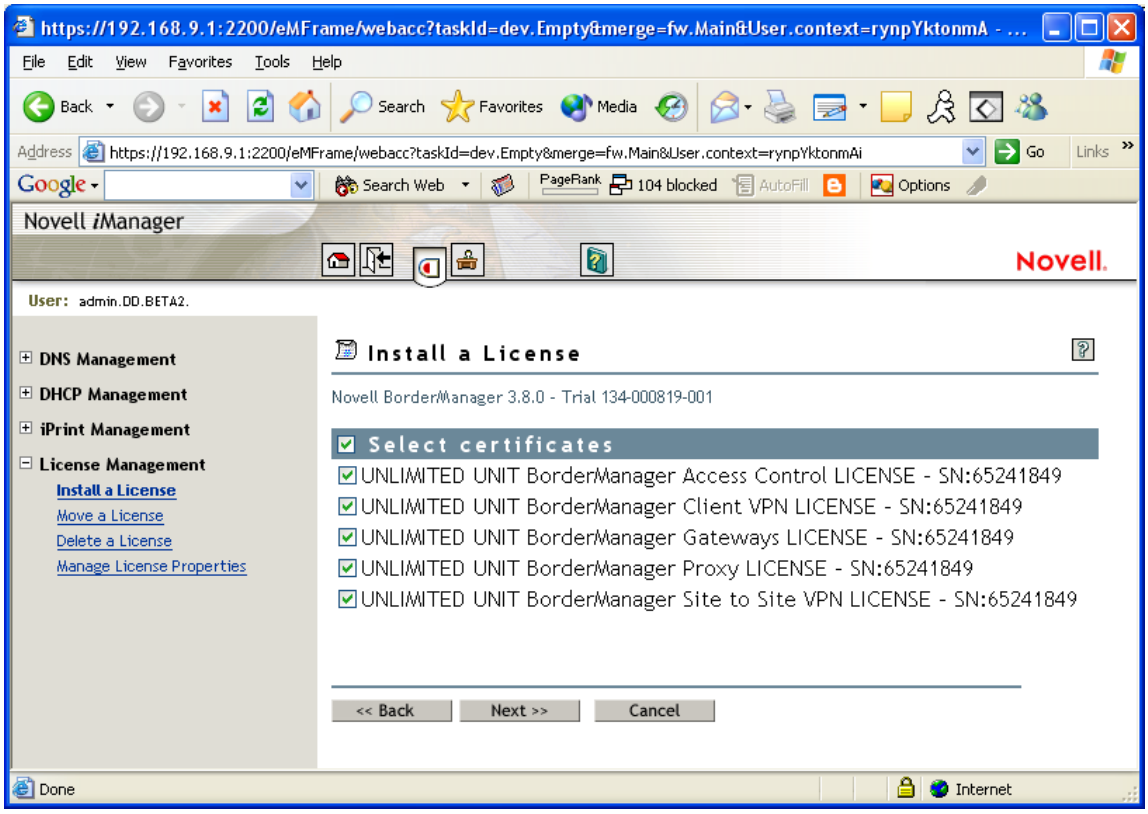


Log in as admin or admin-equivalent.

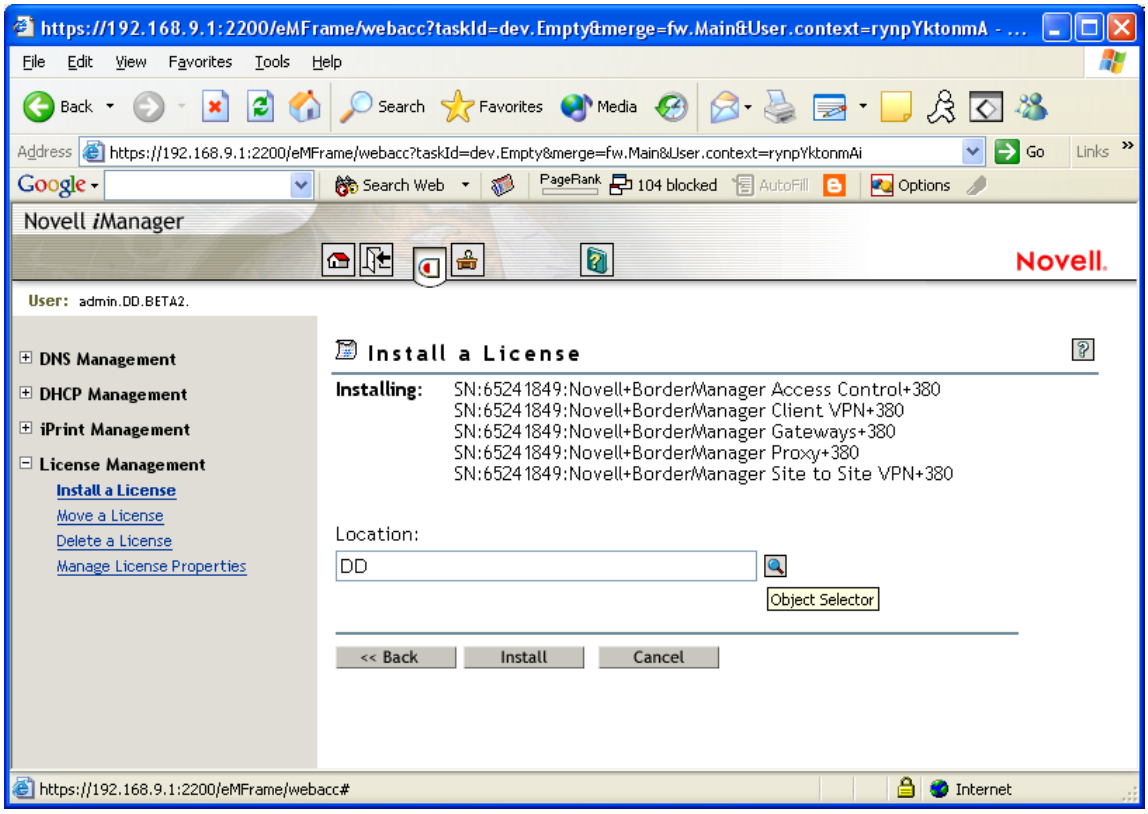


You want to select **License Management**, and **Install a License** on the left.

You should have a window to browse to the license file. Browse to the license file (probably on a floppy disk).



Select all of the licenses to install.



Browse to the location in the NDS tree where you want the licenses to be installed. I recommend putting them in the same container as the BorderManager 3.8 server.

Once the licenses are installed, you will see a window that tells you they have been successfully installed, and which gives you a '**Done**' option.

The FILTSRV MIGRATE Procedure

If you have just installed BorderManager 3.7 or upgraded to BorderManager 3.7 or 3.8 from an earlier version, you now need to migrate filtering information into NDS. The following procedure needs to be done once, when BorderManager is first installed.

Note The same procedure can be used later, in order to restore filtering information from a backup file, in case of disaster. There is more discussion on this point in the book "Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions", available from http://www.craigjconsulting.com/.

---

1. UNLOAD IPFLT
2. UNLOAD IPXFLT
3. UNLOAD FILTSRV
4. LOAD FILTSRV MIGRATE
5. UNLOAD FILTSRV
6. LOAD FILTSRV
7. REINITIALIZE SYSTEM

That should get the IP filter information (filters and exceptions) copied into NDS so that iManager can see them. (IPX and Appletalk filter exceptions are not copied to NDS or managed with iManager).

If you see –603 errors when you reinitialize system, or FILTCFG.NLM comes up when empty menus, you might need to manually extend the schema, and then repeat the FILTSRV MIGRATE process. Manually extend the schema with the following command:

```
LOAD SCHEXT <.admin.org> <admin password>
```

I recommend using FILTCFG to administer filters and exceptions as it writes filtering information to both FILTERS.CFG and NDS, thereby giving you a backup of filters in a file. (I cover filtering administration in much depth in my book "*Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions*". The Third Edition (or later) of that book covers the BorderManager 3.7 and 3.8 filtering system.

Starting BorderManager

You may wish to customize the AUTOEXEC.NCF file to more efficiently load BorderManager because of issues with BorderManager and Novell Licensing Services (NLS), and command line options available on certain modules. The following examples show portions of the AUTOEXEC.NCF file used on a BorderManager server. These examples point out a number of useful tips for launching BorderManager.

BorderManager 3.0 / NetWare 4.x

This is from a BorderManager **3.0** server that is a Site-to-Site VPN master, and is used for proxy services. I have included explanations and some options that are more oriented towards BorderManager 3.5 and 3.6 with later patches.

```
FILE SERVER NAME BORDER1
IPX INTERNAL NET 1234
#
load conlog  MAXIMUM=100
; Network driver LOADs and BINDs are initiated via
; INITSYS.NCF. The actual LOAD and BIND commands
; are contained in INITSYS.NCF and NETINFO.CFG.
; These files are in SYS:\ETC.
sys:\etc\initsys.ncf
#
SET NAT DYNAMIC MODE TO PASS THRU=ON
# STATIC NAT FOR PCANYWHERE, FTP SERVER, CITRIX
ADD SECONDARY IPADDRESS 4.3.2.253
# REVERSE PROXY ACCELERATION FOR WEB SERVER
ADD SECONDARY IPADDRESS 4.3.2.252
# STATIC NAT TO MAIL SERVER
ADD SECONDARY IPADDRESS 4.3.2.251
Search Add SYS:\JAVA\BIN
Load NLSLSP
Mount All
Load CSAUDIT
# BEGIN SAS/PKI (ADDED BY SASI)
Load CCS
Load PKI
# END SAS/PKI (ADDED BY SASI)
? Load MONITOR
? Load RDATE /P 240 /V 2 /U /M 999999999 171.64.7.77
# Load BorderManager Services
? Load BRDSRV.NLM
Load SYS:\ETC\CPFILTER\CPFILTER
Load VPMASTER
```

1. **SET NAT DYNAMIC MODE TO PASS THRU=ON** – This command keeps dynamic NAT from blocking inbound VPN and reverse proxy connections to the server. It is equivalent to the DISABLE NAT IMPLICIT FILTERING setting in INETCFG, Protocols, TCPIP.
2. **ADD SECONDARY IPADDRESS x.x.x.x** – These commands add the secondary IP addresses needed for static NAT. Depending on the version of BorderManager (3.5 or later), IP addresses defined in NWADMN32 will be loaded as secondaries automatically when PROXY.NLM loads.
3. **? Load MONITOR** - The ? tells NetWare to stop for 10 seconds and ask (on the server console) if the module should be loaded. After 10 seconds, the module is loaded if you do nothing. I simply use the ? to introduce a 10-second delay in the load sequence to give NLS licensing services a chance to complete so BorderManager Proxy will load without an error.
4. **? Load RDATE /P 240 /V 2 /U /M 999999999 171.64.7.77** – Used only on NetWare 4.11-5.1, RDATE sets the server clock. Once again, I introduce a 10-second delay to give NLS services time to complete the startup sequence so that PROXY.NLM will load without an error later. RDATE is used to set the clock on the server to an internet time source. In this case, **171.64.7.77** is, a time server in Stanford, California. The RDATE options are: /P 240 (check time every 240 minutes), /V 2 (allow up to 2 second variance on the clock before time is changed), /U (use UDP protocol), /M 9999999999 (a large number of seconds, the time the clock can be off and still be reset by RDATE), and the IP address of the target server. For NetWare 6.0 server, use the built in TIMESYNC.NLM to do NTP time services instead of RDATE.
5. **? Load BRDSRV –** The BRDSRV command will automatically load all other BorderManager services except for site-site VPN and RADIUS components. The ? option again delays the load command for 10 seconds, so that the licensing services have a chance to complete the initialization process. If you have a fast server, you may not need to use as many ? commands as I show in this example!
6. **LOAD CPFILTER** – This statement loads CyberPatrol
7. **LOAD VPMASTER** – This statement loads the module used to provide VPN service control from within NWADMN32 for a VPN master server in a Site-to-Site VPN configuration. If you have a VPN slave server, you would instead LOAD VPSLAVE.

BorderManager 3.7/3.8 / NetWare 5.x/6.x

This is from a BorderManager **3.7** / NetWare 6.0 server that is a Site-to-Site VPN master, and is used for proxy services

```
FILE SERVER NAME BORDER1
IPX INTERNAL NET 1234
#
# Get licensing services started early
Load NLSLSP
Load NLSTRAP
Load NLSFLAIM
#
; Network driver LOADs and BINDs are initiated via
; INITSYS.NCF. The actual LOAD and BIND commands
; are contained in INITSYS.NCF and NETINFO.CFG.
; These files are in SYS:\ETC.
sys:\etc\initsys.ncf
#
# Load Secondary IP Addresses
SECOND.NCF
#
Search Add SYS:\JAVA\BIN
#
Mount All
# BEGIN SAS/PKI (ADDED BY SASI)
Load CCS
Load PKI
# END SAS/PKI (ADDED BY SASI)
Load MONITOR
#
# Load BorderManager Services
Load SYS:\ETC\CPFILTER\CPFILTER
?STARTBRD
LINKWALL
Load VPMASTER
```

1. **Load NLSLSP, LOAD NLSTRAP, LOAD NLSFLAIM** – The purpose of these statements is to try to force licensing services to initialize as soon as possible so that when BorderManager needs to load, the licenses will be available.
2. **SECOND.NCF** – This NCF file contains all the secondary IP addresses needed for static NAT only. It is more convenient to call all those ADD SECONDARY IPADDRESS x.x.x.x commands out in an NCF file because you can simply type SECOND at the console prompt should you ever have lost the secondaries. (You can sometimes lose the secondaries when reinitialize certain LAN drivers).

3. **LOAD CPFILTER** – This statement loads SurfControl in BorderManager 3.7. SurfControl recommends that CPFILTER be loaded before BorderManager proxy loads.
4. **?STARTBRD –** The STARTBRD command will automatically load all other BorderManager services except for site-site VPN in BorderManager 3.7. (IKE-based VPN is auto-loaded from STARTBRD with BorderManager 3.8). The ? option delays the load command for 10 seconds, so that the licensing services have a chance to complete the initialization process.
5. **LINKWALL** – If you are using Connectotel's LINKWALL product, it is loaded after PROXY is loaded.
6. **LOAD VPMASTER** – This statement loads the module used to provide VPN service control from within NWADMN32 for a BorderManager 3.7 VPN master server in a Site-to-Site VPN configuration. If you have a VPN slave server, you would instead LOAD VPSLAVE. This command should not be required for BorderManager 3.8.

General Installation Notes

Working Around Licensing Startup Delays

Note See the section on NLS licensing below for an explanation of licensing in general. This segment is intended to show you a way to get BorderManager to start automatically, working around a slow initialization of licensing services problem.

NetWare 5.1 and later includes NLS updates that take much longer to start licensing services. NLS updates should be applied in the NetWare service packs. (The same issue happens on NetWare 4 and 5 servers if you have installed the NLS patches that include the NLSFLAIM database manager). A consequence of these updates is that BorderManager licenses may not be available when BorderManager tries to load because the licensing services are not yet available. The work-around is to delay the BorderManager load somewhat.

BorderManager 3.0, 3.5 and 3.6

The following technique works for me. First, move the LOAD BRDSRV line to the end of AUTOEXEC.NCF. Also move any VPMASTER, VPSLAVE and LOAD RADIUS statements to the end. Then, cause a 10-second delay to occur before loading BRDSRV by adding a ? to the beginning of that line in AUTOEXEC.NCF, as follows:

```
?LOAD BRDSRV
```

This generally gives NLS a chance to complete initializing before BorderManager launches. The key is usually seeing the NLSFLAIM.NLM module complete its loading before launching BorderManager. Should you see licensing error messages come up when certain BorderManager components are loading, yet loading those modules manually later works fine, you probably need to introduce more delays in the load sequences before BorderManager services try to load. Try adding a ? to other load statements preceding the LOAD BRDSRV line in AUTOEXEC.NCF.

BorderManager 3.7 and 3.8

BorderManager 3.7 and 3.8 launch from within a STARTBRD.NCF file called from AUTOEXEC.NCF. You can delay the start of that NCF file if you need to because of issues with BorderManager and Novell Licensing Services (NLS). The BorderManager 3.7 installation should have inserted a STARTBRD command in the AUTOEXEC.NCF file.

Normally, the STARTBRD command should work fine to automatically load all modules. However, for reasons involving occasional issues with licensing services, you should try to keep the STARTBRD command at the end of AUTOEXEC.NCF. If you should find that you get error messages about licenses not being available for BorderManager when the server boots, but that you can manually launch BorderManager when the boot sequence is completed, you may simply need to delay the STARTBRD command for a bit. The easiest way to do this is to add a question mark and space in front of the STARTBRD command.

```
?STARTBRD
```

This should have the effect of delaying the command by 10 seconds, which is often enough time to allow licensing services to initialize before BorderManager requests a license.

NDS –601 Error Messages At Startup

It is **normal** to get a –601 error when first starting the server after you install BorderManager on a NetWare 4.11 server. This error occurs because the BorderManager services are loaded before BorderManager itself has been configured. When you launch NWADMN32 (with proper BorderManager snapins), the snapins will recognize that the NDS schema for BorderManager may not have been extended and will submit schema extensions. Configuring the BorderManager attributes in NWADMN32 after that point should take care of any –601 errors on the next server reboot. The GUI installation process on NetWare 5.x and 6.x should already have made several settings for you. Enforcing rules, defining IP addresses as public and private, enabling HTTP proxy are all things that the NetWare 5 BorderManager GUI installation process tries to do for you. If those settings are made, you should not get the –601 error after a reboot, but even if you do, adding the public and private IP addressing configuration in NWADMN32 should take care of the –601 errors.

Loading and Unloading BorderManager Manually

You may well find the need to unload and reload BorderManager manually as you start the configuration process. In addition, it can be much faster to down the server if you first unload the BorderManager modules. (BorderManager tries to release NLS licenses as it is unloaded, but downing the server will probably disable NDS first, resulting in long timeout delays while BorderManager finds out that it cannot contact NDS to release the licenses).

Note BorderManager 3.7 and 3.8 comes with two NCF files that you can use, or modify, as desired. STARTBRD.NCF and STOPBRD.NCF. The STARTBRD.NCF file may also launch RADIUS, or set certain parameters. The STOPBRD.NCF file does not unload RADIUS. Neither NCF file contains any commands to start or stop 3rd-party products like SurfControl or LinkWall.

I have found the following two NCF files to be useful for me in stopping and restarting the BorderManager services. Feel free to modify them for your own purposes. Just use a text editor (LOAD EDIT at the server will work) to create the following two files in the SYS:\SYSTEM directory. Typing BMOFF at the console prompt should then unload the BorderManager files, and typing BMON should reload the files.

You will find it useful to stop and restart the BorderManager services, or at least the PROXY.NLM, for the following purposes:

1. You have just set up the BorderManager for the first time.
2. You have just changed the proxy cache location or other parameters.
3. You have just changed the log file location
4. You have just added or changed a custom error page for the HTTP Proxy.
5. You want to force a reload of the services for troubleshooting.

BMOFF.NCF (BorderManager 3.6 or Earlier)

If you have BorderManager 3.7 or 3.8, use STOPBRD.NCF.

```
rem Craig Johnson, Feb. 12, 2002 See http://www.craigjconsulting.com
rem Unloads most BorderManager-related NLM's
unload proxy
rem You may want to delay unloading proxycfg until proxy.nlm
rem unloads completely.
rem Some users have seen an abend without the delay, though
rem most are fine.
rem The ? should cause a 10-second delay before proxycfg
rem unloads, unless you press Y.
?unload proxycfg
rem Unload CyberPatrol.
unload cpfilter
rem unload IPX/IP, IP/IP and SOCKS Gateway
unload ipxipgw
rem Unload VPN authentication module
unload authgw
unload authchk
rem Unload Access Rules module
unload aclcheck
rem Unload BorderManager alert module
unload nbmalert
rem The next two lines unload VPN modules.
unload vpmaster
unload vpslave
rem Unload main BorderManager monitoring modules
unload brdmon
unload brdsrv
```

BMON.NCF (BorderManager 3.6 or Earlier)

If you have BorderManager 3.7 or 3.8, use STARTBRD.NCF.

```
Rem COMPLEX SECTION - uncomment the Load lines if you really need them.
Rem *** Don't use the /NOLOAD section unless you really need to
Rem use the -M option
rem *** with Mail Proxy! The /NOLOAD option can really make
rem loading & unloading BorderManager tricky. (Meaning possible
rem ABENDS on reloading)
rem *The NOLOAD proxy prevents autoloading of most other
Rem BorderManager modules
rem Load BRDSRV /NOLOAD
rem *The /S options represses certain (cosmetic) error messages.
rem Load ACLCHECK /S
rem *Not needed if already loaded, but the /NOLOAD option above
rem will cause an ABEND when
rem *PROXY loads if you don't load this first.
rem Load IPXF
rem *The /M option tells Mail Proxy to query more than one MX
rem record if needed
rem Load PROXY -M
Rem *Loads CyberPatrol
rem Load SYS:\ETC\CPFILTER\CPFILTER
Rem *Load additional options that do not autoload with the
Rem BRDSRV /NOLOAD option
rem Load AUTHGW

Rem SIMPLE BorderManager Load Section
Rem *Start most BorderManager services
Load BRDSRV
Rem *Load CyberPatrol
Load SYS:\ETC\CPFILTER\CPFILTER
Rem *Loads VPN control module - select the one you are using,
Rem *or comment out both if not using VPN.
Load VPMASTER
rem Load VPSLAVE
```

BorderManager Licenses

BorderManager 3.0, 3.5 and 3.6 were sold in several different bundles. The Enterprise Edition contained licenses for all the BorderManager services, which are Proxy, Access Control, Client-to-Site VPN, Site-to-Site VPN and Gateways. Other versions of BorderManager 3.x, such as VPN or Firewall, contain only some of the licenses, however, all versions of BorderManager 3.x prior to 3.7 included trial licenses for all of the services. Be careful that you do not install a trial license if you intend to install the actual license. Trial licenses can be easily identified by the file name of the license files as they end in a 'T'.

In addition, BorderManager 3.0, 3.5 and 3.6 shipped with a run-time license for NetWare 5 or 5.1, consisting of a NetWare 5/5.1 Server Connection license and a NetWare 5/5.1 2-user license

BorderManager 3.6 uses BorderManager 3.5 licenses. All other versions of BorderManager use their own licenses.

BorderManager 3.7 and 3.8 is only sold with licenses for all services – essentially like the Enterprise Edition of previous versions. BorderManager 3.7 or 3.8 licenses may require iManager to install them on NetWare 6.x.

What Are NLS Licenses?

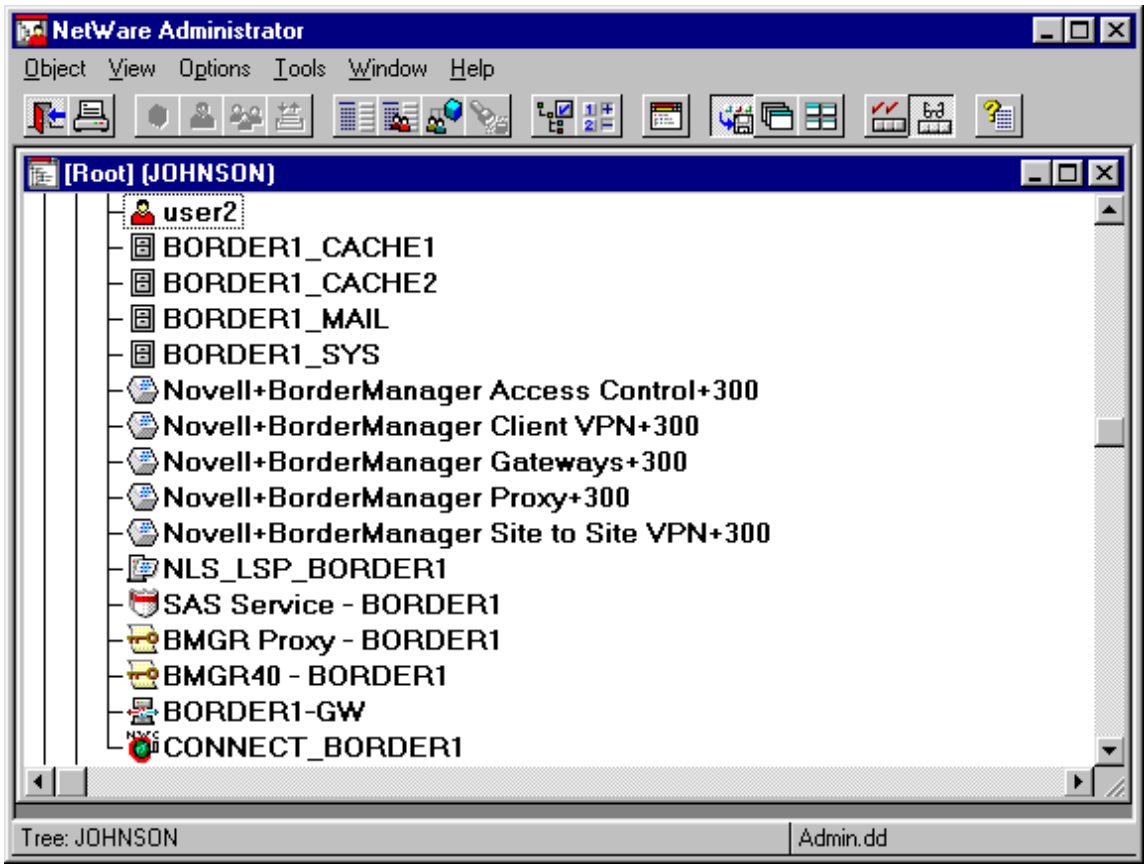
Unlike NetWare 4 and earlier versions of NetWare, BorderManager licenses are NDS-based, making use of Novell Licensing Services (NLS), like NetWare 5 and 6. This leads to a number of issues, because NLS itself was plagued with problems when it first was introduced. (NLS issues were reduced with each service pack). NLS-based licenses are created as NDS objects, and can only be maintained by the same user ID that created them. In the later versions of NLS, following certain patches, the NLS licenses cannot even be backed up to tape, so keep the license diskettes themselves in a safe place. It is a good idea to copy the files on the license diskettes to one or more servers so that the files themselves can be backed up as needed.

License information is communicated between NDS and the server by the NLSLSP.NLM program running on a NetWare 4.x, 5.x or 6.x server. When you install NLS, the SETUPNLS.NLM program is run at some point, and that program creates an NLS object for the server, in the server context, called NLS_LSP_<servername>.

BorderManager 3.x contains NLS licenses (either production or trial) for:

- Access Control

- Proxy
- Gateways
- Client-to-Site VPN
- Site-to-Site VPN



The licenses shown in the example above are for BorderManager 3.0. You can tell because they end in +300. (Actually, those are the license containers – the actual license objects are inside each of the license container objects.)

NLS Issues

NLS licenses can, theoretically, be installed anywhere in the NDS tree above the server object or in the same container as the server object and the server will walk the tree to find them. **Don't put the licenses in another container unless you just want to increase the number of licensing problems you might see.** Install the licenses into the same container with the server. Licensing is very sensitive to NDS issues and timing issues. If a license cannot be found, some services may fail. Licensing usage information is also updated frequently, so constant NDS communications are needed. Failure to communicate successfully with license objects also results in very

annoying messages being sent to the server console, the users, or both.

Since BorderManager Enterprise Edition, 3.7 and 3.8 contain five separate NDS-based license objects, in addition to two for NetWare 5.x/6.x servers, the administrator of a BorderManager server has a better chance than most to see licensing-related issues. See the troubleshooting section of this book for information on how to deal with licensing issues.

License objects, NLSLSP and associated schema definitions have undergone changes with various patches since BorderManager 3.0 was released. As a rule of thumb, expect that any change involving NLS may result in the need to delete and reinstall the licenses, and perhaps the NLS_LSP_<servername> object.

License objects can be installed by two methods for NetWare 5.x/6.x servers and one method for NetWare 4.11 servers. Both server versions can use NWADMN32 to install license objects. NetWare 5.x/6.x servers can use a menu option in NWCONFIG.NLM to install license objects. NWCONFIG will always install the license objects into the same context as the server, and it will automatically assign the licenses to the server. NWADMN32 will install the license objects (called envelopes in NWADMN32) wherever you like, but it will NOT assign the license objects to the server automatically. You must manually go into the license objects themselves and assign them to a server with the NWADMN32 installation method.

Note Note: You can also use the LICMAINT.NLM utility to install licenses on NetWare 4.11, and it may work when no other methods do. Look for the utility in the NIAS42\INSTALL directory on a BorderManager CD.

MLA Licenses

MLA licenses are special. They can be installed as many times as desired (in separate NDS containers), and NLS MLA licenses do not have to be explicitly assigned to a server. In fact, a server assignment can create a problem in some cases. The server assignment issue comes up if you have one MLA license for all your servers (and this can apply to NetWare 5.x or 6.x or BorderManager 3.x licenses), and you have more than one server in the same NDS container. Because you cannot have more than one object by the same name in a container, you cannot install a MLA license twice in the same container. However, if you do not make a server assignment for the MLA licenses, all servers without an explicitly-assigned license will find the MLA license in the container and use it automatically. But if NWCONFIG has been used to install the MLA license, it may already have an explicit assignment to a server and be

unavailable for use by other servers. In this case, removing the server assignment from the license object would be required.

Note If you have NOT installed the MLA license to the server using NWCONFIG, you may have to manually copy the NICI files from the license diskette to the DOS partition (and rename them) in order to get encryption services to work. See TID 2945674.

Changing Out A BorderManager Server

There are at least two reasons you might want to change your old server for another:

- You are replacing an old server with a new one that has been built on different hardware.
- You wish to work on the production server while maintaining connectivity for the users, minimizing downtime, and working on the production server during normal working hours. In this case, the idea is to swap in a temporary server, work on the production server, and swap the production server back into place.

Concerns

The procedure described below has some drawbacks, but will at least give you some possibility for minimizing the disruption of changing the server. The most serious implications are for inbound traffic, and time-sensitive traffic such as Telnet. Site-to-Site VPN connections will **not** be supported with the method described below, but would have to be recreated from scratch. Client-to-Site VPN connections would have to be restarted. Outbound connections through a browser generally require the browser to be stopped and restarted. In some rare cases, the server may be connected to a switch that refuses to release the old ARP table entry matching an IP address to a network card MAC address, and the switch may need to be reset.

Concept

Substitute the IP addresses on one BorderManager server to another one, avoiding having both servers online at the same time with the same IP addresses. Timing and sequencing of the changes is critical.

Procedure 1 – Primary IP Addresses Used

This procedure would tend to be used if you are permanently changing one server for another, as in upgrading from a BorderManager 2.1 server to a BorderManager 3.6 server.

1. Both servers should be up and running in the same NDS tree. You need to have a replica on the new server that holds at least the new BorderManager server object.
2. Change the SYS:\ETC\HOSTS file on the new server to the new IP address.

3. You may have to reattach and log into the server if you had an IP connection to the server. In order to log in, you will have to have a replica on the server holding your user ID.
4. In NWADMN32, BorderManager Setup, change the IP addresses.
5. In NWADMN32, change any proxies (and access rules) as needed to listen on the new IP addresses. At this point, all the IP address-related settings on both servers should match.
6. Notify users that a brief outage of Internet services may occur.
7. Quickly disconnect the old server private side connection, and reconnect to the hub or switch being used by the new server.
8. Quickly disconnect the old server public side connection and reconnect to the new server public interface.
9. At this point, you might have to reset an internal switch if connectivity cannot be made to the new server. (ARP caching issue.) The only way to tell if this will be an issue is to test this procedure ahead of time – something that could be done using test servers.
10. If you were browsing through the old server, close and re-open the browser, and you should reconnect right away to the desired web site. If you were using proxy authentication, a new authentication request will be sent from the proxy to the clients.
11. Test all outbound and inbound applications to ensure that they are working.
12. If you had a site-to-site VPN set up before, it will have to be reconfigured from scratch on the new server, and if the server being replaced was the Master VPN server, ALL of the servers involved in the VPN would have to be reconfigured.
13. When things are working, you should be able to reconnect the server to the internal network and remove the hub or switch that was temporarily in use. This could be done much later, when convenient.
14. In order for NDS synchronization to continue, the old server must be brought back online. Use the BMOFF.NCF files described in this book to unload BorderManager services first.
15. Using INETCFG, change the IP addresses on the old server.
16. Comment out the BorderManager load statements and any secondary IP address assignments in AUTOEXEC.NCF.
17. Reconnect the private interface on the old server to the production network. The old server should reconnect to the NDS tree and establish time synchronization.

18. When you are confident that the new server is functional, you can remove NDS from the old server to take it out of the NDS tree permanently.

Procedure 2 – Secondary IP Addresses Used

This procedure is much simpler than the first procedure, and can be used in many cases if the two servers are properly configured ahead of time. It is an excellent way to move a standby server into place as a temporary replacement while you work on the production server. It is also the procedure you use to prepare BorderManager servers to be clustered. It requires you to have a public side subnet mask other than 255.255.255.252 and at least one available public IP address to assign to the server. It requires the main private proxy IP address on both public and private servers to be a secondary IP address. Internal routers and hosts would be pointing to this secondary IP address as a default route, and browsers would be pointing to this secondary IP address for the HTTP Proxy settings.

If all of the traffic of concern is outbound, this procedure becomes extremely simple. However, site-to-site **VPN is not supported**, and other inbound traffic via static NAT or reverse proxies would have to be set up again or redirected via DNS services as needed. Client-Site VPN essentially becomes a pair of Client-Site servers, with only one of them working at a time.

In this procedure, two BorderManager servers are run in parallel at the same time, with both public and private interfaces connected. The servers will remain connected to the network at all times with this procedure, which tends to minimize NDS disruptions.

For this example, the old server is configured with a private IP address of 192.168.10.2, and the new server is configured with a private IP address of 192.168.10.3. The old server has a secondary IP address of 192.168.10.1 on the private side, and all of the proxies are set to use the 192.168.10.1 address. The default gateway of internal hosts are also pointing to 192.168.10.1.

The concept here is going to be to move the 192.168.10.1 address to the new server, at which point all outbound traffic should follow.

1. The new server is configured in NWADMN32 to listen on its primary IP binding for proxies. The old (production) server is configured to use a secondary IP address for proxies. Default routes are pointing to the old server's secondary private IP address. Testing indicates that all services are working on both servers.

2. Using NWADMN32, change the private IP address on the new server to 192.168.10.1 (main production server private IP address being used). Do NOT press OK to save changes!

3. Using NWADMN32, change all of the proxies (and any access rules) as needed to use the new (192.168.10.1) private IP address. Do NOT press OK to save changes!
4. On the old (production) server, type DELETE SECONDARY IPADDRESS 192.168.10.1 (or whatever your private address is). Do NOT press Enter yet.
5. On the new server, type ADD SECONDARY IPADDRESS 192.168.10.1 (or whatever the your private IP address is). Do NOT press Enter yet!
6. At this point you should have a workstation ready to commit the proxies to listen on a new IP address, the old server ready to delete a secondary IP address, and the new server ready to add a secondary IP address. Notify users that there will be a short disruption of services.
7. Press Enter on the old server to delete the secondary IP address. After that, no traffic should be going through the proxies.
8. Press Enter on the new server to assign the secondary IP address. Traffic going out via default router and filter exceptions should begin flowing immediately. If not, you may have an internal switch that is holding old ARP cache data which needs to be reset.
9. Press Enter on the workstation to assign all of the IP address and proxy changes to the BorderManager server. As soon as the server rereads its configuration from NDS, the proxies should begin listening on the new secondary IP address.
10. Test outbound connectivity. Users will have to close and reopen their browsers. In the best cases, I have seen this procedure work with as little as 5 seconds of downtime for the switch. You should test in your environment.
11. This procedure primarily takes care of outbound traffic, not inbound or Site-to-Site VPN. Inbound static NAT connections will move as easily as the outbound services did, as long as you have moved the old public secondary IP addresses to the new server, have static NAT already configured, and have filter exceptions already configured. I normally use an NCF file to remove secondary IP addresses, and another one to add them.
12. If you had reverse proxies configured for secondary IP addresses, they can also switch over as easily.
13. If you are using Client-Site VPN, it needs to be configured on both servers. As VPN normally works only on the primary public IP address, the easiest way to get this working is to tell remote clients to use the new server's IP address. Site-Site VPN simply will not transfer to a new server without being reconfigured.

14. You may now work on the new server as needed, applying patches, replacing hardware, etc. Be aware that reloading the proxy would try to reassign the IP addresses and result in messages on the console that the IP address were already in use. You may want to reconfigure the IP addresses in the BorderManager Setup menu in NWADMN32 to not conflict with those on the other server, or unload the BorderManager services with the BMOFF.NCF file (or STARTBRD.NCF) shown in this book.
15. When ready to put the production server back in place, you follow the same procedure to swap IP addresses.

Critical BorderManager-Related Files

Configuration Tools

INETCFG.NLM

A menu-driven utility used to configure networking components. This utility writes data to the NETINFO.CFG, TCPIP.CFG, RESOLV.CFG and GATEWAYS files.

NIASCFG.NLM

A utility used to configure NIAS dial-in/out services and VPN services. Actually, all it does is serve as a menu to launch other menus, such as VPNCFG.

VPNCFG.NLM

Used to configure Site-to-Site VPN parameters, and is also required if configuring Client-to-Site VPN.

BRDCFG.NLM

Use to set up the default packet filters and default packet filter exceptions at any time after the BorderManager installation. Should you ever need to delete filter exceptions and replace the defaults, use BRDCFG.

FILTCFG.NLM

A utility used to configure packet filter exceptions. Makes changes to the SYS:\ETC\FILTERS.CFG file as well as to NDS.. BorderManager 3.7 and 3.8 can also use iManager. I recommend continuing to use FILTCFG.

INSTALL.NLM

A utility used to configure the server components and install product options on NetWare 4.2 and 4.11. In NetWare 5.x, this file is called NWCONFIG.NLM.

NWCONFIG.NLM

A utility used to configure the server on NetWare 5.x and 6.x.

SYS:\PUBLIC\WIN32\NWADMN32.EXE

The main configuration utility used by Win95/98/NT PCs to configure NDS-related objects and services, including most of the BorderManager services. Requires you to be logged into NDS with Client32.

SYS:\PUBLIC\MGMT\CONSOLEONE\1.2\BIN\CONSOLEONE.EXE

The replacement for NWADMN32 for many new features in NetWare 5.1. There are no snapins for BorderManager 3.x for ConsoleOne (as of the writing of this book), but you may have to use ConsoleOne to create SSL certificates for BorderManager SSL Proxy Authentication. ConsoleOne can also be used for Certificate-related objects for BorderManager 3.8 VPN, and creating cache volumes on NetWare 6.0.

iManager 2.0

iManager is not actually a file, but a Java-based application running under Apache/Tomcat used to manage BorderManager 3.7 and 3.8 filters, licenses for NetWare 6.x, and the new BorderManager 3.8 VPN components. iManager is something you see in your browser.

iManager 2.0 is required to configure the BorderManager 3.8 VPN components, but earlier versions of iManager can be used to manage packet filtering. FILTCFG can be used to manage filters on all versions of NetWare and BorderManager.

iManager 2.0 has requirements for a newer version of JAVA than previous versions of iManager. This version of JAVA can be problematic with many services that used previous versions of iManager, and so you should be very careful when trying to upgrade to iManager 2.0 on existing servers. iManager 2.0 is not supported on NetWare 5.1. As of this writing, a version of iManager 2.0 was to be supplied for NetWare 6.0 servers. iManager 2.0 comes as the default version on NetWare 6.5.

You can use iManager 2.0 from any NetWare 6.5 server to administer your BorderManager 3.8 VPN services, or use a Windows installation of iManager 2.0 (from the BorderManager 3.8 companion CD).

IManager 1.5

iManager is not actually a file, but a Java-based application running under Apache/Tomcat used to manage BorderManager 3.7 or 3.8 filters, and licenses for NetWare 6.0. Also can be used to schedule tasks (commands) for events such as launching SurfControl updates. iManager is something you see in your browser. iManager 1.x comes with NetWare 6.0, while iManager 2.0 comes with NetWare 6.5. You cannot use iManager 1.x to administer the BorderManager

3.8 VPN components. With some effort, you can get iManager 1.5 and 2.0 to run at the same time on a NetWare 6.0 server.

CRON.NLM

CRON is a scheduling utility, which can be used to launch commands on a schedule. It can be used to launch SurfControl updates. CRON executes commands listed in the SYS:\ETC\CRONTAB file.

Novell Remote Manager (NRM)

NRM is a browser-based utility that can be used not only for monitoring a NetWare server, but also for creating partitions and volumes. For BorderManager 3.8, NRM provides VPN monitoring functions not available elsewhere. NRM is sometimes called Portal, because it comes from the PORTAL.NLM module. (Another module, called HTTPSTK.NLM, is also required).

Data Files

SYS:\ETC\HOSTS

A text file containing host name/IP address information. Especially useful in regard to configuring reverse proxy. Essential to have Loopback and server name configured for NetWare 5.x./6.x Be sure to leave a blank line at the end of this file for best results.

SYS:\ETC\HOSTNAME

A text file containing host name/IP address information. Similar to the HOSTS file, but only for the server name itself. The address should reflect the internal IP address in this file.

SYS:\ETC\GATEWAYS

A text file holding static routing assignments, the most important of which is the default route. Normally edited transparently through INETCFG, but can be edited manually. Site-to-Site VPN also puts static routes in this file.

SYS:\ETC\RESOLV.CFG

A text file holding DNS resolver configuration for the server. Normally edited transparently through INETCFG, Protocols, TCP/IP, DNS Resolver Configuration, but can be edited manually.

SYS:\ETC\TCPIP.CFG

A file that contains TCP/IP configuration information. Edited transparently through INETCFG. Not recommended to edit this file manually unless you know what you are doing.

SYS:\ETC\NETINFO.CFG

A file that contains almost all networking information. Normally edited through INETCFG, but can be manually edited in a pinch if you know what you are doing. Sometimes 'protected' by a CRC check held by NETINFO.CHK (which should be deleted if you are going to manually edit NETINFO.CFG). Problems in NETINFO.CFG can lead to odd failures, particularly with static NAT.

SYS:\ETC\FILTERS.CFG

The file that holds packet filters and packet filter exceptions. Can be manually edited if you know what you are doing. **By backing up this file, you can back up your packet filters and exceptions**!

Note IP filters are stored in NDS with BorderManager 3.7 and 3.8, and can be managed via a browser interface with iManager. It is possible to import and export the NDS-based filter data to a text file, but that procedure is outside of the scope of this book. See the Third Edition of my book "Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions".

SYS:\ETC\CRONTAB

The file that holds scheduling data used by CRON to launch programs. Useful for updating SurfControl.

SYS:\ETC\PROXY\PROXY.CFG

The file that contains both required and optional settings for PROXY.NLM, as well as anti-virus patterns. The default file should be updated when you install BorderManager 3.5 or later.

Startup Files

C:\CONFIG.SYS

Used to provide CDROM drivers when installing NetWare from CD, if you did not boot from the CD. (NetWare 5.x/6.x CD's are bootable, bios permitting, NetWare 4.x CD's are not). You should not load any DOS drivers when starting NetWare, except when

needing to install NetWare at first, and you should never load HIMEM.SYS when using NetWare.

Note: If using DOS 6.22, you SHOULD have at least FILES=30 and BUFFERS=30 lines in CONFIG.SYS to reserve files and buffers for NetWare to use when starting up. (Higher values are OK.)

C:\AUTOEXEC.BAT

Used to launch SERVER.EXE from DOS, which begins loading NetWare.

C:\NWSERVER\STARTUP.NCF

Launches the initial NetWare drivers, and some memory related commands, including disk drivers so that the NetWare partition can be seen.

SYS:\SYSTEM\AUTOEXEC.NCF

Launches most of the NetWare services as NetWare loads, including the commands to start BorderManager services.

Troubleshooting Tools

TCPCON.NLM

A utility used to view ARP and TCP/IP routing tables. It is useful for debugging multiple network environments and a host of TCP/IP-related issues.

CALLMGR.NLM

A utility used to force dial-up connections manually, and also can be used to bring up VPN links in some cases. If you are trying to set up a test BorderManager server with a modem and having problems, you will want to use this utility to help debug the connection. Works well with PPPTRACE.NLM.

PPPTRACE.NLM

A utility used to view PPP connections for dial-up interfaces. If you are trying to set up a test BorderManager server with a modem and having problems, you will want to use this utility to help debug the connection. Works well with CALLMGR.NLM.

Keeping BorderManager Up-to-date

Patches

BorderManager has had a history of unreleased field test or partner release patches being available long before those patches make it to the Minimum Patch List. It is best to keep an eye on the Novell Support Connection public forums to find out what the latest field test patch name is. In the same forums you can find information about the quality and stability of the latest patches. They also have tended to change revision often enough that they never quite seem to make it to the minimum patch list. As an example, the BACL105.EXE patch for BorderManager 2.1 was available for almost nine months before making it to the minimum patch list. If you have problems with a BorderManager server, strongly consider applying the latest available patches, even if they have not yet made it to the minimum patch list.

Review the Novell Minimum Patch List at http://support.novell.com/misc/patlst.htm for released patches. Note that these are *minimum* patches – considered essential by Novell for the best stability. There are often other patches available, and are often beta and pre-beta patches available.

Keep an eye on the Novell Support Connection public forums to find out about the latest patch issues. You can also visit http://www.craigjconsulting.com and check **tip #1** there find out about the current BorderManager patches and installation sequence.

PROXY.CFG Settings

The SYS:\ETC\PROXY\PROXY.CFG file contains optional settings for the proxy configuration. With new proxy patches, Novell often adds a new configuration option, to be enabled or disabled in the PROXY.CFG file. Sometimes one patch will have an optional parameter that is turned on by default in a later patch.

The parameters to configure are tied to the patch level of the server. See Novell TID 10059667 for a list of parameters and their meanings, and also read the patch installation instructions carefully.

There is an example PROXY.CFG file shown later in this book in the Performance Tuning chapter. You should also check my web site at http://www.craigjconsulting.com for a current version of PROXY.CFG with recommended settings and discussion of pertinent issues.

The BorderManager 3.5 Enhancement Pack

Novell typically views Enhancement Packs as a means of introducing new features, where patches are only supposed to fix bugs. Adding an Enhancement Pack usually makes the product being 'enhanced' a whole new version - without changing the revision number. This was certainly true of BorderManager 3.5 and GroupWise 5.5 enhancement packs. Why do you care? Because once you apply an enhancement pack, you **may** have to use entirely different patch sets for the product! For instance, the BorderManager 3.5 Enhancement Pack included code through the interim BM35C02.EXE patch, but not the later patches, such as BM35C03.EXE through BM35C08.EXE. In fact, these later patches were incompatible with the BorderManager 3.5 Enhancement Pack and the Enhancement Pack had to be (manually) uninstalled if you wanted to put the later patches on.

This patch situation has changed with the BorderManager 3.5 Service Pack 2 patch. This patch includes the functionality of the Enhancement Pack and is compatible with the Proxy/ACL patches BM35C09.EXE and later, as of the time of this writing.

If you have patched your servers with the latest BorderManager patches, you should have all of the capabilities provided with the BorderManager 3.5 Enhancement Pack, and none of the problems.

Tips For Getting NWADMN32 To Work With BorderManager Servers

A number of people have had trouble getting NWADMN32.EXE to work well with BorderManager 3.x. Here are some tips to try.

-601 Errors when Accessing BorderManager Servers

This error is caused by a bug in certain versions of NMAS installed on the client, usually seen with Client32 4.90 or 4.90sp1a. There are two ways to cure the problem:

- Remove NMAS from the PC, using Control Panel, Add/Remove Programs, and look for NMAS Client Components. Naturally, this will prevent you from using certain NMAS-related features, but it is a quick and easy workaround.
- Patch Client32 with a post-4.90SP1a patch. As of this writing, there is a patch called 49psp1a_netwin32.exe. Download it from Novell and install it. After a reboot, the –601 errors should be gone.

Fix NWADMN32 Crash by Renaming the ACNWAUTH.DLL Snapin

If NWADMN32 crashes as soon as you try to view the details on a BorderManager 3.x server object, try renaming **ACNWAUTH.DLL** so that it will not run. That snapin is for ActivCard authentication objects only, and if you are not using ActivCard, you can live without the snapin.

Get The Latest Version of NWADMN32

The latest version of NWADMN32.EXE is 5.19f, and is available from http://support.novell.com in a patch named ADMN519F.EXE. However, this version should already be included on NetWare 5.1 and 6.0 servers.

Fix Invalid BorderManager Snapin Modules Errors

Create a shortcut to NWADMN32.EXE using the path \\<servername>\sys\public\win32, and then put \\<servername>\sys\public in the 'starts in' field of the link. The 'target' value should be: \\<servername>\sys\public\win32.

Copy the NLSAPI32.DLL from SYS:PUBLIC to SYS:PUBLIC\WIN32.

Fix “No BorderManager Licenses Available” Messages

Look at Novell TID 2954946, "BorderManager 3.0 License Fix", which discusses the BM3LICFX.EXE patch, if you are using BorderManager 3.0.

Delete .LG Files in the SYS:\PUBLIC\WIN32\NLS\ENGLISH Directory

See Novell TID 10025511 at for some details and general NWADMN32 issues help. (That TID mentions NWADMN32 5.18, but 5.19f is the latest available version now).

PC Hangs When Accessing NWADMN32

If you have a Windows 2000 PC that wants to freeze up when accessing NWADMN32, try SET CLIENT FILE CACHING ENABLED=OFF on the server console. Also, in the Novell Client32 properties on the PC, set File Caching to Off.

NWADMN32 Fails After BorderManager 3.8 Upgrade

In general, after upgrading BorderManager or installing a new BorderManager patch, it is a good idea to run the BorderManager snapin installation program in SYS:\PUBLIC\BRDRMGR\SNAPINS if you have any NWADM32 snapin-related issues. One specific file to look at is the MFC42.DLL file in SYS:\PUBLIC or perhaps SYS:\PUBLIC\WIN32. Incorrect versions of this file can cause problems with NWADMN32. My NetWare 5.1, BorderManager 3.8 server has such a file dated 1/31/1997, but my NetWare 6.5, BorderManager 3.8 server has no such file at all.

What snapins should I have?

This is NOT a comprehensive list, but it may help some people to see what I have in my BorderManager test servers.

BorderManager 3.8 / NetWare 6.0

The following snapins are used on one of my BorderManager 3.8 servers.

```
BorderManager 3.8 / NetWare 6.0

Volume in drive Q is SYS
 Volume Serial Number is C0A8-0901

 Directory of Q:\PUBLIC\win32\snapins

09/13/2003  02:39 AM    <DIR>          .
09/13/2003  02:39 AM    <DIR>          ..
05/19/1999  04:45 PM            85,504 ALERT.DLL
03/02/2000  09:09 AM            11,776 audit32.dll
09/15/1999  10:19 AM           119,296 BSCOV.DLL
01/24/2003  05:28 PM           803,328 BSMON.DLL
09/27/2003  10:29 PM               148 dir.txt
06/10/1998  09:13 AM           174,592 MANAGEIP.DLL
02/08/2000  09:27 AM           153,600 NCSSnap.dll
08/02/2000  06:26 AM           561,152 NLSMGR32.DLL
06/02/1998  06:33 PM            71,680 NWCADM32.DLL
11/04/1998  08:48 AM            78,848 NWSLPSI.DLL
12/19/2002  06:19 PM           532,992 proxycfg.dll
12/11/1999  08:49 AM           195,072 REGEDT32.DLL
08/07/2003  05:13 PM           364,032 restrict.dll
09/13/2003  09:53 AM    <DIR>          Ini
              13 File(s)      3,152,020 bytes
               3 Dir(s)   1,220,911,104 bytes free
```

BorderManager 3.7 / NetWare 6.0

The following snapins are used on one of my BorderManager 3.7 servers, with no BorderManager patches installed.

```
BorderManager 3.7 / NetWare 6.0
 Volume in drive O is SYS
 Volume Serial Number is C0A8-0A03

 Directory of O:\PUBLIC\win32\snapins

04/15/2002  06:10 PM    <DIR>          .
04/15/2002  06:10 PM    <DIR>          ..
06/01/1999  10:20 AM           225,280 ACNWAUTH.DL_
05/31/1999  10:47 PM           192,000 ADMSNAP.DLL
05/19/1999  04:45 PM            85,504 ALERT.DLL
03/02/2000  09:09 AM            11,776 audit32.dll
09/15/1999  10:19 AM           119,296 BSCOV.DLL
09/14/1999  12:07 PM           803,328 BSMON.DLL
06/10/1998  09:13 AM           174,592 MANAGEIP.DLL
02/08/2000  09:27 AM           153,600 NCSSnap.dll
08/02/2000  06:26 AM           561,152 NLSMGR32.DLL
06/02/1998  06:33 PM            71,680 NWCADM32.DLL
11/04/1998  08:48 AM            78,848 NWSLPSI.DLL
05/31/1999  10:44 PM           304,128 RADSNAP.DLL
12/11/1999  08:49 AM           195,072 REGEDT32.DLL
10/24/2001  12:42 PM           343,552 RESTRICT.DLL
04/16/2002  01:26 AM    <DIR>          Ini
              14 File(s)      3,319,808 bytes
               3 Dir(s)   2,949,763,072 bytes free
```

You should note that I have **renamed ACNWAUTH.DLL** so that it will not run. It sometimes causes NWADMN32 to GPF on loading, and I don't use that snapin, so I disabled it. That snapin is for ActivCard authentication objects).

BorderManager 3.6 / NetWare 5.1

The following snapins are used on one of my BorderManager 3.6 servers, with BorderManager 3.6 Service Pack 1 and the BM36C01 patch installed. I had also previously installed the PXY027.EXE patch (which contains an updated RESTRICT.DLL).

```
BorderManager 3.6 / NetWare 5.1
Volume in drive J is SYS
 Volume Serial Number is C0A8-0AFC

 Directory of J:\PUBLIC\WIN32\SNAPINS

03/13/2001  04:57 PM    <DIR>          .
03/13/2001  04:57 PM    <DIR>          ..
05/31/1999  10:47 PM           192,000 ADMSNAP.DLL
06/01/1999  10:20 AM           225,280 ACNWAUTH.DL_
08/02/2000  01:26 PM           561,152 NLSMGR32.DLL
05/31/1999  10:44 PM           304,128 RADSNAP.DLL
05/19/1999  04:45 PM            85,504 ALERT.DLL
09/15/1999  10:19 AM           119,296 BSCOV.DLL
09/14/1999  12:07 PM           803,328 BSMON.DLL
06/02/1998  06:33 PM            71,680 NWCADM32.DLL
03/02/2000  04:09 PM            11,776 audit32.dll
11/16/1999  05:34 PM            30,720 DBBACKUP.DLL
06/10/1998  04:13 PM           174,592 MANAGEIP.DLL
08/31/1999  11:08 AM             7,168 EPSNAPIN.DLL
09/18/1998  06:55 PM            78,848 NWSLPSI.DLL
07/12/1999  01:33 PM            28,672 NWIEASST.DLL
12/11/1999  03:49 PM           195,072 REGEDT32.DLL
11/16/1999  05:34 PM            31,232 REPORT~1.DLL
05/27/1999  03:42 PM            48,128 RXLGN.DLL
06/29/2000  11:03 AM           405,504 NDPSW32.DLL
02/18/1999  02:40 PM           447,488 PKISNAP.DLL
10/24/2001  12:42 PM           343,552 restrict.dll
03/31/2001  11:13 PM    <DIR>          MISC
03/13/2001  04:58 PM    <DIR>          Ini
03/18/2001  05:25 PM    <DIR>          95Only
03/18/2001  05:25 PM    <DIR>          NTOnly
              20 File(s)      4,165,120 bytes
               6 Dir(s)   1,240,924,160 bytes free
```

You should note that I have **renamed ACNWAUTH.DLL** so that it will not run. It sometime causes my NWADMN32 to GPF on loading, and I don't use that snapin, so I disabled it. That snapin is for ActivCard authentication objects).

There are some other DLL files besides BorderManager snapins present in my example. The snapins should be the same as for BorderManager 3.7.

BorderManager 3.5 / NetWare 5.0

The following snapins are used on one of my BorderManager 3.5 servers, with BorderManager 3.5 Service Pack 1 and the BM35C09 patch installed.

```
BorderManager 3.5 / NetWare 5.0
Volume in drive K is SYS
Directory of K:\public\WIN32\SNAPINS
.              <DIR>                          .
..             <DIR>                          ..
AUDIT32  DLL        11,776  03-02-00  4:09p AUDIT32.DLL
RADSNAP  DLL       304,128  05-31-99 10:44p RADSNAP.DLL
ALERT    DLL        85,504  05-19-99  4:45p ALERT.DLL
RESTRICT DLL       343,040  09-15-99 10:41a RESTRICT.DLL
NWCADM32 DLL        71,680  06-02-98  6:33p NWCADM32.DLL
BSMON    DLL       803,328  09-14-99 12:07p BSMON.DLL
PKISNAP  DLL       447,488  02-18-99  2:40p PKISNAP.DLL
ADMSNAP  DLL       192,000  05-31-99 10:47p ADMSNAP.DLL
NLSMGR32 DLL       556,544  02-29-00  5:17p NLSMGR32.DLL
ACNWAUTH DL_       225,280  06-01-99 10:20a ACNWAUTH.DL_
BSCOV    DLL       119,296  09-15-99 10:19a BSCOV.DLL
INI            <DIR>        06-25-00 11:37a Ini
95ONLY         <DIR>        06-25-00 11:48a 95ONLY
NTONLY         <DIR>        06-25-00 11:48a NTONLY
12 file(s)      3,160,064 bytes
5 dir(s)  3,261,267,968 bytes free
```

You should note that I have **renamed ACNWAUTH.DLL** so that it will not run. It sometimes causes my NWADMN32 to GPF on loading, and I don't use that snapin, so I disabled it. That snapin is for ActivCard authentication objects).

BorderManager 3.0 / NetWare 4.11

The following snapins are used on my BorderManager 3.0 server with the BorderManager 3.0 Service Pack 2 installed, and the BM3PC17 patch.

```
Volume in drive I is SYS
Directory of I:\PUBLIC\WIN32\SNAPINS
.              <DIR>                          .
..             <DIR>                          ..
NLSMGR32 DLL       556,544  02-29-00  5:17p NLSMGR32.DLL
ALERT    DLL        76,288  10-12-98  2:24p ALERT.DLL
BSCOV    DLL       117,760  11-23-99  3:51p BSCOV.DLL
RESTRICT DLL       342,016  12-03-99  1:29p RESTRICT.DLL
NWCADM32 DLL        71,680  06-02-98  6:33p NWCADM32.DLL
BSMON    DLL       803,328  11-23-99  4:05p BSMON.DLL
AUDIT32  DLL        11,776  03-02-00  4:09p AUDIT32.DLL
PKISNAP  DLL       447,488  02-18-99  2:40p PKISNAP.DLL
ADMSNAP  DLL       192,000  05-31-99 10:47p ADMSNAP.DLL
INI            <DIR>        07-19-00  8:59a INI
10 file(s)      2,618,880 bytes
3 dir(s)     232,718,336 bytes free
```

Chapter 4 – Understanding Packet Filtering

Note Packet filtering is explained in detail in the book "Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions", by Craig Johnson, and available from Craig's web site at http://www.craigjconsulting.com. A few sections of that book have been taken out and used in this book.

Packet filtering is critical to the operation of a BorderManager server when being used as a firewall. You MUST enable at least TCP/IP packet filtering support in order to have a secure server. Packet filtering consists of two parts – packet filters and exceptions. Both packet filters and exceptions are configured by default if you do a complete BorderManager installation, or if you manually run BRDCFG.NLM once.

Default packet filters block all packets that are not allowed by exceptions, but the whole "filtering" action includes filters and exceptions. The default packet filters are few and simple; they block all traffic to and from the public interface.

Filter exceptions always override the packet filters. BorderManager versions prior to 3.7 had a standard set of default exceptions, but BorderManager 3.7 and 3.8 can have a completely different set of defaults. In addition, BorderManager 3.7/3.8 reads IP filtering information from NDS, while previous versions read filtering information from files in the SYS:\ETC directory. **There are very significant ramifications to how BorderManager handles filtering in version 3.7 and later!**

The default packet filter exceptions are put in place to allow the proxies (mostly), the IP Gateway and the VPN services to operate. Without at least some exceptions, the BorderManager server would not be functional as a firewall.

Default Packet Filters

The default packet filters basically block all traffic between the public interface and all private interfaces (in both directions), as well as all traffic from the Internet to the public interface. (Packet filter exceptions then allow selected traffic to the public IP address). Packet filters are set up to block routing updates as well as TCP and UDP traffic. The default packet filters do not block traffic to or from the private interface(s) - except from private to public interface. By cutting off traffic between the public and private interfaces, BorderManager controls both incoming and outgoing traffic.

The BorderManager 3.x Default Packet Filters

The following is a list of all of the default packet **filters** (not exceptions) set up by BRDCFG.NLM for BorderManager 3.x. Should you see additional packet filters using FILTCFG.NLM, you may have accidentally used BRDCFG.NLM twice - once on the public interface and once on the private interface. (You would need to delete the incorrect entries to get BorderManager to function). These packet filter definitions are based on the example configuration shown earlier in this book in the complex, multiple server scenario number 8. IP Network 192.168.99.0 is the virtual IP network assigned for the VPN. The name of the interface connected to the Internet side of the BorderManager server is PUBLIC. No AppleTalk protocol was enabled on the BorderManager server, or some packet filters pertaining to AppleTalk would also have shown up.

Outgoing RIP Filters:

- Filtered Route: Route to Network or Host: Network, IP address of Network/Host: 0.0.0.0, Subnetwork mask: 0.0.0.0, Do Not Advertise Route To: Destination Type: Interface, Destination: VPTUNNEL
- Filtered Route: Route to Network or Host: Network, IP address 192.168.99.0, Subnetwork mask: 255.255.255.0, Do Not Advertise Route To: Destination type: Interface, Destination: <All Interfaces>
- Filtered Route: Route to Network or Host: Network, IP address of Network/Host: 4.0.0.0, Subnetwork mask: 255.0.0.0, Do Not Advertise Route To: Destination type: Interface, Destination: VPTUNNEL
- Filtered Route: Route to Network or Host: Network, IP address of Network/Host: 4.3.2.0, Subnetwork mask: 255.255.255.0, Do

Not Advertise Route To: Destination type: Interface, Destination: VPTUNNEL

Incoming RIP Filters

- Filtered Route: Route to Network or Host: All Routes, IP address of Network/Host: <blank>, Subnetwork mask: <blank>, Do Not Accept Route From: Source Type: Interface, Source: PUBLIC

Outgoing EGP Filters:

- Filtered Route: Route to Network or Host: All Routes, IP address of Network/Host: <blank>, Subnetwork mask: <blank>, Do Not Advertise Route To: Destination Type: Interface, Destination: PUBLIC

Incoming EGP Filters

- Filtered Route: Route to Network or Host: All Routes, IP address of Network/Host: <blank>, Subnetwork mask: <blank>, Do Not Accept Route From: Source Type: Interface, Source: PUBLIC

OSPF External Route Filters

- Routes denied: All Routes

Packet Forwarding Filters

- Source Interface Type: Interface, Source Interface: <All interfaces>, Destination Interface Type: Interface, Destination Interface: PUBLIC (Public), Packet Type: <ANY>, Protocol: IP. Src Addr Type: Any Address, Dest Addr Type: Any Address
- Source Interface Type: Interface, Source Interface: PUBLIC (Public), Destination Interface Type: Interface, Destination Interface: <All Interfaces>, Packet Type: <ANY>, Protocol: IP. Src Addr Type: Any Address, Dest Addr Type: Any Address

Packet Filter Exceptions

What are the Default Packet Filter Exceptions?

BorderManager 3.0, 3.5 and 3.6

Note The default packet filter exceptions allow all outbound traffic from proxies, and some inbound traffic. However, the default packet filter exceptions do not allow certain types of inbound traffic to some of the proxies, such as inbound SMTP, NNTP or almost any special traffic for a Generic TCP or UDP Proxy. In addition, no default packet filter exception allows any inbound or outbound traffic for secondary IP addresses. You must manually add packet filter exceptions for all of these situations as needed.

BorderManager 3.0, 3.5, and 3.6 should have the following default packet filter exceptions, designed to allow the proxy services and VPN to function. These are the packet forwarding filter exceptions as shown in FILTCFG.

1. Allow all outbound IP packets from the BorderManager public IP address to the public interface.
2. Allow all inbound TCP packets with the destination port in the range 1024-65535 from the public interface to the public IP address of the BorderManager server.

Note There is an important distinction to be made here between the public interface and the public IP address. **All of the default exceptions specify the public IP address rather than the interface.** This is a necessary distinction as calling out the interface instead of the public IP address results in allowing undesired traffic. It also means that the default packet filter exceptions do not cover any secondary IP addresses that you might add to the public interface. Also, because a source or destination IP address is specified in the filter exception, it is not necessary to specify the interface.

---

3. Allow all inbound UDP packets with the destination port in the range 1024-65535 from the public interface to the public IP address of the BorderManager server.
4. Allow all inbound TCP packets with the destination port 213 from the public interface to the public IP address of the BorderManager server in order to allow VPN client-server communications.

5. Allow all inbound TCP packets with the destination port 353 from the public interface to the public IP address of the BorderManager server in order to allow VPN client authentication to the server.
6. Allow all inbound UDP packets with the destination port UDP 353 from the public interface to the public IP address of the BorderManager server in order to allow VPN client to send periodic keep-alive packets to the server.
7. Allow the SKIP protocol (protocol 57) from the public interface to the public IP address of the BorderManager server. The SKIP protocol is necessary for Novell VPN to function.
8. Allow all inbound TCP packets with the destination port 80 (HTTP) traffic from the public interface to the BorderManager public IP address in order for the web server accelerator to function.
9. Allow all inbound TCP packets with the destination port 443 (HTTPS/SSL) traffic from the public interface to the BorderManager public IP address in order for proxy authentication to a reverse web proxy accelerator to function.

Note The default packet filters cover both IPX and IP traffic, though this book is exclusively concerned with IP packet filters and exceptions. The default packet filters should not be blocking ANY traffic to or from the private interface, so if enabling packet filters causes communications problems, it may indicate that the packet filters were applied incorrectly with BRDCFG.NLM, and need to be redone, especially if IPX communications have been affected. However, there are some issues with certain types of IP communications to NetWare 5.x servers trying to go to the public IP address instead of the private IP address. In this case, the following command may be needed: SET NCP INCLUDE IP ADDRESSES = x.x.x.x. You will have the option to INCLUDE an NCP address in Monitor, Server Parameters, NCP. It is better to simply include only the private IP address of the server there, since that will automatically exclude all public addresses AND the VPN tunnel address.

BorderManager 3.7

BorderManager 3.7 differs greatly from previous versions in how the filtering is managed, and in what default filters are installed.

Note BorderManager 3.7 Service Pack 2 contains a new version of BRDCFG.NLM that builds different default exceptions from either a fresh installation of 3.7 or the version of BRDCFG that shipped with 3.7. The newer version of BRDCFG also automatically puts the new exceptions into NDS, meaning that you do not have to perform a FILTSRV MIGRATE procedure.

The first time you start BorderManager 3.7, you need to migrate filtering information into NDS with the FILTSRV MIGRATE procedure (described elsewhere in this book). You will have to unload FILTSRV first to do that, and you will have to unload other filtering modules in order to unload FILTSRV.

If you upgrade an older BorderManager server in-place to BorderManager 3.7, your old exceptions will be used.

If you install BorderManager 3.7 without a previous version of BorderManager in place, and without any packet filters or exceptions having been set up, you will have stateful filter exceptions designed for outbound communications for the proxies, plus some (incomplete) filter exceptions for VPN connections. All of the following filter exceptions have the following characteristics:

- a source IP address equal to the public IP address of the server
- a destination IP address equal to any address
- a source interface equal to the public interface name
- a destination interface equal to All interfaces
- stateful filtering is enabled

The BorderManager 3.7 default filter exceptions allowing outbound communications are:

- DNS/TCP-ST – TCP destination port 53, for DNS queries by the proxies
- DNS/UDP-ST – UDP destination port 53, for DNS queries by the proxies
- FTP-PORT-PASV-ST – FTP control and data ports 20 and 21 – for FTP connections from the proxies
- NTTP-ST – (a misspelling of NNTP) , TCP destination port 119 – for NNTP communications from the News Proxy

- POP3-ST – TCP destination port 110, for POP3 retrieval by the Mail Proxy
- REALAUDIO-ST – TCP destination port 7070, for RealAudio connections by the RealAudio & RTSP Proxy
- RTSP-ST – TCP destination port 554, for RTSP connections by the RealAudio & RTSP Proxy
- SMTP-ST – TCP destination port 25, for sending SMTP mail from the Mail Proxy. (This exception does not allow for inbound SMTP mail TO the Mail Proxy)
- TELNET-ST – TCP destination port 23, for TELNET connections from the Transparent Telnet Proxy.
- WWW-HTTP-ST – TCP destination port 80, for HTTP connections from the HTTP and Transparent HTTP Proxy
- WWW-HTTPS-ST – TCP destination port 443, for SSL (HTTPS) connections from the HTTP Proxy

The following inbound filter exceptions are also created by default on BorderManager 3.7 servers:

- VPN-AuthGW – TCP destination port 353, for Client-to-Site VPN authentications communications
- VPN-KeepAlive – UDP destination port 353, for Client-to-Site VPN keep-alive communications
- VPN-SKIP – Protocol 57, for VPN key exchange.

CAUTION *None of these VPN exceptions make allowance for the fact that the BorderManager 3.7 does not allow all outbound IP from the public IP address by default, and as such there is not a way for the return packets necessary to create a connection to exit the server. You must manually configure such exceptions. There is also no provision in the default exceptions for inbound or outbound traffic on UDP 2010, required for Client-to-Site VPN over NAT connections.*

Note The version of BRDCFG shipped in the BM37SP2 (BorderManager 3.7 Service Pack 2) patch creates an entirely different set of filter exceptions that do contain particular exceptions, which will allow VPN services to function. Versions shipped in later patches have additional changes.

BRDCFG.NLM is not used to create exceptions during a fresh install of BorderManager 3.7. The filter exceptions which are created for the proxies (during installation of BorderManager 3.7) are far more specific than the previous BorderManager versions' default exceptions, and are also more secure. But you must know how filtering works in detail if you want to allow additional proxies beyond what was selected in the initial installation. If you run

BRDCFG manually after installing BorderManager 3.7, then you will have different filter exceptions than if you simply let the BorderManager 3.7 installation configure your filters.

A full discussion of BorderManager 3.7 filtering is out of the scope of this book, but is covered thoroughly in the book "Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions", available at http://www.craigjconsulting.com.

BorderManager 3.8

BorderManager 3.8 differs greatly from previous versions in how the filtering is managed, and in what default filters are installed. It also differs substantially even from BorderManager 3.7.

If you upgrade an older BorderManager server in-place, your old exceptions will be used. You must manually migrate them into NDS using the FILTSRV MIGRATE command.

If you install BorderManager 3.8 without a previous version of BorderManager in place, and without any packet filters or exceptions having been set up, you will have filter exceptions based on the proxies you selected during the installation. See the example earlier in this book showing filter exceptions in the iManager screen following a BorderManager installation on NetWare 6.0.

The following exceptions should be in place if you selected all of the proxies during the BorderManager installation.

10. AH-st – Two instances, one for inbound and one for outbound traffic. Used for VPN.
11. ESP-st - Two instances, one for inbound and one for outbound traffic. Used for VPN.
12. IKE-NAT-st - Two instances, one for inbound and one for outbound traffic. Used for VPN.
13. IKE-st - Two instances, one for inbound and one for outbound traffic. Used for VPN.
14. ipx/tcp-st - Two instances, one for inbound and one for outbound traffic. Used for Legacy VPN.
15. pop3-st - Two instances, one for inbound and one for outbound traffic. Used for Mail Proxy.
16. smtp-st - Two instances, one for inbound and one for outbound traffic. Used for Mail Proxy.
17. VPN-AuthGW-ST - Two instances, one for inbound and one for outbound traffic. Used for Legacy VPN.
18. VPN-KeepAlive-st - Two instances, one for inbound and one for outbound traffic. Used for Legacy VPN.

19. VPN-SKIP-st - Two instances, one for inbound and one for outbound traffic. Used for Legacy VPN.
20. VPTUNNEL-st - Two instances, one for inbound and one for outbound traffic. Used for Legacy VPN .
21. dns/tcp-st – Outbound only. Used for proxy DNS queries.
22. dns/udp-st – Outbound only. Used for proxy DNS queries.
23. ftp-port-pasv-st – Outbound only. Used for FTP proxy.
24. nntp-st – Outbound only. Used for News proxy.
25. realaudio-st – Outbound only. Used for RealAudio/RTSP Proxy.
26. rtsp-st – Outbound only. Used for RealAudio/RTSP Proxy.
27. telnet-st – Outbound only. Used for Transparent Telnet Proxy.
28. www-http-st – Outbound only. Used for HTTP Proxy to access web sites using port 80.
29. www-https-st – Outbound only. Used for HTTP Proxy to access web sites using port 443.

Note The default packet filters cover both IPX and IP traffic, though this book only discusses IP packet filters and exceptions. The default packet filters should not be blocking ANY traffic to or from the private interface, so if enabling packet filters causes communications problems, it may indicate that the packet filters were applied incorrectly with BRDCFG.NLM, and need to be redone, especially if IPX communications have been affected. However, there are some issues with certain types of IP communications to NetWare 5.x/6.x servers trying to go to the public IP address instead of the private IP address. In this case, the following command may be needed: SET NCP INCLUDE IP ADDRESSES = x.x.x.x. You will have the option to INCLUDE an NCP address in Monitor, Server Parameters, NCP. It is better to simply include only the private IP address of the server there, since that will automatically exclude all public addresses AND the VPN tunnel address.

This book is not really intended to cover filtering. For much more information on understanding packet filtering, see my book "*Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions*", at http://www.craigjconsulting.com.

These are the DEFAULT filters and exceptions. They do NOT include exceptions necessary for any inbound traffic besides VPN or Mail Proxy, so if you add a generic proxy or reverse proxy after the installation routine, you will have to manually add filter exceptions to allow the packets to get to the proxies.

The astute reader may also notice that the default exceptions will not allow the HTTP Proxy to browse to web sites that use ports other than 80 or 443.

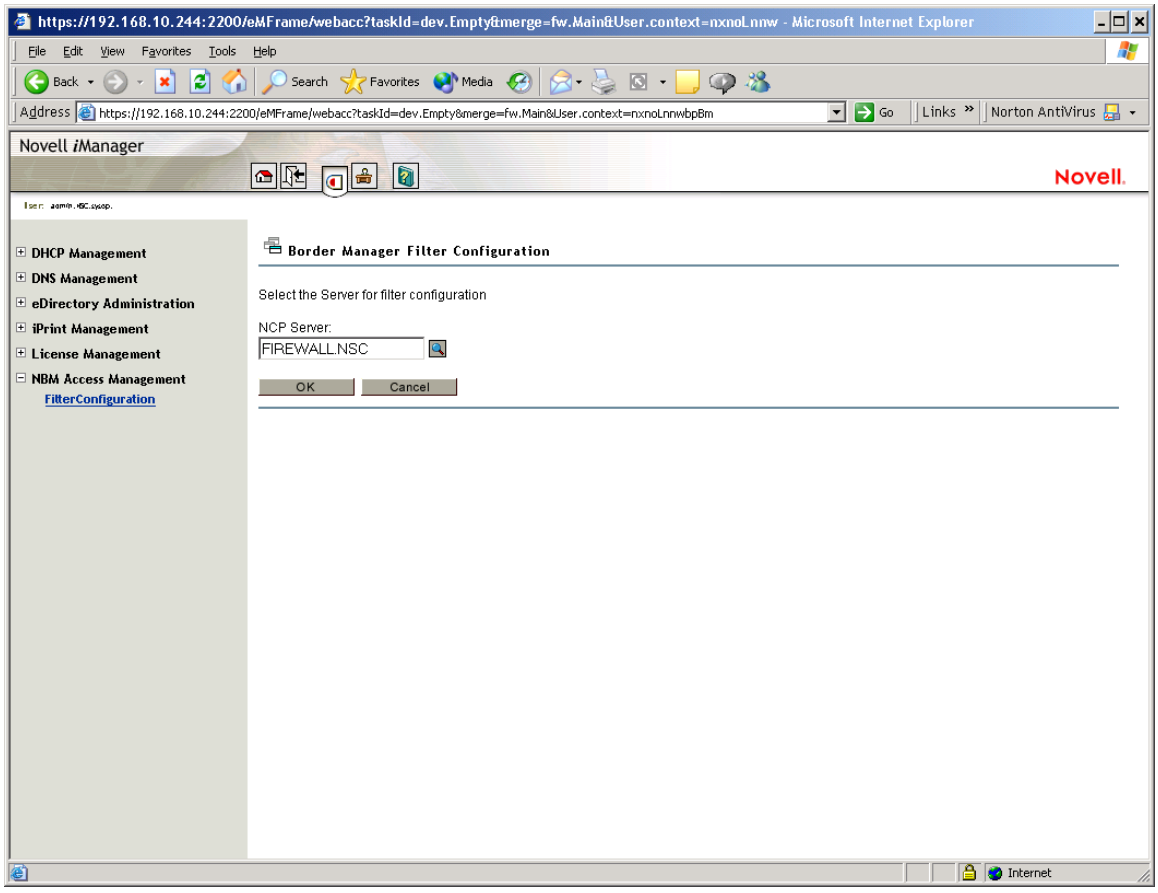
Using iManager to View Filtering Information

Note The following example is for iManager 1.5 running on a NetWare 6.0 server and with BorderManager 3.7 installed. I still recommend using FILTCFG, as I think it is faster and easier to use, plus it automatically copies filtering information to the FILTERS.CFG file as well as NDS.

Start iManager by pointing a browser (Internet Explorer is the only browser likely to work correctly) to your BorderManager server private IP address as follows. This example assumes the server's IP address is 192.168.10.244.

https://192.168.10.244:2200

You should see an option for iManager. Select it, and you should have a login window. Log in to the NDS tree.

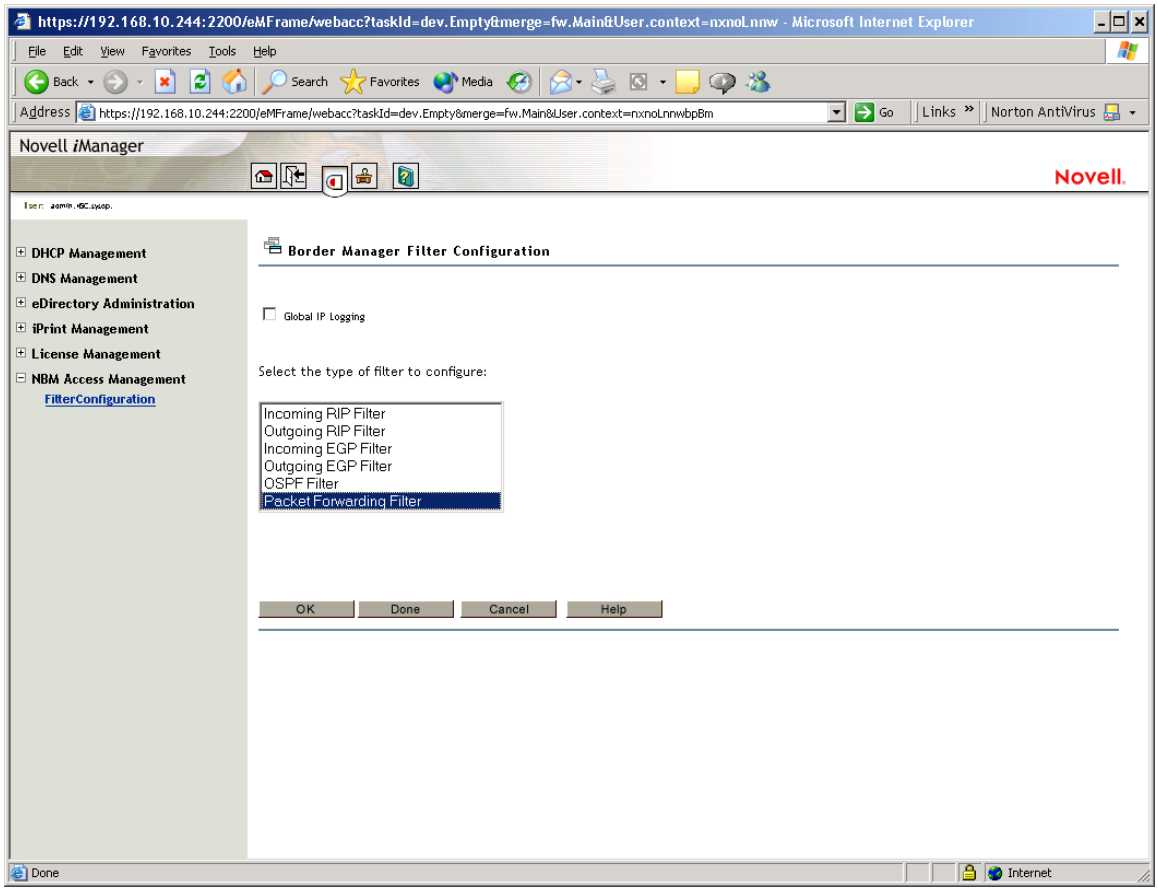


If the proper emFrame Java plugin files were successfully installed when BorderManager was installed, you should have an option in

iManager on the left side called **NBM Access Management**, with an link below it called **FilterConfiguration**.

Select **NBM Access Management**, and then **FilterConfiguration**.

Browse to the BorderManager 3.7 server, in the NCP Server option. Then select **OK**.



Selecting the BorderManager server, and the FilterConfiguration link within NBM Access Management will present you with a list of filtering operations. All of these options have to do with IP filtering only. IPX and Appletalk filtering options (rarely used) remain administered by FILTCFG.NLM.

Note This book does not cover packet filtering in any great detail. Packet filtering can be a complex subject, and is covered thoroughly in my book "Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions". The Third Edition of that book covers how iManager and filtering work.

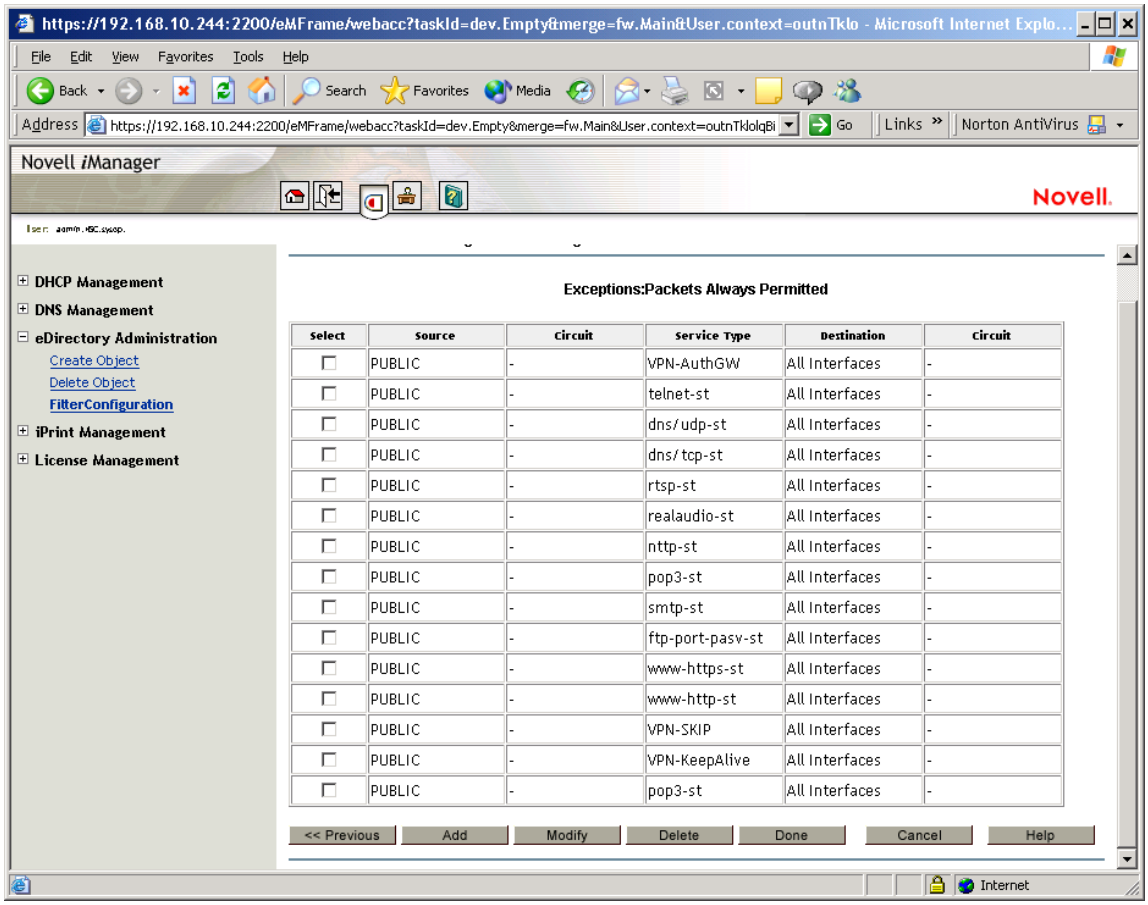
The filter exceptions you see will depend on whether or not you upgraded a previous version of BorderManager. If you do a fresh install of BorderManager 3.7, you will be prompted to select the proxies you wish to use, and some specific stateful exceptions will be created based on those choices. If you are upgrading over a previous version of BorderManager, your old filter exceptions should remain in place. In each case, the FILTSRV MIGRATE

procedure described earlier must have succeeded in order for the filters and exceptions to appear in iManager.

The filter exceptions created will allow outbound communication from the selected proxies. You will need to add some custom exceptions if any proxy is set up to use a secondary IP address or if static NAT is involved. If you are familiar with using FILTCFG, I recommend continuing to use it.

In iManager, if you want to add your own custom filter exceptions, you define new packet filter types in the Configure Service Type menu. You can then select those definitions when you configure a packet forwarding filter. Packet forwarding filters are where you add new exceptions, and, as of this writing, the whole procedure is a graphical version of the steps used in FILTCFG.

Selecting **Configure Packet Forwarding Filter** brings you to the menu above, where you can enter a new filter exception by selecting Exception List.



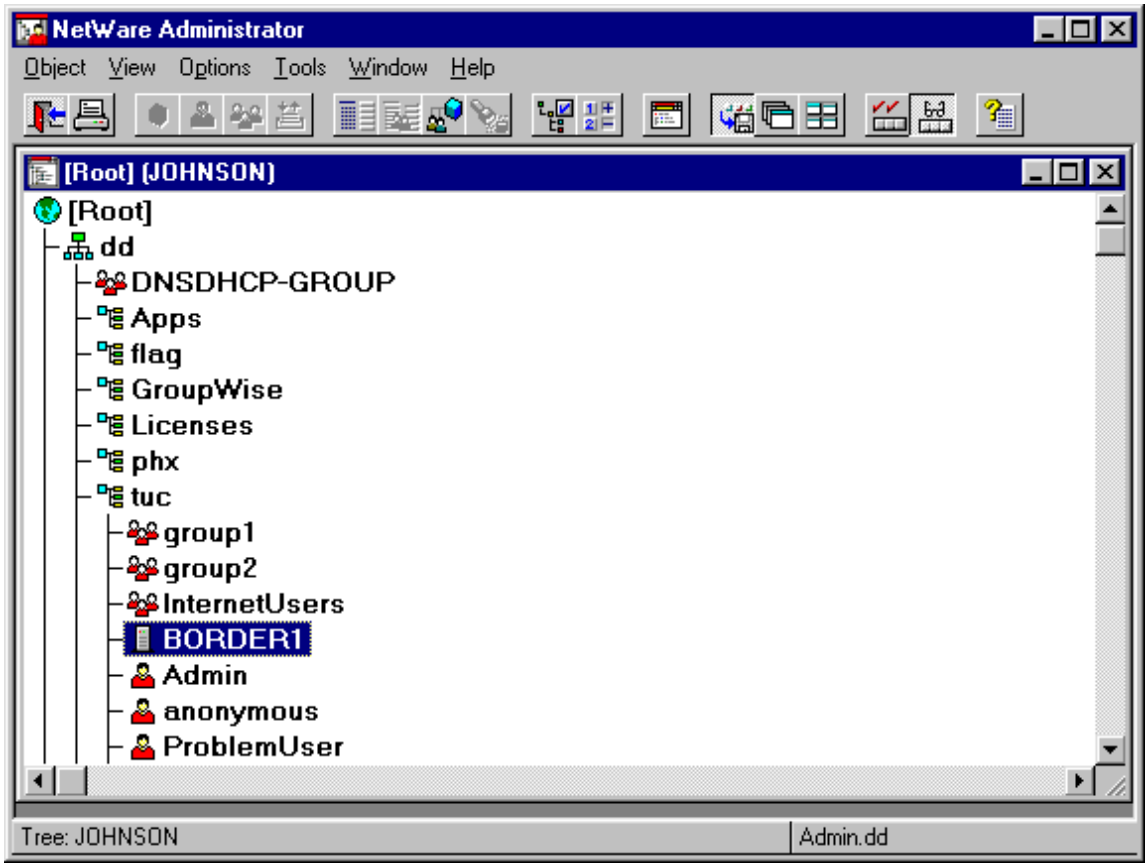
Once you select **Exception List**, you should see a list of all the current IP filter exceptions. You can select individual exceptions in order to edit or delete them.

The screenshot above shows the exceptions that resulted from selecting all of the proxies when doing a fresh install of BorderManager 3.7 on a NetWare 6.0 server.

<This page intentionally left blank. This is to facilitate putting in chapter tabs in a ring binder for double-sided printing. The main chapters should start on an odd-numbered page.>

Chapter 5 – The Initial Configuration

Almost all BorderManager administration and configuration is done in NWADMN32. You must open NWADMN32 and browse to the **BorderManager server object** to begin. The examples in this book are (mostly) taken from the test servers in my LAN. Double-click on the **BorderManager server** object to set BorderManager configuration options.



The very **first** time you configure the BorderManager server (on a NetWare 4.x server), you may be asked to specify how your default access rule is to function. You should choose the **Deny** option, so that all access not specifically permitted by an access rule is denied. This configuration option should be done within the BorderManager installation process on a NetWare 5.x / 6.x server. (The NetWare GUI installation for BorderManager will ask you for certain details

and make the changes for you. However, should the installation process fail before the java code writes the changes to NDS, you may end up with a BorderManager system that needs to be configured in NWADMN32 just like NetWare 4.11 – this includes BorderManager 3.8 on NetWare 6.5.)

In order to configure BorderManager 3.x parameters, you must use the NWADMN32.EXE program located in the BorderManager server's SYS:\PUBLIC\WIN32 directory. Otherwise you may not have the proper snapins needed to work with the BorderManager NDS attributes. The BorderManager snapins are installed on the BorderManager server when BorderManager is installed, and can be reinstalled or updated by running the SYS:\PUBLIC\BRDRMGR\SNAPINS\SETUP.EXE program.

If you want to run NWADMN32 from a non-BorderManager server and still manage BorderManager, you need to install the snapins to the other server. Running the SETUP.EXE program in the BorderManager SYS:\PUBLIC\BRDRMGR\SNAPINS directory will allow you to easily copy the snapins to any server where you have mapped a drive. However, you must still manually update the snapins with any patch versions, and you must already have NWADMN32 installed in the SYS:\PUBLIC\WIN32 directory.

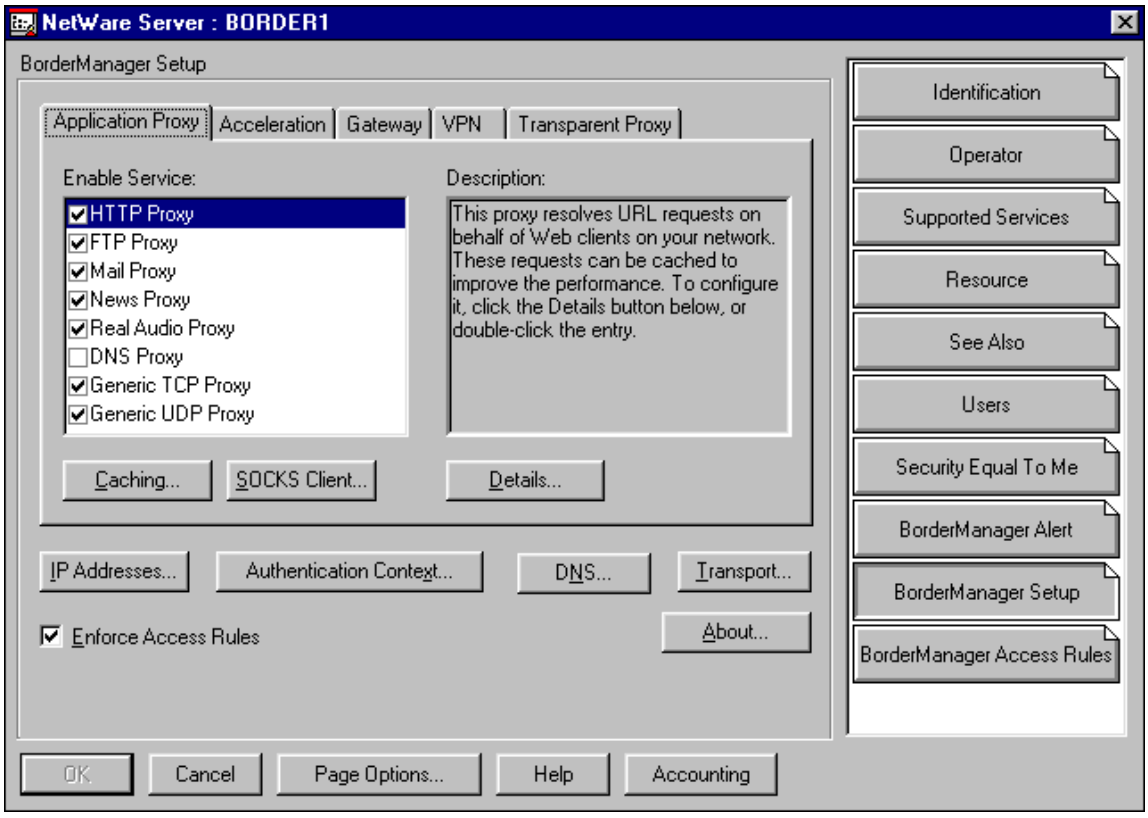
Some BorderManager patches update the snapin files by updating the files under the SYS:\PUBLIC\BRDRMGR\SNAPINS directory. In order to apply these updated snapins, you must run the SYS:\PUBLIC\BRDRMGR\SNAPINS\SETUP.EXE program once for each server needing updated versions of the snapin files.

If you have launched NWADMN32 from a server that contains the BorderManager snapins, you should see three BorderManager-related tabs on the right side of the screen – BorderManager Alerts, BorderManager Setup and BorderManager Access Rules.

Note If you have problems getting NWADMN32.EXE to launch, try renaming the SYS:\PUBLIC\WIN32\SNAPINS\ACNWAUTH.DLL file to something else so that it will not load. This file is used for configuring ActivCard parameters, but often causes NWADMN32 to crash. Refer to the Troubleshooting section at the end of this book if you have other problems getting NWADMN32 to work with BorderManager.

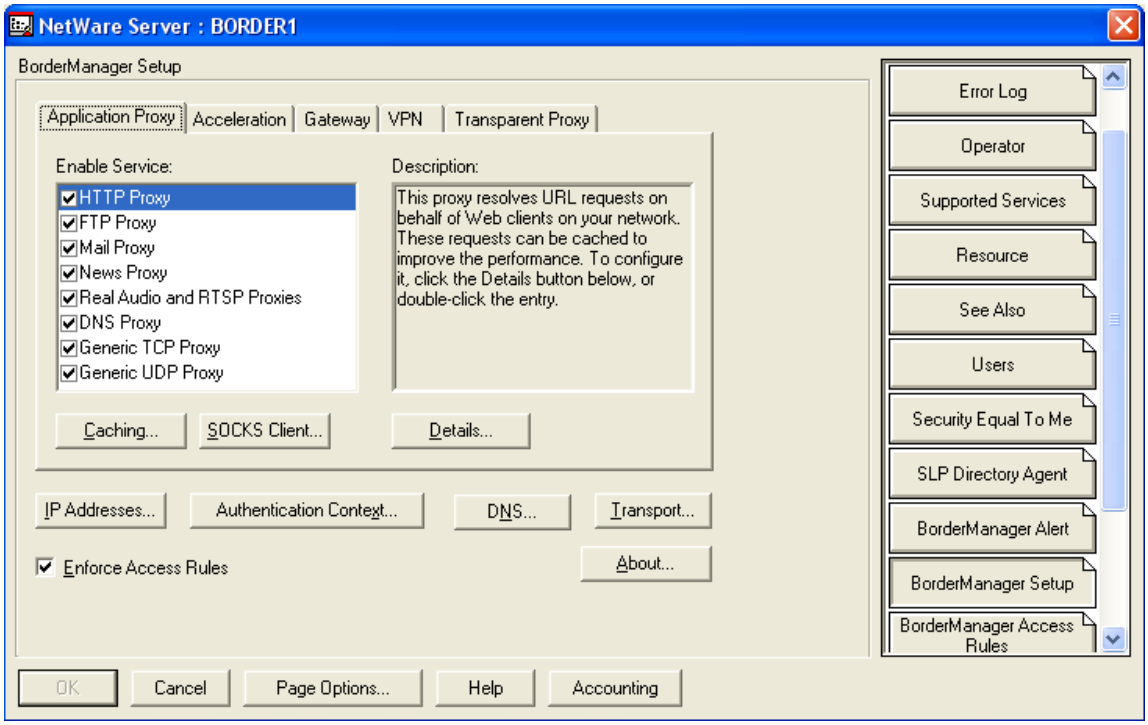
BorderManager Setup Main Menu

Many parts of this book will refer to the BorderManager Setup main menu, shown below.



BorderManager 3.0 Setup main menu page for BORDER1

Note that the Real Audio Proxy in BorderManager 3.0 does not include an RTSP Proxy.



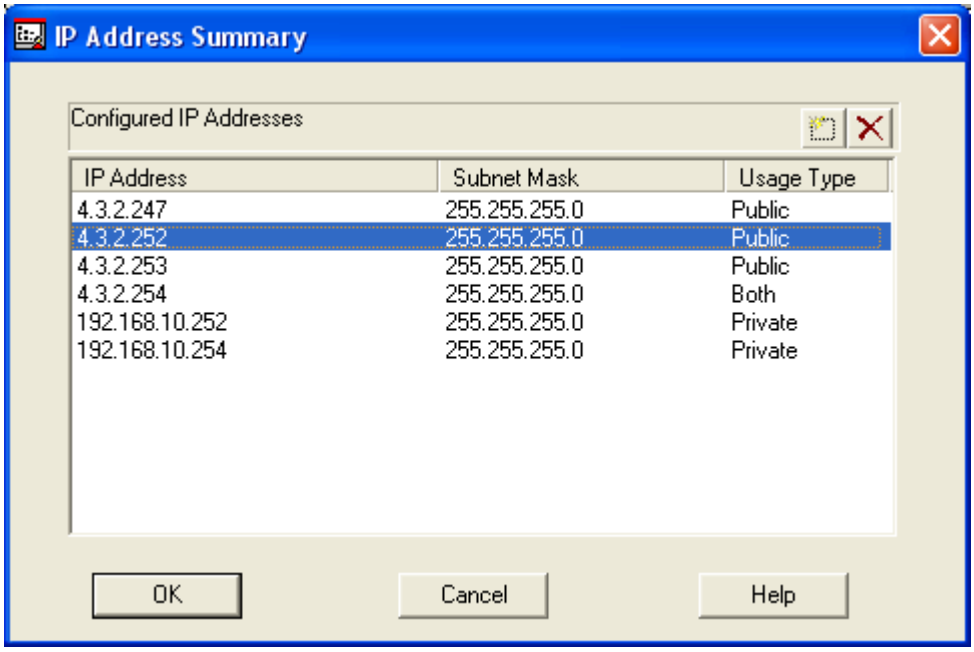
BorderManager 3.5, 3.6, 3.7 or 3.8 Setup main menu

The only difference between a BorderManager 3.0 server and later versions that can be seen from the main menu is that later versions show a Real Audio and RTSP Proxies entry instead of a Real Audio Proxy.

BorderManager IP Address Configuration

A number of BorderManager menu options in NWADMN32 will present you with a choice of IP addresses. The addresses presented to you are only available if you first define them as available for BorderManager.

The BorderManager installation routine (on NetWare 4.11 servers) will not define any IP addresses, nor define them as public or private for you.



From the BorderManager Setup main menu, select **IP Addresses**, and configure a public and a private IP address from those addresses set up on BORDER1. (Including any secondary IP addresses, if present, for reverse proxy or other proxy).

In the example shown:

- 4.3.2.254 is the primary public IP address for BORDER1
- 192.168.10.252 is the primary private IP address for BORDER1
- 192.168.10.254 is a secondary private IP address for BORDER1
- The 4.3.2.253, 4.3.2.252, and 4.3.2.247 addresses are all secondary IP addresses assigned to BORDER1 and used for one proxy or another.

Note There could be additional secondary public IP addresses configured on the BorderManager server that **do not** show up in this NWADMN32 menu. Adding a secondary IP address to the server is done with the ADD SECONDARY IPADDRESS command. Addresses used for static NAT do not require configuration in the BorderManager IP Address summary menu. However, if a secondary IP address were to be used for one of the proxies, it would have to be entered in the BorderManager IP Address Summary menu in order to configure that proxy. In the example above, there is no 4.3.2.251 IP address shown in the screenshot, but that IP address happens to be set up on the server and is used with static NAT, to bypass the BorderManager proxies for certain types of inbound traffic.

If you set a public IP address to be both Public and Private, it means that certain proxies will listen for traffic on that IP address when they would not have done so otherwise. For instance, the HTTP Proxy will listen for HTTP (TCP destination port 80) traffic on any IP address designated as Private, and you can then access the HTTP Proxy from either side of the firewall, a situation which can be useful when using BorderManager in a lab setting. Other proxies make no use of the Public or Private designation. Reverse proxy acceleration does expect you to designate a Public IP address so that the IP address will show up on a list of addresses to choose from when configuring that proxy.

In summary:

- Most proxies only listen on addresses flagged as private.
- The generic proxies can listen on addresses flagged private or public. They can be used for either outbound or inbound connections.
- An address that is flagged as both public and private can be used by any proxy. This can allow people on the Internet to relay traffic from your server, so be certain you know what you are doing.
- You can see what ports are being monitored on what IP addresses by looking at the BorderManager server console, Proxy Console screen, option 17. From this information, you can deduce which proxies are listening, and where.

Press **OK** to save the address settings on BORDER1. Press **OK** to save all settings on BORDER1. **You must first complete the addressing of BorderManager before you can continue configuring other parameters**.

Secondary IP addresses used on BORDER1

The following addresses are assigned as secondary IP addresses in some of my examples. Not all of them have been defined in NWADMN32. If using a secondary IP address for static NAT, you do not define it in NWADMN32. If using a secondary IP address for a reverse proxy or a generic proxy, you define it in NWADMN32.

- 192.168.10.254 is a secondary private IP address on BORDER1 that is used as the default gateway and proxy IP address for internal hosts. The reason for using a secondary private IP address is that it allows you to easily switch from one BorderManager server to another, for clustering, upgrading the server, or simply replacing the server with another one for an afternoon while patching the main server.
- 4.3.2.253 is a secondary public IP address on BORDER1 used for reverse proxy to an internal web server.
- 4.3.2.252 is a secondary IP address on BORDER1 used for a reverse proxy to another internal web server.
- 4.3.2.251 is a secondary public IP address on BORDER1 used to static NAT to an internal SMTP/POP3 mail server for certain tests. *Note that this IP address does **not** show up as a configured IP address in NWADMN32 because it was not defined as a BorderManager public or private IP address.* **You should not use a secondary IP address for both Static NAT and proxy at the same time.**
- 4.3.2.247 is a secondary public IP address on BORDER1 used for a Generic TCP proxy designed to pass port 12345 traffic through to the Remote Web Manager service on a NetWare 5.1 server.

Note When a secondary IP address is defined in the BorderManager IP addresses in NWADMN32, they will be automatically added when PROXY.NLM is loaded on the server. This has ramifications when transferring IP addresses from one server to another.

Authentication Context (Proxy Authentication)

Concept

Proxy Authentication exists for a single reason – to provide a means to make Access Rules work that call out an NDS user, group or container. When a request is made to the HTTP Proxy, (also FTP Proxy, and Transparent Proxies), the server has no idea what user ID sent the packets to the server. The only identity information that is contained in the packet is a source IP address. Proxy authentication is a method whereby the source IP address of the packet is related to an NDS user name.

There are two methods of proxy authentication. Both accomplish the exact same thing, but with different methods. CLNTRUST and SSL Proxy Authentication are the methods – relating the source IP address of a proxy request packet to a user name is the result.

Configuration

Select **Authentication Context** from the BorderManager Setup main menu to configure proxy authentication.

Be sure to review the chapter on Access Rules to see examples of how Proxy Authentication is used with proxy services to control access.

Proxy Authentication is used to authenticate TCP/IP traffic to NDS objects (associate the source of TCP/IP traffic to an NDS user name).

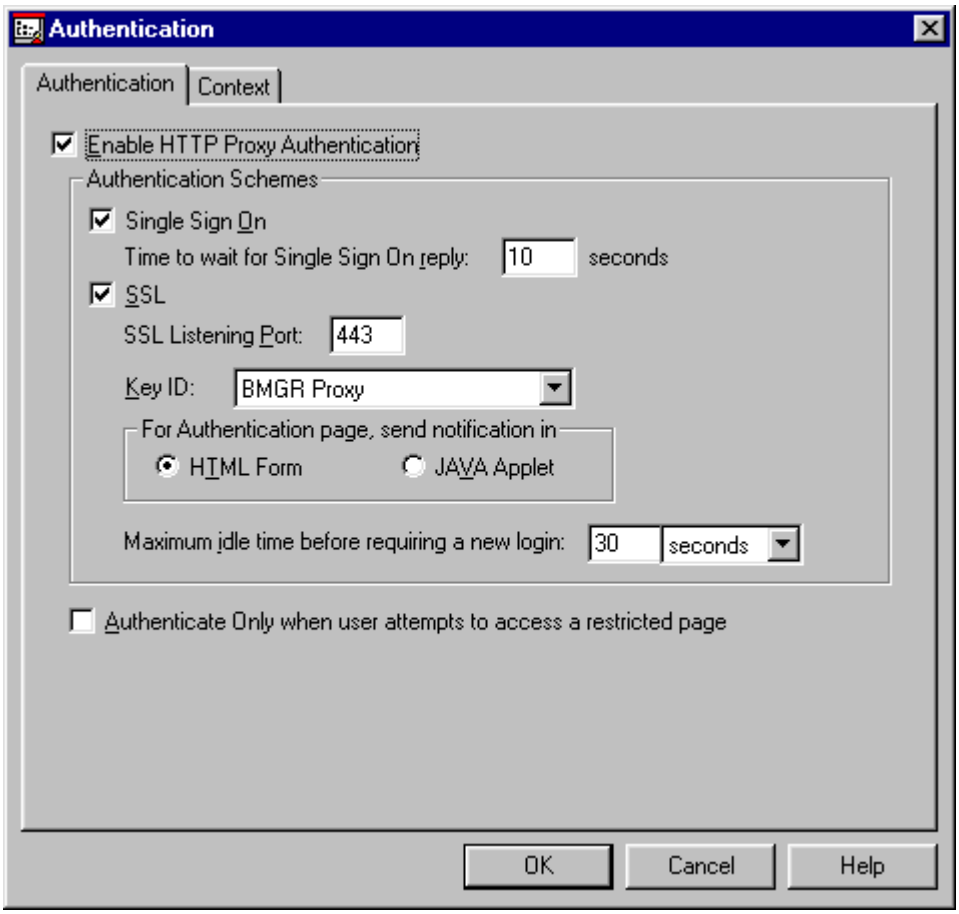
Proxy Authentication allows access control based on NDS objects (users, groups or containers) to be set up, and it allows logging of traffic by NDS user name.

If proxy authentication is enabled, users must be logged into the same NDS tree as your BorderManager server and be running the CLNTRUST program (normally loaded from a login script) or using the web browser-based SSL proxy authentication method.

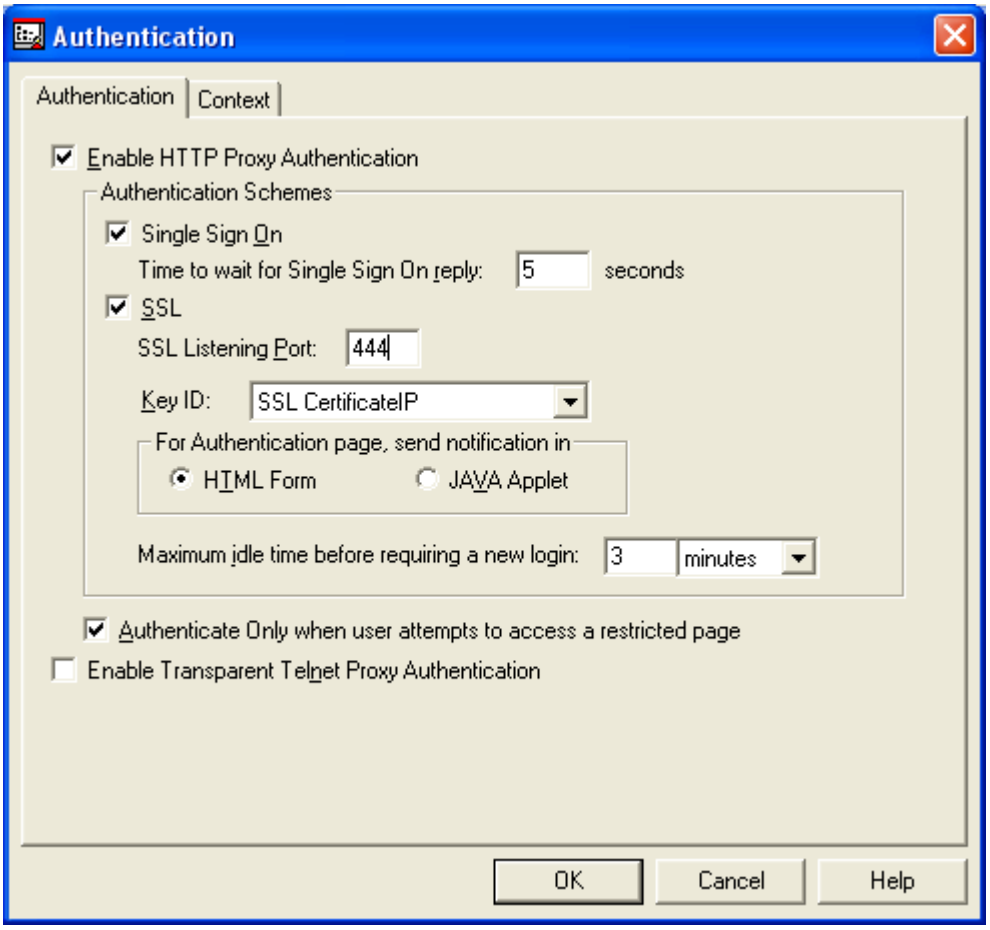
It is important to know that if a workstation does not proxy authenticate (CLNTRUST not running, not using SSL Proxy Authentication, or authentication simply fails), access rules based on NDS users, groups or containers will be ignored.

Note NDS-based rules can also be used with the FTP Proxy and TELNET Proxies. But the username/password has to be passed to these proxies in different ways. Also, the CLNTRUST utility has not worked with FTP Proxy in BorderManager 3.5 with patch sets up through at least BM35C11.EXE. It does work with much later patch sets, in 3.5 and later versions of BorderManager.

Proxy Authentication Settings



The example above shows a BorderManager 3.0 Authentication Context screen. There is no entry for Transparent Telnet Proxy Authentication.



The example above shows a BorderManager 3.5, 3.6, 3.7 or 3.8 Authentication Context menu. Note that there is an additional entry for Transparent TELNET Proxy Authentication, as compared to BorderManager 3.0.

Select **Authentication Context** from the BorderManager Setup main menu screen.

Enabling **Single Sign On** proxy authentication will allow users to authenticate to NDS using their normal NDS user ID and password. (This happens with no user interaction if CLNTRUST is running on the PC).

SSL authentication is enabled, and the port number has been changed from the default value of 443 to 444. The port number set here is pushed to the browser as part of SSL Proxy Authentication, and can be set to whatever port is desired.

Note The reason that the port number was changed from the default value of 443 is to show that you can change the value. On some servers, particularly NetWare 6.5, there may be other services loaded that already bind to port 443, resulting in a port conflict when BorderManager PROXY loads. Changing the SSL port to 444 here resolves the conflict.

If **SSL** authentication is enabled, you must also create a security Key Material Object in NDS, assigned to the BorderManager server, and associate that key to proxy authentication. You can use the default NetWare 5.x/6.x SSL CertificateIP certificates for this purpose. In addition, you should set up one or more default containers for the authentication context or the users will have to type in the fully distinguished NDS username during SSL authentication. (CLNTRUST is transparent to the user and is much faster, but it only works with Client32, and thus is available only to Windows clients).

There are examples later in this book, in the chapter on Access Rules, on how to set up Key Material Objects.

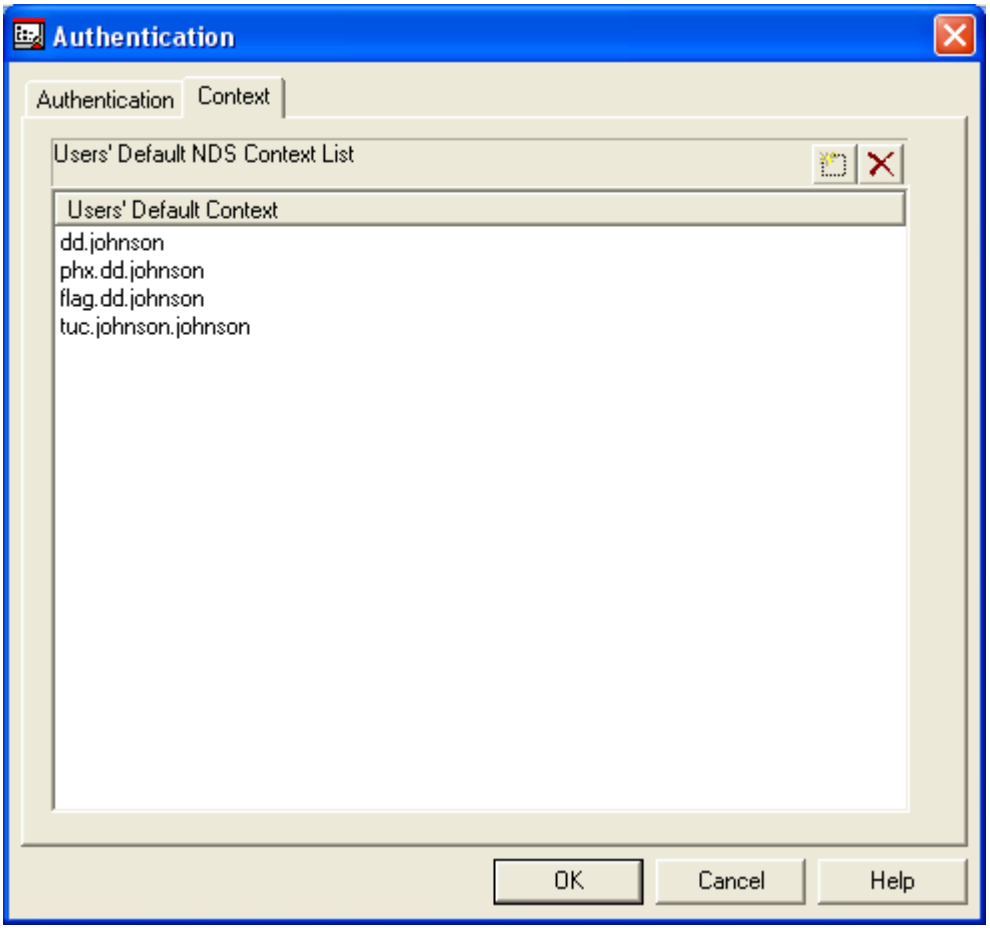
Note SSO, (or SSoN), is popularly thought of as meaning to use the CLNTRUST utility. However, both CLNTRUST and SSL authentication both make use of SSO. SSO stands for Single-Sign On, and SSO really means that the same user ID and password as the users normal login account are used for proxy authentication. This was not always the case. BorderManager 2.1 used a separate password tied to the user account, and that led to a lot of administrative burden. CLNTRUST and SSL are simply different ways to pass the user ID and password to the BorderManager server. CLNTRUST does not actually send the password across the wire, but makes use of Client32 RSA security features. SSL does send the password across the wire, but encrypts it. Unfortunately, the User ID and password for the FTP Proxy and Transparent TELNET Proxy are sent across the wire in clear text, and the FTP Proxy does not make use of the CLNTRUST utility, at least in BorderManager 3.6 patch sets up through BM36C01.EXE. Another point: Single Sign On in BorderManager is not the same as the Novell Single Sign On or Secure Login product.

Authenticate Only when user attempts to access a restricted page is of particular importance here. Do not enable this without a good reason to do so. This option is intended to invoke selective Proxy Authentication only when you have a Deny (or Allow) access rule calling out an NDS object for a source. The practical effect comes about when using SSL Proxy Authentication and you would like users to only have to go through the HTML/Java login process when accessing certain sites. For example, if there is an access rule with source="any" nobody will be required to authenticate to access that destination. The reader is urged to experiment with this setting before invoking permanently it so that the effects on the users are understood.

Refer to the example rules shown in the Selective Proxy Authentication Example section at the end of the Access Rules chapter for an example of using this option.

The way this option works is that, in effect, two passes through the Access Rules might be made. The first pass goes through looking for any rules that might apply to only the IP address of the source. (Actually, any non-NDS-based rule definition). If a rule is found that matches, then the rule is invoked. However, if a matching rule is not found, then a second pass through the rule list is made, checking for NDS-based rules. At the time of the second pass, NDS authentication may be invoked if some allow rule based on NDS user, group or container is found. This could result in SSL Proxy Authentication being invoked and popping up a login screen on a browser. So this option can be set up such that certain URL's are allowed without anyone having to proxy authenticate, but then later forcing an authentication for other web sites.

Select the **Context** tab to set the default context(s) for proxy authentication.



In the example shown, all the contexts containing user objects have been entered into the default context list in order to ease SSL login. As long as the user's context has been entered in the NDS Context List, the user will only need to put in the user ID to log in for Proxy Authentication, instead of having to put in the fully-qualified NDS name + NDS tree.

If user names are not unique throughout the NDS tree, the first name encountered will be assumed by proxy authentication if a fully-qualified NDS name is not entered by the user. A drop-down box should be available to select the context for the user name from those entered in NWADMN32.

40-bit, 56-bit and 128-bit Encryption

Note Since about 2002, Novell produces only Null (no encryption) and Domestic (128-bit) encryption versions of TCPIP.NLM. The old Export version is no longer needed since the United States relaxed requirements on exporting cryptographic products. All BorderManager 3.7 and 3.8 servers should capable of 128-bit encryption for both SSL Proxy Authentication and VPN. All earlier versions of BorderManager can be patched to 128-bit capability. Two versions of 128-bit TCPIP modules are available: NICI (Domestic) and Domestic. (Domestic) NICI is always required for BorderManager 3.8 VPN. Domestic is required for earlier BorderManager versions, *except* when NW51SP7 or NW6SP4 patches have been installed.

Proxy Authentication relies on SSL encryption when CLNTRUST is not being used on the client side. However, **encryption is done by the browser,** and the server does NOT require an encrypted TCPIP stack. The TCP/IP stack encryption is only used for VPN operations. Nevertheless, there are other encryption-related components to BorderManager that might affect the encryption level that SSL Proxy Authentication

SSL encryption is available in USA Domestic and Canada 128-bit or Export 40-bit (56-bit later on) versions. The version to be used depends on a number of factors, including whether or not a 128-bit version of NetWare is installed, a 128-bit version of BorderManager is installed, 128-bit patches to both BorderManager and TCPIP.NLM and IPFLT.NLM have been installed and the browser being used.

Note 40-, 50-, and 128-bit encryption is different in the strength of the encryption process that is used. The practical meaning is that the higher the bit number, the harder it is to break the encryption by brute force attack.

Service packs have had a history of upgrading installed components, but reducing the encryption level to 40- or 56-bit. Upgrading those components to 128-bit has typically required the system administrator to contact Novell to get the 128-bit versions of certain NLM's. This situation has changed in recent years, but you might find older servers that are limited to weaker encryption levels.

Note As of this writing, a BorderManager server can be upgraded to 128-bit encryption by using a 128-bit version of TCPIP.NLM from the latest NetWare support pack, and installing the NICID157.EXE, or later, patch. If a VPN was originally configured without 128-bit encryption, it must be reconfigured (in VPNCFG) in order to upgrade to 128-bit encryption.

Not having 128-bit components has the practical effect of a) requiring a 40-bit Key Material Object to be configured for BorderManager Proxy Authentication and b) allowing use of 40-bit browsers at the client side.

Two Key Material Objects have been set up in the event a 128-bit TCPIP.NLM patch is available. You can select the appropriate key from a drop down list in the Proxy Authentication configuration screen:

Note At one time, a bug has been seen in the certificate creation process when using NetWare 5.1 certificate server. ConsoleOne is used to create certificates with the newer certificate server, and it appears to be unable to create an SSL certificate at less than the highest value of encryption capable by the host server. In other words, although you may try to create a 40-bit certificate on a 128-bit server, the certificate will still be 128-bit. I have seen this happen on some networks but not others, and as of this writing do not know the cause.

When the 40-bit TCPIP.NLM is being used, and a 128-bit key is enabled for Proxy Authentication, the SSL login system will not function.

Using Proxy Authentication on the Client with CLNTRUST

There are only two ways to get Proxy Authentication to work on the client side – CLNTRUST.EXE and SSL Login. CLNTRUST is designed to do all of the authentication work automatically so the user has to do nothing. CLNTRUST is a 'helper program' that works with Client32.

The CLNTRUST utility works only with 32-bit Windows running Client32 and logged into the same NDS tree as the BorderManager server.

CLNTRUST is normally launched from the login script, though it can be launched from a ZENworks application, or manually.

CLNTRUST is unloaded at the PC using the DWNTRUST.EXE program. In order to ensure that CLNTRUST loads cleanly, and to ensure that only one copy of CLNTRUST runs at any one time, you should launch DWNTRUST before launching CLNTRUST. The following syntax should be used in a login script to launch CLNTRUST. This syntax assumes that the F: drive is mapped to the SYS volume of a server holding copies of CLNTRUST and DWNTRUST in the SYS:\PUBLIC directory.

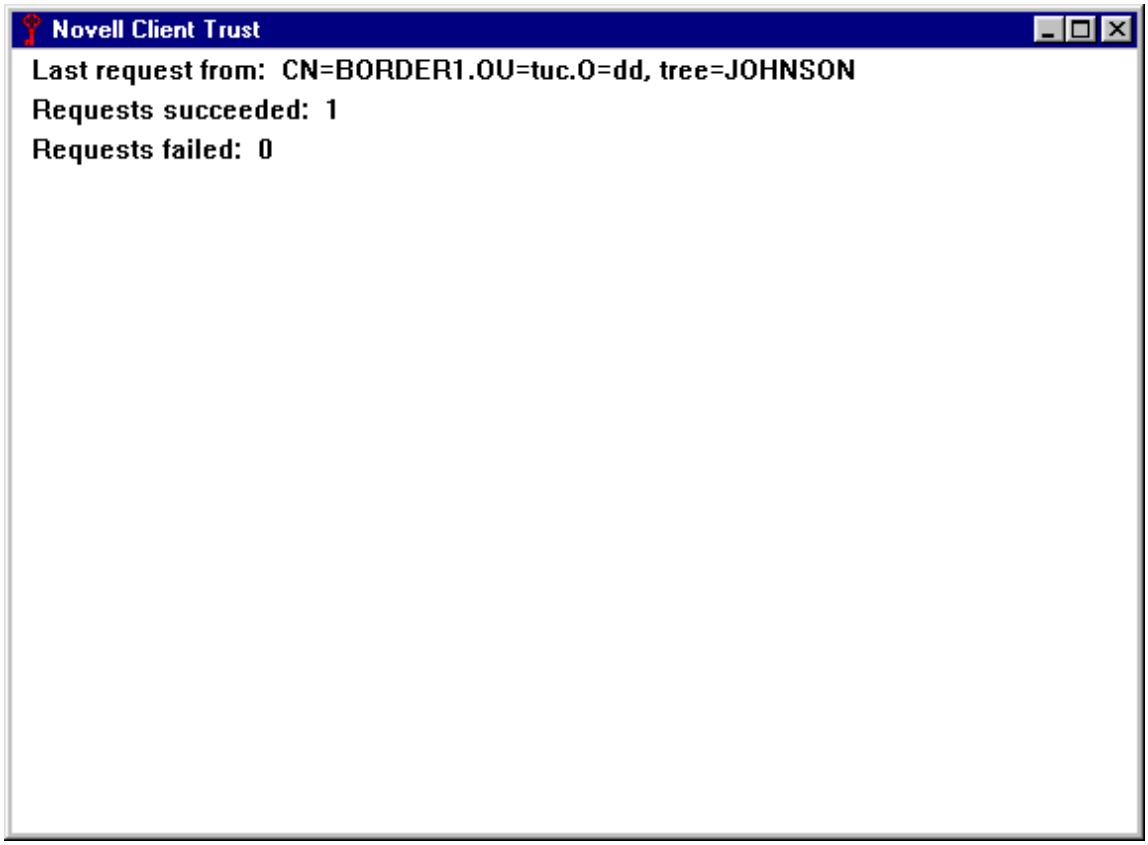
```
#F:\PUBLIC\DWNTRUST.EXE
#F:\PUBLIC\CLNTRUST.EXE
```

You do not have to launch CLNTRUST from the BorderManager server. You can even copy CLNTRUST to the local PC and launch it from there.

Because CLNTRUST is held open when a user launches it from a server, it can be a problem to upgrade to a newer version. You will find that CLNTRUST cannot be replaced or renamed if anyone is still using it. But you can use a trick – put CLNTRUST (and DWNTRUST) in a subdirectory called CLN under the SYS:PUBLIC directory on any server. Point to that location in the login script. Next, when you need to upgrade CLNTRUST to a new version, **rename the CLN directory** to something else, then create a new CLN directory and put the new CLNTRUST and DWNTRUST in there. When users log in again, they will start picking up the new version.

```
#F:\PUBLIC\CLN\DWNTRUST.EXE
#F:\PUBLIC\CLN\CLNTRUST.EXE
```

The example above shows how to launch CLNTRUST from a directory under PUBLIC called CLN.



Once CLNTRUST is running on the PC, you should see a small red key icon in the system tray. Double-click on that icon to see statistics on whether proxy authentication attempts are successful or unsuccessful.

Note If you should see many unsuccessful authentication requests (thousands), it may be that the user is not logged into the same NDS tree as the BorderManager server.

CLNTRUST Problem Work-Around

One problem that has been seen with CLNTRUST is a tendency to sometimes try to communicate with the BorderManager server's public IP address, which will fail because the default packet filters will block that traffic. The symptom would be a) authentication failing, and b) CLNTRUST showing many repeated unsuccessful authentication attempts. There are two solutions to this issue:

Set up a stateful packet filter exception as follows:

```
source interface=<private interface>,
destination interface=<public interface>
source ports=Any
destination port=524
protocol=TCP
destination IP address=<BorderManager server public IP address>
```

This will allow the necessary CLNTRUST traffic from the internal LAN only to get to the public IP address of the BorderManager server.

A better alternative: For NetWare 5.x or 6.x servers, prevent the public IP address from listening for NCP calls over IP. Use the following set statement, where xx.xx.xx.xx is the BorderManager server public IP address. The newer NetWare 5.x / 6.x NCPIP.NLM allows a SET parameter to be used to exclude or include advertisements on certain IP addresses. You may need to include all public secondary IP addresses defined.

```
SET NCP EXCLUDE IP ADDRESSES x.x.x.x
```

For the version in the service packs, use:

```
SET NCP EXCLUDE IP ADDRESSES = x.x.x.x
```

(that is, add the = sign.)

Or

```
SET NCP INCLUDE IP ADDRESSES x.x.x.x
```

(which may be better as you should be able to list only the internal, fixed, IP addresses) .

For the version in the service packs, use:

```
SET NCP INCLUDE IP ADDRESSES = x.x.x.x
```

(add the = sign.)

Once you get CLNTRUST working, your NDS-based access rules for the HTTP Proxy (and FTP and Transparent Proxy, and for IP Gateway) should all begin to be functional.

If you find that CLNTRUST is not working all the time, or if you need to refresh a web site to gain access the first time you browse, you may need to up the timeout value for SSO Proxy Authentication in NWADMN32, Authentication Context. The timeout value is the number of seconds allowed for the BorderManager server to wait for a response from CLNTRUST to a proxy authentication request. If you have a large network, you may need to increase the value, perhaps to as high as 10 seconds.

The downside of increasing the timeout value is for those users relying on SSL Proxy Authentication. They will not see an SSL login screen until the timeout value expires.

Configuring SSL Proxy Authentication

The alternative to using CLNTRUST is to use SSL Proxy Authentication. This method of relating a TCP/IP data stream to an NDS user ID involves using a Java- or HTML-based login screen on the browser to prompt the user to log in. SSL Proxy Authentication can be used for MAC's, UNIX hosts, PC's not running Client32, etc.

Whereas CLNTRUST uses RSA password authentication technology to authenticate a user in the background without sending a password over the wire, SSL Proxy Authentication must send the password to the BorderManager server. SSL encryption is used between the browser and the BorderManager server to encrypt the password. Once the login process is completed, encryption is stopped, and the user is redirected to the URL of interest.

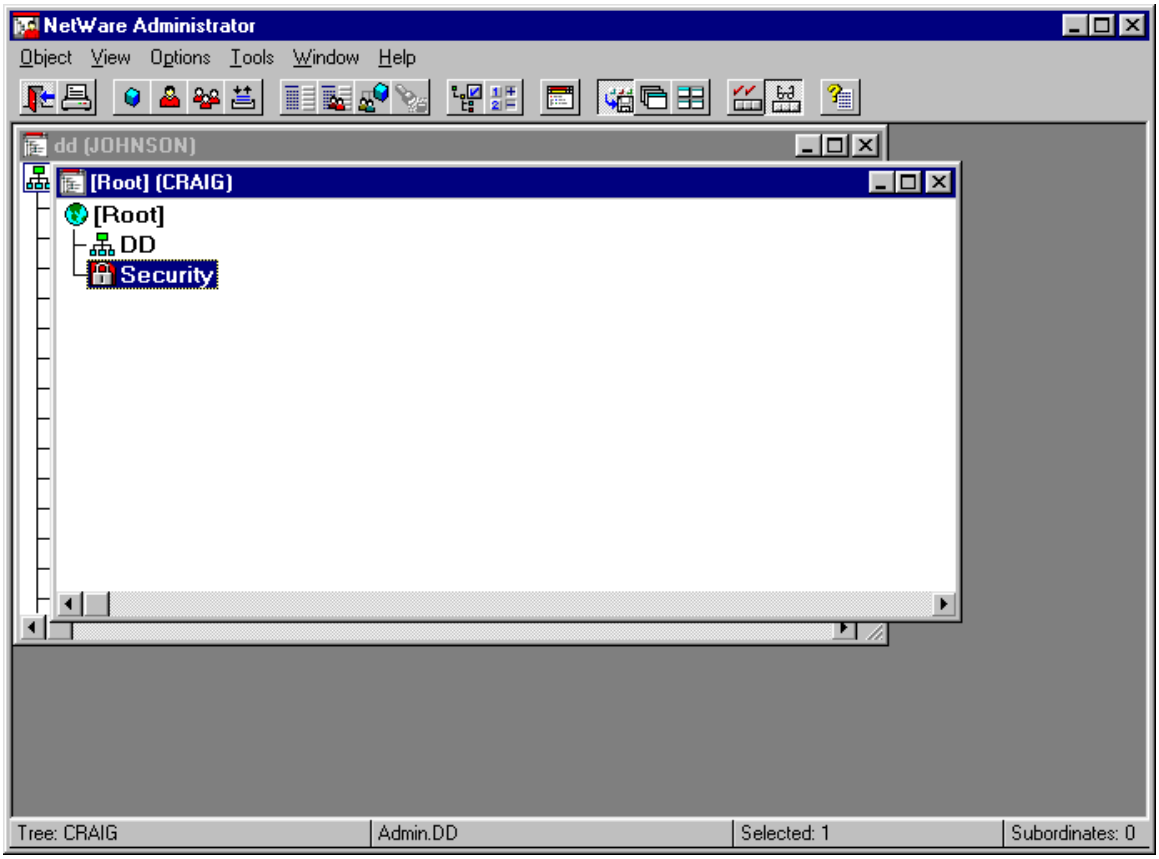
In both CLNTRUST and SSL Proxy Authentication methods, the authentication is good for a certain period of inactive time before another authentication request is generated. As long as the browser is active, the authentication will be maintained. The inactivity timeout period is configurable in NWADMN32.

In order for SSL Proxy Authentication to function, a certificate must be exchanged between the BorderManager server and the browser. The certificate requires that a Key Material Object be created in NDS and assigned on the BorderManager server. In order to create a Key Material Object, a Certificate Authority object must first be created in the NDS tree. The Certificate Authority is created inside a special Security container under the root of the tree, and only one Certificate Authority can be created (or more properly, be active) at one time.

If you must create all of these objects and the Security container for the first time, follow this procedure.

Creating a Security Container

The procedure shown below is for an NDS tree that has not had NetWare 5.1 or 6.x installed in the tree. This procedure uses NWADMN32. Once NetWare 5.1 is installed in the NDS tree, schema changes are put in place that are not supported with the NWADMN32 snapins.



If you have **not** installed a NetWare 5.1 server in your tree, and this is the first BorderManager server, you may have to create a **Security Container** and a **Certificate Authority**.

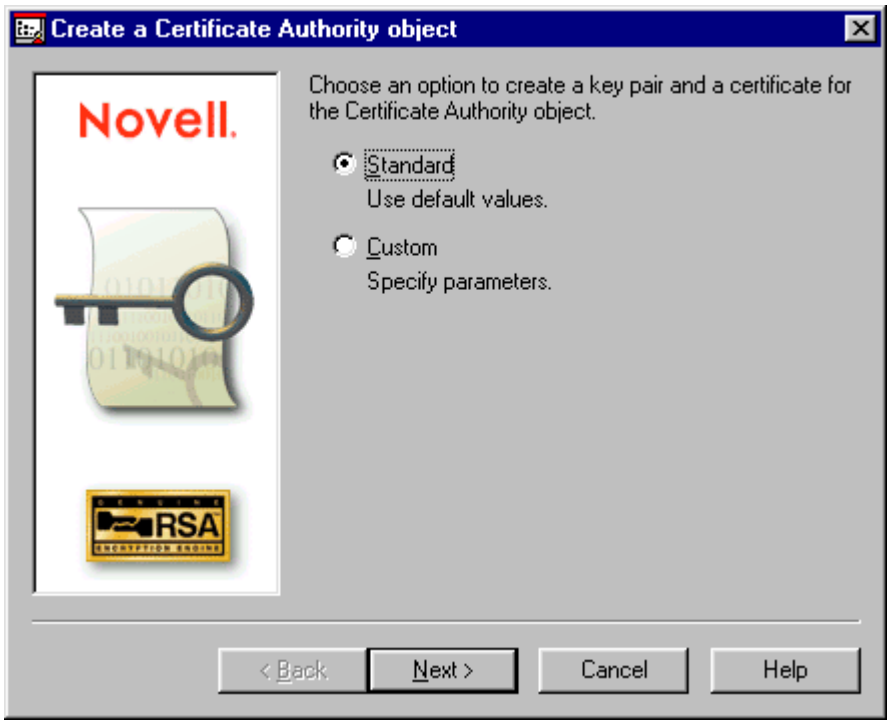
The BorderManager installation should create the Security container (under the Root of the NDS tree) for you, but if it did not, you can create it by loading SASI.NLM (on NetWare 5.0) at the BorderManager server console. For NetWare 5.1 and 6.0 servers, you can use PKIDIAG.NLM to create a new Security Container, and a Certificate Authority, or use ConsoleOne.

Creating a Certificate Authority, pre-NetWare 5.1

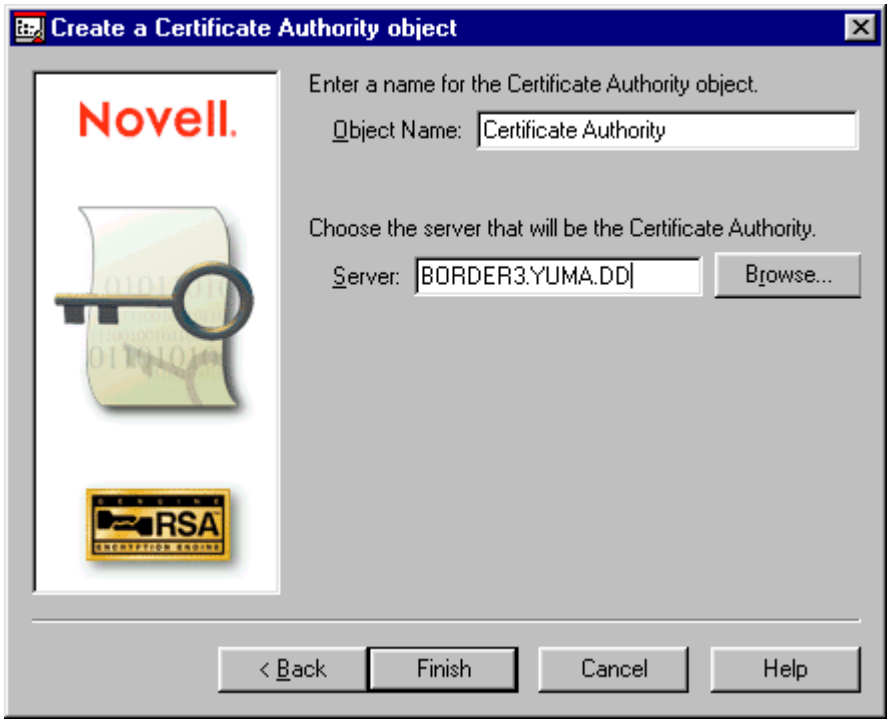
Installing the first NetWare 5.1 server creates a Certificate Authority using a newer version of security services than with NetWare 4.11 or NetWare 5.0. Follow these instructions if you have no Certificate Authority in your tree when you have just installed BorderManager 3.0, 3.5, 3.6 or 3.7.

With the Security container selected, press **Insert** to create a new object.

Select **Certificate Authority** and click **OK**.



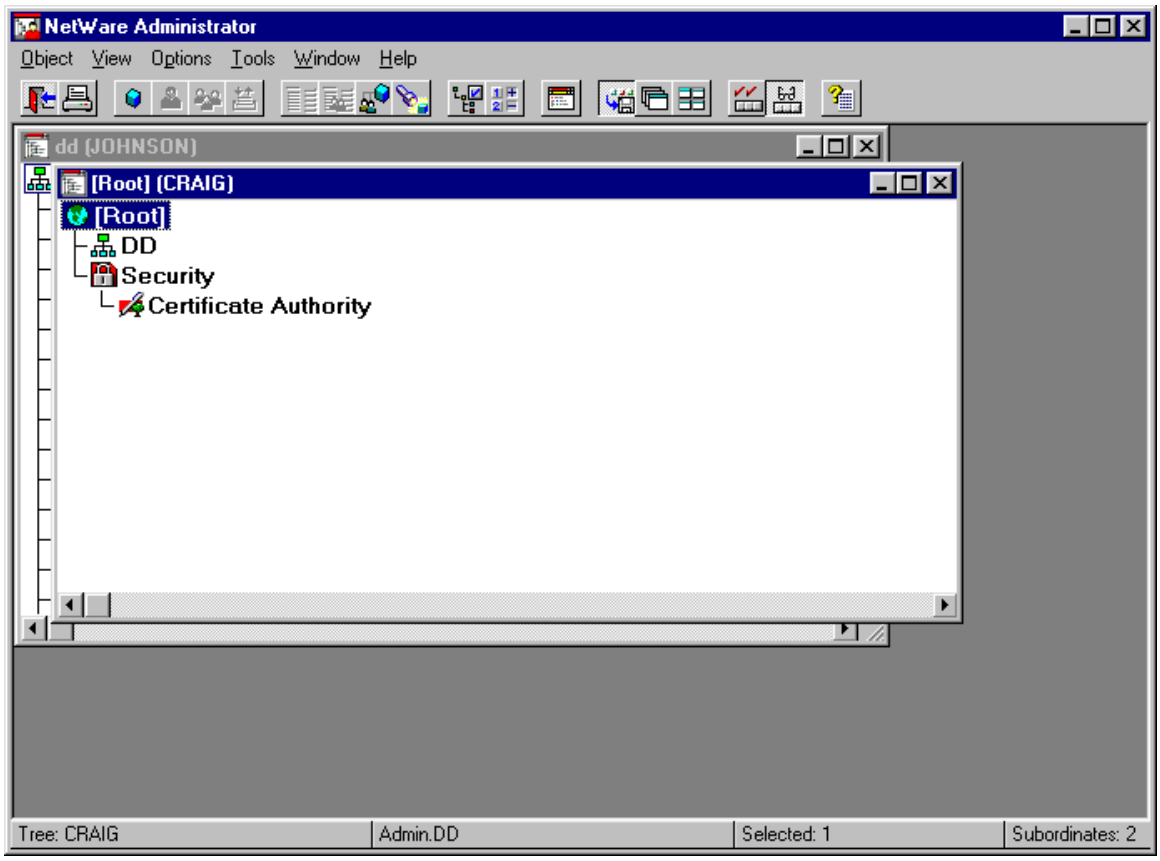
Choose **Standard**, and click on **Next**.



Fill in a descriptive object name, such as **Certificate Authority**.

Browse to the BorderManager server and select it to fill in the **Server** field. You must select a server that runs Novell's PKI software. Once you choose a server, the Certificate Authority is tied to that server and cannot be moved. You would have to delete the Certificate Authority object and recreate it on another server if you want to move the object.

Click on **Finish** to create the new Certificate Authority.



You should now have a **Certificate Authority** object in the NDS tree. You can then create **Key Material Objects**, based on the Certificate Authority.

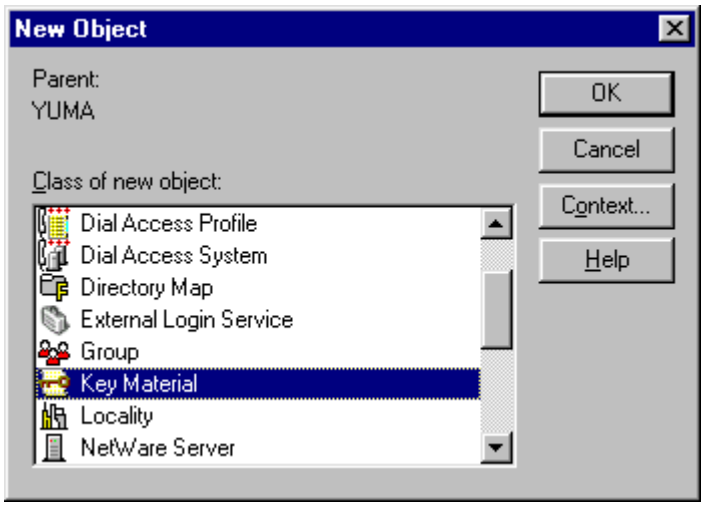
Creating a Certificate Authority, with NetWare 5.1 or 6.x

Simply installing the first NetWare 5.1 or 6.x server should result in a Security container being created, with a new Certificate Authority object created inside that container.

If you have already created a Certificate Authority in the NDS tree from BorderManager 3.0, 3.5 or 3.6 on NetWare 4.11, the NetWare 5.1 server installation will still create a new Certificate Authority object, and the old Certificate Authority object will no longer function. You will have to use ConsoleOne to recreate a Certificate Authority object or any Key Material Objects once a NetWare 5.1 server is installed in the NDS tree.

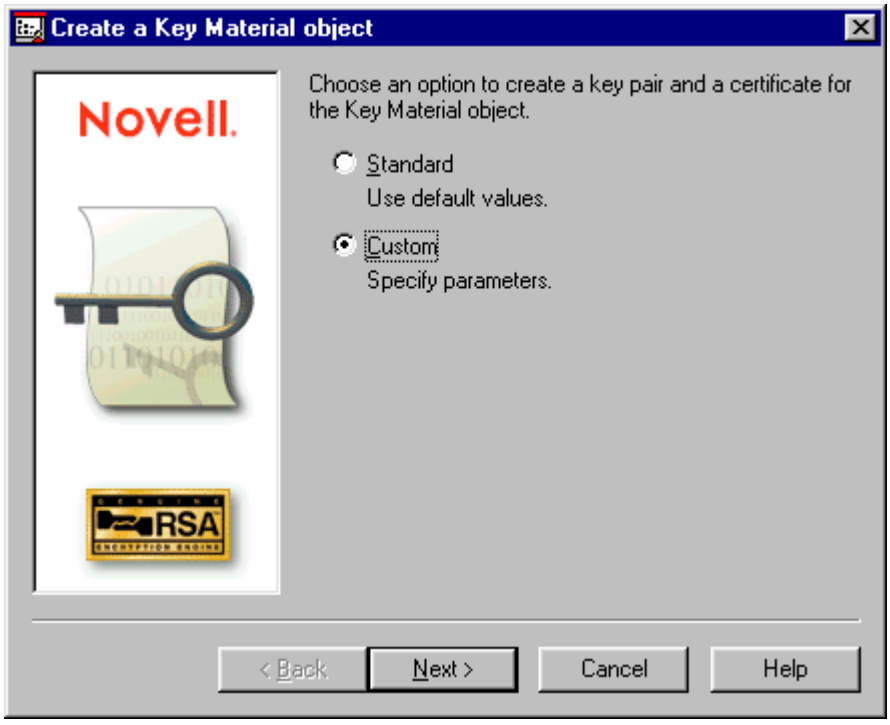
Creating a Key Material Object for BorderManager with NWADMN32

If you do not have BorderManager 3.5, 3.6 or 3.7 installed on a NetWare 5.1 server, you should use NWADMN32 from a BorderManager 3.x server to create a **Key Material Object** to use for SSL Proxy Authentication. (You can also use an existing CertificateIP Key Material Object if it already exists). If you have BorderManager installed on a NetWare 5.1 server, or if you have NetWare 5.1 installed in your tree, or if you have installed Certificate Server 2 in your tree, you may have to use ConsoleOne to create a Key Material Object.



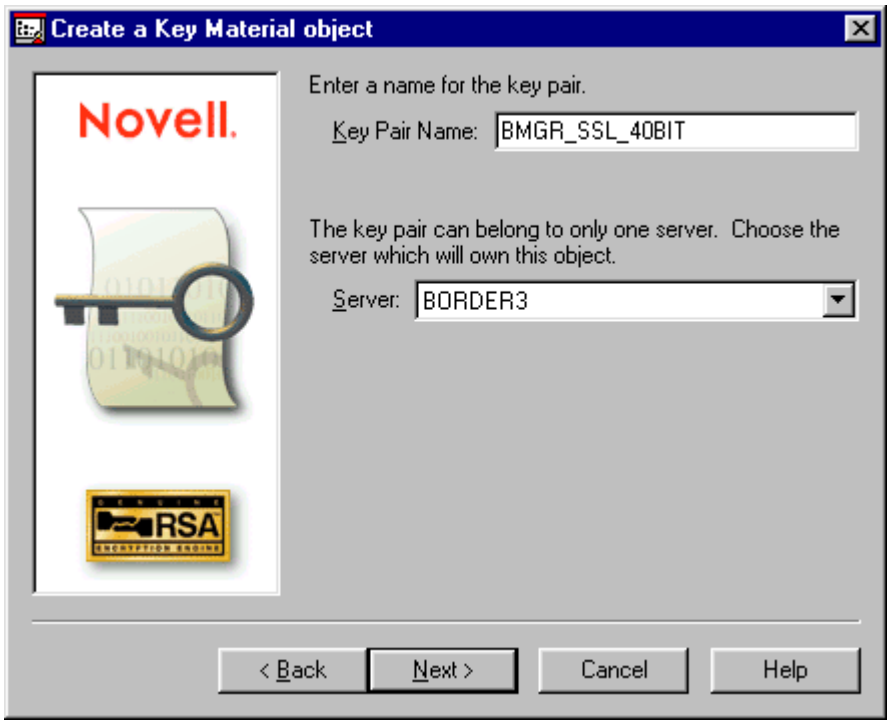
Select the container holding the BorderManager server object, and press **Insert** to begin creating a Key Material Object.

Select the **Key Material** icon, and click on **OK**.



Select **Custom**, and click on **Next**. In order to prevent a problem with the browser accepting certificates created with this Key Material Object, one of the parameters will have to be changed from a default value.

Enter a descriptive name in the **Key Pair Name** field. In this case, a 40-bit Key Material Object is to be created. If you have very old browsers involved, I recommend you create a 40-bit Key Material Object the first time you configure SSL Proxy Authentication in order to guarantee that you have created a certificate that can be accepted by any browser. Should SSL Proxy Authentication work in your testing, you can later go back and try creating a 128-bit certificate. Not all browsers will accept a certificate using greater than 40-bit encryption, so it is worthwhile to start with a 40-bit Key

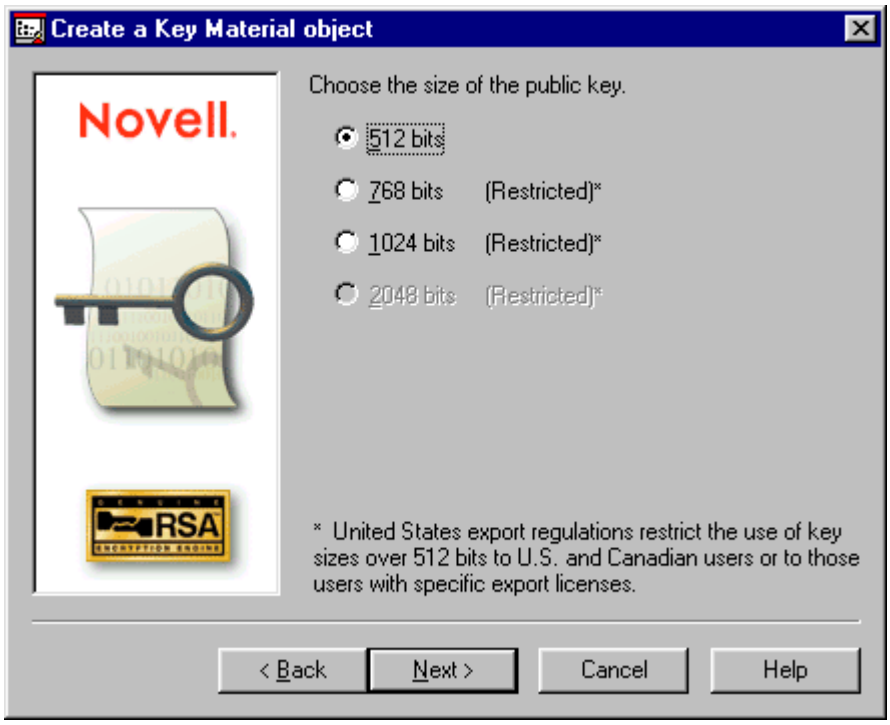


Material Object for testing purposes.

Note As of this writing, a bug has been found in creating 40-bit certificates with ConsoleOne and Certificate Server 2 on some networks. Even though you try to create a custom certificate with 40-bit encryption, it comes up in the browser as using the highest level of encryption available on the server.

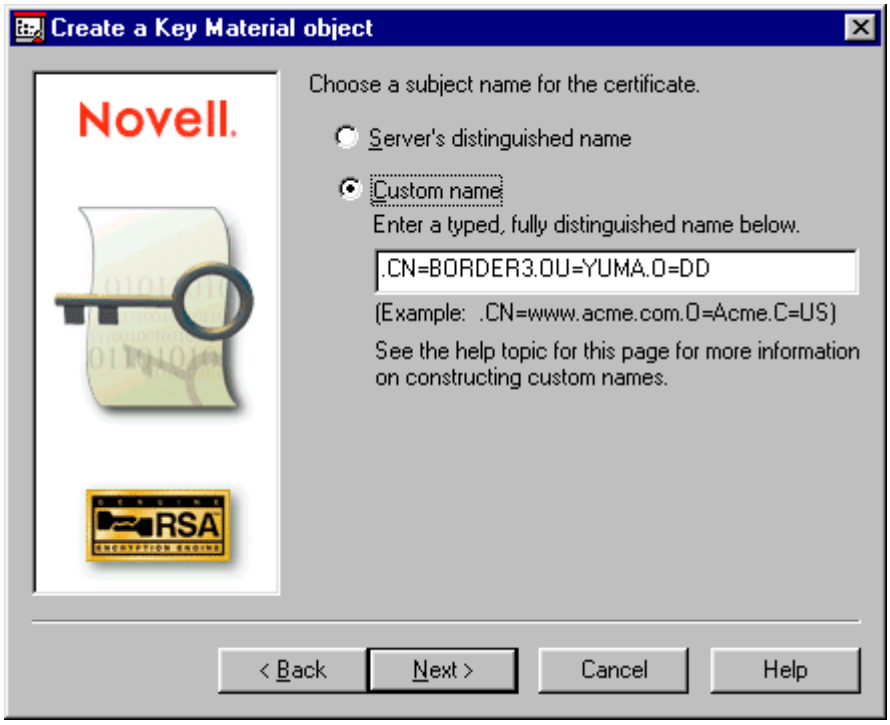
For SSL Proxy Authentication, the Key Material Object must be assigned to the BorderManager server itself. Select the BorderManager server to fill in the **Server** field.

Click **Next** to continue.

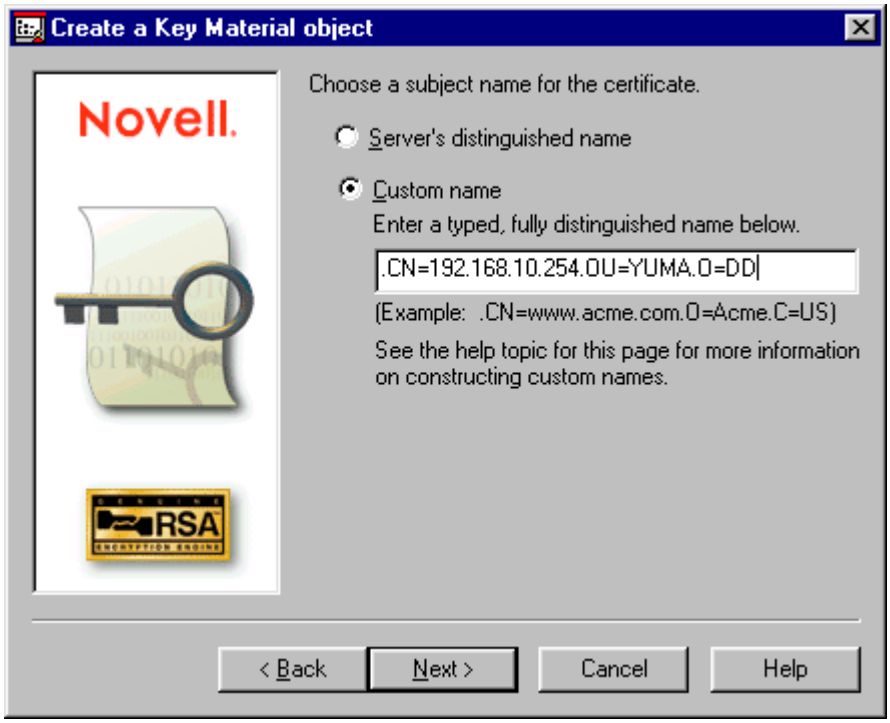


For the first Key Material Object that you create, select the lowest available bit size for the size of the public key. Selecting **512 bits** will result in a 40-bit Key Material Object, which should be universally accepted by the available browsers. If you select a higher bit size, you will have to ensure that the browsers in use can accept the chosen encryption level.

Click on **Next** to continue.



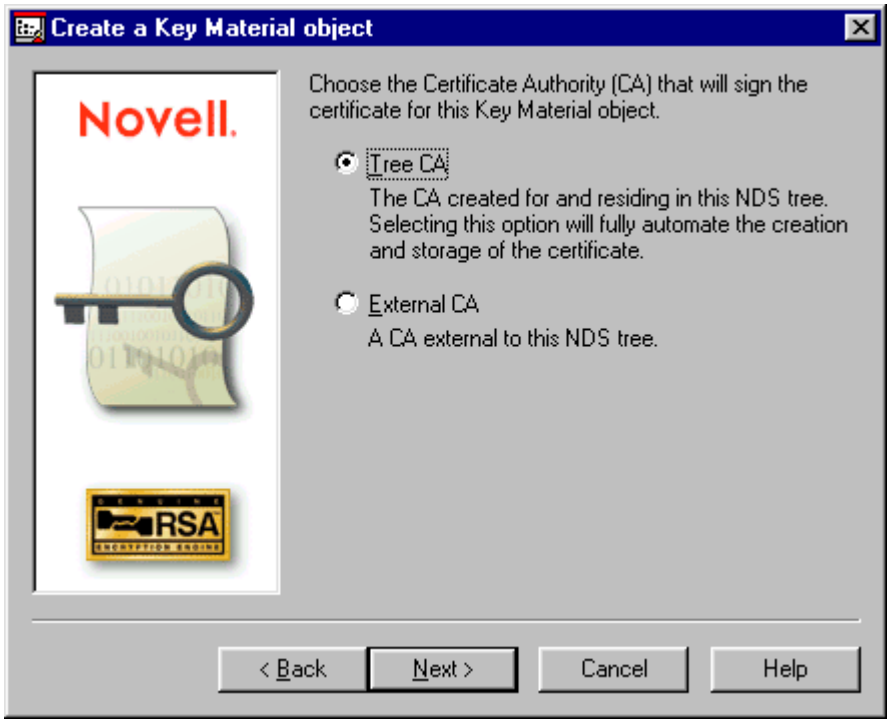
At this point, you should see the BorderManager server's distinguished NDS name appear in the Key Material object creation menu. You need to change this selection, so select **Custom name**.



Change the server name portion of the **Custom name** to the private IP address of the BorderManager server. In the example shown, .CN=BORDER3.OU=YUMA.O=DD has been changed to:

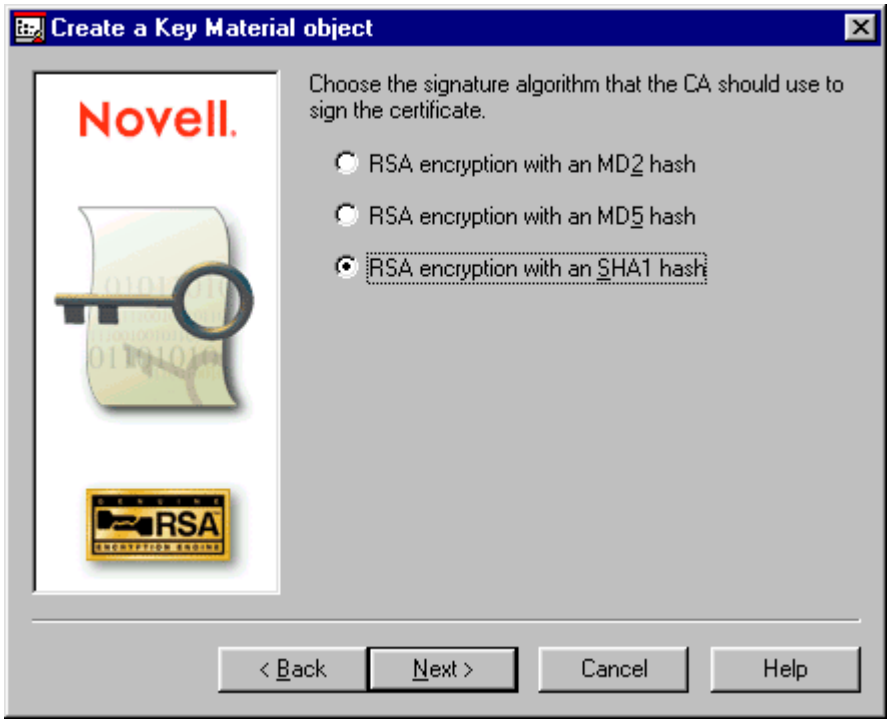
.CN=192.168.10.254.OU=YUMA.O=DD.

Click **Next** to continue.

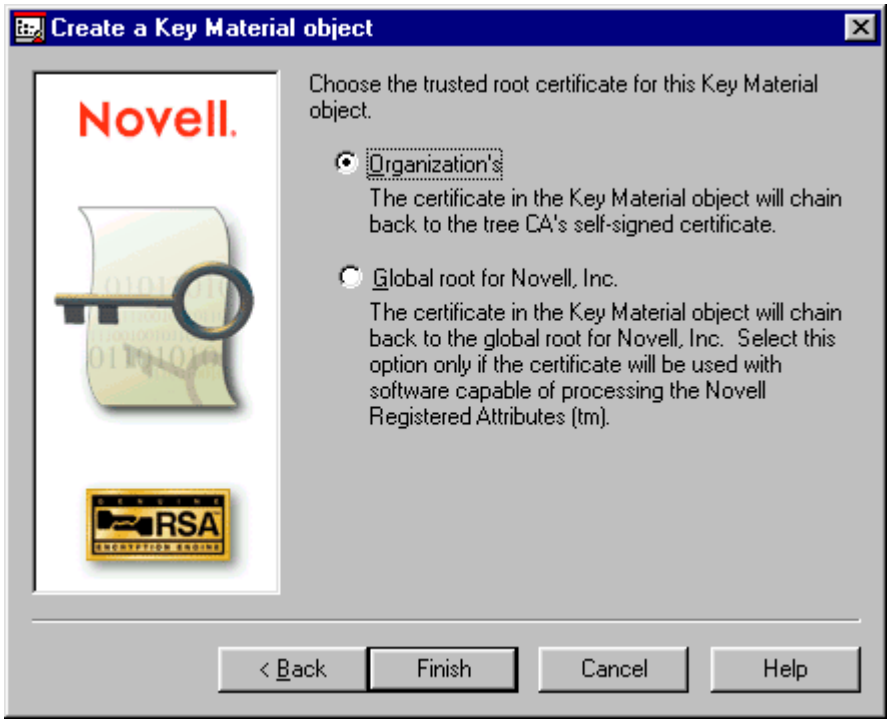


Select the **Tree CA** as the Certificate Authority to sign the certificate for this Key Material Object.

Click **Next** to continue.

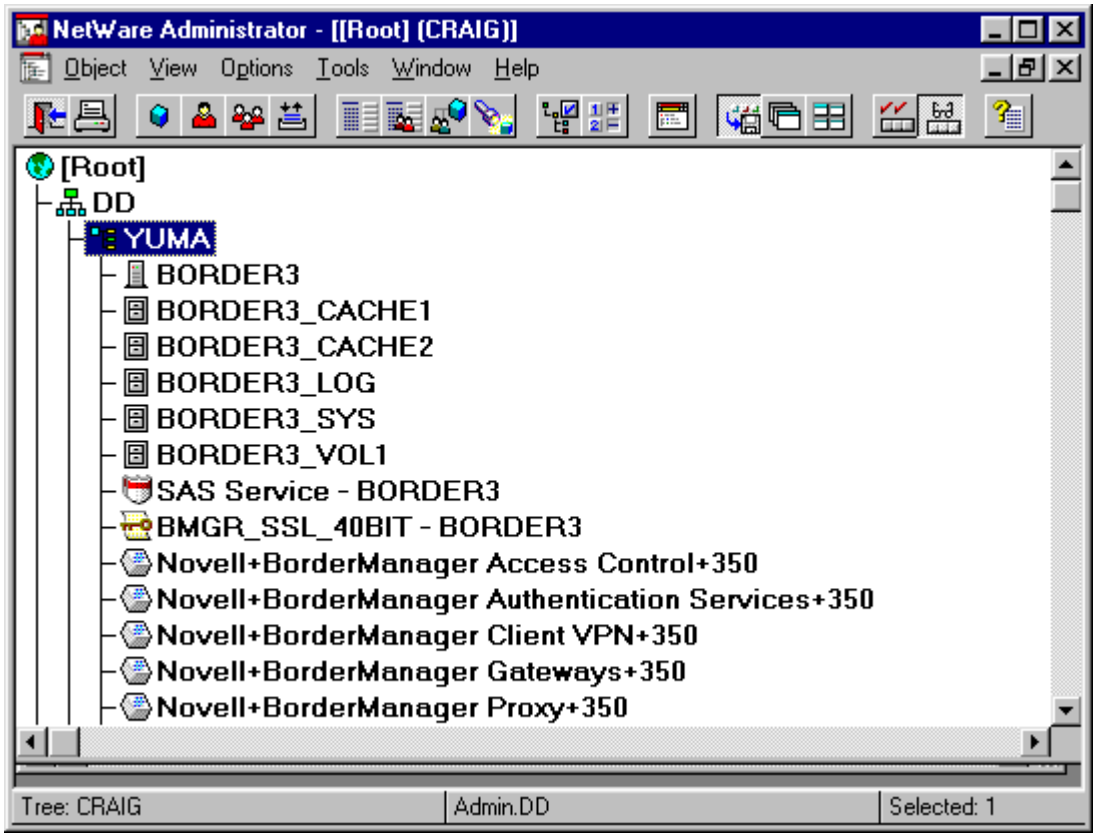


Select the **RSA encryption with an SHA1** hash choice, and click on **Next** to continue.



Select **Organization's** and click on **Finish** to complete the Key Material Object creation.

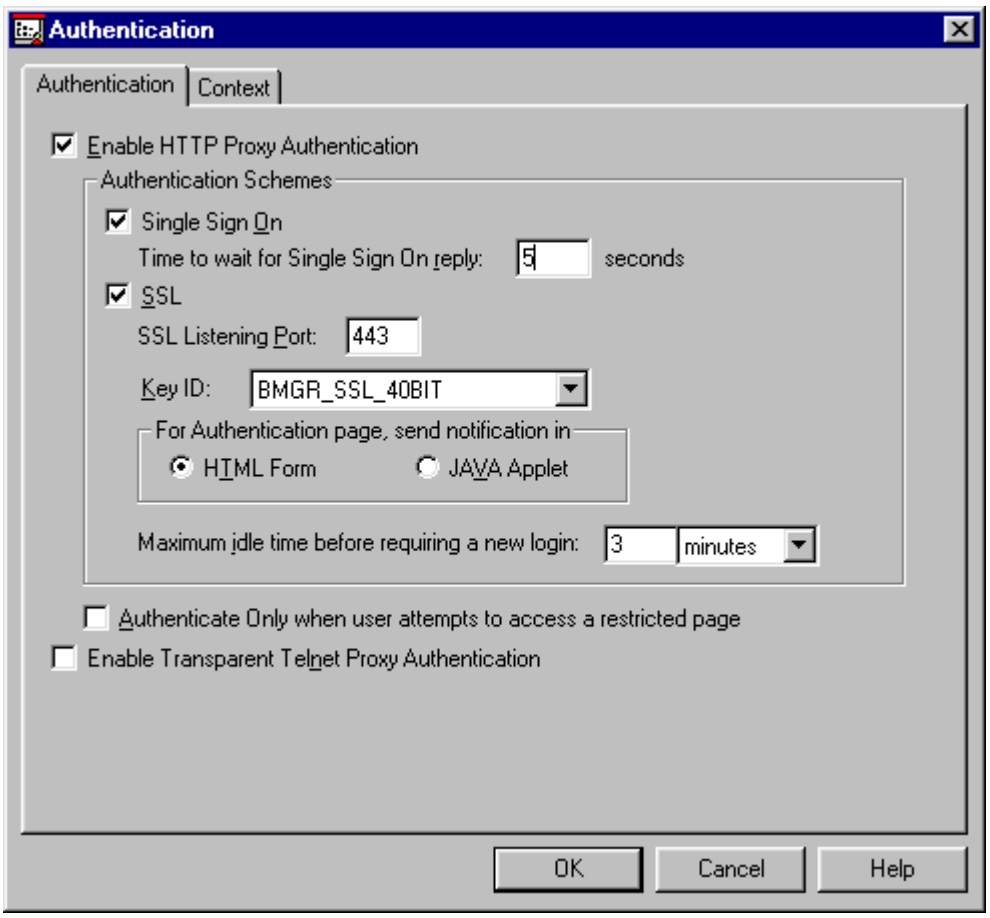
You should see a message that the Key Material Object has been created. Click on **OK**.



The new **Key Material Object** should now show up in the NDS tree. You can now assign the key for SSL Proxy Authentication.

Assigning the Key Material Object for SSL Proxy Authentication

To assign a Key Material Object for use in SSL Proxy Authentication, select the BorderManager server object, and then Authentication Context.



You should now be able to assign any Key Material Object created on the BorderManager server in the Key ID field. The encryption level required on the browser will be set by the Key Material Object selected. Start with a 40-bit key, and if that works, try a 128-bit key, if you have 128-bit BorderManager encryption available to you.

In very old PC's, not all browsers will support a key with greater than 40-bit encryption, so be sure to try a 40-bit key first!

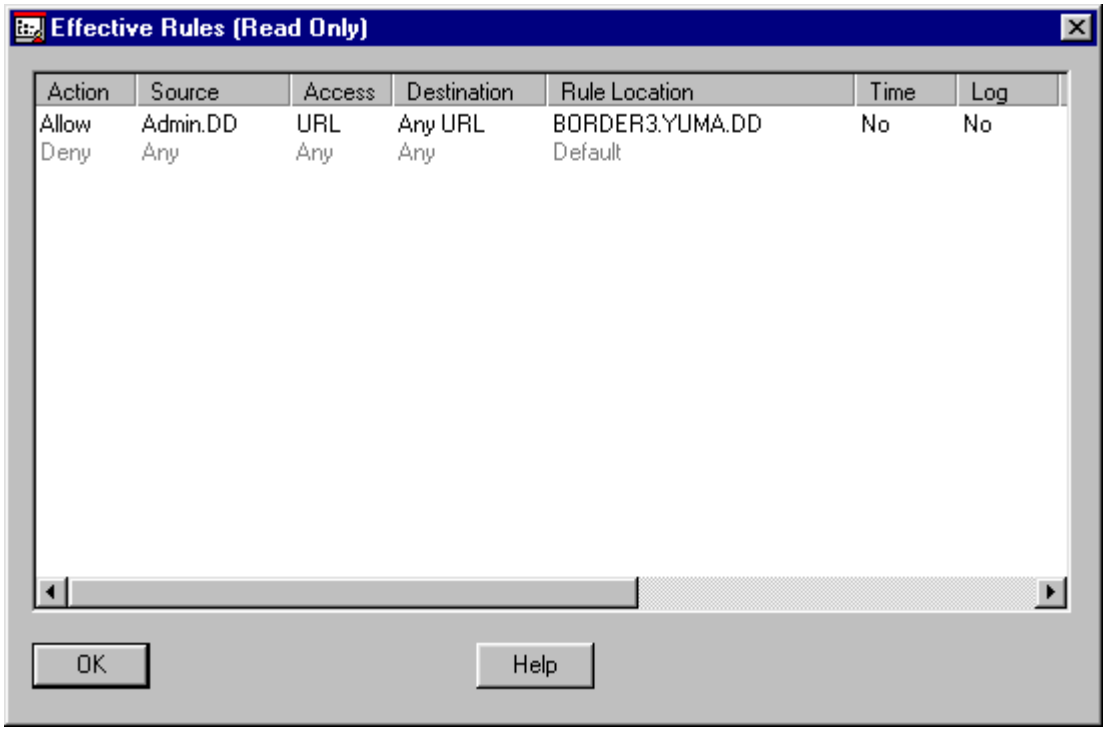
In the example show, the **Time to wait for Single Sign On reply** has been set to 5 seconds. This amount of time will have to elapse after the browser contacts the BorderManager server before an SSL Proxy Authentication login screen pops up.

HTML form is the only reliable method for SSL authentication. The Java form has some compatibility and security issues.

Using SSL Proxy Authentication

In order for Proxy Authentication to be used, you must

- have an Access Rule that calls out an NDS object as a source
- require proxy authentication in the Authentication Context menu in NWADMN32.



The example above shows the Effective Rules for a test of SSL Proxy Authentication. Only one Allow URL rule has been set up, and it specifies a source equal to the NDS user ID **ADMIN.DD**. The default rule Deny Any will block any other attempts to use the HTTP Proxy.

Test Conditions

Netscape Navigator 4.71 was used, with the HTTP and Security proxy settings filled in with the BorderManager server BORDER3 private IP address and port 8080.

CLNTRUST.EXE was not running on the PC.

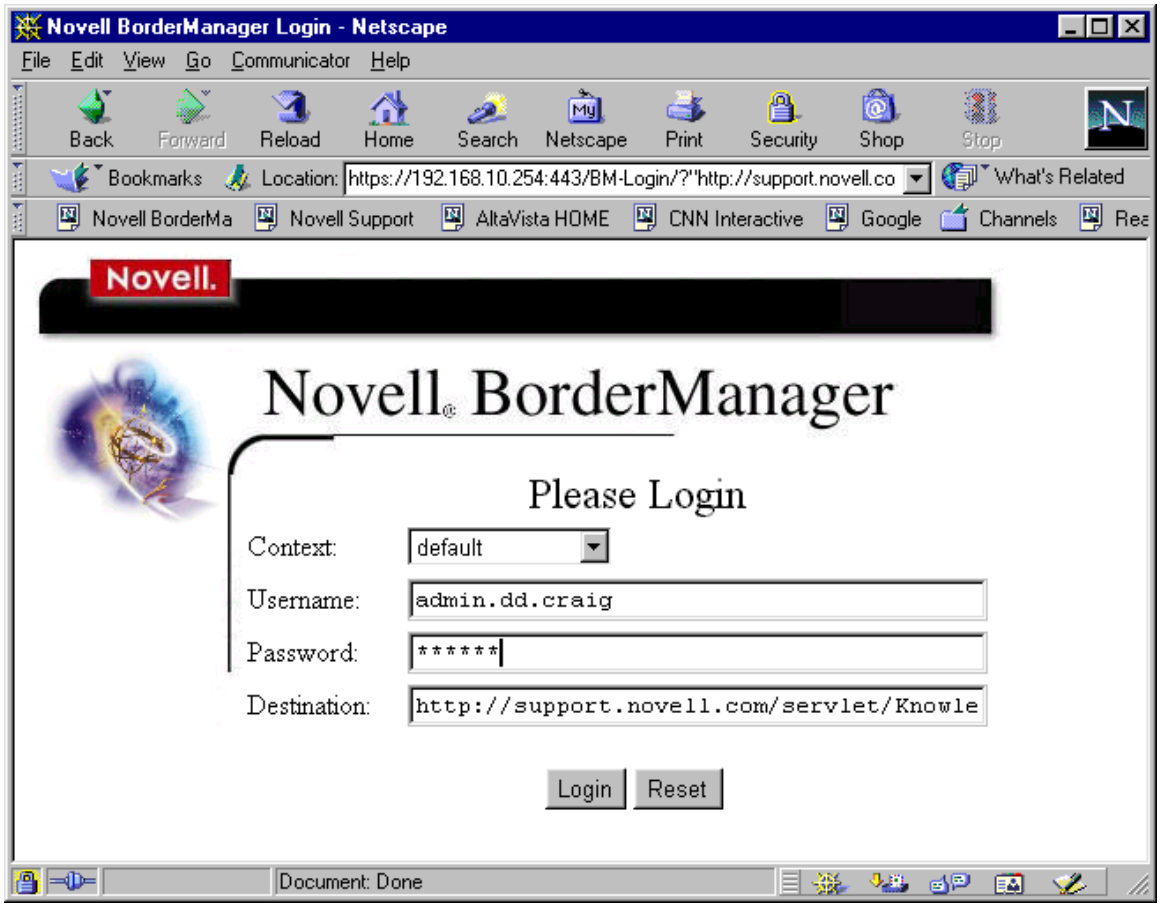
Netscape was launched, and after 5 seconds of inactivity, a certificate acceptance dialog began on the browser.

The first of several certificate acceptance menus is shown in the example above when SSL Proxy Authentication was invoked by the BorderManager server at the browser.

The certificate is necessary to identify the site requesting secured data. The only data to be passed to the BorderManager server in encrypted format will be the login ID and password.

Accept the certificate defaults as desired in order to get to the SSL Proxy Authentication login screen.

The SSL Proxy Authentication Login Screen (HTML)



BorderManager 3.7 and earlier SSL Proxy Authentication HTML Login Menu.

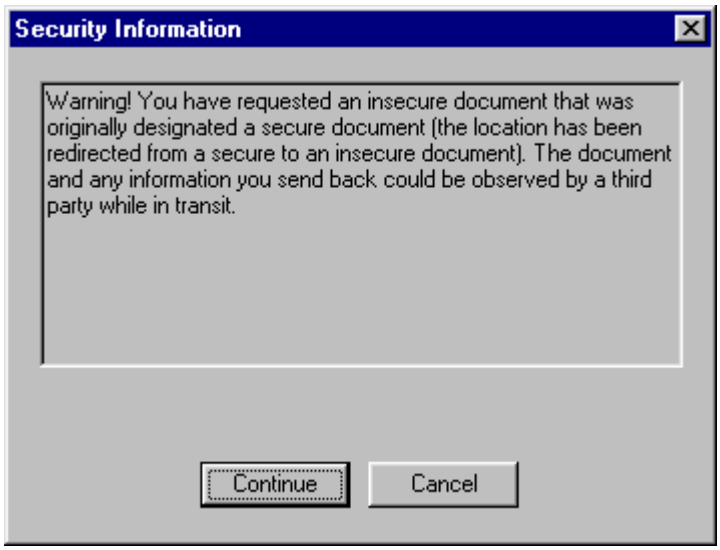
In the example shown, the BorderManager miniwebserver has created a login screen on the user's browser. Note the small padlock in the lower left corner of the browser, which indicates that a secure, encrypted session is in progress.

In order to authenticate to the BorderManager server, which has an access rule allowing only the ADMIN.DD user to access a URL, the fully distinguished user name must be typed into the **Username** field, without the leading period and **with the NDS tree name** (CRAIG in this example) trailing. If the context DD in the NDS tree CRAIG has been configured as a default context in NWADMN32, then only Admin needs to be typed into the Username field.

The admin user's NDS password is typed into the **Password** field.

You cannot change an NDS password from a BorderManager proxy authentication web page.

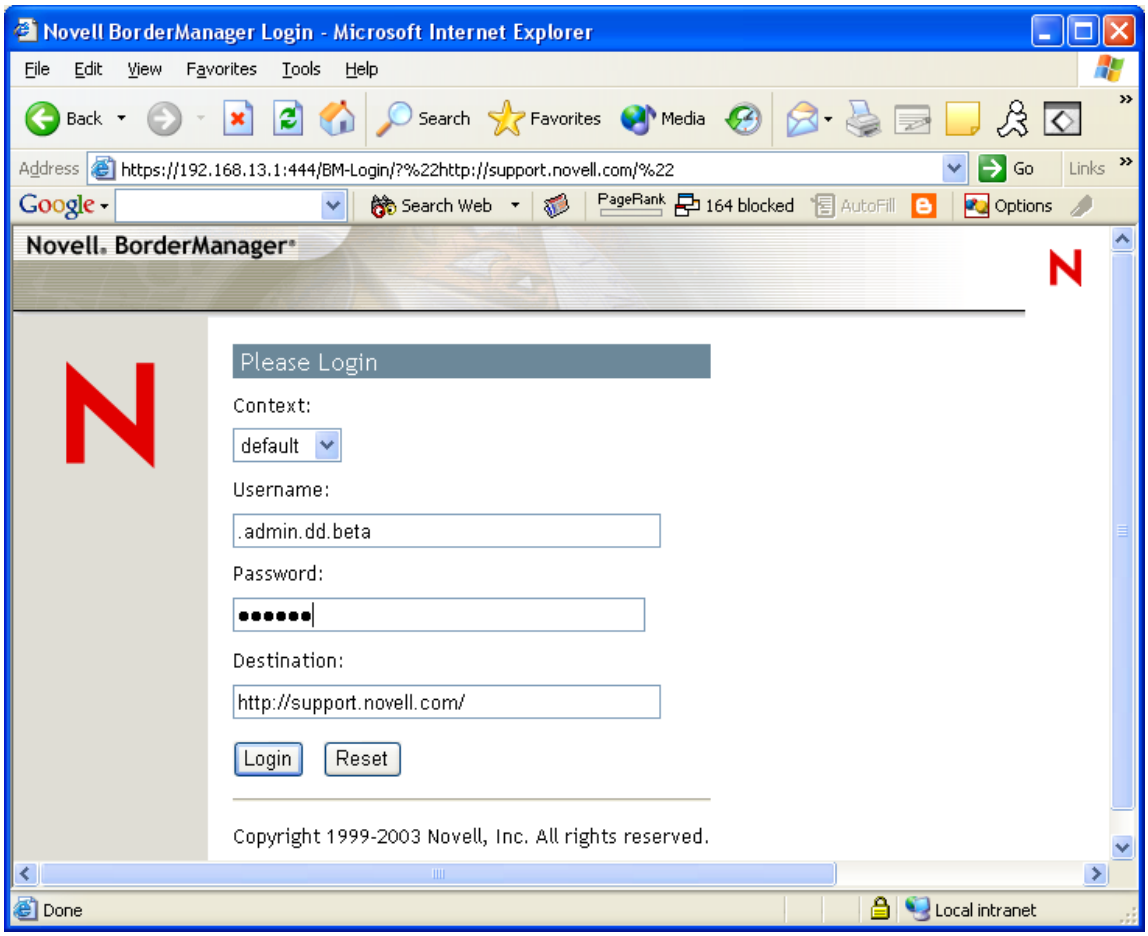
Click on the **Login** button send the data to the BorderManager server.



If the login ID and password are accepted, the session will changed from a secure (encrypted) session to a normal session, and you may see a dialog box warning you of the transition.

Click **Continue**, and your original URL request should then be proxied by BorderManager.

BorderManager 3.8 SSL Proxy Authentication Login Screen (HTML)

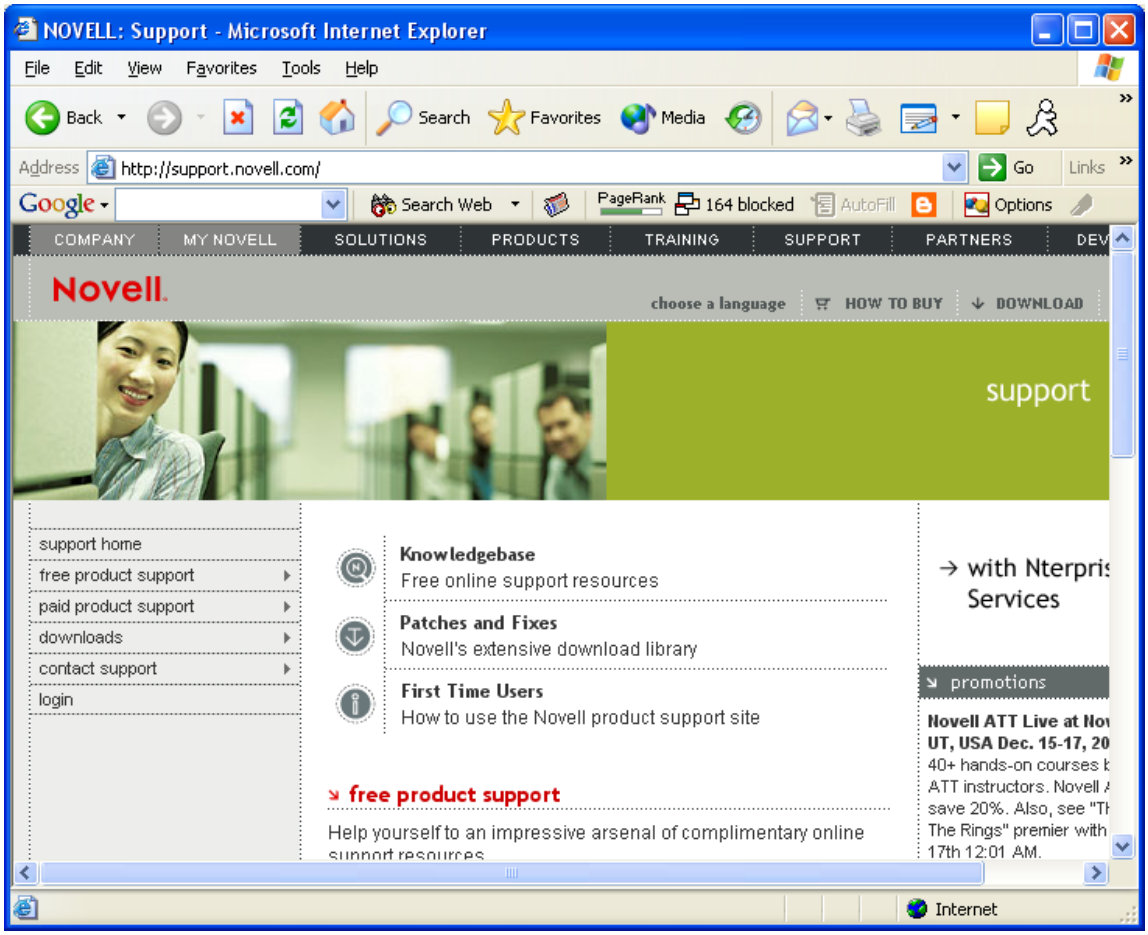


BorderManager 3.8 SSL Proxy Authentication HTML Login Menu

BorderManager 3.8 provides a newer HTML login screen for SSL Proxy Authentication. The major difference between the 3.8 version and earlier versions is that it can be more easily customized, to add corporate legal warnings, for instance.

The main SSL login screen HTML code is contained in the SYS:ETC\PROXY\DATA\BMLOGIN.HTM file.

The usage of the login page is the same as with the earlier versions. Enter the fully-qualified login name (including NDS tree!) and NDS password, and click on Login.



The example above shows the proxied connection requested after the SSL Proxy Authentication login dialog occurred.

Proxy Authentication will be in effect as long as there is a browser connection to the BorderManager server, or the inactivity timeout value (specified in the Authentication Context menu in NWADMN32) has not been exceeded. The default timeout value is three minutes. BorderManager will consider ANY data coming from the same IP address within that three-minute interval to be related to the user ID authenticated earlier. You could even reboot the PC and have another user log in and still have authenticated access, as long as that was done within three minutes of the last activity. If you have a situation where you do not want this to occur, shorten the timeout value dramatically. If you can use CLNTRUST instead of SSL Proxy Authentication, the process of authenticating will be much easier on the users. Unfortunately, CLNTRUST does not run on all platforms.

Note Macintosh computers may not be able to use SSL Proxy Authentication with Internet Explorer as the browser. Try a later version of Netscape instead. The problem is mostly related to an old version of SSL used in BorderManager, but the problem has been addressed in BorderManager 3.7 and later. In either case, be sure to disable TLS in the browser if you have issues with SSL Proxy authentication working.

Cookie-based Proxy Authentication

With the release of BorderManager 3.5 Proxy/ACL patch BM35C09.EXE, BorderManager Proxy Authentication can be done with cookie-based authentication. Prior to this patch, Proxy Authentication only related a host's IP address to the HTTP data stream coming through the BorderManager server. Because all Citrix or Terminal Server users share the same IP address, Proxy Authentication was effectively useless, since it ended up authenticating all Citrix/Terminal Server users to the access rights of the first person to authenticate. With the new patch, the capability existed to authenticate on a session-by-session basis with a cookie stored on the Citrix user's browser. The cookie-based authentication process requires the use of SSL Proxy Authentication (no CLNTRUST), and has some severe limitations. Check the readme of the latest patch sets to see how (or if) this feature is implemented.

One severe limitation of the patches BM35C09 through (at least) BM36C01 is that HTTPS sites **cannot be browsed** from a Citrix server if cookie-based authentication is being used.

Cookie-based authentication is not available for BorderManager 3.0.

Cookie-based authentication requires the following entry in the SYS:\ETC\PROXY.CFG file:

```
[BM Cookie]
BM_Forward_Cookie=1
```

Cookie-based authentication had so many limitations that it was replaced with Terminal Server Authentication in BorderManager 3.7 service pack 2 and later. Terminal Server Authentication can be applied to BorderManager 3.5 and 3.6 servers by using the PROXY.NLM from BorderManager 3.7.

Proxy Authentication For Citrix and Terminal Servers

Concept

Terminal Server Authentication uses a browser-based SSL login menu to collect authentication on individual browser sessions, and tracks the authentication by means of a cookie, used only for a single browser session. Users must log in to the BorderManager proxy server each time they open a browser, but will not have to log in again as long as the browser is not closed.

Terminal Server Authentication is aimed at Microsoft Terminal Server clients (or Citrix clients) where many users can share a single IP address. This method of authentication discriminates among individual users on a terminal server, and as such can provide different access levels per user, based on access rules calling out a NDS user, group or container as the source.

Terminal Server Authentication essentially eliminates all of the major problems that afflicted the cookie-based authentication method engineered for BorderManager 3.5 and 3.6.

Pros

- Authenticates and tracks individual users, per browser session, on a terminal server.
- Unlike the earlier cookie-based authentication, terminal server authentication can be targeted to individual IP addresses, ranges of IP addresses, or IP network addresses. Hosts not in the range of targeted addresses are not affected by this authentication method and can continue to use CLNTRUST.
- Unlike the earlier cookie-based authentication, terminal server authentication allows browsing of SSL sites.

Cons

- The authentication process is not transparent to the users. An SSL Proxy Authentication login menu appears on the browser at the beginning of each browser session making use of HTTP Proxy. CLNTRUST cannot be used.
- The authentication method only supports a limited range of browsers, including Internet Explorer 5.5 and 6.0, and Netscape 6.0, as of BorderManager 3.7 service pack 3.
- The authentication lasts only for the life of the browser session. If the browser is closed, the user must authenticate again the next time the browser is opened. However, some

browsers can be configured to automatically fill in the login information.

Configuring Terminal Server Authentication

A special application called PXYAUTH.EXE is required to be installed on the terminal server to automate part of the authentication process for the user. PXYAUTH.EXE should be found in the SYS:PUBLIC directory of the BorderManager 3.7 (patched to at least Service Pack 2) or later server. This application should be installed on the terminal server before clients make use of terminal server authentication. The terminal server administrator simply needs to run the program once to install it, in the same way that most applications are installed to a terminal server. (That is, there should be no user sessions open on the server.)

Once the PXYAUTH.EXE application is installed on the terminal server, a critical part of the authentication method is automated for the users. Users may see a brief flash of a login menu right after the SSL Proxy Authentication login process is completed. In the background, the PXYAUTH program is automatically running a second authentication process required for the terminal server authentication method to function.

PROXY.CFG Configuration

All other configuration aspects of Terminal Server Authentication are configured using SYS:ETC\PROXY\PROXY.CFG entries.

The PROXY.CFG file must contain the following entries

```
[Extra Configuration]
EnableTerminalServerAuthentication=1
```

These entries enable Terminal Server Authentication, but are not sufficient to tell the proxy what IP addresses are to be targeted for this authentication method.

There are three other possible sections which can be used in the PROXY.CFG file to target the terminal server IP addresses. These sections can be used individually or in combination

- Authentication Subnets
- Authentication Ranges
- Authentication Addresses

```
[Authentication Subnets]
PrivateSubnet1=11.0.0.0/255.0.0.0
PrivateSubnet2=11.4.5.100/255.255.252.0
PrivateSubnet3=164.99.145.98/255.255.252.0
```

The **[Authentication Subnets**] section allows you to define entire subnet addresses that are used for terminal server farms. Each IP address subnet is preceded by the PrivateSubnetX= command, where X is 1, 2, 3, etc.

```
[Authentication Ranges]
PrivateRange1=100.25.4.5-100.25.4.60
PrivateRange2=20.1.1.1-20.4.5.25
```

The **[Authentication Ranges]** section allows you to define IP address ranges that are used for terminal servers. Each IP address range is preceded by the PrivateRangeX= command, where X is 1, 2, 3, etc.

```
[Authentication Addresses]
PrivateAddr1=192.168.10.50
PrivateAddr2=192.168.11.50
   ivateAddr3=192.168.12.50
```

e

The **[Authentication Addresses]** section allows you to define individual IP addresses that are used for terminal servers. Each IP address is preceded by the PrivateAddrX= command, where X is 1, 2, 3, etc.

Configure the PROXY.CFG file with the desired entries for Subnets, Ranges or Addresses, and load (or reload) PROXY.NLM on the BorderManager server. Be sure the PXYAUTH.EXE program was installed on the terminal server. Enable **SSL Proxy Authentication** in NWADMN32, **BorderManager Setup** main menu, **Authentication Context**. Configure access rules as needed to call out NDS users, groups or containers, and then test by browsing from a terminal server session.

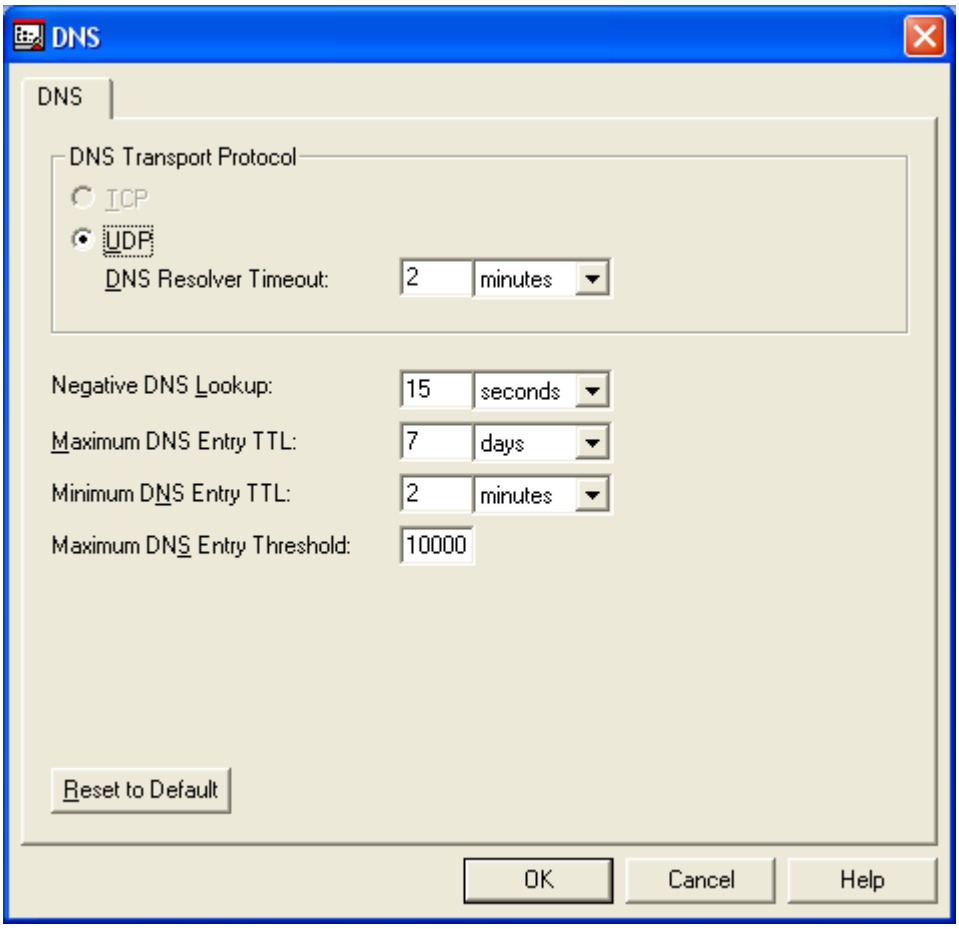
If the authentication method is working properly, the users should receive a SSL Proxy Authentication prompt when they first browse, and each user on the terminal server should be individually authenticated and subject to different access rules, based on their SSL login user ID.

On the BorderManager server proxy console screen, Option 24 should show that terminal server authentication is enabled, and should show more than 0 terminal server authentication requests.

DNS Parameters

BorderManager proxy has its own DNS caching scheme, used to hold DNS address query results in memory to avoid having to make unnecessary DNS lookup requests. This is NOT a DNS service running on the server, but a caching of the replies. In this configuration, DNS services should be running on another server, which could be internal on the network or at the ISP's network.

Select the **DNS** button on the BorderManager setup main menu page to configure DNS parameters.



BorderManager 3.7 Service Pack 2 Example – *note that the TCP DNS Transport Protocol option has been disabled in the later patches.*

One parameter has been changed from the default – set the **Maximum DNS Entry Threshold** up from the default of 2500 to 10000. This allows BorderManager to cache up to 10,000 separate DNS entries in DNS cache memory at one time. If the upper limit is

reached, the oldest entries will be flushed from cache to make room for new ones.

The **Negative DNS Lookup** parameter requires some explanation. If BorderManager cannot resolve a name, a negative entry is held for this period of time. During that time period, any additional requests for the same hostname are answered (immediately) with a message about a failed DNS request. Only after the timeout period expires are additional DNS lookups to that hostname sent again to a DNS server. This feature prevents many people from needlessly overloading a DNS server asking for the same (invalid) hostname. This feature only applies to web browsing requests through the proxy server, or if the DNS proxy is being used.

The other options are best left at the default values. A brief explanation of each parameter can be found using the online help in NWADMN32. Some additional explanation is given below:

DNS Transport Protocol: Most DNS queries are done using UDP protocol. However, there are some cases where your ISP may not be routing UDP or there is some issue preventing UDP DNS queries from working well in a particular environment. In case of problems with DNS resolution (using HTTP Proxy or DNS Proxy), try changing the transport protocol here to TCP. Most DNS servers will support either UDP or TCP lookups.

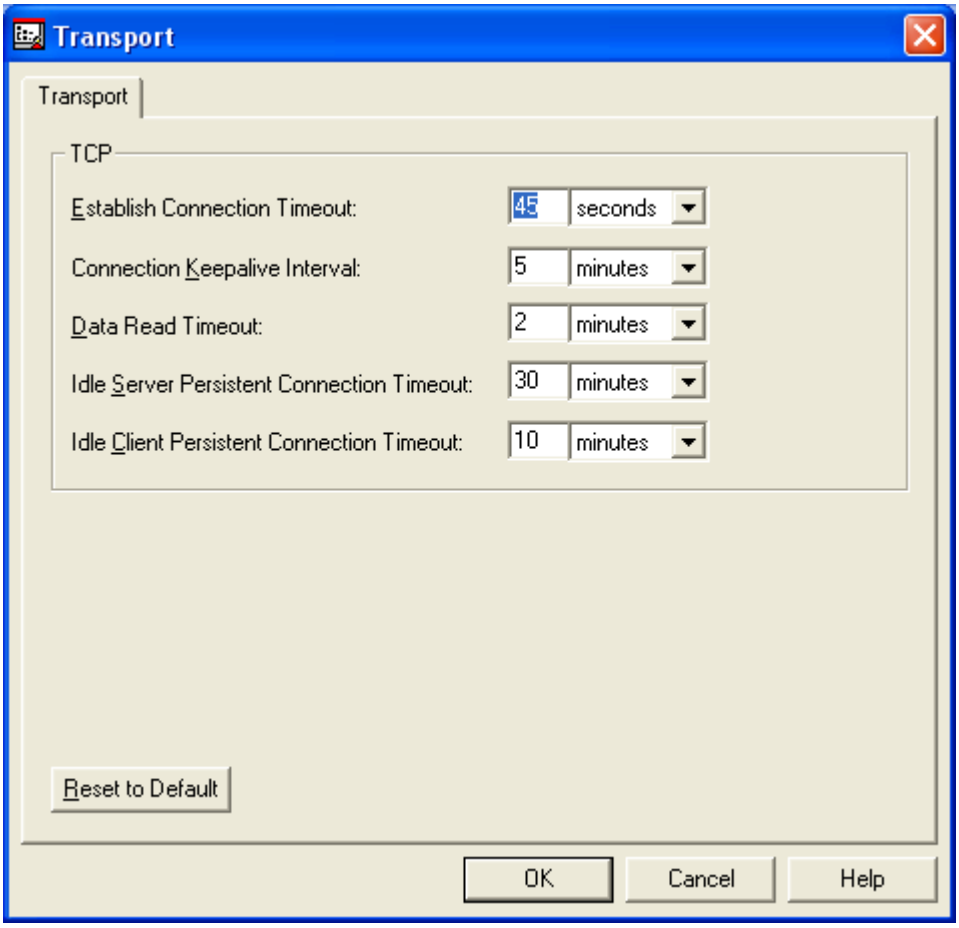
Maximum DNS Entry TTL: TTL stands for Time To Live, and this parameter is the maximum allowed time that a DNS address is to be cached by BorderManager. After that time period, a new query is sent to reconfirm the address of a host name.

Minimum DNS Entry TTL: This value indicates that a DNS lookup result should be held in cache for no less than the specified time before a new query is tried to the same host name.

Note If you put entries in the BorderManager server's HOSTS file, anyone using DNS Proxy can resolve those entries as 'A' type resource records. Thus, the DNS Proxy can act like a 'poor man's DNS server'.

Transport

From the BorderManager setup main menu, select **Transport** to configure timeout values.



One change has been made to the default settings. The **Establish Connection Timeout** has been changed from 30 seconds to 45 seconds to give additional time to connect to slow web sites.

The other options are best left at the default values. Some of these settings may provide a workaround to or relief from problems connecting to particular web sites, but only trial-and-error testing will tell for sure.

A brief explanation of each parameter can be found using the online help in NWADMN32. Some additional explanation is given below:

Establish Connection Timeout: This is the amount of time that BorderManager will spend trying to get a response from a site before giving up and returning an error to the user.

Connection Keep-Alive Interval: Connection Keep-Alive Interval: If persistent connections are being used (see below), this is the time

interval between the packets that the BorderManager proxy sends to a web server to keep the connection open. Reducing this value may result in additional unnecessary use of WAN bandwidth as additional unnecessary keep-alive packets are sent.

Data Read Timeout: When data starts transferring from an external server to BorderManager, this is the amount of time that BorderManager will wait before dropping the connection if data stops flowing. On slow connections or very busy WAN links, you may need to increase this time value to prevent incomplete web pages or data transfers from occurring.

Idle Server Persistent Connection Timeout: BorderManager will attempt to hold open connections to browsers for some period of time even when no requests are currently being made from that browser. This parameter is supposed to improve performance, but in some cases may cause problems to certain web sites. This time interval is the amount of time that BorderManager will use before dropping a connection to a browser. Establishing a new connection from a browser takes longer than requesting data from the HTTP Proxy when a connection has already been established.

Idle Client Persistent Connection Timeout: BorderManager will attempt to hold open connections to web servers for some period of time even when no requests are currently being made to that web server. This parameter is supposed to improve performance, but in some cases may cause problems to certain web sites. This time interval is the amount of time that BorderManager will use before dropping a connection to a web server. Establishing a new connection takes longer than requesting data from a web server when a connection has already been established.

Chapter 6 - HTTP Proxy

Concepts

The purpose of the HTTP Proxy is to take requests from a browser, and regenerate those requests onto the BorderManager public (or private) interface, get the results back from a web server, cache the results, and send the results back to the requesting browser. The traffic being proxied can be subjected to control by means of Access Rules.

The HTTP Proxy listens on the port number that you configure (normally port 8080), and that port number should not be the same as normal HTTP traffic (TCP port 80).

The browsers must be configured to use a proxy server in order to make use of HTTP Proxy. HTTP Proxy is also known as 'Forward Acceleration'.

The HTTP Proxy will automatically listen and proxy traffic on any IP address configured as **Private** in NWADMN32, BorderManager Setup, IP Addresses. If you want the HTTP proxy to be available to users on the public side of the BorderManager server, you can define the public IP address as private and public. The HTTP proxy will then listen on the public IP address, as well.

Pros

- The use of the HTTP Proxy can be controlled by Access Rules based on URL's to be Allowed or Denied. If the default packet filters have been enabled (using the BRDCFG.NLM utility) and the **Enforce Rules** box has been checked in NWADMN32, BorderManager Setup, then no one on the internal LAN will be able to browse through the BorderManager server. The default packet filters will prevent anyone from bypassing the HTTP Proxy because HTTP Port 80 traffic will be filtered, while the default Deny All rule will prevent any users from using the HTTP Proxy until an Allow URL Access Rule has been added.
- The HTTP Proxy has many configuration options. The HTTP Proxy can make full use of NDS-based Access Rules, as long as Proxy Authentication is enabled.
- HTTP Proxy caches data retrieved, so that later requests can be served from disk or RAM without having to use Internet

bandwidth. The caching behavior of the HTTP Proxy can be configured in great detail.

- The HTTP Proxy does more than just proxy the HTTP data (as a Transparent Proxy would) – it also does the DNS lookups for the requesting browser, and it tunnels HTTPS requests. DNS queries are cached as well as the HTTP data for better performance.

Cons

- The browsers must be configured to use HTTP Proxy by pointing to the proxy IP address and proxy port number.
- Some web servers and browsers do not correctly follow RFC guidelines, resulting in occasional problems viewing certain web sites. Typically, these problems are addressed in patches from Novell and settings in the PROXY.CFG file.
- Caching, an integral part of HTTP Proxy, does not work well when an NSS cache volume is used. It is essential that the server is configured with a traditional cache volume.
- The default filter exceptions for BorderManager 3.8, and in some cases 3.7, are designed to allow only port 80 and 443 to be used by the HTTP Proxy, meaning that web servers using non-standard port numbers will not be accessible unless custom filter exceptions are configured. This subject is well covered in my book on configuring BorderManager filter exceptions.

How BorderManager HTTP Proxy Works With DNS

It is important to know how the HTTP Proxy interacts with DNS requests.

When a browser is configured to use the HTTP Proxy, a request is sent to the HTTP Proxy to retrieve the data at the specified URL. All of the work of getting that data is then done by the HTTP Proxy, and that includes looking up the IP address of the URL. When the browser is configured to go 'direct to Internet' (no proxy), the browser's PC must resolve the URL to an IP address. The point here is that the HTTP Proxy (unlike the HTTP Transparent Proxy) will perform the DNS lookup instead of the PC, which means that the BorderManager server must be configured to point to a DNS server.

The HTTP Proxy will go through several steps in order to resolve an IP address from a URL. It does not simply send a request to a DNS server as a PC might. BorderManager keeps the most recent DNS addresses in memory for better performance on subsequent requests. The maximum number of DNS addresses held in memory is configured in NWADMN32, and defaults to 2,500 entries. (I recommend setting that limit up to 10,000 entries).

The HTTP Proxy also writes those DNS addresses entries to disk every 10 minutes in the SYS:\ETC\PROXY\PXYHOSTS file. This is so that the next time that PROXY.NLM loads, it will immediately read all of those addresses back into memory so that the addresses do not have to be resolved again. (The entries also age out after a time, and the HTTP Proxy will recheck the addresses in time). Because a new PXYHOSTS file is written so often, I recommend flagging the SYS:\ETC\PROXY directory for immediate purge of deleted files. (FLAG PROXY P /DO)

The HTTP Proxy will pull in addresses from the SYS:\ETC\HOSTS file as well as from a DNS server. This has important ramifications for internal web servers. If you do not have an internal DNS server, you can still have the HTTP Proxy resolve an internal URL as long as you put the correct entry into the BorderManager server's HOSTS file. Consider the following example:

```
# SYS:\ETC\HOSTS
#
127.0.0.1        loopback lb localhost    # normal loopback
address
192.168.10.252   BORDER1
192.168.10.250   www.yourdomain.com
192.168.10.249   www2.yourdomain.com
192.168.10.251   www3.yourdomain.com
```

Each HOSTS file should contain at least the 127.0.0.1 LOOPBACK entry and an entry for the server itself (here 192.168.10.252 BORDER1). The example shown also gives internal IP addresses for www.yourdomain.com, www2.yourdomain.com and www3. yourdomain.com. With these entries in the HOSTS file, the HTTP Proxy (and reverse proxy acceleration of internal web servers, explained later) does not need to point to an internal DNS server in order to pull data from those web servers. More importantly, if there is no internal DNS server, the proxy knows to go to the internal IP addresses of the web servers when a request comes from the internal to one of those URLs.

If the BorderManager server is set to point to an internal DNS server, the HOSTS file entries should still take precedence. A NetWare server will periodically check the HOSTS file every minute or so in order to catch new entries with no action required on behalf of the server administrator. When an entry is read from the HOSTS file, it is placed into BorderManager's DNS memory cache.

Both the HTTP Proxy and the DNS Proxy read from the same DNS memory cache. The entries are read from cache, not from the PXYHOSTS file. The PXYHOSTS file is only read when PROXY.NLM loads, in order to immediately populate the DNS memory cache.

When the HTTP Proxy receives a request for a certain URL, the proxy first checks the memory cache to see if one (or more) IP addresses exist for the URL. If no entry is found, the first DNS server configured will be requested to provide an IP address for the URL. (The DNS server entries are configured in INETCFG.NLM, Protocols, TCP/IP, DNS Resolver Configuration. The data entered there is stored in the text file SYS:\ETC\RESOLV.CFG).

In general, if the first DNS server does not respond at all in a certain amount of time, the next DNS server in the list is tried, assuming you configured more than one DNS server. (You can configure up to three DNS servers, but generally only the first one is used – the others are for backup). This is true for how NetWare uses DNS resolution. BorderManager proxy has an additional feature – it constantly sends a query for www.novell.com to each DNS server configured in the RESOLV.CFG file. If it does not get an answer back in a certain amount of time, it marks that DNS server as down and will not send queries to it until it begins responding again. You can see the DNS status on menu option 4 on the Proxy Console screen on the BorderManager server.

If you have internal web servers, you MUST have BorderManager configured to resolve the web server to the internal IP address! This simple point is often overlooked. If you only specify your ISP's public DNS servers in INETCFG, your BorderManager server will not know how to get to the actual web server. If you do not have an

internal DNS server, put the entries in the BorderManager server's HOSTS file, simple as that!

The question sometimes comes up – how do I set up internal DNS servers and the DNS proxy and the BorderManager server itself? This can seem very confusing, as it seems that everything is pointing back at itself, or in circles. Here is one scenario that explains how the process works

1. There is an internal DNS server with some internal IP addresses.
2. Dynamic NAT with a stateful DNS packet filter exception has been configured on the BorderManager server to allow internal DNS requests to go out to the Internet, and allow the responses to those requests.
3. The internal DNS server is forwarding non-authoritative requests to the ISP's DNS servers. (Non-authoritative requests just means 'requests to a domain that I am not set up for'). Those requests go out through the BorderManager server by means of dynamic NAT and filter exceptions.
4. The BorderManager server has DNS proxy enabled.
5. The BorderManager server has three DNS servers configured in INETCFG. The first server in the list is the internal DNS servers. The two backup servers (second and third in the list) are the ISP's DNS servers.

In this scenario,

- A browser requests a URL from the HTTP Proxy.
- The HTTP Proxy checks its DNS memory cache, and finds that it does not have an entry.
- The HTTP Proxy sends a DNS requests to the first configured DNS server – the internal DNS server.
- The internal DNS server checks its memory cache and finds that it does not have an entry. The internal DNS server then makes a request to one of the ISP's DNS servers.
- The DNS request passes out through the BorderManager server by way of the packet filter exceptions.
- The ISP's DNS server finds the needed IP address, and passes that data back to the internal DNS server, by way of the BorderManager server.
- The internal DNS server adds the entry to its memory cache, and passes the answer back to the BorderManager HTTP Proxy.
- The HTTP Proxy adds the entry to its memory cache, and then goes out and requests the HTML data from that IP address.

If the URL was for an internal host, the BorderManager server may have found the entry in its own DNS memory cache from a HOSTS file entry, or the internal DNS server would have had the IP address in its memory cache.

If an incorrect entry gets into the BorderManager server's DNS memory cache, you will see that there are two places you must change that entry. (Perhaps an internal web server just changed IP addresses, and you want to make sure the HTTP Proxy doesn't go to the old IP address). The first place to make a change is the DNS memory cache. You cannot change an entry there, so you must clear it by unloading PROXY.NLM. However, when PROXY.NLM loads again, it will simply read back in the old IP address from the PXYHOSTS file. So you must also delete the SYS:\ETC\PROXY\PXYHOSTS file while you have PROXY.NLM unloaded. In this way, when PROXY.NLM loads again, there will not be any old entries for the old URL, and a new DNS lookup will take place.

You cannot delete the PXYHOSTS file while PROXY.NLM is loaded, and even if you did, the file would be rewritten within 10 minutes with the contents of the DNS memory cache. Unloading and reloading PROXY –CC will clear the PXYHOSTS file on BorderManager 3.5 and later.

If you wonder what IP address is actually being held in cache on the BorderManager server, you can look up the address on the Proxy Console menu option 12 at the BorderManager server. That procedure is shown toward the end of this book, in the section on Proxy Console Screens.

Some web sites have more than one IP address because multiple servers are being used for load balancing purposes. BorderManager will try to use all of the IP addresses as well for fastest performance.

How Browsers Are Configured For HTTP Proxy

In order to use the HTTP Proxy, the individual browsers must be set to point to the HTTP Proxy. The following examples show a typical configuration, when the HTTP Proxy is set up at private IP address 192.168.10.254.

If you leave the browsers set to 'Direct Connection to the Internet', no one should be able to browse as long as

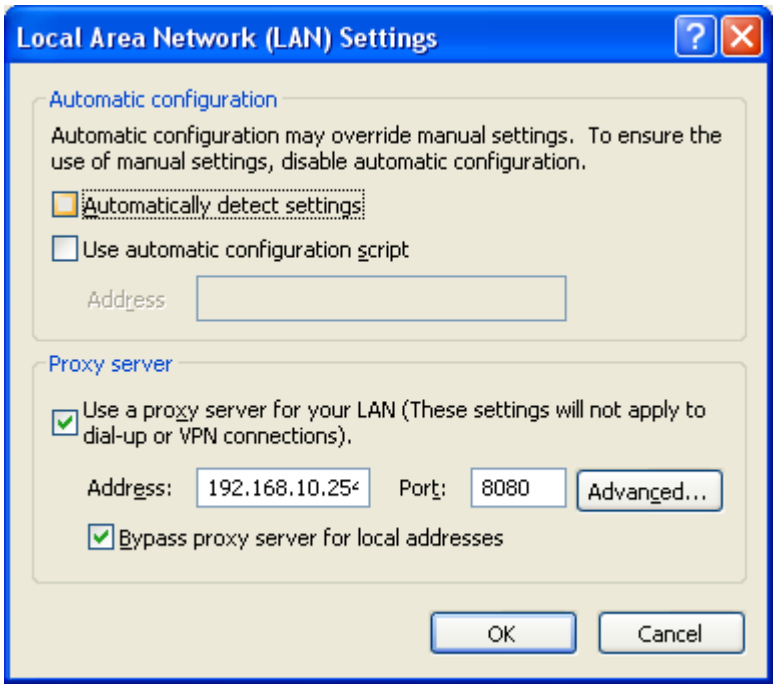
a) the default packet filters have been configured, and

b) Transparent Proxy is not enabled, and

c) access rules are enforced.

Note There are ways to configure the browser proxy settings automatically without having to visit each workstation and do it yourself. Please see the section on this in the Odds & Ends chapter later in this book.

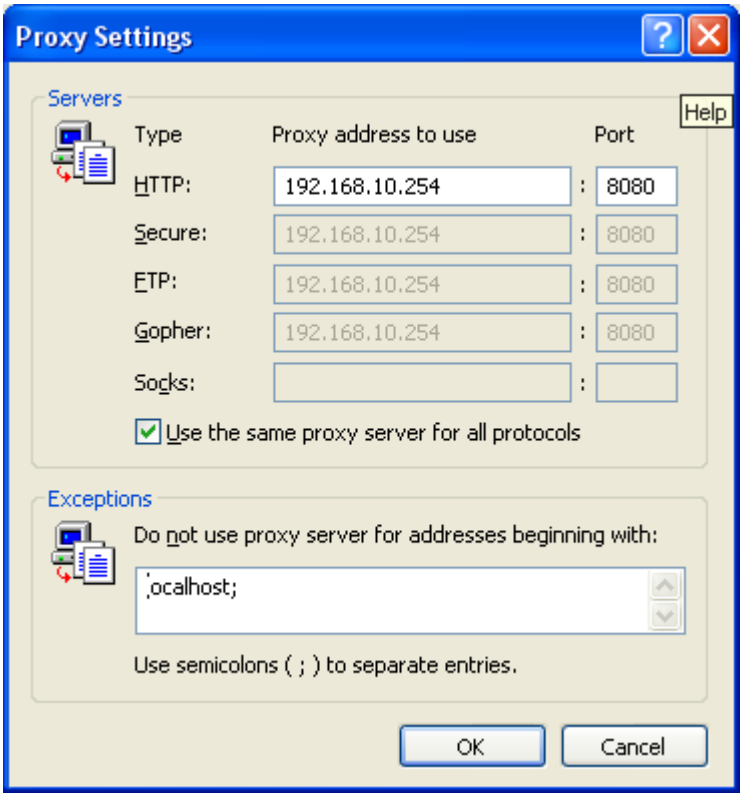
Internet Explorer



Internet Explorer, (version 6.0, 5.x is the same), is configured under the Tools, Internet Options, Connections, LAN Settings, Proxy Server option. Enter the HTTP Proxy server IP address and port number (usually) 8080, and set the following options:

- Do **not** Automatically detect settings. Doing so will only slow things down. (If you really want that option to work, start your research by searching the Internet for the WPAD option. I have some information on that at my web site, http://www.craigjconsulting.com.)
- Do not Use automatic configuration script, unless you want to make use of a PROXY.PAC file. I have some information on that at my web site tip #64 (http://www.craigjconsulting.com) along with some sample files.
- Check the option 'Use a proxy server for your LAN…'
- Check the option to Bypass proxy server IF you have an internal DNS server to resolve local addresses. (Otherwise, leave that option unchecked – the local traffic should go through the BorderManager proxy, which may help with certain DNS name resolution issues).

Clicking on the Advanced button brings you to the following menu:

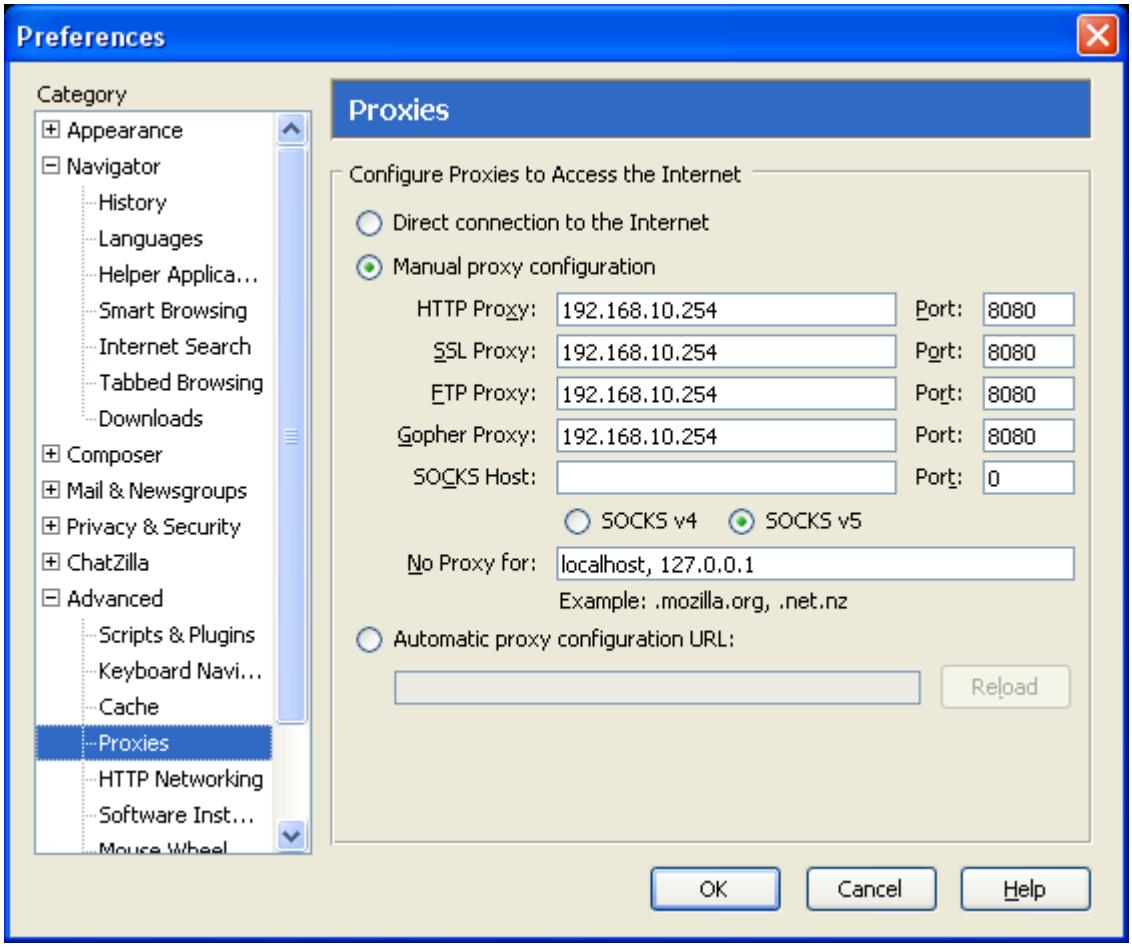


If you check the box (default setting) to Use the same proxy server for all protocols, the same proxy server and port number will be used for HTTP, Secure, FTP and Gopher. This is normally what you want.

The Exceptions area at the bottom of this menu is where you enter various URL's that you do not want the browser to use a proxy to access. The syntax on these entries can be tricky, and I advise you to approach a proxy-bypass proxy with some patience.

A PROXY.PAC file is a centralized way to manage when to use and not to use a proxy, as well as what proxy to use. An example of a PROXY.PAC file is shown in the Odds & Ends chapter later in this book.

Mozilla 1.5

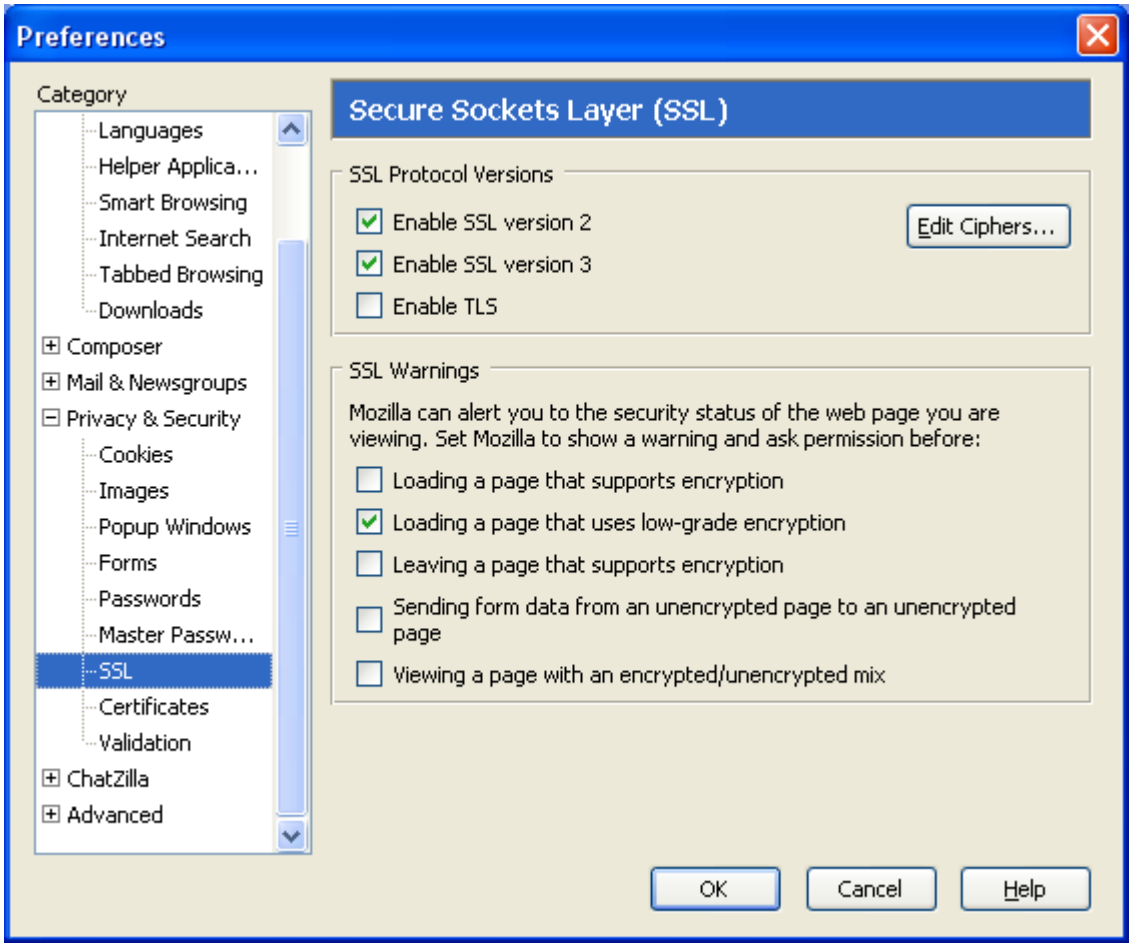


In **Mozilla 1.x**, go to Edit, Preferences, Advanced, Proxies. Fill in the **HTTP**, **SSL**, and **FTP** fields with the HTTP Proxy IP address and **port number** (usually **8080**). If you happen to use GOPHER, filling in that line as well will allow you to pass GOPHER requests through the HTTP Proxy.

The SSL field allows you to pass HTTPS (SSL) requests through the HTTP Proxy to secure web sites. As one example, this field needs to be filled in if you want authentication to WWW.HOTMAIL.COM.

The FTP field allows you browse PASV FTP servers using a browser. This is not the same as using FTP Proxy, which is used by true FTP clients, not browsers.

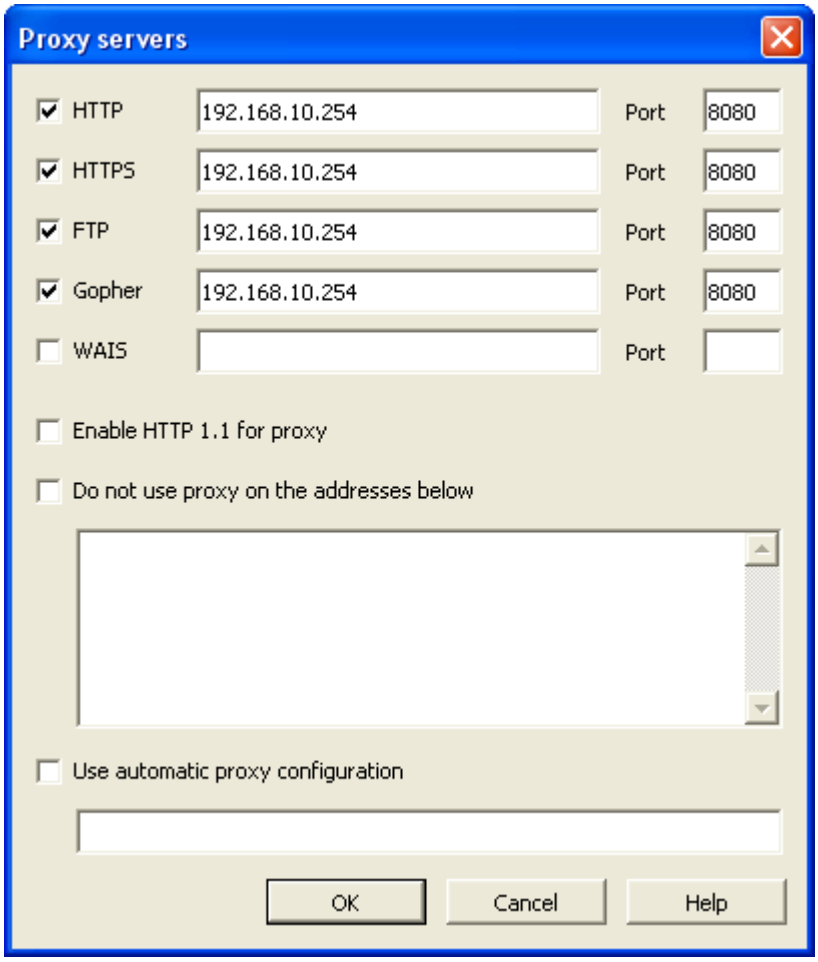
Note that the Socks field is left blank! Unless you happen to be using a SOCKS server, filling in the SOCKS field will cause your browser to have problems communicating.



Next, under **Edit**, **Preferences**, **Privacy & Security**, **SSL**, ***disable*** the **Enable TLS** option, if you intend to use SSL Proxy Authentication.

Unless either Mozilla changes things in a later version, or a BorderManager patch fixes the issue, attempting to use SSL Proxy Authentication may result in the cryptic error message '**Document Contains No Data**'. This same issue occurs with a number of browsers. Disabling TLS support generally makes proxy authentication work OK.

Opera 7



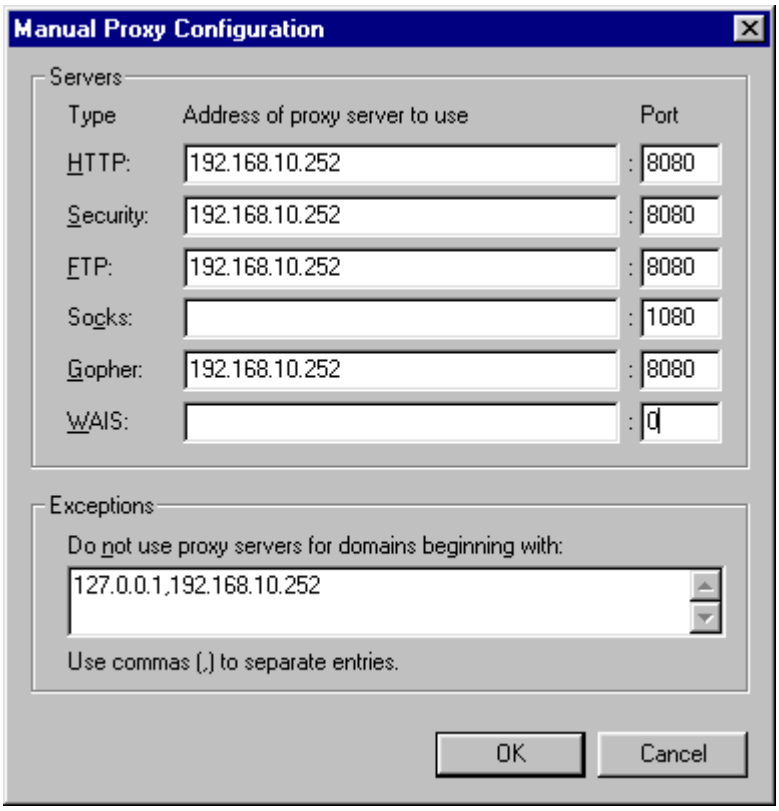
In Opera 7 (version 7.20 used for the example above), go to File, Preferences, Network, and click the Proxies button. You should then see the menu shown above. Fill in the **HTTP**, **HTTPS**, and **FTP** fields with the HTTP Proxy IP address and **port number** (usually **8080**). If you happen to use GOPHER, filling in that line as well will allow you to pass GOPHER requests through the HTTP Proxy.

The HTTPS field allows you to pass HTTPS (SSL) requests through the HTTP Proxy to secure web sites. As one example, this field needs to be filled in if you want authentication to WWW.HOTMAIL.COM.

The FTP field allows you browse PASV FTP servers using a browser. This is not the same as using FTP Proxy, which is used by true FTP clients, not browsers.

Note that the Socks field is left blank! Unless you happen to be using a SOCKS server, filling in the SOCKS field will cause your browser to have problems communicating.

Netscape 4.7



Netscape Navigator, (version 4.71 is shown here), is configured under the **Edit**, **Preferences**, **Advanced**, **Proxy**, **Manual Proxy Configuration** menu. Fill in the **HTTP**, **Security**, and **FTP** fields with the HTTP Proxy IP address and **port number** (usually **8080**). If you happen to use GOPHER, filling in that line as well will allow you to pass GOPHER requests through the HTTP Proxy.

The Security field allows you to pass HTTPS (SSL) requests through the HTTP Proxy to secure web sites. As one example, this field needs to be filled in if you want authentication to WWW.HOTMAIL.COM.

The FTP field allows you browse PASV FTP servers using a browser. This is not the same as using FTP Proxy, which is used by true FTP clients, not browsers.

Note that the Socks field is left blank! Unless you happen to be using a SOCKS server, filling in the SOCKS field will cause your browser to have problems communicating.

It is a good idea to add the private IP address of the BorderManager HTTP Proxy to the Exceptions field. In some cases, adding this entry will prevent a problem with SSL Proxy Authentication, should

you be using that. It may also help with certain issues to add the loopback address 127.0.0.1 to the **Exceptions** menu.

Netscape Navigator settings are stored in a PREFS.JS text file, which can be modified in various means (like ZENworks applications) if necessary.

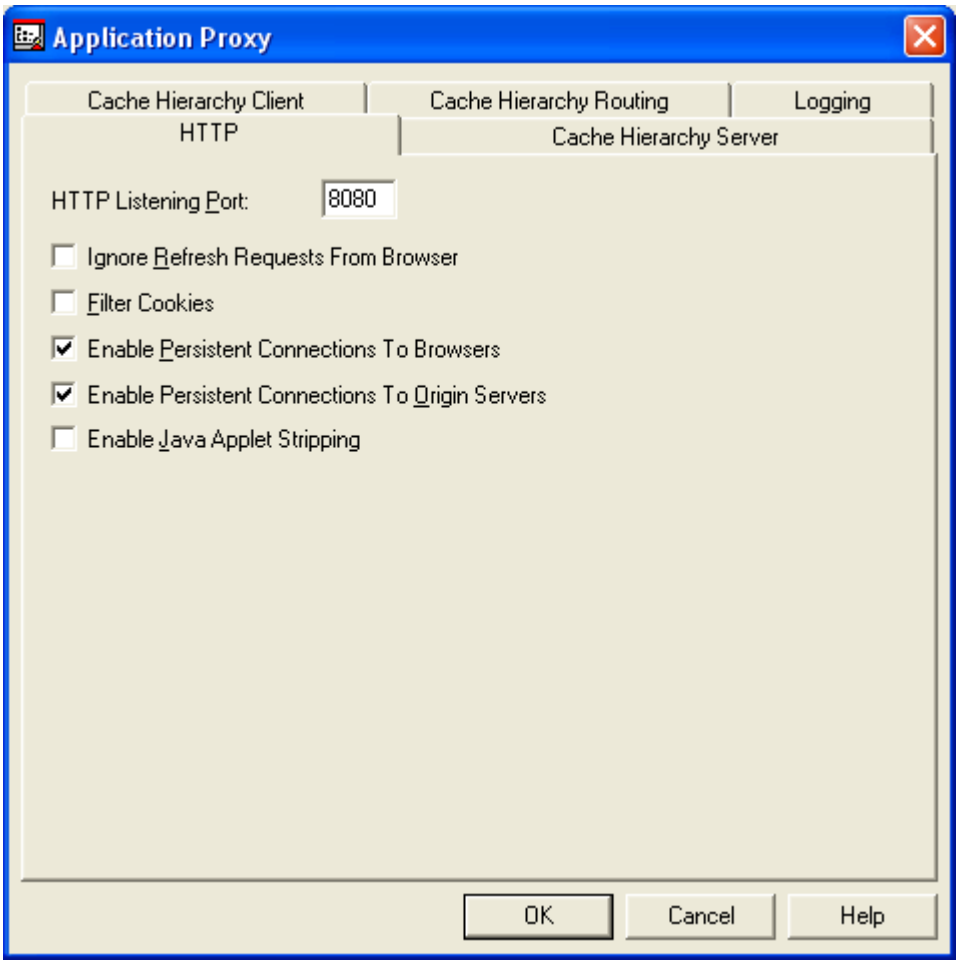
HTTP Proxy Details

The following parameters are configured by selecting the HTTP Proxy, and then clicking on the **Details** button on the BorderManager Setup main menu in NWADMN32.

HTTP

From the BorderManager Setup main menu, select the **HTTP Proxy** check box to enable HTTP web proxy caching.

The following screens show the options configured when selecting the **Details** button for the HTTP Proxy.



Select **HTTP Proxy** and click on **Details** to get the above screen. Most users accept these default values.

The **HTTP Listening Port** number is normally left at port 8080. This port number must also be configured in the browser proxy settings.

The **Ignore Refresh Requests From Browser** option is normally left unchecked. Checking this box causes the HTTP Proxy to ignore Reload requests from the browser. Normally, a Reload request from the browser will cause the HTTP Proxy to clear old cache data and immediately download a new page.

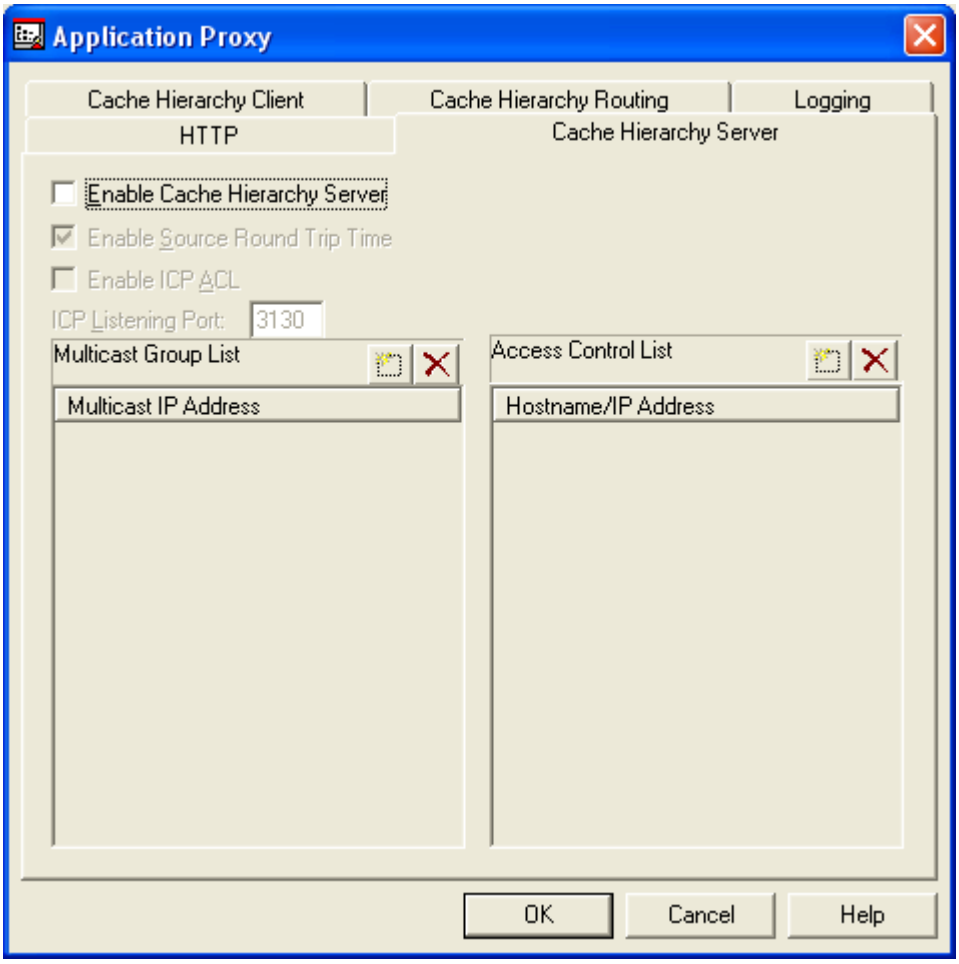
The **Filter Cookies** option is normally left unchecked. Checking this box will cause the HTTP Proxy to filter all cookie requests to the browser, and would result in many web services relying on cookies to fail.

Enable Persistent Connections To Browsers is normally enabled. This option is a performance-enhancing feature which greatly reduces the time and traffic needed for the HTTP Proxy and a browser to re-establish communications by maintaining keep-alive traffic. Should you have problems with connections to particular web sites, try disabling this option to see if things improve.

Enable Persistent Connections To Origin Servers is normally enabled. This option is a performance-enhancing feature which greatly reduces the time and traffic needed for the HTTP Proxy and an origin web server to re-establish communications by maintaining keep-alive traffic.

Enable Java Applet Stripping is normally left unchecked. Enabling this option will improve security, but also cause web pages requiring Java applets to be downloaded to the browser to fail.

Cache Hierarchy Server

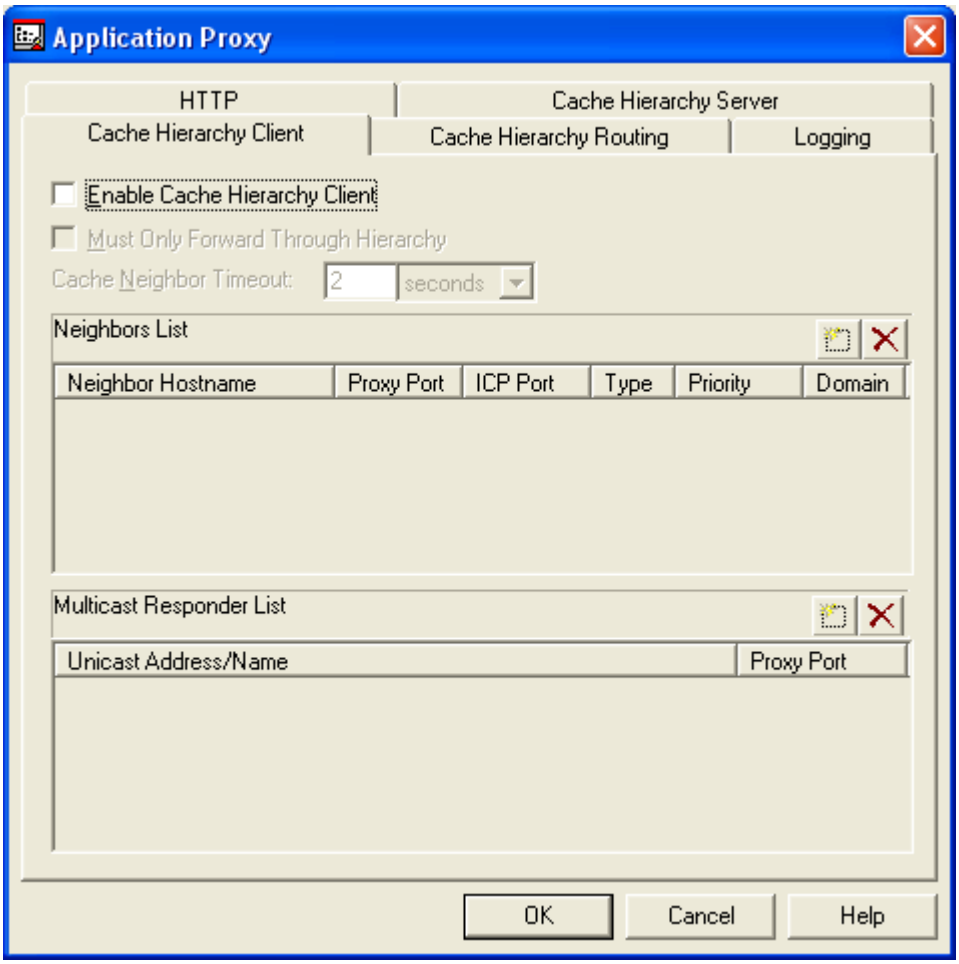


Leave these settings at the default (nothing selected), unless you want to have this server act as a parent server in a caching hierarchy. (Caching hierarchy is explained in more detail elsewhere in this book).

Cache Hierarchy Client

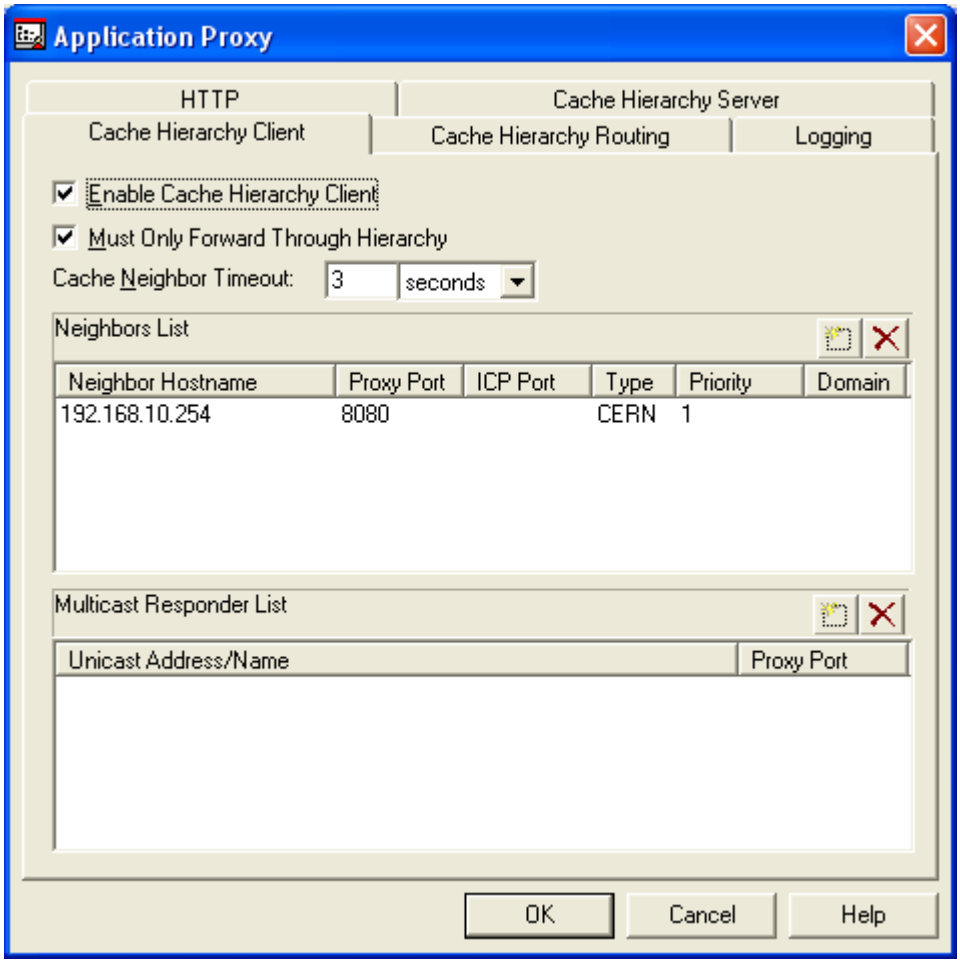
If you do not want to forward HTTP requests through another proxy, leave the Cache Hierarchy Client settings blank, or do not check the box labeled '**Enable Cache Hierarchy Client**'.

No Cache Hierarchy



The default values are all blank.

Cache Hierarchy Client Set

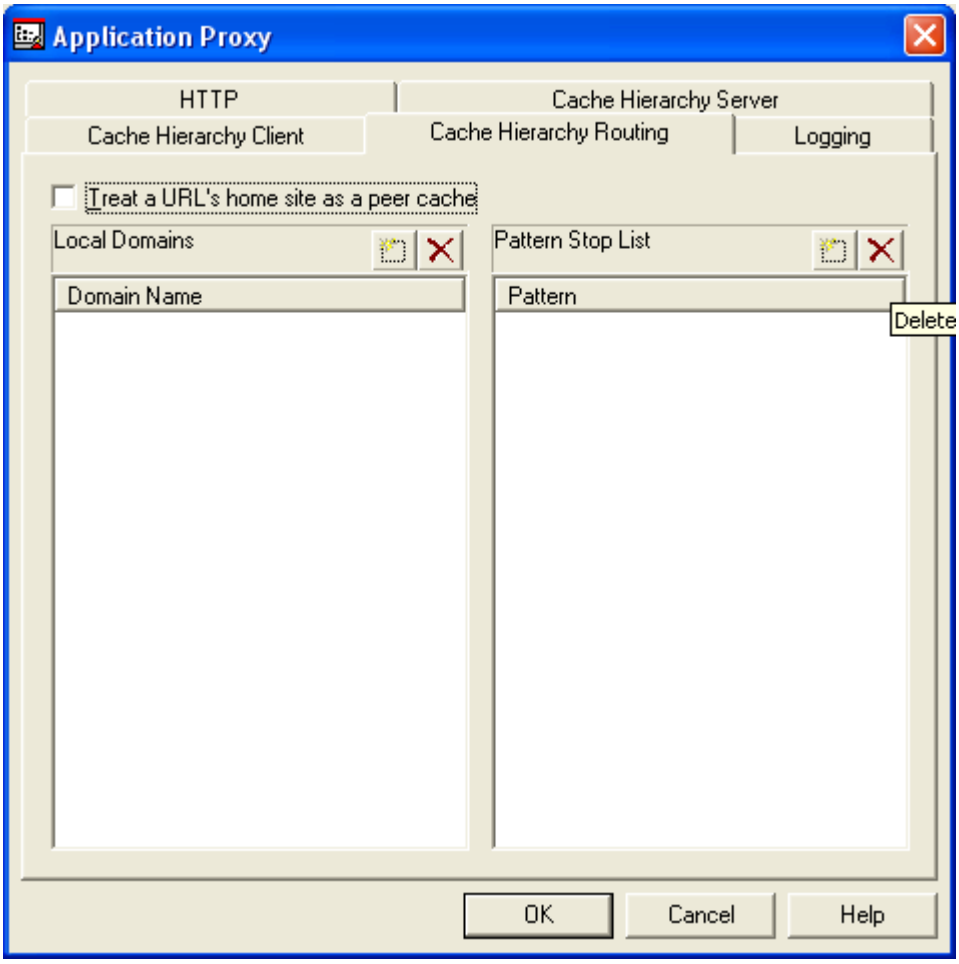


In the example shown, an HTTP Proxy has been configured to forward all HTTP requests through an 'upstream proxy' using the CERN protocol. The upstream proxy is located at 192.168.10.254, and it is listening for requests on proxy port 8080. (This configuration is shown in the Scenario 9B in Chapter 2. This screenshot was taken from BORDER2, which points to the HTTP Proxy address of BORDER1, and accesses that proxy via Site-to-Site VPN).

One reason for using a BorderManager server as a cache hierachy client is to point the server to your ISP's caching server when they are doing content filtering for you. Another reason is if you have remote offices connected to the Internet through WAN links to a central office, and you have BorderManager servers in each location.

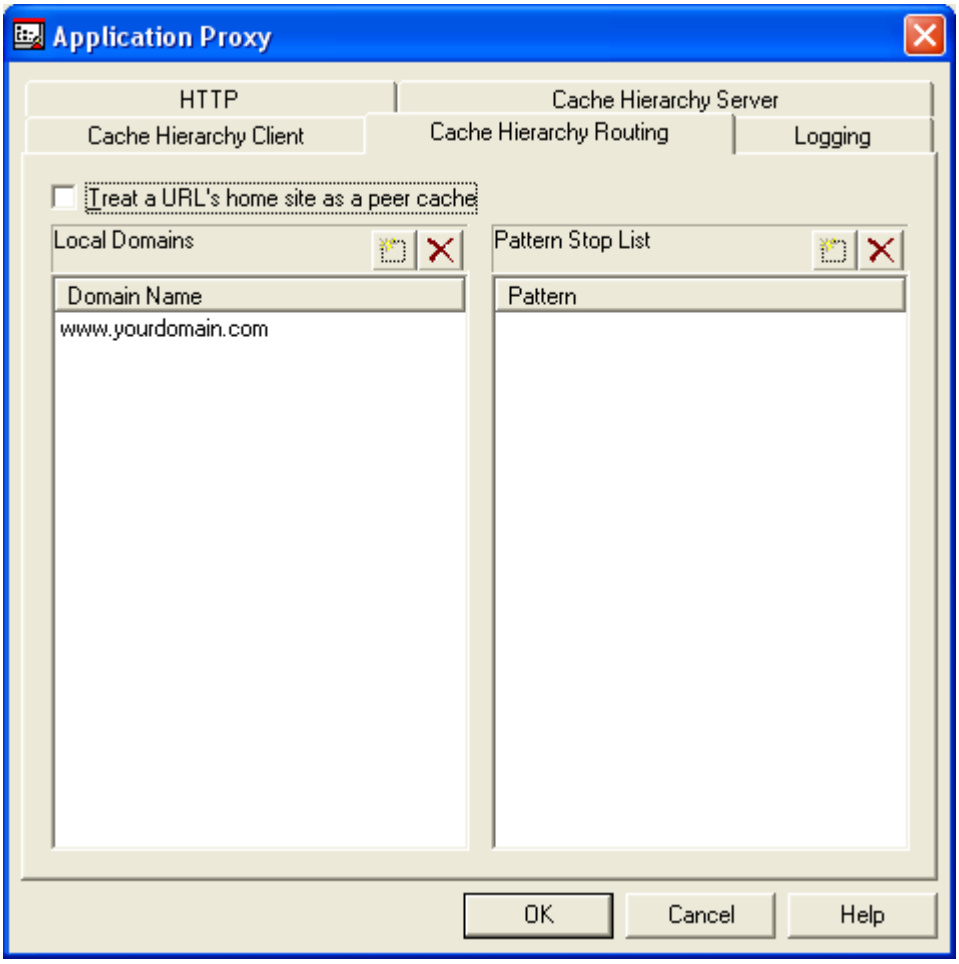
Cache Hierarchy Routing

No Cache Hierarchy



The default values are all blank.

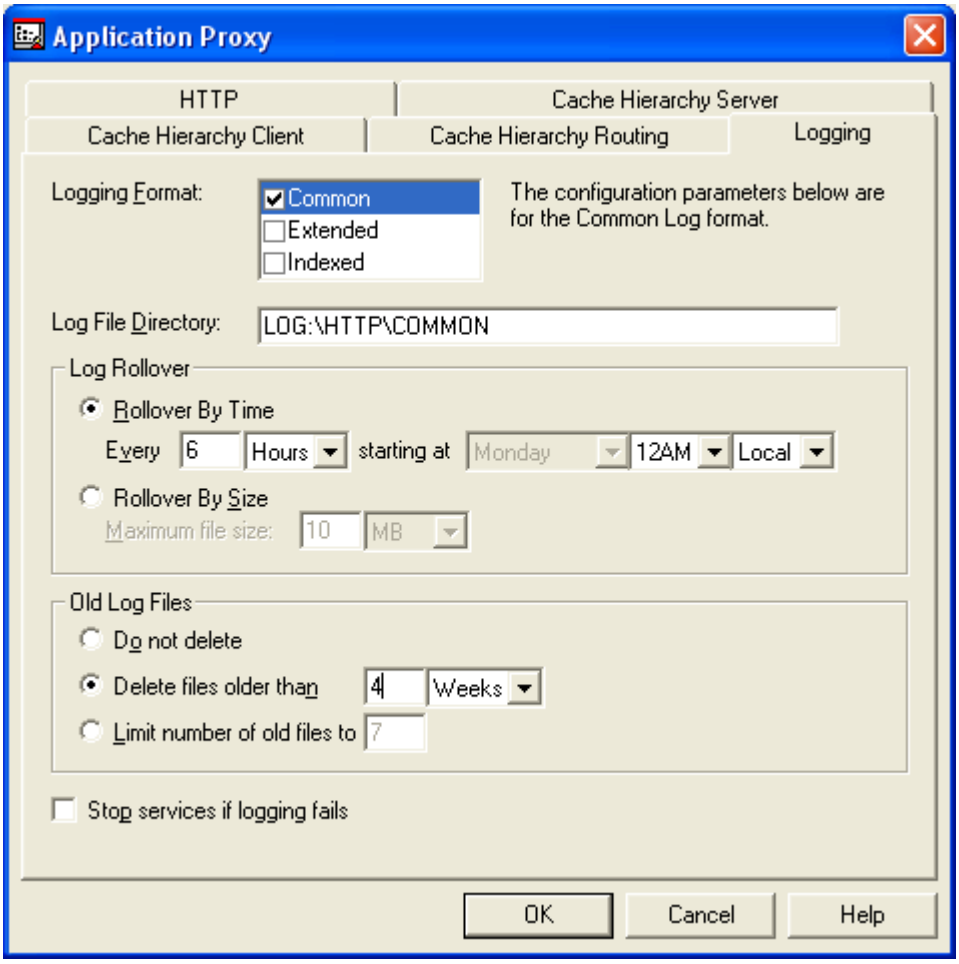
Cache Hierarchy Configured



In the example shown, a single web site has been configured as a local domain in regard to cache hierarchy routing. The **Local Domains** entries allow you to specify individual addresses that are to be accessed without going through an upstream proxy. These settings are to allow you to set up exceptions for the proxy so that no cache hierarchy routing is used. The **Pattern Stop List** can be used to specify additional exceptions based on addressing patterns rather than individual URL's.

Logging

Common Logging



Click on the **Logging** tab, and check **Common** logging. For common logging, change the **Log File Directory** to LOGS:\HTTP\COMMON.

Select the **Rollover By Time** option and change the default to roll the log files every 6 hours, or some option that is appropriate for your environment. You may find it useful to roll files more often as the latest file in use will be held open by the server, and some analysis programs may have problems reading a file held open.

Select **Delete files older than**: 4 Weeks to keep some old log files around. You may wish to shorten or lengthen this value depending on the size of the log files created.

CAUTION *Do not leave the Old Log Files option set to the default of 'Do not delete', and the log files set to the default SYS volume as you may eventually run the SYS volume out of space!*

Please refer to the Logging chapter later in this book to see ways of analyzing the common log files.

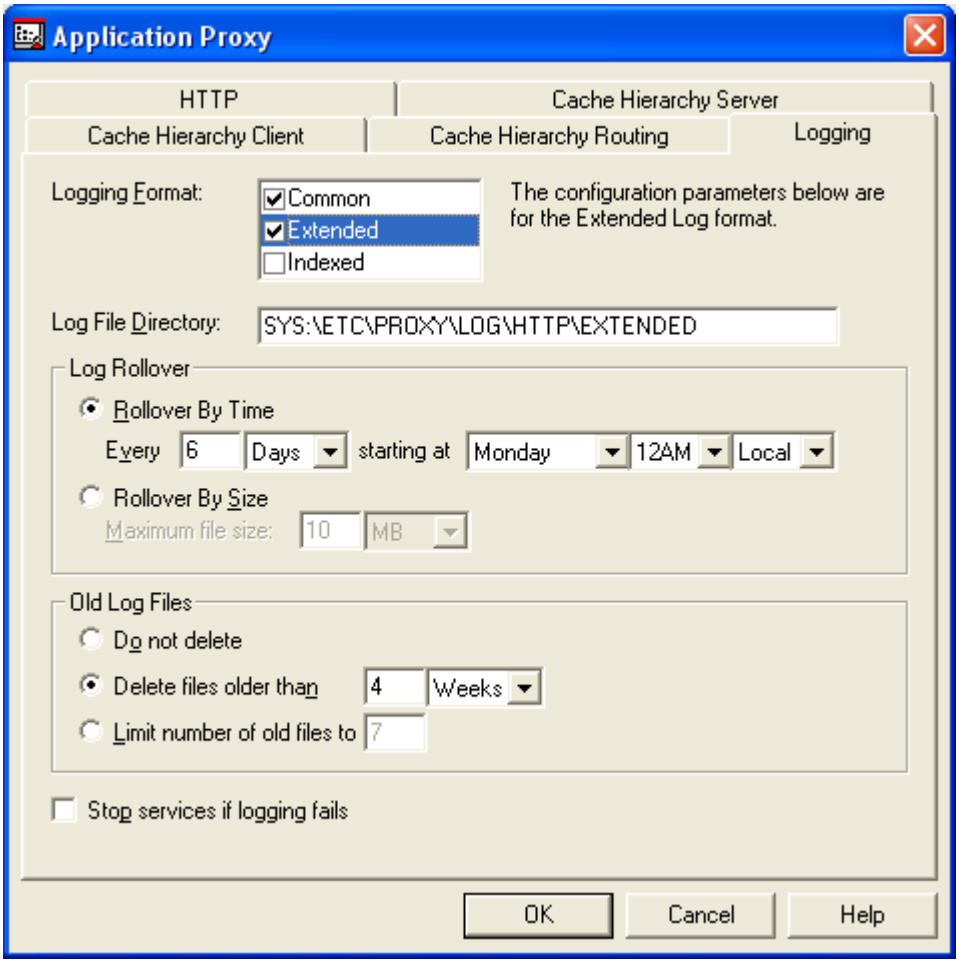
If you want to see additional data in the logs, you can either enable Extended logging or both Common and Extended logging. Note that enabling both Common and Extended will create two sets of log files, and they can get pretty large.

I **do not recommend** enabling Extended logging unless you have a program that recognizes the formatting used by Novell in the Extended log files. Otherwise you will be wasting disk space without being able to analyze the log files.

As of this writing, the only program I have heard of that reports compatibility with BorderManager extended log files is Webspy.

Note You should not allow the Common log files to be created on the (default) SYS volume unless you keep a very close eye on the amount of space the log files are using. I recommend setting up a dedicated log volume and directing all common log files there.

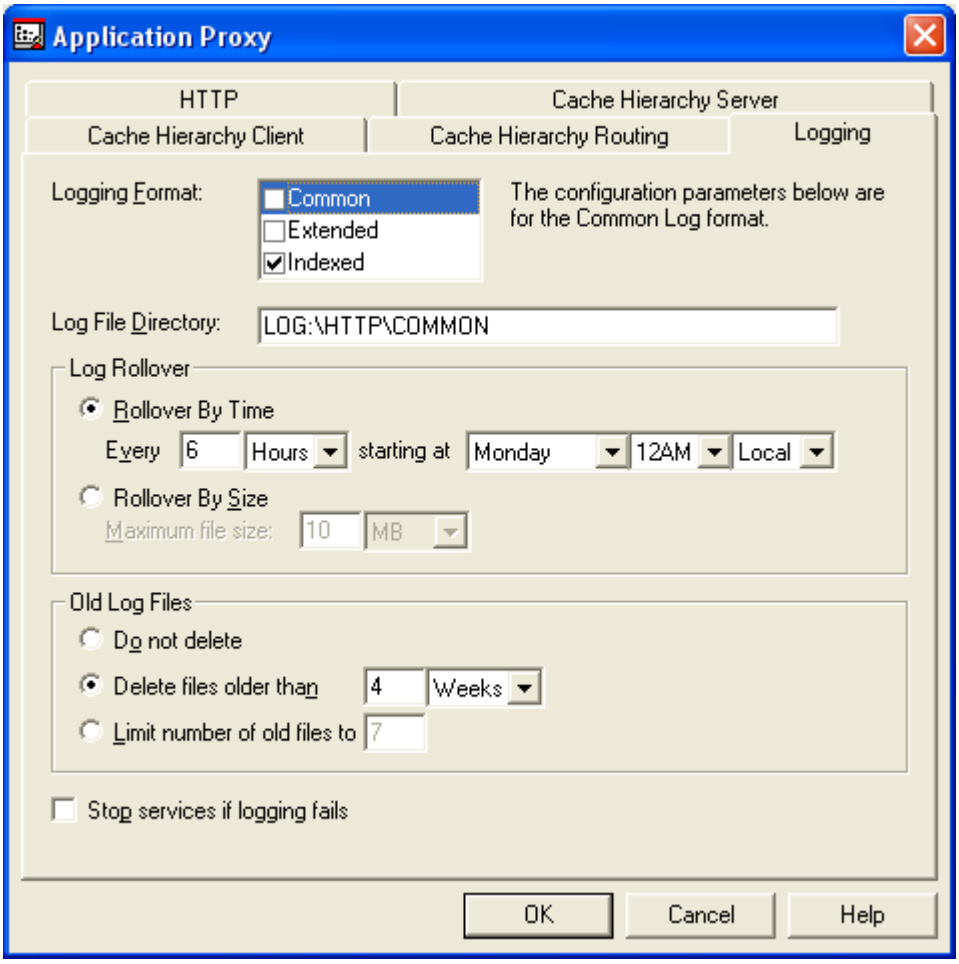
Extended Logging



Extended logging can be enabled by checking the **Extended** box, though it may do you little good as the note below indicates. It is worth noting that the Extended log files do **not** automatically get created in the same location as the common logs.

Note At the time of this writing, there are very few programs which support the extended log format used by BorderManager. I recommend that you do not enabled Extended logging.

Indexed Logging



Several options in BorderManager can have a choice of indexed logging. Some ONLY have a choice of Indexed Logging, such as FTP Proxy logging. Indexed logging uses Btrieve to store data, and the only way to view that data is to export the data from within NWADMN32. I do not recommend enabling Indexed logging for the HTTP Proxy.

There are a number of issues to consider when using Indexed logging.

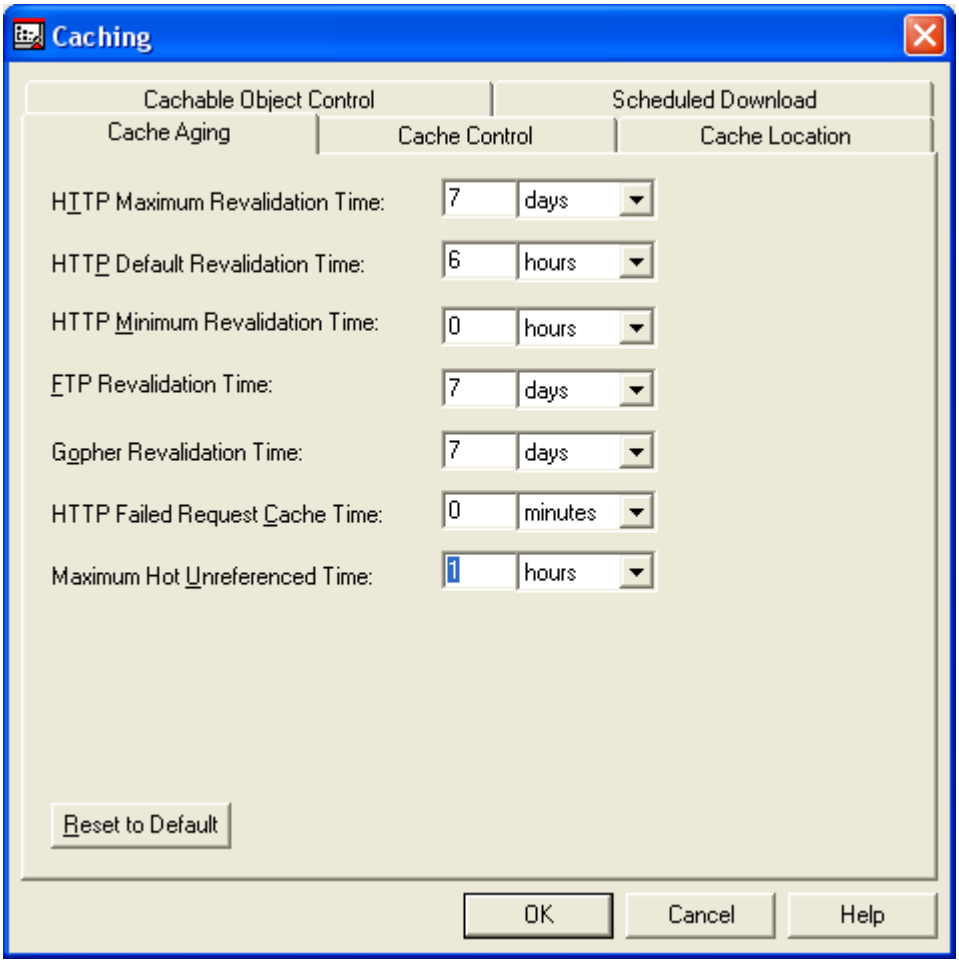
- Indexed (and Access Control) logs are the only kind of log files that can be viewed (or exported) in the NWADMN32 logging screens.
- You have **no control over the location** of the log files, which are kept in the SYS:\SYSTEM\CSLIB directory. (All of the Indexed Log files, VPN, Proxy, Gateway, etc, are kept in this directory).

- You have **little control over the size** of the log files, which can get quite large. You can somewhat control the log file size using the CSAUDIT command. See Novell TID 2938132, "Managing the proxy cache log files". Type CSAUDIT at the console prompt and look at the menu options. Do not type 'LOAD CSAUDIT' as you will get something completely different!
- Because the log files are kept in Btrieve format, **you cannot read the log files directly**, and there are no third-party applications that can read them.
- NWADMN32 can read and export the log file data, but it **can be very slow** pulling the data out of the log file.

HTTP Proxy Caching

The following parameters are configured by selecting the **Caching** button on the BorderManager Setup main menu in NWADMN32.

Cache Aging

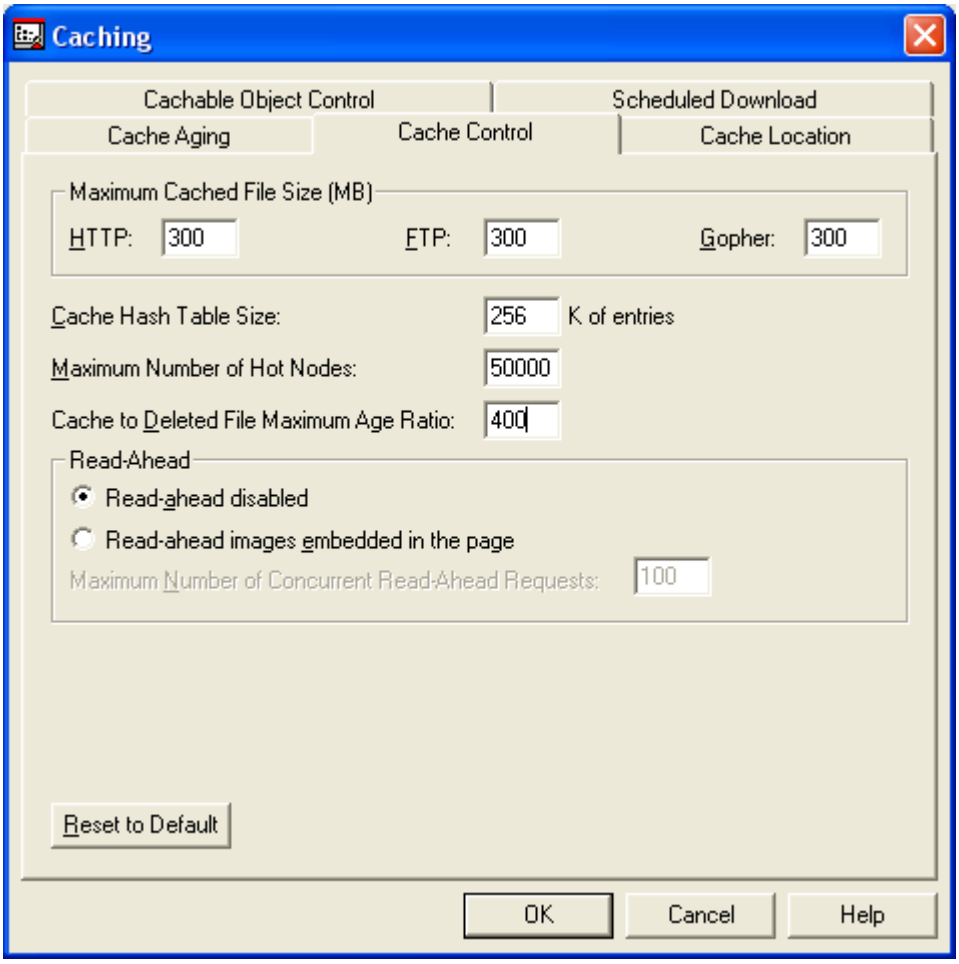


From the BorderManager Setup main menu select the **Caching** button to configure caching parameters.

You can accept the defaults from the Cache Aging window, but if you want to tune a BorderManager server more aggressively, you might want to change the **Maximum Hot Unreferenced Time** from **30** minutes to **1** hour. This change assumes you have an adequate amount of RAM to hold data in memory for a long time. BorderManager servers like lots of RAM when tuned for aggressive performance!

Cache Control

Click on the **Cache Control** button to change default parameters for cache control.



If you have a lot of traffic, a reasonably fast Internet connection (T1 or faster), and a good-sized cache volume, consider changing the default values from 30MB for HTTP, FTP and GOPHER **Maximum Cached File Size** to something considerably larger, like 300MB. (Files larger than these settings will be passed through uncached).

If you have very large cache volume(s), with a lot of cached data, according to Novell, you may benefit from increasing the **Cache Hash Table Size** from the default of 125 to a higher number, such as 256. Probably 'a lot of cached data' means more than 4-5GB of cache.

Change the **Maximum Number of Hot Nodes** to 50000. This allows many more open files to be used, which will speed up cache performance under heavy load. This parameter must also be paired with certain SET parameters on the server to allow more than the default hot nodes to be used. (See Novell TID 10018669,

"BorderManager PROXY Performance Tuning", which has been summarized in the chapter "Performance Tuning" later in this book, along with my comments.

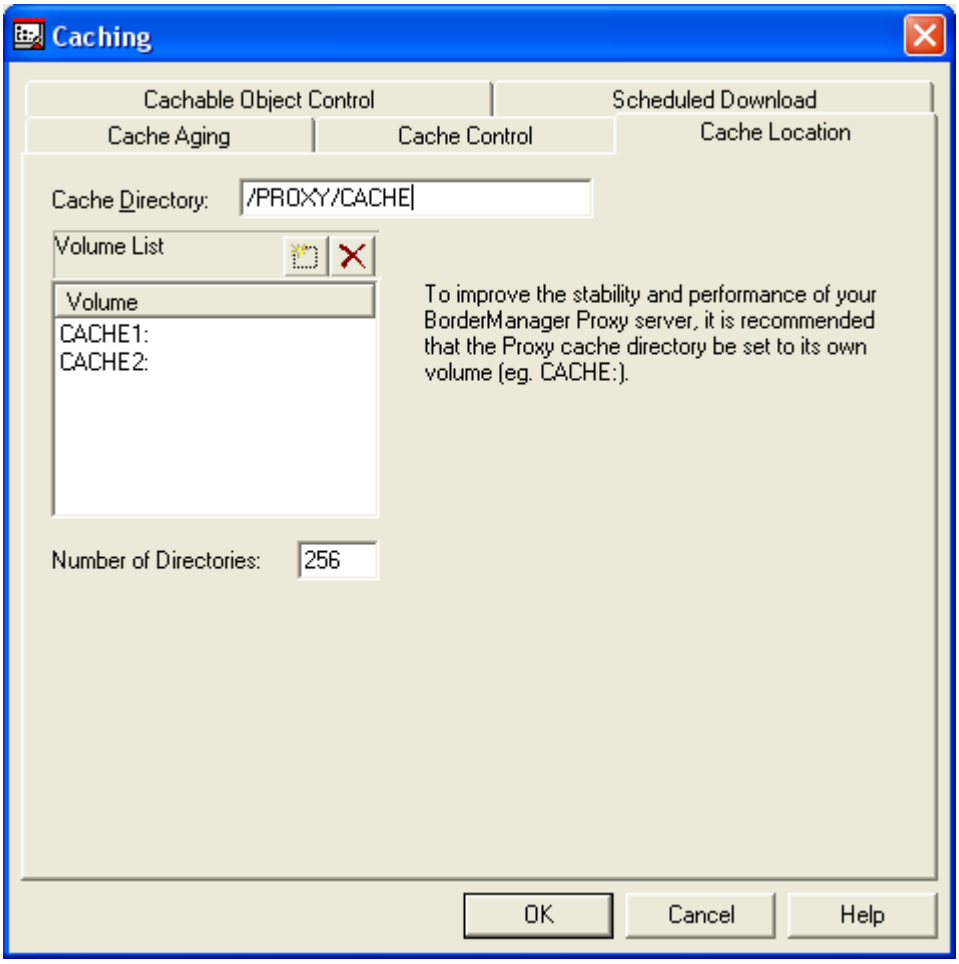
CAUTION ***Caution!*** *Do* ***not*** *enable read-ahead in most BorderManager servers, unless you extensively test the results. Many BorderManager servers suffer from a bug that causes ALL data to be cached, including data that should not be cached, when read-ahead is enabled. The problem will cause issues with particular web sites, often involving a login of some kind. This situation may change with patches, but the problem was widespread as of this writing. Unpatched BorderManager 3.0 servers also have a bug that can cause the HTTP Proxy to continuously loop back and request the same web page over and over if there is a broken link on the page. The read-ahead setting generally improves performance, but it is critical to apply the latest BorderManager patches to avoid the bug, which can appear to the web site's ISP as a denial of service attack, and to you as a large waste of bandwidth.*

Note Many changes to caching parameters do not go into effect unless you reload PROXY.NLM. If in doubt, restart the server, or unload and reload PROXY.NLM.

Cache Location

CAUTION **This is a very important section! You should never leave the cache location on the default volume (SYS)!**

Click on **Cache Location** to specify where the cached HTTP (and FTP) files are to be stored.



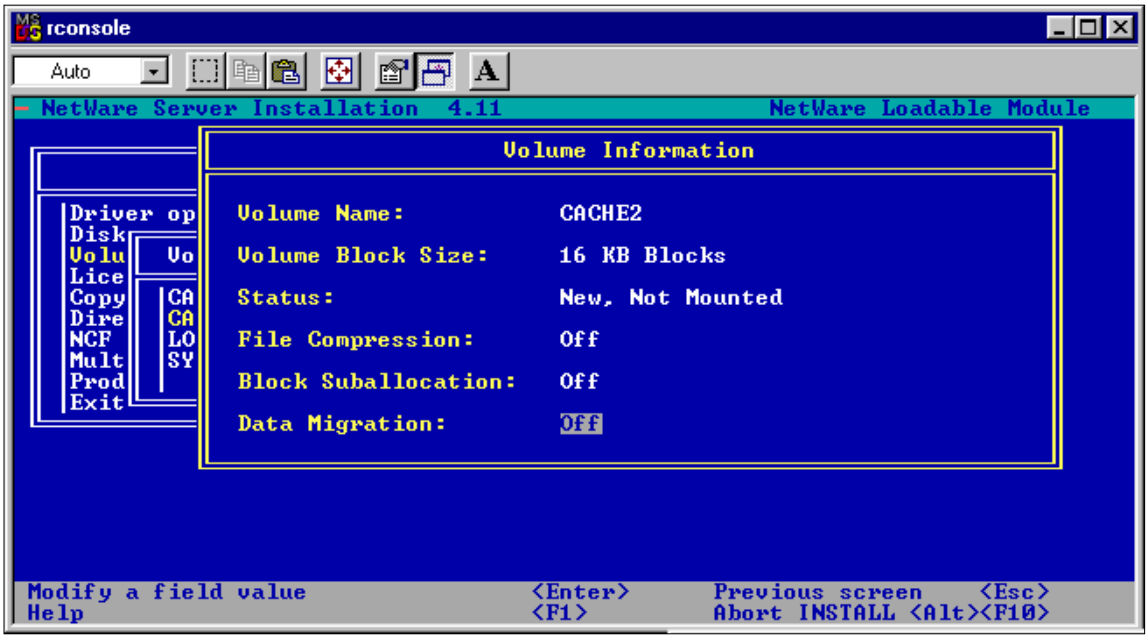
One of the **most critical changes** to the default settings for BorderManager is contained on this menu! It is vital that **the Cache Directory be set to other than the default SYS volume**. You must have a **dedicated volume** set up for the web proxy cache to use so that the SYS volume doesn't run out of disk space.

Rather than set up one huge cache volume, you will generally get better performance by setting up multiple smaller cache volumes. I recommend capping a cache volume at about 4-5GB. If you have 18GB of space available for caching, try setting up four cache volumes equal to 4.5GB each.

The **Number of Directories** should be no less than 64 per cache volume. This number represents the number of directories used to hold the cached files, and a large cache can have several thousand individual files in each directory. More directories splitting the cached files up should improve performance somewhat. A value of 128 per cache volume has worked well for many people. The total number of directories entered here will be divided up between each volume. BorderManager also may round up to a higher value than you enter, using multiples of two and based on the number of volumes in use. (In other words, BorderManager will actually use a number like 512, etc, even though you enter a value of 400. You can see the number of cache directories created on the proxy console screen at the server).

Note When setting up the HTTP Proxy cache location, for BorderManager 3.0 you must create the initial directory (in this case you must manually create the CACHE1:PROXY\CACHE and CACHE2:PROXY\CACHE directories). BorderManager 3.5 and later will automatically create all the subdirectories needed according to the cache location parameters.

CAUTION *A dedicated, traditional cache volume should be set up with 8K or 16K block size, no suballocation and no compression enabled for correct caching performance. Only DOS name space should be used on a cache volume. LONG name space can be removed using VREPAIR. If you do not have any free space to create a traditional partition and cache volume (all space used in a single large NSS partition, for example), I recommend adding another drive for cache, or reinstalling the server from scratch to leave space for a traditional cache volume!*



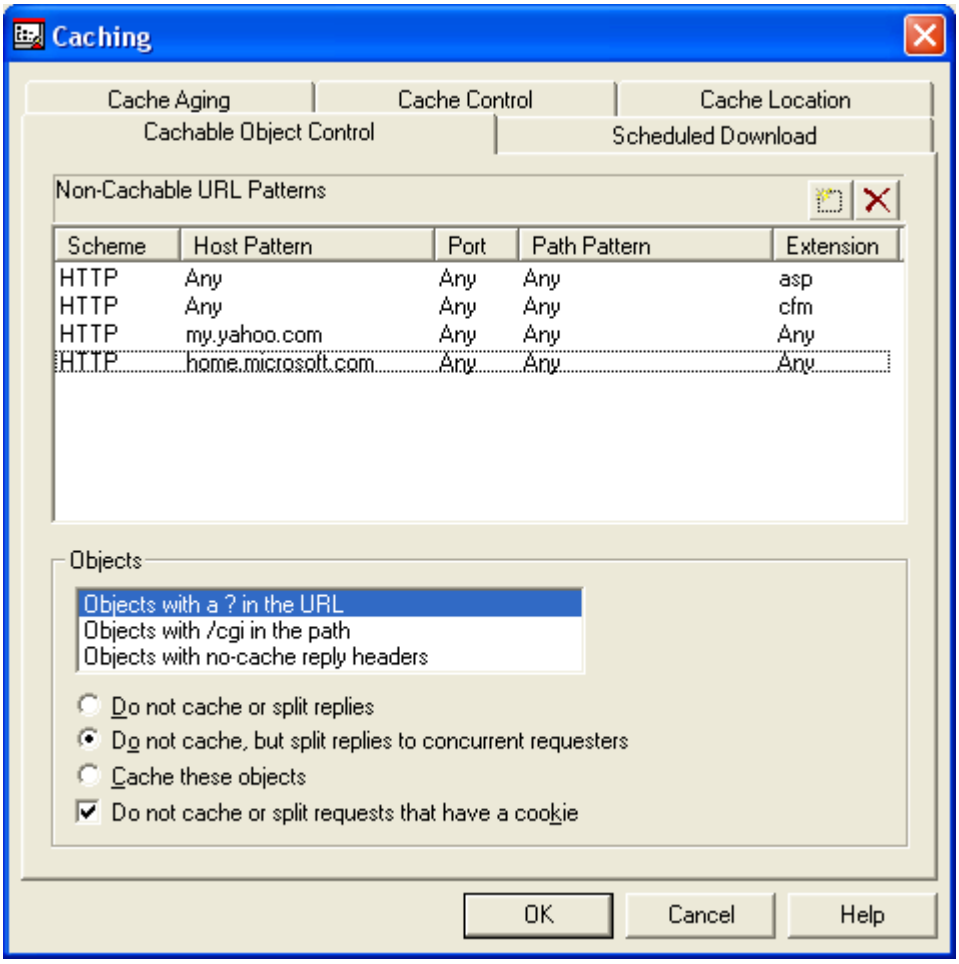
The example above shows the volume settings to use when creating a cache volume. I do not recommend using NSS volumes for caching, as you will certainly see issues with caching (such as incomplete page displays) if you do. The BorderManager caching engine was designed with low-level access to traditional volumes in ways that enhance performance, but which are not replicated in NSS volumes.

You must use VREPAIR to remove LONG name space in NetWare 5.x./6.x NetWare 5.x/6.x volumes are created with LONG name space enabled by default, unlike NetWare 4.x. You cannot remove name spaces or change NSS volume parameters at all. It is not really critical to remove LONG name space, but it will increase memory efficiency.

If you did not set up the server with dedicated volumes for caching or logging, you may be able to use a third-party utility to reduce the size of existing volumes to free space to create new volumes. However, as of this writing (Apr. 2004), I am unaware of any utility that can shrink a NSS partition to make space for a new Traditional partition.

Cachable Object Control

Select the **Cachable Object Control** tab to set patterns not to be cached by BorderManager.



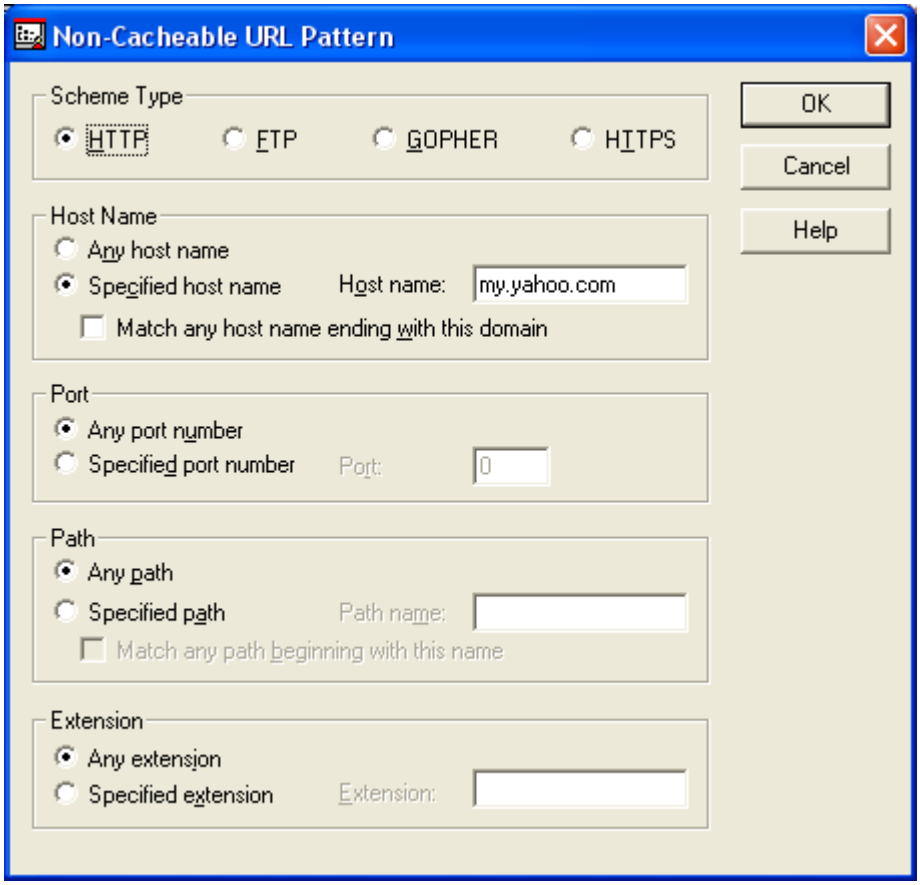
You may leave the settings at the bottom of the menu at the defaults, but consider adding the following patterns:

- HTTP URL – any 'personalized' portal type web sites like my.yahoo.com or home.microsoft.com, (To avoid one person getting another's personal page from cache).
- Extension ASP – do not cache any web pages that end in .ASP. BorderManager might have problems with Active Server Pages if you try to cache them.
- Extension CFM (Cold Fusion) extensions is a good entry to add. Caching CFM pages can result in issues logging in to some web sites.

Note The entries you configure here will not be cached AFTER you make the entries, but if you have already browsed to them, entries will already be in cache. You may need to clear the cache data by unloading PROXY.NLM, and then using a LOAD PROXY –CC command (clear ALL cache entries).

Entering a Non-Cacheable URL Pattern

The following example shows how to configure the proxy not to cache a certain request.



Enter a host name, port number, path, etc, not to be cached.

Note: If you have **already browsed** to a site that you now mark as non-cacheable, you will not see an immediate effect from making this change. That is because there is already data cached for that site. Unless you want to wait for the site to age out of cache, you should clear the cached data. The only way to do that is to clear ALL the cached data when you load PROXY.NLM.

Clearing the Proxy Cache

Here is the sequence to manually clear not only the cached data, but also the cached DNS data for the site (in case the cached DNS data is incorrect).

1. UNLOAD PROXY.NLM
2. For BorderManager 3.0, or BorderManager 3.5 and 3.6 servers not running the latest proxy patches, delete the SYS:\ETC\PROXY\PXYHOSTS file. This file holds cached DNS data. You only need to delete this entry if you think you also have a bad DNS name in cache.
3. LOAD PROXY –CC

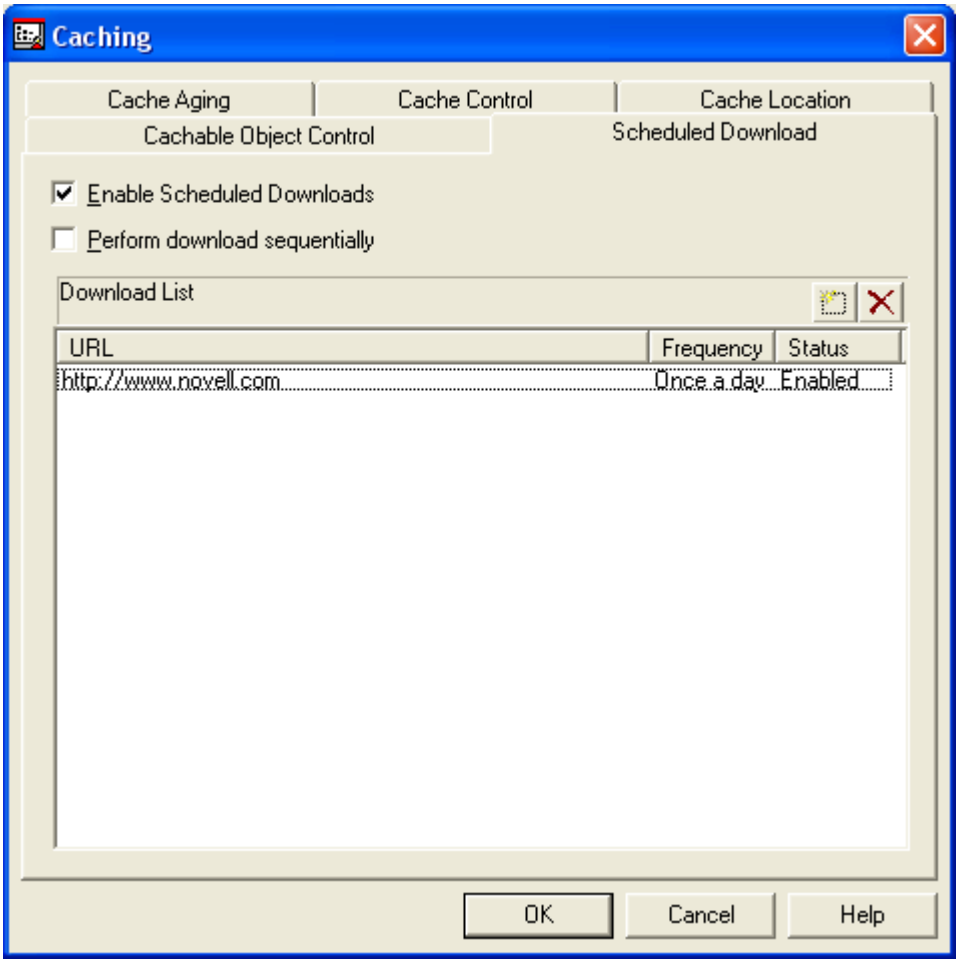
Note A faster way, to be used only when the cache is on a dedicated volume (and you should ALWAYS have the cache on a dedicated volume), is to delete and recreate the cache volume itself. Clearing the cache with the –CC option can be fairly slow on large cache volumes with many cached nodes.

Scheduled Downloads

You can pre-cache web sites on a periodic basis at selected times of the day. This maximizes available bandwidth during normal working hours and allows much faster browsing of typically used or overloaded slower sites.

Note You must check the **Enable Scheduled Download** box to be able to manually pre-cache data from the server console, using the "Proxy" console screen, option 22. That option allows you to immediately pull data into cache (one time) from a URL.

Select the **Scheduled Download** button to configure periodic pre-cache downloads.



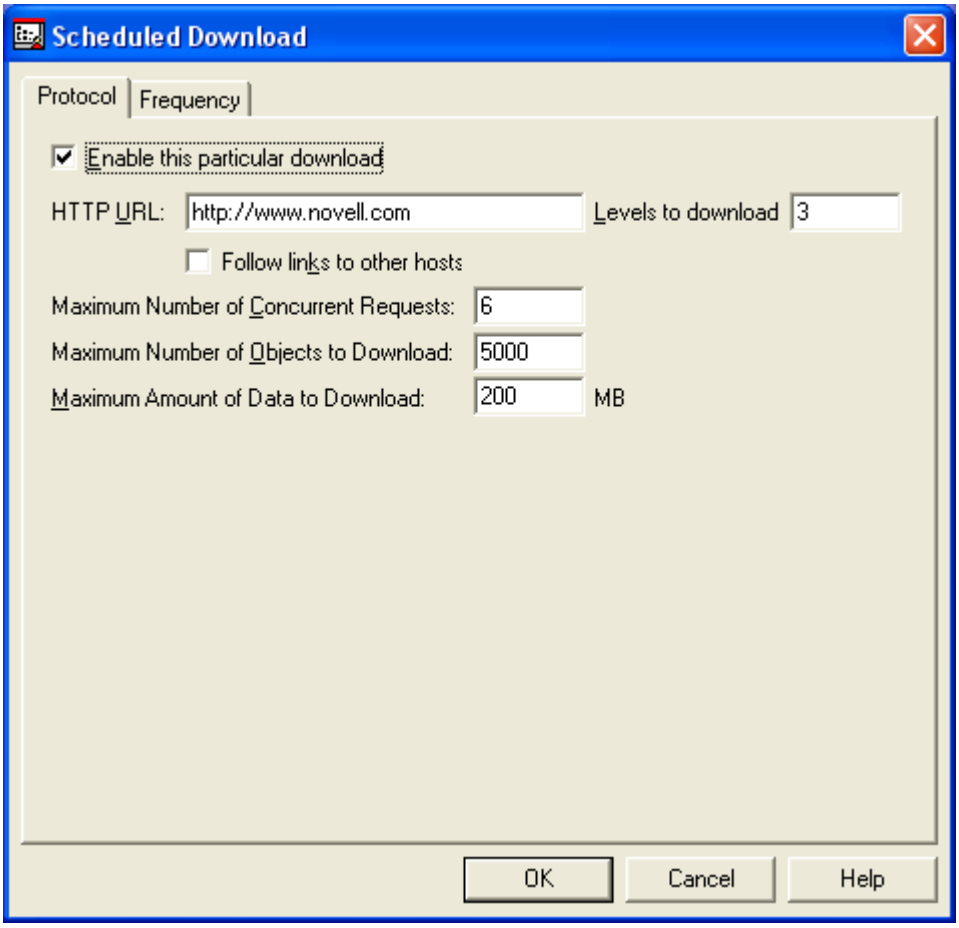
Several sites may be set up for scheduled downloading. The effect of downloading a site automatically is usually to shift some internet bandwidth usage to the middle of the night.

Click on individual sites to view the parameters used.

Downloading sequentially will prevent multiple scheduled downloads from happening all at the same time, taking all available bandwidth.

Entering a URL to download on a schedule

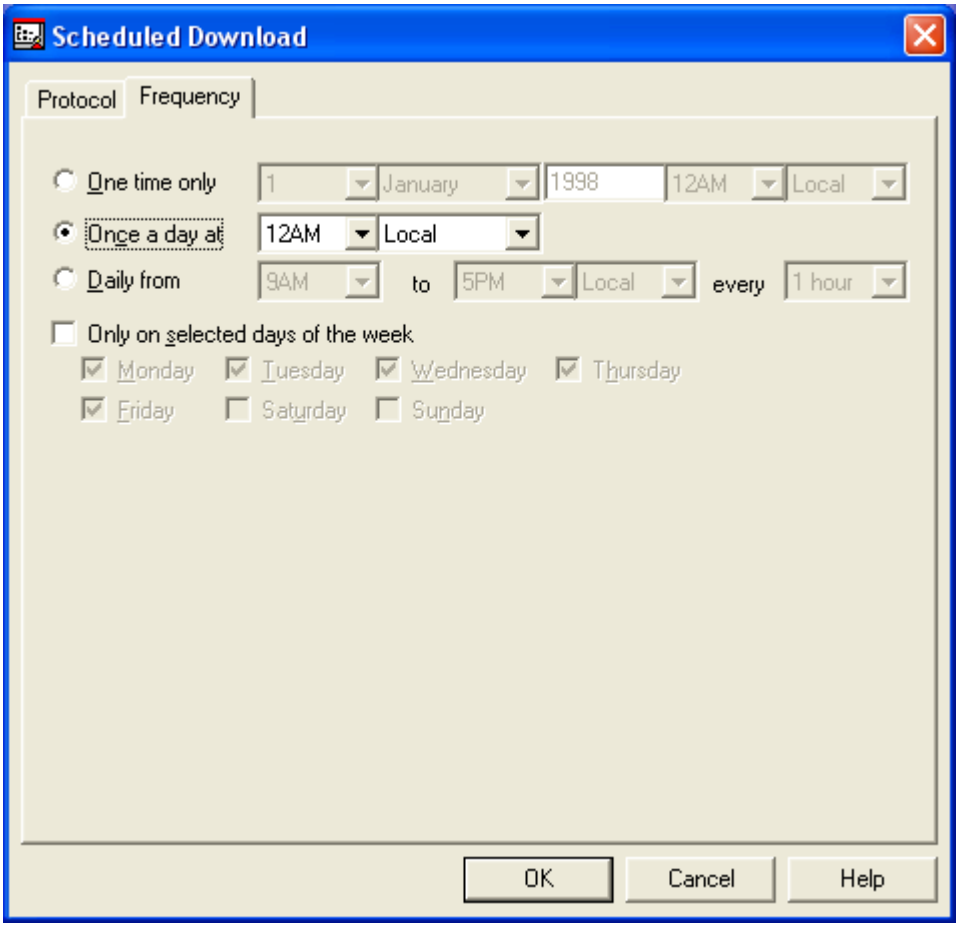
Clicking on the icon to add a URL brings up the following menu:



Type in the name of the site to be downloaded, and the number of links (how many levels deep) to follow. It is generally *not advisable* to follow links to other hosts due to the high amount of traffic that could result.

Click on **Frequency** to set the schedule for the download.

Set Download Frequency



Pick a periodic schedule or a one-time value to be used for downloading the site. Try not to schedule different large sites to download at the same time.

Click **OK** to save the scheduled download settings.

HTTP Proxy - SOCKS Client

Concept

The HTTP Proxy can act as a SOCKS client to a SOCKS server in order to allow browsing in an existing SOCKS environment. This option would only be used when the BorderManager server is forced to access the Internet through a SOCKS server.

Pros

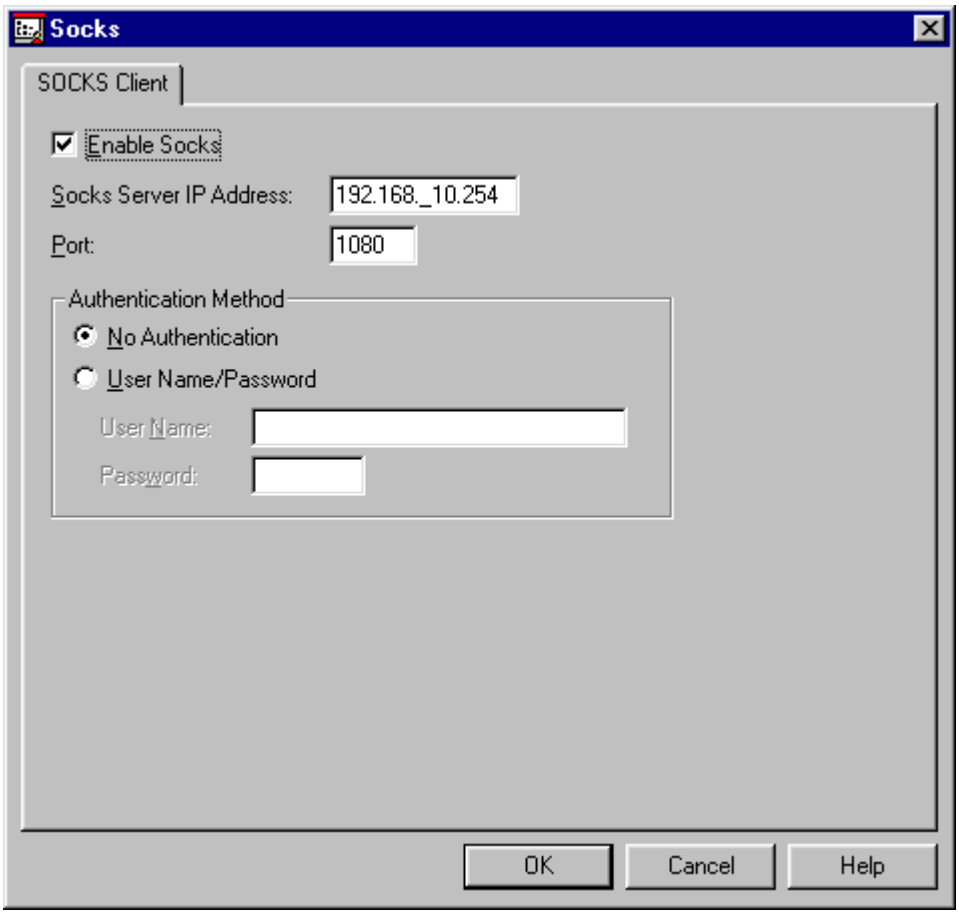
If the only method of accessing the Internet is through an upstream SOCKS server, this option will allow you to get HTTP Proxy access to the Internet.

The SOCKS client option is not the same as making the BorderManager server a SOCKS Gateway, which can be done in the Gateway option at the BorderManager Setup main menu.

Cons

SOCKS client only works for HTTP Proxy, meaning that only browsing access will function when the BorderManager server must access a SOCKS server in order to connect to the Internet.

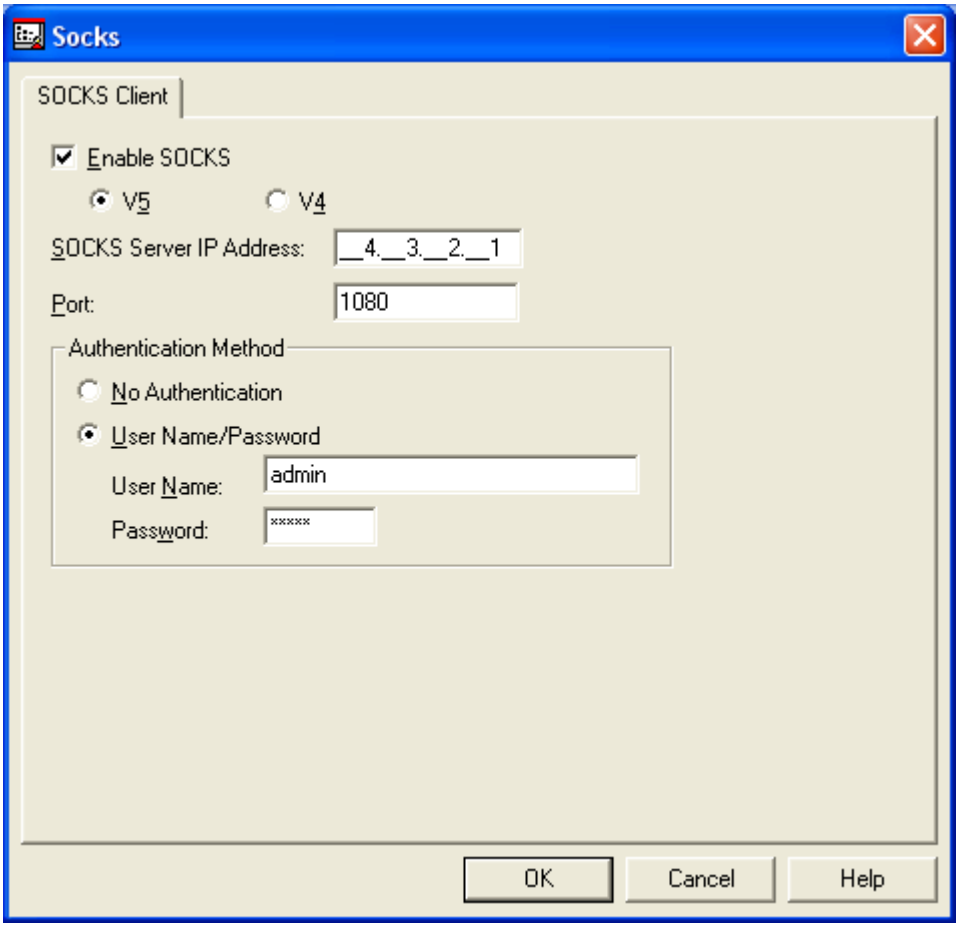
In the BorderManager Setup main menu, highlight the HTTP Proxy, and then select **SOCKS Client**.



In the example shown, a BorderManager 3.0 server is configured to act as a SOCKS client to a SOCKS server at 192.168.10.254. Authentication to that SOCKS server has not been required.

BorderManager 3.0 cannot act as a SOCKS client to a SOCKS4 server.

Note Only the HTTP Proxy really makes use of the SOCKS client. Other proxies will not use the SOCKS client setting (including the FTP Proxy, although the menu option makes it look like it can use SOCKS).



The example above shows the SOCKS client configuration menu on a BorderManager 3.5 or later server. Compared to BorderManager 3.0, you also have the ability to specify SOCKS version 4 or version 5.

With SOCKS version 5, you can require authentication by name and password. The example shown above allows the HTTP Proxy to make requests to the Internet via a SOCKS 5 server at 4.3.2.1. The SOCKS 5 server is requiring authentication, and BorderManager is passing a user name and password to the SOCKS server.

Setting Up a Cache Hierarchy

Concept

A cache hierarchy is designed to share data from one HTTP Proxy cache to another without having to go directly to the origin server. It can be used to reduce Internet bandwidth demands by sharing data among multiple internal proxy cache servers, and it can be used where one proxy cannot go directly through a firewall, but is able to pull cache data from another proxy cache server. Two types of cache hierarchies are supported by BorderManager 3.x – CERN and ICP. The essential difference is that ICP cache servers exchange status updates between themselves before data is requested from cache, while CERN proxy servers immediately request the data from the parent proxy. When BorderManager is set up to be a CERN client, it acts much like a browser going to an HTTP proxy server on port 8080. A CERN caching hierarchy seems to work with the least amount of problems. Both ICP and CERN cache hierarchies can be set up between a BorderManager server and a non-Novell caching server.

Note As far as I know, all HTTP Proxies can serve as a CERN proxy, but not all have ICP proxy capability. Linux (SQUID) proxy servers that I have worked with typically seem to default to ICP.

As a CERN client, the BorderManager server asks for another server to provide HTTP data. The other server may have the data in cache, or it may have to go directly to an origin server (or another caching server) to get the data. When the 'upstream' caching server receives data, it passes that data back to the BorderManager HTTP Proxy server.

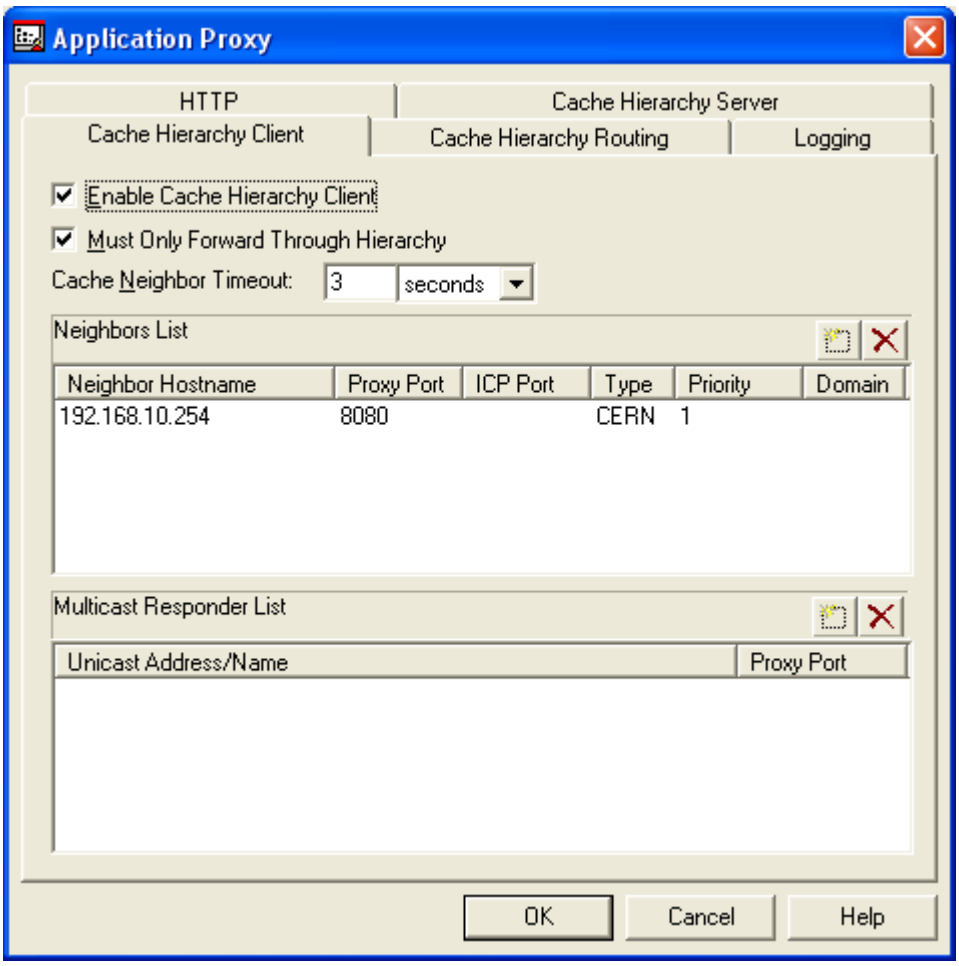
The upstream CERN server does not have to be a BorderManager server. It only needs to be configured as a CERN proxy server.

When using a CERN cache hierarchy with the BorderManager server as a client, the BorderManager server acts like a browser to another HTTP proxy.

Note The latest patch for BorderManager 3.5 and later provides the capability of passing authentication information to an upstream caching server. The authentication information is configured in the PROXY.CFG file.

CERN Configuration, BorderManager Server as a Client

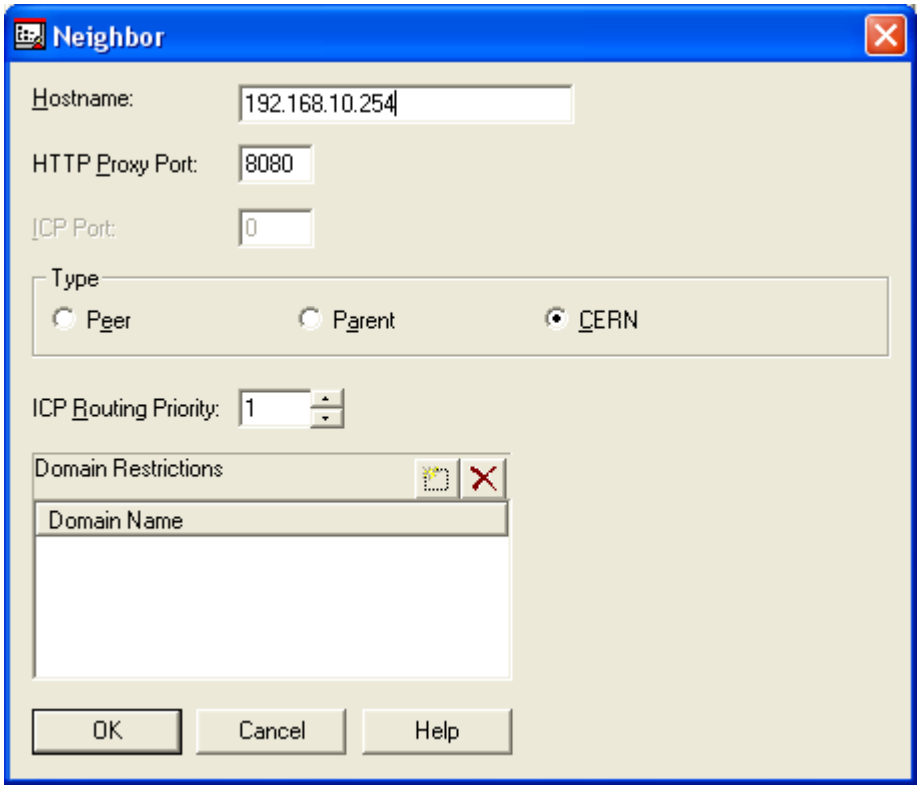
The example shown is taken from Scenario 9b in Chapter 2, the complex multi BorderManager server scenario. The menu entries shown below are from the BORDER2 server.



Click on the **HTTP Proxy**, **Details** button in the BorderManager Setup main menu. Then select the **Cache Hierarchy** Client tab.

In the example shown, the BorderManager server (BORDER2) must get all of its HTTP data from a CERN neighbor at **192.168.10.254**. (BORDER1) The option **Must Only Forward Through Hierarchy** is selected, so that the BorderManager server cannot go directly to any origin server, even an internal web server. However, that option really only applies to ICP cache hierarchy servers, because a CERN proxy will ALWAYS go through the parent! (Still, setting this option to enabled may result in preventing useless ICP error messages when running a CERN hierarchy).

If exceptions are desired, entries can be made in the Cache Hierarchy Routing menu.



The example above shows the entry needed to tell BorderManager to go to the CERN proxy at 192.168.10.254.

The **ICP Port** value is not used for a CERN proxy.

Domain restrictions can be entered to restrict the HTTP requests to an upstream proxy to only selected domains. In other words, if one CERN proxy should only be used to pull data from a certain domain (mydomain.com), you can add the domain name here. Then, when queries for http://www.mydomain.com come in, they will be requested from the upstream CERN proxy, but URL's for other domains will not.

In the absence of domain restrictions, ALL URL's will be requested from the upstream CERN proxy.

The upstream CERN proxy will perform all DNS queries for the URL.

ICP Cache Hierarchy

An Internet Caching Protocol (ICP) cache hierarchy differs from a CERN hierarchy primarily in one detail – ICP data packets are sent between caching servers to determine if a server already has the data in cache. If data is already in cache at some server, that server tells the requesting server, and the requesting server may then follow up with a request for the data itself. In a CERN hierarchy, the data is simply requested.

Note ICP packets are not sent if only one other ICP server is defined. There is no need to query the other ICP servers unless a choice is to be made for which of those servers might already have the data.

Both servers need to be configured as ICP servers or the hierarchy will not function. ICP packets are also time-sensitive, and you may see error messages on a BorderManager server about ICP requests having expired.

ICP cache hierarchies are best suited to situations where multiple caching servers exist.

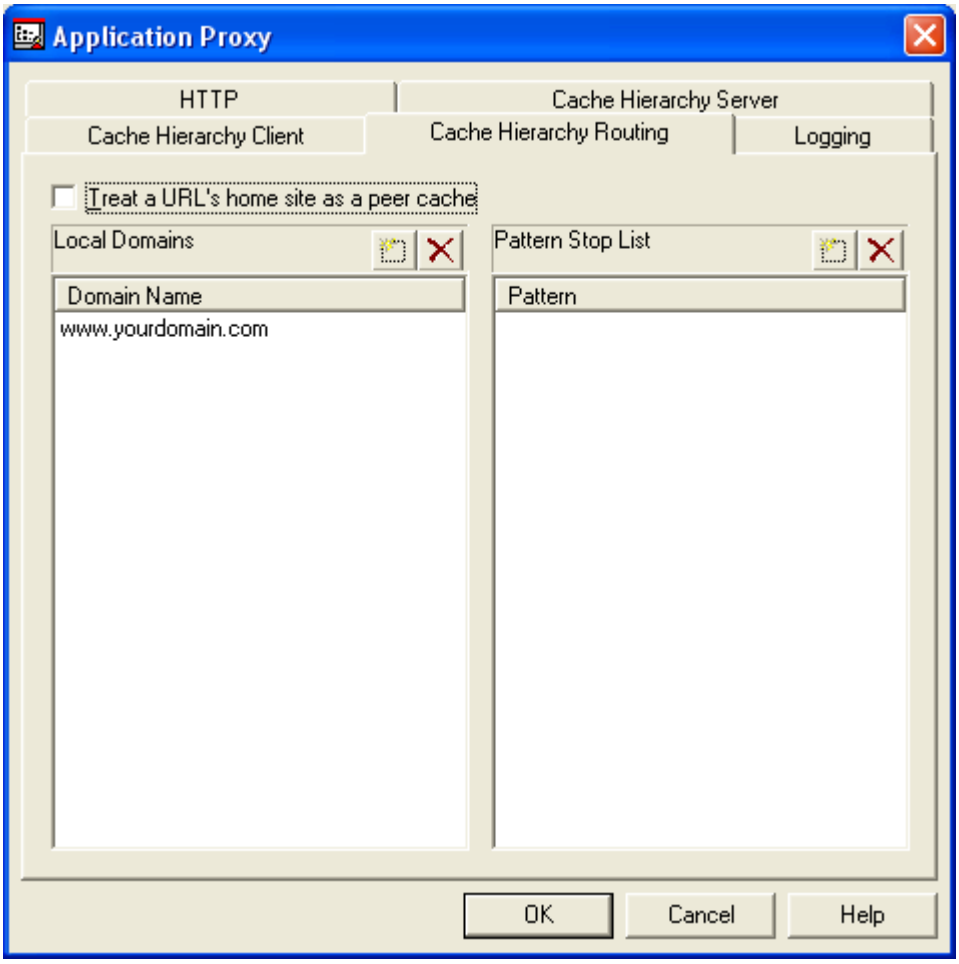
Cache Hierarchy Routing Exceptions

You may want to force most, but not all, of the HTTP traffic to come from another caching server. The example below shows one way to accomplish this. An explanation of the test setup may be useful.

Note See Scenario 9b, earlier in this book, for a diagram of the servers and addressing used. The cache hierarchy being described is between BORDER2 and BORDER1.

In this example, a BorderManager server has been set up such that the only path to the Internet is through another CERN proxy server. That server has been set up with internal IP address 192.168.10.254. That server has been configured as a BorderManager 3.7 server running HTTP Proxy, though it could have been any CERN proxy.

There is an internal web server called http://www.yourdomain.com at 192.168.10.250. The domain used for the test setup is http://yourdomain.com. However, yourdomain.com is not legally registered to the test network, and there is actually a public web server called www.yourdomain.com out on the Internet. The purpose of the test setup is to force all HTTP data to come through the CERN cache hierarchy **except** for http://www.yourdomain.com, which should instead come directly from the (local) origin server. An internal DNS server has been configured on the test LAN with a local entry for http://www.yourdomain.com. In addition, a local address entry for http://www.yourdomain.com was added to the BorderManager server BORDER2 SYS:\ETC\HOSTS file. Even with the local DNS and HOSTS file entries, the HTTP Proxy will still try to pull data from internet through the upstream CERN proxy because it passes the URL to the upstream proxy to resolve. (In other words, the local DNS and HOSTS file entries are ignored, and the upstream proxy decides where to get the data for http://www.yourdomain.com).



Exceptions to the cache hierarchy routing were needed in order to pull data from local web servers. Add an entry for a local web server in the **Local Domains** field under the **Cache Hierarchy Routing** menu in order to tell the HTTP Proxy NOT to go to the upstream CERN proxy to fill data from the various yourdomain.com websites. A pattern (yourdomain.com) could also have been entered to prevent any URL containing that pattern from being filled from the upstream CERN proxy.

<This page intentionally left blank. This is to facilitate putting in chapter tabs in a ring binder for double-sided printing. The main chapters should start on an odd-numbered page.>

Chapter 7 - Transparent Proxy

Transparent Proxy (HTTP)

Concept

The transparent proxy intercepts all HTTP traffic and processes it, independently from the fact that the client browser was configured to use the proxy or not.

Pros

- Does not require the browser to be configured for a proxy server
- Can use Access Rules for control
- Is the only way to use proxy caching with IPX/IP Gateway clients if Proxy Authentication is enabled.

Cons

- Until the BM36C01 (or later) patches, Transparent HTTP Proxy listened on all IP addresses listed in NWADMN32, BorderManager Setup, IP Addresses. This means it listened on the Public IP address. Coupled with the default filter exception in various versions of BorderManager that allow port 80 to the public IP address, the Transparent HTTP Proxy allowed external users to relay off the proxy. (Used to relay to pornographic web sites, for instance).
- The Transparent Proxy will also intercept inbound HTTP Traffic, and can interfere with a reverse HTTP proxy, and packet filters set up for static NAT to a web server.
- Logging – The log files will only show the IP address of the web sites requested.
- HTTPS – Until recent BorderManager 3.7 patches, the Transparent Proxy did not support HTTPS (SSL), and sites that require a user to log in did not work.
- Software Virtual Servers – Until recent BorderManager 3.6 patches, the Transparent Proxy did not work with Software

Virtual Servers. (Only one web site at the same IP address will be seen). This issue is fixed with the later patches and a proxy.cfg file setting.

- Speed – The Transparent Proxy is slower than HTTP Proxy, partly because the DNS lookups are not cached.
- DNS – The Transparent Proxy does not perform a DNS lookup, unlike the HTTP Proxy. Therefore the workstations have to be configured and able to perform their own DNS lookups.
- Access Rules – Access Rules seem to work somewhat inconsistently. One problem is that access rules generally call out a web site URL, but the Transparent Proxy sees the HTTP traffic after the DNS lookup has already occurred. SurfControl does not support Transparent Proxy for their product.

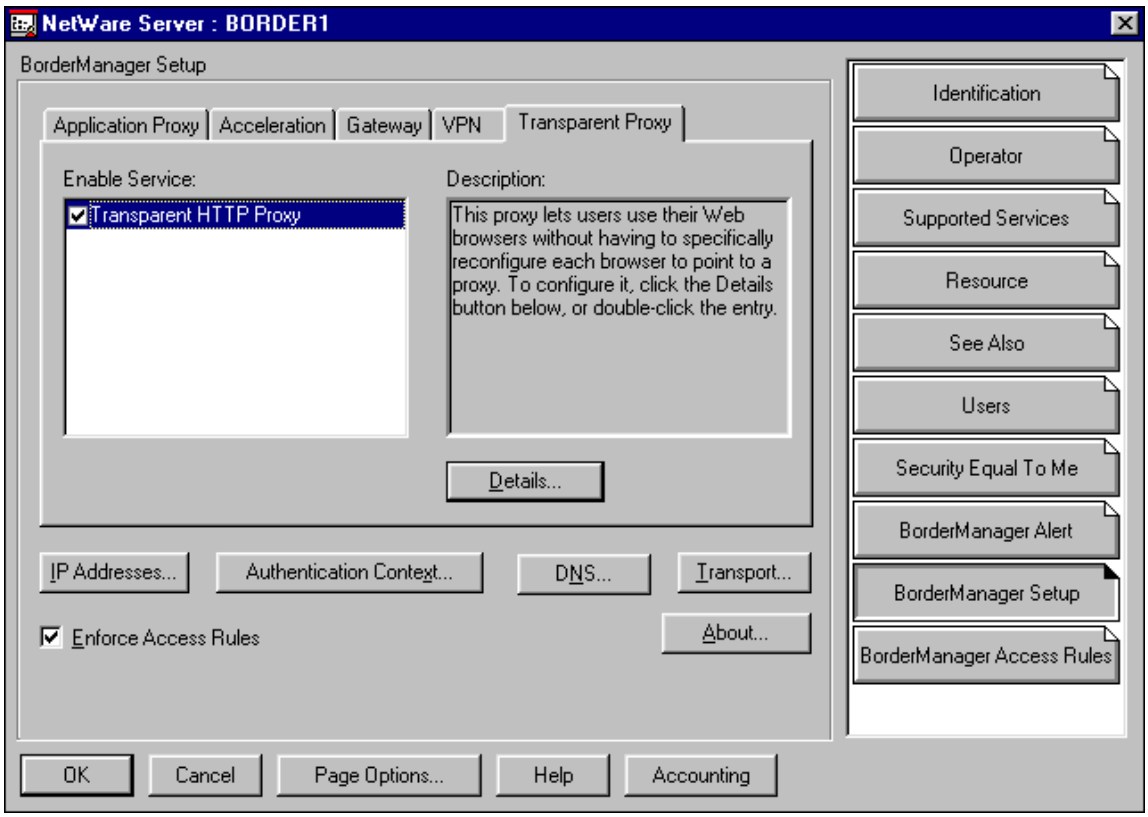
Transparent proxy is used to redirect HTTP requests to the web proxy cache without having to reconfigure the browsers on each workstation. However, it only works if HTTP traffic is directed to a private interface on the BorderManager server. Traffic routing to internal web servers may never go to a BorderManager server, therefore not go to the caching mechanism. However, all outbound HTTP traffic will go to cache with transparent proxy enabled if the BorderManager server is the default route to the Internet.

Note that Transparent Proxy works by redirecting TCP port 80 requests, and will only redirect traffic after DNS name resolution has successfully occurred (unlike the HTTP Proxy which performs DNS lookups on behalf of the client).

Configuring Transparent Proxy

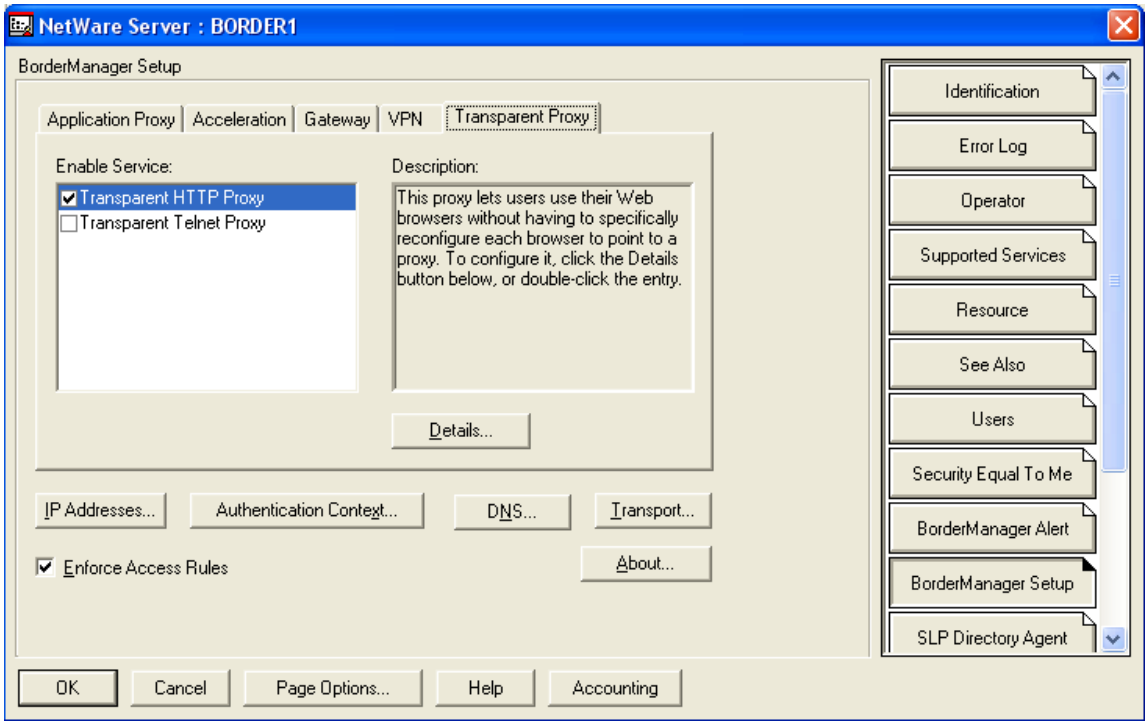
From the BorderManager Setup Main Menu, select the **Transparent Proxy** tab.

BorderManager 3.0 Transparent Proxy configuration menu



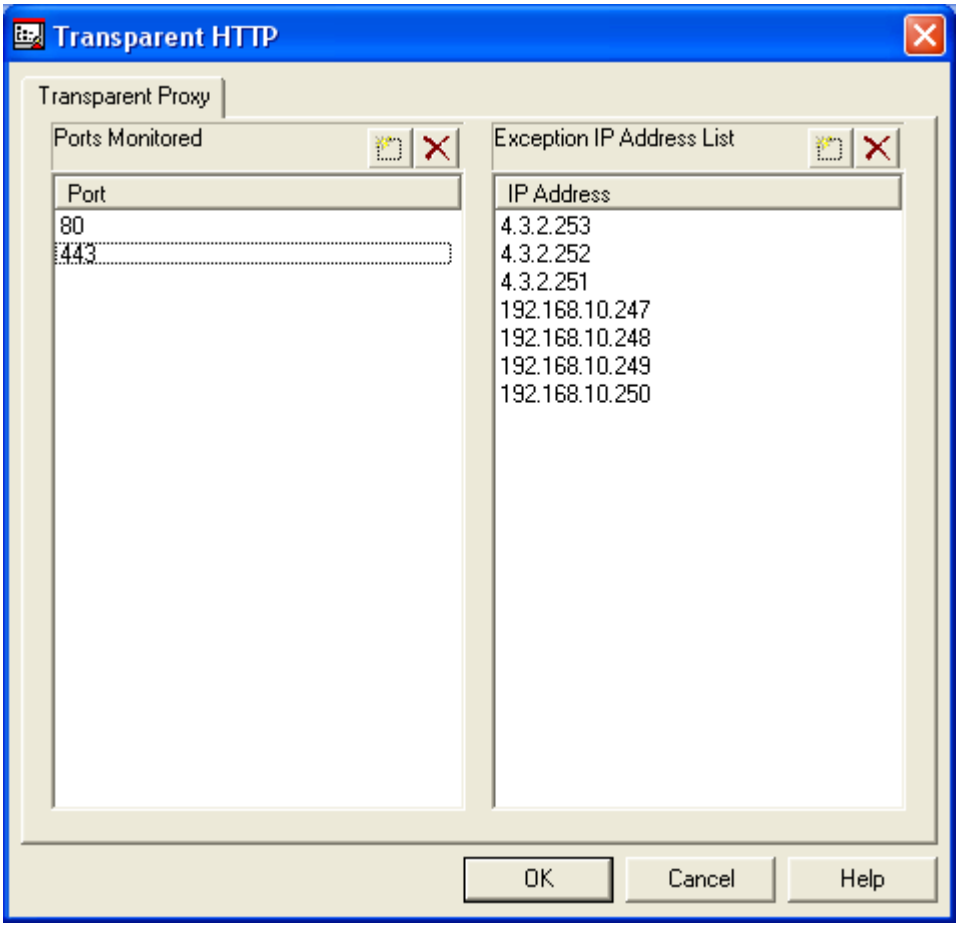
Note that on a BorderManager 3.0 server, you will not see an entry for Transparent TELNET Proxy.

BorderManager 3.5 and Later Transparent Proxy configuration menu



The Transparent Proxy menu is one of the places where differences between BorderManager 3.0 and 3.5 or later can be seen, as version 3.5, 3.6, 3.7 and 3.8 include a Transparent TELNET proxy setting as well as a Transparent HTTP Proxy setting.

Click on **Details** to configure Transparent Proxy.



There are very few details to configure, but they are very important details.

Set up Transparent Proxy to monitor port **80**. This will result in any traffic to the BorderManager server's private IP address on port 80 to be redirected into the web proxy server. Thus, browsers do not have to be set up for proxy to access Internet web pages through the BorderManager web proxy server.

If you have the latest BorderManager 3.7 PROXY.NLM file in your BorderManager 3.5, 3.6 or 3.7 server, you can also configure Transparent HTTP Proxy to listen on port **443**. This option also requires a PROXY.CFG setting.

CAUTION *To avoid having Transparent HTTP Proxy pick up HTTP going through a reverse proxy or static NAT address, and getting into a loop, configure all secondary IP addresses and internal web servers as exceptions.*

Note Transparent Proxy will cache data from a web site as a different node than the same web site accessed through HTTP Proxy. That is, the same data might be cached twice, once for Transparent Proxy and once for HTTP Proxy. Because of this difference, you also will continue to cache data that has been entered as a non-cacheable URL if you are using Transparent Proxy instead of HTTP Proxy.

Click on **OK** to return to the main menu.

Note There are ways to get browsers configured with proxy settings without you having to go visit every workstation. See the section on this in the Odds & Ends chapter later in this book.

Transparent TELNET Proxy

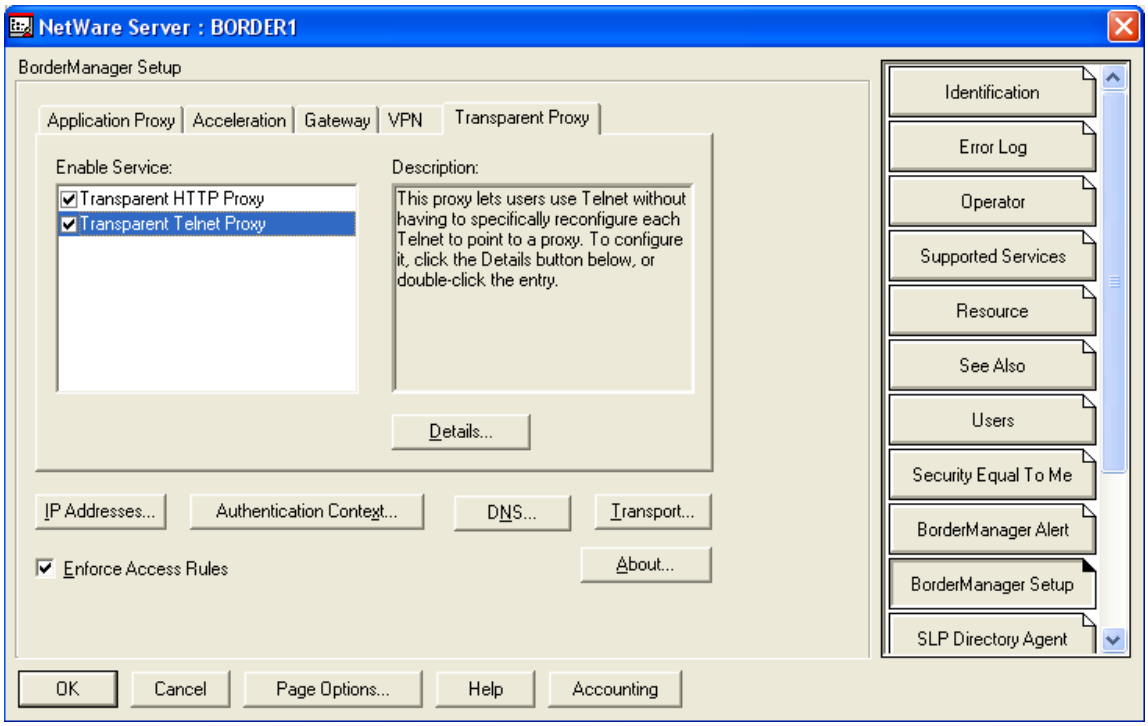
Transparent TELNET proxy is available only in BorderManager 3.5 and later. It is not present in BorderManager 3.0.

CAUTION *I have found this proxy to be problematical in causing server instability. If you decide to use it, be sure you have the latest patches installed. If you find that the server is having problems, disable this proxy for a while as a test, and see if the problems go away.*

Concept

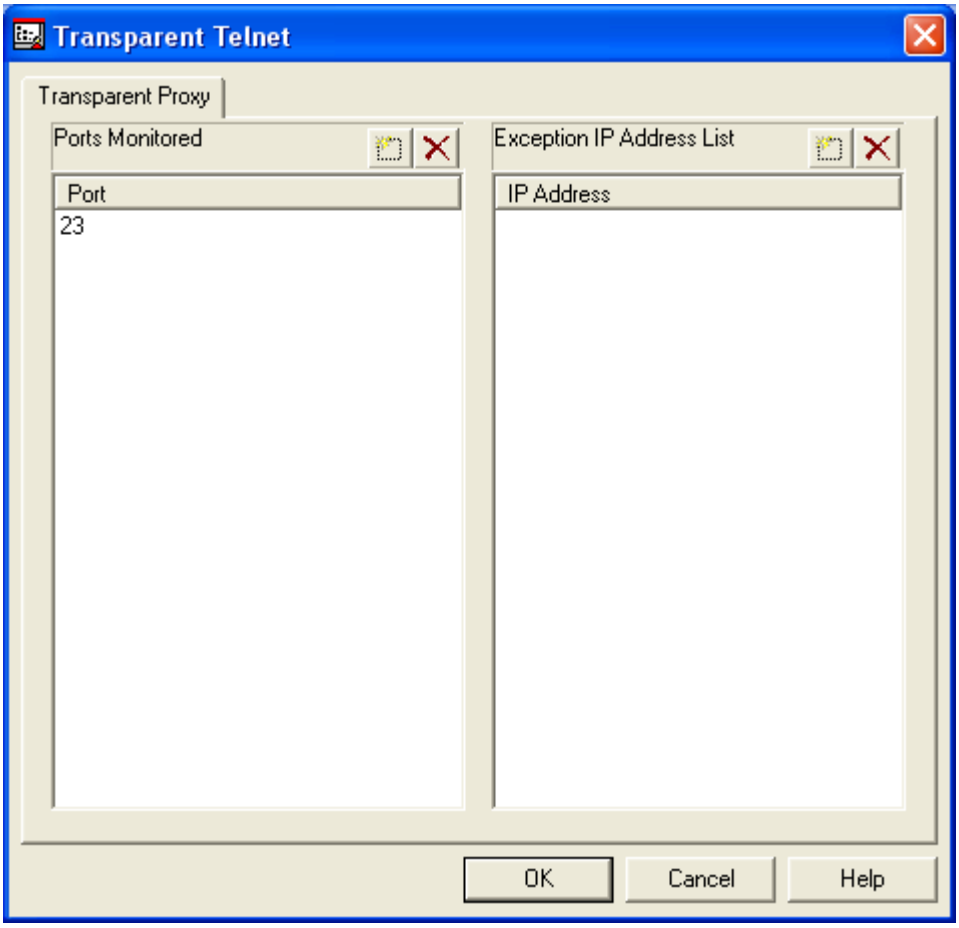
Transparent TELNET Proxy, much like the Transparent (HTTP) Proxy, is designed to intercept traffic on a specific port, usually TCP port 23, and proxy the traffic to the public (Internet) side. By using an application proxy for this purpose, access control rules can be applied to limit the traffic allowed, and at the same time allow greater flexibility to external TELNET Servers than with individual Generic TCP proxies.

Configuring Transparent TELNET Proxy



From the BorderManager Setup Main Menu, select the **Transparent Proxy** tab.

Check the **Transparent TELNET Proxy** box to enable it. Click on the **Details** button to configure Transparent TELNET Proxy settings.

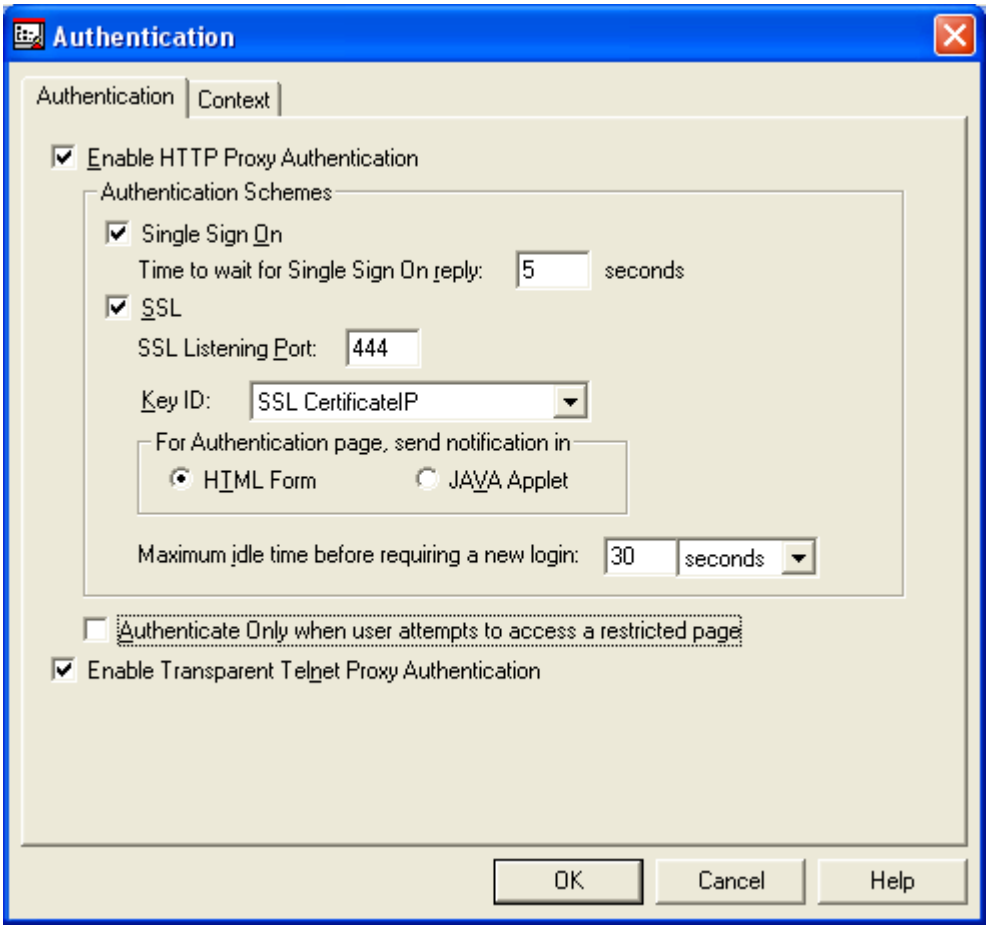


TELNET usually (but not always) is used on TCP port 23. For most purposes, you will configure Transparent TELNET Proxy to monitor port 23.

If for one reason or another Transparent TELNET Proxy is intercepting a request that should be destined for an internal TELNET Server, you can put the IP address in the **Exception IP Address List** and your BorderManager server will ignore it.

User Authentication

You have a choice with Transparent TELNET proxy to either restrict access with a rule that is based on a NDS user ID or you can chose not to require one at all. If you do require a NDS user ID, when it is input at the login prompt, the password it is not encrypted when it is sent across the wire.



Select **Authentication Context** at the BorderManager Setup main menu.

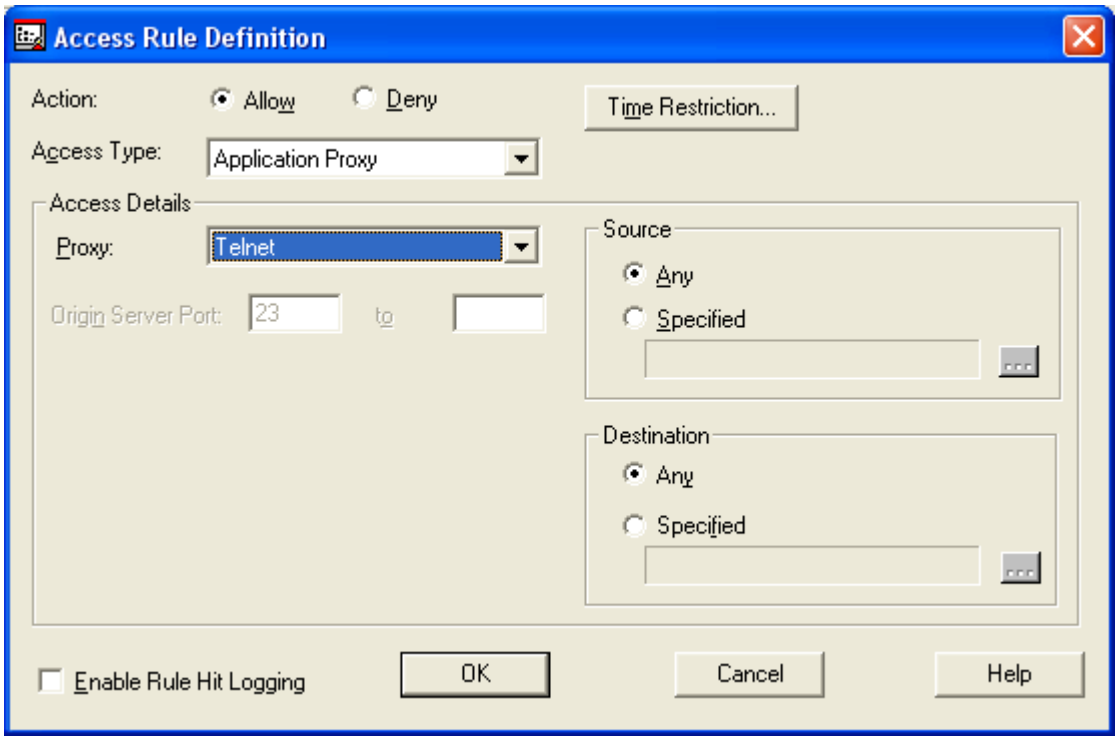
In order to tell the Transparent TELNET Proxy what user name is associated to a requesting IP address so that an NDS-based Access Rule can be used, you must put a check mark next to **Enable Transparent TELNET Proxy Authentication** in the Authentication Context menu. With that option selected, you will be prompted for a Novell username when you attempt to TELNET to any server on the public side of the BorderManager firewall.

Finish setting up Transparent TELNET proxy by adding an access rule to allow it to be used based on whether you choose to use NDS-based authentication or not.

Transparent TELNET Proxy Usage

Example 1 – No User-based Authentication Required

In this example a user wishes to access an external UNIX Server UNIXSERVER.COM requiring no NDS Username from the Microsoft Win2000 TELNET client.



In this example, an Allow access rule for **Application Type Application Proxy**, **TELNET**, is configured allowing Source=Any and Destination=Any.

Open a DOS window on the client.

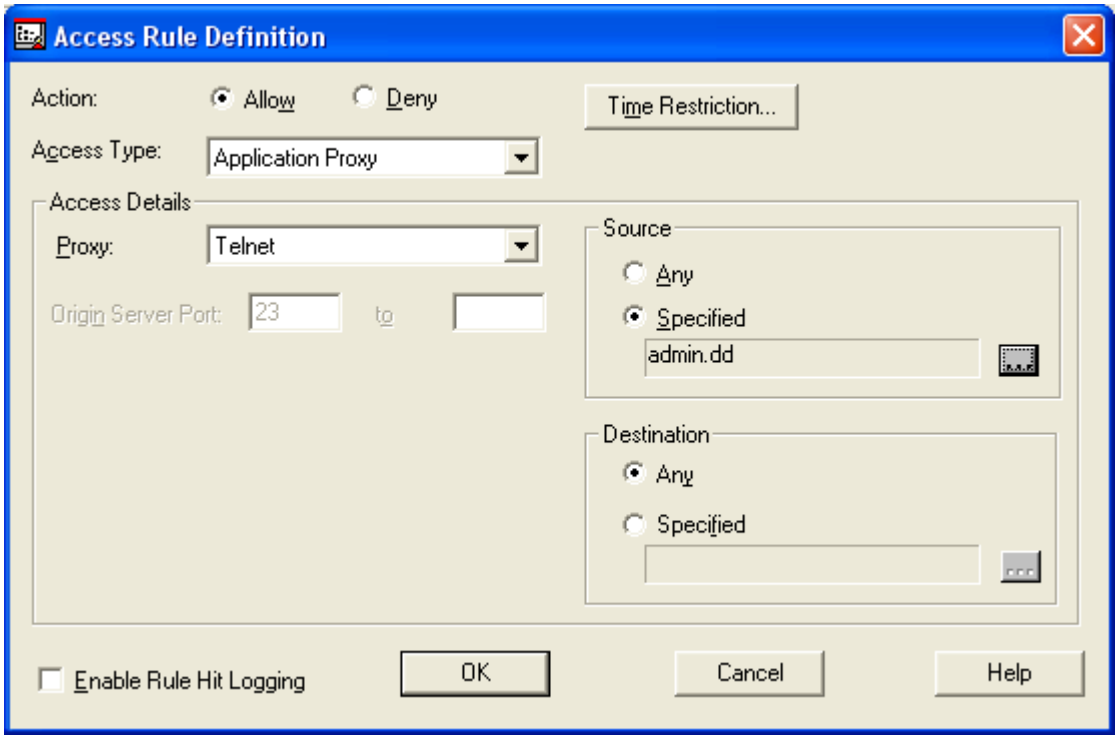
Type:

```
TELNET UNIXSERVER.COM
```

At this time, your client will do a DNS lookup for UNIXSERVER.COM and attempt to TELNET to it. Your BorderManager server will then intercept the request and forward you to UNIXSERVER.COM. You will then receive the Unix Server login prompt at which time you procede as you normally would when logging in.

Example 2 – NDS-Based User Authentication

In this example a user wishes to access an external UNIX Server UNIXSERVER.COM using the NDS user account TESTUSER from the Microsoft Windows 2000 TELNET client.



In this example, an Allow access rule for **Application Type Application Proxy**, TELNET, is configured with a **Source** equal to **Admin.DD** and **Destination** equal **Any**. You can also create the rule based on a NDS group that the user is a member of.

Open a DOS window on the client.

Type:

```
TELNET UNIXSERVER.COM
```

At this time, your client will do a DNS lookup for UNIXSERVER.COM and attempt to TELNET to it. Your BorderManager server will then intercept the request and provide you with the following prompt:

```
      Novell Border Manager TELNET Proxy Service
You are required to authenticate before connecting to the
target host

User Name:
```

At this time you can use the common name if you have configured the **Context Tab** of the Authentication Context menu. Type in the NDS user name and press **Enter**:

```
User Name: Admin
```

You will then receive the Unix Server login prompt at which time you procede as you normally would when logging in.

You can debug problems with NDS-based authentication from the error messages received after a login attempt**:**

```
Access Denied by Novell Border Manager:Access Control failure
```

If you receive the above error, it indicates an issue with your access rule. Verify that the user you are attempting to login has been permited with an Allow access rules.

```
Access Denied by Novell Border Manager:user login failure
```

The above error indicates that either the user name used is incorrect, or you are attempting to use a common NDS name and you have not configured the Context tab of the Authentication page to include the context where the user is located. It can also mean that the password for the user was typed incorrectly. Note that the Transparent TELNET Proxy will provide two retry attempts before you will have to initiate your TELNET session again.

<This page intentionally left blank. This is to facilitate putting in chapter tabs in a ring binder for double-sided printing. The main chapters should start on an odd-numbered page.>

Chapter 8 - FTP Proxy

Concept

The FTP Proxy is used to proxy outbound PASV FTP requests on behalf of FTP clients. (This does not include browsing FTP sites through a web browser).

Pros

- You can control user access to FTP servers by access rules, including control of access by user ID.

Cons

- The FTP Proxy supports only FTP clients (not browser-based FTP), though some browsers have some options to be configured to act as FTP clients. In general, a true FTP client tends to work better through FTP Proxy than a browser acting as an FTP client, especially if authentication is involved.
- FTP Proxy only supports FTP servers accepting PASV FTP requests. If you need to access a server which only supports Active mode, you will need to use packet filter exceptions and dynamic NAT instead.
- FTP Proxy may have problems accessing some types of FTP servers.
- FTP Proxy requires FTP clients to be set up with a particular syntax, and authentication in particular requires a syntax for accessing the FTP Proxy that can be complicated.

Alternative For ACTIVE (PORT) FTP

Because of the limitation of the FTP Proxy not supporting Active-mode FTP servers, an alternative is needed. You can still access Active-mode FTP servers by enabling Dynamic NAT on the public IP binding in INETCFG, and setting up a stateful packet filter exception using the FTP-PORT-ST packet filter definition. Use source interface=<your private interface> and destination interface=<your public interface>.

Configuring FTP Proxy

Check the FTP Proxy box on the BorderManager Setup main menu screen, and click on Details to configure the parameters.

User Authentication

Two types of user authentication are available.

User authentication is used if you want to create an Access Rule to control the use of the FTP Proxy by NDS user ID.

In order to tell the FTP Proxy what user name is associated to a requesting IP address so that an NDS-based Access Rule can be used, one of the following authentication methods must be used.

Clear Text User/Password

In this method, the user passes their user name and password to the FTP Proxy as part of the user ID and password strings for accessing the FTP site. Thus, you might enter a user ID and password in this manner.

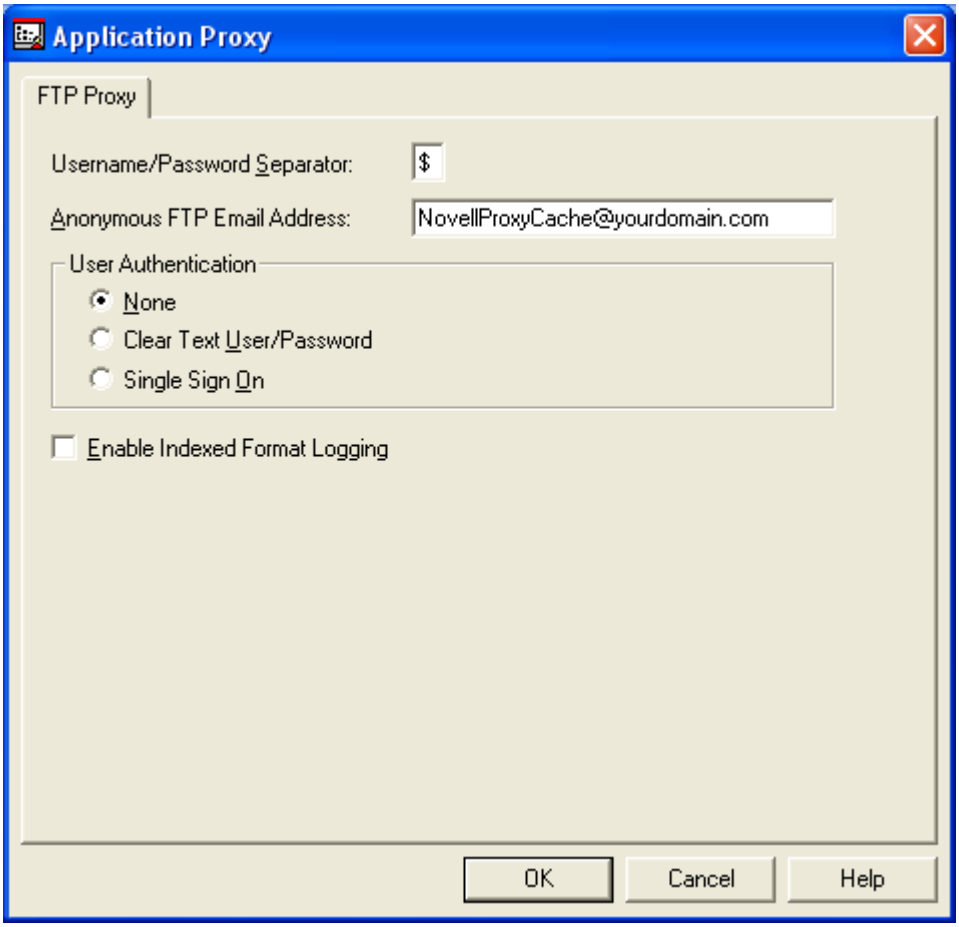
Single Sign On

In the single sign on method, the user must be logged into the same NDS tree as the BorderManager server, be using Novell Client32, and be running the CLNTRUST.EXE program. Unfortunately, this functionality was **broken** in BorderManager 3.x, at least up through patches BM35C11 and Service Pack 2 in BorderManager 3.5. Later patch versions work, but I am unclear at which point the feature was fixed.

FTP Proxy Usage

Example 1 – No User-based Authentication Required, DOS FTP Client

In this example, an internal user wants to access the FTP.SYSOP.COM FTP server using an anonymous login from the Microsoft Win98 DOS FTP client. User-based authentication is not required in the FTP Proxy configuration.



In this example, an Access Rule for Application Proxy, FTP, is configured allowing Source=**Any** and Destination=**Any**.

Open a DOS window on the client.

Type:

```
FTP BORDER1
```

BORDER1 is the name of the BorderManager server, and an internal DNS server or local HOSTS file entry must resolve the name to the private IP address of the BorderManager server. As an alternative, you could use the private IP address of the BorderManager server instead of the server's DNS name. (FTP 192.168.10.252)

The FTP Proxy server responds:

```
Connected to BORDER1.YOURDOMAIN.COM.
220 Service Ready
User (BORDER1.YOURDOMAIN.COM:(none)):
```

Type in the FTP user name to be sent to the remote FTP host, followed by the separator characted configured for the FTP Proxy ($ in this case), followed by the DNS name of the remote FTP server:

```
User (BORDER1.YOURDOMAIN.COM:(none)): anonymous$ftp.sysop.com
```

The FTP Proxy responds:

```
331 Anonymous access allowed, send identity (e-mail name) as
password.
Password:
```

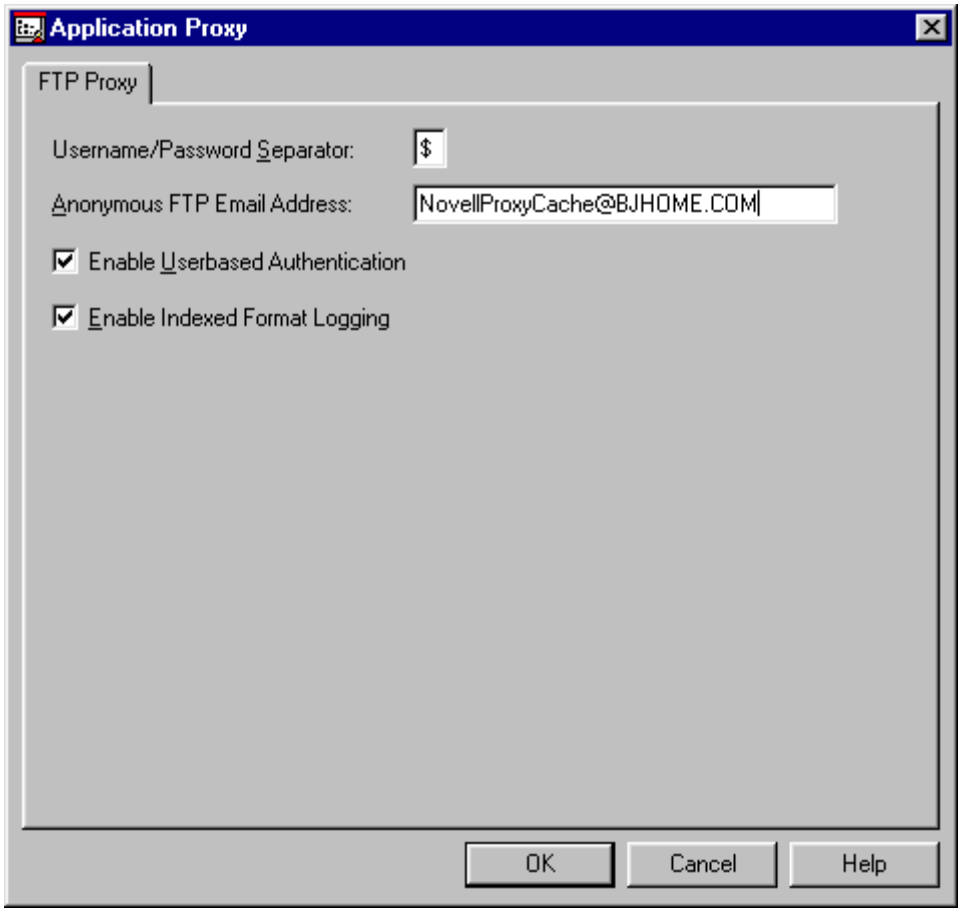
Here you should be able to just press Enter (or type your email address) to send the anonymous FTP Email Address (configured in NWADMN32, FTP Proxy, Details) as the password. The server should respond in a manner similar to below:

```
230-Welcome to the FTP Server
230 Anonymous user logged in.
ftp>
```

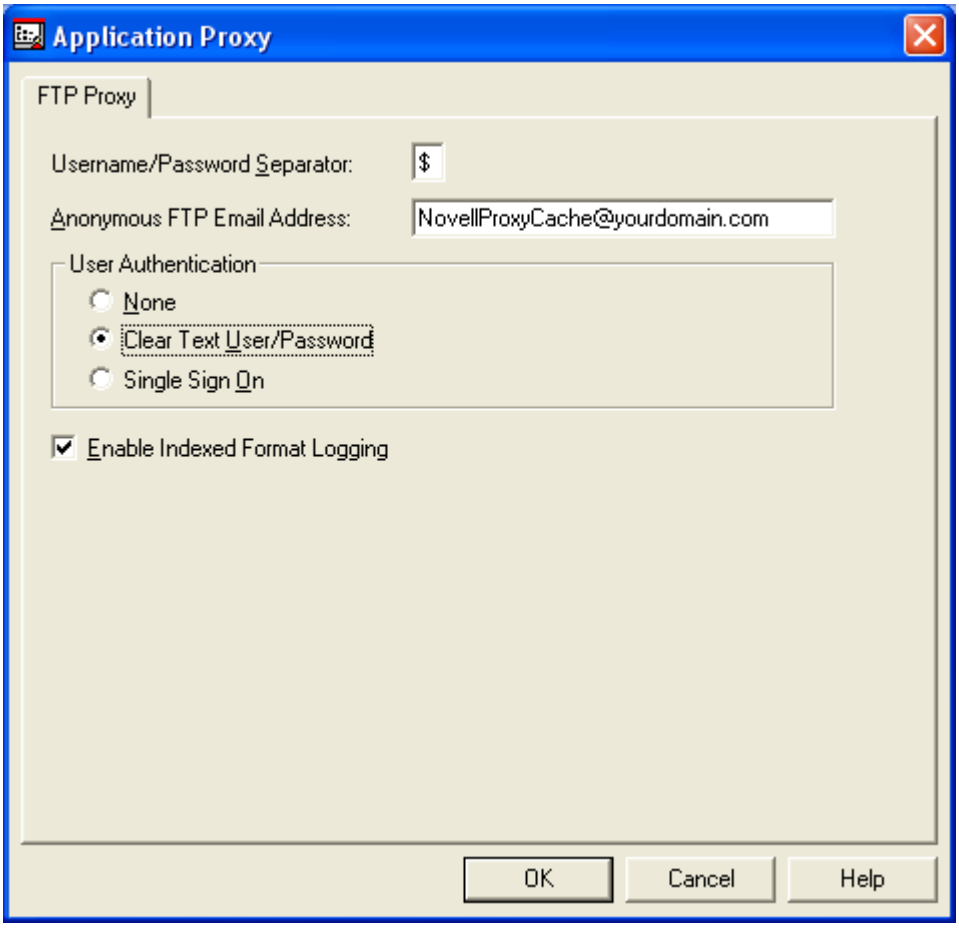
And now you should be able to perform FTP duties.

Example 2 – User-based Authentication Required, DOS FTP Client

In this example, an internal user wants to access the FTP.SYSOP.COM FTP server using an anonymous login from the Microsoft Win98 DOS FTP client.

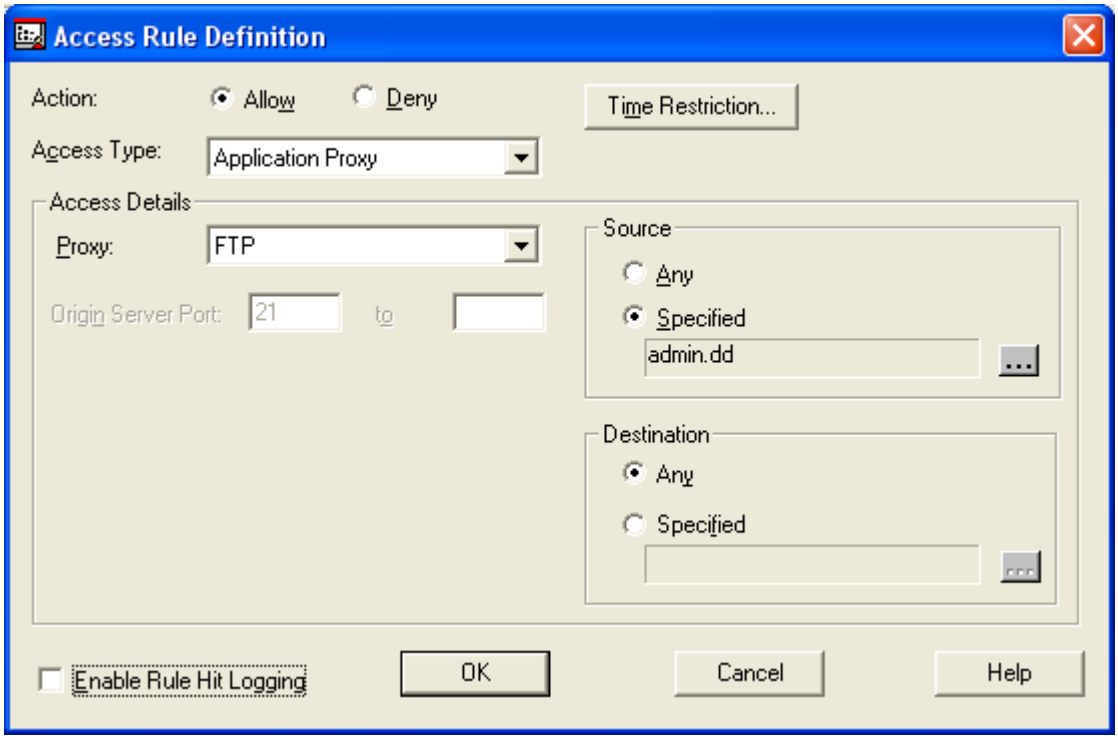


BorderManager 3.0: Enable User-based Authentication in the FTP Proxy configuration BorderManager 3.0 menu).



BorderManager 3.5 and later: Select **Clear Text User/Password** in the User Authentication section of the FTP Proxy Details menu.

As noted earlier, Single Sign On (using CLNTRUST) will work, with the latest patches.



In this example, an **Allow** Access Rule for **Application Proxy**, **FTP**, is configured allowing Source=**Admin.dd** and Destination=**Any**. Only the Admin user should be able to use the FTP Proxy.

Open a DOS window on the client.

Type:

```
FTP BORDER1
```

BORDER1 is the name of the BorderManager server, and an internal DNS server or local HOSTS file entry must resolve the name to the private IP address of the BorderManager server. As an alternative, you could use the private IP address of the BorderManager server instead of the server's DNS name. (FTP 192.168.10.252)

The FTP Proxy server responds:

```
Connected to BORDER1.YOURDOMAIN.COM.
220 Service Ready
User (BORDER1.YOURDOMAIN.COM:(none)):
```

Type in the just the FTP user name to be sent to the remote FTP host, followed by the separator characted configured for the FTP Proxy ($ in this case), followed by the DNS name of the remote FTP server, as in the previous example:

```
User (BORDER1.YOURDOMAIN.COM:(none)): anonymous$ftp.sysop.com
```

The FTP Proxy responds:

```
530 Access Denied by Novell Border Manager:Access Control
failure
 Connection closed by remote host
ftp>
```

This message comes up if you did not enter the proper NDS credentials to access the FTP Proxy. Instead, you now must add the fully distinguished user ID for Admin.DD. Only the Admin.DD user ID will work.

```
ftp> Open BORDER1
Connected to border1.
220 Service Ready.
User (border1:(none)): admin.dd$anonymous$ftp.sysop.com
331 Anonymous access allowed, send identity (e-mail name) as
password.
Password: <press enter, or type your email address>
Connection closed by remote host.
ftp>
```

This attempt failed because the Admin user password was not sent to the FTP Proxy when the password was request. Instead, try the following:

```
ftp> Open BORDER1
Connected to border1.
220 Service Ready.
User (border1:(none)): admin.dd$anonymous$ftp.sysop.com
331 Anonymous access allowed, send identity (e-mail name) as
password.
Password: <admin user password>$<press Enter, or type your
email address>
230-Welcome to the FTP Server
230 Anonymous user logged in.
ftp>
```

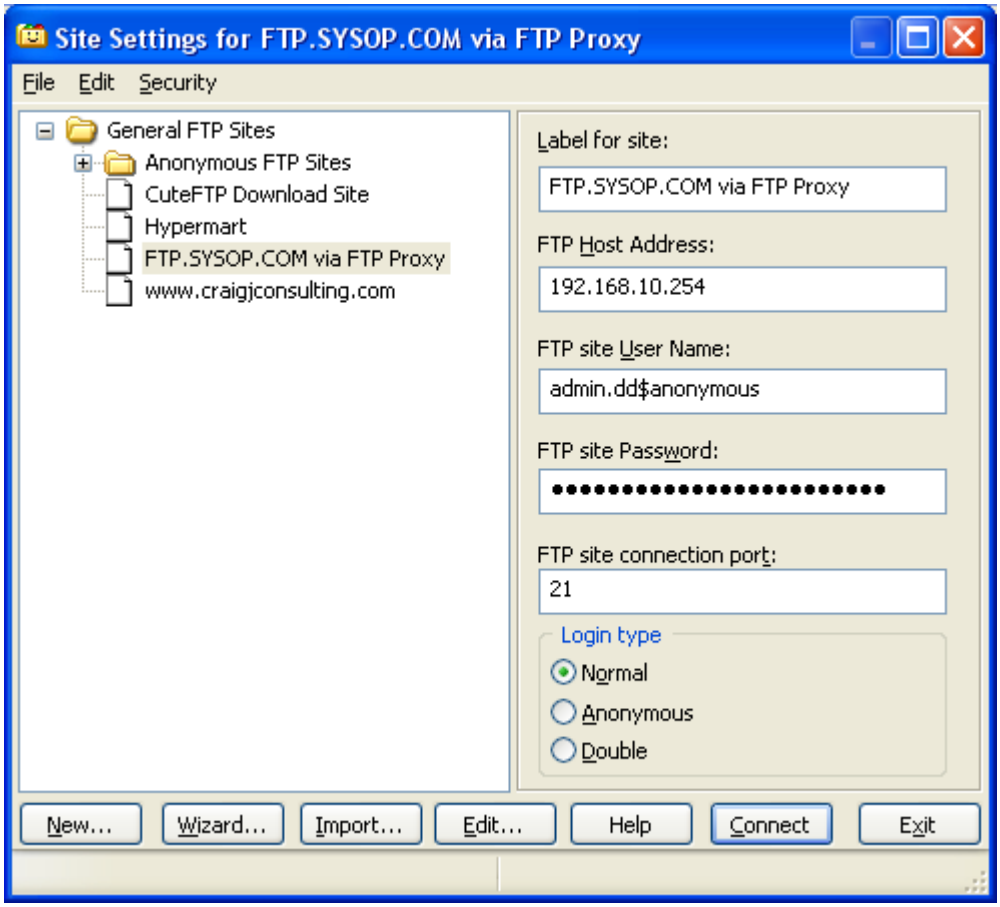
And now you should be able to perform FTP duties.

If you are trying to troubleshoot FTP Proxy connection problems, be sure to look at the BorderManager server console, **Proxy Console** page**, Option 19**, then **Option 2** '**Display FTP Proxy statistics'**. That screen will show you if the password has not been seen by the proxy (ACL rejects), and other useful information.

Example 3 – User-based Authentication Required, CuteFTP Client

In this example, an internal user wants to access the FTP.SYSOP.COM FTP server using an anonymous login using CuteFTP (version 3.0**). User-based authentication** is required in the FTP Proxy configuration.

In this example, an Access Rule for **Application Proxy, FTP**, is configured allowing **Source=.Admin.dd** and **Destination=Any**. Only the Admin user should be able to use the FTP Proxy.



CuteFTP Example

The **Host Address** is the DNS name or the private IP address of the BorderManager FTP Proxy server.

The **User ID**, most of which is not visible in the example, consists of the following:

```
Admin.DD$anonymous$ftp.sysop.com
```

The **Password** consists of:

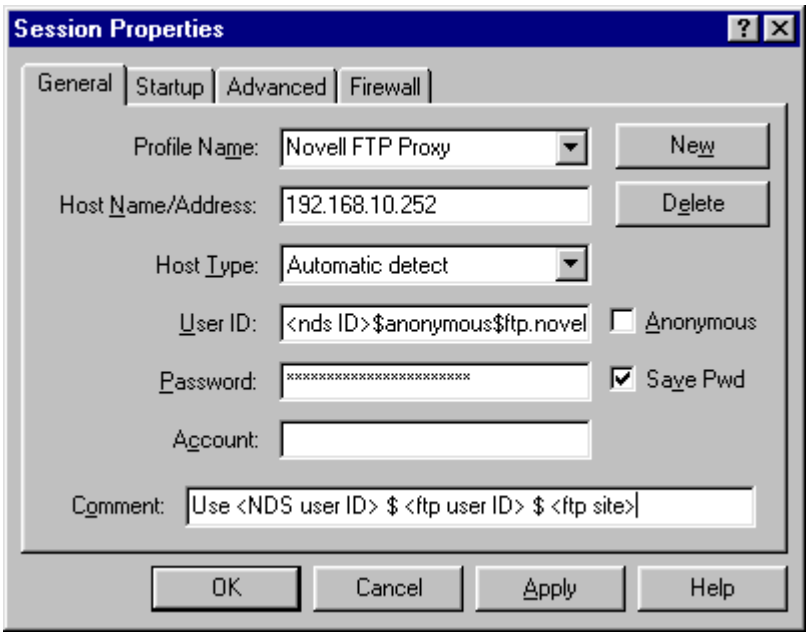
```
<admin.dd NDS password>$<your email address>
```

(For instance, if the password is NOVELL and the email address is CRAIG@YOURDOMAIN.COM, the full password to be entered is NOVELL$CRAIG@YOURDOMAIN.COM).

This connection wizard works quite nicely. Just remember that if your NDS user ID changes, you will have to change the password in the CuteFTP connection wizard as well.

Example 4 – User-based Authentication Required, WS_FTP Client

The WS_FTP program is a popular FTP client. While it has settings for use with a firewall, none of them match the way that the BorderManager FTP Proxy expects to see the authentication data passed to it. In order to use WS_FTP with the FTP Proxy, configure it NOT to use a firewall, and then use the following settings:



In the example shown above, WS_FTP has been configured to point to the FTP Proxy at the internal IP address 192.168.10.252 in the **Host Name/Address** field.

Both the NDS and FTP user ID's, plus the FTP site desired, are passed to the FTP Proxy in the **User ID** field. The syntax uses the separator character (**$** in this case) configured in the FTP Proxy Details menu. For this to work, **Enable Userbased Authentication** (BorderManager 3.0) or **Clear Text User ID/Password**) (BorderManager 3.5 or later) must be enabled.

The syntax for the **User ID** field is:

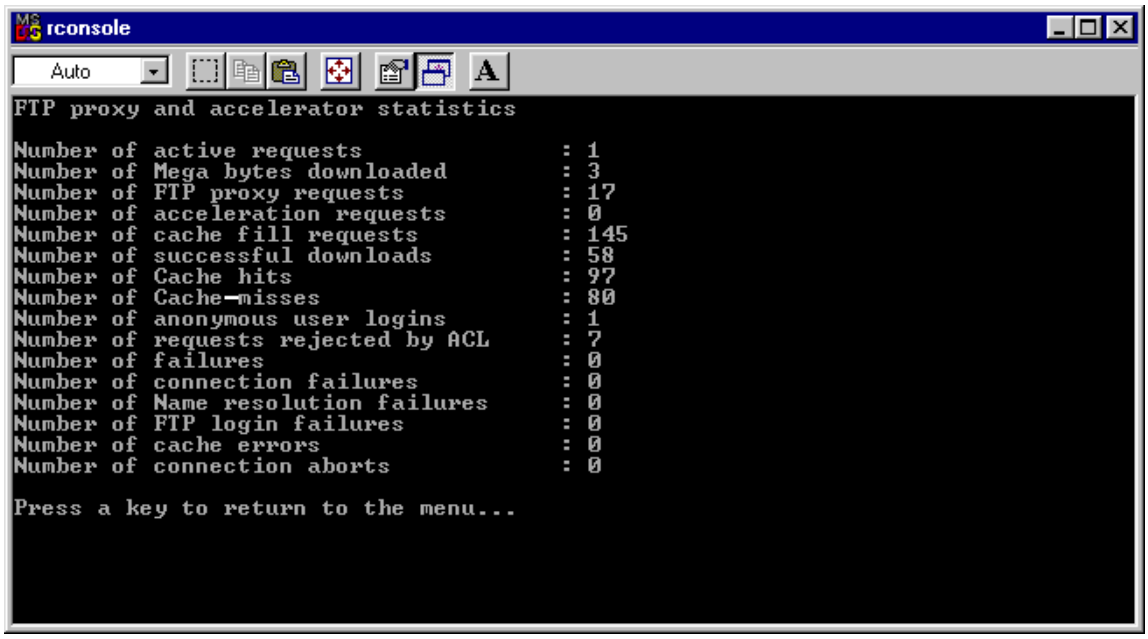
<NDS user ID> $ <ftp user ID> $ <ftp URL>

The Password field also is used to pass multiple entries to the FTP Proxy by using the $ separator character.

The syntax for the **Password** field is:

<NDS password> $ <ftp site password>

All Examples, FTP Proxy Statistics Screen



You can help debug connection issues with the FTP Proxy by looking at the BorderManager server console, **Proxy Console**, option #**19 Application Proxies**, option #**2 Display FTP Proxy statistics**:

Look at the statistics for **Number of requests rejected by ACL**. If this number increases when you try to make a connection through the FTP Proxy, you are not entering the username correctly, or you are using an NDS user name that is not allowed by an access rule.

<This page intentionally left blank. This is to facilitate putting in chapter tabs in a ring binder for double-sided printing. The main chapters should start on an odd-numbered page.>

Chapter 9 - Mail Proxy

Concept

The Mail Proxy is intended to work as a store-and-forward mail relay application that can be controlled through access rules. It will automatically listen for SMTP and POP3 traffic on all interfaces, and can be used when there is only one available public IP address to proxy traffic from the Internet to an internal SMTP mail server. The Mail Proxy can also be used to relay SMTP and POP3 mail for internal mail clients to external SMTP and POP3 servers at an ISP.

With BorderManager 3.8, more than one internal mail domain is supported. With previous versions of BorderManager, Mail Proxy will forward only one domain to an internal SMTP server.

Pros

- The main advantage for using Mail Proxy is to forward mail from the Internet to an internal SMTP and/or POP3 server in the private LAN without requiring an additional public IP address. (You can use the main BorderManager public IP binding, without having to use another public IP address for static NAT).
- Mail Proxy can also provide a limited means for accessing an external POP3 or SMTP server, which might be useful if you are trying to tightly control email systems inside your network.

Cons

- Mail Proxy, until BorderManager 3.8, supports only a single mail domain.
- Mail Proxy has had a history of problems through all versions of BorderManager 3.x. However, the problems continue to be less with ongoing patches and BorderManager revisions. Problems of some notoriety have included occasional ‘stuck’ mail in the spool directory, spam relay vulnerabilities (fixed with patches), problems sending

to secondary MX records (fixed with patches), and server instability (fixed with patches).

An Alternative

Many people have found the Mail Proxy to be somewhat problematical, especially without the latest BorderManager patches applied. In addition, there have been problems preventing people from relaying spam e-mail from the mail proxy. For these reasons, many people prefer to use a static NAT configuration to pass SMTP traffic through BorderManager to an internal SMTP mail server. This configuration is quite reliable, but a static NAT configuration requires a secondary public IP address to be added to the BorderManager server, and not everyone has more than one public IP address available to assign.

A GWIA Alternative

If you are using GroupWise with GroupWise Internet Agent (GWIA), you have an additional alternative – running GWIA on the BorderManager server itself. You will want to configure a secondary domain on the BorderManager server, and then TCP/IP-based communications will work between the BorderManager server and an internal GroupWise server.

For GWIA to receive SMTP, POP3 and IMAP4 traffic from the Internet, packet filter exceptions will need to be added with FILTCFG.NLM to allow TCP destination ports 25 (SMTP), 110 (POP3) and 143 (IMAP4) to the public IP address of the BorderManager server.

Configuring Mail Proxy

The Mail Proxy can be configured for use either with or without an internal mail server. If you have an internal mail server, you will have to add custom packet filter exceptions to permit inbound SMTP and POP3 traffic as the default exceptions do not cover this type of traffic. These packet filter exceptions are described later in this section.

It is extremely important that you stay up to date with the latest BorderManager patches when using the Mail Proxy. Not only have many problems with the Mail Proxy been addressed with patches, some of the patches provide additional capabilities. Check the readme files for the patches you are installing.

No Internal Mail Server, Mail Through Proxy

In this example, the only mail server exists outside the network at the ISP. Internal users must configure their mail programs (Outlook Express, Eudora, etc.) to point to the Mail Proxy internal IP address. The Mail Proxy then generates new mail (SMTP or POP3) requests to the external server on behalf of the user.

An access rule must be configured to allow access to the Mail Proxy. Generally, the rule will allow a source=Any and a destination=Any.

For outbound SMTP mail, user email comes to the Mail Proxy, and the Mail Proxy looks up the address of the mail server for the message recipient's mail domain and forwards the message. (The Mail Proxy looks at the address of the message, determines the domain, looks up the MX record for that domain, and sends the message on to the mail server defined in the MX record).

When an internal user wants to retrieve email from the ISP's mail server using POP3 protocol, the same process is used, except that the Mail Proxy uses POP3 to retrieve the message.

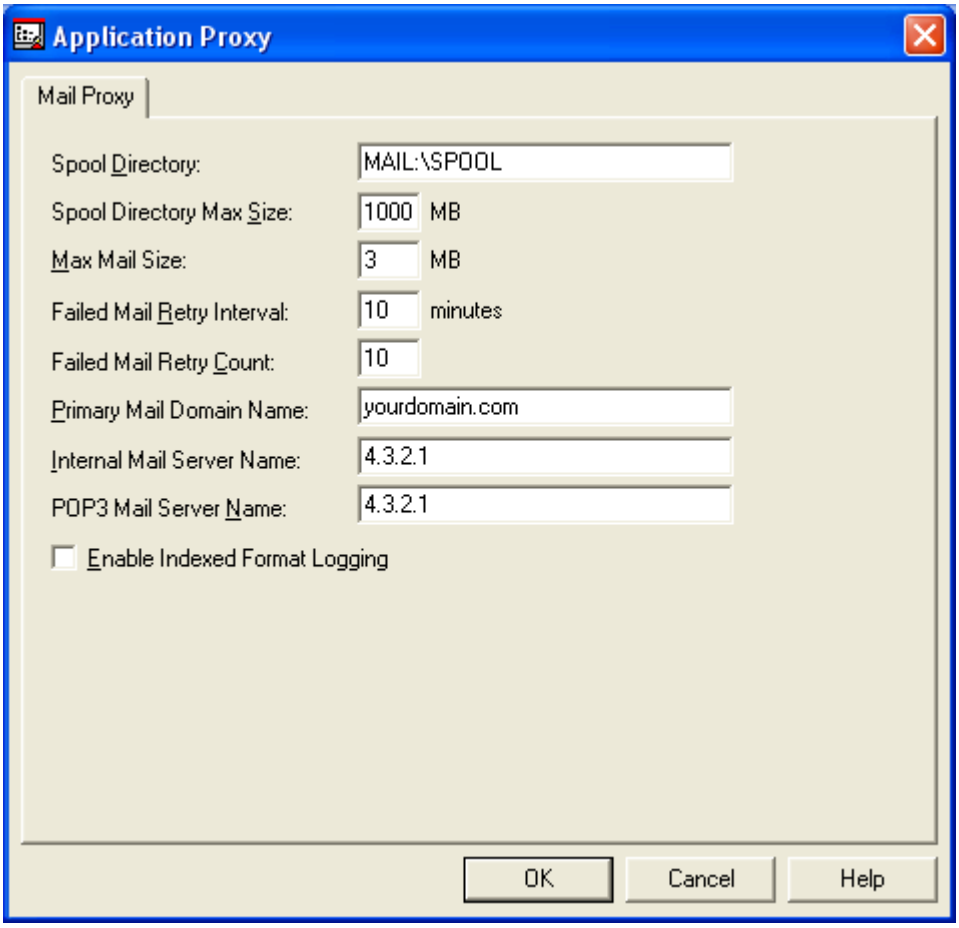
In both cases, the email is temporarily saved to either an Incoming or Outgoing directory used by the Mail Proxy. Those directories are, by default:

SYS:\ETC\PROXY\SPOOL\INCOMING

and

SYS:\ETC\PROXY\SPOOL\OUTGOING

The SPOOL directory is defined in NWADMN32, BorderManager Setup main menu, **Mail Proxy**, **Details**.



The example above shows the mail proxy set up to forward all SMTP and POP3 mail to an external mail server at IP Address **4.3.2.1**. The mail proxy is only being used as a mail relay to the external mail server.

The default spool directory location has been changed off of SYS:\ and onto a volume called **MAIL**, under the directory **SPOOL**. When PROXY.NLM loads the first time after this parameter is changed, it will create the entire directory structure, including the INCOMING and OUTGOING spool directories, in the location specified.

Note Using an NSS volume to hold the spool directory may cause problems.

Outbound SMTP mail will have the domain "**YOURDOMAIN.COM**" substituted for the email domain in the mail message. If the **Primary Mail Domain Name** field were not filled in, Mail Proxy would substitute the domain name in the SYS:\ETC\RESOLV.CFG file. If that file did not specify a name, no domain name would be substituted in the outgoing mail, and the user email program settings would be left intact.

The **Internal Mail Server Name** is somewhat misleading. This field actually is the SMTP server name, regardless of whether or not the SMTP server being configured is internal to the network or out on the Internet. Enter the IP address or DNS name of the SMTP mail server to be used. In general, this server is where the Mail Proxy will attempt to send email.

The **POP3 Mail Server Name** is the IP address or DNS name of the POP3 server that the Mail Proxy will use to retrieve POP3 mail.

Note The latest Proxy/ACL patch will have specific settings required in the SYS:\ETC\PROXY\PROXY.CFG file to be used for configuring the mail proxy. Check the patch instructions carefully.

Internal Mail Server, All Mail Through Proxy

In this example, an internal mail server exists on the private side of the BorderManager server. Internal users must configure their mail programs (Outlook Express, Eudora, GroupWise, etc.) to point to the internal Mail Server.

Besides the Mail Proxy settings to be configured, you must also set up Access Rules and Filter Exceptions. Both are shown later in this chapter.

The Internal Mail Server must point to the private IP address of the BorderManager server as a mail relay host.

An access rule must be configured to allow access to the Mail Proxy. Generally, the rule will allow a source=Any and a destination=Any. However, in this case, an access rule could be configured to allow a source equal only to the IP address of the internal Mail Server. The access rule is only used for outbound traffic.

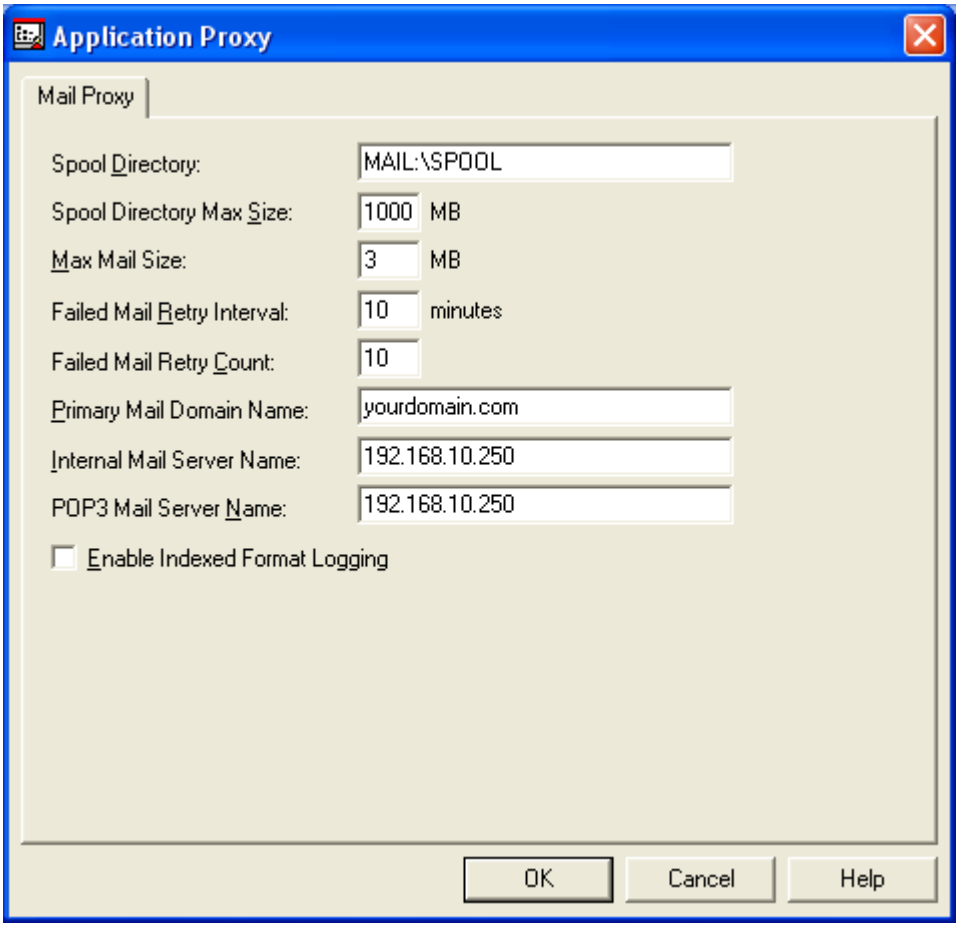
For outbound SMTP mail, user email goes first to the Internal mail server. The SMTP server must be configured to use a mail forwarder, with the BorderManager private IP proxy IP address being used as the forwarding address. The internal mail server sends SMTP mail to the Mail Proxy, and the Mail Proxy looks up the address of the mail server for the message recipient's mail domain and forwards the message. (The Mail Proxy looks at the address of the message, determines the domain, looks up the MX record for that

domain, and sends the message on to the mail server defined in the MX record).

Inbound SMTP mail comes to the public IP address of the BorderManager server and is picked up by the Mail Proxy, assuming you have entered a packet filter exception for SMTP as described above. The Mail Proxy will forward the inbound email to the internal mail server as long as the message is addressed to the domain configured in NWADMN32 as the **Primary Mail Domain Name**. The Mail Proxy can only proxy a single internal mail domain.

When an internal user wants to retrieve email from the ISP's mail server using POP3 protocol, the same process is used, except that the Mail Proxy uses POP3 to retrieve the message.

When an external user wants to retrieve POP3 mail from the internal mail server, that user's email program must be configured to point to the BorderManager server's public IP address.



The example shown above shows settings for an internal SMTP and POP3 mail server at **internal IP address 192.168.10.250.**

The default spool directory location has been changed off of SYS:\ and onto a volume called **MAIL**, under the directory **SPOOL**. When PROXY.NLM loads the first time after this parameter is changed, it will create the entire directory structure, including the INCOMING and OUTGOING spool directories, in the location specified.

Incoming SMTP mail addressed to <username>@YOURDOMAIN.COM will be forwarded on to the mail server. Incoming POP3 mail requests will be forwarded to the mail server as well.

Only mail addressed to the domain **YOURDOMAIN.COM** will be accepted and forwarded, unless using BorderManager 3.8, where you can configure multiple mail domain support.

Note The **Spool Directory** can be located on volume other than SYS, and it is a good idea to keep the spooled data off the SYS volume.

The example shows a maximum mail size of only 3 MB. You may want to set a higher limit.

Note Be sure to check the installation instructions in any BorderManager patches. The Proxy/ACL patch BM35C11 in particular calls out different values to be used than the ones shown in this example.

The **Primary Mail Domain Name** is that name that will be substituted for all outgoing mail messages. If that field is blank, the domain name specified in the SYS:\ETC\RESOLV.CFG file will be substituted in outgoing mail messages. If both are blank, the name supplied by the internal mail server or mail program will be used.

PROXY.CFG Settings for Mail Proxy

BorderManager 3.5 through 3.7

Depending on the patch level of your server, you may be required to have the following entries in the SYS:ETC\PROXY\PROXY.CFG file for Mail Proxy to work. These entries were required in one of the BorderManager 3.5 patches and later to control spam relay problems, and eventually have become requirements.

See Novell TID **10023303.**

```
BM Mail Proxy]
BM_Domain=xyz.com
BM_Incoming_Relay=0
BM_Proxy_Domain=mail-proxy.acctg.xyz.com
```

Edit PROXY.CFG with a text editor, and add the new section **[BM Mail Proxy]**, and underneath that the entry **BM_Domain=xyz.com** where xyz.com would be replaced by the domain name for your email system, such as novell.com.

BM_Incoming_Relay=0 tells Mail Proxy not to allow any relay attempts from the public side, and is the default value.

BM_Proxy_Domain=mail-proxy.acctg.xyz.com should hold the fully-qualified DNS name of the mail proxy, and mail-proxy.acctg.xyz.com is replaced with your domain's actual public record. (The 'A' record for your primary mail domain's MX record). This value is used by the Mail Proxy to advertise its correct name to other SMTP servers, and it may be necessary for the receiving SMTP server to accept mail from you.

BorderManager 3.8, With Multiple Domain Support

Unlike previous versions of BorderManager, version 3.8 can have the Mail Proxy accept incoming email for more than one domain. The email can also be sent to different internal mail servers. The multiple domain support feature is configured with PROXY.CFG entries only – as of this writing, access rules did not affect mail Proxy. The following entries are required in the SYS:ETC\PROXY\PROXY.CFG file in BorderManager 3.8 for support of multiple email domains through Mail Proxy.

```
[Multiple Domain Support]
MultiDomain1=192.168.10.250/home.com
MultiDomain2=192.168.10.251/sysop.com
```

In the example shown above, Mail Proxy will accept email for email domains HOME.COM and SYSOP.COM and forward the inbound SMTP mail to internal servers 192.168.10.250 and 192.168.10.251.

An unpatched BorderManager 3.8 server should not have the section

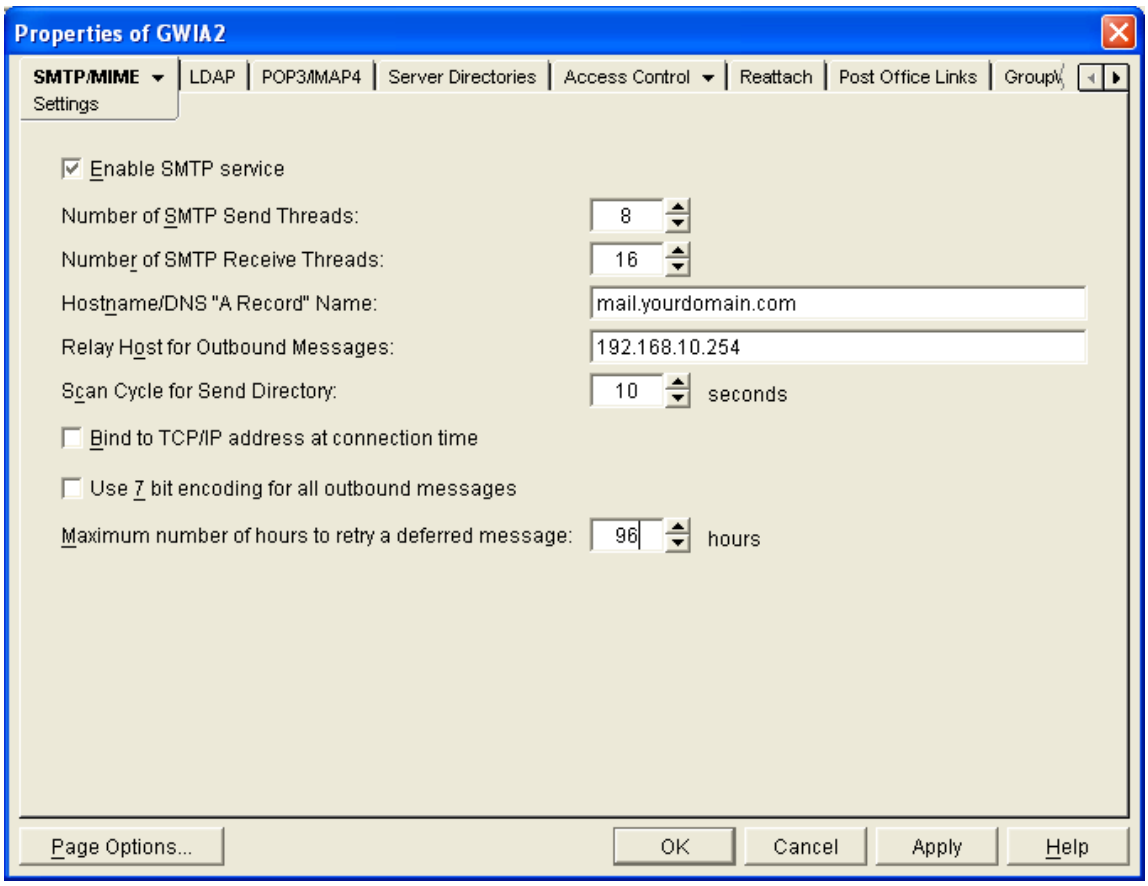
[BM Mail Proxy]

in the PROXY.CFG file, or multiple mail domain support may fail.

GWIA Example Settings

Note This example is for GroupWise Internet Agent running on an internal mail server, NOT on the BorderManager server. If you are running GWIA on the BorderManager server, you would not be using the Mail Proxy.

If you are using GroupWise Internet Agent (GWIA) to send and receive SMTP and POP3 mail, configure the SMTP/MIME Settings to point to the internal IP address of the BorderManager server as shown below.



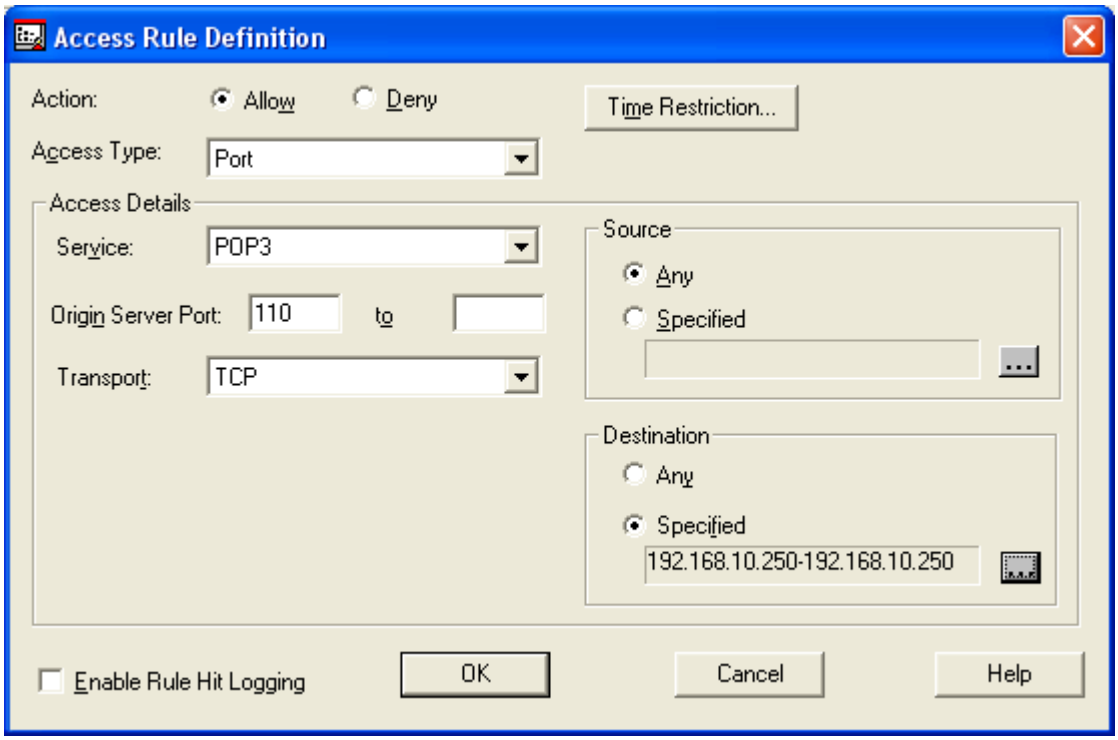
In this example, GWIA is hosted on server ZEN01, and the Mail Proxy is listening on IP address 192.168.10.254. The Mail Proxy is being used as a relay host for outbound email from GWIA.

Note An alternative is to NOT use a relay host, and bypass Mail Proxy for outbound SMTP traffic, by means of filter exceptions and dynamic NAT. This avoids problems like mail getting stuck in the Mail Proxy spool directories, and some other issues.

Access Rules to Allow POP3 Through Mail Proxy

Inbound POP3 to Internal Mail Server

If a user on the Internet wishes to access data from an internal POP3 mail server, via the Mail Proxy, an access rule and a packet filter exception must be configured.



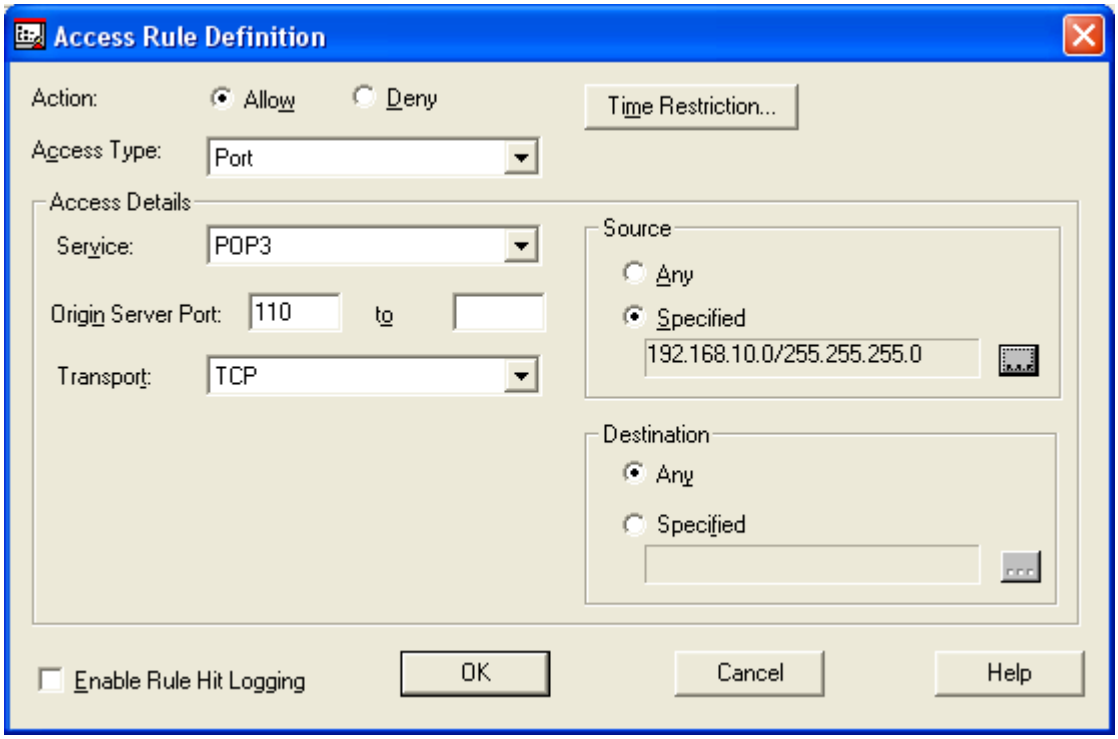
The example shown allows any source to use POP3 protocol through the Mail Proxy to reach internal IP address 192.168.10.250, which is an internal POP3 server.

Note that the Mail Proxy configuration is completely different when used with an internal mail server than when used for an external mail server (at an ISP).

This rule is intended to be used when the Mail Proxy is configured to point to an internal mail server providing POP3 service. Users on the Internet can access the internal POP3 server by pointing their email client to the BorderManager server's public IP address, assuming that filter exceptions are in place allowing port 110 to that IP address.

Outbound POP3 to External Mail Server

If a user on the internal LAN wishes to access data from an public POP3 mail server, via the Mail Proxy, an access rule must be configured.

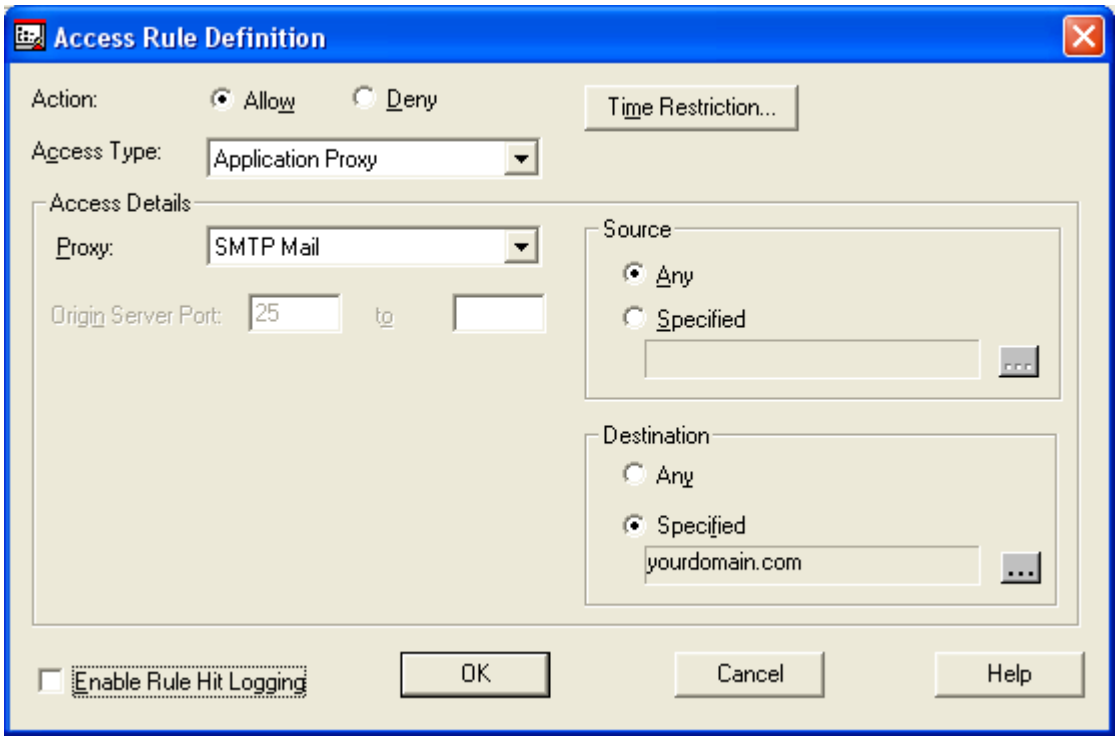


This access rule allows any host on the internal subnet 192.168.10.0 to make a POP3 request through the Mail Proxy to an external POP3 server on the Internet. The Mail Proxy must already have been configured to point POP3 to a public mail server.

The mail program on the internal host should be configured for the internal IP address of the BorderManager server, not the Internet POP3 server. When the POP3 requests are received by the Mail Proxy, they are passed on to the Internet POP3 server configured in the Mail Proxy settings.

The default filter exceptions for BorderManager 3.6 and earlier allow all outbound traffic from the primary public IP address, so outbound POP3 requests do not require an additional packet filter exception. BorderManager 3.7 and later may or may not have those filter exceptions in place, depending on the installation sequence, and patch level.

Access Rule To Allow SMTP Through Mail Proxy



Access rules controlling SMTP usage through the Mail Proxy have varied with patch level. In some cases, outbound SMTP mail will not be sent if you do not have an access rule set up to allow the use of the SMTP Mail Proxy, but Inbound mail will still be accepted and forwarded to the internal mail server without an access rule.

With later patches, inbound mail required an access rule, and the destination domain name was required to be added, as shown in the example above.

At some point, patches were added that required certain entries be added to the PROXY.CFG file to prevent spam relay, and to specify the domain name to be used by Mail Proxy.

With BorderManager 3.8, virtually all control of the mail proxy is done with entries in PROXY.CFG and not with access rules. Both single and multiple domain support is defined in PROXY.CFG, as well as anti-relay measures to prevent relaying on the public IP address used by Mail Proxy.

If you want, or need, to control Mail Proxy with access rules, configure the source or destination mail user name or domain as needed to specify how Mail Proxy allows SMTP traffic.

Access Rules to Control Use of Mail Proxy

The previous page discussed how access rules might or might not be applicable, depending on the Mail Proxy patch level. (Much of the access control for Mail Proxy has been gradually shifted to PROXY.CFG settings over time.)

BorderManager 3.5 and later require PROXY.CFG settings described earlier, possibly in addition to the access rules shown below. See Novell TID **10023303**.

This section shows the access rules that would be required in versions of Mail Proxy that honor access rules.

The way to control unwanted mail relaying involves using a series of Access Rules to allow certain hosts to send mail, and deny everyone else. Even with the access rules shown, there is a vulnerability to mail relaying that requires the BorderManager server to be patched, so stay abreast of the latest patch sets.

Internal Mail Server

If you have an internal SMTP mail server, use the following rules. The theory is this:

1. Allow any internal user to send SMTP mail anywhere – or allow your internal mail server to send mail anywhere.
2. Allow external SMTP mail to be sent only to your domain. (This means to allow inbound SMTP mail through to your internal mail server, and block any other mail being relayed to some other domain) Without this rule, mail sent to some other domain can be bounced off your mail server.
3. Deny all other access.

No Internal Mail Server

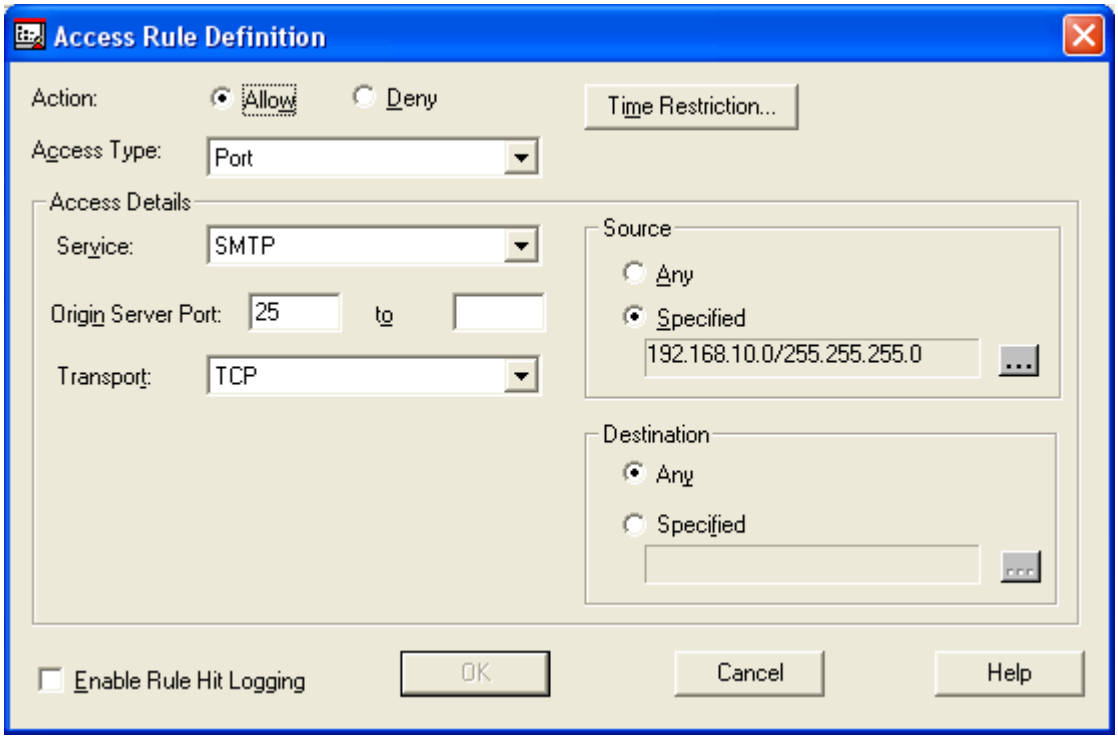
In this case, you only want to allow SMTP mail to be sent out. When your internal users want to receive mail, they do that with POP3, not SMTP. This case is simpler than the earlier example in that you simply want to allow internal users to send SMTP out and deny everything else.

1. Allow any internal user to send SMTP mail anywhere.
2. Deny all other access.

Access Rule Examples

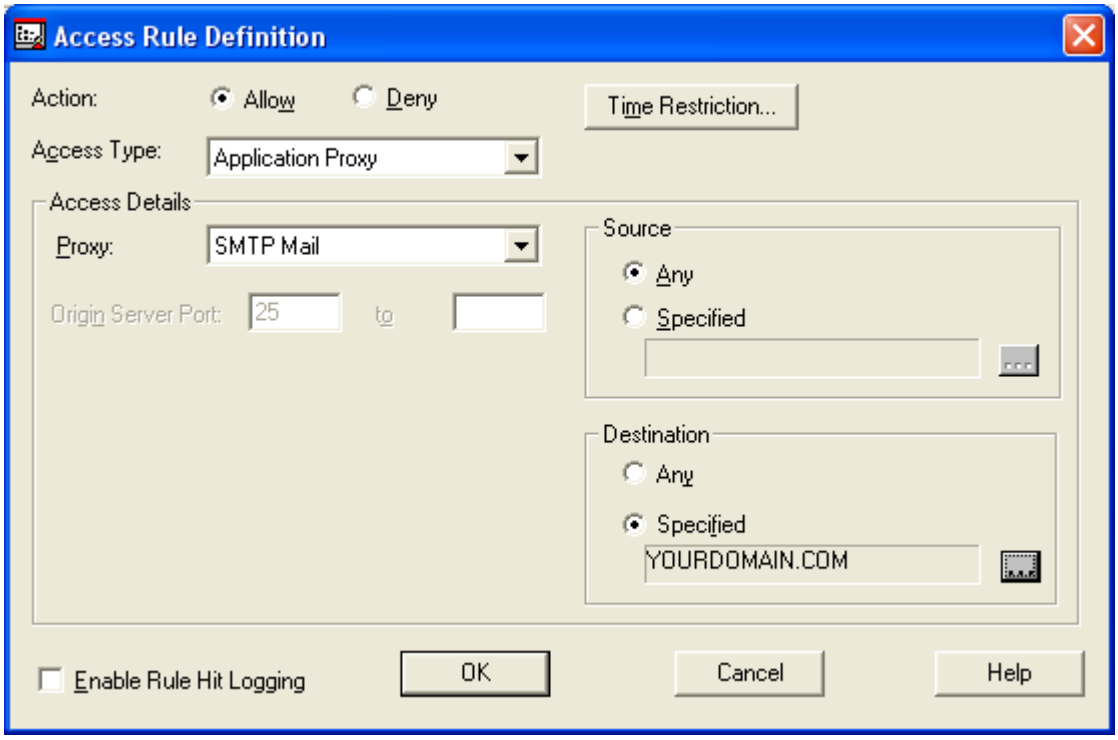
Allow outbound SMTP

The Mail Proxy does not allow specifying a source equal to an IP address, so you must instead use a port-based rule.



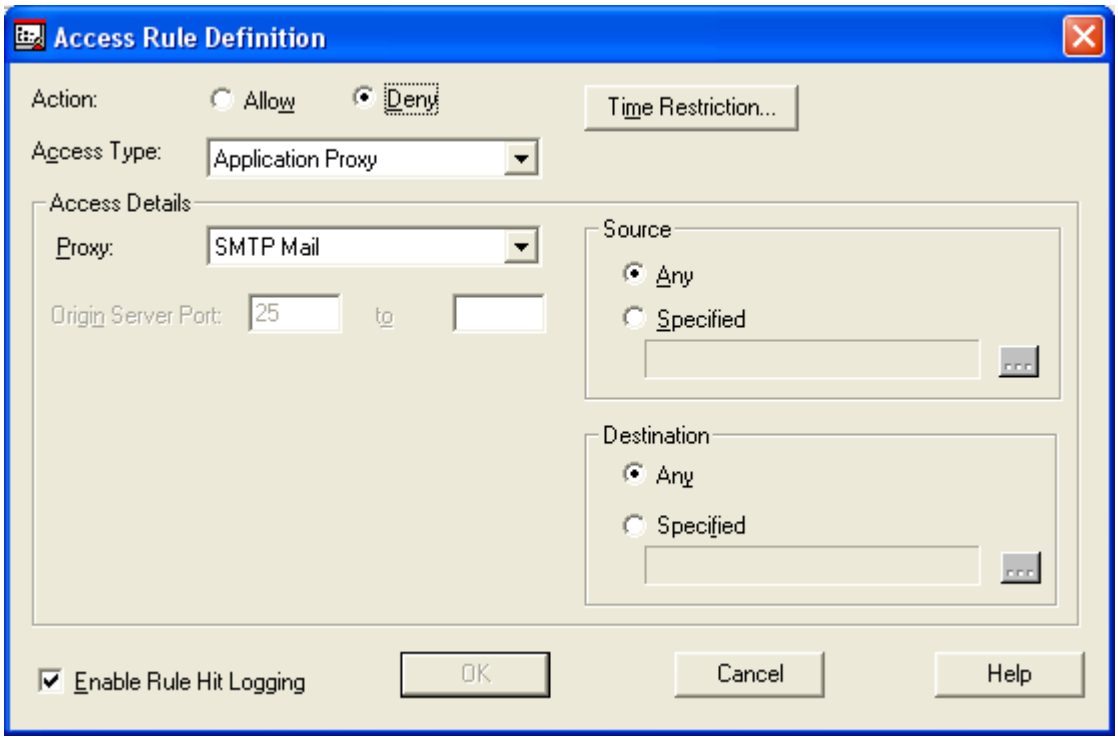
This access rule allows any host on the private internal subnet 192.l68.10.0 to use port 25 (SMTP).

Allow Inbound SMTP to Internal Mail Domain



This access rule will allow SMTP from anywhere to be forwarded only to the internal mail domain YOURDOMAIN.COM.

Deny All SMTP

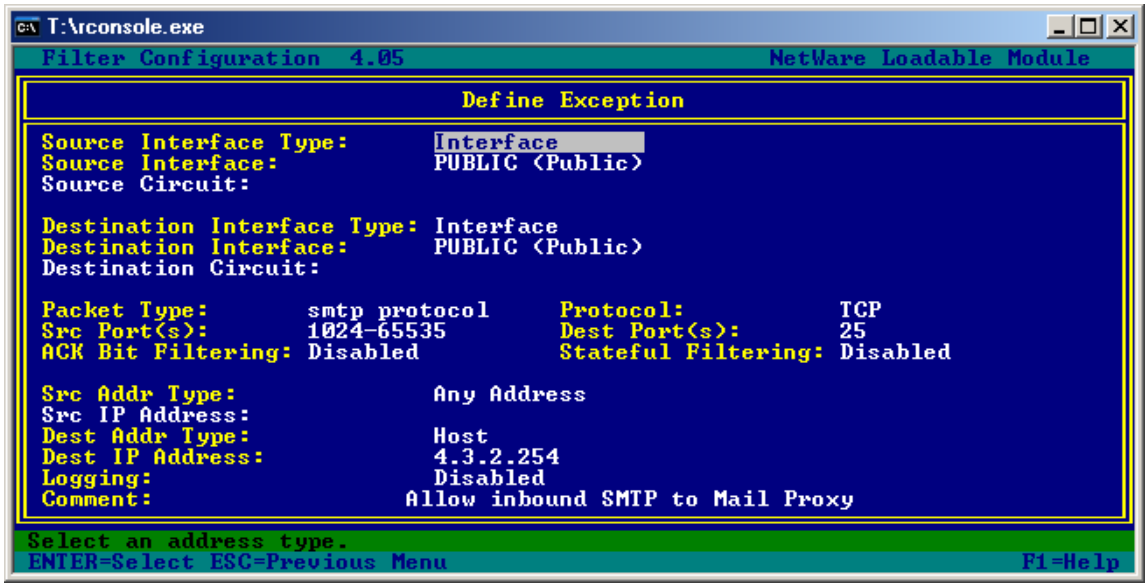


After allowing selected SMTP mail out and in, you need to have an access rule to deny all other SMTP traffic. The default rule can also do this for you. This rule simply adds logging capability to the denial so that you can see if someone is attempting to use the Mail Proxy for SMTP mail relay.

Filter Exceptions Required for Mail Proxy with Internal Mail Server

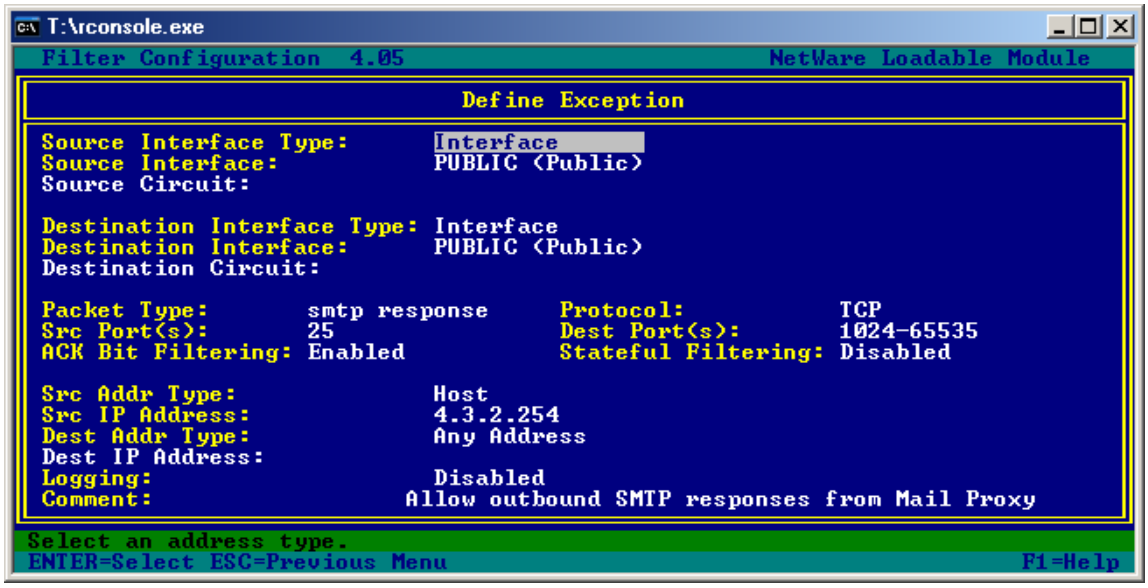
SMTP Filter Exceptions

In order for the Mail Proxy to receive SMTP mail from the Internet, a non-stateful packet filter exception needs to be configured using FILTCFG.NLM as follows:



The public IP address must be defined as the MX record in the public DNS servers for your domain in order for mail to be forwarded to your email server from the Internet. This exception is only need if you have an internal SMTP server receiving mail from the Internet. If you are using Mail Proxy only for sending mail outbound, this exception is not required.

If you have a BorderManager 3.7 server, the default exceptions can be different from prior versions, and you might require another filter exception to allow outbound responses to inbound SMTP packets.

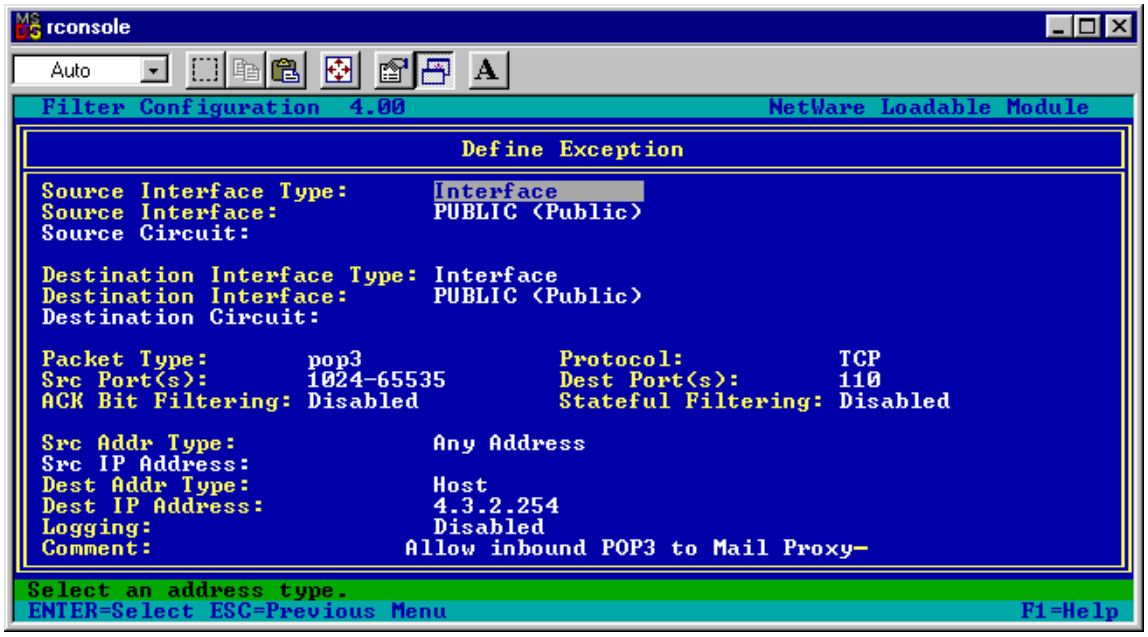


The filter exception shown above allows the Mail Proxy to send outbound responses to inbound SMTP requests. This filter might be needed for BorderManager 3.7 servers, but the default exceptions for prior versions should already allow this traffic.

POP3 Filter Exceptions

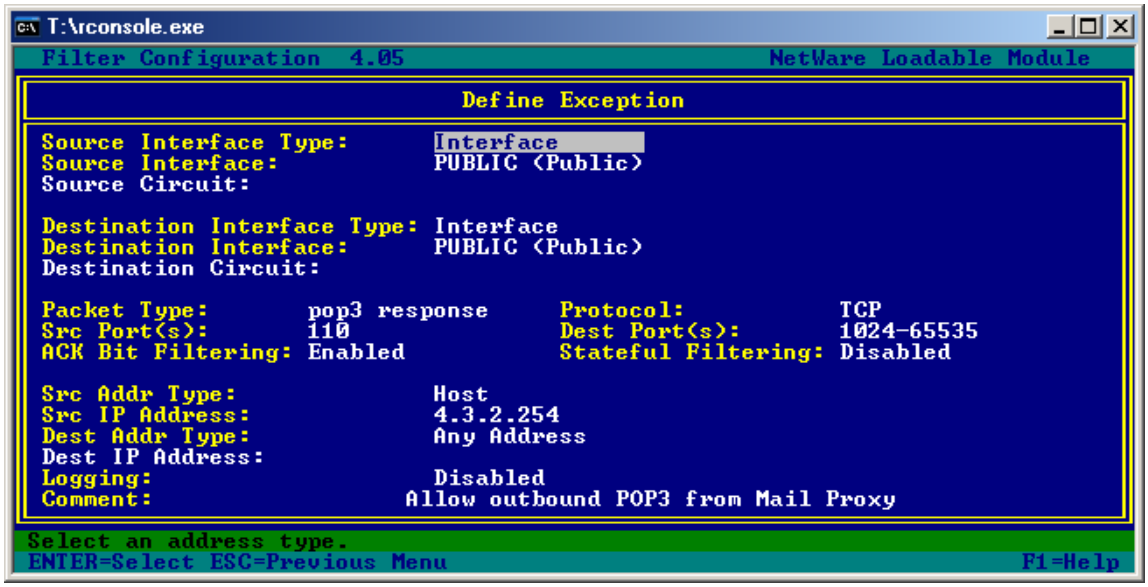
Unlike outbound POP3 traffic, inbound traffic also requires a custom packet filter exception to be configured to allow TCP port 110 to whichever public IP address is being used for POP3 mail. The default packet filter exceptions do not include an exception for POP3.

Configure a POP3 filter exception using FILTCFG.NLM as follows to allow POP3 to the BorderManager server public IP address.



The custom packet filter exception shown above allows TCP destination port 110 to be allowed through the default filters to the public IP address 4.3.2.254 only.

For BorderManager versions prior to 3.7, this should be the only filter exception needed. For BorderManager 3.7, you must also add an exception to allow outbound SMTP responses to inbound requests.



The example above shows a filter exception allowing a BorderManager 3.7 Mail Proxy to respond to inbound POP3 requests from the Internet.

<This page intentionally left blank. This is to facilitate putting in chapter tabs in a ring binder for double-sided printing. The main chapters should start on an odd-numbered page.>

Chapter 10 - News Proxy

Concept

Use a special proxy to pass NNTP (Usenet) traffic through BorderManager with control of individual Usenet groups by access rules.

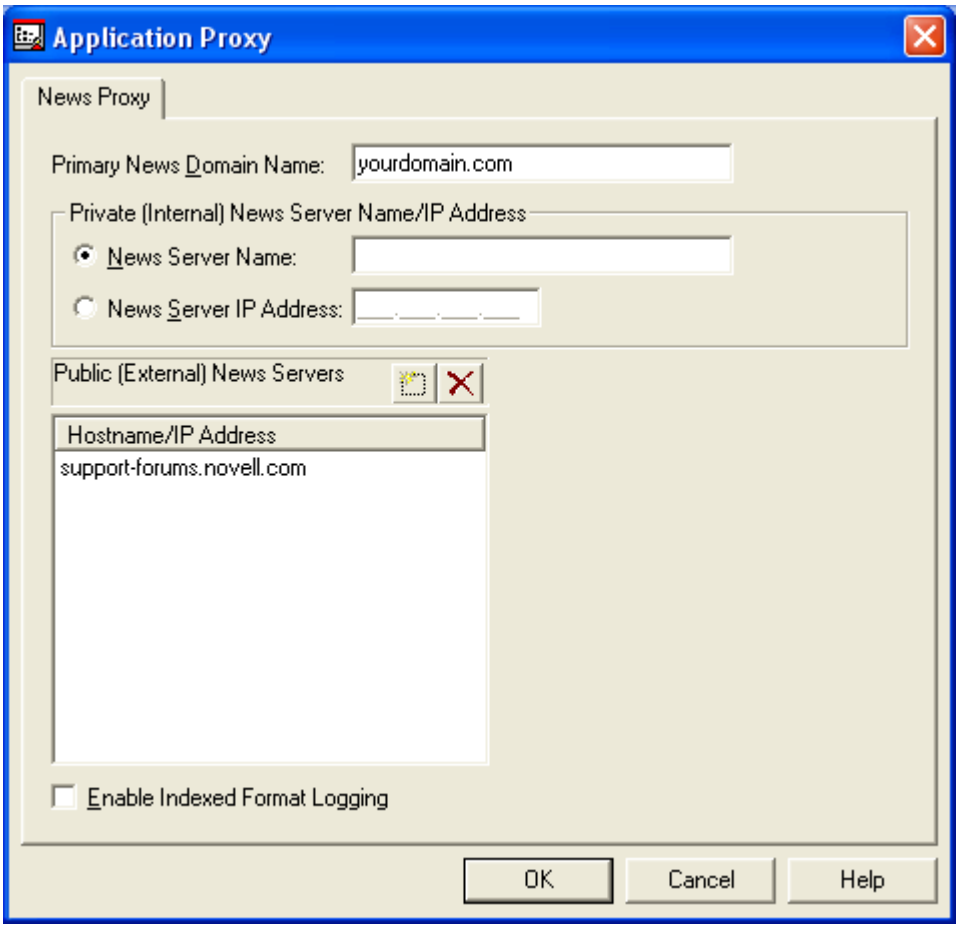
Pros

- You can tightly control what Usenet groups are accessible to internal hosts, by access rules that call out individual newsgroups.
- You can control posting as well as reading, through use of access rules.

Cons

- You can only proxy a single external Usenet server.
- It can be extremely tedious to enter in all the individual newsgroups that internal users may wish to access. (There are over 30,000 newsgroups).
- Internal NNTP programs (Outlook Express, Free Agent, etc.) must be configured to point to the private IP address of the BorderManager proxy server.

Using News Proxy With An External NNTP Server



In the BorderManager Setup main menu, check the **News Proxy** box, and then click on **Details** to configure this proxy.

In the example shown above, the NNTP proxy will provide access to the NNTP server support-forums.novell.com. In your newsreader configuration, you will have to use the private IP address of the BorderManager server instead of the real IP address of the NNTP server you are proxying.

While you can fill in multiple External news server addresses, only one of them will be used. Normally, the first news server address on the list is used, with additional entries being used for failover, in case the first news server does not respond to NNTP requests.

Filling in the Primary News Domain Name (in this case with YOURDOMAIN.COM) will replace the NNTP message headers on message you post with the name configured instead of passing on

whatever name is configured on the newsreader program. If you leave this field blank, the domain configured in the SYS:\ETC\RESOLV.CFG file will be substituted. If that entry also is blank, the IP address of the server may be substituted.

This example does not show an internal NNTP server being used. If you want to use the News Proxy to proxy data to and from an internal NNTP server, you need to enter the internal DNS name or internal IP address of your local NNTP server. On top of that, you will have to set up a packet filter exception to allow NNTP traffic (TCP destination port 119) to the public IP address of the BorderManager server, and add access rules to allow inbound NNTP traffic through this proxy.

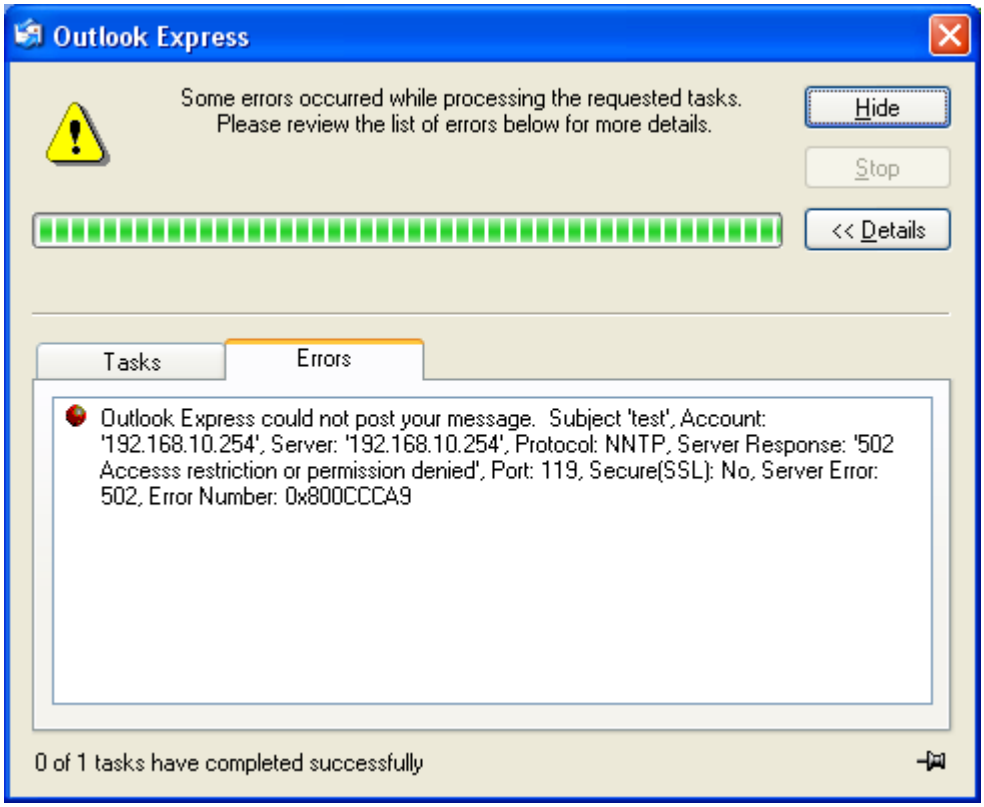
You will need to add an access rule to allow outbound use of the News Proxy. The access rules can specify which news groups are allowed to be proxied. Examples of the access rules required are shown in the chapter on access rules.

Two different kinds of access rules are available for the News Proxy: News Proxy (Read) and News Proxy (Post). Read is used to control which newsgroups can be read, while Post is used to control which newsgroups you can post to.

You must add a packet filter exception to allow NNTP traffic to the BorderManager public IP address in order to allow the News Proxy to pass NNTP traffic through to an internal NNTP server. The default packet filter exceptions for BorderManager 3.6 and earlier already allow the outbound traffic needed by the News Proxy. Later versions of BorderManager may or may not have the required exceptions depending on the installation sequence.

If you do not have an internal NNTP server, you do not need to add any special packet filter exceptions beyond the default packet filter exceptions, for BorderManager 3.6 and earlier. Later versions of BorderManager may or may not have the required exceptions depending on the installation sequence.

Access Rules Blocking Posting

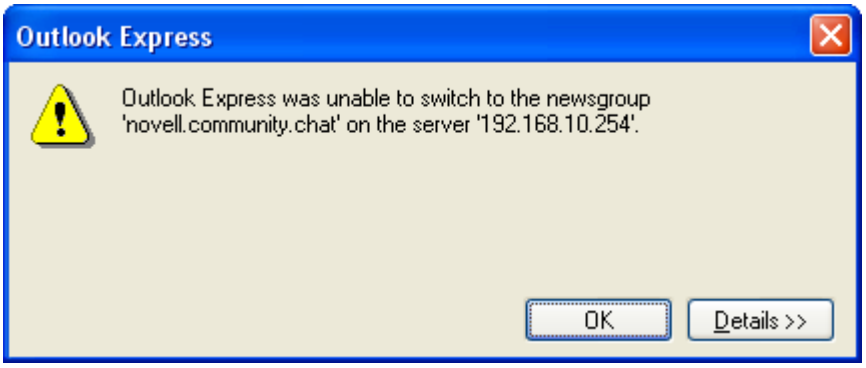


If you do not have an access rule to allow posting through the News Proxy, or if you have an access rule to deny posting to a specific newsgroup, your newsreader should give you an error message.

In the example shown above, Outlook Express was blocked from trying to post a message to the novell.community.chat newsgroup by a Deny access rule for News Proxy posting.

News Proxy was configured to point to support-forums.novell.com, and Outlook Express was configured to point to a NNTP server at the BorderManager proxy address 192.168.10.254.

Access Rules Blocking Reading



If you do not have an News Proxy access rule allowing you to read a specific newsgroup, your newsreader should give you an error message.

In the example shown above, a Deny rule for News Proxy was used to block reading the newsgroup novell.community.chat, and Outlook Express was blocked when trying to access that group. News Proxy was configured to point to support-forums.novell.com, and Outlook Express was configured to point to a NNTP server at the BorderManager proxy address 192.168.10.254.

<This page intentionally left blank. This is to facilitate putting in chapter tabs in a ring binder for double-sided printing. The main chapters should start on an odd-numbered page.>

Chapter 11 - Real Audio Proxy

Concept

Use a special proxy to pass RealAudio or RTSP traffic through BorderManager with control by access rules.

BorderManager 3.0 provides some means of proxying RealAudio data. BorderManager 3.5 and later also provides the ability to proxy data using RTSP.

Pros

You can control individual host or internal network IP addresses that are allowed to use RealAudio (and RTSP). This can have a major impact on bandwidth usage, by reducing the amount of streaming audio and video that flows through the server.

You can control access to particular DNS addresses, to tightly control any RealAudio or RTSP traffic in the extreme.

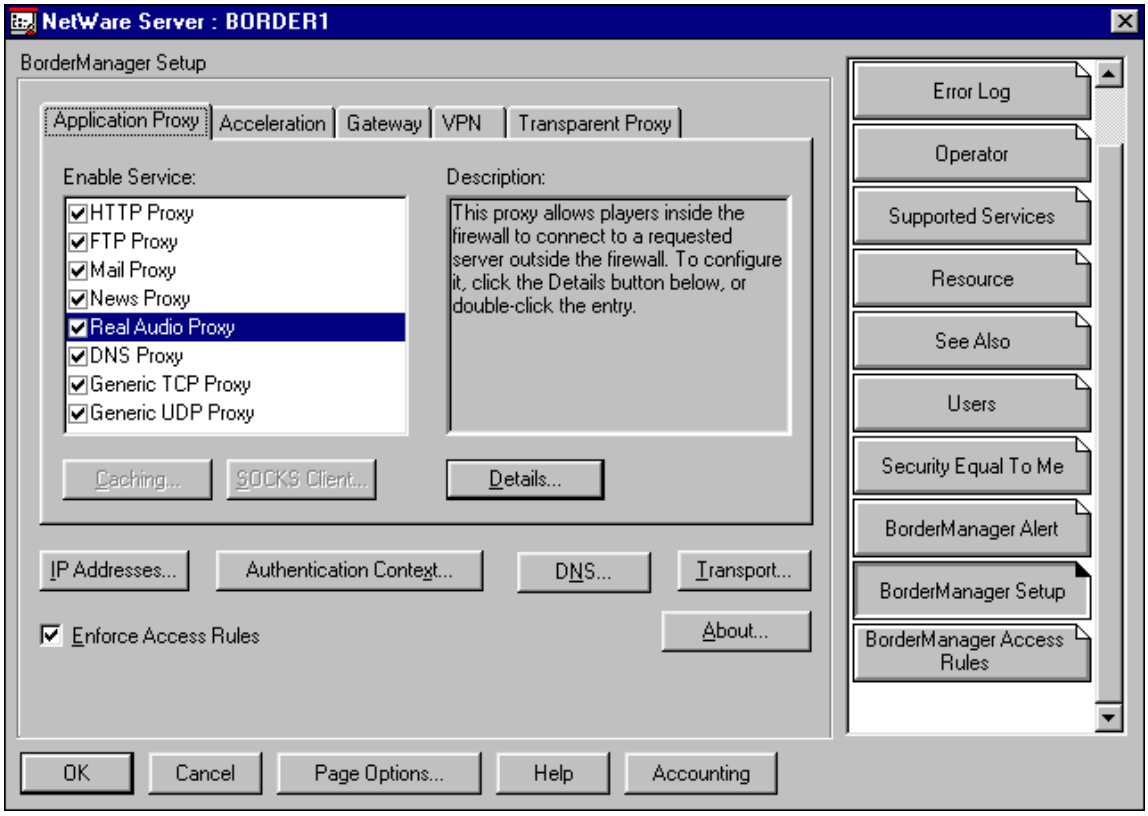
Cons

You must configure non-standard settings on the RealAudio and RTSP clients to make use of the proxy.

QuickTime (and potentially other) RTSP clients don't work well, or at all, with the RTSP proxy.

You can only control access to the proxy via IP address or network address.

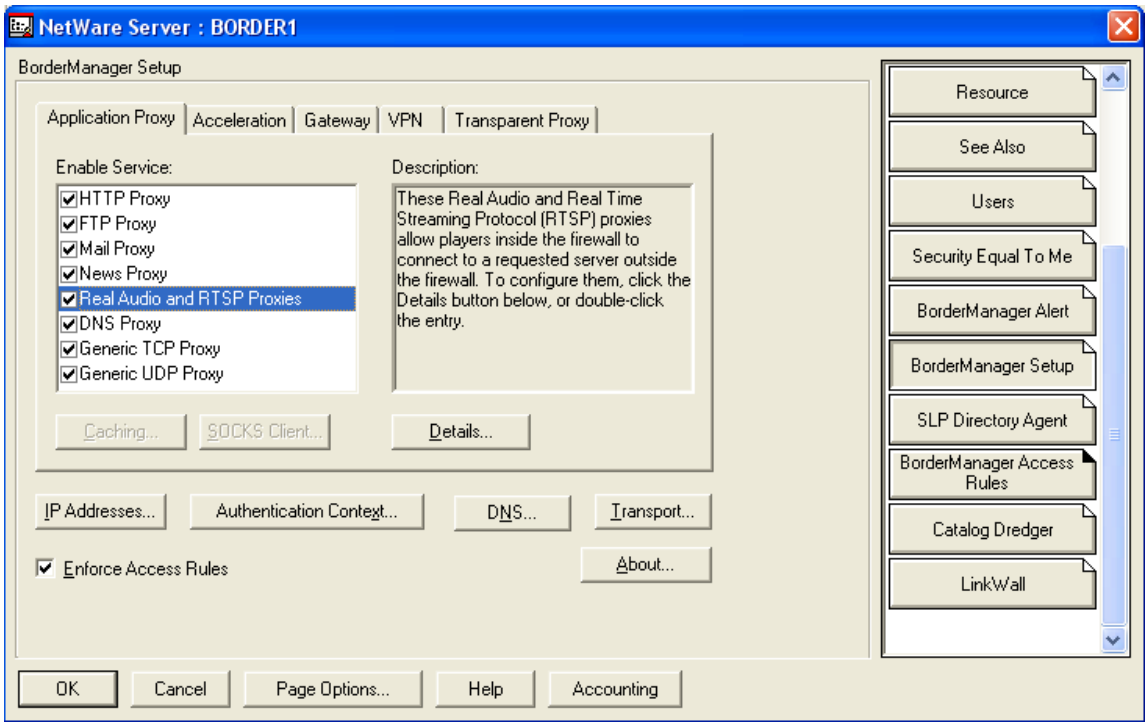
BorderManager 3.0 Settings



BorderManager 3.0 RealAudio Proxy

There is very little configuration done at the BorderManager Setup main menu screen to enable the Real Audio Proxy. Simply check the Real Audio Proxy box. Click on **Details** to bring up a menu where you can also enable Indexed logging.

BorderManager 3.5 & Later Settings

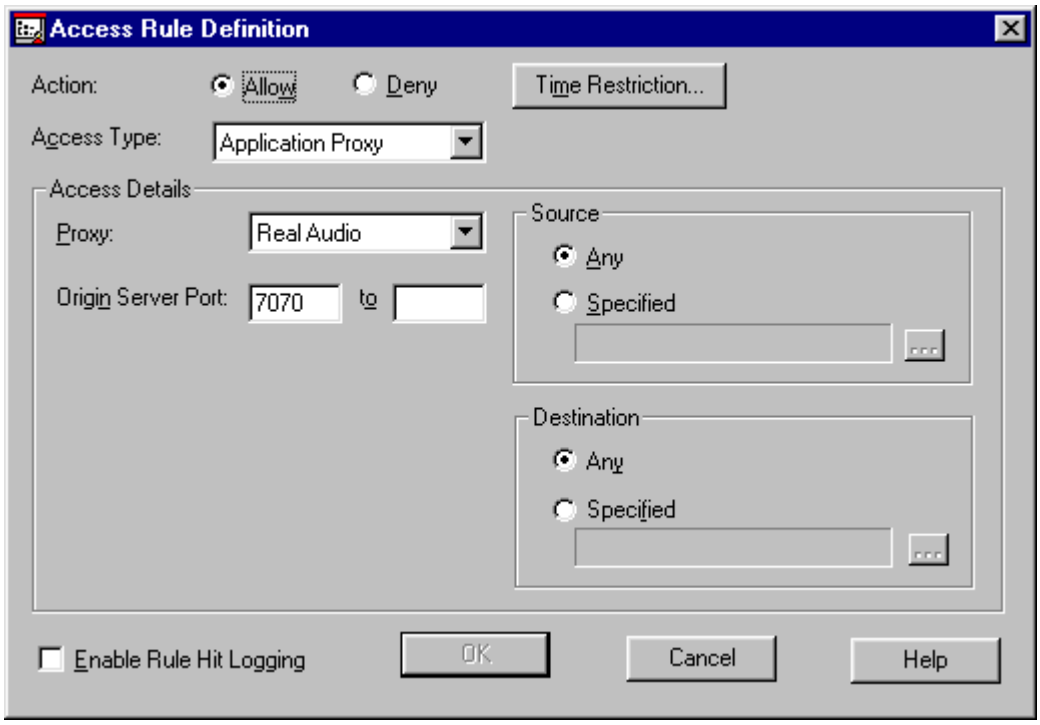


BorderManager 3.5 & Later Real Audio and RTSP Proxies

BorderManager 3.5, 3.6, 3.7 and 3.8 have the additional capability to proxy RTSP (real time streaming proxy)

You need to add an access rule to allow the use of the Real Audio proxy.

BorderManager 3.0 RealAudio Proxy Access Rule

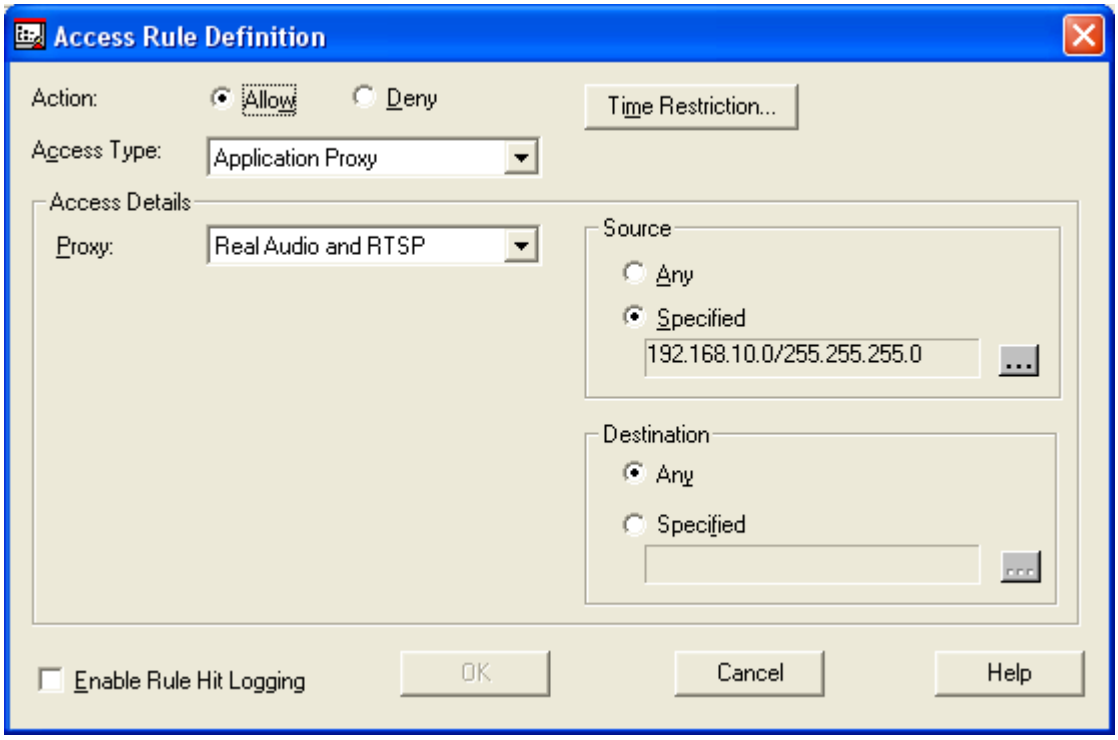


The example above shows a BorderManager 3.0 Access Rule to allow the Real Audio proxy to function for any internal user to any external Real Audio IP address.

Access rules for the RealAudio proxy cannot use NDS objects (user, group or container) in the Source definition.

You must match the Real Player settings at the PC to the port numbers used in the Access Rule.

BorderManager 3.5 & Later RealAudio and RTSP Access Rule



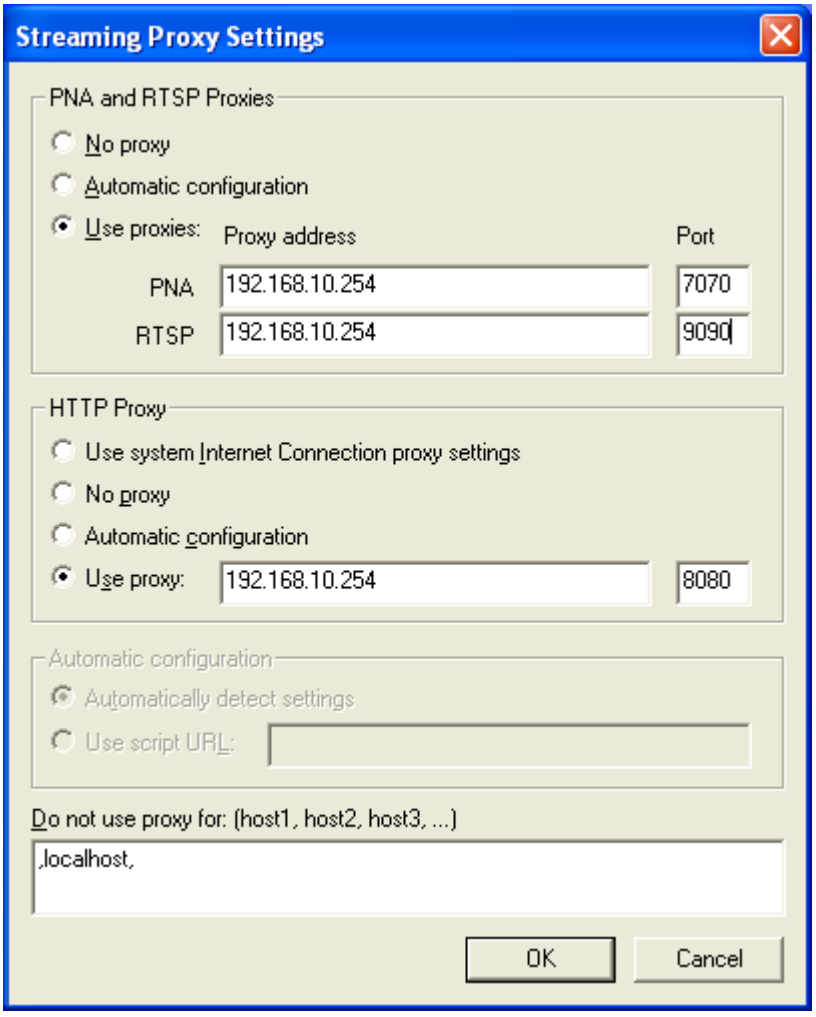
BorderManager 3.5, 3.6, 3.7 and 3.8 access rules are different from BorderManager 3.0 when it comes to the Real Audio and RTSP Proxy. With BorderManager 3.5, 3.6, 3.7 and 3.8, you do not configure the port number in the access rule. However, the port numbers are still fixed at 7070 (RealAudio/PNA) and 9090 (RTSP).

Access rules for the RealAudio and RTSP proxy cannot use NDS objects (user, group or container) in the Source definition.

The example shown above allows use of the RealAudio/RTSP proxy, but only for internal users on the 192.168.10.0 network.

RealOne (Free) Player Configuration

With the RealOne Player (version 2.0 shown here) installed, select **Tools**, **Preferences**, **Proxy Settings**. RealOne will probably default to using HTTP Proxy settings for Internet Explorer for HTML contents.



To configure the streaming content to use the RealAudio/RTSP Proxy from BorderManager 3.5 or later, click on the Streaming Settings **Change Settings** button in the lower half of the menu screen.

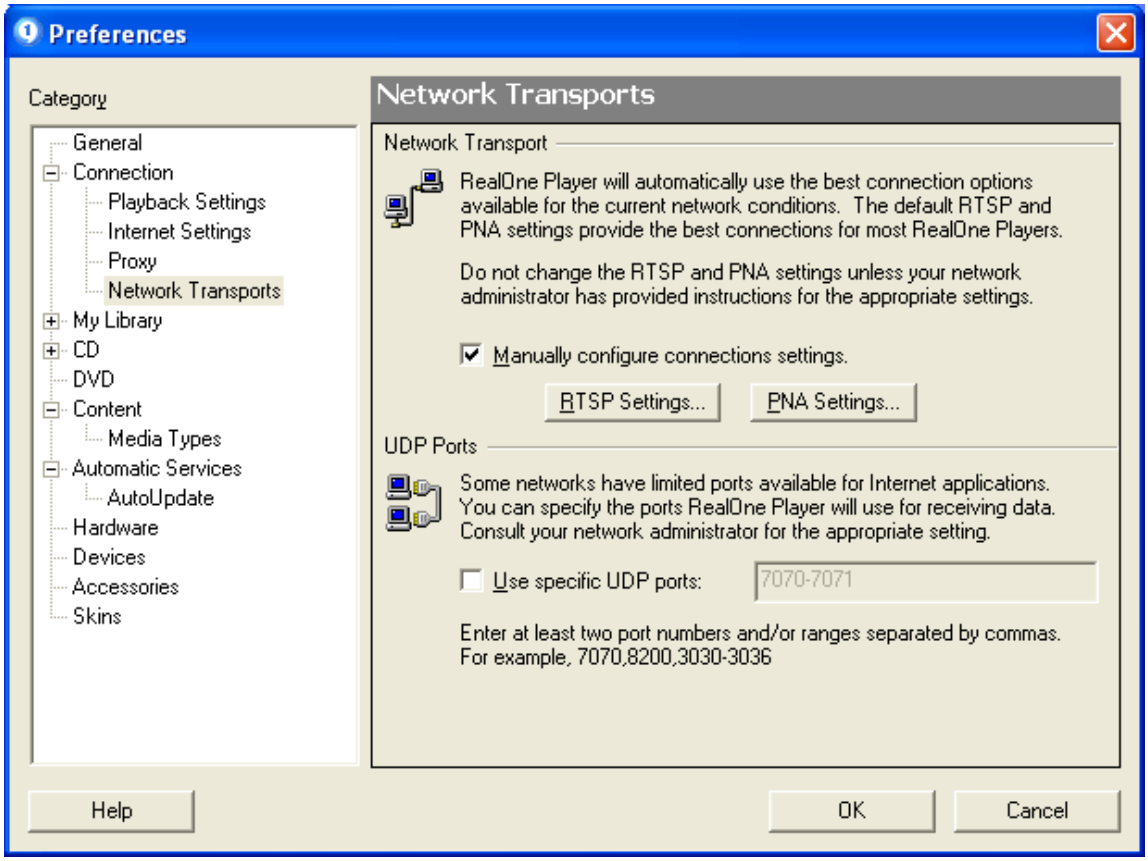
Select **Use proxies** in the PNA and RTSP Proxies menu.

Enter the BorderManager server **private proxy IP address** in both the **PNA** and **RTSP** fields.

Enter port **7070** for PNA proxy port and **9090** for RTSP proxy port.

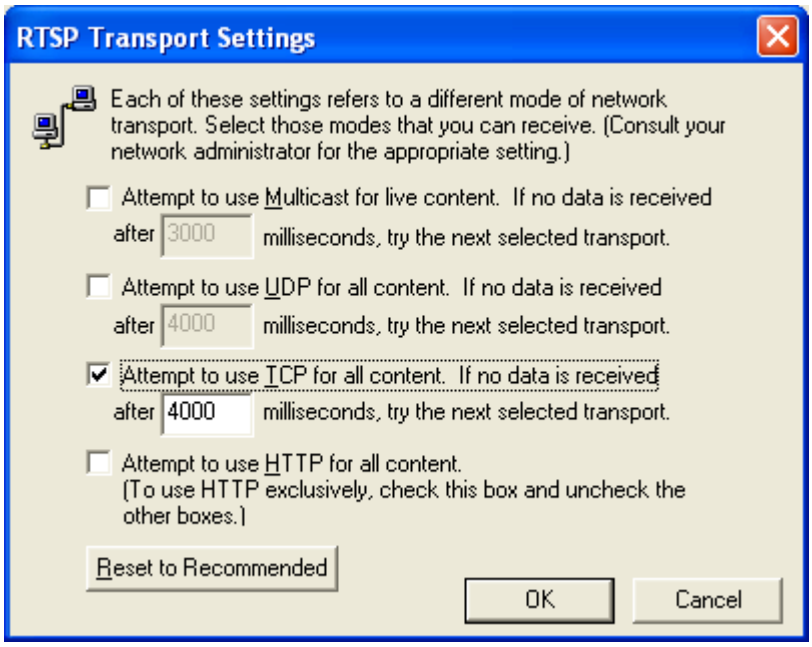
The HTTP Proxy settings should match your browser settings for HTTP Proxy, using the BorderManager private proxy IP address and port 8080.

Click **OK** to save those settings.



Now select **Network Transports**. Then check the box labeled '**Manually configure connections settings'**.

Select the **RTSP Settings** button.

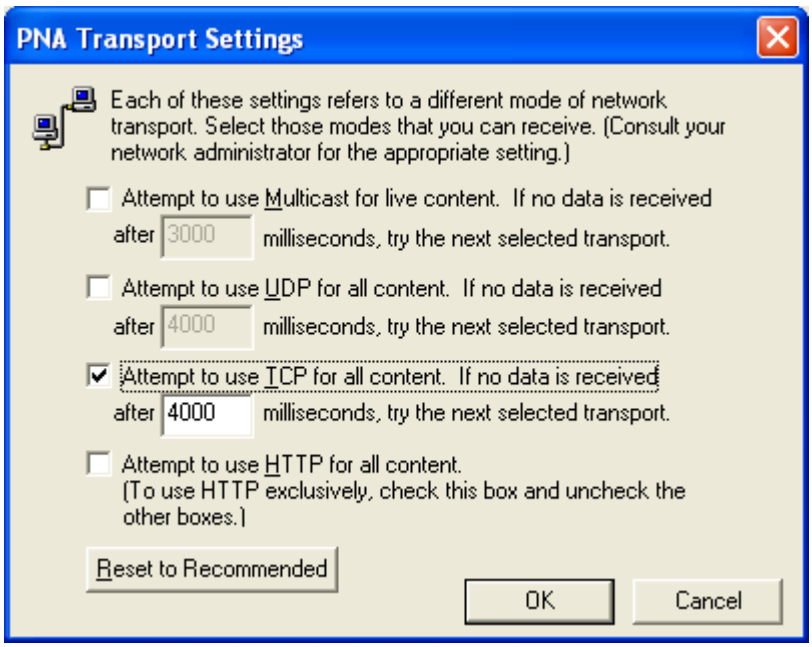


Uncheck all boxes except '**Attempt to use TCP for all content**'.

If you want to allow RealOne to try to also make use of streaming through the HTTP Proxy, leave the '**Attempt to use HTP for all content.**' box checked.

Click **OK**.

Click on the **PNA Settings** button.



Uncheck all boxes except '**Attempt to use TCP for all content**'.

If you want to allow RealOne to try also to make use of streaming through the HTTP Proxy, leave the '**Attempt to use HTP for all content.**' box checked.

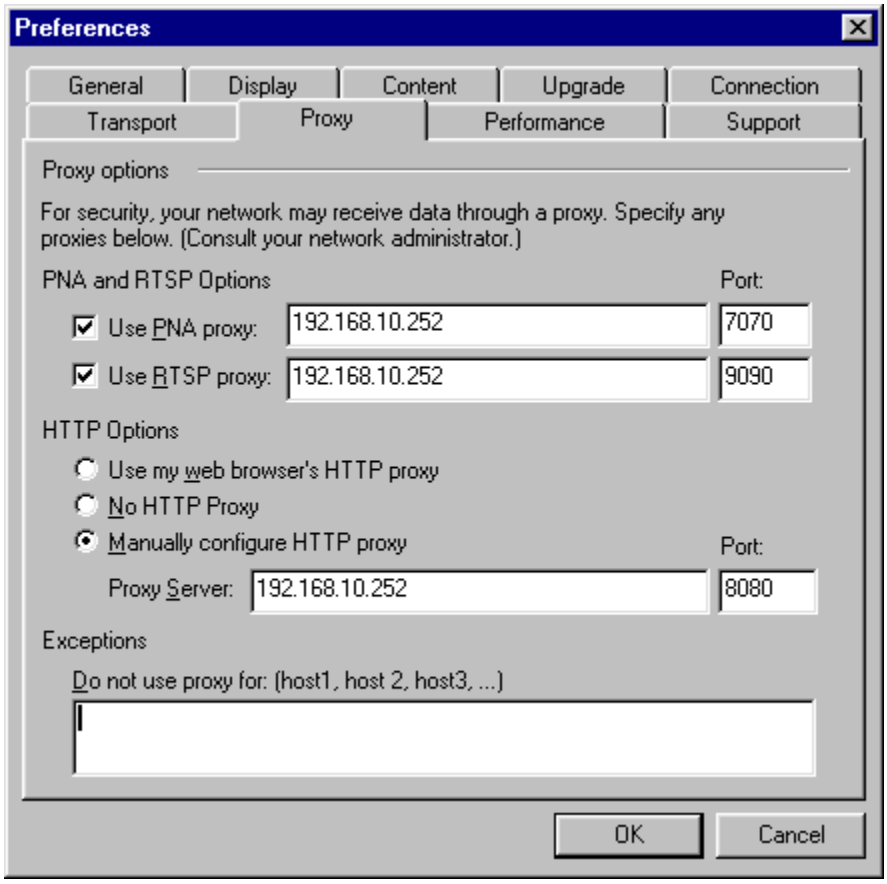
Click **OK**. Then click **OK** again to save all the preferences.

Add an access rule to allow use of RealAudio/RTSP Proxy. An example is shown in the access rules chapter.

Test RealOne. If content is being received through the RealAudio proxy, Proxy Console (at the BorderManager server) option 19, then option 5 should show RealAudio proxy statistics increasing. If RTSP Proxy is being used, Proxy Console option 19, then option 7 should show statistics increasing. ACL denials on those screens indicate that an access rule to allow usage is needed.

RealPlayer G2 Configuration

In order to use the BorderManager proxy, the RealAudio client (RealPlayer G2 version 7.0 in this example) must be configured to use the BorderManager proxy settings.



These are settings on RealPlayer G2 for use through a proxy. The PNA and RTSP port numbers are NOT the default options.

If you select '**Use my web browser's HTTP proxy'**, be aware that the browser referred to is Internet Explorer and not Netscape.

If you have configured Proxy Authentication on the BorderManager server, you will need to be running CLNTRUST on the PC to allow the HTTP Proxy to be used.

RealAudio / RealPlayer 'locates' multimedia sites using the HTTP port number, then transfers data on the PNA (RealAudio) or RTSP (Real Time Streaming Protocol) port numbers.

Note The PC-to-proxy data for the RTSP protocol is sent using port 9090, while the proxy-to-RTSP host data will use port 554.

Chapter 12 - DNS Proxy

Concept

The DNS Proxy sends DNS requests to the Internet for a) better security, and b) better performance. The DNS data is cached at the BorderManager server so that multiple requests from the clients do not actually have to be sent to the DNS server again.

The clients (user PC's) would be configured to use the BorderManager private IP address in their DNS settings.

I recommend only using the DNS Proxy if you do not have an internal DNS server. However, with the proper configuration of the DNS server, you can easily use both.

Pros

- BorderManager caches DNS queries so that later requests for the same URL do not generate Internet bandwidth and can be answered quickly.
- The DNS Proxy can serve as a 'Poor Man's DNS Server', by allowing DNS queries to URL's entered in the BorderManager server's SYS:ETC\HOSTS file. (Only 'A' type records can be used in the HOSTS file).

Cons

- None, really, if the server is properly patched and tuned. The DNS Proxy will conflict with a DNS server running on the same server, as both will need to use port 53, but that is not really a valid argument against using DNS Proxy.
- Because DNS proxy caches data, if you make a change to an internal DNS server record, you may still get the old value out of the cached DNS Proxy data.

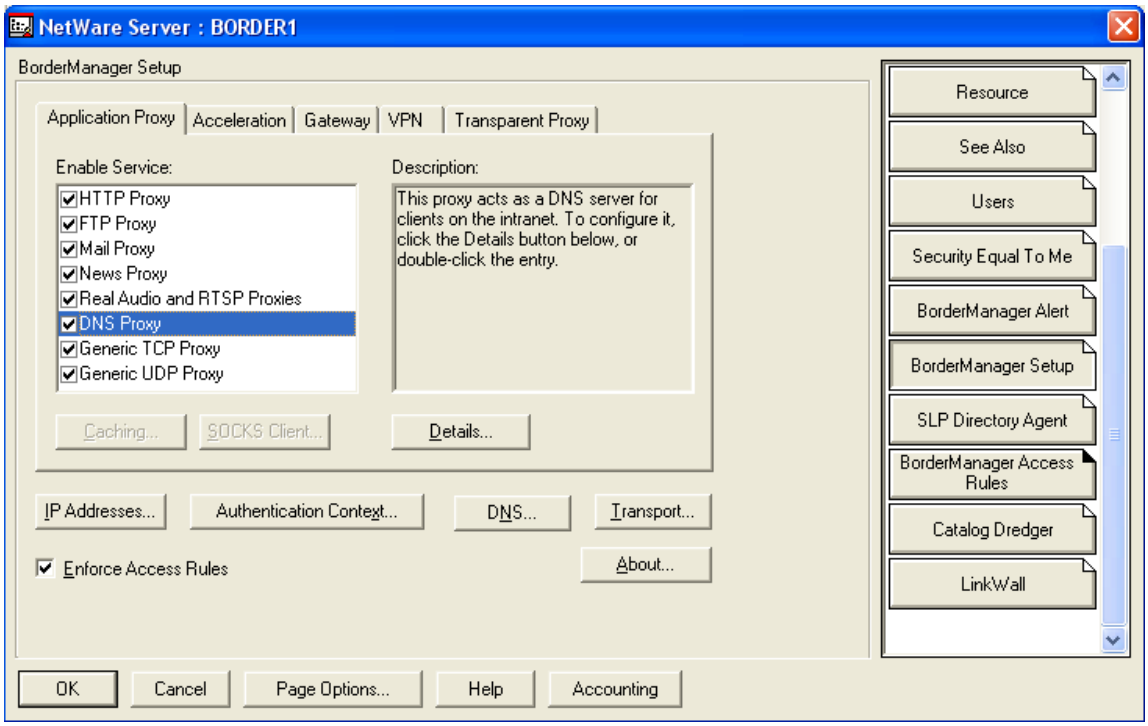
An Alternative

A reliable alternative has been to use dynamic NAT and a stateful packet filter exception to allow the clients to directly query an ISP's DNS server. The HTTP Proxy still makes use of DNS caching, and

will resolve URL's on behalf of the clients (if HTTP Proxy is used and not Transparent Proxy). Since most DNS queries are typically done for browsing HTTP, allowing DNS queries out through a packet filter exception does not generally represent a lot of traffic.

This alternative provides no provision for resolving internal URL's. With the increasing popularity of internal web-based services (web sites, Netstorage, iFolder, etc.), it is recommended that you have either an internal DNS server configured, or at least use DNS Proxy with HOSTS file entries on the BorderManager server for internal URL's.

Configuring DNS Proxy



From the BorderManager Setup main menu, check the **DNS Proxy** box to enable it.

Click on **Details** to turn on Indexed logging, if required, which is the only configurable option for DNS proxy.

To make use of the DNS Proxy, the workstations must be configured with the private IP address of the BorderManager server in the list of DNS resolvers. The setting can be made manually or with DHCP.

The BorderManager server needs to be set up to query your ISP's DNS servers.

Configure the DNS settings on the clients, manually or via DHCP, to point to the BorderManager private IP address.

Note If you configure DNS Proxy, you cannot run a DNS server on the same server as BorderManager because only one will be able to listen on port 53. (I do not recommend running a DNS server on BorderManager).

The DNS proxy is one proxy that does not need an access rule to allow it to be used.

<This page intentionally left blank. This is to facilitate putting in chapter tabs in a ring binder for double-sided printing. The main chapters should start on an odd-numbered page.>

Chapter 13 - Generic TCP Proxy

Concept

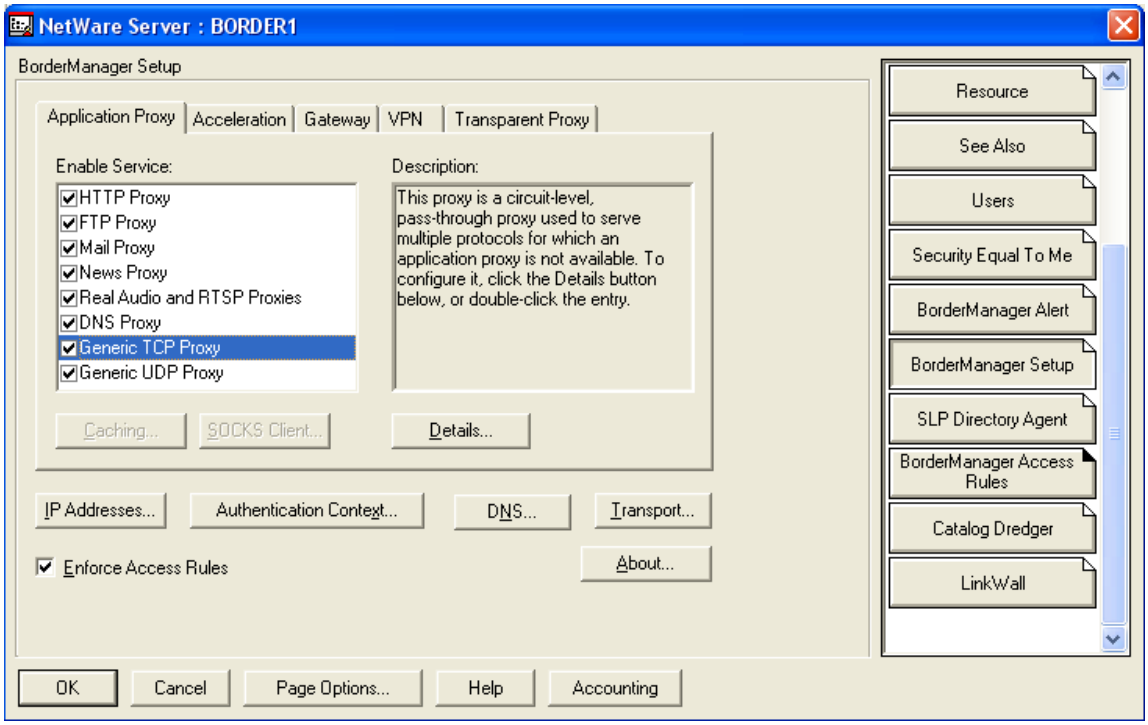
If you do not want to use packet filter exceptions to allow inbound or outbound TCP traffic, you may be able to configure a Generic TCP proxy to pass the traffic through, and control the traffic with access rules. The port numbers can be different on each side of the proxy.

Pros

- Using a Generic proxy for inbound traffic from the Internet has the advantage (as compared to static NAT), that internal hosts do not require the default gateway to be pointed to the BorderManager server.
- Generic TCP Proxy can be set up to redirect a particular TCP port from one public address to one private address. A different TCP port can be directed from the same public IP address to a different private address. This capability means that a single public IP address can be used to map many different port numbers to multiple internal hosts. The alternative, static NAT, would require a separate public IP address for each internal host.
- You can translate port numbers with generic UDP Proxy, which in some cases can be used to preserve IP addresses, and in other cases can obscure a connection for security purposes.

Cons

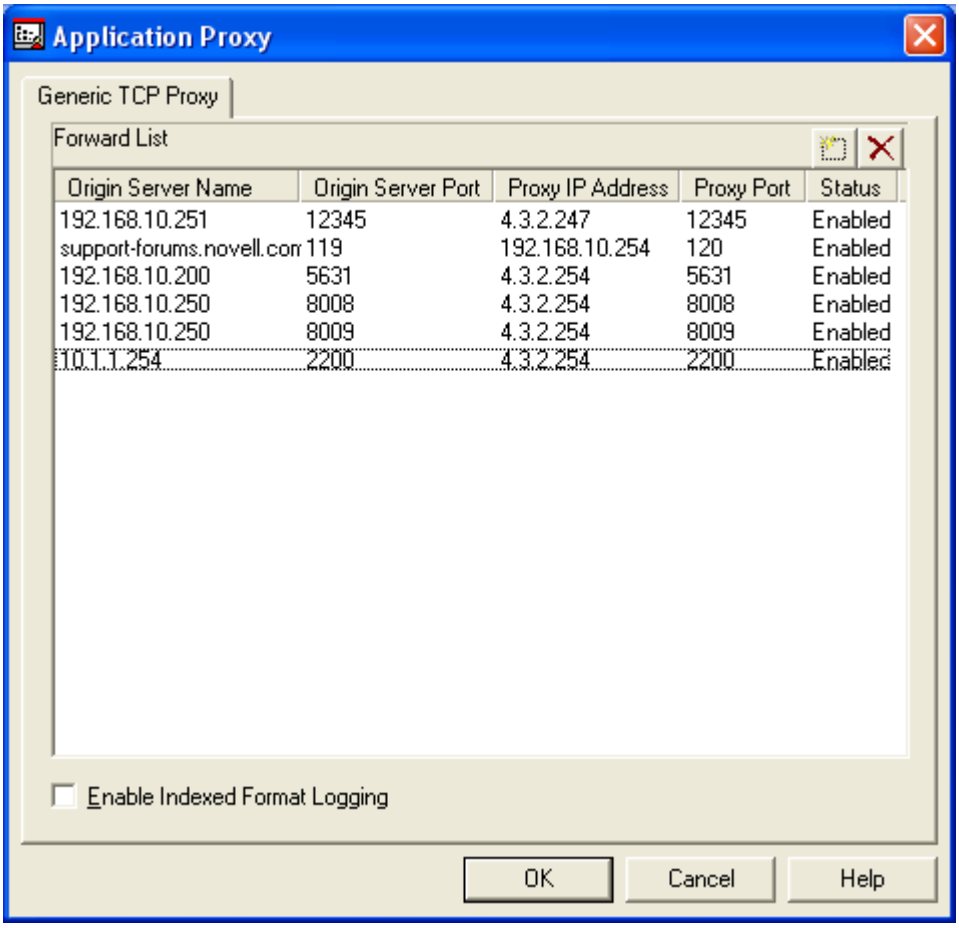
Generic Proxies require the BorderManager proxy to be loaded and functioning. In a scenario where generic proxies are being used for remote control to an internal host (pcANYWHERE, or VNC, for example), unloading PROXY.NLM (to clear cache or make some sort of update) will instantly drop the remote control connection.



The Generic TCP Proxy shown enabled on a BorderManager 3.5 or later server.

Note You cannot set up the same TCP port number as that used by some of the non-generic proxies, such as the HTTP, Mail, or News Proxies. Those port numbers are reserved, even if those proxies are not enabled. See the example on NNTP proxy below for a possible alternative.

Configuring Generic TCP Proxy



Select the **Generic TCP Proxy** from the BorderManager Setup main menu, and click on the **Details** button.

The **Origin Server Name** is the URL or IP address of the host or server that the Generic TCP Proxy will communicate with. The **Proxy IP Address** is the address on the BorderManager server itself that will be listening for the traffic being proxied.

The **Origin Server Port** is the port number on which the origin server is listening. The **Proxy Port** is the port on which the BorderManager server is listening. These ports are generally the same, but do not have to be. An example using different ports is given for NNTP.

The example above shows that several Generic TCP proxies are configured, and enabled.

- The top example is for Novonyx Web Manager (or Apache iManager), and is described below. It is listening on a secondary public IP address 4.3.2.247, and forwarding port

12345 to a server at internal IP address 192.168.10.251. The Web Manager example shows that you can use generic proxy on a secondary public IP address. (Static NAT could have been used here instead).

- The second entry is for NNTP (Usenet), listening on secondary private IP address 192.168.10.254, and forwarding to the URL support-forums.novell.com. The proxy listens for traffic on port 120, and sends it to the server on port 119. The NNTP example shows how to listen for traffic on the internal LAN and direct it to a server on the Internet, and do port translation in the process.
- The third entry is for is for pcANYWHERE, using listening on the primary public IP address 4.3.2.254 and forwarding to a PC at 192.168.10.200. The port used is 5631. The pcANYWHERE example shows how to listen from traffic from the Internet and direct it to a PC on the internal LAN. pcANYWHERE also requires UDP port 5632, and an example of that is shown in the Generic UDP Proxy example later in this book. This example shows that you do not need static NAT to make use of pcANYWHERE. (Static NAT requires a secondary public IP address).
- The fourth and fifth entries are used for Novell Remote Manager. The proxy listens on public IP address 4.3.2.254, and forwards ports 8008 & 8009 to a NetWare server at IP address 192.168.10.250.
- The sixth entry is for iManager, on a NetWare 6.5 server. Generic proxy is listening for port 2200 on public IP address 4.3.2.254, and forwarding the traffic to 10.1.1.254.

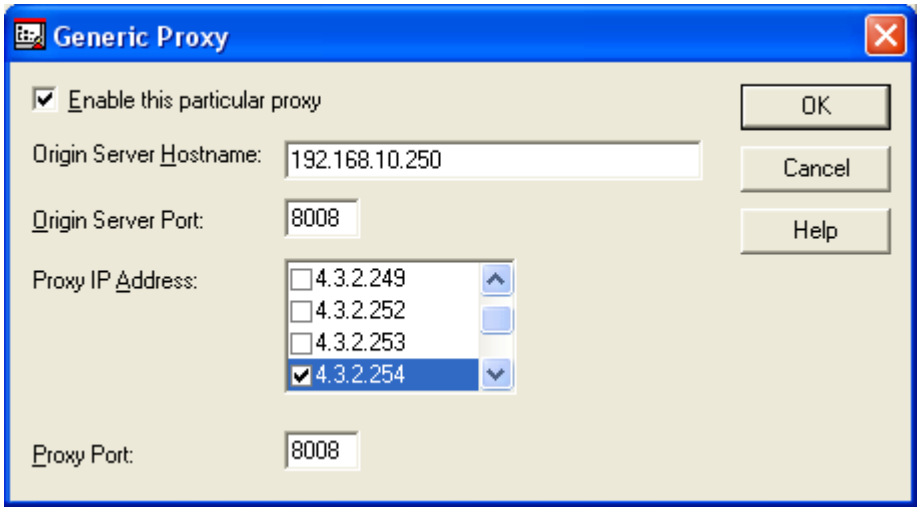
All of the examples above may require custom filter exceptions to allow the traffic either in to the public IP address or out from the public IP address or both, depending on the version of BorderManager and your filtering configuration. The example for Web Manager definitely will require custom filter exceptions, because it makes use of a secondary public IP address. The default filter exceptions for all versions of BorderManager do not have any allowance for secondary public IP addresses. Some versions (BorderManager 3.6 and earlier) of BorderManager default filter exceptions will allow the pcANYWHERE and NNTP traffic, and some will not. A brief example of adding filter exceptions is shown for the Web Manager later in this book. A full treatment of filtering and adding exceptions is out of the scope of this book, but is covered in my "*Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions*" book. See http://www.craigjconsulting.com for more information on that book.

All of the examples require access rules to allow the TCP ports to be used, regardless of the version of BorderManager.

Example for Novell Remote Manager

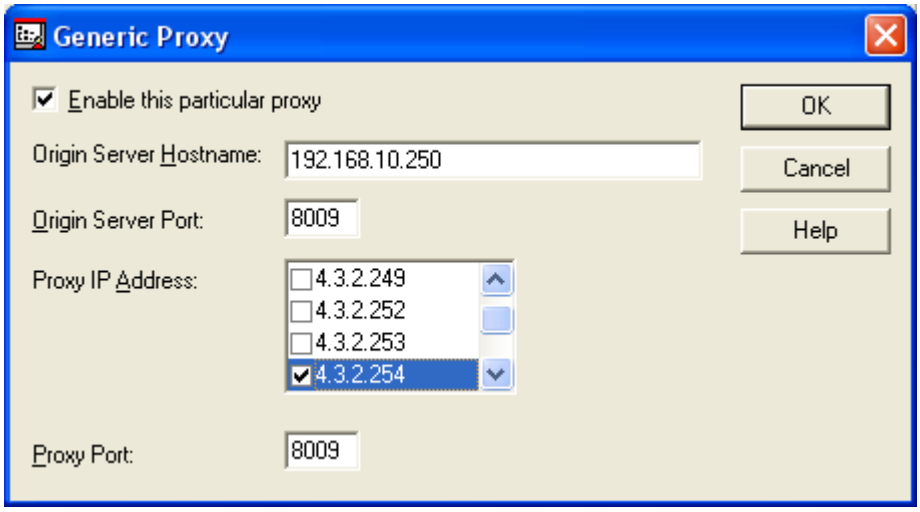
Novell Remote Manager (NRM) listens on port 8008 and 8009. Configuring the Generic TCP Proxy to listen on port 8008, and again on port 8009, each time listening on the same public IP address, and pointing to an origin server IP address of the server running NRM that you wish to access from the Internet.

Generic Proxy Configuration for Novell Remote Manager



Two generic proxies are required.

Here is the configuration for port 8008.

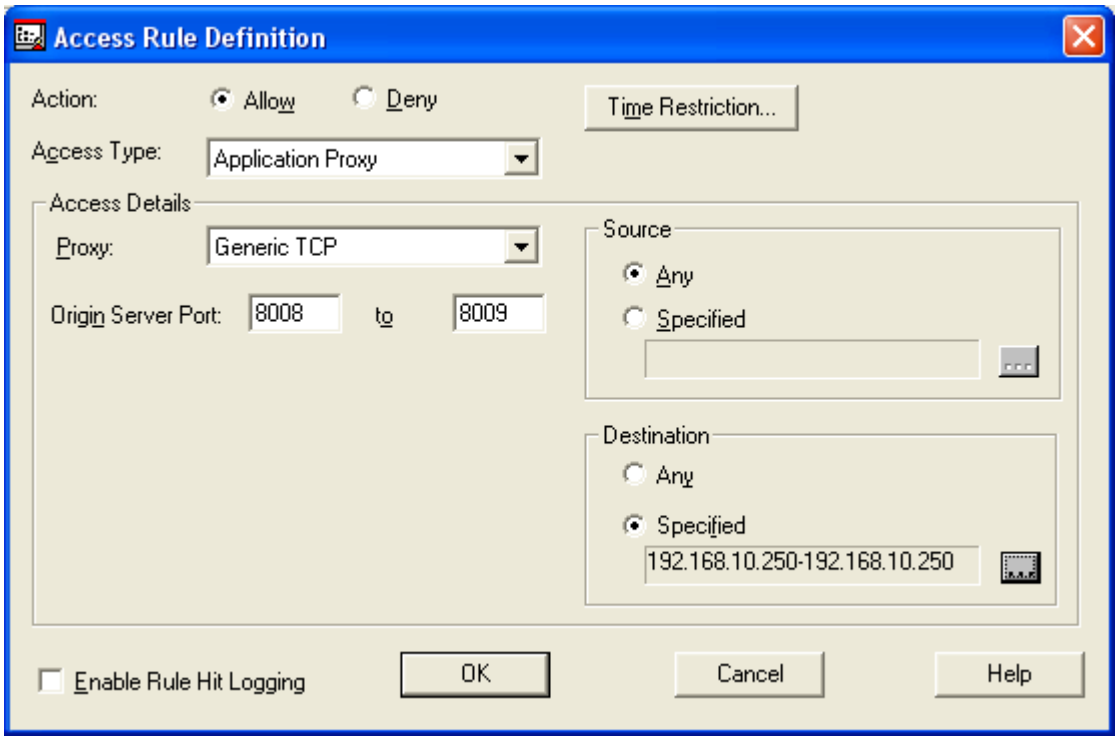


Here is the configuration for port 8009.

You may require filter exceptions to allow TCP destination ports 8008-8009 to the public IP address, as well as exceptions allowing the responses from the public IP address.

You will require an access rule allowing TCP ports 8008-8009.

Access Rule Configuration for Novell Remote Manager

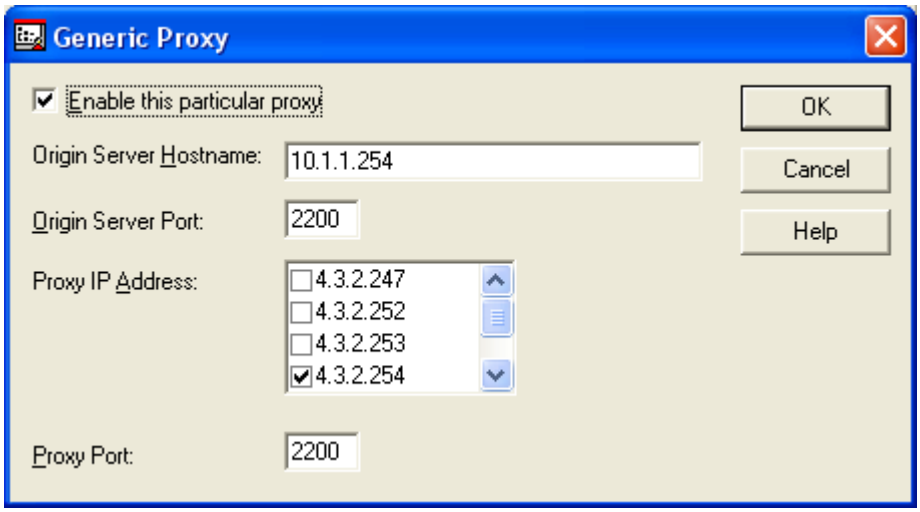


You must add an access rule for Application Proxy Generic TCP Proxy, ports 8008 to 8009 to either Any destination IP address or the IP address of the NetWare server running Novell Remote Manager.

Example for iManager

iManager on NetWare normally listens on port 2200. Configure the Generic TCP Proxy to listen on port 2200, listening on a public IP address, and pointing to an origin server IP address of the server running iManager you wish to access from the Internet.

Generic Proxy Configuration for iManager

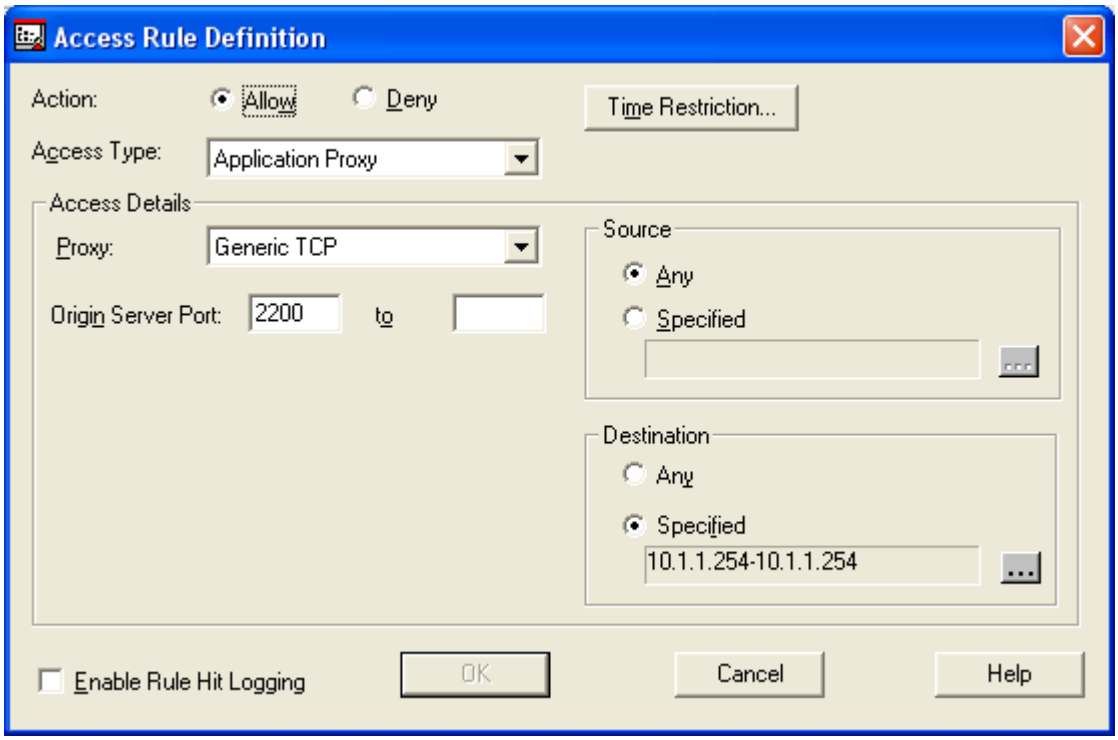


Here is the configuration for iManager using port 2200.

You may require filter exceptions to allow TCP destination port 2200 to the public IP address, as well as an exception allowing the responses from the public IP address.

You will require an access rule allowing TCP ports 2200.

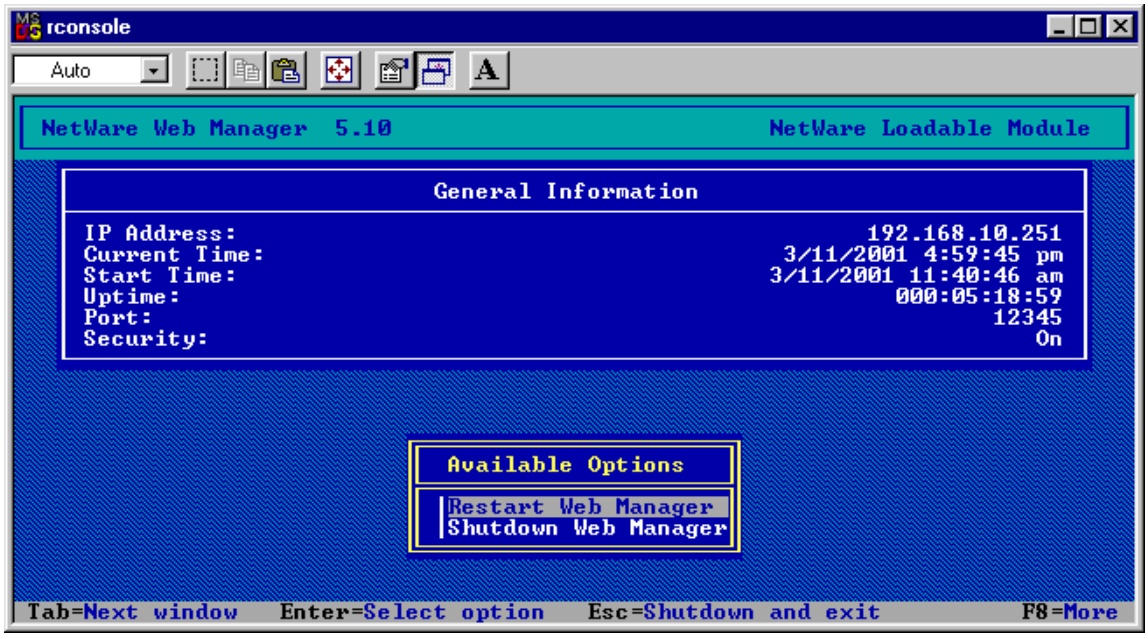
Access Rule Configuration for iManager



You must add an access rule for Application Proxy Generic TCP Proxy, port 2200 to either Any destination IP address or the IP address of the NetWare server running iManager.

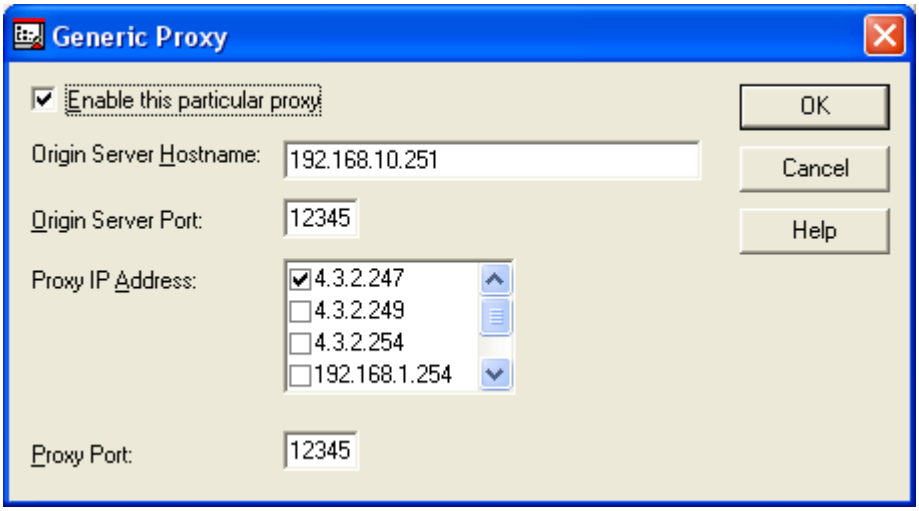
Example for NetWare Web Manager

NetWare 5.x Netscape Enterprise (Novonyx) web servers can be administered using a web-based management tool called Web Manager. The Web Manager can be configured to listen on a particular port number, defaulting to port 2200. (NetWare 6.x uses Apache and iManager, but the same concept applies). In the following example the port number was configured at 12345.



While the Web Manager is displayed in a browser, it does NOT use HTTP, and using reverse proxy acceleration for HTTP will NOT work. Instead, set up a Generic TCP Proxy which listens on a public IP address for the port number configured for Web Manager.

Generic Proxy Configuration for Web Manager

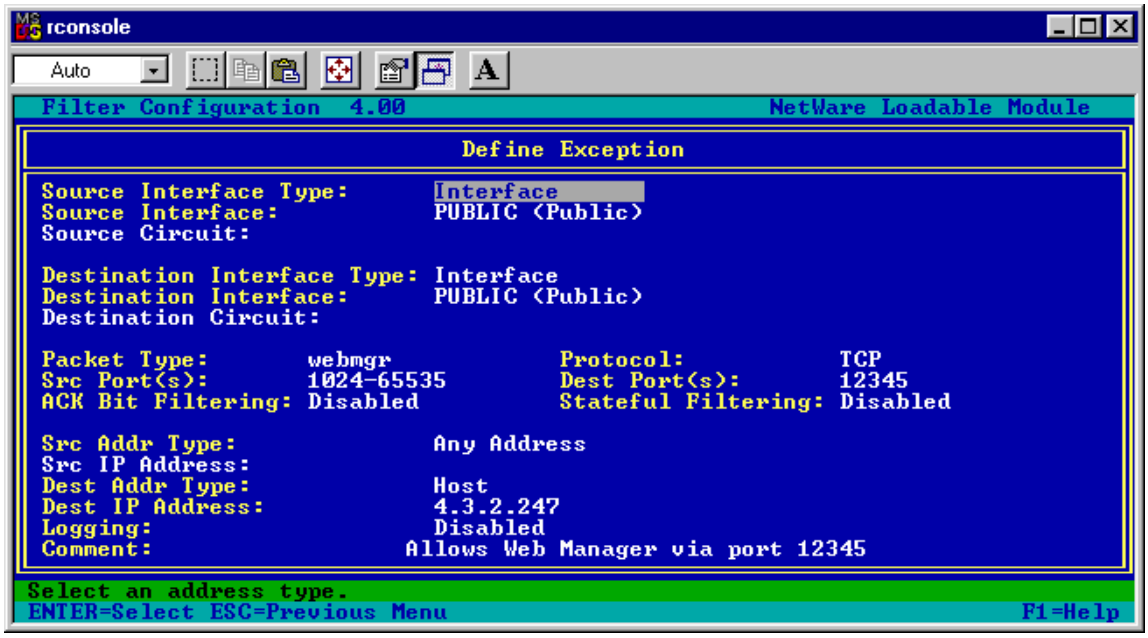


In the example shown above, a NetWare 5.1 server at IP address 192.168.10.251 is running Web Manager, listening on port number 12345. The Web Manager will become available outside BorderManager on public IP address 4.3.2.247.

Because, in this case, 4.3.2.247 is a secondary IP address added to the BorderManager public interface (with the ADD SECONDARY IPADDRESS 4.3.2.247 command), filter exceptions **must** be configured to allow the traffic both to and from that IP address.

Add two custom packet filter exceptions using FILTCFG.NLM as shown below.

Filter Exceptions for Web Manager



This custom packet filter exception allows TCP port 12345 in to the public IP address being proxied to the internal Web Manager.

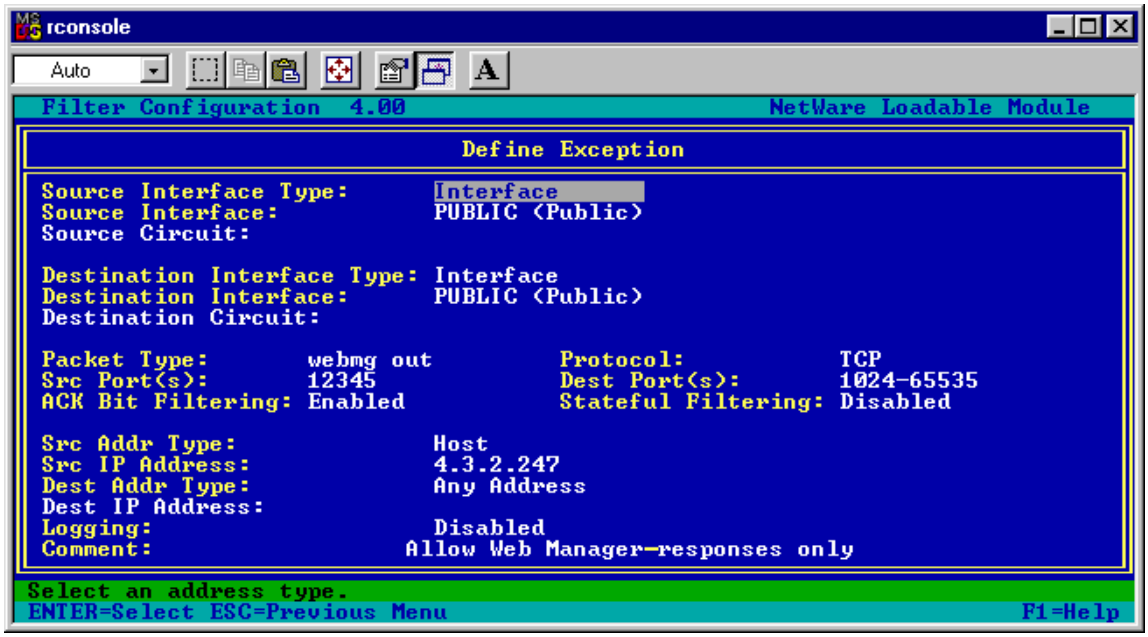
The **Source and Destination interfaces** are fixed to the **Public** interface.

The **Protocol** is **TCP**.

The **Source Ports(s)** have been defined as **1024-65535**

The **Destination Port** has been defined as **12345**.

The **Destination IP Address** has been restricted to **4.3.2.247**



This custom packet filter exception allows TCP port 12345 out from the public IP address being proxied to the internal Web Manager.

The **Source and Destination interfaces** are fixed to the **Public** interface.

The **Protocol** is **TCP**.

The **Source Ports(s)** have been defined as **1024-65535**

The **Destination Port** has been defined as **12345**.

ACK Bit Filtering has been **enabled** on this packet filter exception for additional security.

The **Source IP Address** has been restricted to **4.3.2.247**

Browser Configuration for Web Manager

To use the Generic TCP Proxy for Web Manager on port 12345, simply use the following syntax for the URL:

```
HTTPS://4.3.2.247:12345
```

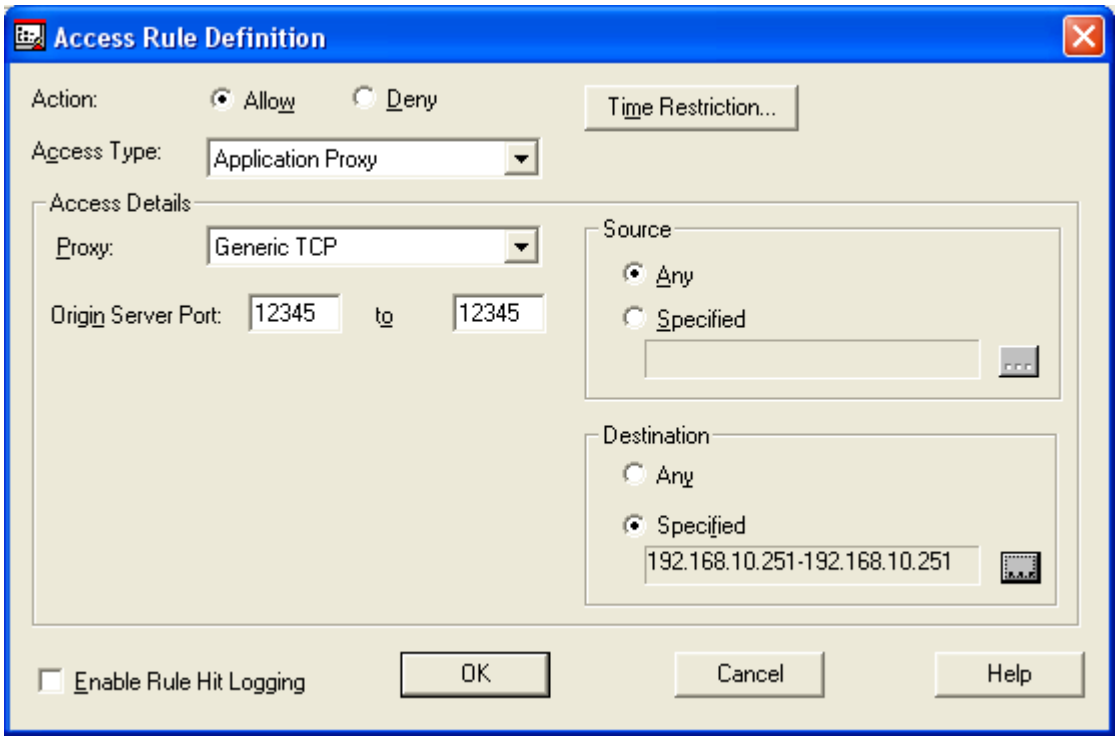
For this Web Manager configuration, it is required to type "HTTPS" and not "HTTP" as well as adding the ":12345". All traffic will be sent or received using port 12345. (SSL Encryption has been enabled on this Web Manager. If SSL was disabled, HTTP would be used instead of HTTPS).

If you have defined a public DNS entry for the 4.3.2.2.247 IP address (such as www3.yourdomain.com), you can use that in the URL in the browser:

```
HTTPS://www3.yourdomain.com:12345
```

Access Rule Configuration for Web Manager

You must add an access rule for Application Proxy Generic Proxy, port 12345 to the destination IP address of the NetWare server running Web Manager.



The access rule **Access Type** is **Application Proxy**.

The **Origin Server Port** is **12345**.

The rule **Source** has been left at **Any**, allowing any remote host to access the proxy. The rule **Destination** has been specified to the IP address of the internal server running the Web Manager.

For a generic proxy, you cannot specify an NDS object as the source. You could, if desired, specify the host IP address of the remote host trying access the proxy as the source in order to restrict access to this proxy. However, Web Manager also requires a user to log in to access the service, using a valid NDS account.

Example For NNTP with Port Translation

This example shows how to configure a generic proxy to access a Usenet (NNTP) server as a valid alternative to the built-in News Proxy. This capability is especially useful as it provides a means of using proxies to handle more than one NNTP server.

Note "News", "NNTP" and Usenet are synonymous in this case.

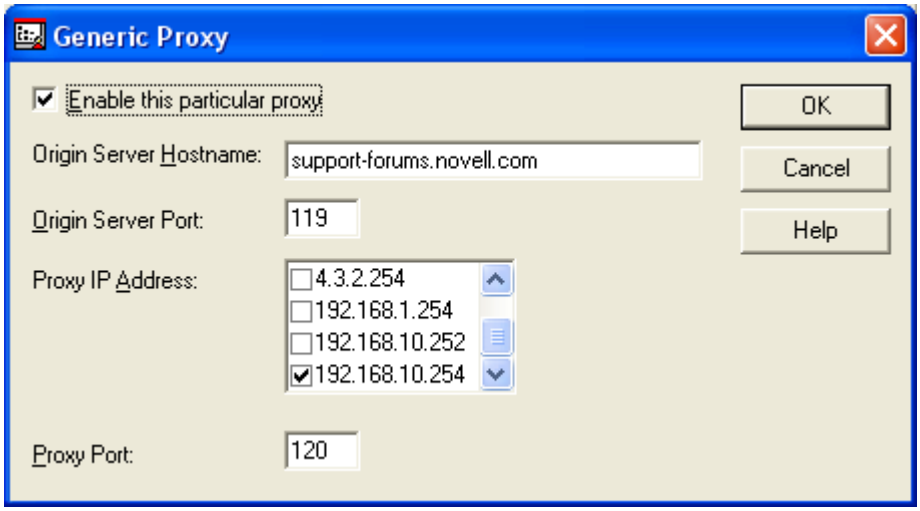
The News Proxy is limited to mapping an internal IP address/ port number combination to a single external Usenet server. The News Proxy will automatically listen on all BorderManager private IP addresses, using port number 119. Even though multiple Usenet servers can be specified in the Origin servers list, the servers after the first one on the list are only used if the first server fails to respond. That is, the additional servers are listed only for failover purposes. The example shown here can be used at the same time as the News Proxy, but point to a different NNTP server than the News Proxy.

Note An alternative to using any proxies for Usenet access is to set up a stateful packet filter exception, usually in combination with Dynamic NAT, to allow routing of outbound NNTP traffic to any Usenet server.

The key point to be made in this example is that both the generic proxy port and the host program running on an internal PC must be changed from using the default port number (119) to some custom port number. As long as the combination private IP address/port number is unique, multiple Generic TCP proxies can be set up, with each pointing to a different Internet Usenet server. Each of these proxies would require a custom port number to be configured on the Usenet reader program, but the traffic between the BorderManager server and the Usenet server would still take place on port 119.

In NWADMN32, BorderManager Setup, select the **Generic TCP Proxy**, and click on **Details**. Check Enable this particular proxy.

Generic Proxy Configuration for NNTP



In the **Origin Server Hostname** field, enter the IP address or DNS name of a Usenet server on the Internet (or your intranet) to be accessed.

In the **Origin Server** Port field, enter **119**, which is the default port number for Usenet (NNTP) servers.

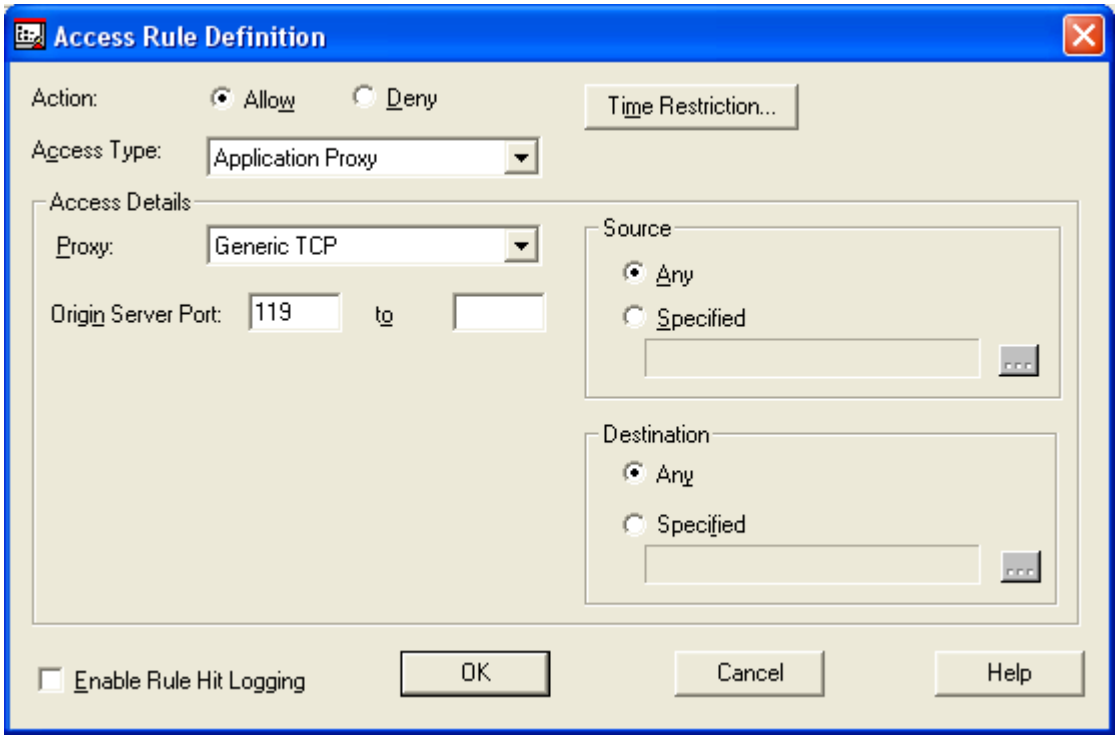
In the **Proxy IP Address** field, select the BorderManager server private internal IP address to be used. The addresses will show up in this selection if they have been defined in the IP Addresses menu in NWADMN32, BorderManager Setup. Multiple addresses might show up, if internal multiple network cards or secondary IP addresses are being used. The address(es) selected here will be available for use by internal News reader programs.

In the **Proxy Port** field, enter a custom port number **not already being used** for some other purpose on the BorderManager server. In this example, port 120 is being used, so that the BorderManager server will listen on IP address 192.168.10.254, TCP destination port 120. You **cannot** enter a port number that is reserved for certain other 'fixed proxies' (like the News Proxy). For instance, you cannot enter port numbers 25, 53, 110 and 119 because those port numbers are reserved for Mail, DNS, Mail and News proxies – even if those proxies are not currently being used.

Click **OK** to save the settings.

Access Rule Configuration for NNTP

Select the **BorderManager Access Rules** tab. You will need to enter an Access Rule to allow access to this custom Application Proxy.



You need to add an Access Rule for **Application Proxy**, **Generic TCP**.

The access rule should call out port **119** for the Origin Server Port number. This port number needs to match the port number being used by the NNTP server, not the listening port of the generic proxy.

Note The access rule only specifies the destination port to be used on the Internet side of the BorderManager server. The custom port (listening port on the internal side of the BorderManager server) is not specified in an access rule.

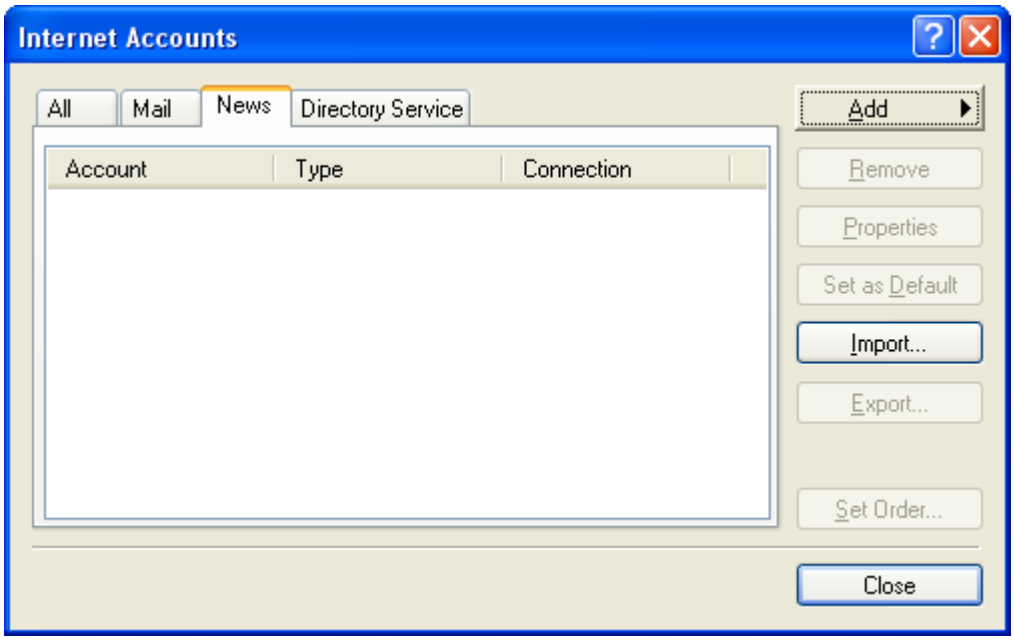
If you specify a **Source**, to limit access to this proxy, you will only be able to choose between a DNS name and IP addresses. You cannot base an access rule for a generic proxy on an NDS user, group or container.

The destination hardly matters in this case, as the generic proxy is already set up to forward traffic to a particular IP address. However, should you enter a destination IP address, it needs to be the IP address of the news server to which the proxy is going.

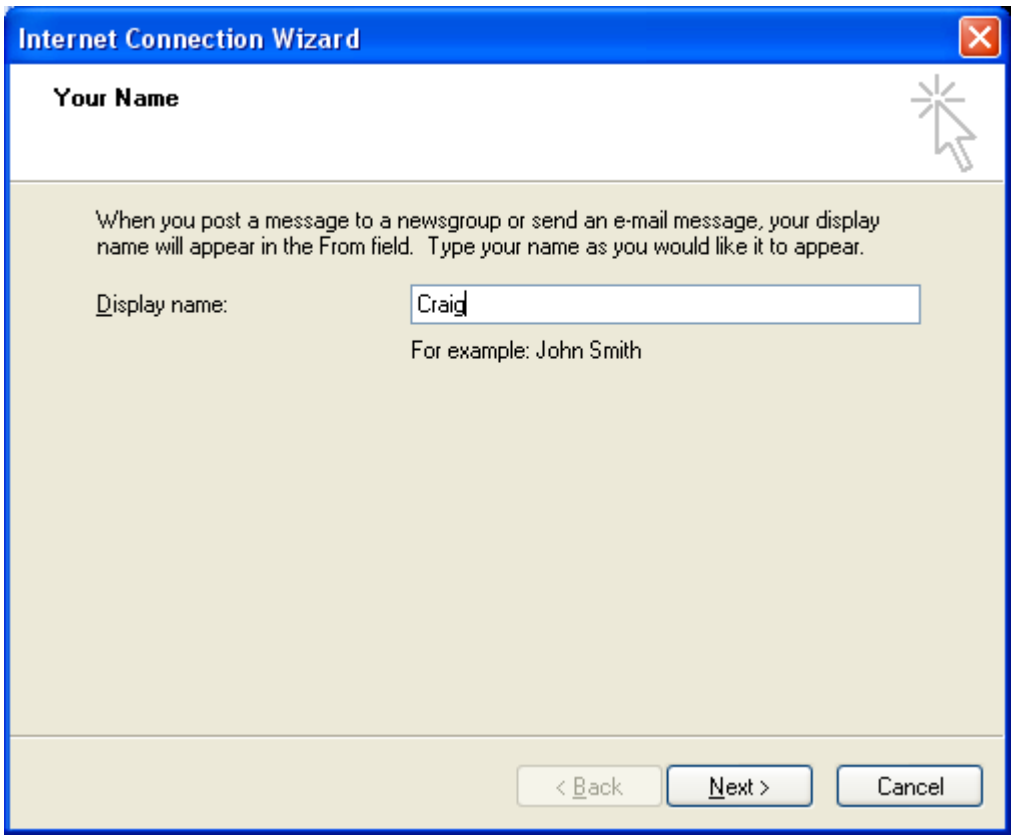
You must now use a newsreader program that gives you the option of specifying a custom port number for the NNTP server.

Outlook Express Configuration

This example shows how to set up Outlook Express to access the Generic TCP proxy using port **120**.

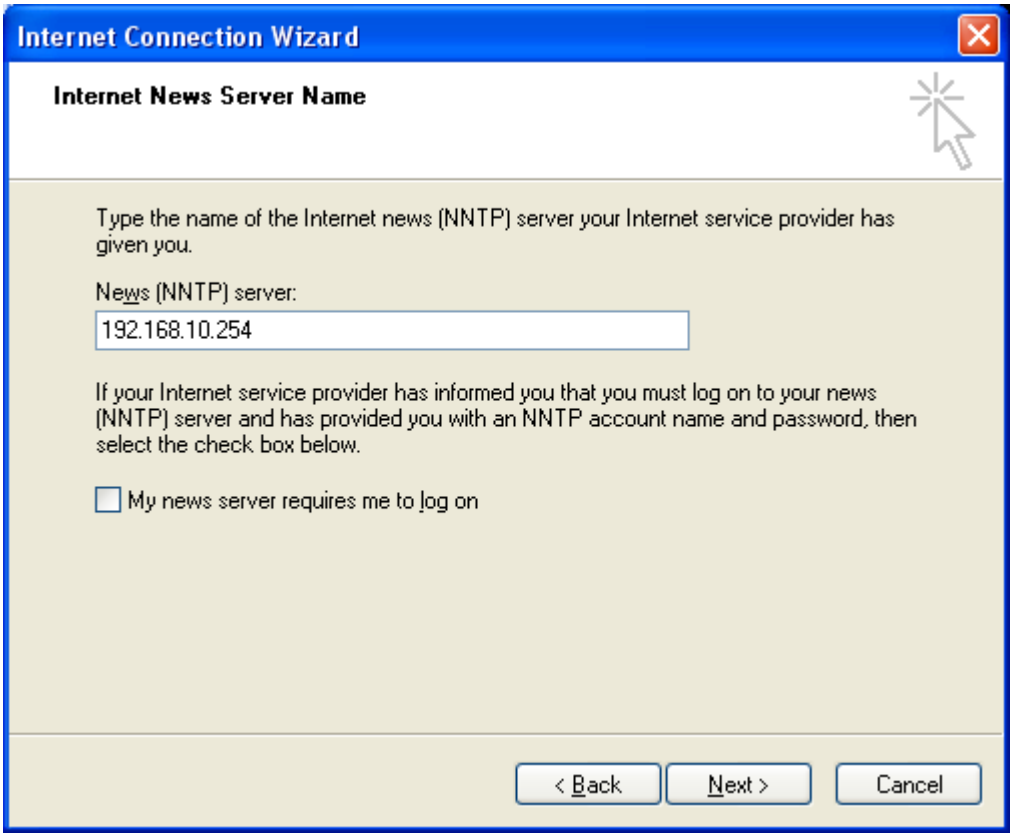


Launch Outlook Express, and select **Tools, Accounts, News, Add, News.**

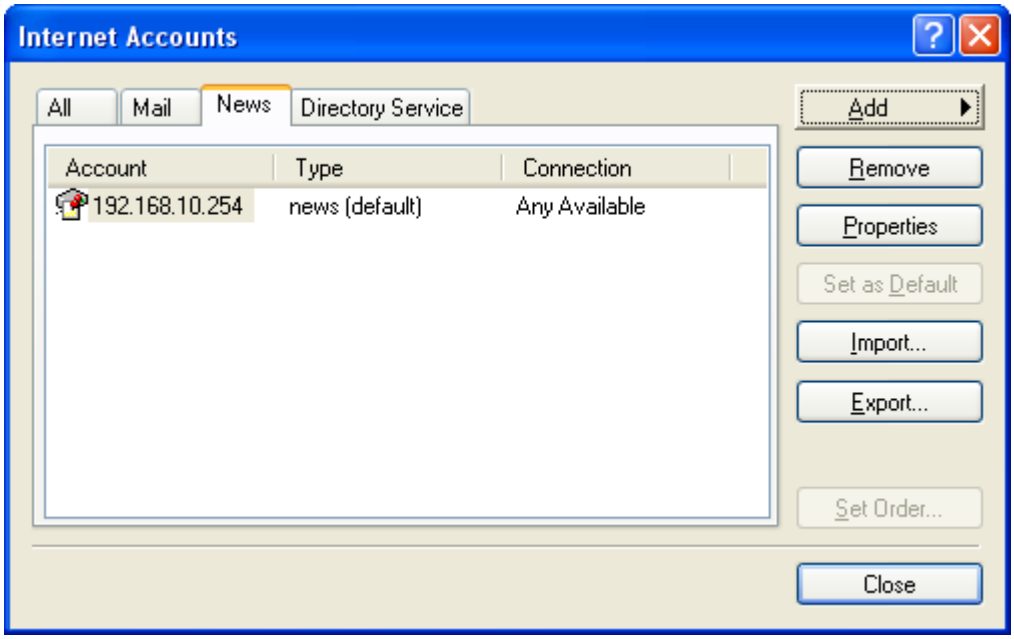


Enter the **Display Name** to be used on your postings, and click **Next**.

Enter your **Email Address**, if you want to send responses to Usenet messages via Email, and click **Next**.

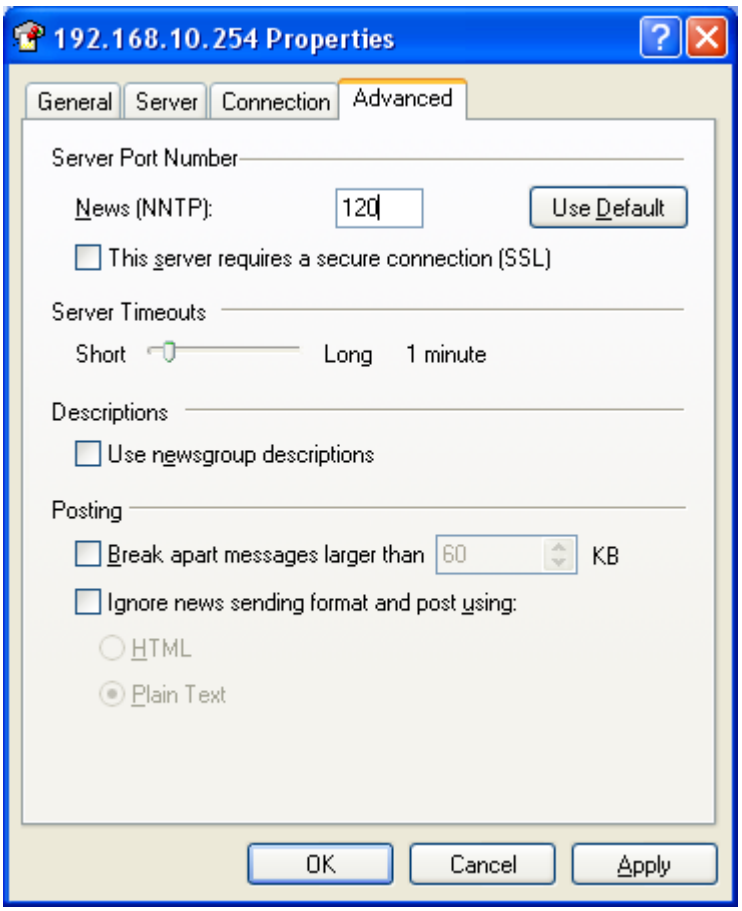


When you get to the **Internet News Server Name** menu, enter the IP address of the internal IP address of the BorderManager server that was configured with the Generic TCP Proxy. Click **Next**. Then click **Finish**.



Now select the new news account you just set up, and click on **Properties** so that you can configure the non-standard port number to match the Generic TCP Proxy.

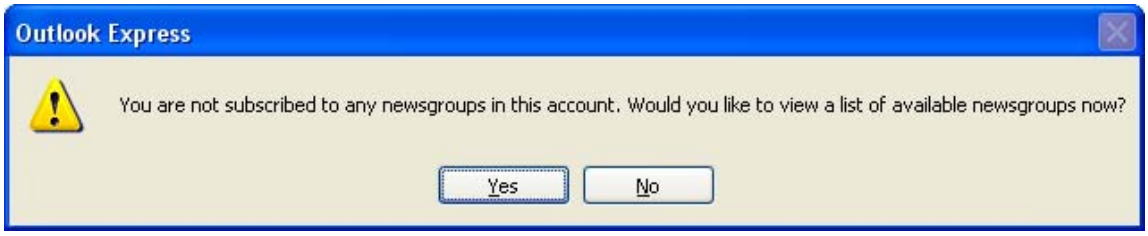
Click on the **Advanced** tab.



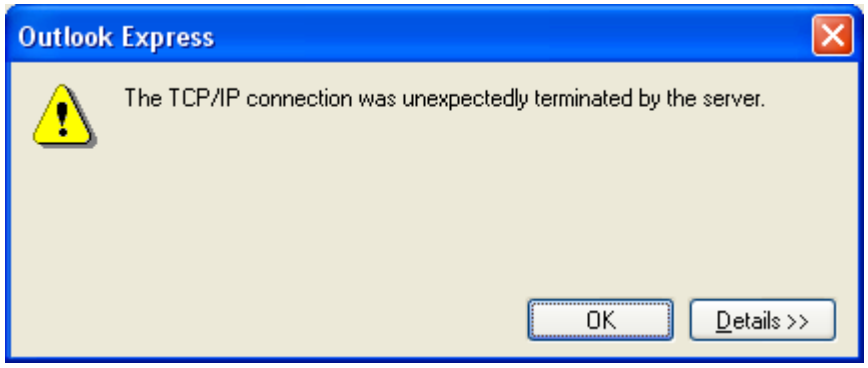
Enter a port number matching that of the Generic Proxy you configured earlier.

Click on **OK**, and then click on **Close** to save all the changes.

You should get a message asking if you want to download the news groups list. Select **Yes**.

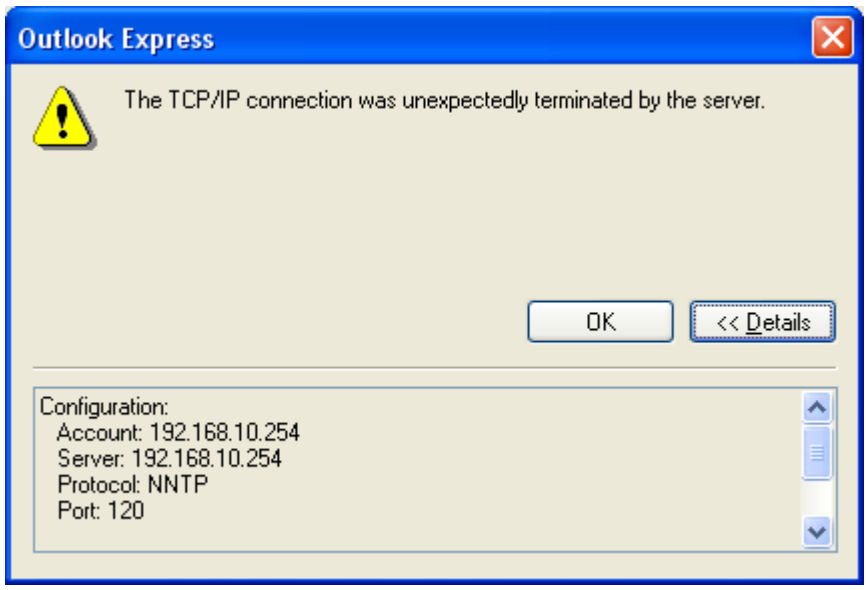


You may be asked to subscribe to newsgroups. Ask Outlook Express to view a list of newsgroups in this case. Select **Yes**.



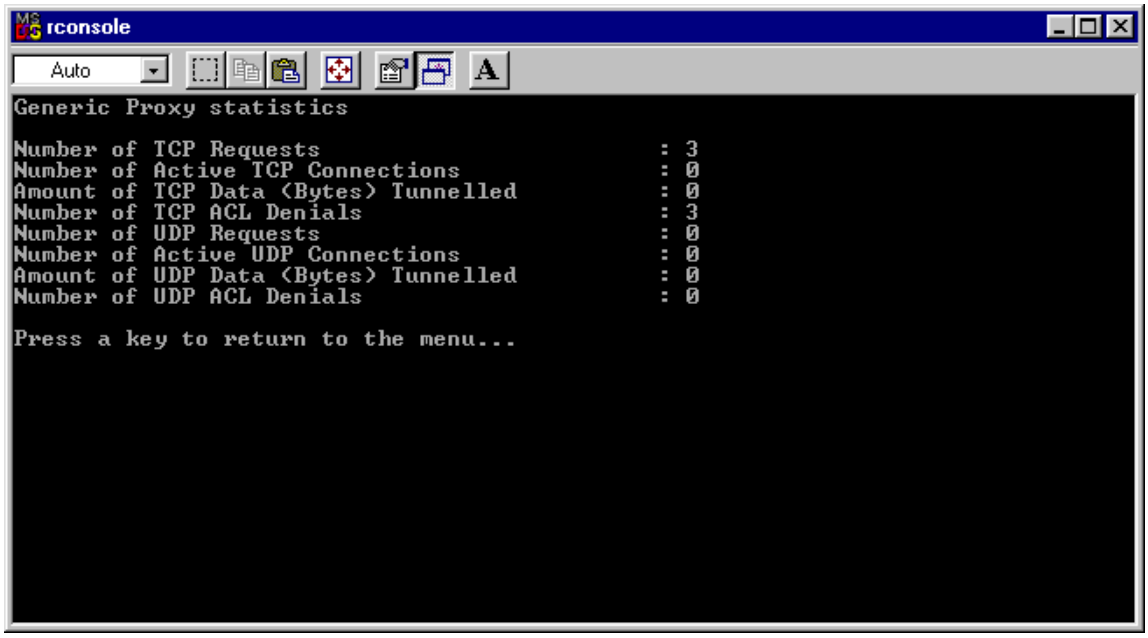
If you have a problem getting the news groups, you may see a message about the connection being terminated by the server. This may be cause by a problem with the Access Rule, or a missing Access Rule.

Click on the **Details** button of the error message, and you can verify that your Usenet settings are as you expected.



In the example above, there may be multiple causes for a failure. The account and server number could be wrong. In this case the cause was a lack of an access rule to allow port 119 to be used by the proxy.

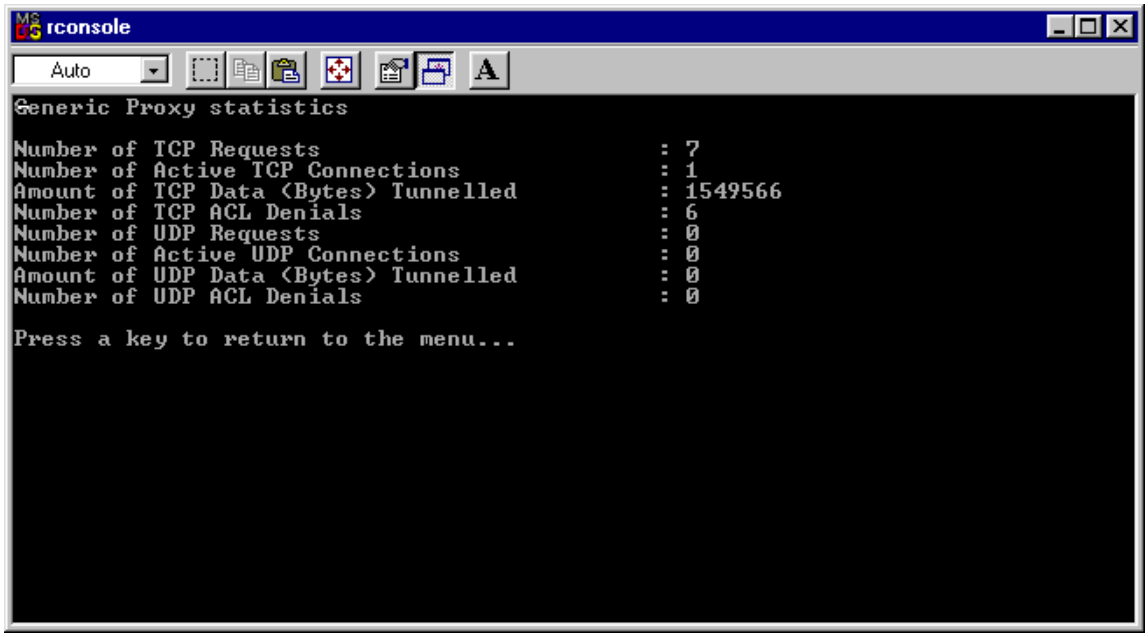
To check to see if you have an Access Rule issue, you can go to the BorderManager server and look at the **Proxy Console** screen, option **19** "Application Proxies", then option **4** "Display Generic proxy statistics".



The example above shows that three TCP requests have been made to the generic TCP proxy. That's good, and it means that a generic proxy saw some data coming in on a listening port number. But three **TCP ACL Denials** were also seen. That's bad, and it means your Access Rules denied the traffic.

Be sure you have an Access Rule to allow the correct Application Proxy port in place, and that there is no Deny Port (or Deny Any) rule above it. Be sure that in the Access Rule, the **Origin Server** port number is **119**, not the custom port number configured for the Proxy IP Address. Do not specify a destination IP address in the access rule for best results.

Once you have the access rule configured correctly, you should see data going through the generic proxy in the Generic Proxy Statistics.



The figure above shows an example of the statistics seen for successful data transfer using a Generic TCP proxy.

Note Not all Newsreader programs have a menu entry for setting a non-default port number. However, those programs, like Forte Free Agent, may allow you to change the default listening port number in an INI file.

Agent /Free Agent Configuration

The settings in Agent are used in the same way that Outlook Express is configured, but there is no menu option for the port number to be used to change to a non-standard port. However, you can still configure Agent to use the port number of your choice by setting the port number in the AGENT.INI file. Part of the file is shown below:

```
[Servers]
NewsServer="192.168.10.254"
MailServer="<your mail server goes here>"
POPServer=""
NNTPPort=120
SMTPPort=25
POPPort=110
SMTPServerPort=25
```

Simply change the NNTP Port value from 119 to the port number configured for your generic proxy.

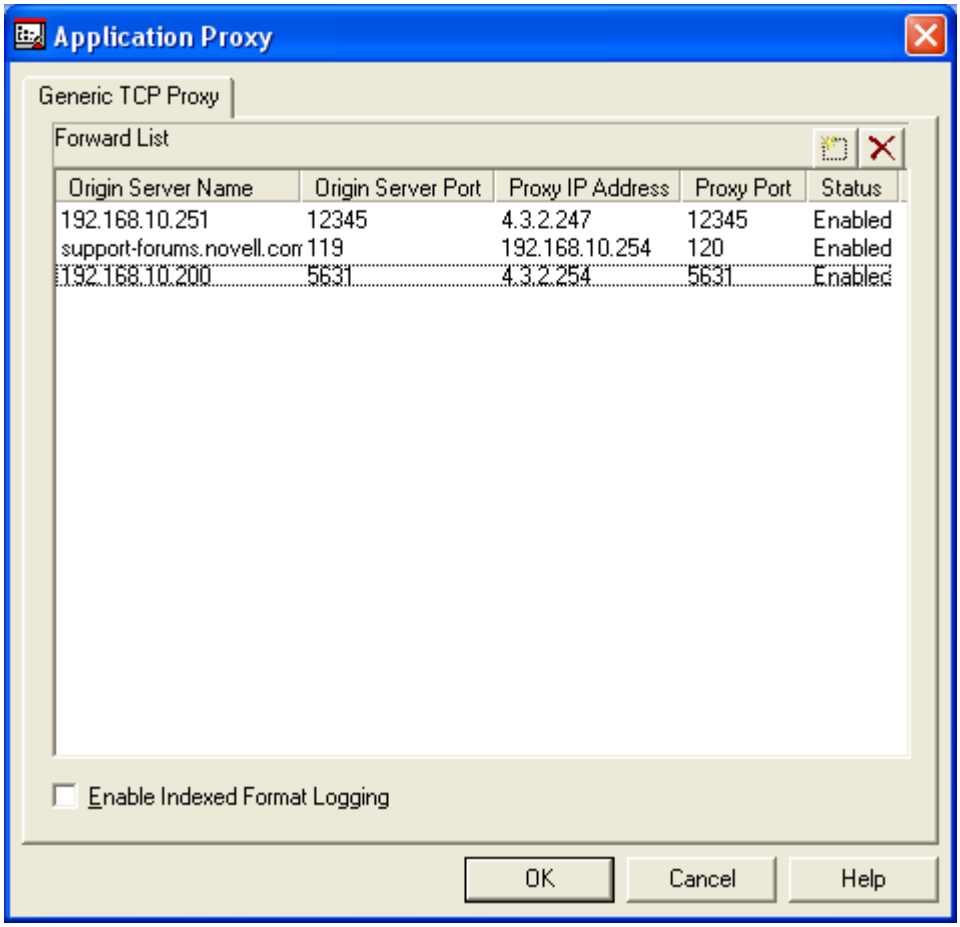
Example Generic TCP Proxy for Inbound pcANYWHERE

This example shows a generic proxy being used to pass certain *inbound* traffic from the Internet to an internal host, on a port number used by pcANYWHERE.

In order to proxy pcANYWHERE, you must set up TWO generic proxies – one Generic TCP Proxy (shown here) and one Generic UDP Proxy (shown in the chapter for Generic UDP Proxy).

Note pcANYWHERE locates other pcANYWHERE hosts using UDP port 5632, and if no response is received on 5632, then UDP port 22 is also tried. Once a pcANYWHERE host is located, a connection is made and traffic is exchanged on TCP port 5631. Both a UDP and a TCP generic proxy (along with appropriate access rules, and packet filter exceptions if using a secondary public IP address) are required.

Generic Proxy Configuration for pcANYWHERE



In the BorderManager Setup main menu, select the **Generic TCP Proxy**, and click on **Details**.

The **Origin Server Name** is the IP address of the internal pcANYWHERE host.

The **Origin Server Port** is **5631**, the TCP port number that pcANYWHERE uses to transfer data.

The **Proxy IP Address** is the public IP address on the BorderManager server that clients on the Internet use to connect to the internal pcANYWHERE host.

The **Proxy Port** is **5631**, the TCP port number that pcANYWHERE uses to transfer data. Generally, the port number matches the Origin Server Port number.

See the chapter on Access Rules for the access rule required to allow this generic proxy to be used.

<This page intentionally left blank. This is to facilitate putting in chapter tabs in a ring binder for double-sided printing. The main chapters should start on an odd-numbered page.>

Chapter 14 - Generic UDP Proxy

Concept

If you do not want to use packet filter exceptions to allow inbound or outbound UDP traffic, you may be able to configure a Generic TCP proxy to pass the traffic through, and control the traffic with access rules. The port numbers can be different on each side of the proxy.

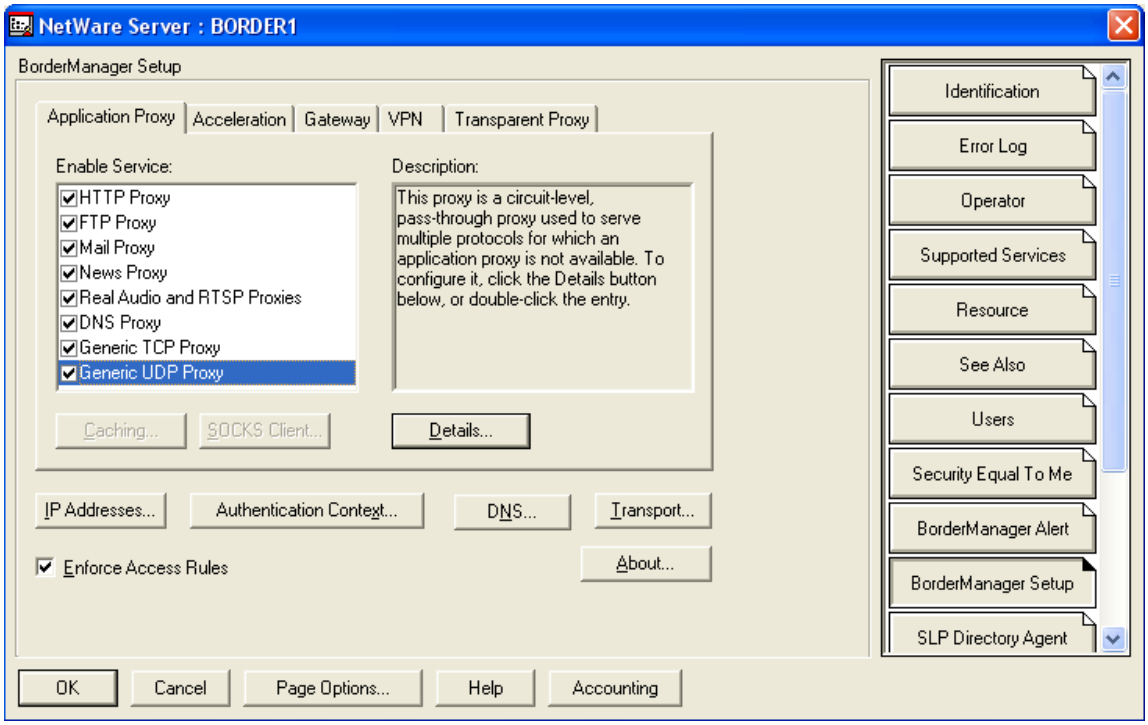
Pros

- Using a Generic proxy for inbound traffic from the Internet has the advantage (as compared to static NAT), that internal hosts do not require the default gateway to be pointed to the BorderManager server.
- Generic UDP Proxy can be set up to redirect a particular UDP port from one public address to one private address. A different UDPP port can be directed from the same public IP address to a different private address. This capability means that a single public IP address can be used to map many different port numbers to multiple internal hosts. The alternative, static NAT, would require a separate public IP address for each internal host.
- You can translate port numbers with generic UDP Proxy, which in some cases can be used to preserve IP addresses, and in other cases can obscure a connection for security purposes.

Cons

Generic Proxies require the BorderManager proxy to be loaded and functioning. In a scenario where generic proxies are being used for remote control to an internal host (pcANYWHERE, for example), unloading PROXY.NLM (to clear cache or make some sort of update) will instantly drop the remote control connection.

Note You cannot set up the same UDP port number as used by one of the non-generic proxies, such as the DNS proxy. Those port numbers are reserved, even if those proxies are not enabled.

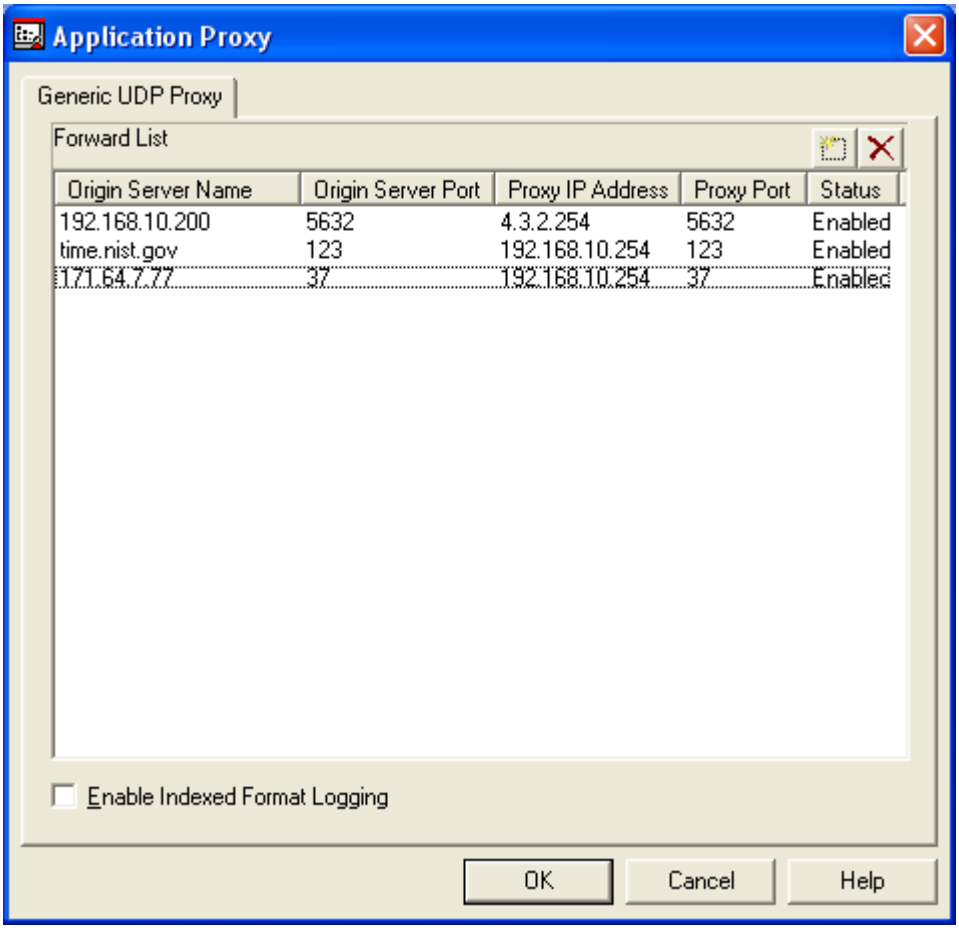


The Generic UDP Proxy shown enabled on a BorderManager 3.5 or later server.

Click on the **Generic UDP Proxy** box and then click on **Details** to configure a Generic UDP Proxy

Generic UDP Proxy - Time Server Proxies

Two Generic UDP proxies are shown to allow outbound time synchronization traffic.



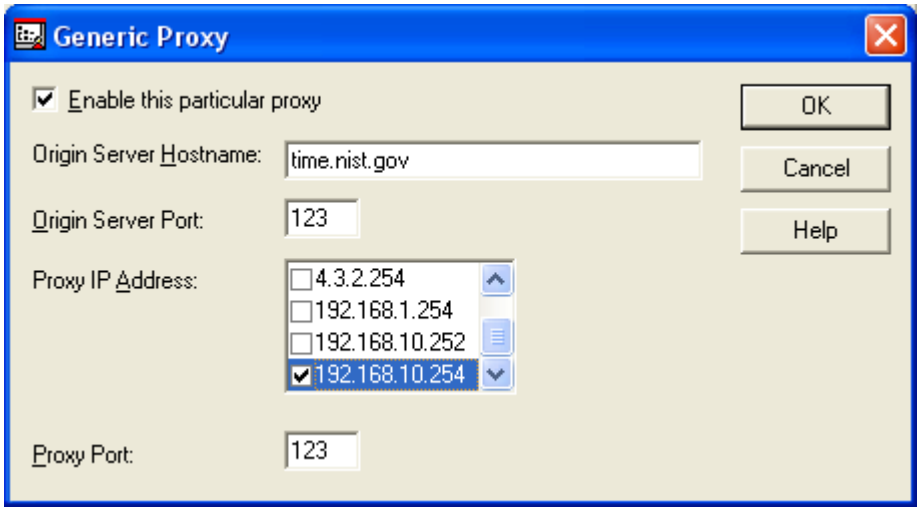
NTP time protocol has been proxied for UDP port 123 traffic to the IP address of the TIME.NIST.GOV Internet NTP timeserver. Setting up NTP clients to point to the 192.168.10.254 address (BORDER1 secondary internal IP address) results in their traffic being proxied to the TIME.NIST.GOV server.

RDATE (daytime) protocol has been proxied for port 37 traffic to an Internet timeserver located at Stanford University in California. RDATE clients pointing to 192.168.10.254 will be proxied to this server. The RDATE.NLM client runs on Novell servers, and other Novell servers would be synched to the server running RDATE.NLM using Novell's TIMESYNC.NLM.

Indexed format logging may be enabled to track the Generic UDP client traffic.

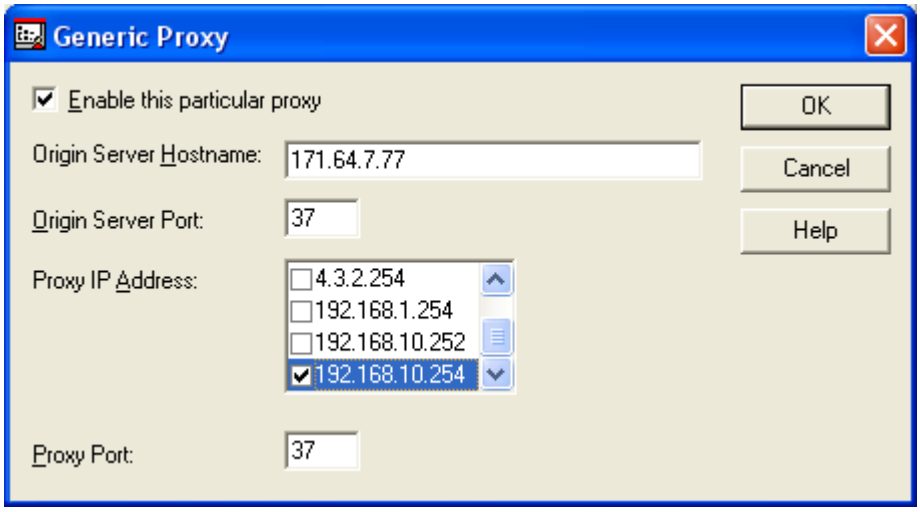
You also need to add Access Control rules to allow port 37 and port 123 outbound for the generic Application Proxies. You can check on the status of the Generic UDP proxies by looking at BORDER1's server console, **Proxy Console** screen, option **19** "Application Proxies", option **4** "Display Generic proxy statistics". From there you can see the number of requests, and if any have been denied based on Access Control rules (ACL Denials).

Configuring A Generic UDP Proxy for NTP



Set the proxy and origin ports to 123, enter the DNS name or IP address for the timeserver, and select the BorderManager secondary internal IP address as the Proxy IP Address.

Configuring a Generic UDP Proxy for RDATE



Set the proxy and origin ports to 37, enter the IP address (or DNS hostname) for a suitable timeserver, and select the BorderManager internal IP address as the Proxy IP Address.

An internal NetWare 3.x, 4.x or 5.x server running RDATE.NLM might be set up with the following Load statement to use this Generic UDP proxy. (In my experience, RDATE does not work with NetWare 6.x).

LOAD RDATE /P 60 /V 2 /U /M 999 192.168.10.254

The RDATE parameters are:

/P 60 Period = 60 minutes, check time every 60 minutes

/V 2 Variance=2 seconds, allow the clock to be off 2 seconds without changing it

/U Protocol=UDP

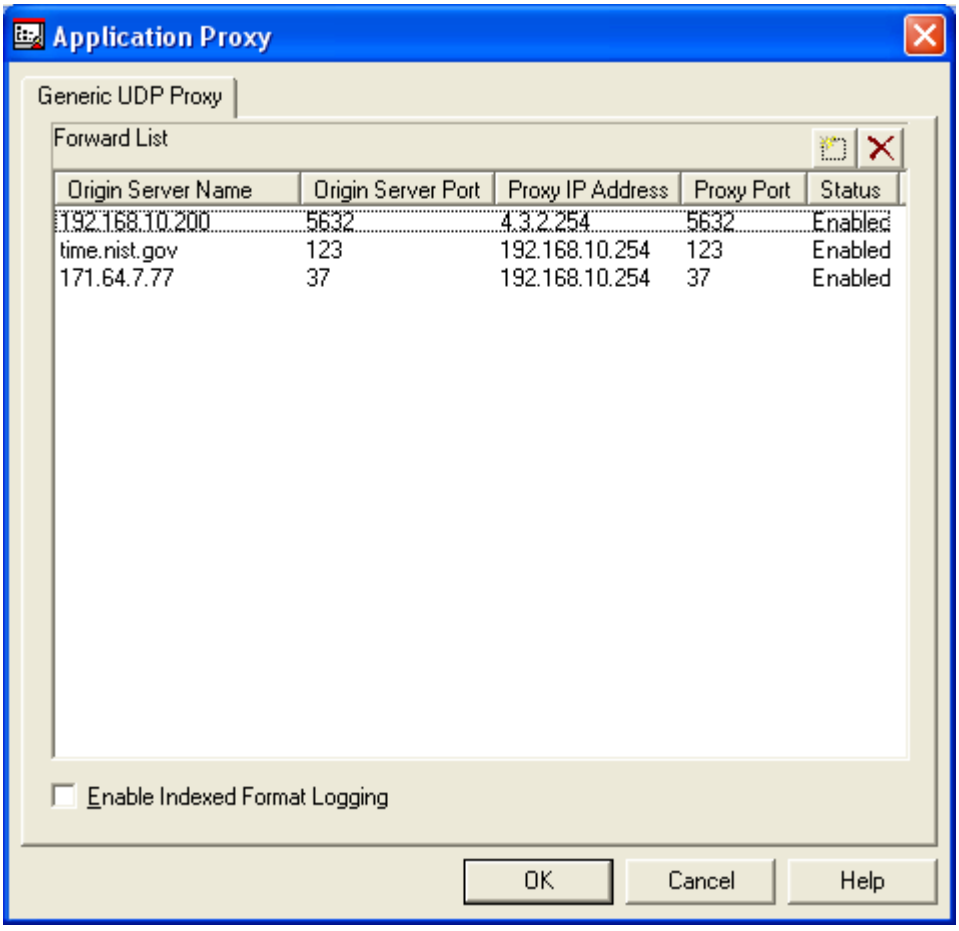
/M 999 Maximum time change allowed, in seconds. Only change the clock is the timeserver time is within 999 seconds of the NetWare server time. (In case the timeserver is radically off, the NetWare server clock will not be changed – however, if the NetWare server time is radically off, RDATE also will not change the time!)

192.168.10.254 The IP address that RDATE uses as a timeserver.

You must add an access rule to allow the use of the generic proxy. The chapter on access rules shows the rule for this example.

Example Generic UDP Proxy for Inbound pcANYWHERE

In order to proxy pcANYWHERE, you must set up TWO generic proxies – one Generic UDP Proxy (shown here) and one Generic TCP Proxy (shown earlier in the chapter for Generic TCP Proxy). pcANYWHERE requires both TCP and UDP protocols, hence the requirement for two generic proxies.



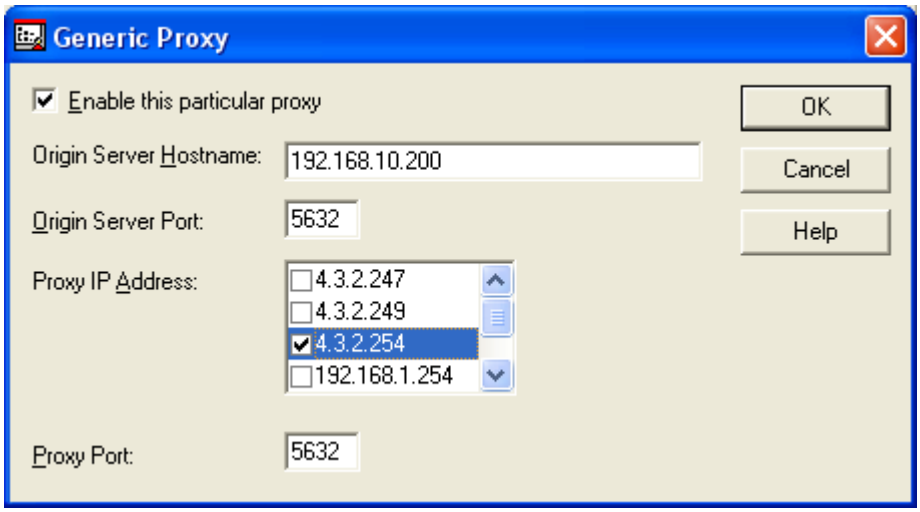
Review the chapter on Access Rules for an example of the access rules required to use this generic proxy.

The **Origin Server Name** is the IP address of the internal pcANYWHERE host.

The **Origin Server Port** is **5632**, the UDP port number that pcANYWHERE uses to locate other pcANYWHERE hosts.

The **Proxy IP Address** is the public IP address on the BorderManager server that clients on the Internet use to connect to the internal pcANYWHERE host.

The **Proxy Port** is **5632**, the UDP port number that pcANYWHERE uses to locate other hosts. Generally, the port number matches the Origin Server Port number.



The origin server hostname is set to 192.168.10.200, the IP address of the PC running pcANYWHERE. The Origin Server Port and Proxy Port are both set to 5632. The Proxy IP Address is set to the primary public IP address 4.3.2.254.

With both Generic TCP and UDP proxies configured properly, filter exceptions in place, access rules in place, and proxy loaded, an inbound pcANYWHERE connection can be made to public IP address 4.3.2.254, and proxied to the internal host at 192.168.10.200.

<This page intentionally left blank. This is to facilitate putting in chapter tabs in a ring binder for double-sided printing. The main chapters should start on an odd-numbered page.>

Chapter 15 – Acceleration (Reverse Proxy)

Concept

Internal web servers can be made securely available on the public side of a BorderManager server through the use of Reverse Proxy Acceleration. HTTP requests come from the Internet to a public IP address on the BorderManager server, and are proxied to the internal web server.

The reverse proxy can be configured such that both HTTP and HTTPS/SSL traffic is also reverse-proxied to the internal web server, though that requires two reverse proxies (one for HTTP and one for HTTPS) to be configured.

Reverse Proxy Acceleration is generally referred to simply as Acceleration or Reverse Proxy.

Pros

- An internal web server can be made available on the Internet without using Static NAT, which requires another public IP address.
- With BorderManager 3.x and later, and the proper PROXY.CFG entries, certain virus attack patterns against the web server can be dropped by the reverse proxy before those patterns ever get to the web server.
- Proxy authentication can be required a reverse proxy, requiring a login to NDS to access the web server.
- Data supplied by the internal web server is cached on the BorderManager server, so that most Internet requests actually are served directly by the BorderManager cache, and not by the internal web server. Thus, the load on the internal web server can be significantly reduced.

Cons

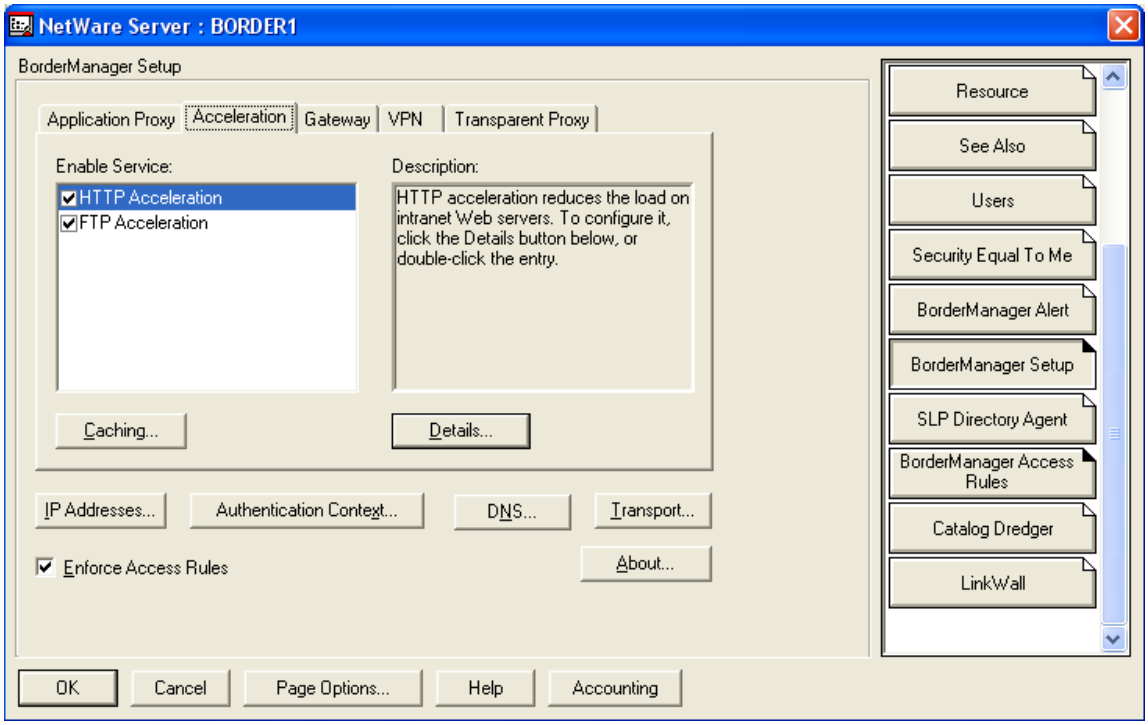
- While proxy authentication can be required for access to a reverse proxy, HTTPS then cannot also be proxied to the internal web server at the same time. Thus, you cannot reverse proxy a secure internal site, if you also require BorderManager to perform authentication for inbound users on that particular reverse proxy.
- Because reverse proxy also caches data from the internal web server, some web page developers working from home do not like reverse proxy. When they make changes to their web pages, the old, cached data still shows up in their browsers.
- The internal HTTP server will only see traffic coming from the private IP address of the BorderManager proxy, which may make log file analysis of the HTTP server useless.

Using The Primary Public IP Address

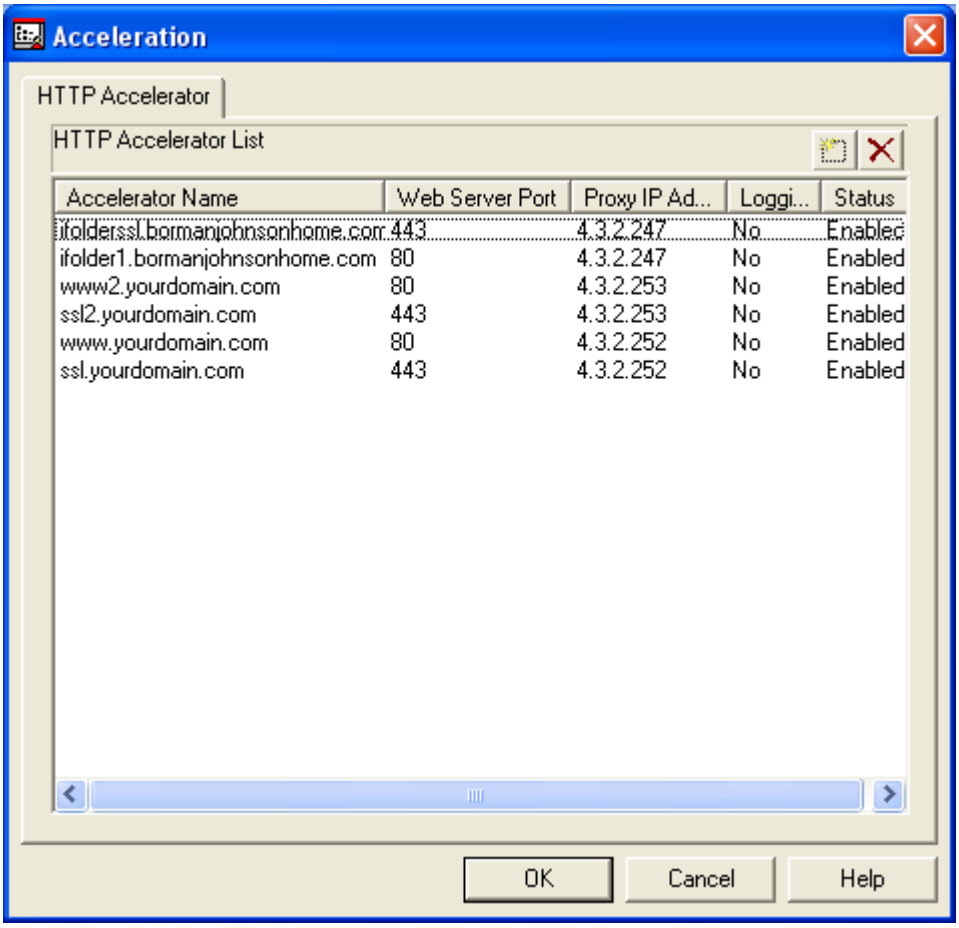
Configuring reverse proxy acceleration for a single internal web server to the main public IP address of the BorderManager server is the easiest configuration. The default packet filter exceptions for BorderManager 3.0 through 3.6 already allow inbound HTTP and HTTPS traffic to the primary public IP address. This is not true for secondary IP addresses.

BorderManager 3.7 may, or may not, have default filter exceptions allowing inbound HTTP and HTTPS to the public IP address – it depends on the installation sequence and patch levels applied when you installed 3.7. BorderManager 3.8 will not include the necessary filter exceptions by default, unless you upgraded in-place from a previous version of BorderManager that had the necessary filter exceptions.

Configuring Reverse Proxy Acceleration



Clicking on the **Acceleration tab** at the BorderManager Setup screen will show you the Acceleration settings enabled. Check the **HTTP Acceleration** box to enable one or more reverse proxies, and click on the **Details** button to configure the settings.



This example shows multiple reverse proxies configured. All of the web servers have been configured with reverse proxy for HTTP and HTTPS/SSL (Notice that http://www.yourdomain.com and http://ssl.yourdomain.com both resolve to the same internal IP address, as do the other two reverse proxies).

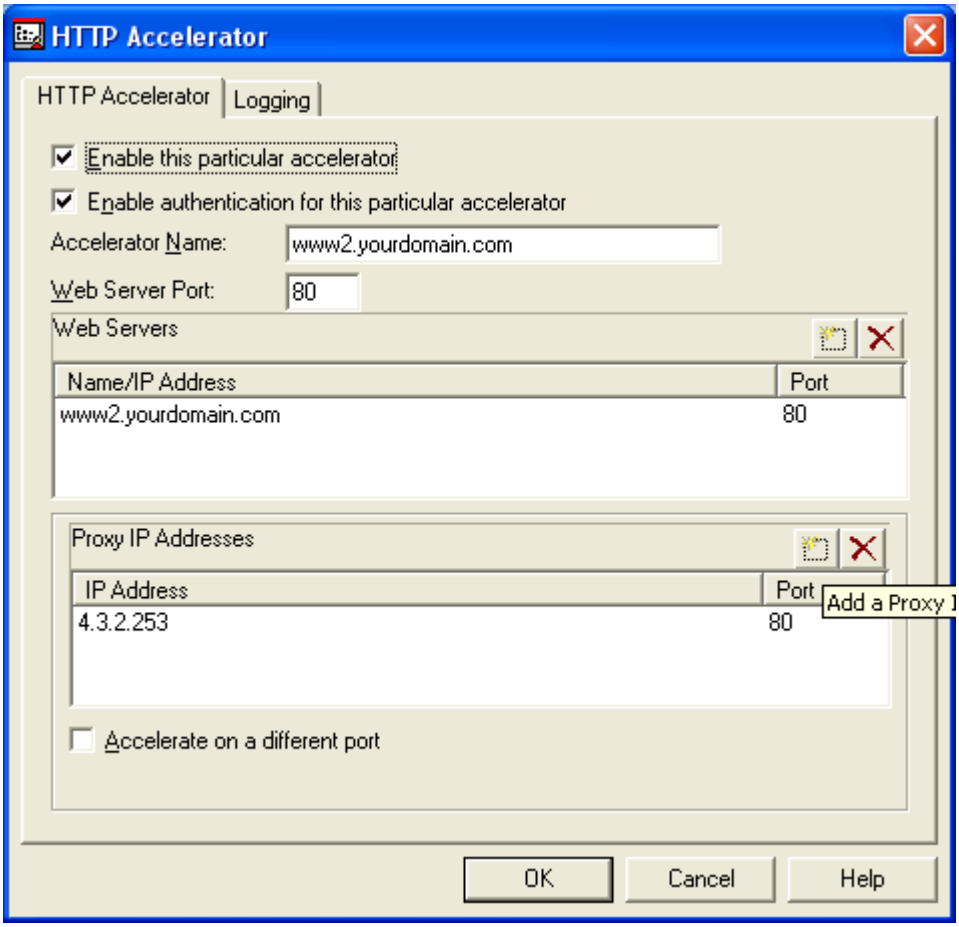
If HTTPS (SSL) needs to be reverse proxied through to an internal web server, you must configure on reverse proxy for port 443 and another reverse proxy for port 80. You cannot repeat the names of the proxies, which is why the entries for SSL.YOURDOMAIN.COM and SSL2.YOURDOMAIN.COM have been added.

Note You can also use Generic TCP proxy for port 443 instead of Reverse Proxy.

Even though the internal web servers have been configured only with the names WWW.YOURDOMAIN.COM and WWW2.YOURDOMAIN.COM, the BorderManager server must also have a way to resolve the IP addresses for

SSL.YOURDOMAIN.COM and SSL2.YOURDOMAIN.COM. The easiest way to accomplish this is to add the IP addresses for SSL.YOURDOMAIN.COM and SSL2.YOURDOMAIN.COM to the BorderManager server's SYS:\ETC\HOSTS file.

You cannot enable Proxy Authentication for a reverse proxy and also pass SSL through to the internal web server. You must choose one option or the other.



The example above shows that the reverse proxy for internal web server WWW2.YOURDOMAIN.COM has been configured to require authentication. Any users wanting to access this reverse proxy will be presented with an SSL Proxy Authentication login screen on their browser. Only those users for which there is an access rule allowing their user ID will be able to access the reverse proxy.

Using a Secondary Public IP Address

If you want to reverse proxy accelerate more than one internal web server (using standard HTTP port 80), or simply wish to accelerate an internal web server on an IP address other than the primary BorderManager public IP address, you **must add packet filter exceptions** in addition to the NWADMN32 configuration details. (You may have to add filter exceptions for web servers reverse proxied to the primary public IP address as well, but that depends on the version of BorderManager installed, and the extent of your filter customizations).

FILTCFG.NLM is used to add packet filter exceptions. You will need to add two, possibly three packet filter exceptions for each secondary IP address being used for reverse proxy acceleration.

Filter Exceptions Needed for Reverse Proxy Acceleration

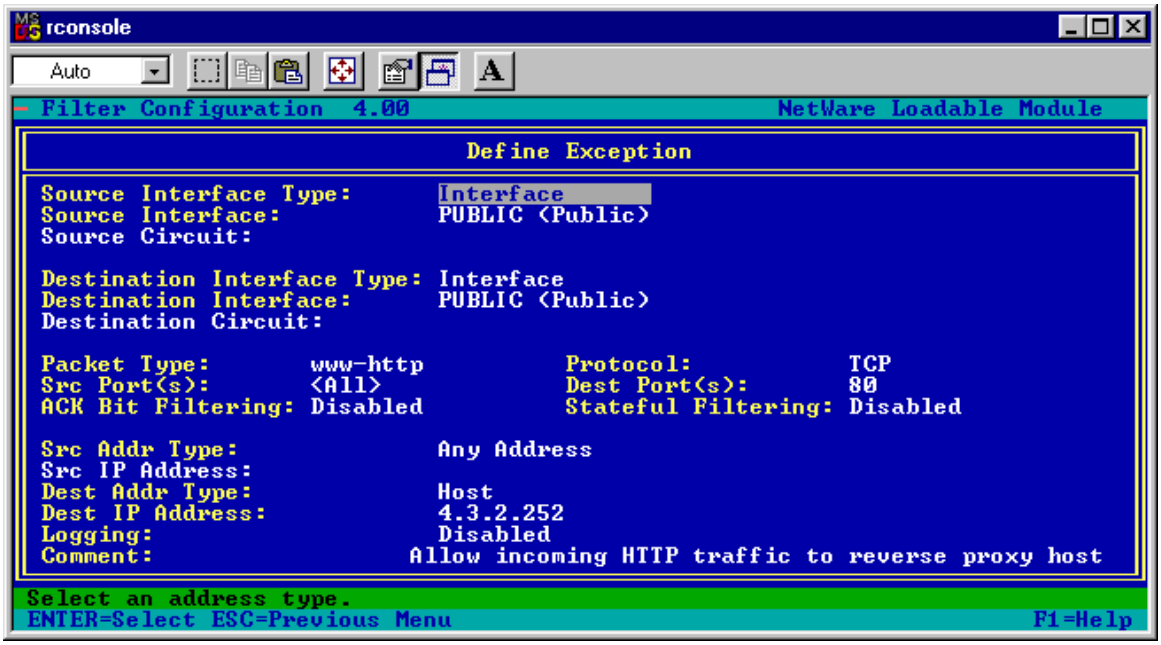
The default packet filter exceptions on BorderManager 3.6 and earlier versions make allowance for inbound HTTP and HTTPS, to the *public IP address*. Because of the default exceptions, you can set up a reverse proxy accelerator on the public IP address and **not** have to deal with packet filter exceptions. However, ANY type of traffic, inbound or outbound, will be blocked both to and from a **secondary IP address** by the default packet filters. You must therefore add packet filter exceptions as needed for static NAT or reverse proxy, or generic proxies, *if using secondary IP addresses*.

Note Review the section toward the front of this book if you are not familiar with secondary IP addresses.

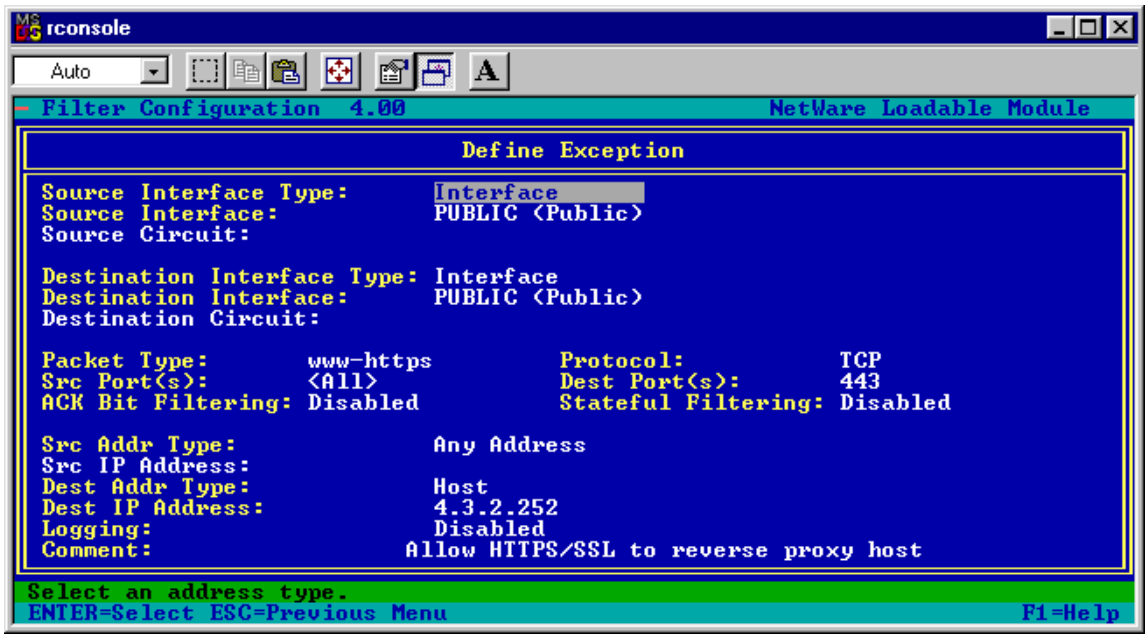
For the reverse proxy accelerator www.yourdomain.com shown earlier to function on a secondary public IP address, at least three packet filter exceptions should be configured. One exception is needed for HTTP inbound traffic. Another exception is needed for HTTPS/SSL inbound traffic. (Note that the reverse proxy accelerator ssl.yourdomain.com is intended to pass HTTPS traffic through to the same IP address as www.yourdomain.com). And a third exception is needed to allow the return traffic from the two reverse proxy accelerators. If you wish for the graphics to display correctly when the user encounters a BorderManager error message, you must also allow TCP destination port 1959 in to the secondary IP address.

Note If you are using Dynamic NAT, you MUST either disable NAT Implicit Filtering in INETCFG, or SET NAT DYNAMIC MODE TO PASS THRU=ON (and put that in AUTOEXEC.NCF). There is also a 'trick' that effectively disables NAT Implicit filtering ONLY for a single IP address – static NAT the public secondary IP address to itself.

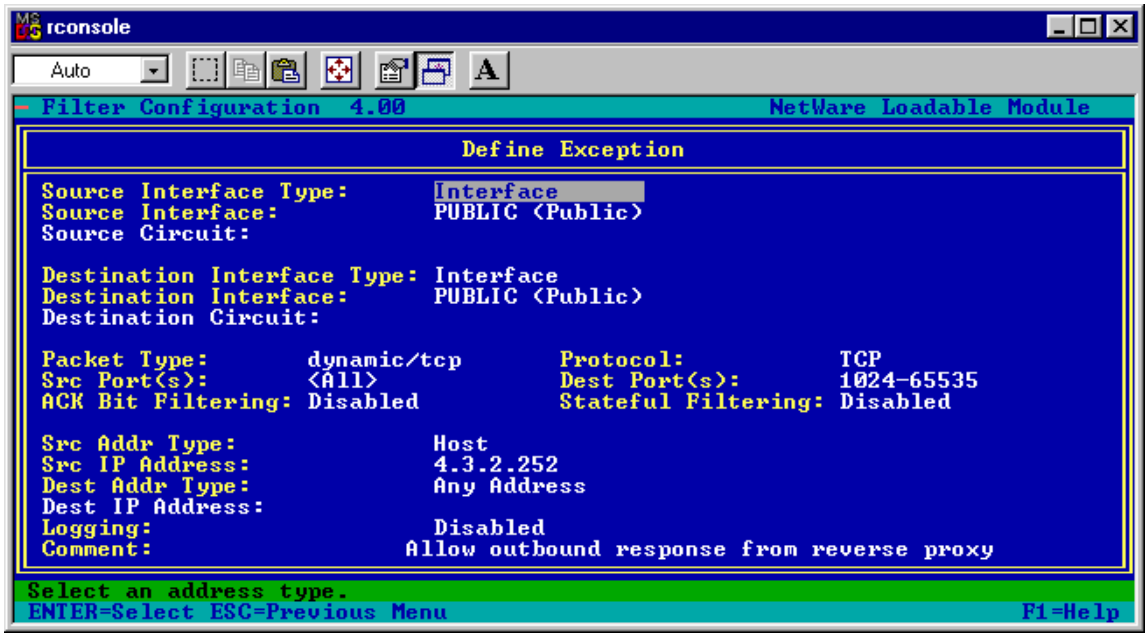
Using FILTCFG.NLM, you would define the packet filter exceptions to end up with the following examples:



Here is the exception to allow HTTP to the public secondary IP address

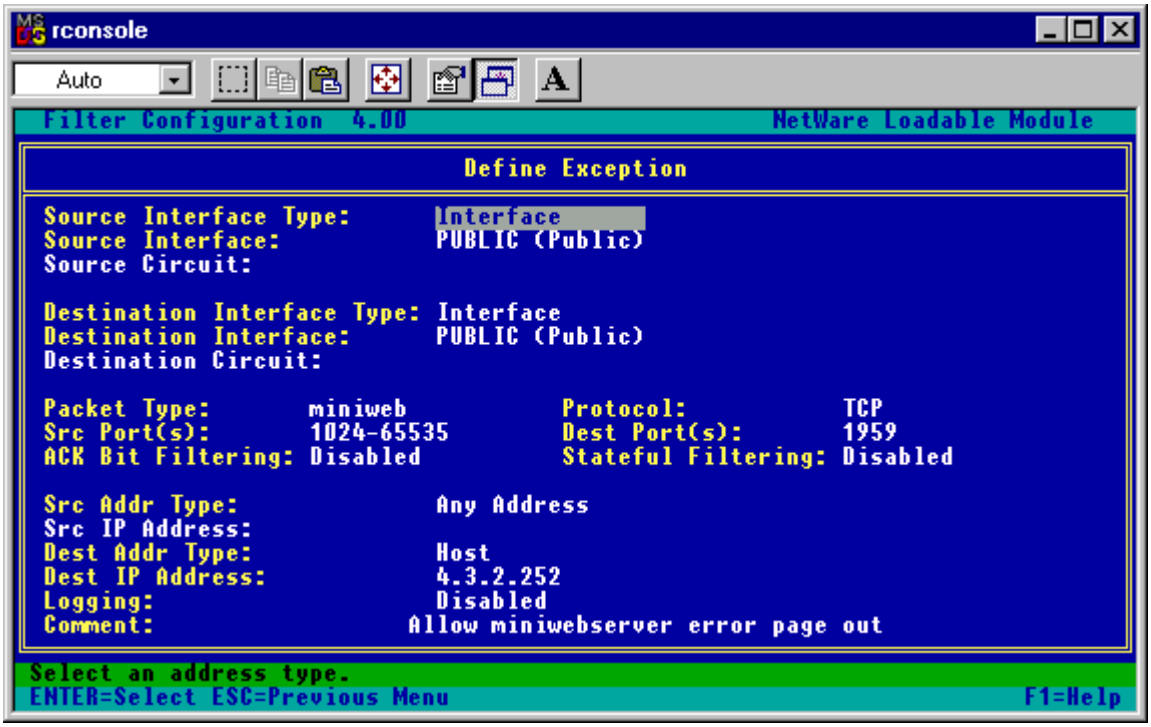


Here is the exception needed to allow HTTPS to the public **secondary IP address** for http://ssl.yourdomain.com. This exception is required for either SSL Proxy Authentication or if needing to pass HTTPS/SSL traffic through to the internal web server.



Here is the exception needed to allow the reverse proxies to return traffic outbound from the public **secondary IP address** for both http://www.yourdomain.com and http://ssl.yourdomain.com.

This exception could also have been split into two more specific exceptions, by specifying the source port number. One exception would have specified source port 80, while the other would have specified source port 443. ACK bit filtering could also be enabled for best security.



This filter exception allows users to request traffic using TCP destination port 1959 via a web browser. That port number is used by the miniwebserver built into BorderManager to serve up the error page graphics when an error is encountered. Without this exception, users will see the text of the error page, but not all the graphics.

The port number used by the miniwebserver is configurable in the SYS:\ETC\PROXY\PROXY.CFG file, but is rarely changed.

Access Rule Required for Reverse Proxy Acceleration

It is only necessary to set up an access rule to allow use of a reverse proxy if you have enabled 'Enable authentication for this particular accelerator' in the Reverse Proxy Acceleration configuration. If you do not enable that option, access rules will NOT be applied to the reverse proxy, and anyone can access it.

If you do enable authentication for a reverse proxy, you will not only require an access rule to allow/restrict its use, you may also have to proxy authenticate to the reverse proxy if SSL Proxy Authentication is enabled for the BorderManager server.

Examples of access rules for the reverse proxy examples given above are shown in the chapter later in this book on Access Rules.

FTP Acceleration

Concept

In the same way that Acceleration of HTTP servers makes internal web servers available to the Internet through a proxy, with caching of the web server data, FTP Acceleration makes internal FTP servers available to the Internet, while caching the data. Access to the data is controlled through Access Rules, and the access rule for source can be based an NDS object (user, group or container).

Pros

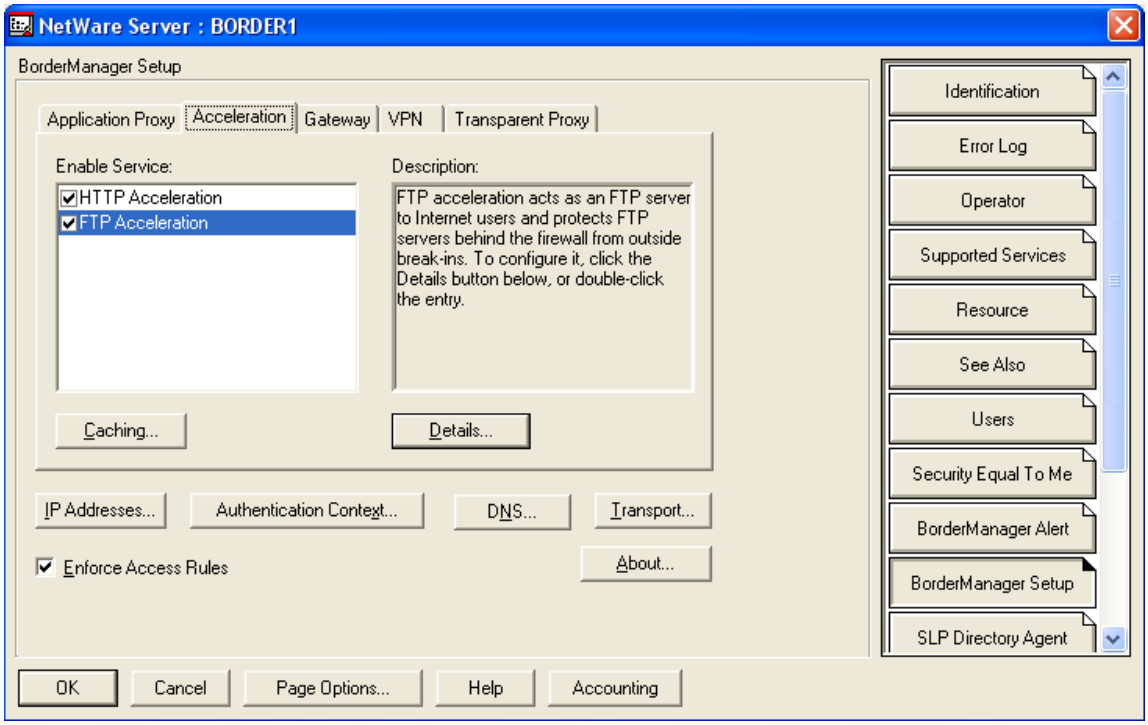
- FTP Acceleration can be used for FTP servers configured for ACTV or PASV mode, though ACTV mode requires that later patches be applied.
- FTP Acceleration caches FTP data, removing that load from the internal FTP server.
- FTP access to an internal FTP server can be done from the primary public IP address, without requiring an additional public IP address for static NAT.

Cons

- Cannot post data to an internal FTP server through FTP Proxy.
- The internal FTP server will only see traffic coming from the private IP address of the BorderManager proxy, which may make log file analysis of the FTP server useless.

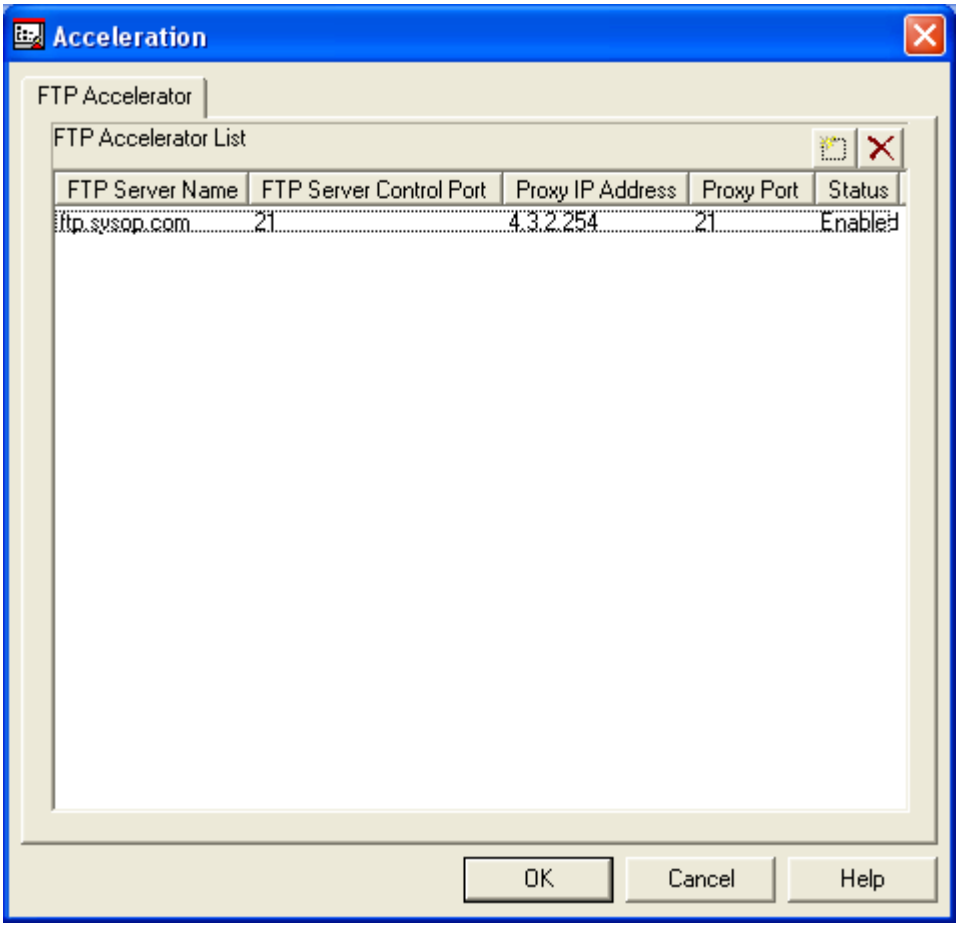
Configuration

This is one case where the default packet filter exceptions for BorderManager 3.7 or earlier do not cover the requirements of a proxy. You must add a packet filter exception to allow TCP destination port 21 to the BorderManager server's public IP address being used for FTP Acceleration.

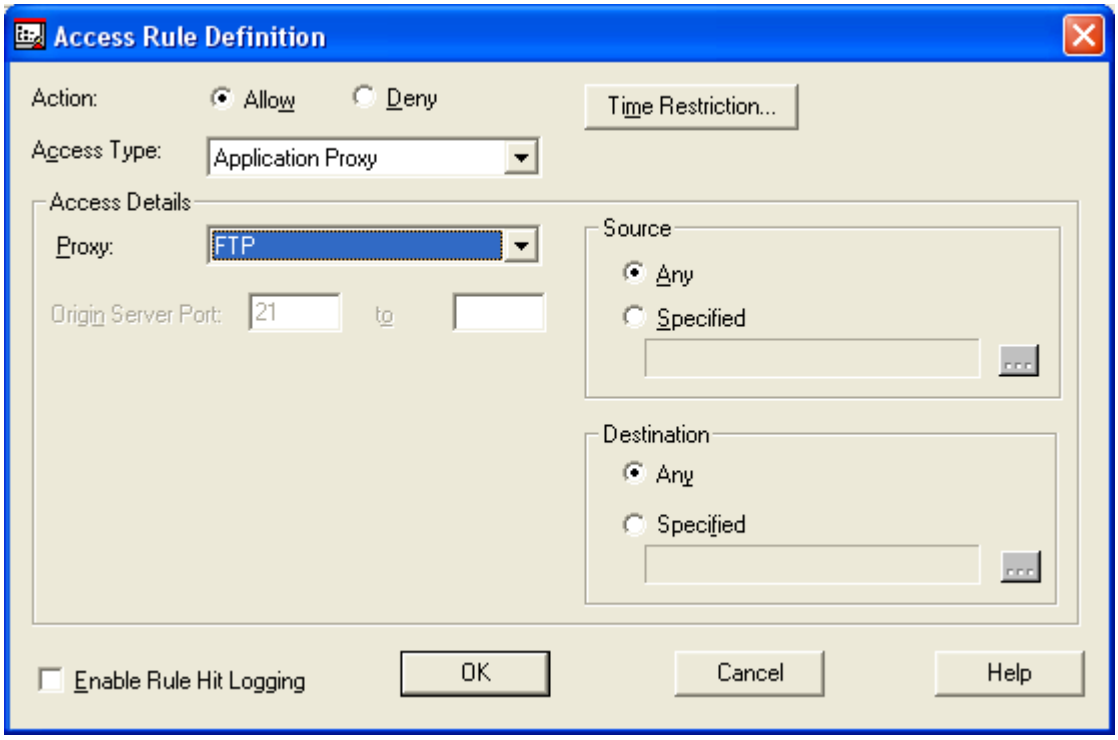


Check the **FTP Acceleration** box under the **Acceleration** tab in the **BorderManager Setup** main menu.

Click on **Details** to configure FTP Acceleration.



The example above shows an FTP accelerator configured to listen on public IP address 4.3.2.254 for traffic on TCP port 21 and pass that traffic through to an internal FTP server called FTP.SYSOP.COM. The IP address of FTP.SYSOP.COM could also be used.



With the appropriate Access Rule in place, and filter exceptions allowing FTP traffic to the public proxy address, you should then be able to access the internal FTP server from the public IP address. Data requested from or posted to the internal FTP server will also be held in cache at the BorderManager server.

The access rule shown will allow anyone to use the FTP Acceleration Proxy for inbound FTP traffic. It will **also** allow any internal user to use the FTP Proxy for outbound FTP traffic. You will have to specify source and destination values to limit inbound and outbound traffic as desired. You can base the Source value on NDS objects such as users, groups or containers.

Examples of the use of access rules to control both outbound access through the FTP Proxy and inbound access through FTP Acceleration are shown in the chapter on Access Rules.

Chapter 16 – The Gateways

IPX/IP Gateway

CAUTION *The IPX/IP and IP/IP Gateways are no longer supported with BorderManager 3.7 and 3.8, though they are included for some backwards compatibility. These gateways require Client32 components that have not really been supported since approximately version 2.5 of Client32. You should not use IP/IP or IPX/IP Gateway anymore. The SOCKS Gateway is still supported. SOCKS Gateway uses the same NLM as IP/IP and IPX/IP Gateways – IPXIPGW.NLM.*

Concept

The purpose of the IPX/IP Gateway is to encapsulate IP packets within IPX packets, allowing TCP/IP communications between a BorderManager server and a TCP/IP destination host without having to set up TCP/IP on the internal LAN. This capability is basically something that was developed when many LAN's were running IPX only, and TCP/IP services had not been set up. There are a few advantages in terms of control and security – access rules can be used to control the TCP/IP traffic, and not having TCP/IP services on the LAN makes it nearly impossible to hack from the Internet.

The IP traffic is controlled by Access Rules, and the Access Rules can be based on NDS objects, such as users, groups or containers.

You can apply access rules to the users going through the IPX/IP gateway by just enabling SSO authentication in the Details page of the IPX/IP Gateway in NWADMN32. If you want to use the proxy in conjunction with the IP gateway, and you still want to maintain the ability to create access rules based on NDS objects, you will have to enable the Transparent Proxy as well.

The IPX/IP Gateway requires a special IP Gateway service to be installed on the workstation as a part of Novell's Client32. IP Gateway service is restricted to platforms running 32-bit Windows operating systems.

Because all traffic from an IP Gateway client must pass through a BorderManager server, the server can become a bottleneck. Even

internal traffic will go from a workstation to the BorderManager server and back to an internal destination.

If you have enabled both IP/IP and IPX/IP Gateways on the BorderManager server, and a TCP/IP stack is present on the workstation, the IP/IP Gateway will be used automatically. IPX/IP is only used if IP/IP Gateway is not enabled on the BorderManager server, or if only IPX is present on the workstation.

Pros

- Easy to configure
- Complete integration with NDS
- Access rules apply to every port and protocol
- Great security and control
- Can provide secure Internet access without having to configure an Internet protocol.

Cons

- Suitable for small environment where the only requirement is for Internet access.
- The workstations always talk to the gateway even for internal traffic. This prevents the usage of certain applications (like ZENworks) that make use of the workstation IP address.
- Some applications requiring a native TCP/IP stack will not work with IPX/IP Gateway.
- Requires a special Client32 service, and will therefore only work with Windows hosts.
- Does not work with all versions of Client32.
- Has not been supported by Novell for years.

History of IPX/IP Gateway

It may be useful to know the history of the Novell IPX/IP Gateway as many people misunderstand its purpose and certain critical details.

IntranetWare IPX/IP Gateway

NetWare 4.11, sold as a bundle of services under the name IntranetWare, contained an IPX/IP service as part of the NIAS (NetWare Internet Access Services) product. (NIAS itself has

undergone a series of revisions, with a different set of services included with each version – but that is another story!)

This version of IPX/IP Gateway was based on purchased code from a third-party vendor. It was designed in a time before the world wide web, and the access controls on it were not particularly suited for internet access control. Approximately 250 users might be able to use the service at the same time, but performance was slow. A special menu option in INETCFG was used to configure this version of IPX/IP Gateway, with some attributes controlled by a snapin for NWADMN3X.

The way that this version of IPX/IP Gateway worked at the client was by using a special version of WINSOCK.DLL and WSOCK32.DLL. A program was used to 'enable' the gateway by simply renaming the Novell and Microsoft versions of these files. Because the Client32 installation also added the Novell Client32 directory to the path, the Novell version of the files would be found. If the Microsoft versions were renamed so that they would not run, then Novell versions would be named so that the Novell versions would run instead. This scheme led to a number of issues, including problems with multiple copies of the Microsoft Winsock files possibly existing in various directories, and programs that were incompatible with the Novell version of winsock.dll.

Only early version of Novell's Client32 were designed to work with the Novell Winsock files.

The IPX/IP Gateway feature allowed an IPX-only LAN (common at the time) to easily and securely access the Internet. The only IP address required was on the public interface of the IntranetWare server, and (for very small LAN's), that interface could even be a dial-on-demand analog modem.

BorderManager 2.1 IPX/IP Gateway

When BorderManager 2.1 was introduced, IPX/IP Gateway software was included. This version of IPX/IP Gateway was written entirely by Novell and provided better performance. The IPX/IP Gateway services were entirely configured from within NWADMN3X.EXE.

Again, like the IntranetWare version of the IPX/IP Gateway client, a special version of WINSOCK.DLL and WSOCK32.DLL were used to encapsulate IP packets inside IPX packets. The versions of Client32 designed to work with BorderManager 2.1 IPX/IP Gateway were (only) version 2.12, 2.2 and 2.5. An NT client was never introduced. **Note that the ONLY versions of Client32 that supported this gateway version are 2.12, 2.2 and 2.5!** This fact has had a lot of implications for organizations wanting to upgrade Client32 (for ZENworks capabilities for instance) while wanting to maintain IPX/IP Gateway connectivity.

Numerous incompatibilities between Novell's special Winsock files began to arise, particularly when 32-bit programs written to Winsock2 requirements were used. A common trick to get these programs to work with IPX/IP Gateway was to copy the Microsoft version of WSOCK32.DLL to the application's directory, so that the Microsoft WSOCK32.DLL would be used by the application along with the Novell WINSOCK.DLL. However, BorderManager 2.1 IPX/IP Gateway supports only WINSOCK1, so true WINSOCK2 programs would not always function through the IPX/IP Gateway.

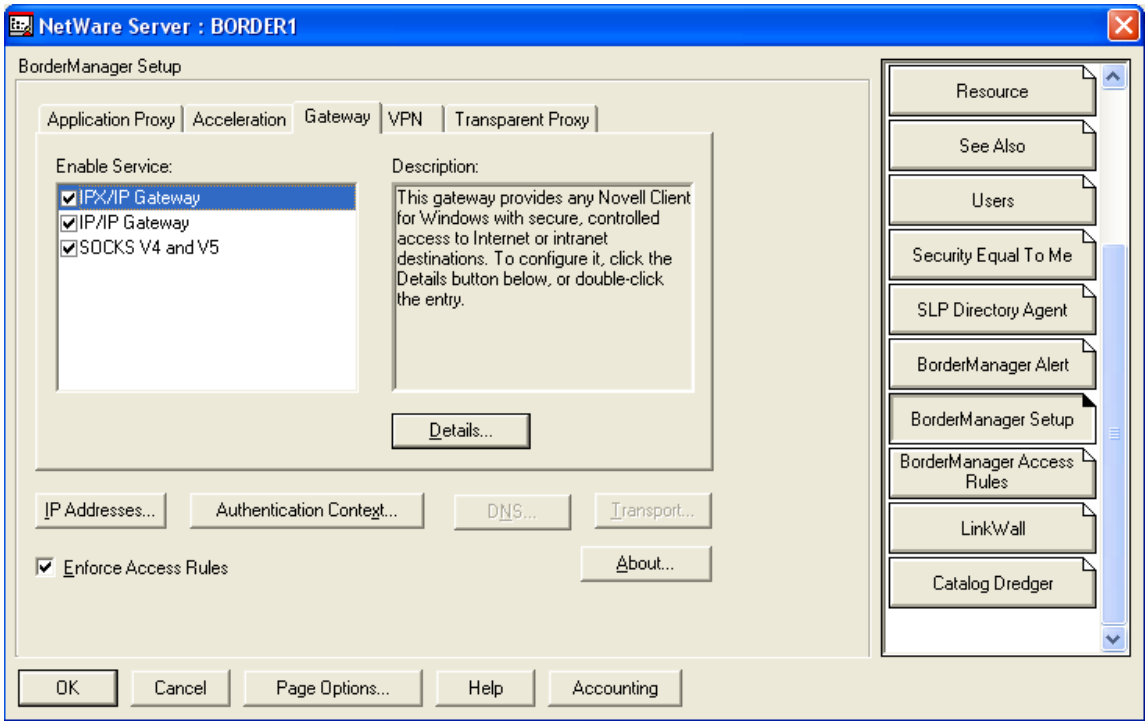
BorderManager 3.x IPX/IP Gateway

By the time BorderManager 3.0 was released, pure IPX networks were rapidly disappearing, and Internet access was being taken for granted. IPX/IP Gateway issues with special Novell Winsock files led to Novell redesigning IPX/IP Gateway to use only the Microsoft-supplied Winsock files. The BorderManager 3.x IPX/IP Gateway now supports WINSOCK2.

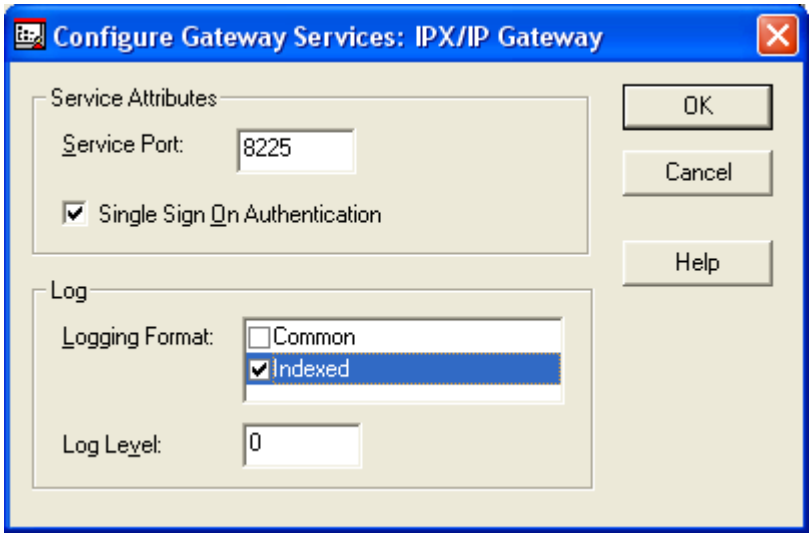
In order to use CLNTRUST or the Transparent Proxy with the IPX/IP Gateway, a newer version of Client32 had to be used (version 3.0 or later, for Windows 9x). The reason is that CLNTRUST and the BorderManager 3.x proxies require WINSOCK2 capabilities.

The change in the IPX/IP Gateway Winsock files basically forced networks to upgrade Client32 on all PC's as soon as BorderManager 3.0 was installed.

The IPX/IP Gateway appears to have been added into the product partly for backwards compatibility. A number of incompatibilities between IPX/IP Gateway and applications occurred, but further updates to the IPX/IP Gateway software have not been seen. NetWare 5.0's introduction further stressed Novell commitment to TCP/IP networks, and there is little need any more for the IPX/IP Gateway in a modern LAN. The reader is strongly urged to migrate from a IPX/IP Gateway design to a pure IP network for Internet access through BorderManager.



The IPX/IP Gateway is enabled by checking the **IPX/IP Gateway** box under the **Gateway** tab on the **BorderManager Setup** main menu.



Click on **Details** to configure additional IPX/IP Gateway parameters.

Check **Single Sign On Authentication** if you want to based access rules on NDS users, groups or containers.

Check the logging format, if any, that you wish to enable for IPX/IP Gateway. Note that you cannot specify the Common log file location.

Note The Single Sign On Authentication and Log settings for IPX/IP Gateway also affect the IP/IP Gateway.

Client Settings For IP Gateway

The combination of settings needed for the IP Gateway service to work the way you want it can be extremely confusing. Use the following guidelines.

Use Proxy, No Authentication, No Rules, No Logging

- Enable the IP gateway at the server in NWADMN32.
- Enable the HTTP proxy
- Do **not** enable proxy authentication
- Do **not** enable access rule enforcement
- Install Client32 with the IP Gateway service
- Configure your browser to use the HTTP proxy

In this configuration is almost impossible to prevent people from bypassing the proxy. The only way to do control usage is to enable IP gateway SSO authentication and create an access rule where you only allow access to the proxy IP address for port 8080.

Use Proxy, Authentication, Access Rules and Logging

- Enable the IP Gateway with SSO authentication in NWADMN32.
- Enable the transparent proxy (the ports monitored are completely irrelevant)
- Enable the HTTP proxy
- Enable proxy authentication (SSO only)
- Enable access rules based on NDS identity
- Install Client 32 with the IP Gateway service
- Enable the HTTP proxy on the Client IP Gateway service (this is for the transparent proxy)
- Do not configure the browser to use the proxy (direct connection to the internet). If you configure the browser to use the proxy the authentication will fail.
- Use CLNTRUST.EXE on the client

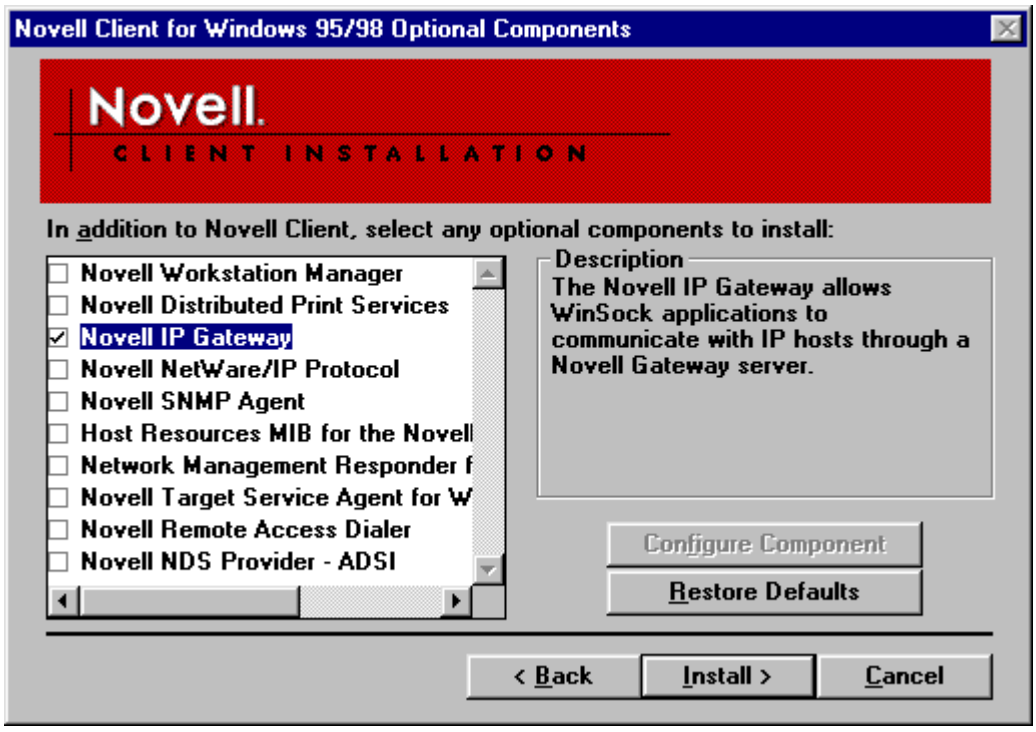
Use IP gateway, No Proxy, Access Rules and Logging

- Enable the IP gateway with SSO authentication in NWADMN32 (for the IPX/IP Gateway this is necessary to apply access rules – I am not sure for IP/IP Gateway.)
- Configure access rules for NDS objects
- Enable common logging on the IP Gateway, not on the HTTP Proxy.
- Install Client32 with the IP Gateway service on the PC
- Do not enable the HTTP proxy in the IP Gateway service
- Use CLNTRUST.EXE on the PC.
- Use "direct connection to the internet" in the browser, do not configure the browser for a proxy server.

Installing IP Gateway Service on the PC

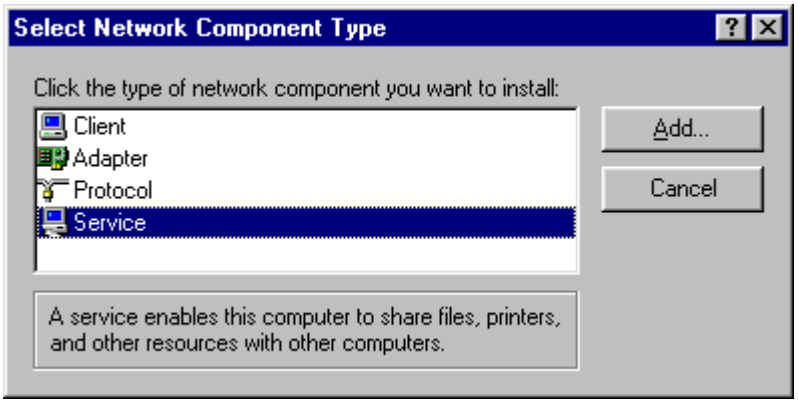
The IPX/IP and IP/IP Gateways can only be accessed with the Novell IP Gateway service installed on Windows PC's.

The IP Gateway service can be installed when you are installing Client32, as shown below.

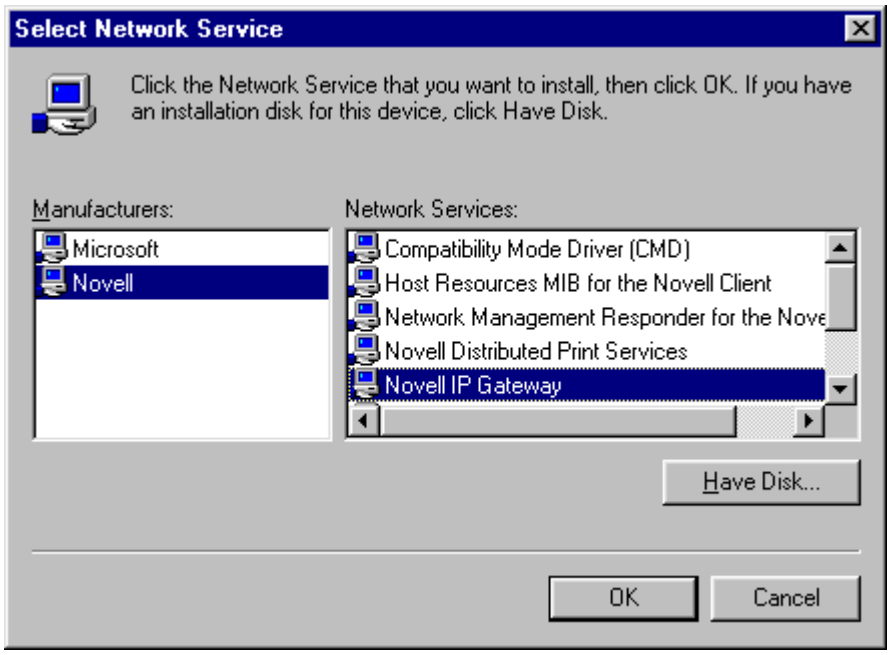


You can also add the Novell IP Gateway service after Client32 has been installed, in Network Neighborhood properties, by adding a Service, selecting Novell, and selecting the IP Gateway service as shown below.

However, experience has shown that installing the IP Gateway after Client32 has been installed is not as reliable as installing IP Gateway with a new Client32 installation.

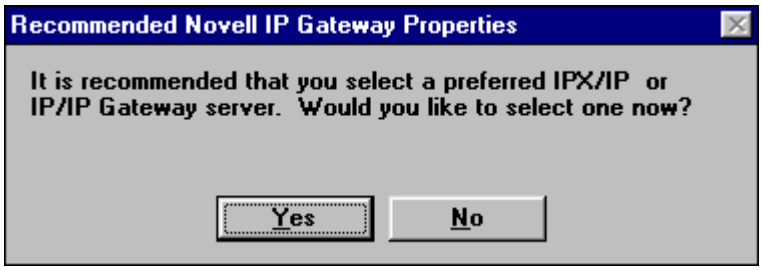


After selecting **Service**, scroll to the Novell selection.

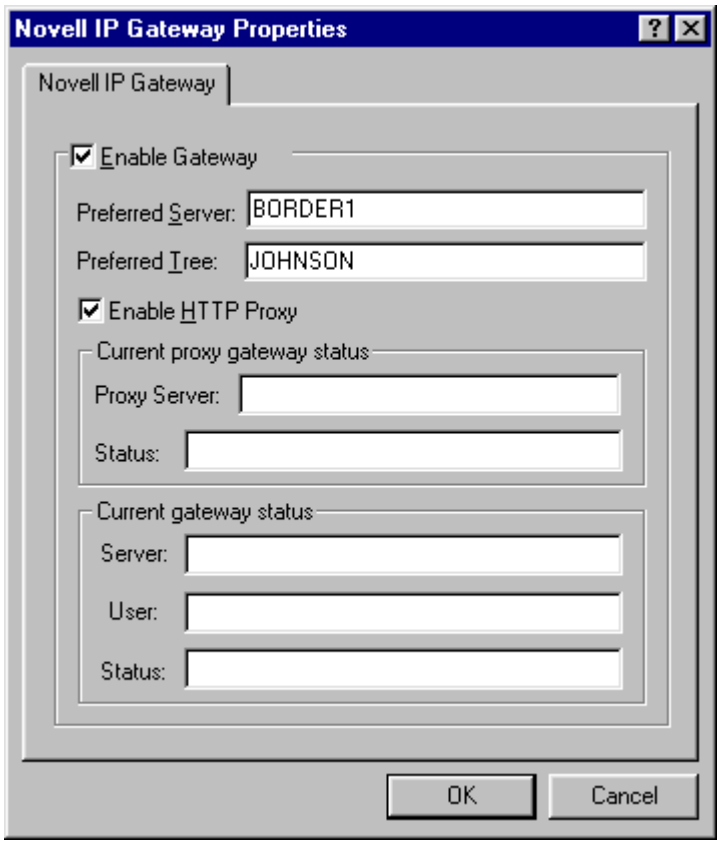


Select the **Novell IP Gateway**, and click on **OK**.

Whether you select to install the IP Gateway at Client32 installation, or afterwards, you will be prompted to set a preferred IP Gateway server, as shown below.



You should click on Yes to proceed.



Configure both the **Preferred Server** and **Preferred Tree** to match your environment, and reboot the PC to have the settings take effect.

Check the **Enable HTTP Proxy** box only if you understand the Client Settings for IP Gateway section shown earlier.

IP/IP Gateway

Concept

The purpose of the IP/IP Gateway is to provide more control over TCP/IP communications than would be possible using only a straight TCP/IP stack. IP packets are generated at the workstation which must first pass through the BorderManager server. The BorderManager server can then control whether or not the packets are passed on to the final destination. The IP traffic is controlled by Access Rules, and the Access Rules can be based on NDS objects, such as users, groups or containers.

You can apply access rules to the users going through the IP gateway by just enabling SSO authentication in the Details page of the IP Gateway in NWADMN32. However, if you want to use the HTTP proxy in conjunction with the IP gateway, and you still want to maintain the ability to create access rules based on NDS objects, you will have to enable the Transparent Proxy, as well.

The IP/IP Gateway requires a special IP Gateway service to be installed on the workstation as a part of Novell's Client32. IP Gateway service is restricted to platforms running 32-bit Windows operating systems.

Because all traffic from an IP Gateway client must pass through a BorderManager server, the server can become a bottleneck. Even internal traffic will go from a workstation to the BorderManager server and back to an internal destination.

Pros

- Easy to configure
- Complete integration with NDS
- Access rules apply to every port and protocol
- Great security and control

Cons

- Suitable for small environment where the only requirement is for Internet access.
- The workstations always talk to the gateway even for internal traffic. This prevents the usage of certain applications (like ZENworks) that make use of the workstation IP address.

- Some applications requiring a native TCP/IP stack will not work with IPX/IP Gateway.
- Requires a special Client32 service, and will therefore only work with Windows hosts.
- Has not been supported by Novell for years.

Access Rules, Proxies and the IP/IP Gateway

The interaction of the IP/IP Gateway with other BorderManager components is somewhat complicated. Use the following combinations for best results.

IP/IP Gateway With Access Rules And Without Proxy

- Enable the IP/IP Gateway
- Enable SSO Authentication to the gateway
- Enable access rule enforcement

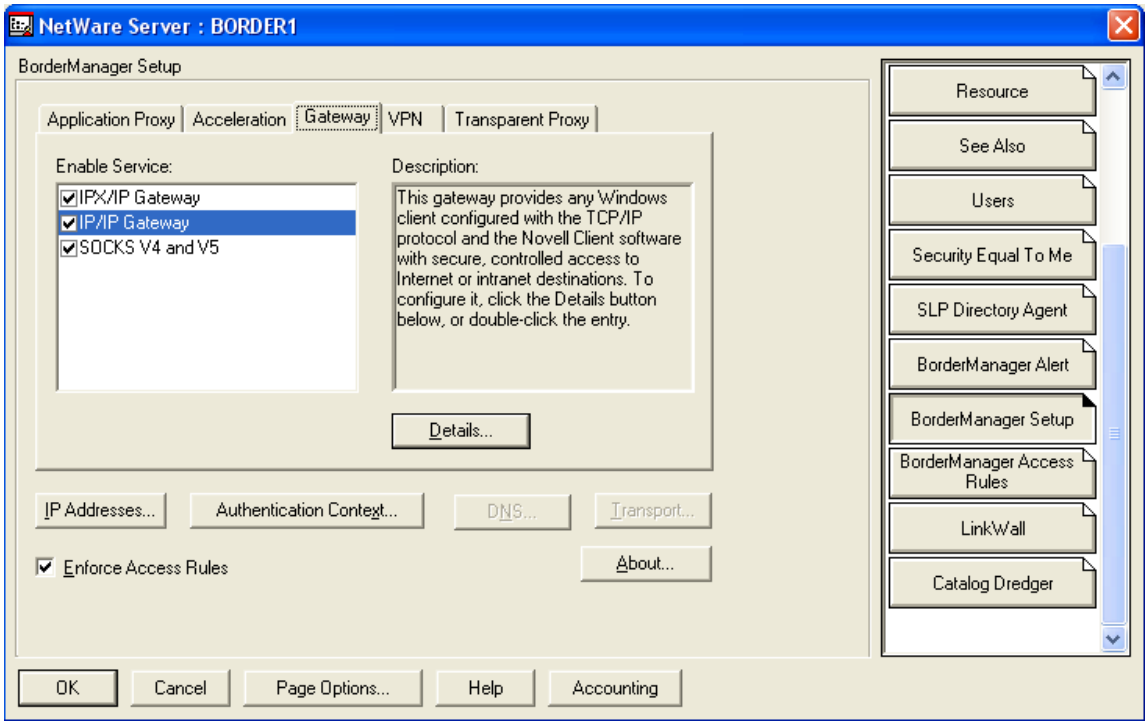
IP/IP Gateway Without Access Rules And With Proxy

- Enable the gateway (without SSO authentication).
- Enable the proxy. (You can't enforce proxy authentication)

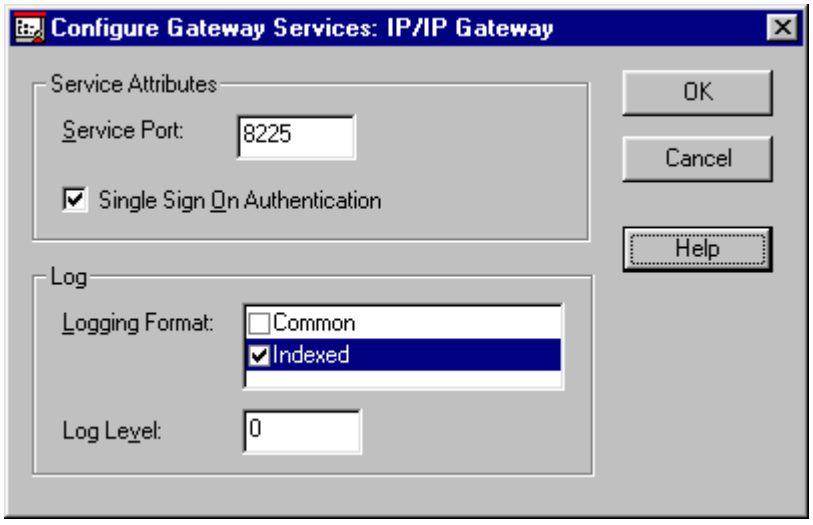
IP/IP Gateway With Proxy and With Access Rules

- Enable the IP/IP Gateway with SSO authentication
- Enable the proxy with SSO authentication. (only SSO will work.)
- Enable Transparent Proxy (Transparent Proxy must be used)
- Enable access rule enforcement

Configuring IP/IP Gateway



The IP/IP Gateway is enabled by checking the **IP/IP Gateway** box under the **Gateway** tab on the **BorderManager Setup** main menu.



Click on **Details** to configure additional IP/IP Gateway parameters.

Check **Single Sign On Authentication** if you want to base access rules on NDS users, groups or containers. (Later versions of BorderManager may not provide this option).

Check the logging format, if any, that you wish to enable for IP/IP Gateway. Note that you cannot specify the Common log file location.

Note The Single Sign On Authentication and Log settings for IP/IP Gateway also affect the IPX/IP Gateway.

SOCKS Gateway

Concept

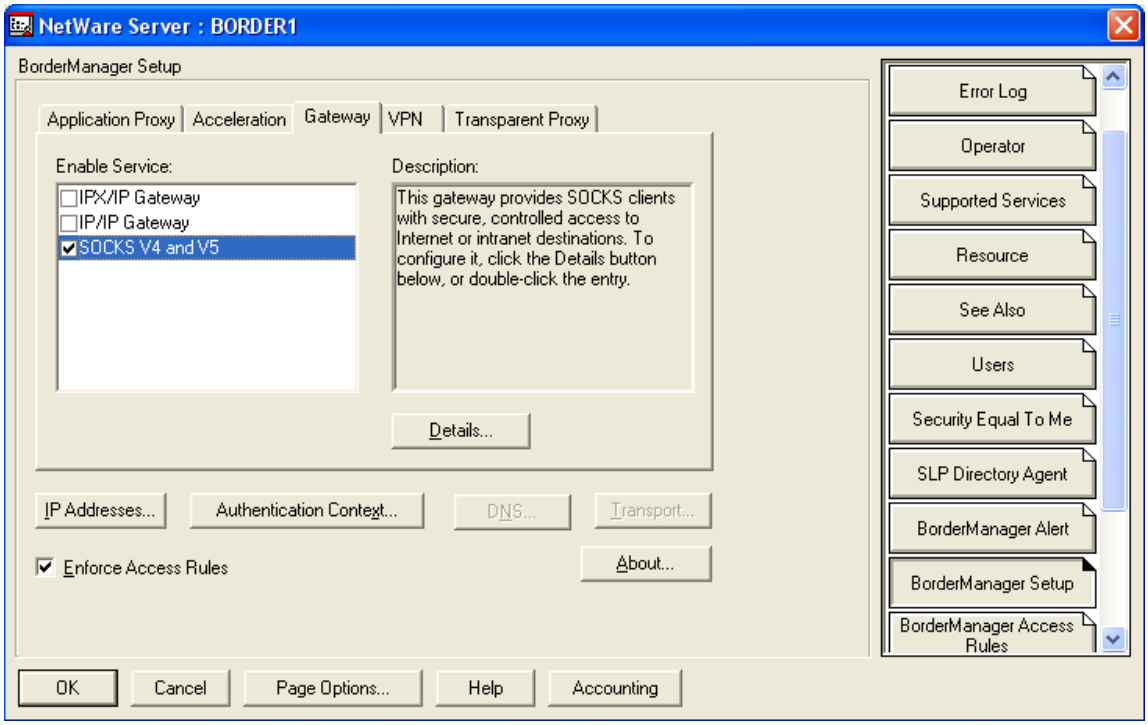
The SOCKS gateway is designed to allow applications configured to use a SOCKS server to access the Internet.

Pros

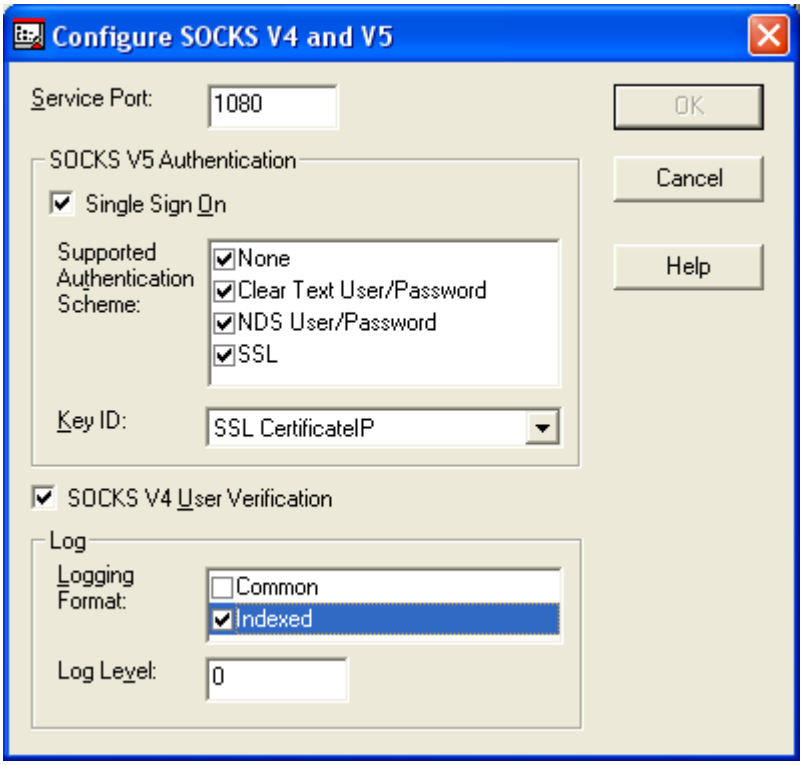
- The SOCKS gateway allows internal SOCKS client to have some access to the internet.
- You can configure authentication with SOCKS to have some control over the use of the gateway.

Cons

- The SOCKS gateway may require you to add filter exceptions for the ports involved.
- Configuring SOCKS version 5 authentication is not necessarily easy.



The SOCKS Gateway is enabled by checking the **SOCKS Gateway** box under the **Gateway** tab on the **BorderManager Setup** main menu.



Quite a few parameters can be configured for the SOCKS gateway.

The standard **Service Port** is **1080** and probably should not be changed.

You have a choice of SOCKS version 4 or version 5 authentication. SOCKS version 4 is easier to set up as it does not match the user ID to any kind of user ID list (NDS).

SOCKS version 5 can authenticate a user ID in four ways:

- **None** - I guess this really means "we don't care if you authenticate, you can still use the SOCKS proxy"!
- **Clear Text User /Password** – A SOCKS5-compliant program running on the PC will send a user ID and password in clear text to the BorderManager server.
- **NDS User/Password** – IF the SOCKS5 software program supports NDS authentication, this option will authenticate the user information to NDS.
- **SSL** – This option actually affect the Clear Text and NDS User authentication options by requiring SSL encryption to be set up before the user authentication takes place. If this option is selected, a Key Material Object must be selected in the **Key ID** field.

For additional information on the authentication methods, look at the online help in NWADMN32.

Chapter 17 – Legacy Site-to-Site VPN

Note BorderManager 3.7 and earlier VPN is called 'legacy' VPN in this book. The new IKE-based BorderManager 3.8 VPN is covered separately in a later chapter. Legacy VPN on a BorderManager 3.8 server is still set up essentially the same as described here – you must run VPNCFG for instance – but access rules are done in iManager 2.0, not NWADMN32.

Introduction to BorderManager Legacy VPN

VPN stands for Virtual Private Network, which is a method for encrypting data to send it securely across an unsecure network (like the Internet). The Novell BorderManager VPN product can be configured in two ways – **Client-to-Site** and **Site-to-Site**. You can use either or both at the same time. Client-to-Site is used to connect a remote PC to a BorderManager–protected network over the Internet. Site-to-Site is used to connect two protected sites together over the Internet. Both IP and IPX protocols can be used in either VPN. Only BorderManager 3.8 can make a connection to a non-Novell VPN client or server.

Whether you configure Site-to-Site or Client-to-Site, the first step is the same for each: you must set up a Master VPN server.

Concept

Site-to-Site VPN establishes a virtual private network between two or more Novell BorderManager 3.x VPN servers. The connection is (generally) made through the Internet. All data passing between VPN end-points is encrypted and tunneled inside TCP/IP packets. One server must be configured as the Master server, while all others must be configured as Slave servers. Up to 254 VPN servers can be connected in one site-to-site VPN.

Filter Exceptions Required

No additional filter exceptions are required for versions of BorderManager prior to 3.7. Version 3.7 however does not add

enough exceptions by default to allow the VPN to function. You must add the following exceptions, which cover both Site-to-Site and Client-to-Site VPN requirements. If you have installed BorderManager 3.7 Service Pack 2 or later (BM37SP2.EXE), you can use the updated BRDCFG to add filter exceptions required for VPN to function.

- SKIP protocol, source address = public IP address, source & destination interfaces = public
- TCP source port 353, destination ports 1024-65535, source address = public IP address, source and destination interfaces = public
- UDP source port 353, destination ports 1024-65535, source address = public IP address, source and destination interfaces=public
- TCP source port 213, destination ports 1024-65535, source address = public IP address, source & destination interfaces = public
- TCP source ports 1024-65535, destination port 213, source address = public IP address, source & destination interfaces = public
- UDP source ports 1024-65535, destination port 2010, destination address = public IP address, source & destination interfaces = public
- UDP source port 2010, destination ports 1024-65535, source IP address = public IP address, source & destination interfaces = public
- UDP source and destination ports 2010, source IP address = public IP address, source & destination interfaces = public

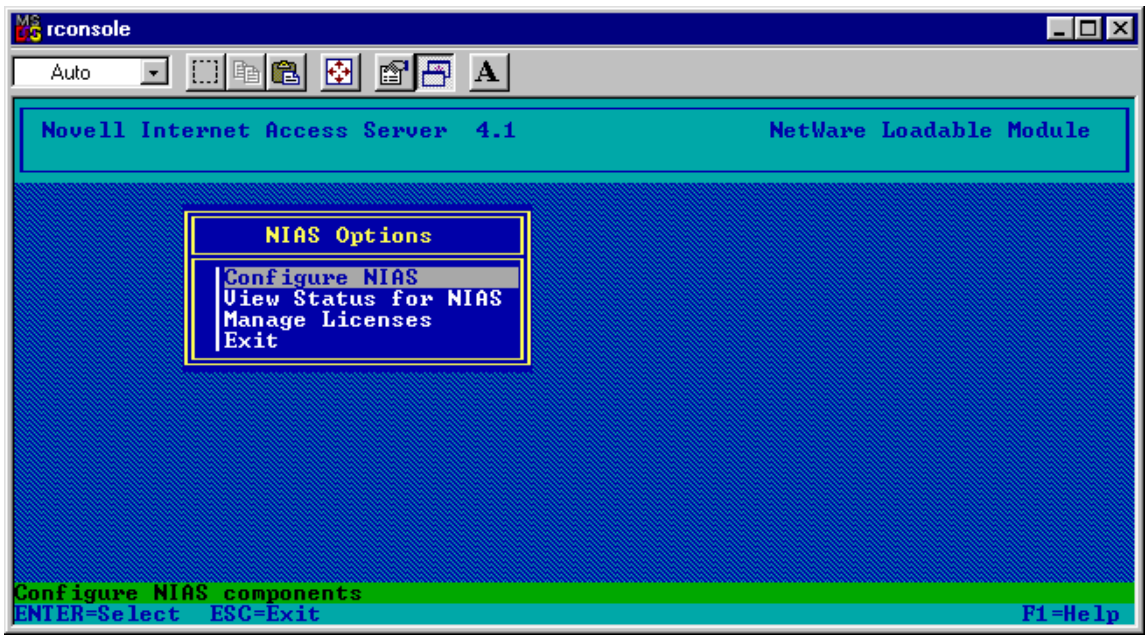
These exceptions are shown, and explained in more detail in my book "*Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions, Third Edition*", available at http://www.craigjconsulting.com.

Setting Up the Master VPN Server

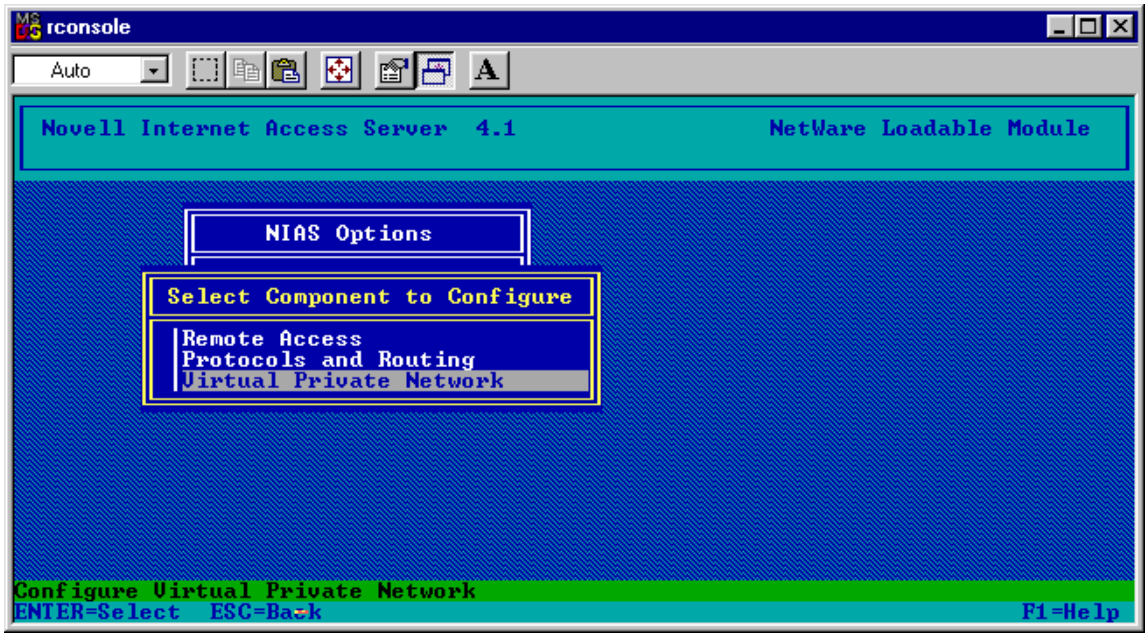
You must set up at least one Master VPN server for either Client-to-Site or Site-to-Site VPN.

Configuration Tasks at the Server Console

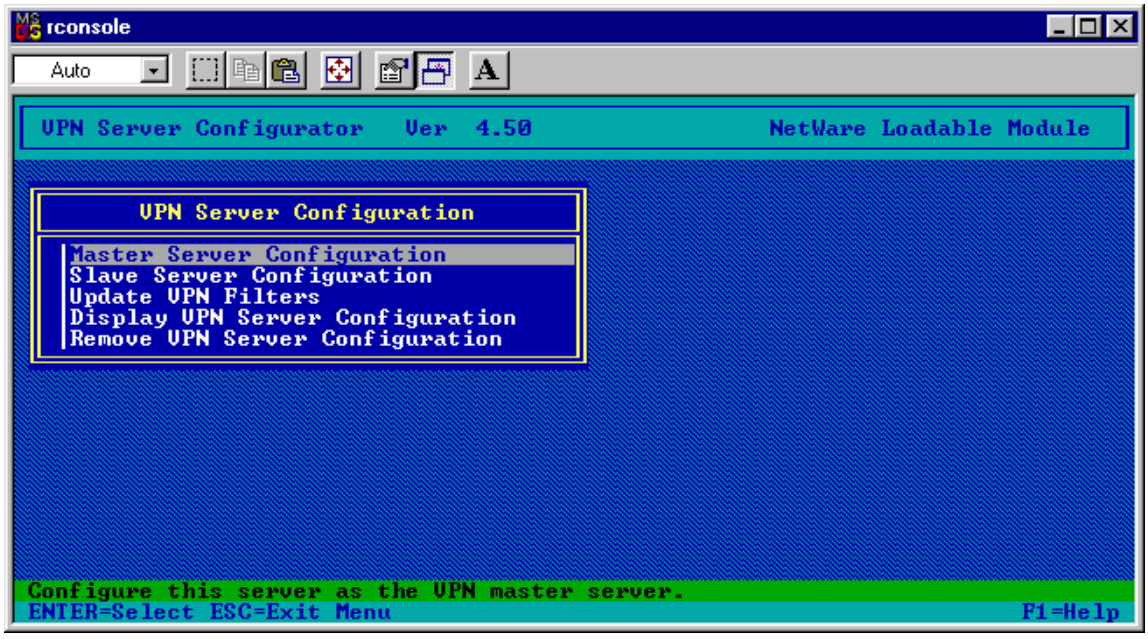
Start by going to the BorderManager server console and loading the NIASCFG utility. (It serves mainly as a menu to launch other configuration utilities, and you can also skip to loading the VPNCFG utility, which does the actual VPN configuration).



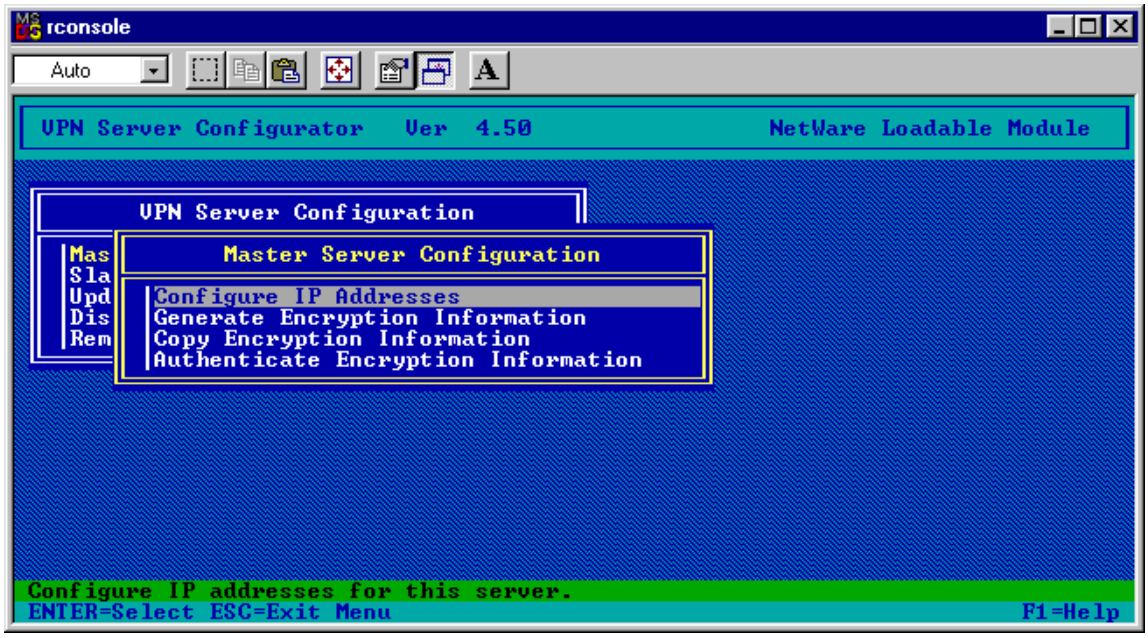
Select the **Configure NIAS** option.



Select the **Virtual Private Network** option. (At this point, NIASCFG should load the VPNCFG module).



If you are setting up the first server for either Client-to-Site or Site-to-Site you must select Master Server Configuration to set up a Master VPN Server. Select **Master Server Configuration** now.



You must first enter IP addressing information. It is a good idea to discuss VPN IP addressing design considerations.

VPN IP and IPX Addressing Design Considerations

A BorderManager VPN uses a virtual IP network and a virtual IPX network in order to properly route data. One key to understanding VPN functionality for configuration and troubleshooting is to realize that the whole service is intimately tied to routing considerations. VPN stands for Virtual Private Network, and this means that VPN segments are actual network segments, from a routing point of view. A VPN segment, whether IPX or IP, must have a unique network address.

The VPN segments must each have unique IPX and IP network numbers not already used anywhere else in your network. If you are joining two remote segments together with a Site-to-Site VPN, the network segments on each end must also be unique. You cannot, for instance, have a network of 192.168.10.0 on one site, and a network of 192.168.10.0 on another site and link them together (with a routed link, like BorderManager's VPN. You could theoretically bridge them together, but not through BorderManager). Same with IPX – you cannot have a network number of BADCAFE on each end of a routed link (like a VPN link); the network numbers must be different. The VPN segments joining the remote sites together, or used for Client-to-Site VPN must also not be in use anywhere else on your LAN.

One example of a Site-to-Site VPN connection would be to have a remote office (IPX network BADCAFE and IP network 192.168.2.0) and a central office (IPX network ABBA, IP Network 192.168.1.0) with a VPN connection between them (IPX network DEADBEEF, IP network 192.168.99.0). With unique addressing, packets can be routed from the main site to the remote side over the intervening VPN network. How do the packets know how to get from one network to the other, and use the VPN segment to do it? Because the VPN segment will show up in the routing tables, and it will show up as the lowest cost route to the other network segment.

It is key that you assign **unique** IP and IPX network numbers to the VPN segments!

Now, a peculiarity of a BorderManager VPN (Site-to-Site) is that it only supports up to 254 nodes, and as such it wants a class C IP address. BorderManager 3.x will allow you to use any IP network number you want, and it will allow you to enter non-Class C subnet masks for the VPN tunnel – but **DON'T DO IT**! Use a Class C network number and subnet mask for the VPN TUNNEL network, and **for best results, use one of the 255 available private networks in the 192.168.0.0 to 192.168.254 range**. Setting the network number is done indirectly by setting the VPN tunnel IP address of

each VPN server. Naturally, all the Site-to-Site VPN servers must be in the same VPN tunnel network in order for them to communicate.

What is a 'tunnel'? The concept is that you are creating a tunnel within a TCP/IP protocol to carry your data packets. The data packets in a Novell VPN tunnel may be either TCP/IP or IPX, or both. To the routers involved on both ends of the tunnel, it looks as if there is a direct low-cost connection between tunnel endpoints, even though there may be many intervening router hops. All routers and devices between the VPN endpoints will only see TCP/IP packets, therefore they will not need to support IPX routing.

Note For the VPN server tunnel IP addressing, use a private Class C IP network number from the range between 192.168.0.0 and 192.168.254.0 for best results, with subnet mask 255.255.255.0. The examples in this book will show 192.168.99.0 in use. Refer to the Site-to-Site VPN scenario earlier in this book.

What are the following?

- Public IP Address
- Public IP Mask
- VPN Tunnel IP Address
- VPN Tunnel IP Mask

A BorderManager VPN server is assumed to be connected to the Internet, though it can be used for private WANs as well. In this book, the author assumes that a typical BorderManager configuration exists – two interfaces, one public and one private. The public interface has a registered, public IP address, while the private interface (or interfaces) can have either public or private IP addresses assigned.

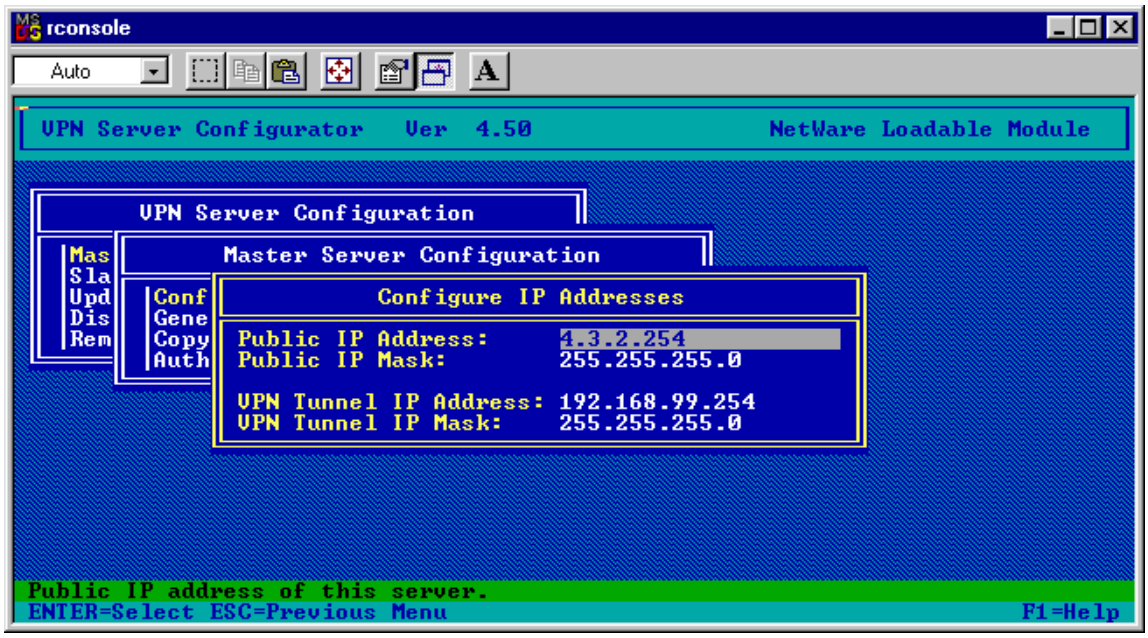
The **Public IP Address** is the public IP binding you have assigned on the public interface of the BorderManager server using INETCFG. This is the main public IP binding (do NOT to try to use a Secondary IP Address for VPN), and it is the IP address of the BorderManager server that can be accessed from the Internet. (If you do not have packet filters loaded, you must be able to PING this IP address from the Internet). The **Public IP Mask** is the subnet mask assigned in INETCFG to the public IP address.

The **VPN Tunnel IP Address** is the IP address that this BorderManager server will use inside the VPN segment. It MUST be unique. It MUST NOT be in a network segment assigned somewhere else on the LAN! It MUST be in the same network segment as other BorderManager VPN Site-to-Site servers you want to have in the same Site-to-Site VPN. A common mistake is to try

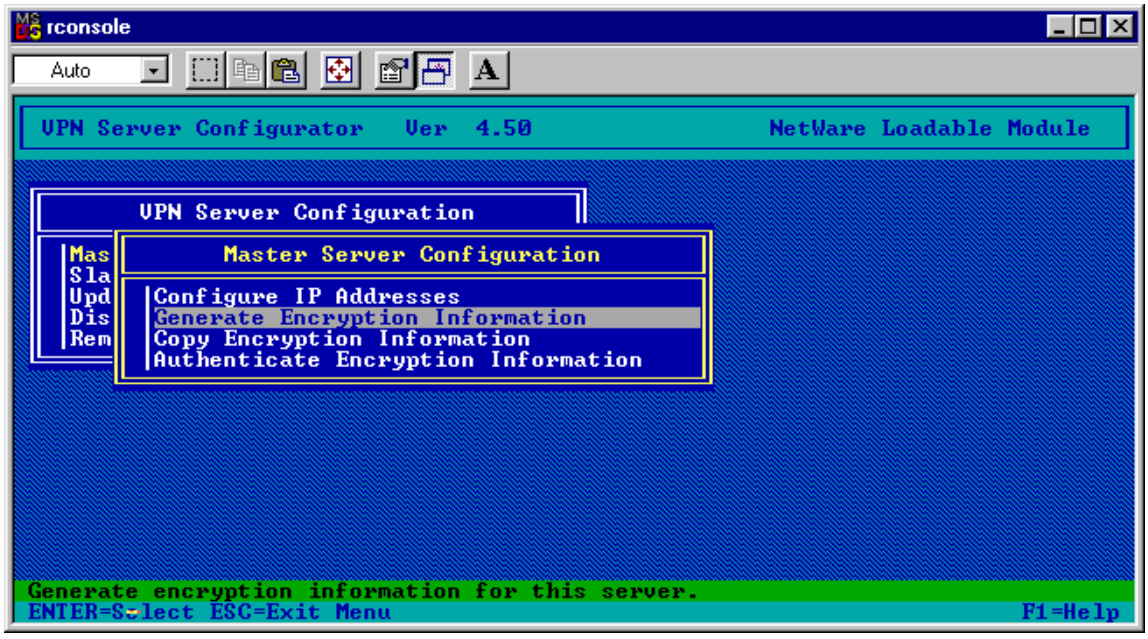
to assign the same IP address as the VPN tunnel IP address as either the public IP address or private IP address of the BorderManager server. The **VPN Tunnel IP Mask** is the subnet mask for the VPN Tunnel IP Address. I highly recommend using a 192.168.x.x IP address for the VPN Tunnel IP Address, and 255.255.255.0 as the VPN Tunnel IP Mask.

CAUTION *Because the VPN Tunnel uses an IP network address to function, you should be careful not to select a network address that might be in use on your VPN clients' home networks. For instance, Linksys routers tend to default to 192.168.1.x and Netgear routers tend to default to 192.168.0.x addresses. If you configure your VPN tunnel to use a 192.168.0.x or 192.168.1.x address, VPN clients in a home network using those address ranges will not be able to make use of the VPN. Avoid using any 192.168.x.x address between the ranges 192.168.0.x and 192.168.10.x.*

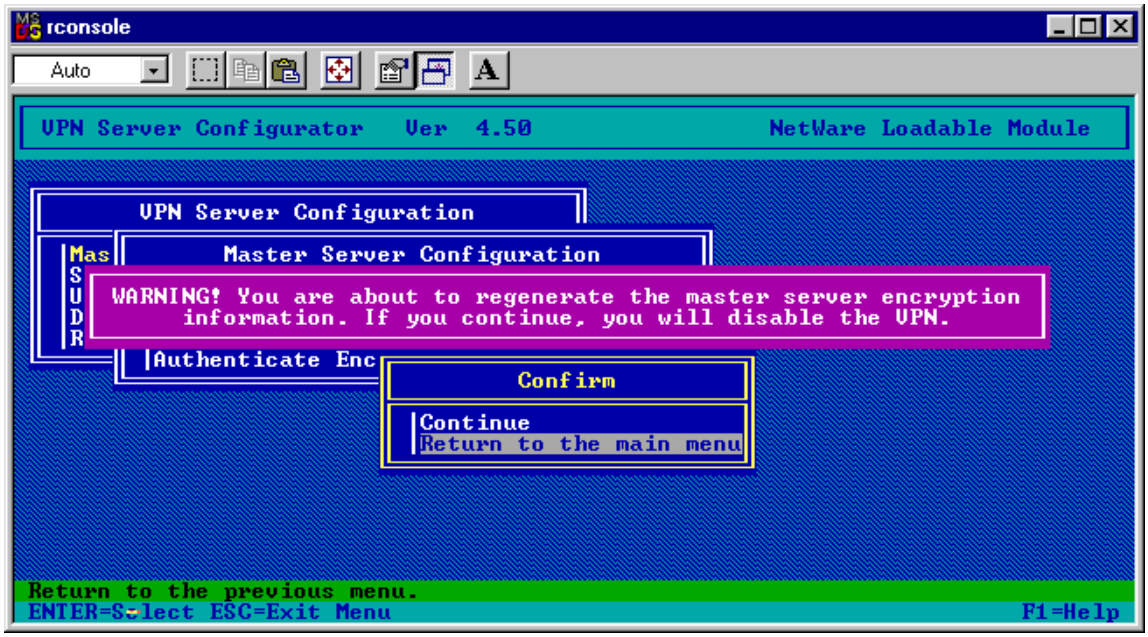
Setting Up The Master VPN Server, Continued



Enter the **public IP address** and **subnet mask**, and the **VPN tunnel IP address** and **subnet mask**, and then press **Escape**. You should be returned to the main VPNCFG menu.

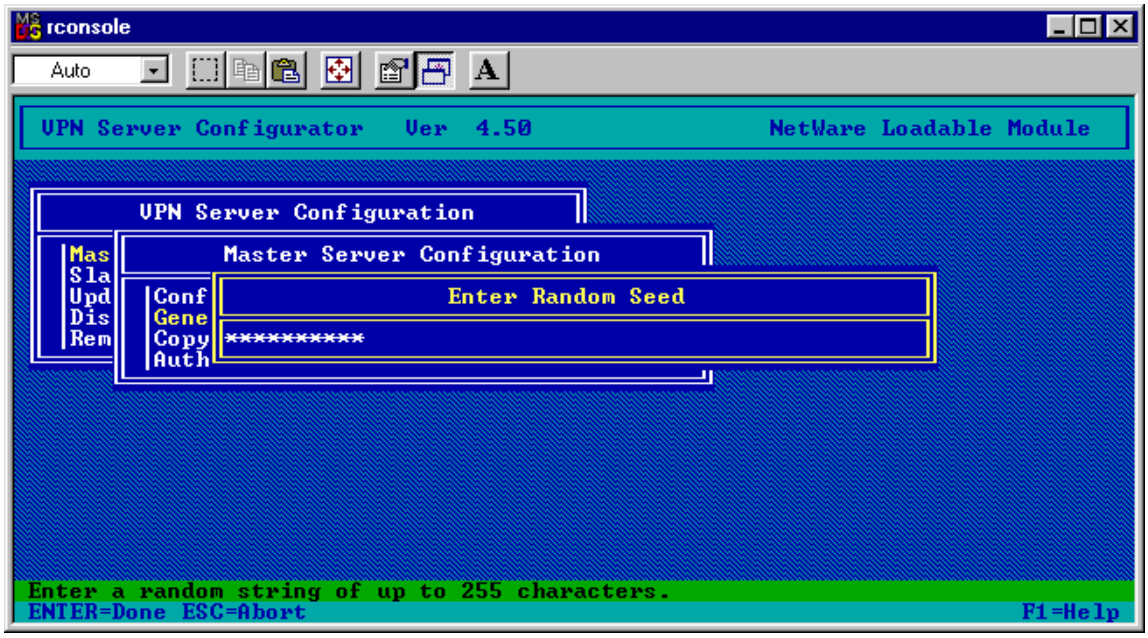


Now select **Generate Encryption Information** from the VPNCFG menu.

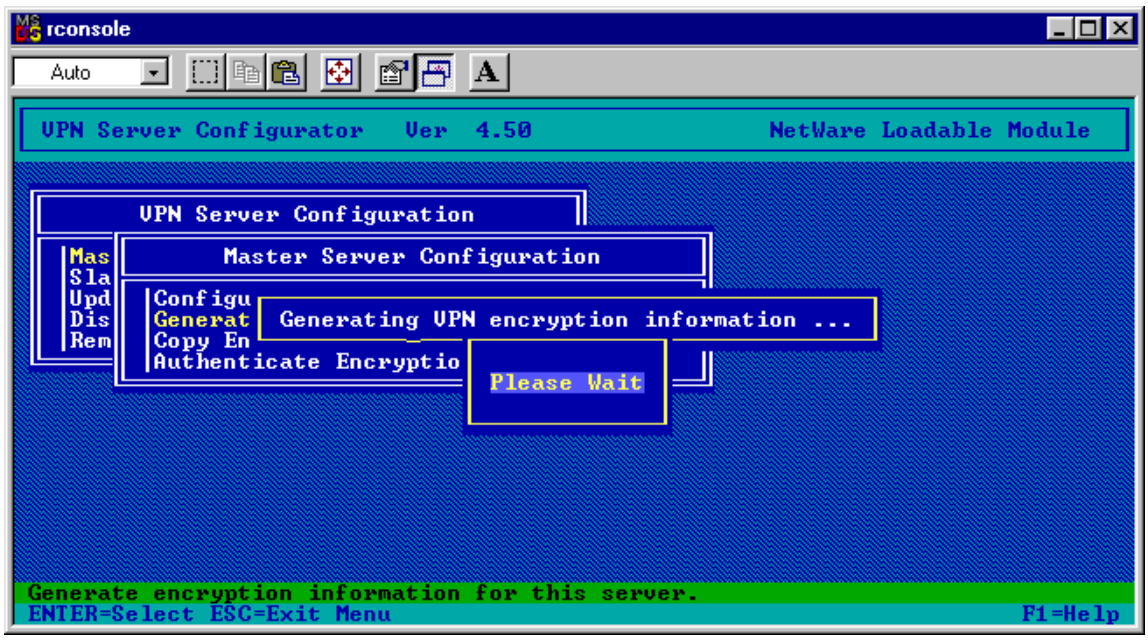


If you already had the server set up as a Master VPN server, regenerating the master server encryption information will disable the VPN, and you will receive a warning message, as shown in the example above. This is because the VPN is tied to the public and private keys which are generated at this point, and changing the encryption information will cause the keys to change, thus disabling ALL of the VPN servers, since they all rely on the Master VPN server to set up the key exchange.

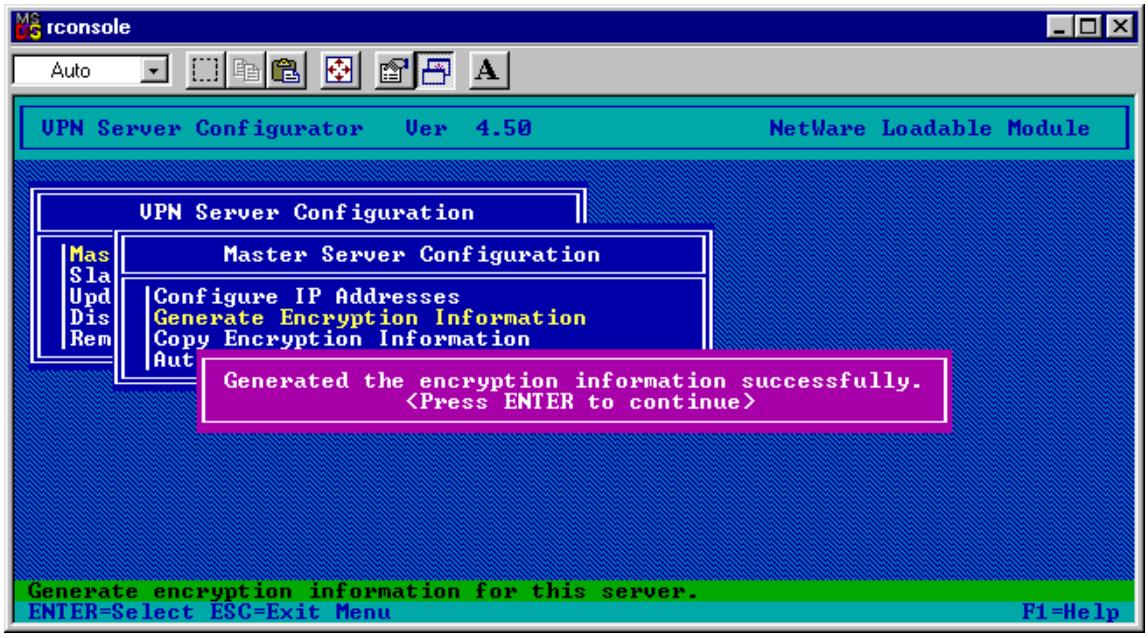
Otherwise, you will not get an error message, and you can enter a random seed to start the key generation.



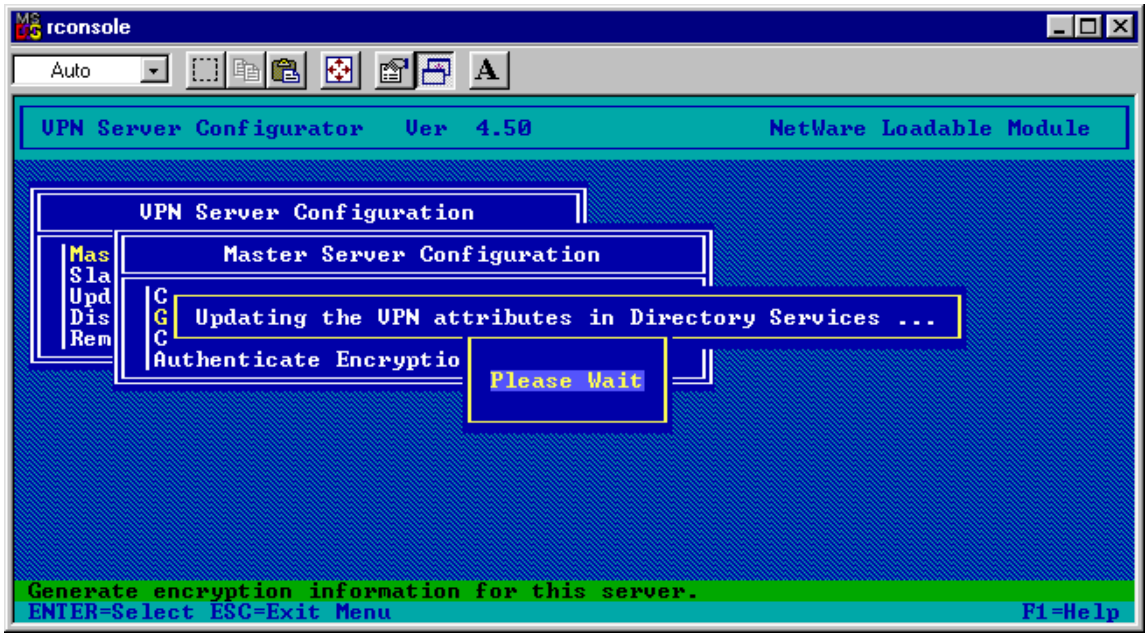
In order to generate the public and private keys needed to establish an encrypted connection, a random seed is used as a starting point. Rather than rely on some possibly non-random algorithm to generate a seed for you, Novell prefers than you enter your own random seed. Simply type in some random collection of numbers and letters to start the process, and press the **Enter** key.



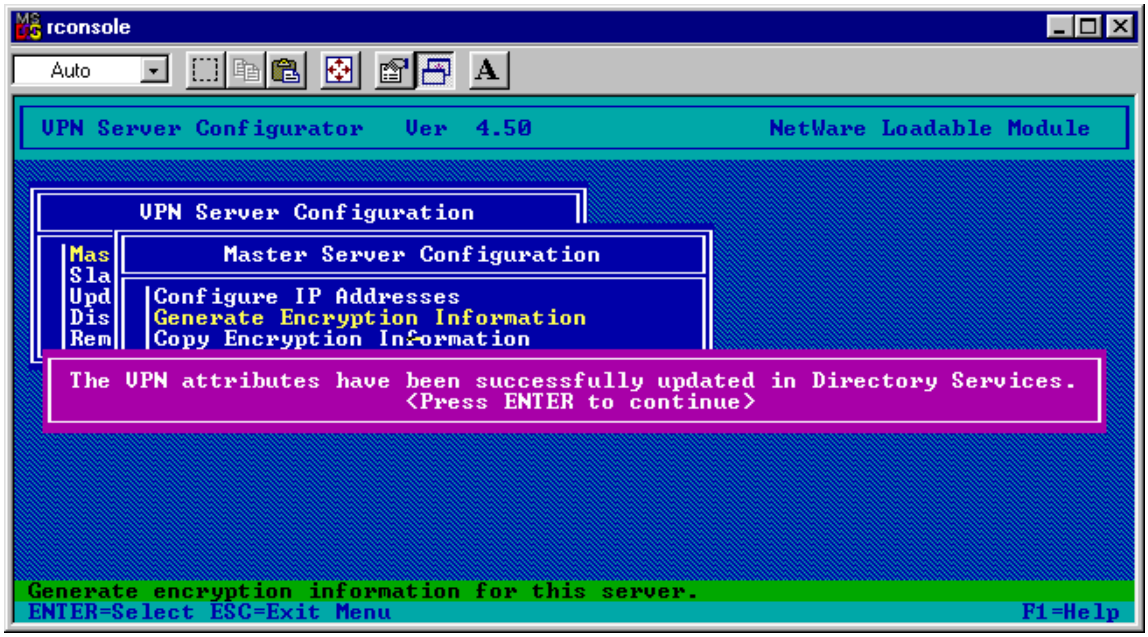
Generating VPN encryption information can be quite a lengthy process. (The author has heard this process taking as long as 15 minutes). Be patient.



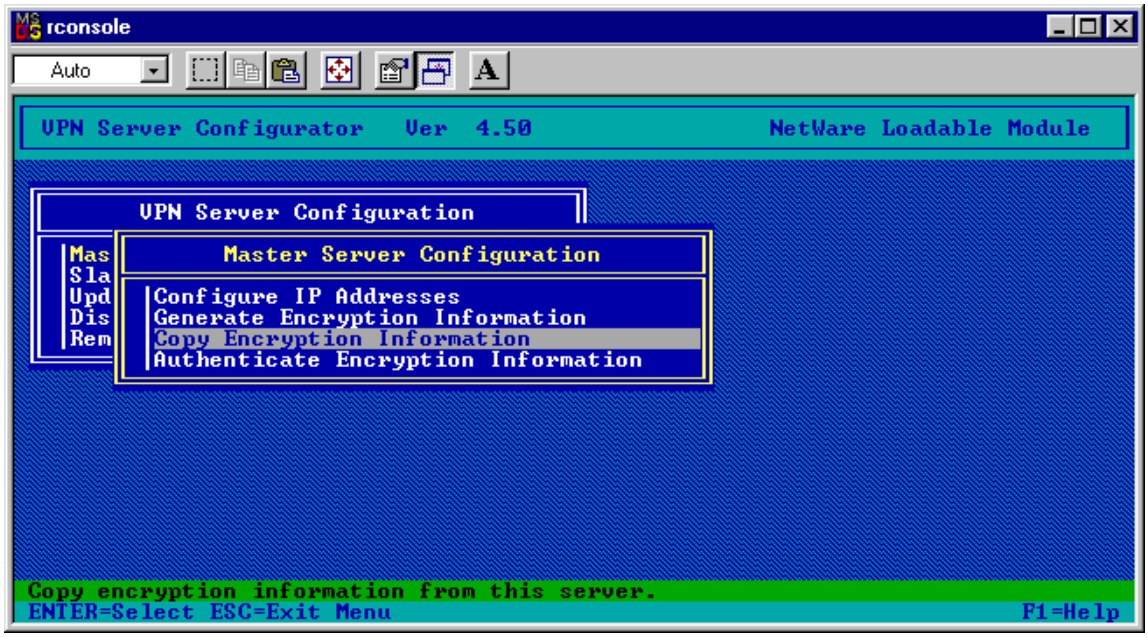
Once the encryption information has been generated successfully, you should see a message indicating that you can press **Enter** to continue.



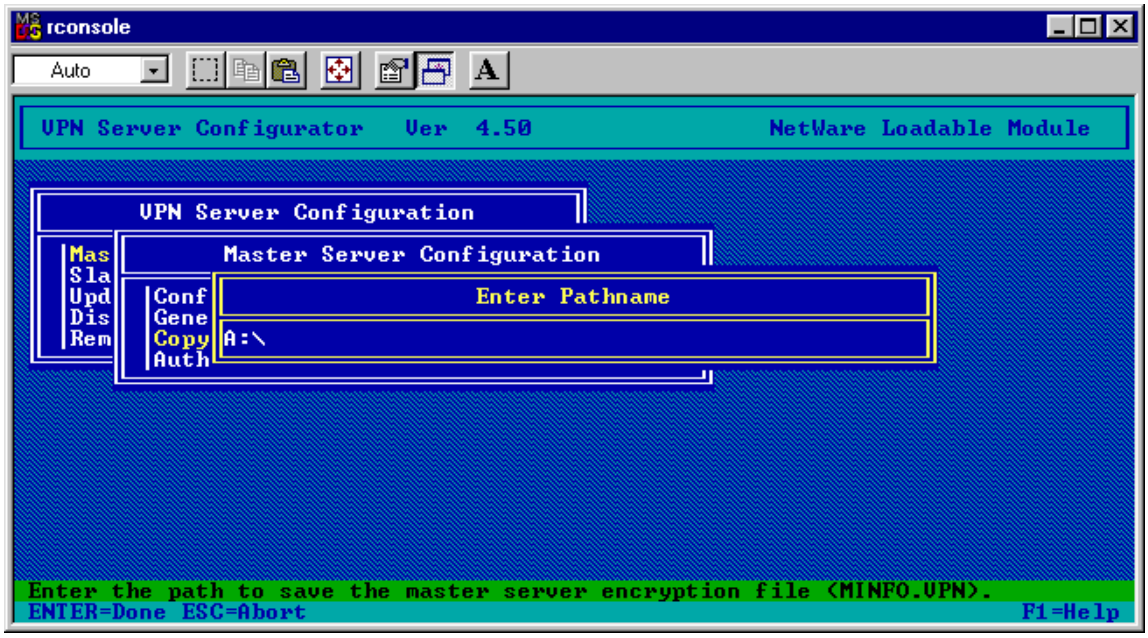
Next, the new encryption attributes are updated in NDS.



Once the information has been successfully updated into NDS (as an attribute of the server object), you should see a message stating that you can press **Enter** to continue. You should then be returned to the VPNCFG main menu.



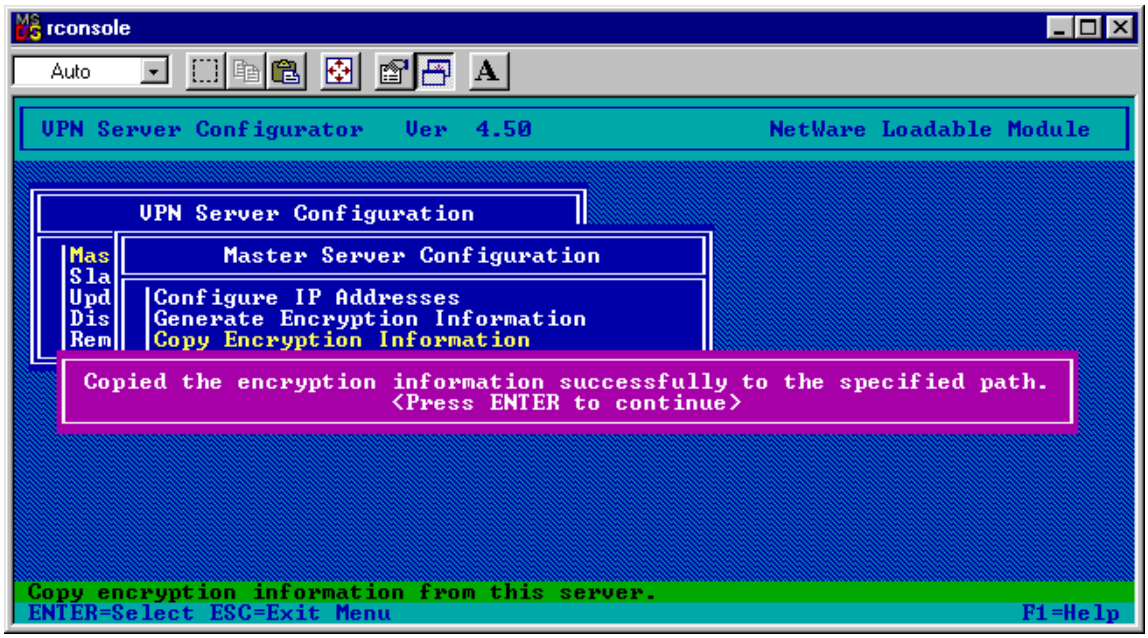
Once the encryption information has been generated, you need to copy the data to a file that is needed at a later step. Select the **Copy Encryption Information** menu item.



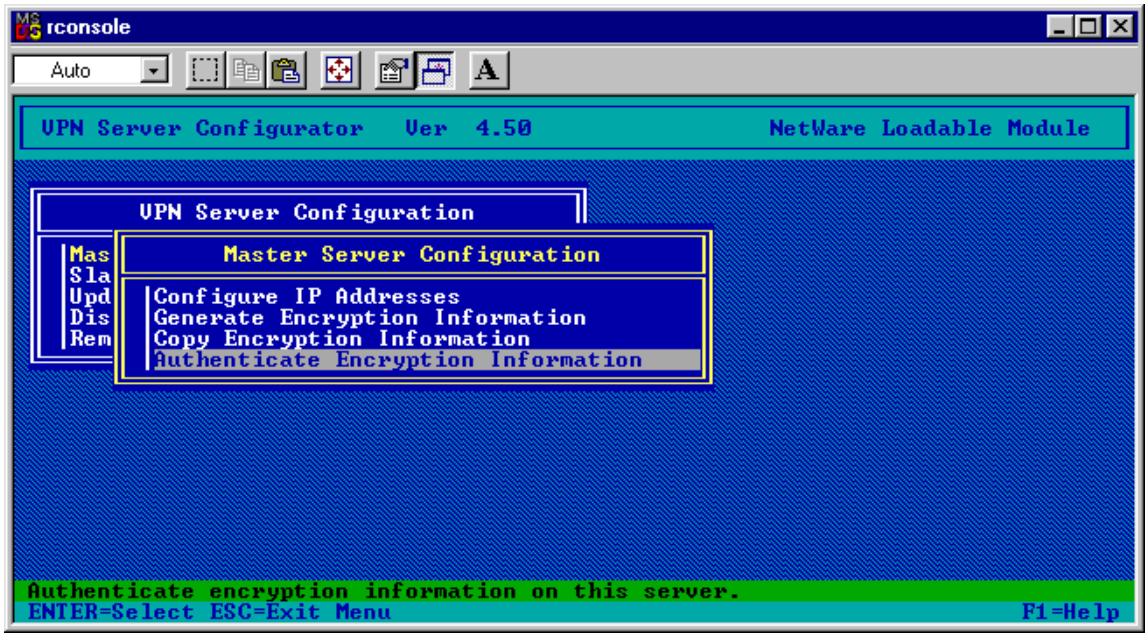
You will be prompted to save the data to the **A:** drive, but the file name is NOT yours to choose. (Note the text at the bottom of the screen). If you are configuring a Master VPN server, the file name will be MINFO.VPN. If you are configuring a Slave VPN server, the suggested file name will be SINFO.VPN, but you will be allowed to enter a different name since you may be setting up multiple VPN slave servers and need to identify each one separately.

Note In order to set up Site-to-Site VPN slave servers, you will be required to supply the MINFO.VPN file at the slave server.

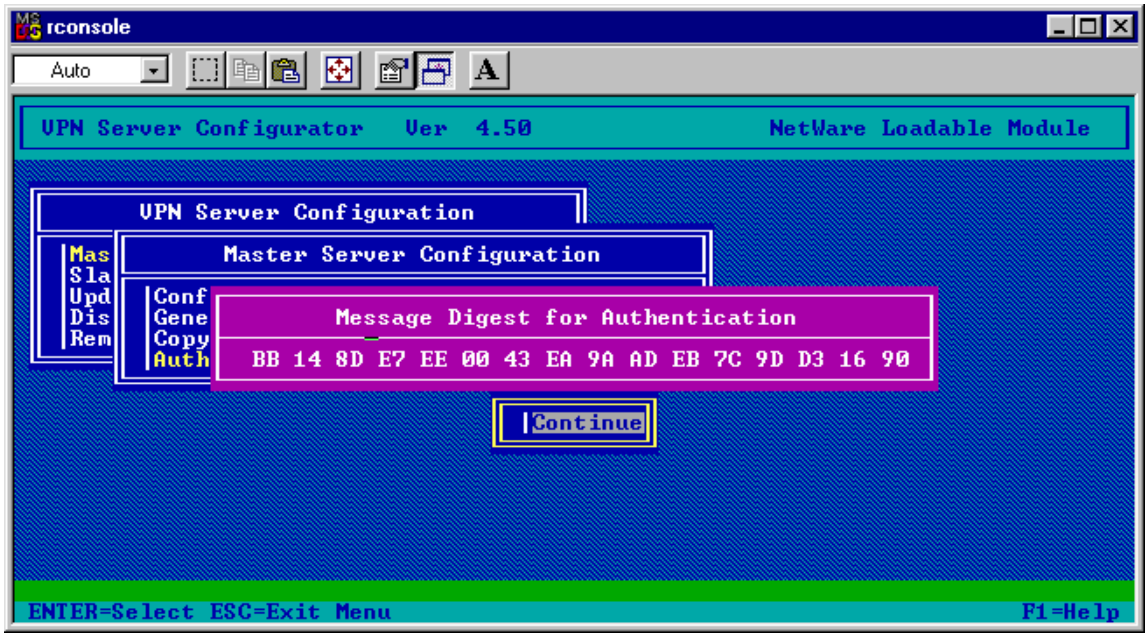
You can also save the file to a VOLUME:\DIRECTORY, such as SYS:\SYSTEM if you like.



Once you have saved the data, you should get a success message indicating that you can press Enter to continue. You should be returned to the VPNCFG main menu.



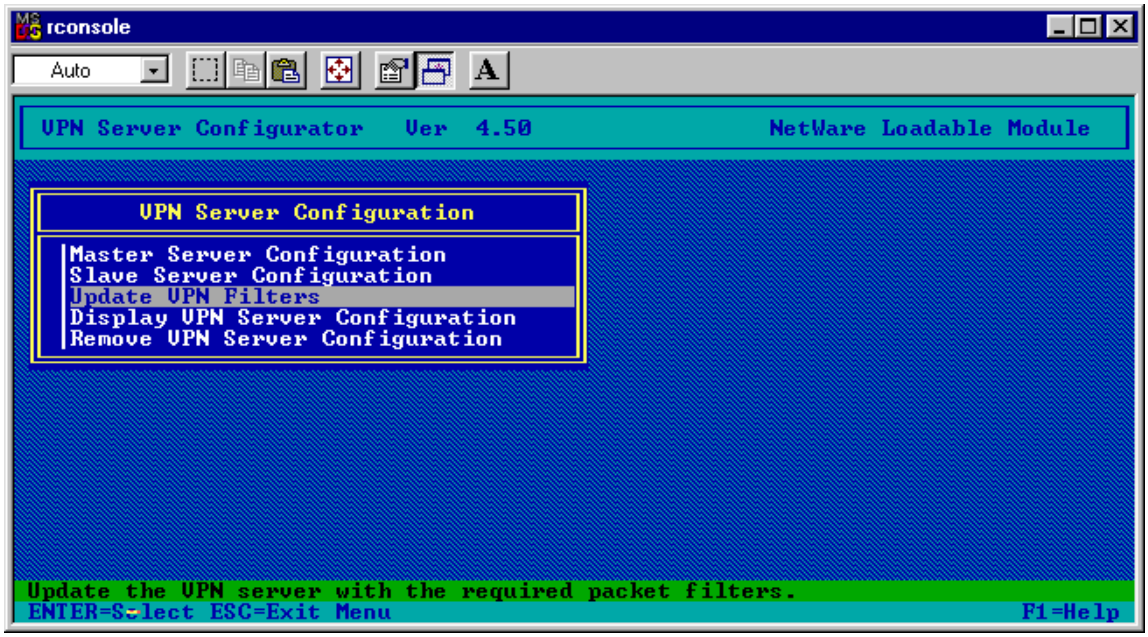
From the VPNCFG main menu, you can select **Authenticate Encryption Information** to see the message digest information. Especially if you are configuring multiple VPN servers, you should check the message digest information to be sure you are configuring the servers you are expecting.



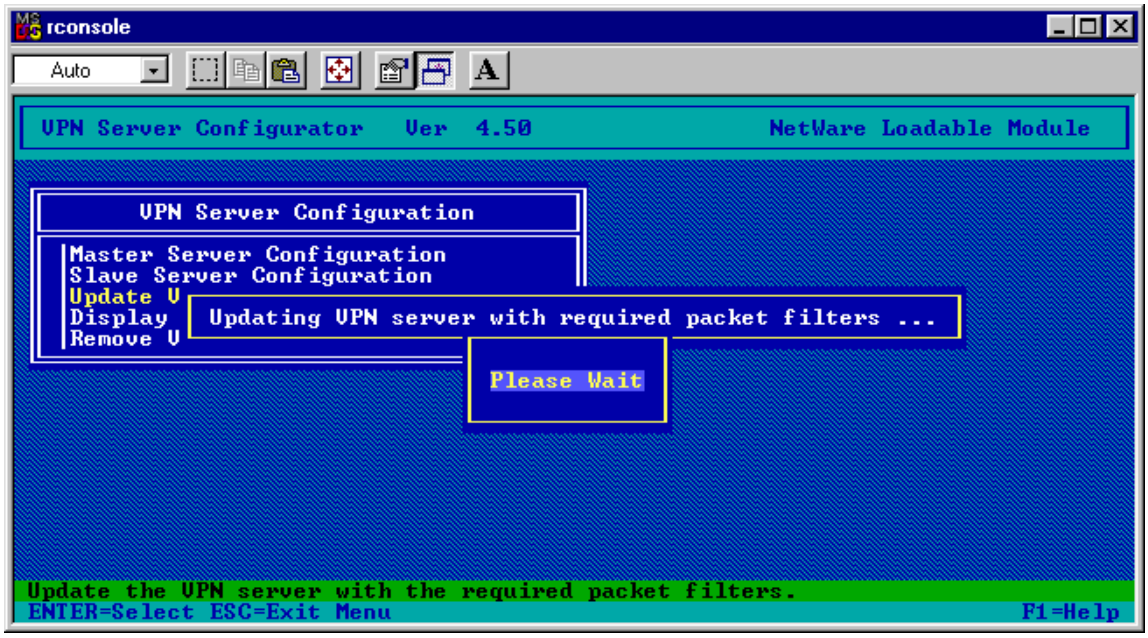
The message digest will be unique for the encryption information generated. The security-conscious administrator will record this information on the floppy disk holding the MINFO.VPN file as well

as on paper so that it may later be checked when using the MINFO.VPN file.

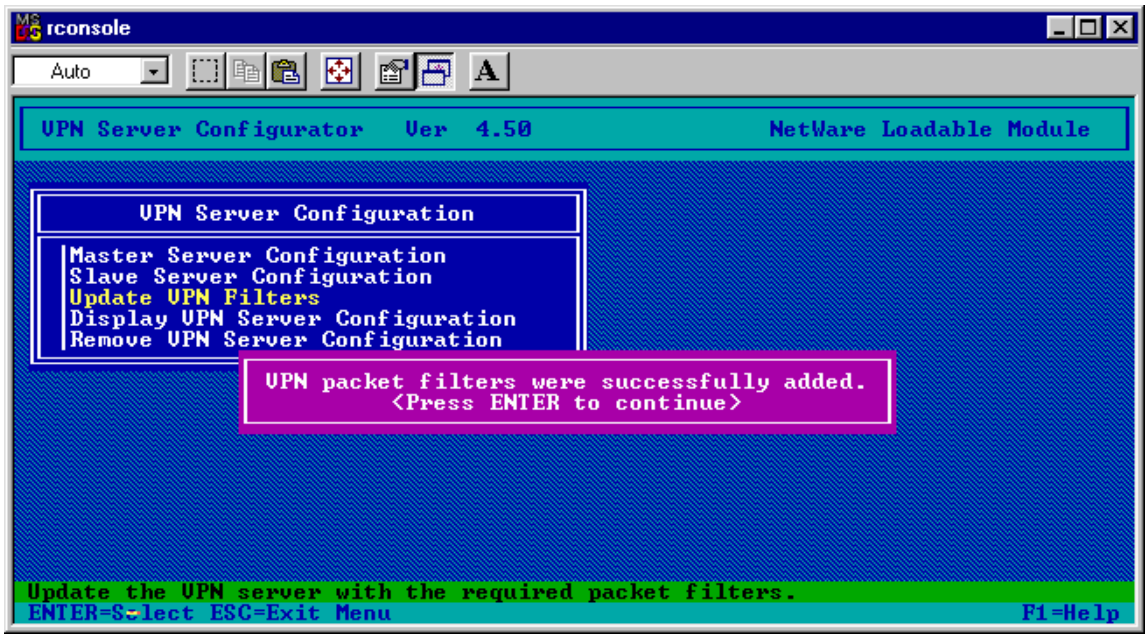
Press **Continue** to return to the VPNCFG main menu.



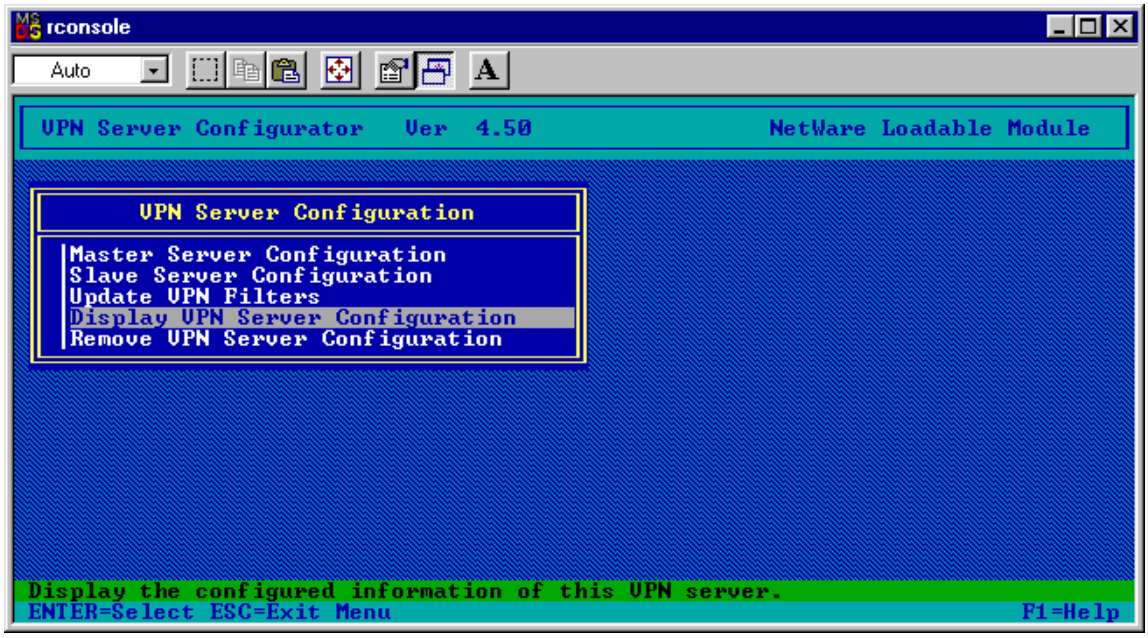
If you have already loaded BRDCFG to set up the default packet filters and exceptions, you should not have to update the VPN packet filters. However, it does not take long to do, and is good insurance that the VPN packet filters have been updated. You should select the **Update VPN Filters** option at this time.



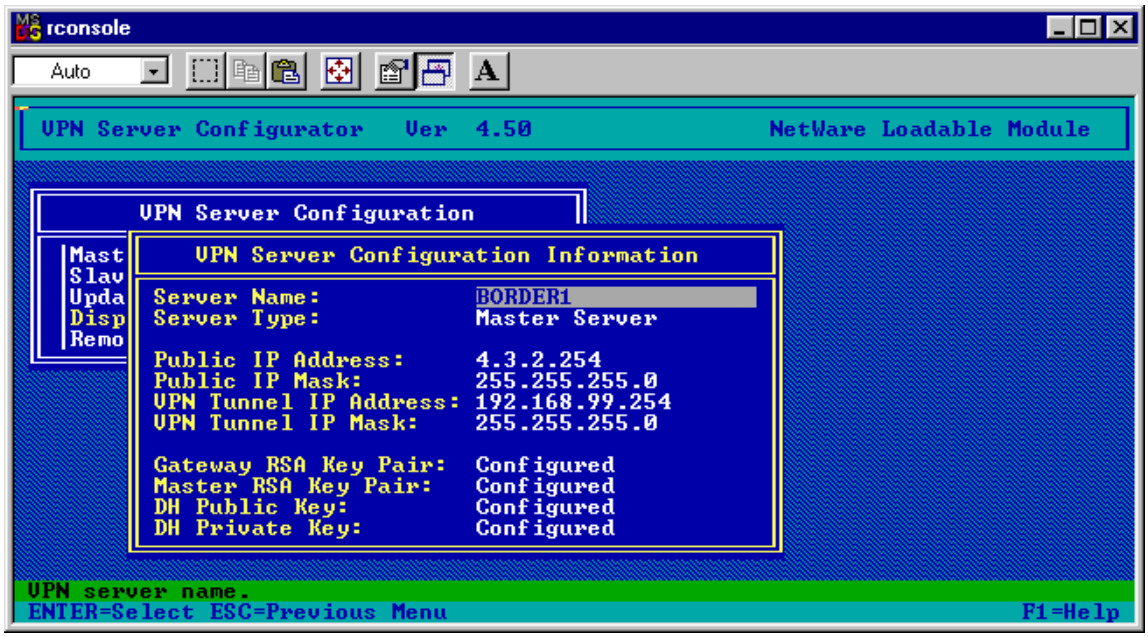
You should see a message indicating that packet filters are being updated.



Once the packet filters have been successfully updated, you should see a message indicating to press **Enter** to continue. You should then be returned to the VPNCFG main menu.



From the VPNCFG main menu, you should now select the **Display VPN Server Configuration** option to review your settings.



If you see any errors on the VPN Server Configuration Information menu, you will have to repeat parts of the configuration process in order to correct the errors.

Note that the server name itself is part of the configuration information. Changing the server name will invalidate the encryption information and cause Site-to-Site VPN to fail, requiring reconfiguration of the VPN.

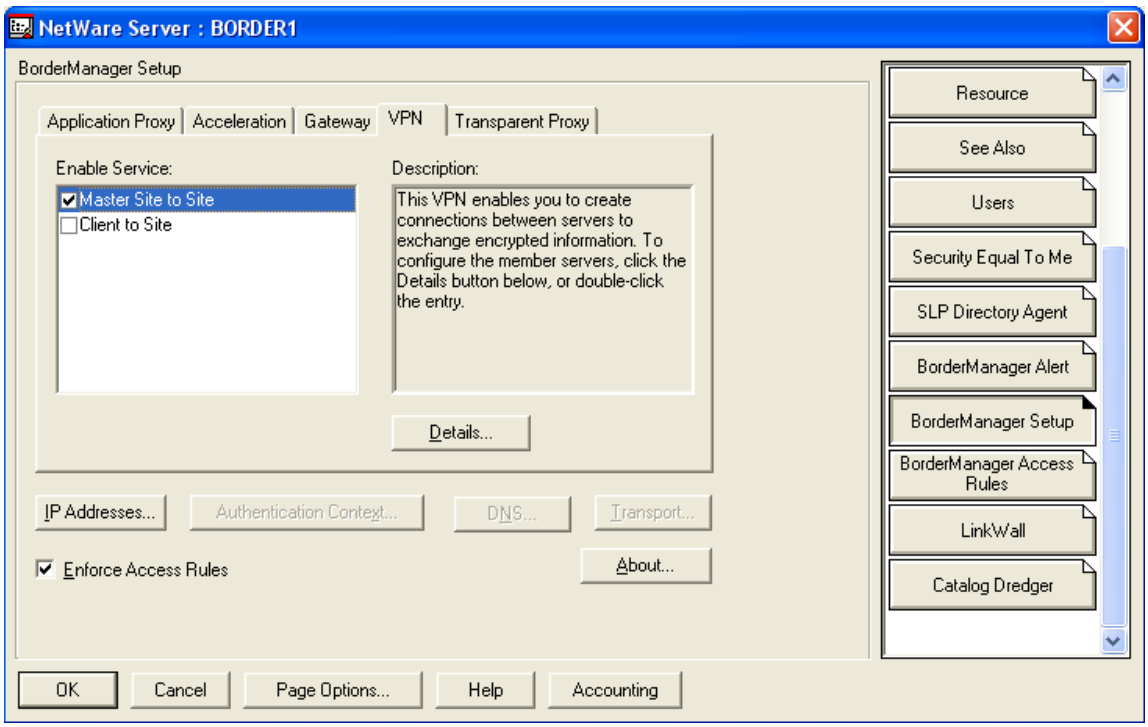
Press the **Escape** key repeatedly to exit the VPNCFG utility.

If you launched VPNCFG manually, you should be returned to the console prompt. If you launched VPNCFG from NIASCFG, you should be returned to the NIASCFG main menu. Press the Escape key repeatedly to exit NIASCFG.

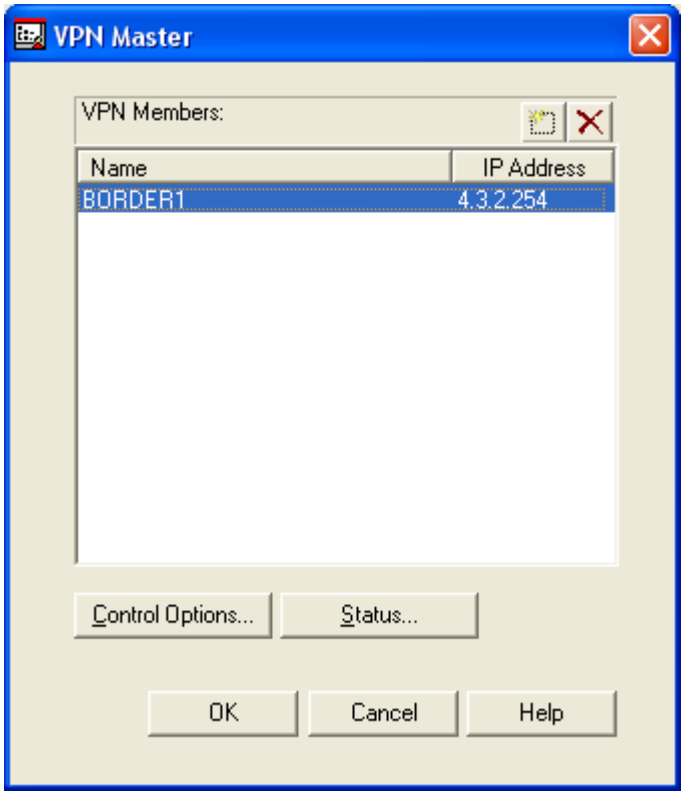
You must now continue the VPN configuration using NWADMN32.EXE from the BorderManager server.

Configuring the VPN Master Server in NWADMN32

Launch NWADMN32.EXE, select the BorderManager server to be configured as a master VPN server, and select the **BorderManager Setup** tab.



Select the **VPN** tab. The server should already have the Master Site to Site box checked because of the configuration done previously in VPNCFG. Select the **Details** button for Master Site to Site.

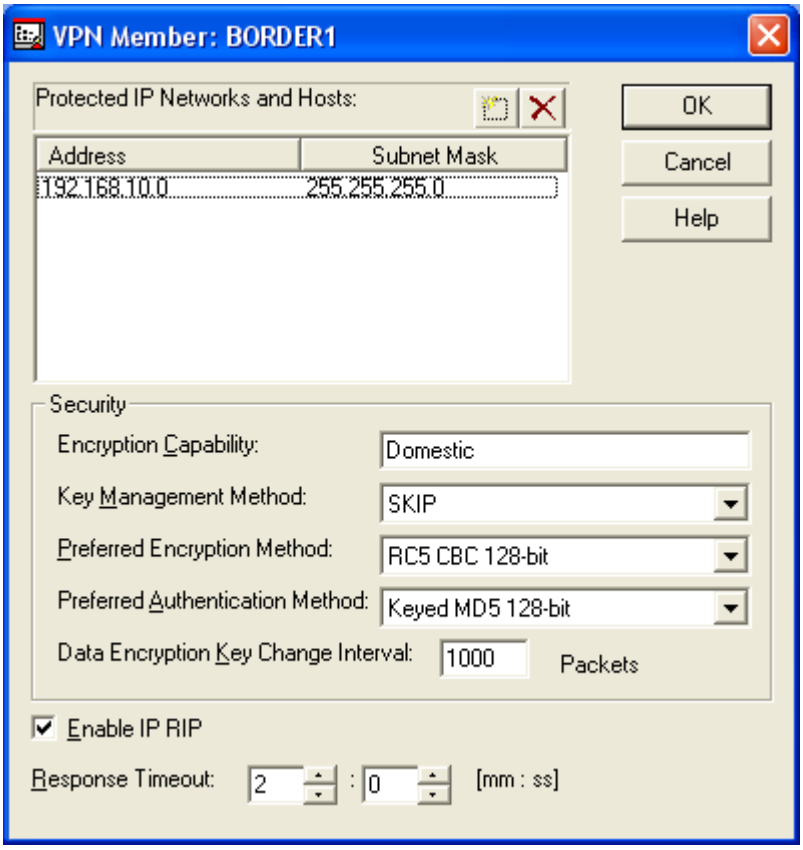


You should see the BorderManager server already set up as a VPN member with the public IP address showing. Control Options can be configured now or later, or left at the defaults.

You can enter three important menus from this screen:

17. Double-clicking on a **server** listed here allows you to configure settings for that server.
18. Selecting **Control Options** takes you to a menu used to configure global VPN options.
19. Selecting **Status** allows you to synchronize settings across the servers, view audit logs, or view real-time activity.

Double-click on the **server name** to configure protected networks.

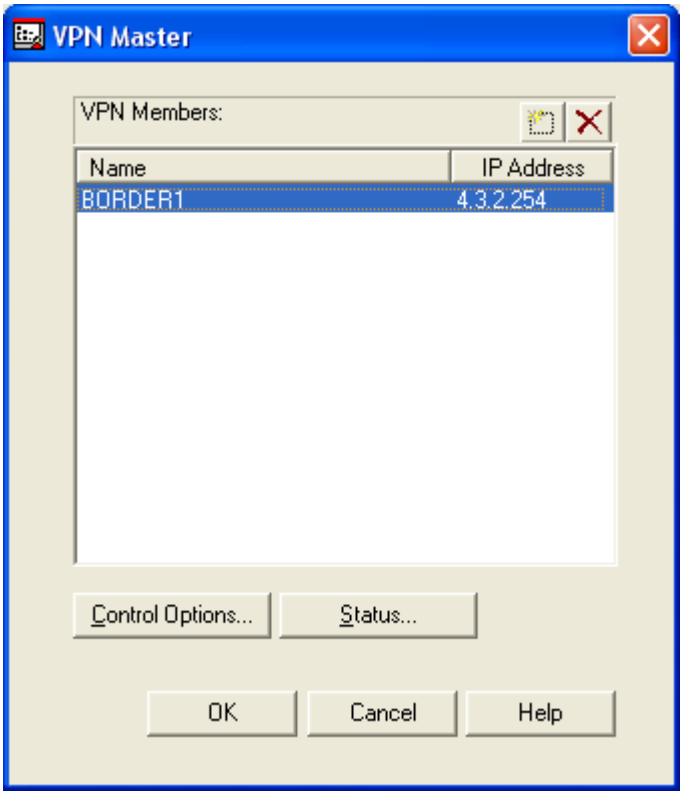


By default, no networks are protected, and you must add in network or host addresses. If you do not add anything to the list of Protected IP Networks and Hosts, slave VPN servers will not be able to send packets to the VPN server's internal network.

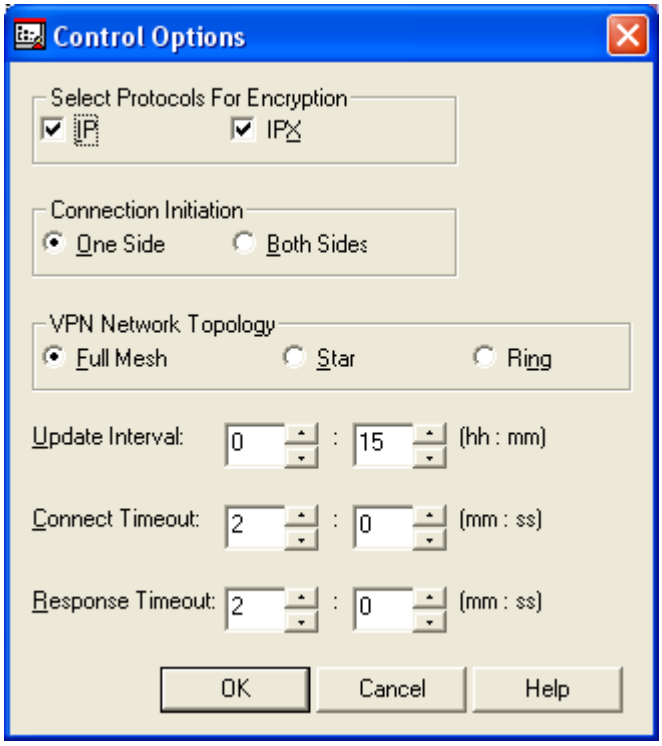
Do not add any protected networks or hosts that are not physically behind the VPN server being configured. The settings here are used to create static routes on the OTHER VPN servers.

In the example above, the subnet of the network behind the VPN server has been added as a protected network. The other parameters have been left at default values. (Encryption capability will depend on the encryption level of the version of TCPIP.NLM installed).

Note the Enable IP RIP setting, which is checked. This (default) setting allows the server's protected networks to be automatically pushed to all other VPN servers. With this option selected, if you add another protected network to a VPN server, and then Synchronize All (shown later), all other VPN servers will be automatically configured with a static route to the protected networks, with next hop IP addresses set to the appropriate VPN tunnel IP addresses.



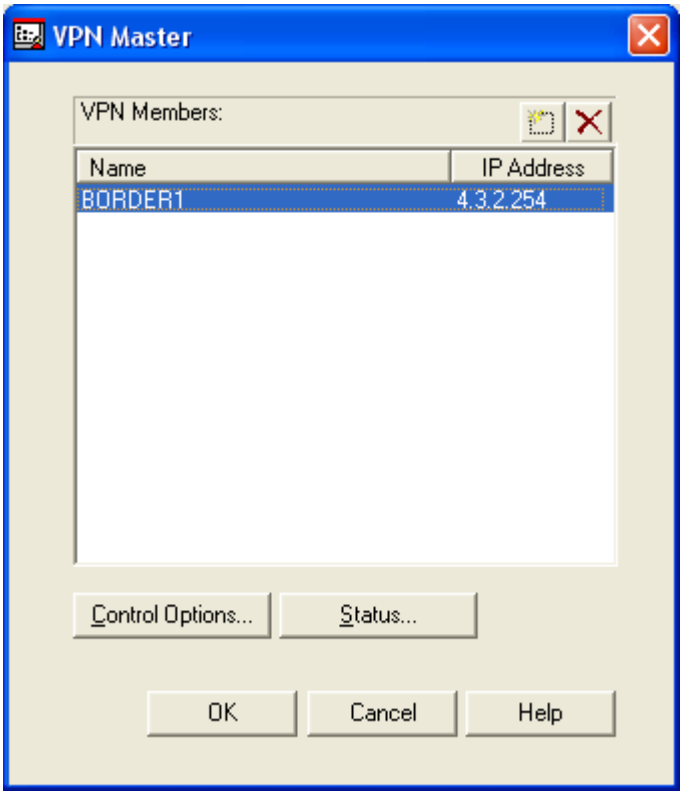
Select **Control Options** to view the default settings.



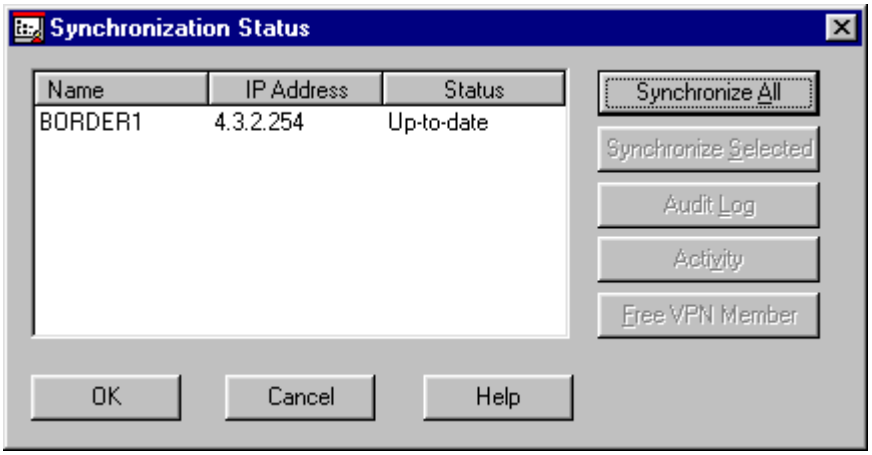
It is best to specify that **the Connection Initiation** is **One Side**. Press **OK** to return to the Master Site to Site VPN Details menu, and select the **Status** button to view the status of the VPN server.

The Full Mesh topology allows all servers to talk to all other servers directly, and creates the most traffic, but should be the most resistant to server outages.

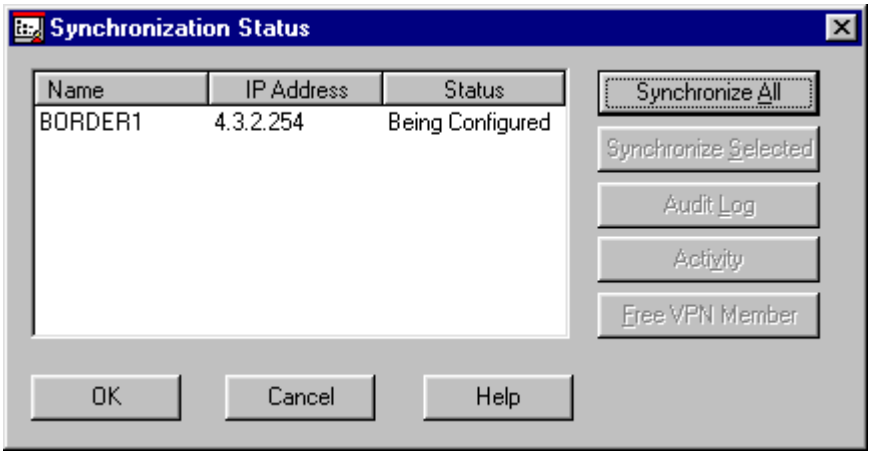
The Star topology has all servers talk only through the master VPN server, and causes the least amount of traffic, but a failure of the master VPN server causes all other servers to lose communications to each other.



Select **Status** to Synchronize settings among servers, to view audit logs, or to see real-time VPN activity.



The status menu should show only one server at this time, though it will show more servers once a site-to-site VPN has been configured. The status of the master VPN server should show **Up-to-date** if all is well. If not, you can try selecting the server from the menu and then pressing the **Synchronize Selected** button (or use the **Synchronize All** button). You can also try using the Reinitialize System command at the BorderManager server console.



During the synchronization phase, the status of the VPN server should show as '**Being Configured**'. If all is well, the status will soon change to '**Up-to-date**'. During the synchronization phase, the server reads the configuration and encryption data from the Master VPN server. If the server being configured is the master VPN server, this process should go quickly and without problems.

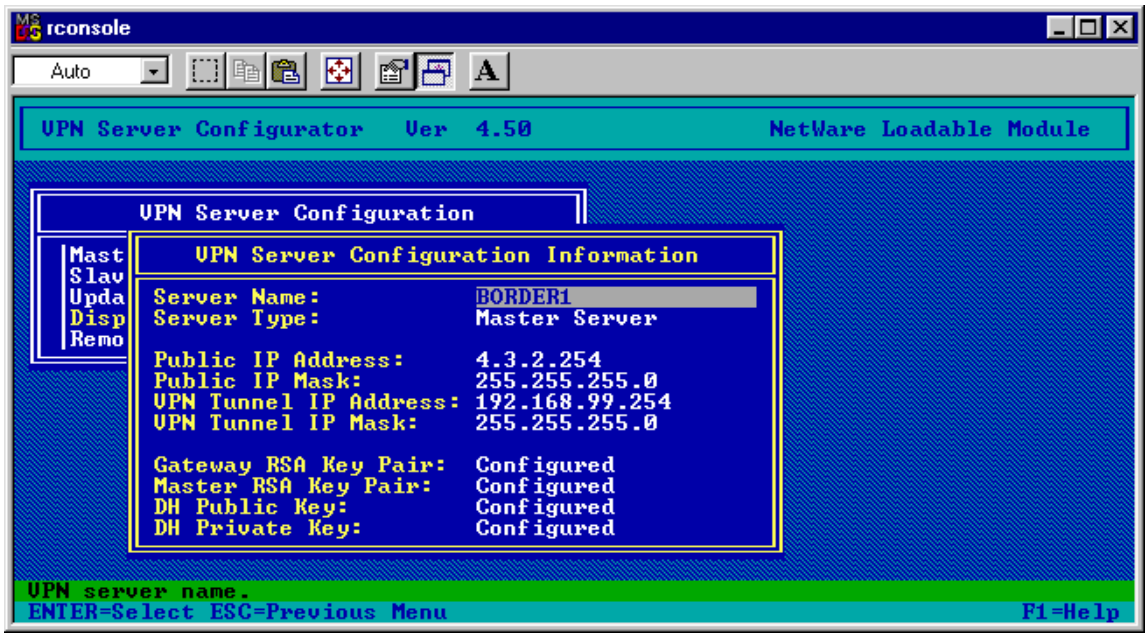
Press **Cancel** to return to the previous menu. Press **Cancel** again to return to the VPN configuration menu.

Adding a Site-to-Site Slave VPN Server – Server Console Procedures

Note Review the section 'Configuring a Master VPN Server' under the section on setting up Client-to-Site VPN for details on getting the first VPN server configured.

BORDER1 has been set up as a master VPN server using virtual IP network 192.168.99.0 with server address 192.168.99.254. VPN configuration is initially done using VPNCFG.NLM at the server, and basic parameters can be changed from there. If the VPN configuration went without error, a LOAD VPMASTER statement should have been added in AUTOEXEC.NCF to start VPN services on BORDER1. If some problem occurred, you may need to manually add the command.

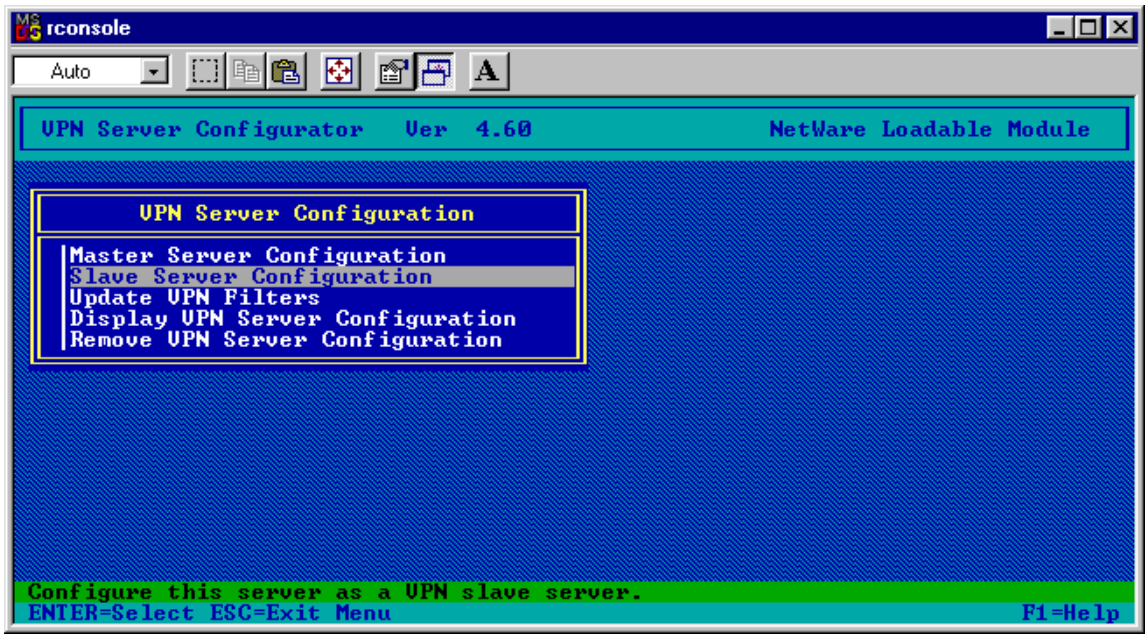
Actually, the VPN connection will start without LOAD VPMASTER due only to the commands in the SYS:\ETC\NETINFO.CFG, but you cannot manage or view the VPN status in NWADMN32 without VPMASTER (or VPSLAVE on a slave VPN server) loaded.



Once the Master VPN server is set up with VPNCFG, you use VPNCFG on the slave server(s) to begin the configuration process.

You will need the master server's MINFO.VPN file for every slave server to be added to the Site-to-Site VPN. Normally you physically have the file on floppy disk and send it to the site with the slave

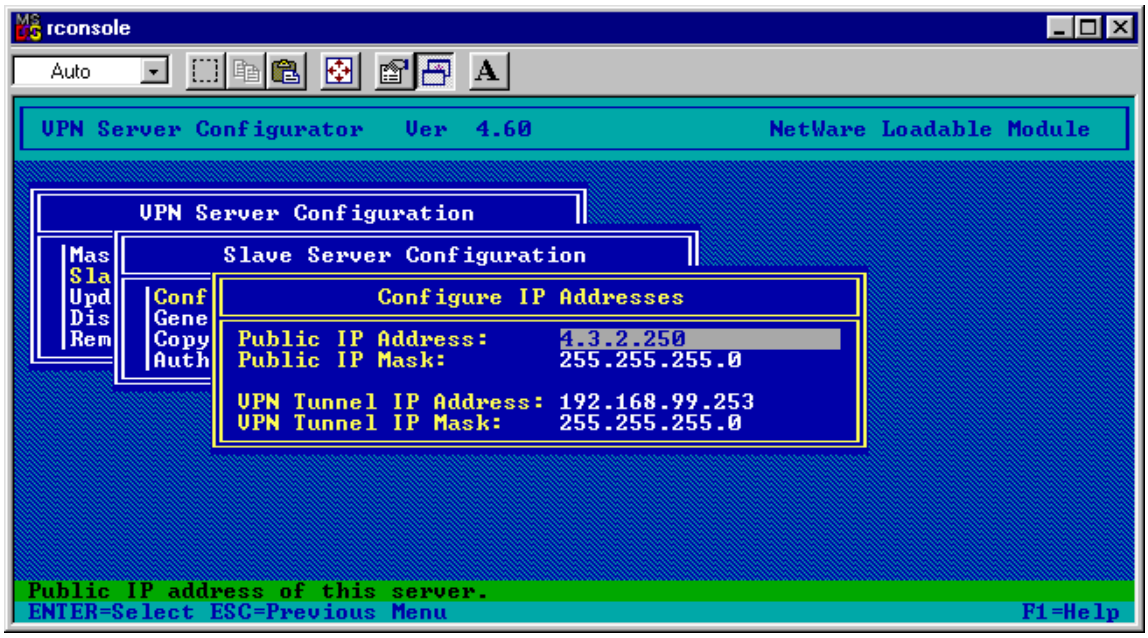
server when the configuration process is begun. You can also email the file, but it must be accessible from the slave server before the VPN connection is available. You will also need the authentication digest string.



At the slave server, you will follow almost all of the same steps as at the master VPN server, with a few important differences.

Start by loading **VPNCFG** at the slave server.

Select **Slave Server Configuration**.



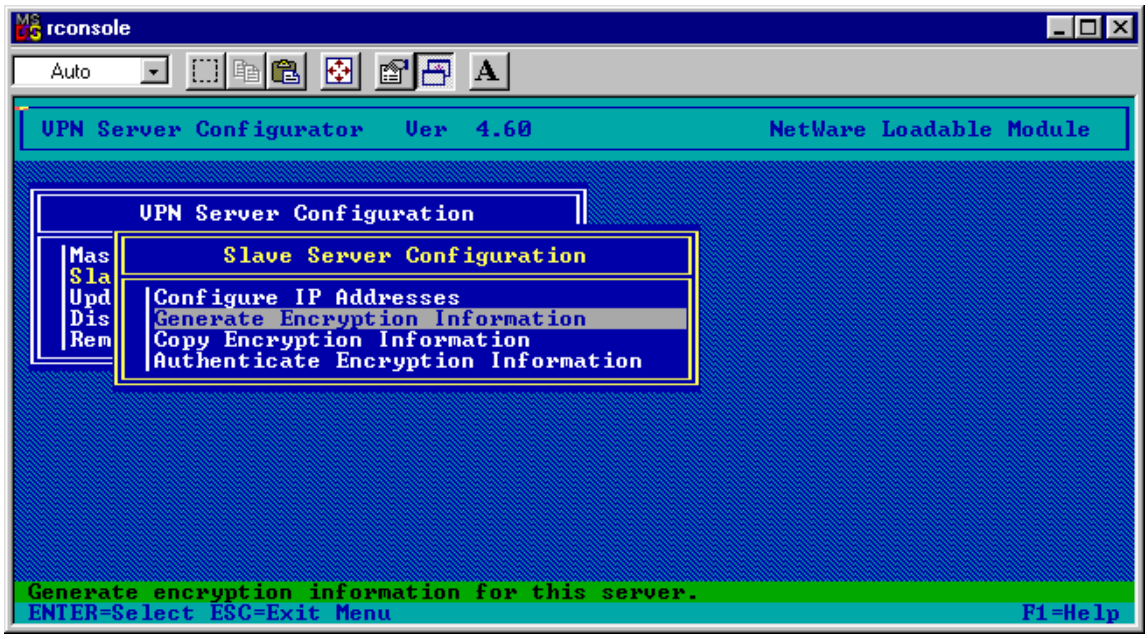
Select **Configure IP Addresses**, and enter IP addressing information.

The **Public IP Address** should be the address assigned to the public interface, and is the address that is accessible from the Internet. This is the IP address binding assigned to the server in INETCFG. The **Public IP Mask** is the subnet mask assigned for the public IP address.

The **VPN Tunnel IP Address** is the IP address of the server within the virtual private network. This IP address must be in the same IP network established for the VPN at the master VPN server. This IP address must be unique, not only within the VPN IP network, but also throughout the LAN and WAN. This IP address should be a class C address and subnet mask for best results. The **VPN Tunnel IP Mask** is the subnet mask for the VPN Tunnel IP Address, and for best results should be a class C subnet mask (255.255.255.0).

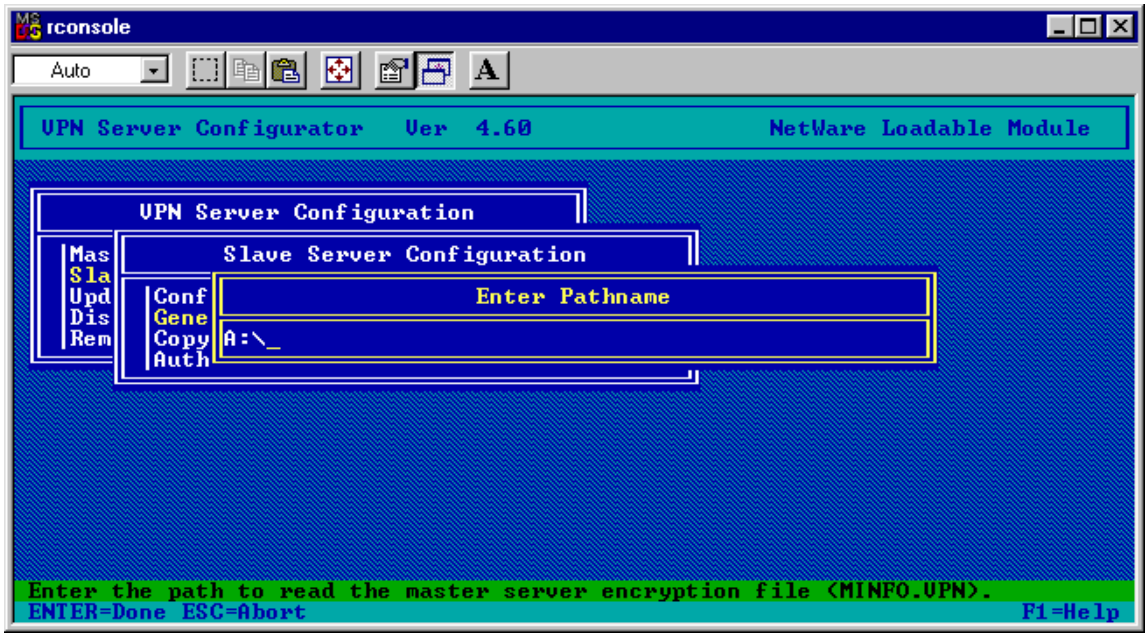
Note See the section in this book on configuring a Master VPN server for more explanation on VPN addressing considerations.

Press the Escape key when done entering slave IP addressing information to return to the VPNCFG Slave Server Configuration menu.



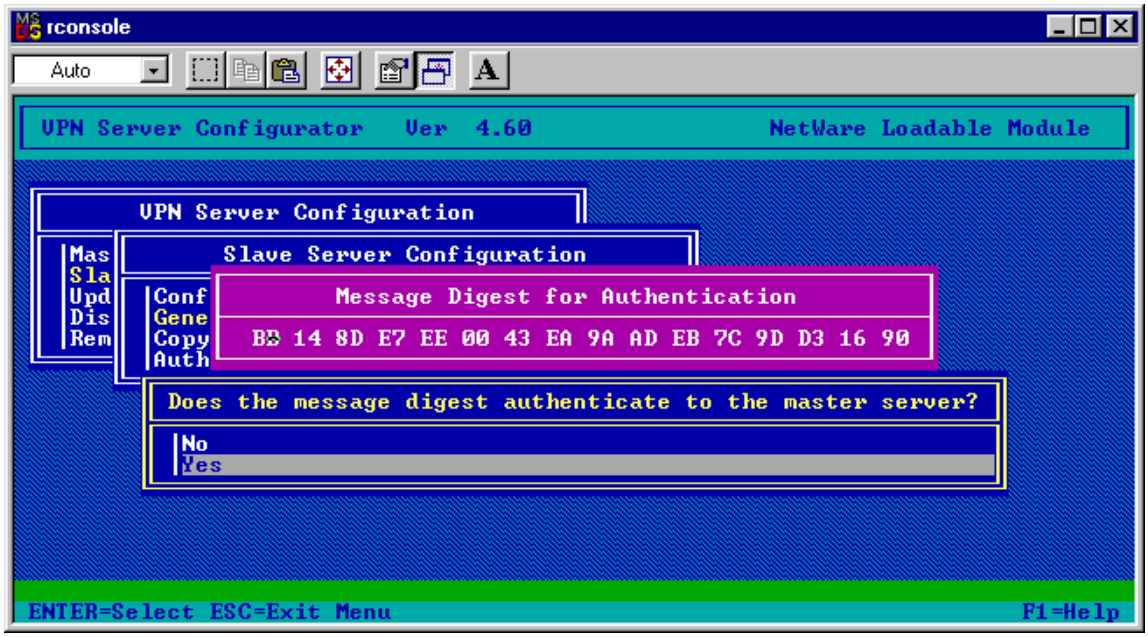
Select **Generate Encryption Information** to begin setting up the encryption keys needed to establish a secure link between master and slave VPN servers.

Note You will be required to provide the MINFO.VPN file from the Master VPN server at this point, and you will need the slave server's authentication digest string (for comparison purposes). The easiest way to enter the data is to have that file on a floppy disk inserted in the slave server at this point.



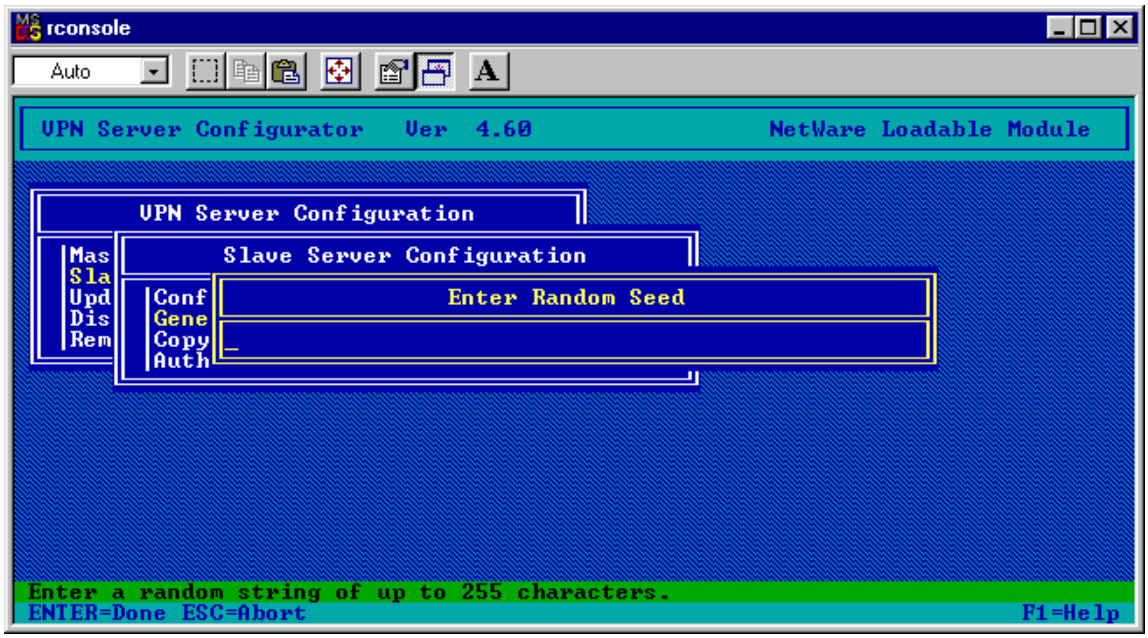
Enter the path to the MINFO.VPN file if you are not supplying the file on floppy disk. You can, for instance, point to SYS:\SYSTEM, or a CD volume to read the file. (The file needs to be in the root directory of a floppy disk).

Once you press the **Enter** key, the MINFO.VPN file will be read from the specified path.

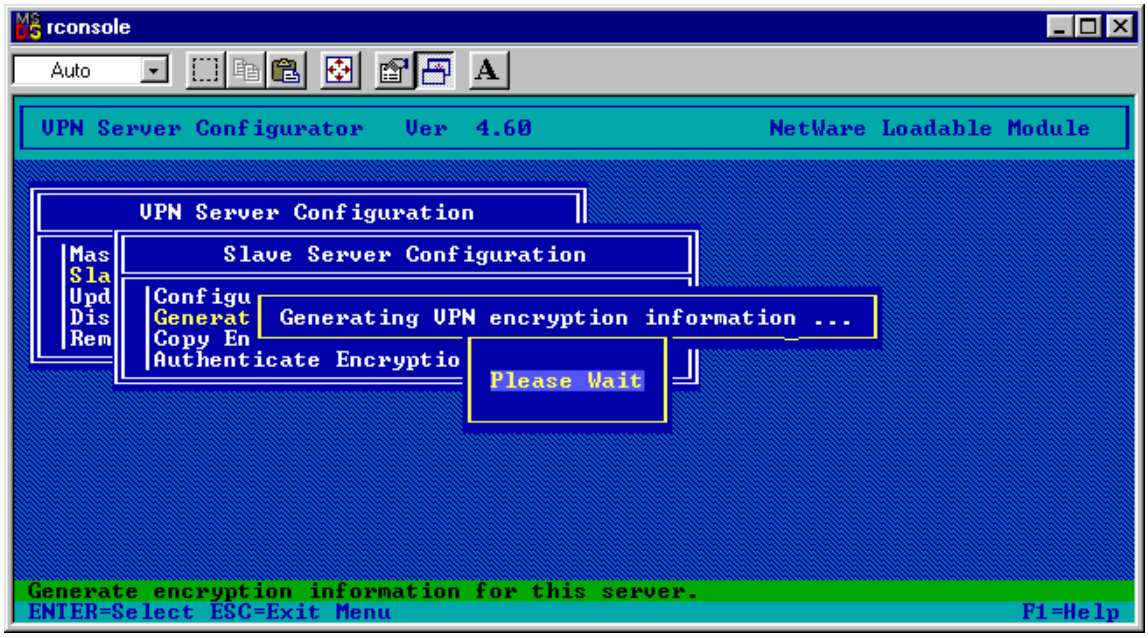


You should now be prompted to confirm that the digest contained in the MINFO.VPN file is correct.

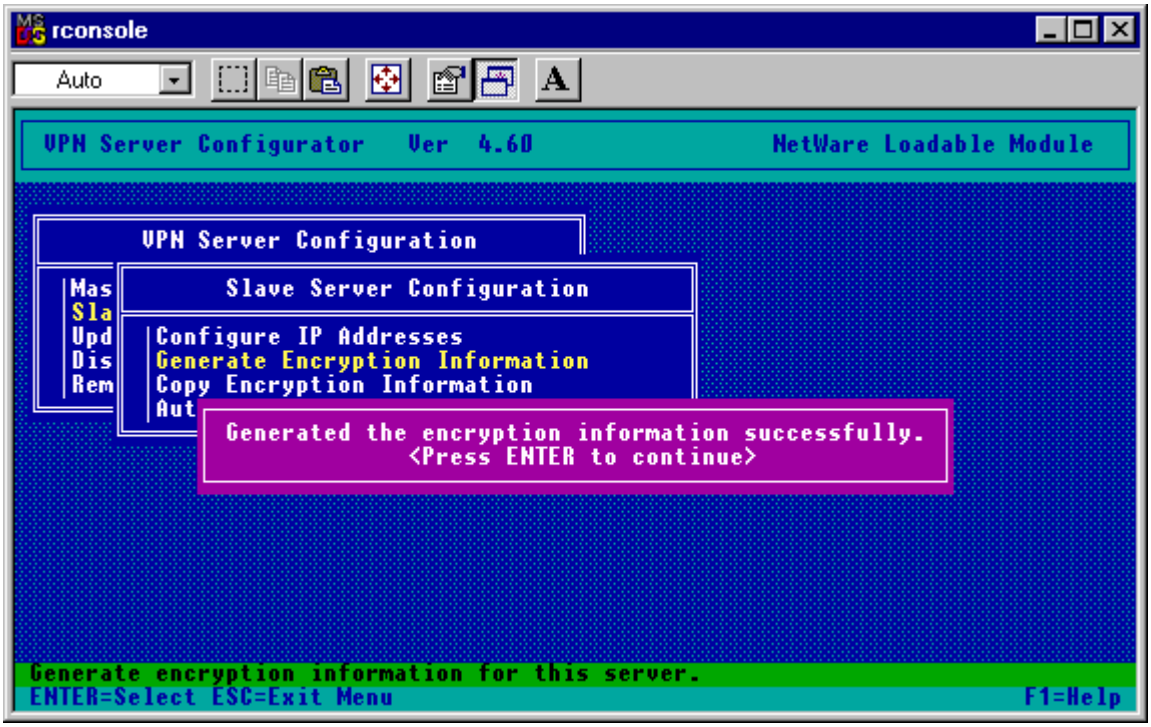
If the message digest matches the digest for the proper VPN Master server, select **Yes** to continue. Otherwise, abort the VPN slave server configuration process, and get the correct MINFO.VPN file.



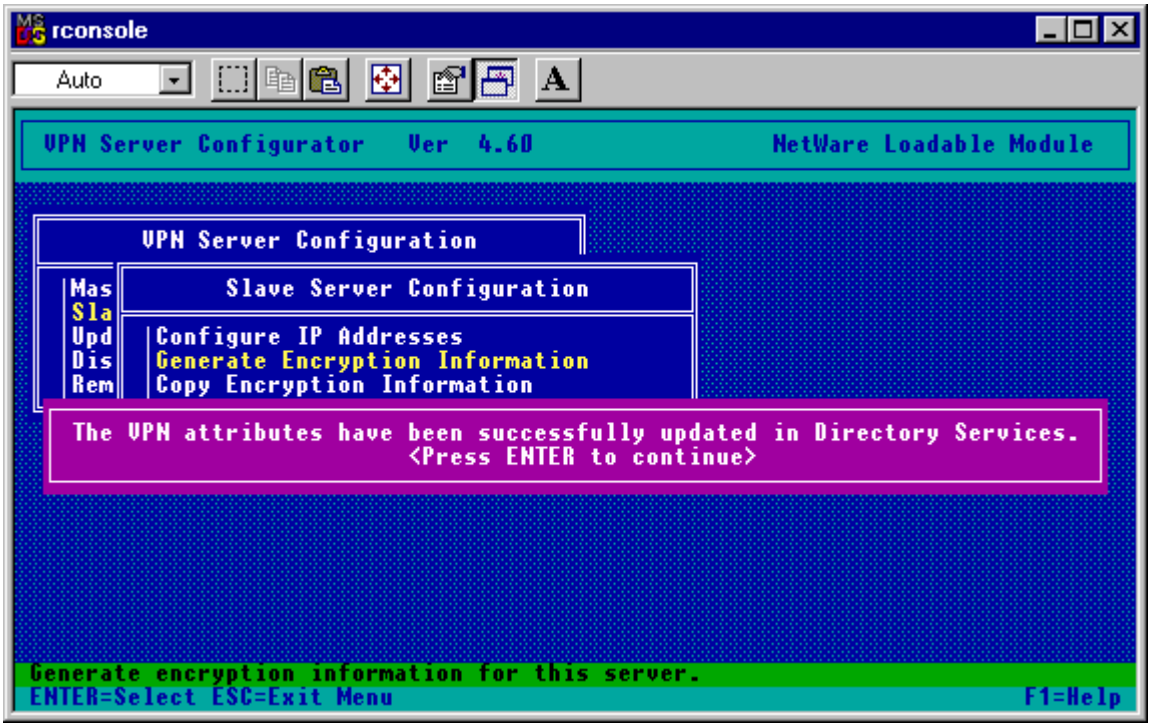
You should next be prompted to enter a random seed. Type in several random letters and/or numbers from the keyboard and press the **Enter** key.



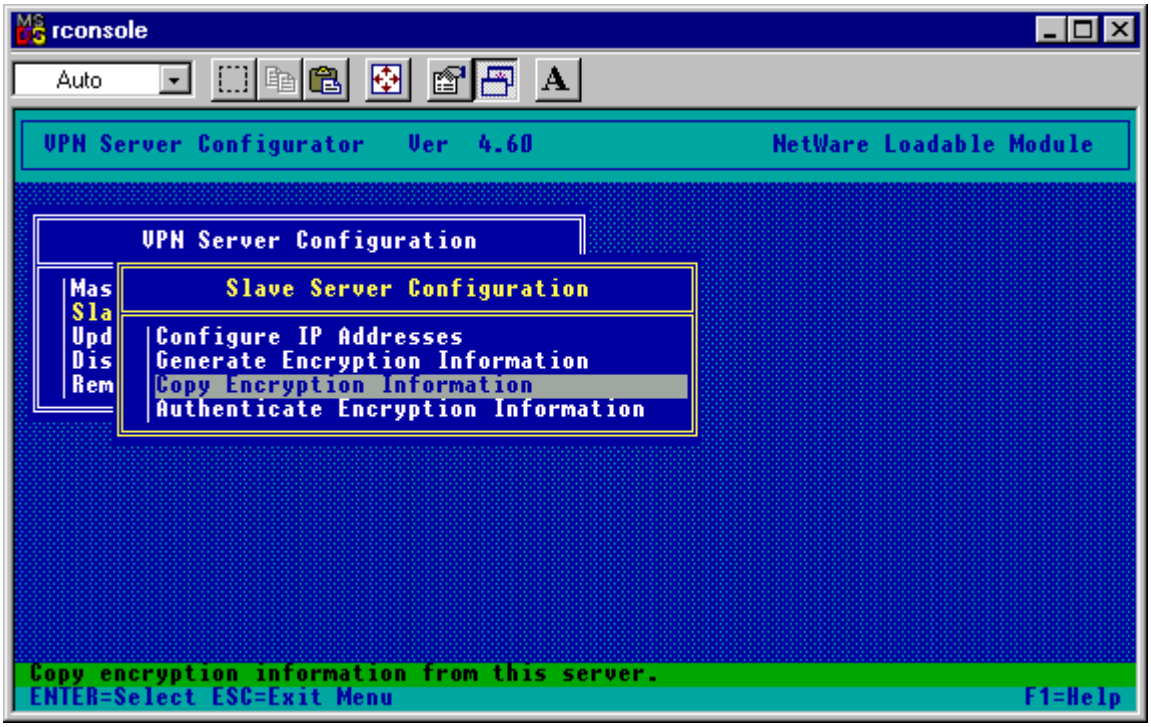
The encryption keys should now be generated for the slave VPN server. This process can take several minutes.



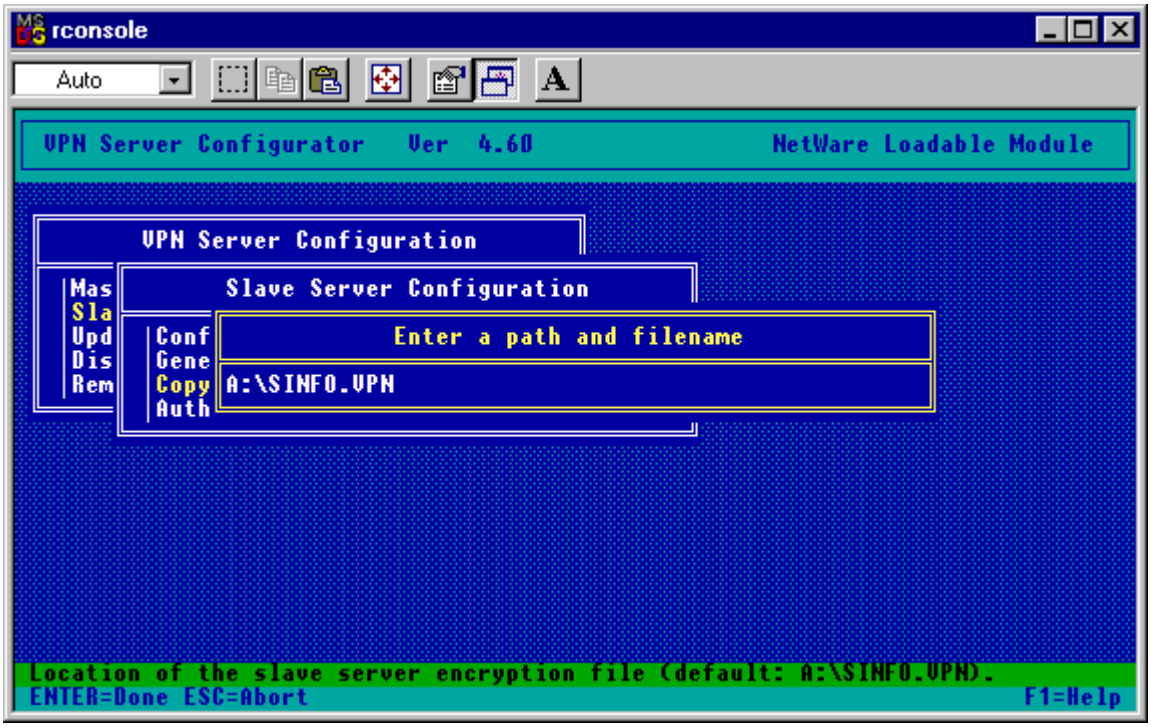
You should next see a message indicating that the encryption information was generated successfully. Press the **Enter** key to proceed.



Next you should see a message indicating that the VPN attributes were successfully updated in directory services. Press **Enter** to continue.

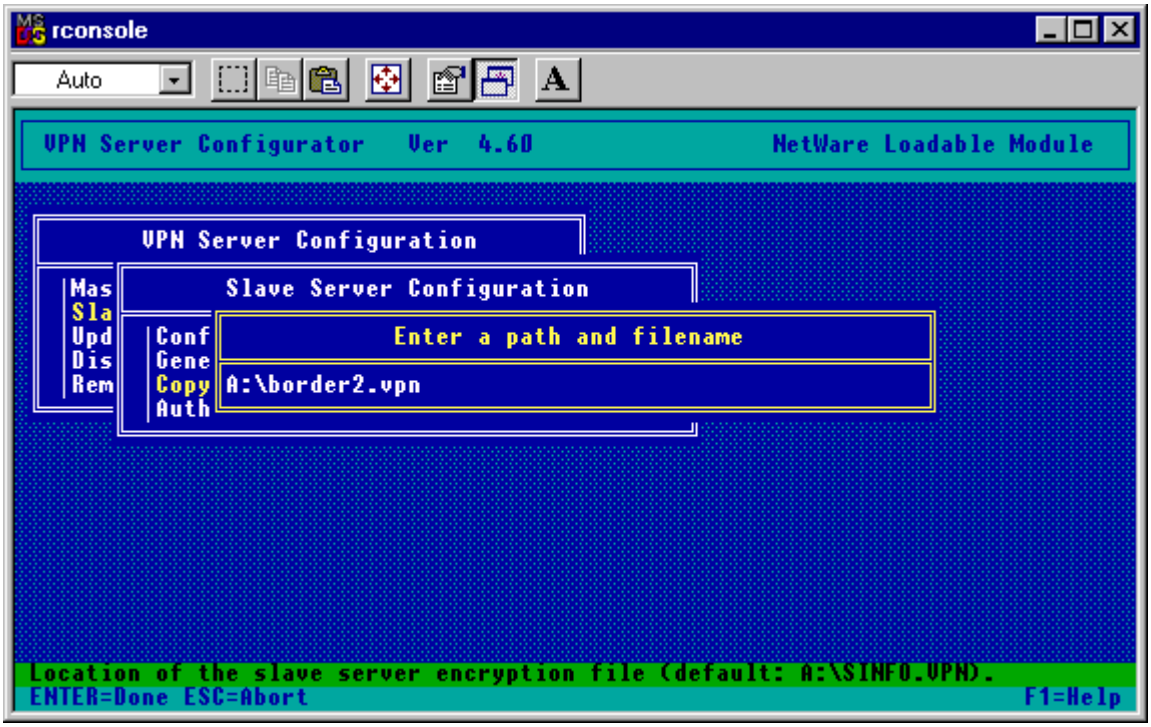


From the VPN Slaver Server Configuration menu, you must now select **Copy Encryption Information** to save the VPN configuration data for the new slave server to a file so that the server can be added to the VPN in NWADMN32.

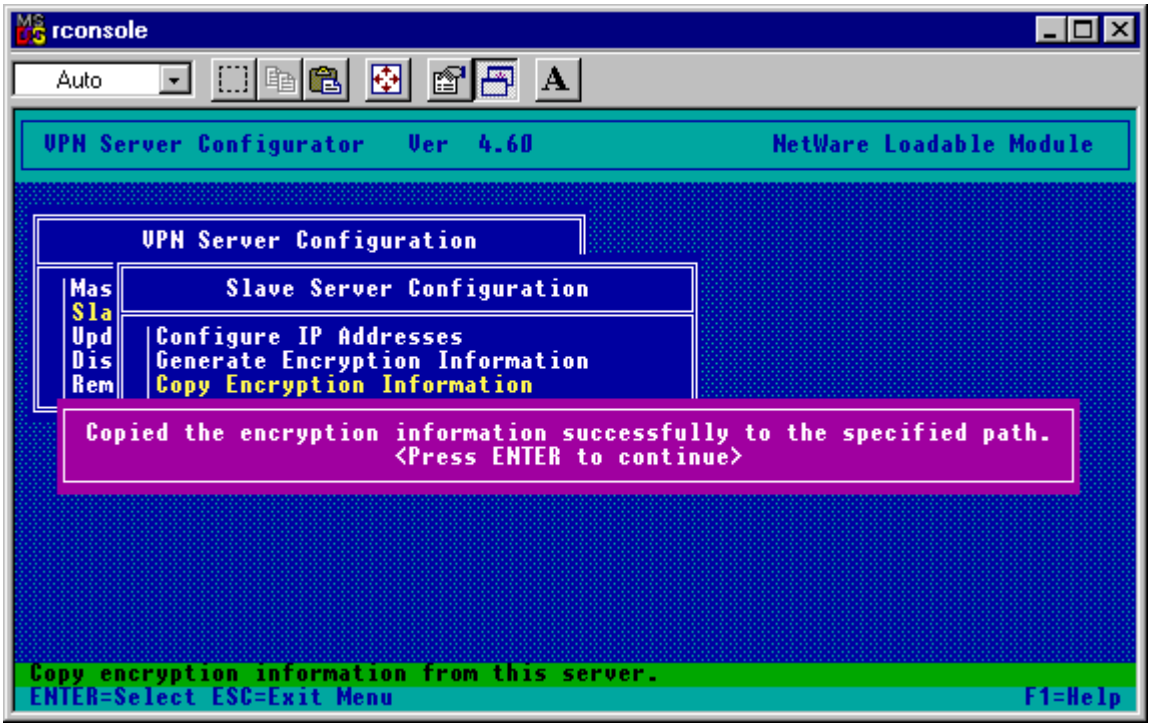


You will be prompted for both a path and a file name, unlike when saving data for a Master VPN server. If you are only setting up a single VPN slave server, the file name SINFO.VPN will be sufficient. However, it may be convenient to save the information using the server's name as the file name, and VPN as the file extension, in order to more easily identify what VPN configuration file belongs to what slave server when multiple slave servers are to be used.

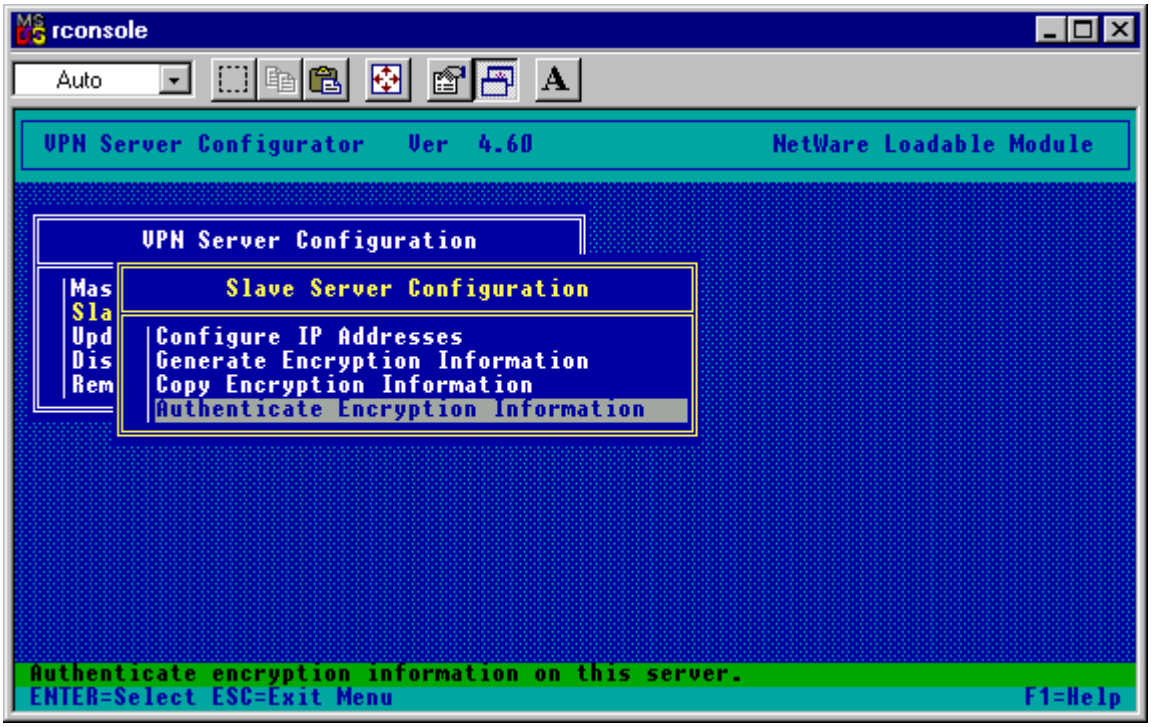
Type in a more descriptive name, as in the following example.



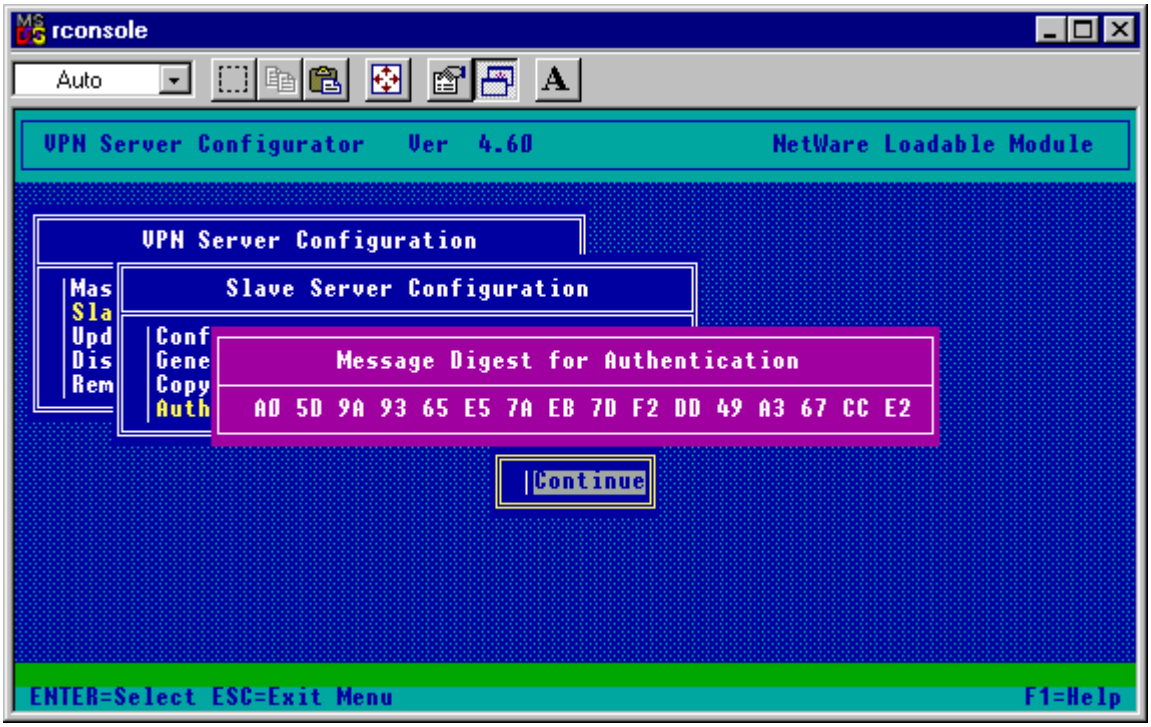
In the example show, the slave server VPN configuration information will be saved to a file on the **A:** drive called **BORDER2.VPN**.



You should see a message indicating that the encryption information was successfully copied to the specified path. Press **Enter** to continue.



You should now select **Authenticate Encryption Information** from the VPN Slave Server Configuration menu.



Record the message digest information where it can be verified later when the slave server is being added into the VPN.

Press **Enter** to continue.

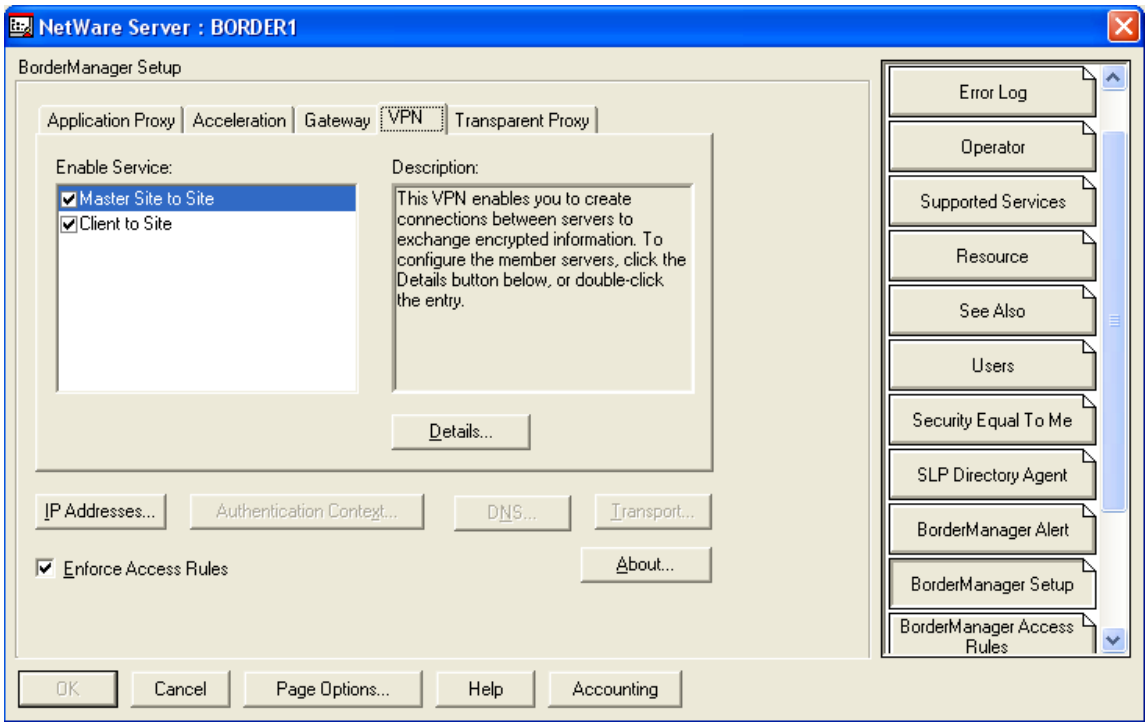
Press **Escape** repeatedly to exit VPNCFG. Take the VPN slave configuration file (in this case BORDER2.VPN on a floppy disk) to the site holding the Master VPN server so that the slave server can be added to the VPN.

Adding a VPN Slave Server – NWADMN32 Procedures

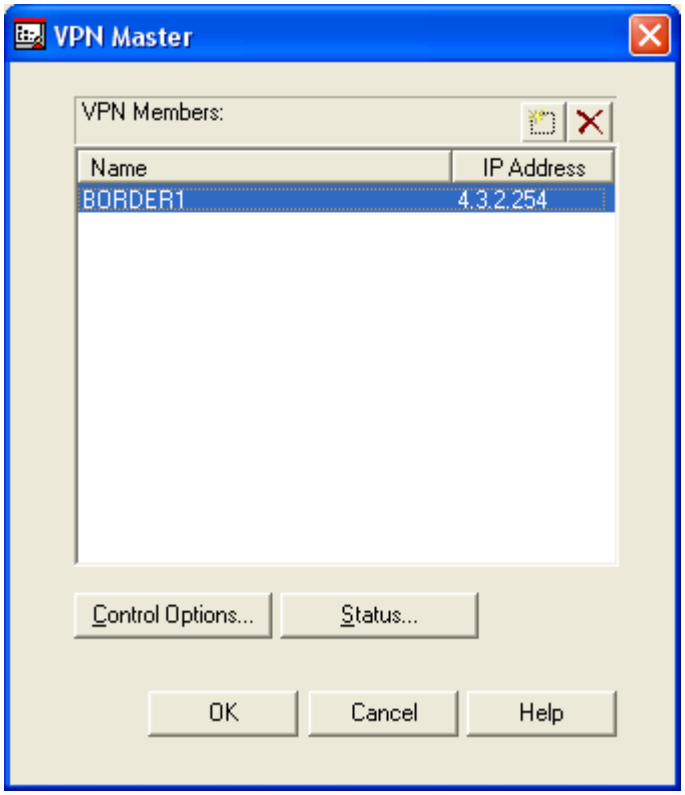
You should have the slave server configuration data file (BORDER2.VPN used in the example in this book) available for this next step.

Begin by launching **NWADMN32** from the Master VPN server. Select the Master VPN server and double-click the server object.

Select the **BorderManager Setup** tab.

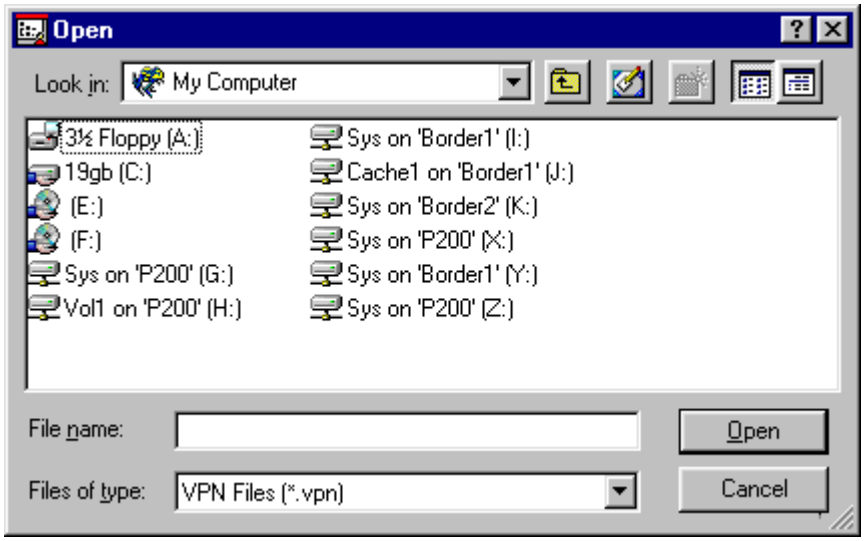


Select the **VPN** tab. Then select **Master Site to Site**, and click on the **Details** button.

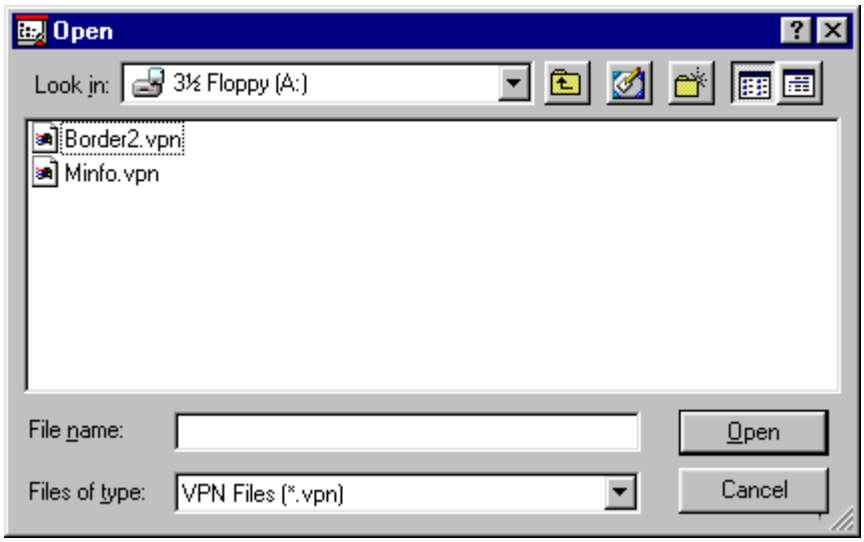


You should see the Master VPN server as a VPN Member. If you are configuring the first slave VPN server, there will be no other VPN Members shown. If the VPN Master server is not shown, you will have to go through the Master VPN server configuration as shown earlier in this book.

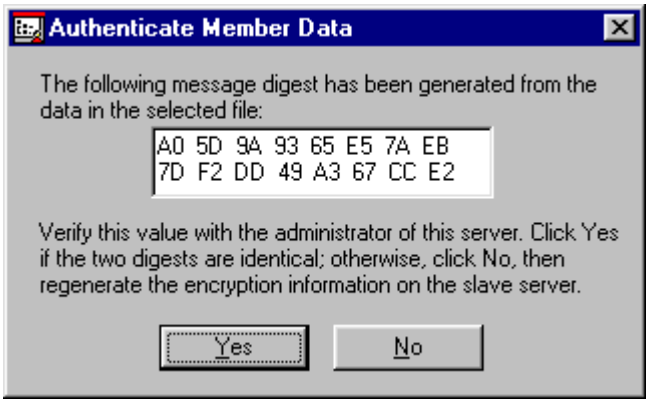
Click on the **rectangle** to add a VPN slave server.



You will have to navigate to the directory holding the slave server's VPN information file. (The default name is SINFO.VPN, but in the example in this book, the configuration data was saved as BORDER2.VPN).

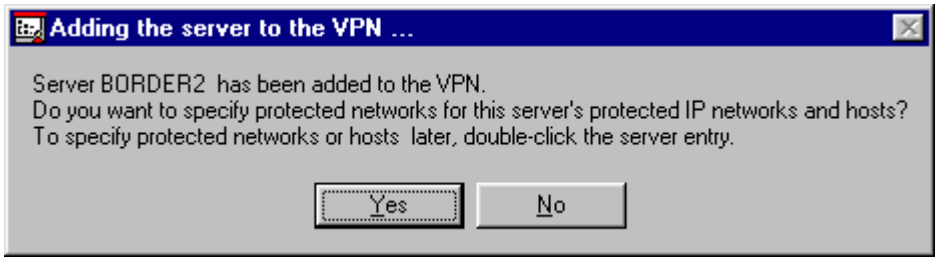


Select the proper .VPN file for the slave server, and click on the Open button.



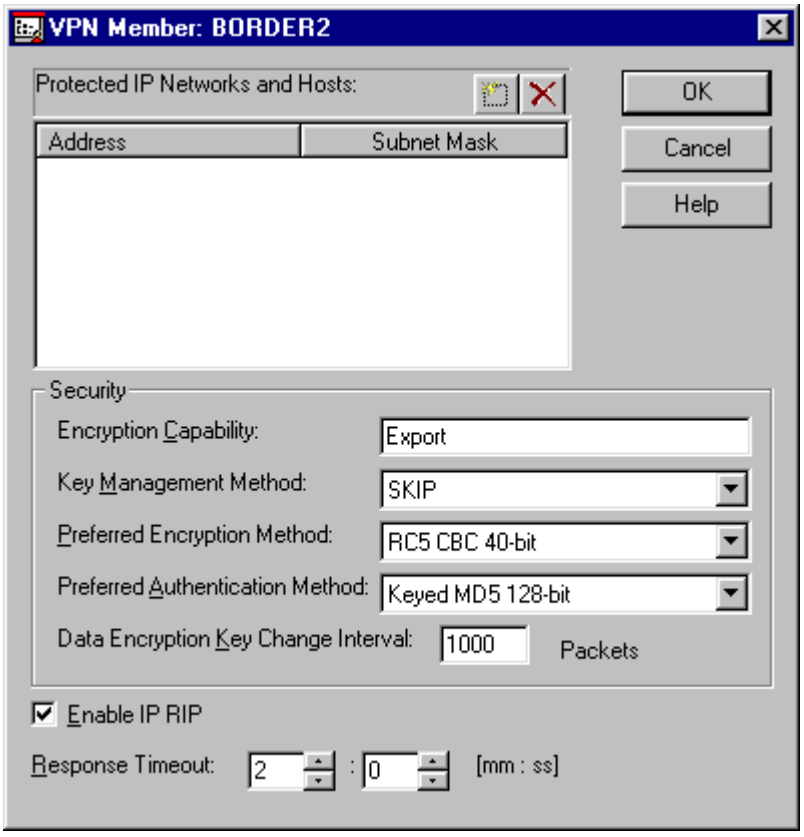
Once you have selected the slave server's .VPN file, you will be shown the message digest. Compare this with the message digest generated by VPNCFG at the slave server to be sure that someone has not substituted their VPN server's configuration file in an attempt to get you to add an incorrect VPN server to your VPN.

If the proper digest information is shown, click on the **Yes** button.



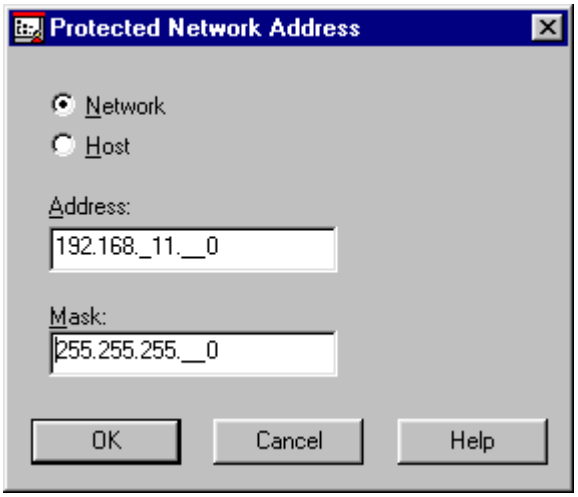
As soon as you click **Yes** on the digest information, the slave server from the .VPN file is added to the site-to-site VPN. You can specify networks to protect now or later. (Protected networks are the networks whose information is to be sent through the VPN tunnel).

Click on the **Yes** button to continue.

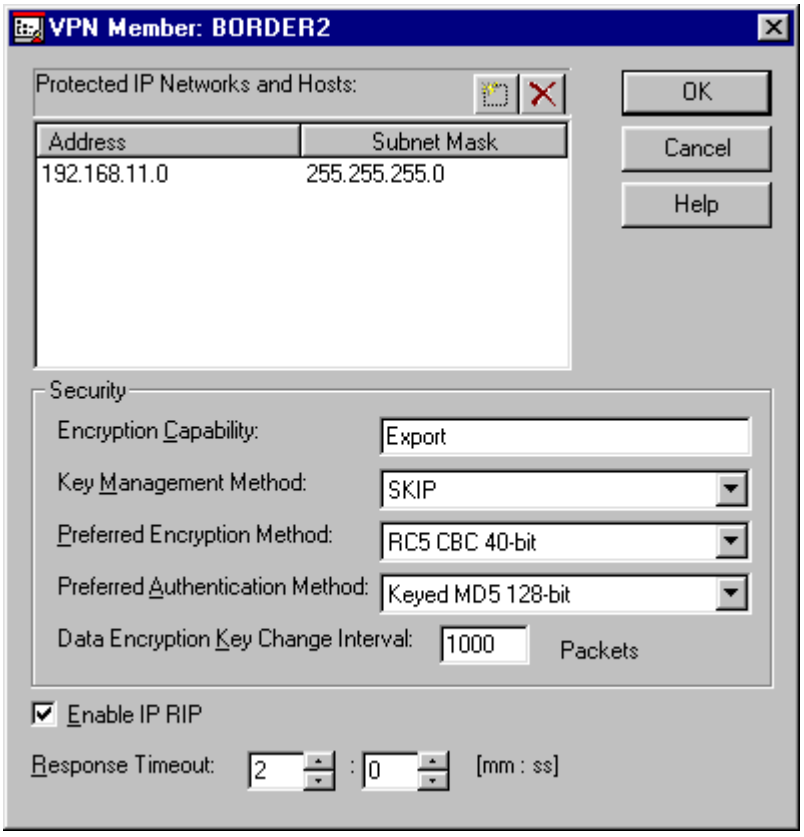


You should see a menu listing various VPN parameters to adjust for the connection to be established between the Master and this slave VPN server.

Click on the **rectangle icon** to add a protected network to the list.



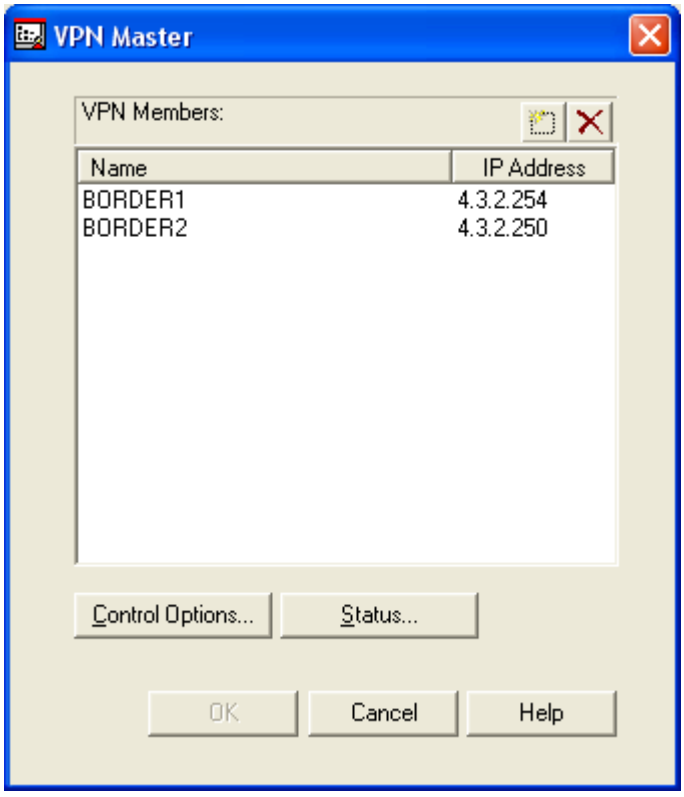
Enter a network number to protect (encrypt) an entire network, or enter a host IP address if you just want to protect data from a particular VPN host.



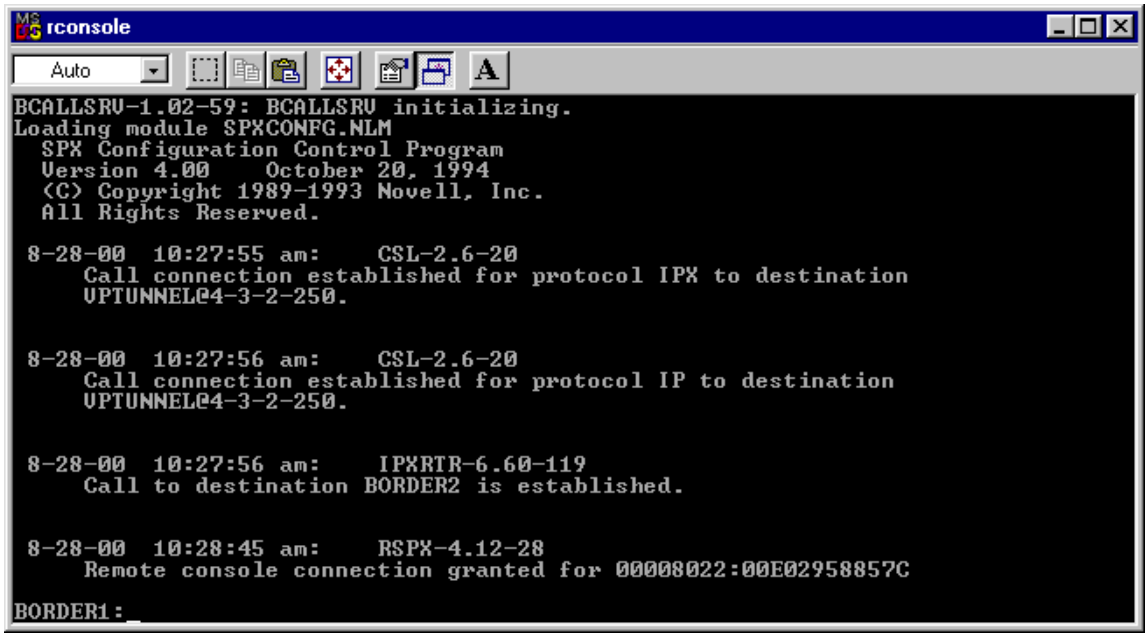
If you have entered the required information, click on **OK** to proceed.

CAUTION *Do not forget to add protected networks or hosts to the master VPN server! You are not prompted to do that when the master VPN server is first configured.*

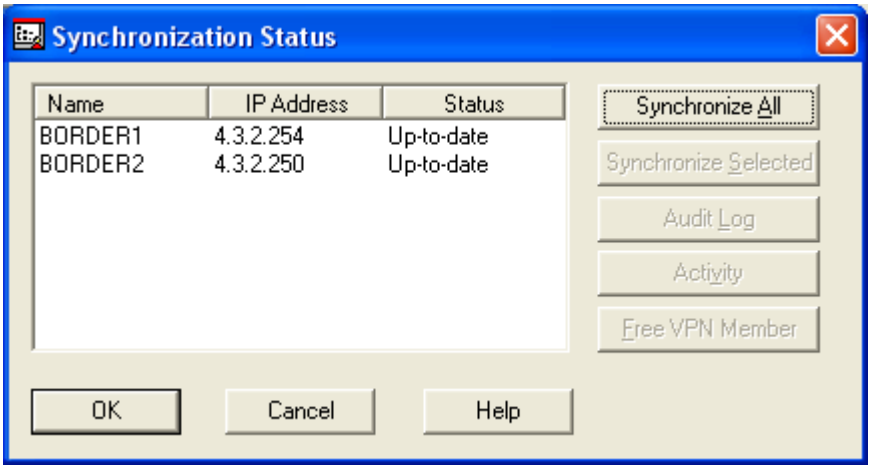
Note Adding a network or host address to the protected list will set a static route on the other Site-to-Site VPN servers pointing to the protecting server's VPN tunnel IP address. In the example shown for BORDER2, if you look at the BORDER1 server's SYS:\ETC/GATEWAYS file, you should see an entry for 192.168.11.0 pointing to a next hop of 192.168.99.253. Only protect networks that are actually 'behind' the server you are configuring.



The slave server should now appear as a VPN Member.



At the master VPN server console, you should see messages indicating that communication was established to the VPN slave server, assuming that a physical connection was present (WAN links are up, SKIP protocol supported by all the ISP's involved, IP addressing is correct, etc.)



Select the **Status** button to confirm that the configuration data for all servers is **Up-to-date**.

Click on **OK** repeatedly to save all settings and exit NWADMN32.

<This page intentionally left blank. This is to facilitate putting in chapter tabs in a ring binder for double-sided printing. The main chapters should start on an odd-numbered page.>

Chapter 18 – Legacy Client-to-Site VPN

Note BorderManager 3.7 and earlier VPN is called 'legacy' VPN in this book. The new IKE-based BorderManager 3.8 VPN is covered separately in a later chapter. Legacy VPN on a BorderManager 3.8 server is still set up essentially the same as described here – you must run VPNCFG for instance – but access rules are done in iManager 2.0, not NWADMN32.

Concept

VPN stands for Virtual Private Networking, and has rapidly grown in popularity along with the Internet as an economical alternative to setting up dedicated dial-in lines. A VPN makes use of the Internet to transport traffic instead of dedicated WAN (or dial-up) links. The key to a VPN is security – all packets traveling through a VPN connection are encrypted in case someone tries to intercept them.

A client-to-site VPN consists of a remote PC running a VPN client making a VPN connection to a VPN server somewhere. In the case of Novell BorderManager 3.7 and earlier, the VPN consists of Novell VPN client software running on a Windows 9x or NT/200/XP PC, and a BorderManager 3.0 or later VPN server. The VPN client software must be Novell's version, and it can support a dial-up connection to the Internet or a LAN (or cable modem or DSL) connection to the Internet. Both IP and IPX protocols are supported through the VPN (except on Windows 2000 or XP clients, where IPX is not supported).

In order for Novell's VPN to work for versions of BorderManager prior to 3.6, both end points must be using public IP addresses. If a NAT hop exists between the end points, the VPN will not work because of the technology involved in IPSec security, which is used in a Novell VPN. In addition, the ISP's involved must not block the SKIP (**S**imple **K**ey-management for **I**nternet **P**rotocols) protocol in order for the VPN key exchange mechanism to succeed. This means that home networks (cable modem, DSL, etc.) behind a NAT router hop will not be able to use Client-Site VPN unless BorderManager 3.6 or later is installed.

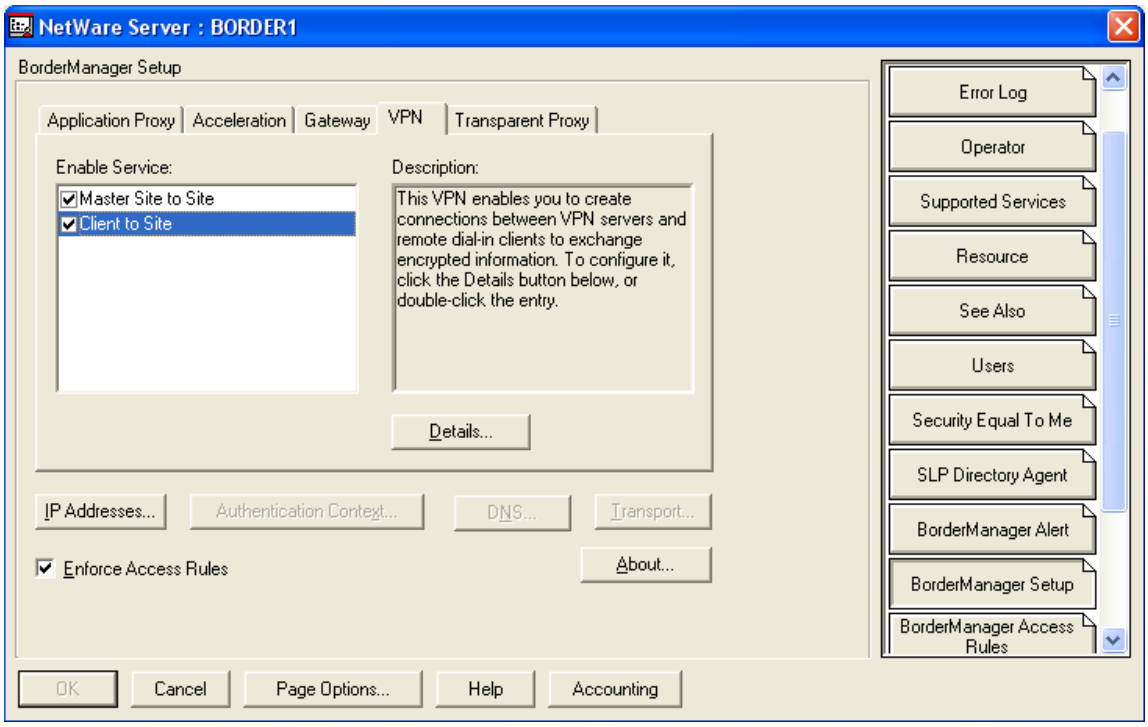
With the release of BorderManager 3.6, it is possible to establish a Client-to-Site VPN when the client is behind a NAT connection.

The VPN server must still have a public IP address and not be behind a NAT connection. BorderManager 3.8 adds the ability for both ends of the VPN to work through NAT, but that capability does not extend to the legacy VPN client.

Note Client-to-Site VPN does not work on WindowsME unless using the BorderManager 3.7 version of the VPN client. Also, the BorderManager 3.7 and later versions of the VPN client do not install to Windows 95, though the earlier VPN clients do. (Windows 98 is supported by older and newer versions of the VPN client).

Setting Up VPN Servers

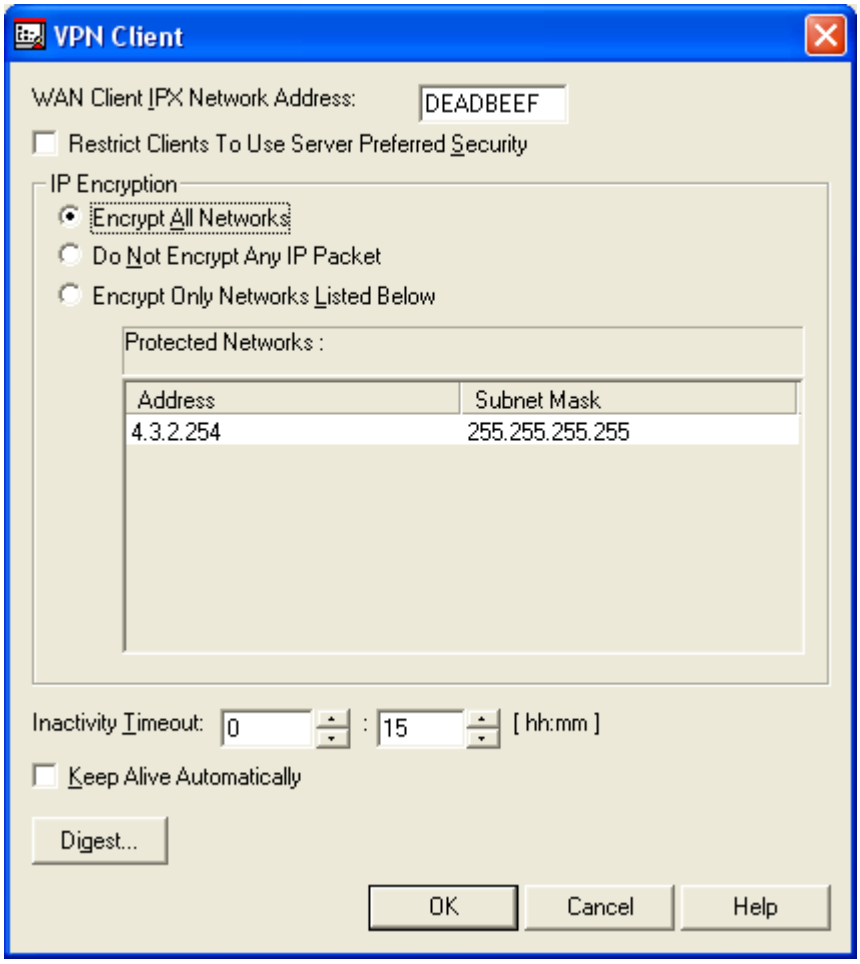
The first BorderManager server in either a Site-to-Site or Client-to-Site VPN must be configured as a master VPN server. If setting up Site-to-Site VPN servers, each slave server can also be set up for Client-to-Site VPN. *Review the previous chapter on Site-to-Site VPN for instructions on configuring the Master VPN server.*



Double-click **Client to Site** to configure Client to Site VPN.

Click on the **Details** button to configure Client to Site VPN settings.

The VPN client screen requires you to enter several extremely important settings, each of which is explained below.



In the **Client to Site** configuration menu, enter a unique **WAN Client IPX Network Address** to be used. The WAN Client IPX Network Address is the IPX network number to be used within the virtual tunnel to route IPX traffic between VPN client and VPN server. IPX traffic to be routed over the Client-to-Site VPN connections from this server will be routed over this network. In actuality, the IPX data will be encrypted inside of IP packets, but the IPX routing tables will not know that a virtual tunnel exists, and the routing engine needs to see an IPX network number in order to route data between client and server. If you leave this setting blank, IPX data cannot be routed across the Client-to-Site VPN. The virtual IPX network number used in this example is DEADBEEF, which is a valid hexadecimal number.

Note The WAN Client IPX Network Address must not be the same as an IPX network number used anywhere else in the network, including on either side of a Site-to-Site VPN or an internal IPX Net Number of a NetWare server.

The **Restrict Clients To Use Server Preferred Security** option is used to force the clients to use the same security settings as on the server. Effectively, this would mean that if the server was configured for 128-bit encryption, the clients would also have to be configured for 128-bit encryption, and 40- or 56-bit clients could not establish a VPN connection.

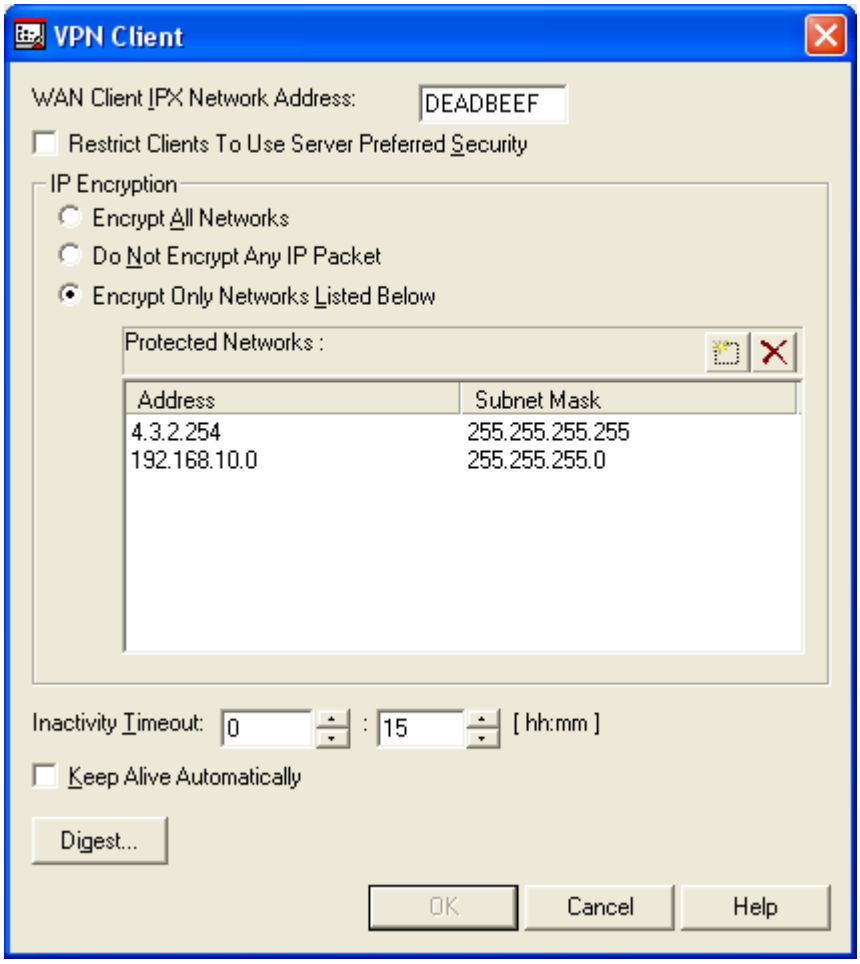
The **IP Encryption** settings are very important, and should usually be changed from the default (Encrypt all networks). This option needs to be understood thoroughly. Encrypting all networks can prevent users from browsing the Internet while using the VPN.

Do Not Encrypt Any Packet would effectively disable the VPN. Don't use this option as it the VPN won't work!

Encrypt All Networks tries to force ALL packets from the remote client to be tunneled to the VPN server, encrypted, and then forwarded by the VPN server. This will effectively encrypt all internal networks, but at the same time will try to send all non-VPN traffic from the remote host through the VPN tunnel. In other words, with this setting turned on, if the remote host tries to browse to http://www.cnn.com while the VPN connection is up, the traffic will be sent to the BorderManager server through the VPN tunnel, and from the BorderManager server back and forth to http://www.cnn.com. Generally, this is undesirable!

Encrypt Only Networks Listed Below is **normally the best option**, and it requires you to manually enter the internal IP networks that the client-to-site VPN should be able to contact. You may have to enter many networks here. Select **Encrypt Only Networks Listed Below**, and enter all the internal subnets you wish to access via an encrypted VPN link.

CAUTION *If you select Encrypt All Networks, ALL traffic from a VPN user will come across the WAN link to the BorderManager server and be encrypted, including that user's regular Internet traffic! This setting often results in the client browsing to the Internet failing.*



The following networks are set up for encryption:

192.168.10.0

and the default VPN server address of 4.3.2.254. (You cannot remove or modify this address).

Note All internal TCP/IP hosts to be accessed via a VPN connection MUST be configured with a valid default gateway.

If you need to add a subnet to the list of encrypted networks, click on the add box.

An important note here – if you want to access a network that is on the other side of a Site-to-Site VPN link, you cannot normally do that with Client-to-Site VPN. Traffic coming in over the Client-Site VPN on one side of the Site-to-Site VPN cannot cross to another side and get back. Filtering and routing issues prevent the traffic. The only way to get that to work with Legacy VPN is to have a dedicated Client-to-Site server that has dynamic NAT enabled on the

private IP address. If you cannot set up a such a dedicated server, you will have to configure Client-to-Site VPN at each Site-to-Site server, and connect to the local BorderManager server to get access to the local server's protected network.

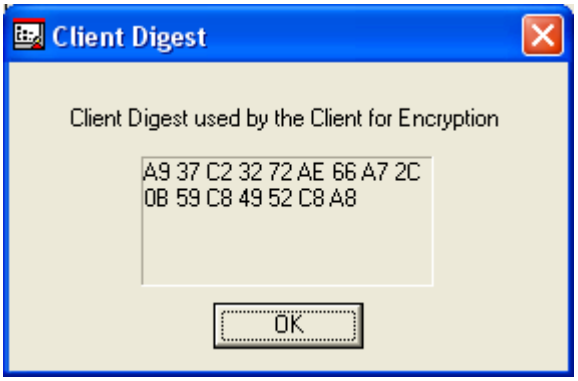
Another note: If you unfortunately have an internal network address that matches the remote VPN user's network, there is a trick you can use to give access to the remote user without having to re-address either your entire network or the remote user's. That trick is to dual-home the BorderManager server and any internal hosts that need to have VPN access, with a second IP address. You would add another IP address in an entirely different network, and add that network as a protected network in the Client-to-Site VPN configuration.

Enter the network number and subnet mask to be protected, and click on **OK**.

Inactivity Timeout, which defaults to 15 minutes, is the length of time that a VPN connection is held active at the VPN server without receiving any encrypted data (not keep-alive packets) from the remote host. After this period expires, any VPN connection is closed by the VPN server. This feature is useful to reduce the load on a VPN server with many client connections, as it will drop inactive connections. Once the connection has been dropped, the remote host will have to re-establish the connection.

Keep Alive Automatically is a feature designed to keep idle client connections established indefinitely. Not enabling this feature helps a busy server by keeping it from trying to maintain circuits where there is no activity. It essentially overrides the Inactivity Timeout.

The **Digest** button will display the digest information created for Client-to-Site VPN connections. This digest is not the same as shown in VPNCFG, which is used for Site-to-Site VPN.



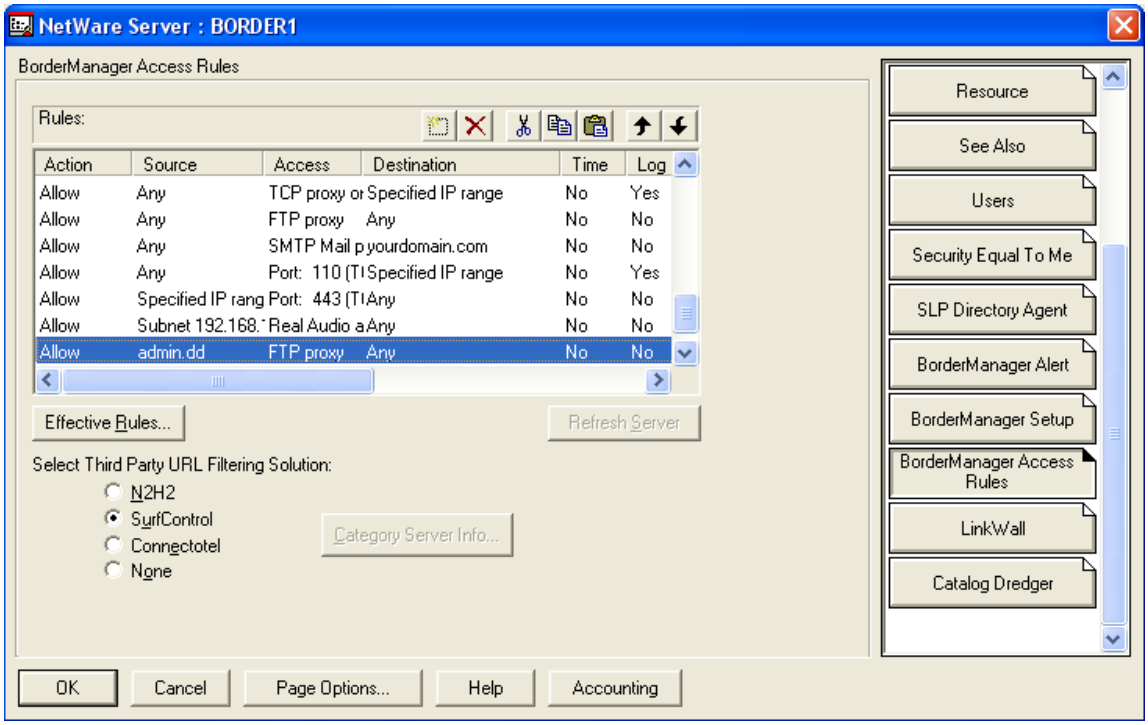
Here is an example of the digest information associated with the configured VPN server. (Your digest information will be different). The digest information is used to confirm that the encryption keys used for VPN services are the intended keys. In other words, if initial VPN connection comes up and reports a different digest, it is possible that someone is trying to spoof your VPN connection at another server. Do not accept a connection that reports a non-matching digest! The digest is only reported for the first connection – after that, the connections are established automatically based on the encryption data exchanged during the first connection.

You can compare the digest information here to that seen by the client in case you suspect a client is connecting to a counterfeited VPN server.

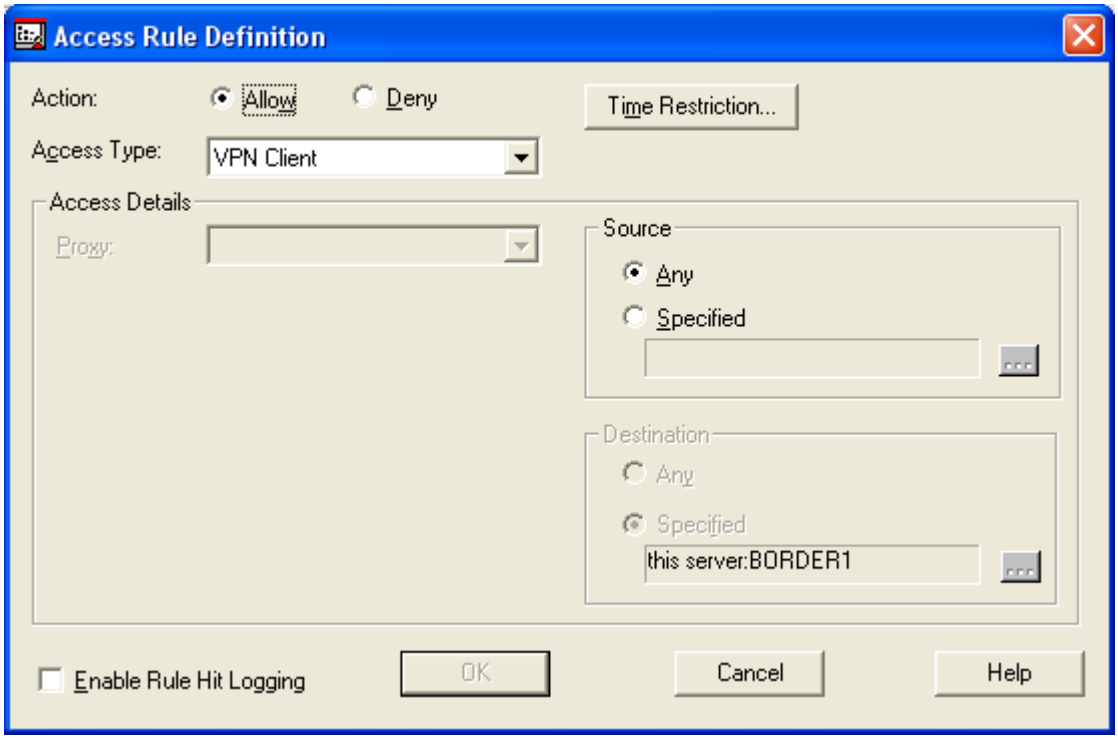
Once you have entered the proper configuration data, press **OK** repeatedly to return to the BorderManager main menu. Then select the **BorderManager Access Rules** tab, and set up access rules allowing selected used to authenticate over a client-to-site VPN connection.

BorderManager Client-to-Site VPN Access Rules

You will need to set up at least one Access Rule for VPN client in order for anyone to make a connection, unless you are not enforcing access rules.



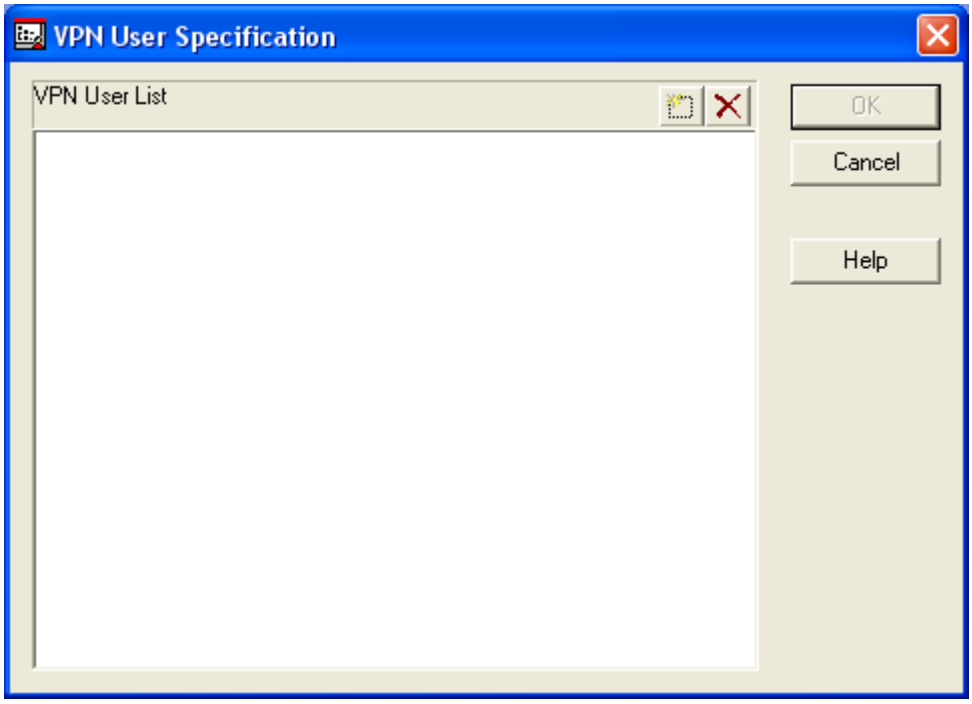
Adding new rules is done by clicking on the small **rectangular box icon** (next to the red x over the rules list). Start by positioning the cursor above the line where you would like to add the rule.



For **Action**, select **Allow**.

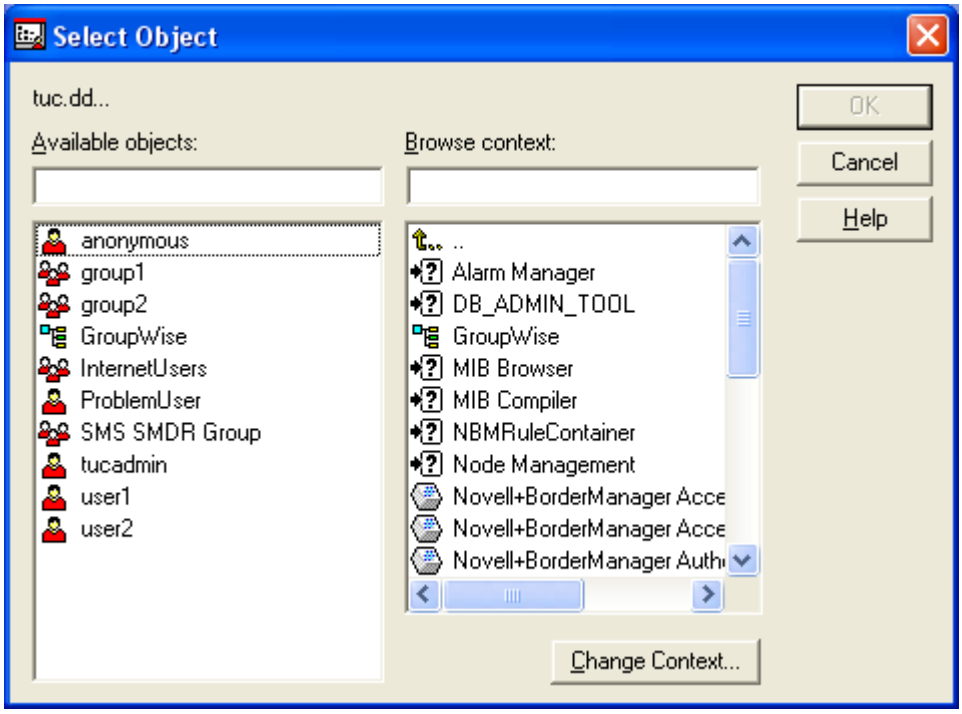
For **Access Type**, select **VPN Client**.

Unless you want anybody (anybody in the NDS tree) to be able to use Client-to-Site VPN, also select a source of **Specified**, and then press the small button in the Source section to select individual NDS objects as sources.



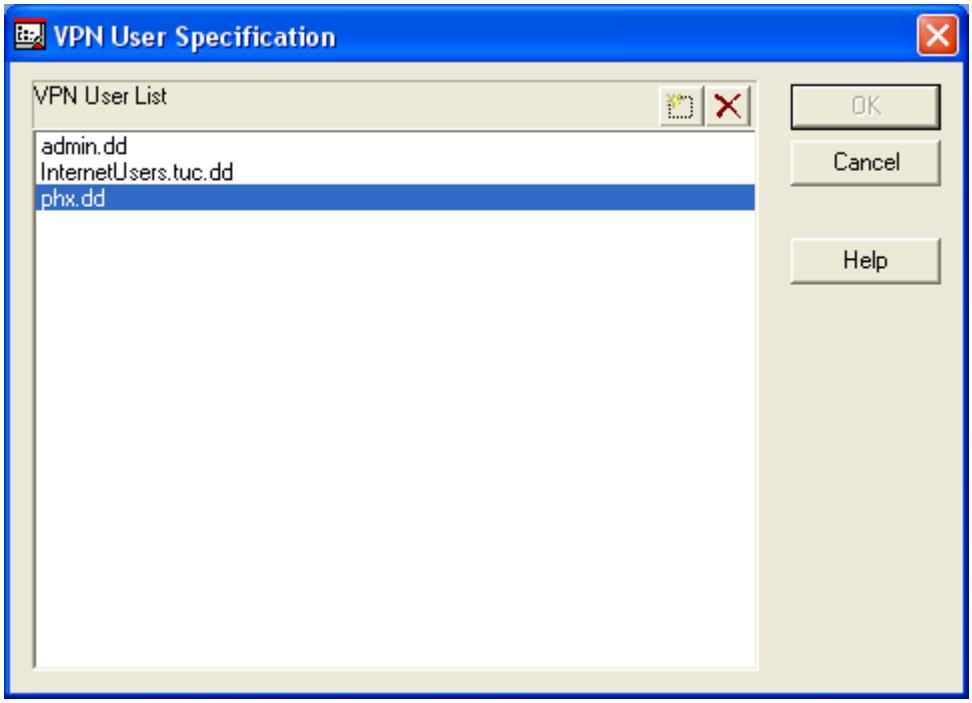
The **VPN User List** will initially be empty, and you will have to add users, groups or containers to allow.

Select the add **rectangle**.



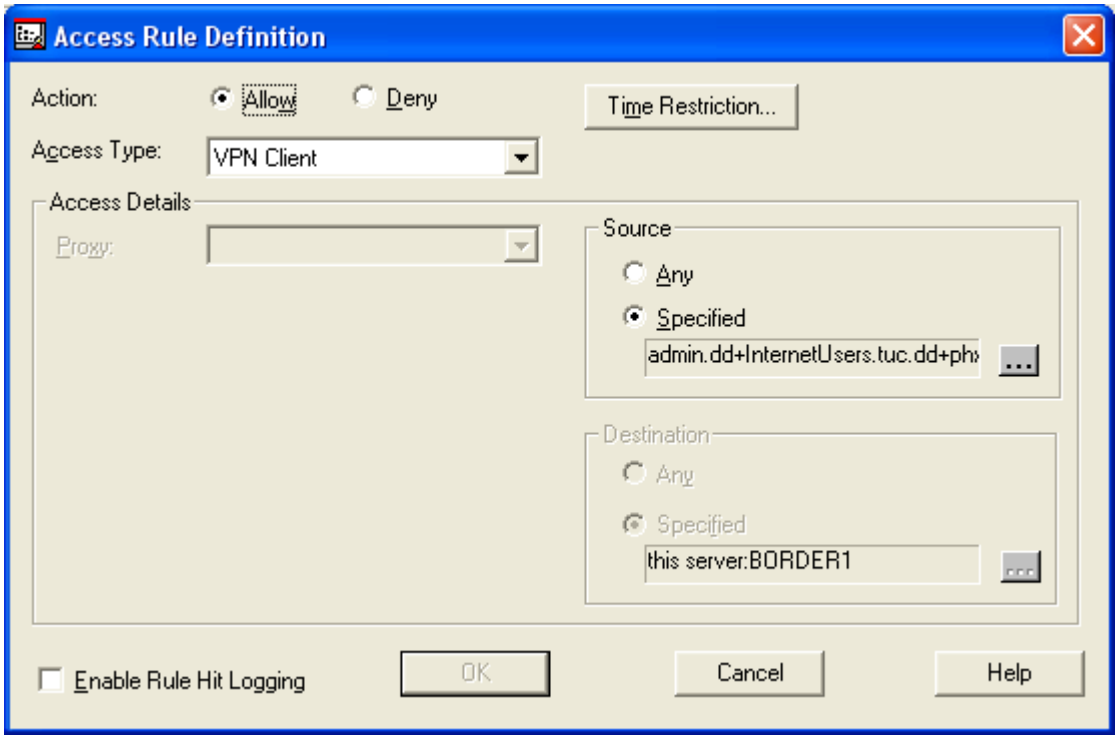
You can now navigate your NDS tree and select objects to allow use of Client-to-Site VPN. Select desired **users, groups** or **containers**.

Selecting a container will allow all users in that container and below to use Client-to-Site VPN.



In the example shown, the container **phx.dd** has been selected as well as the user ID **Admin.dd** and group **InternetUsers.tuc.dd**.

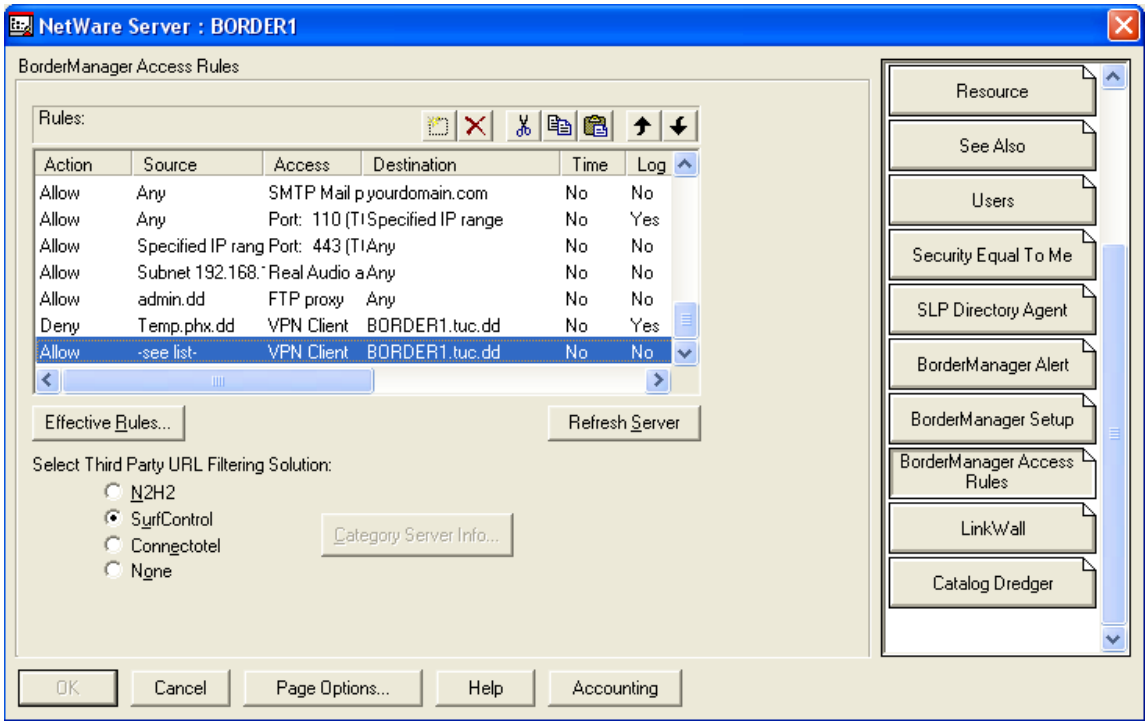
Press the **OK** button to save the selections.



Once you have chosen the desired source objects that are allowed to use the Client-to-Site VPN, you may press the **OK** button to save the rule.

You may want to check the **Enable Rule Hit Logging** to add all VPN client access attempts to the Access Rules log files.

If you wish to allow VPN client access only during selected periods, you may want to click on the **Time Restrictions** button and enable the rule only for selected times and days of the week.



The new access rule appears in the list directly below the rule selected when you started adding a new rule. You may want to move the rule up or down in the list at this time.

Note that you could add a deny rule above the allow rule to deny certain NDS containers VPN access even though a parent container is allowed. The relative position of the access rules in the list is extremely important when mixing Deny and Allow rules, with the rules being read from top to bottom.

The example above shows the a user Temp.phx.dd is denied use of the Client-to-Site VPN while though the following rule allows everyone (everyone else, that is) in the phx.dd container to use Client-to-Site VPN.

Configuring a Client-to-Site VPN Client PC

In order to use client-to-site VPN, a Novell client VPN program must be installed on the workstation. The regular Novell client (Microsoft or Novell version) does not have to be installed on the workstation in order to make a VPN connection, but it does have to be installed if you want to log in to a Novell server once the connection is up. A Novell Client (such as Client32) and the Novell VPN client are two different software programs and serve different purposes. The Novell VPN client makes a secure VPN connection to BorderManager, while the Novell Client32 logs into NetWare servers once a connection has been made. The Novell VPN client does not automatically log the user into NetWare, though it has that option.

Be sure to get the latest VPN client software from Novell. The latest VPN client should be backward-compatible with all previous versions of BorderManager VPN. The latest VPN client supports Windows 98, Windows 98se, WindowsMe, Windows NT 4.0, Windows 2000 and Windows XP. Earlier VPN clients (available on the BorderManager 3.6 and earlier product CD supported Win95 through Windows 2000, but not WindowsMe or Windows XP).

Windows 2000 and Windows XP do not have IPX support over Client-Site VPN.

The only protocols to be used across the VPN connection are the ones checked on the VPN client (IP or IPX, or both).

If only IPX is to be used across the VPN connection, it is best to install Novell's Client32 in IPX only mode, not IP and IPX. This relates only to the newer Novell Client32 clients used to log into NetWare 5.x/6.x servers using TCP/IP.

Using TCP/IP to browse to a web server or access a FTP server over the VPN link has nothing to do with Novell's Client32 software.

After installing BorderManager, the VPN client piece can be installed using the SYS:\PUBLIC\BRDMGR\VPN\SETUP.EXE program, but more than likely a newer version is available via download from support.novell.com (Minimum Patch List).

People have reported that best results occur when installing the Novell VPN client before installing Novell's Client32 program, if both programs are to be installed together.

The VPN client installation provides two icons on the desktop, one for dial-up and one for LAN-based VPN connections. Actually, the dial-up simply has dial-up networking support integrated into the VPN client so that you can use one program to both dial into an ISP and then establish a VPN connection. The LAN-based VPN connection can be used with a dial-up connection as well, although

you must first establish a dial-up connection to an ISP using Microsoft Dial-Up Networking.

The LAN-based VPN client allows you to establish a VPN connection over a cable modem, DSL connection, or leased-line (for instance, a T1 connection). The LAN-based VPN client works only with Ethernet connections; Token Ring is not supported.

VPN connections for BorderManager 3.0 and 3.5 cannot be established if there is a NAT connection between the VPN client and the BorderManager server. Only BorderManager 3.6 and later allows the client to be connected through NAT and still be able to establish a VPN. In addition, the SKIP protocol, (protocol 57), must be supported by the ISP and any local LAN links.

Only BorderManager 3.8 non-Legacy VPN allows the BorderManager VPN server itself to be behind a NAT or port-forward router.

VPN Client Connection Process – A Case Study

Rather than show just a successful VPN connection using Client-to-Site, I thought it might be useful to show one of my early attempts to get the VPN working. A number of problems occurred, and the solutions to each problem are given. Hopefully you will not have as many problems as I did!

The Client-to-Site VPN scenario used here is as shown in Chapter 2, "Scenario 9 - A Complex Multiple BorderManager Server Environment".

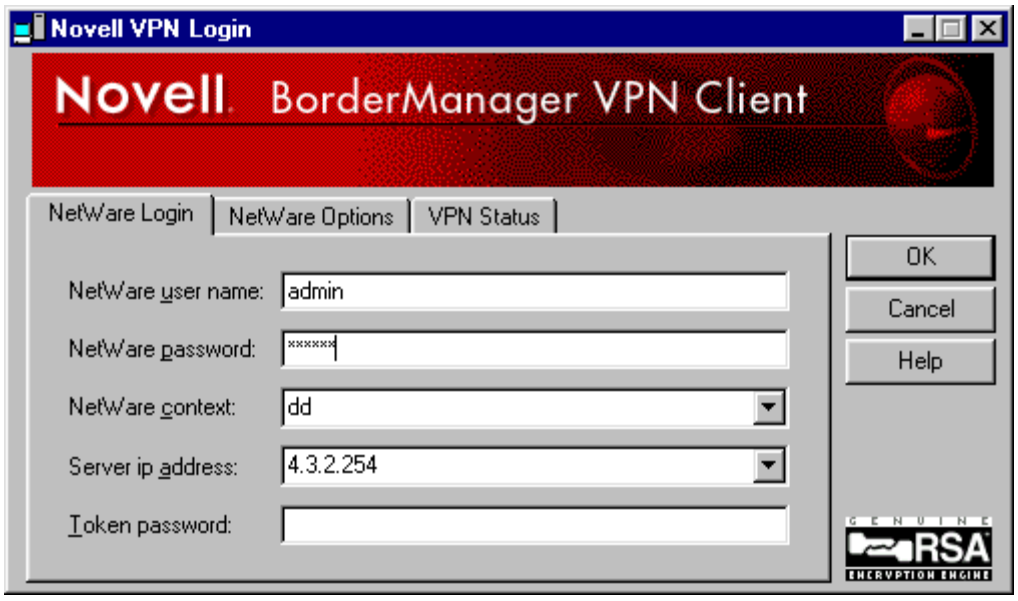
I started with the Client-to-Site VPN settings as described earlier for the VPN servers. An important note here is that BORDER1 was running BorderManager 3.0, while BORDER2 is running BorderManager 3.5.

I also started with the BorderManager VPN client software provided with BorderManager 3.0, in the SYS:\PUBLIC\BRDRMGR\VPN directory. The PC was running Windows 98, and Client32 version 3.21.

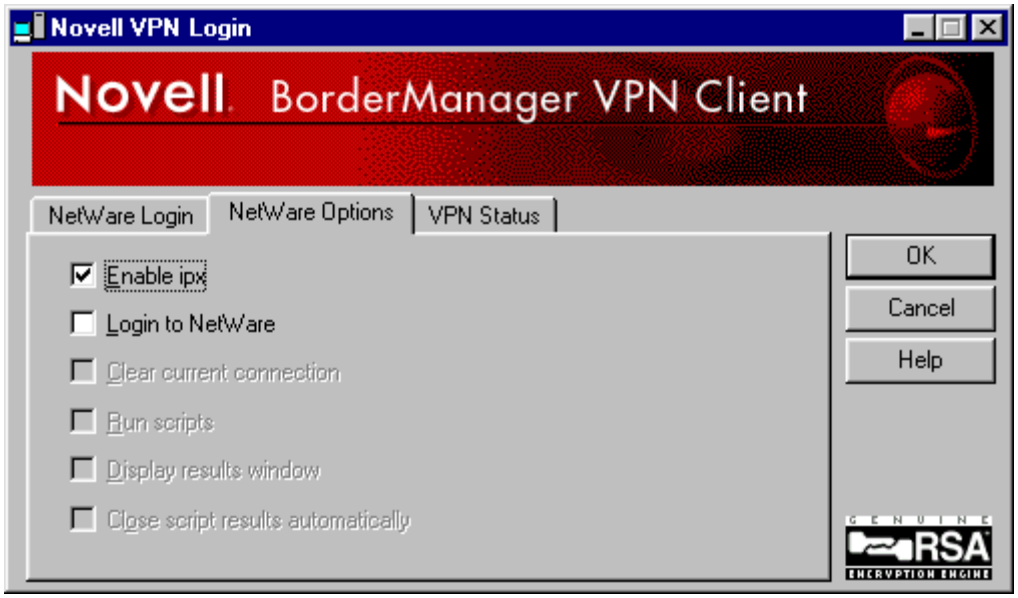
Before trying the VPN Client-to-Site connection, I made sure that I had an Allow access rule allowing a VPN client connection for ADMIN.DD on both the BORDER1 and BORDER2 servers.

This example uses both IPX and IP for logging in. An IP-only configuration is more difficult, due to issues with Service Location Protocol (SLP) and the VPN. These issues are discussed later in this chapter.

Step 1 – Try LAN VPN Client Connection to BORDER1

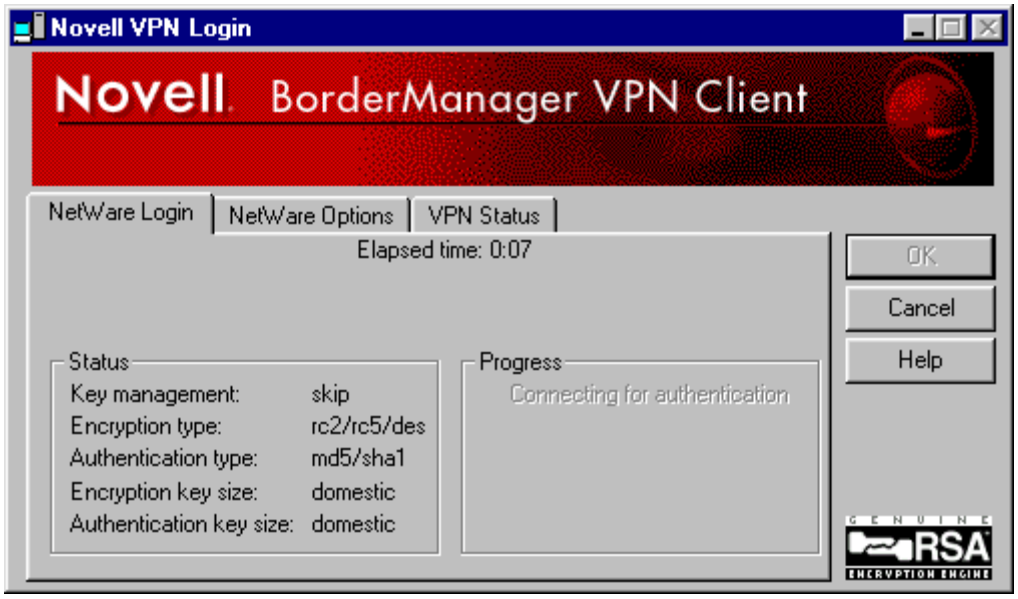


The example given above shows the LAN VPN client settings for NetWare Login. Note that I attempted to connect to the BorderManager 3.0 server at IP address 4.3.2.254. My PC was connected to a hub on the 4.3.2.0 network for test purposes. (It is a good idea to test with a PC connected directly to the BorderManager server at first. This rules out issues that might be related to problems at your ISP.)



These are the **NetWare Options** settings I tried for the first connection attempt. Only **Enable ipx** was selected, in order to simplify the test.

Note IPX is not an available option with Windows 2000 or Windows XP.



After you select **OK** to start the VPN connection process, the VPN client status box is shown.

Now came the first (of several) problems to solve. I was unable to connect to the VPN server, receiving a "Failed to connect to the authentication gateway" error message from the VPN client.

My thoughts for troubleshooting here were:

1. I was using dynamic NAT on the BORDER1 server, and did not disable NAT Implicit Filtering (or SET NAT DYNAMIC MODE TO PASS THRU=ON, which is the same as disabling NAT Implicit Filtering in INETCFG).
2. BorderManager services were not loaded on BORDER1, or Client-to-Site VPN was not configured.
3. I needed an Authentication Policy and Login Policy Object.
4. I had an IP addressing or routing problem

For number 1, I found that NAT DYNAMIC MODE TO PASS THRU=ON was already set.

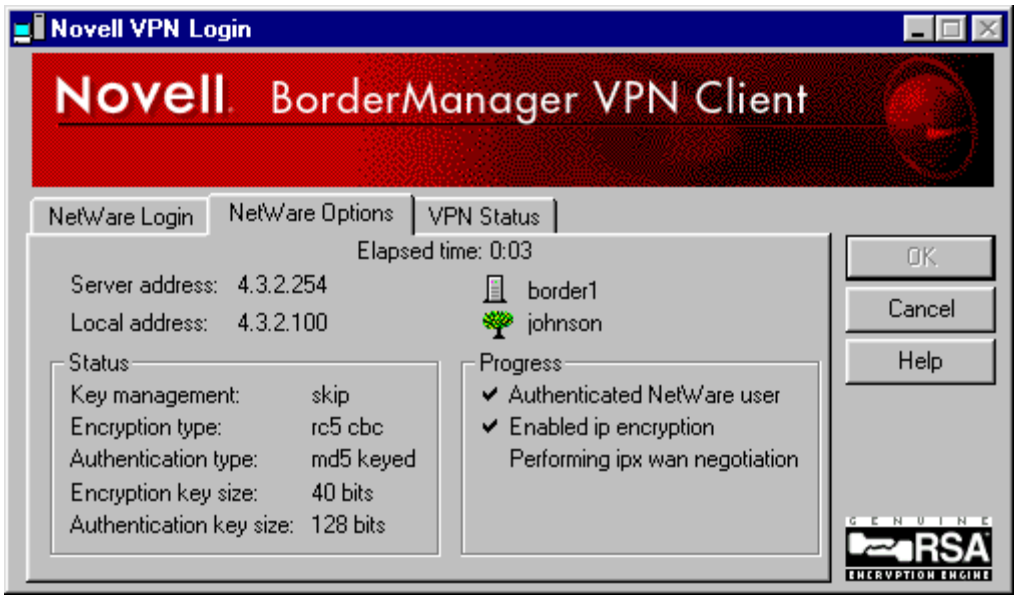
For number 2, I found that BorderManager services were up, running and configured correctly.

For number 3, I ruled out that possibility because I have not seen a Login Policy Object to be required for BorderManager 3.0.

For number 4, I found out that I was using the wrong IP address on the PC! So I changed it to an address on the 4.3.2.0 network. (The same error would have come up if I had entered the wrong IP address for the BorderManager server public interface).

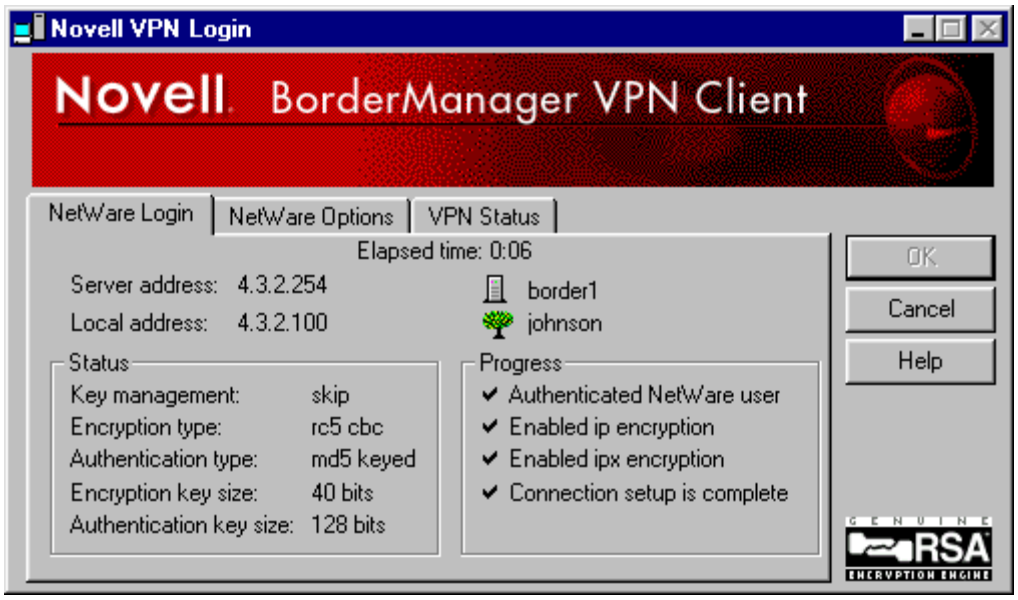
Step 2 – Repeat Test With Valid IP Address

After correcting the IP address problem, I again tried the VPN connection.



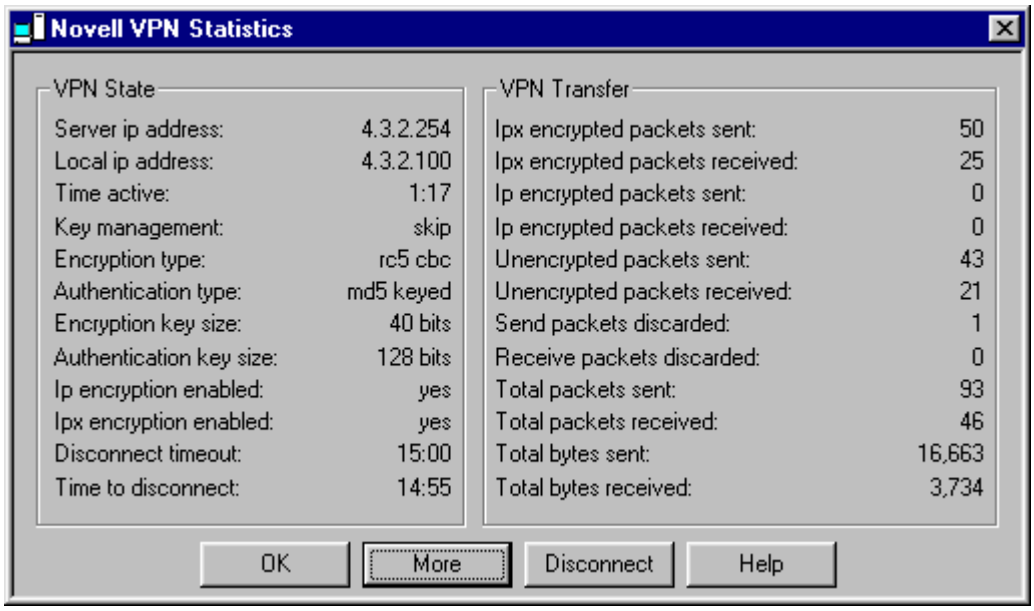
This time I made it a bit farther along, but the VPN client connection stalled at **Performing ipx wan negotiation**.

I did not have a good idea what might be causing this, so I browsed the Novell Knowledgebase at http://support.novell.com. I found a TID that mentioned setting the PC frame type to Auto. Since I had fixed two frame types on my PC, I thought this was an option worth trying. I changed the PC setting to Auto frame type, and rebooted.

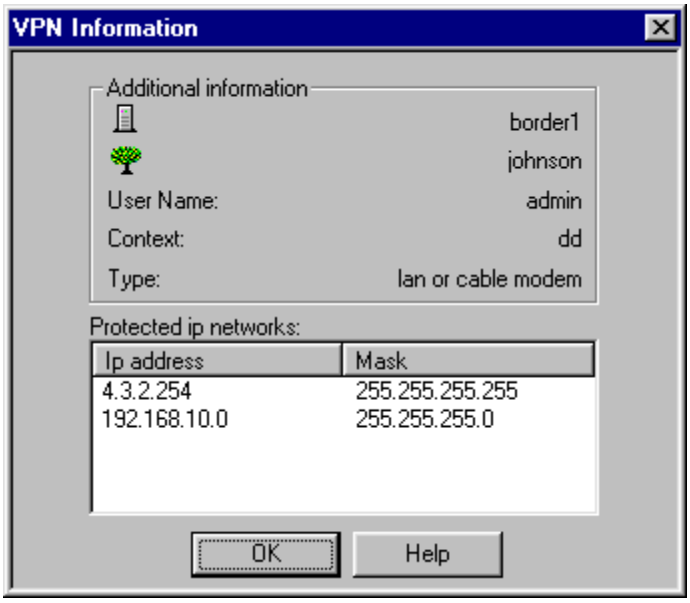


Success! (Or so I thought). With the frame type set to Auto, I was able to connect to the BorderManager 3.0 server and authenticate.

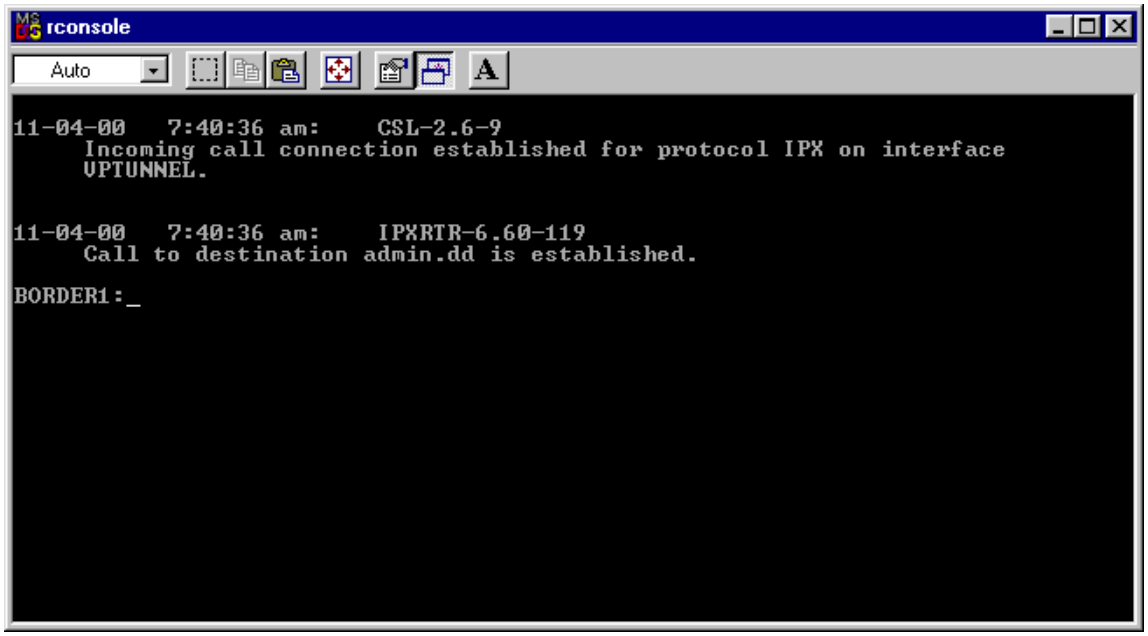
I now had the small VPN client connection icon in the system tray. (Shown above just to the left of the CLNTRUST red key icon).



Clicking on the VPN client connection icon showed the current VPN statistics.



Clicking on **More** within the VPN client connection icon statistics screen showed the IP networks being protected (routed) by the VPN connection.



At the BORDER1 server console, I could also see that I had a successful VPN connection established. (This message only appears if you are making an IPX connection through the VPN).

Thinking I had a working VPN connection, I tried launching Client32 from my PC. However, when I tried to log in, I was unable to find an NDS tree or server.

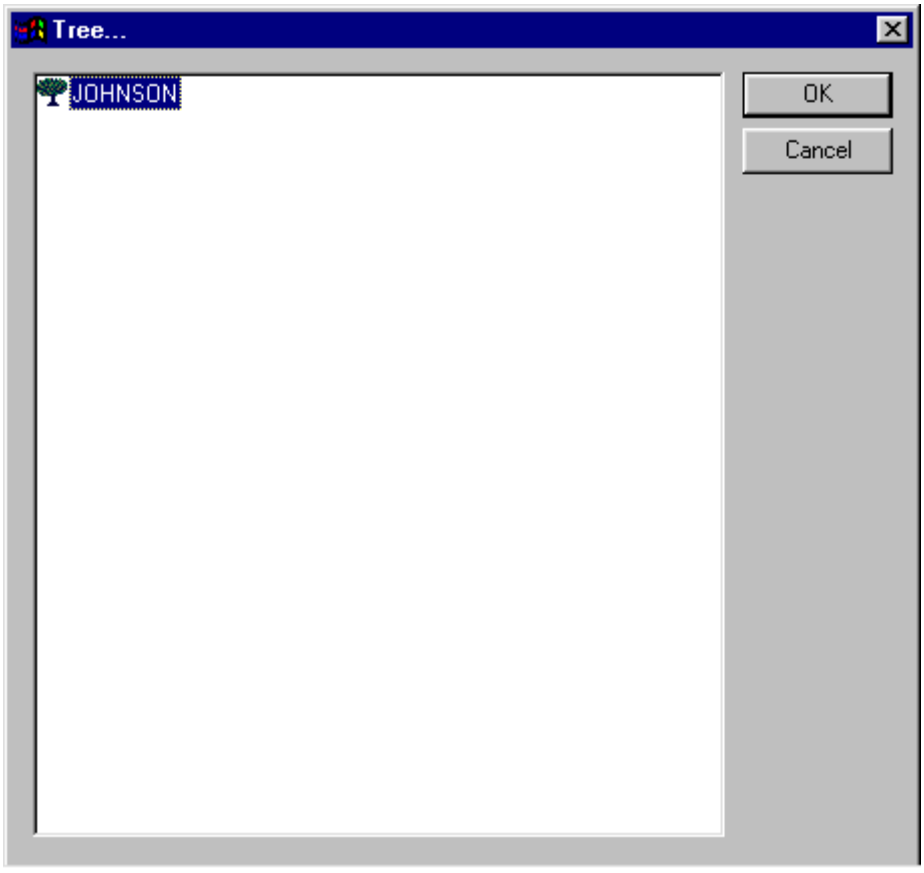
Note The problem with not being able to find an NDS tree or server is very common. There are two main issues here. The first was solved as shown in the next section, where I reinstalled software, but it is essentially related to an IPX VPN connection. The second is a generic name resolution issue for pure IP clients involving SLP issues over Client-to-Site VPN links. The SLP issues are far more common, and typically involve Windows 2000 or Windows XP clients, where there is no IPX support in the Client-to-Site VPN. SLP name resolution issues are discussed later in this chapter.

Step 3 – Install/Reinstall VPN Client Software

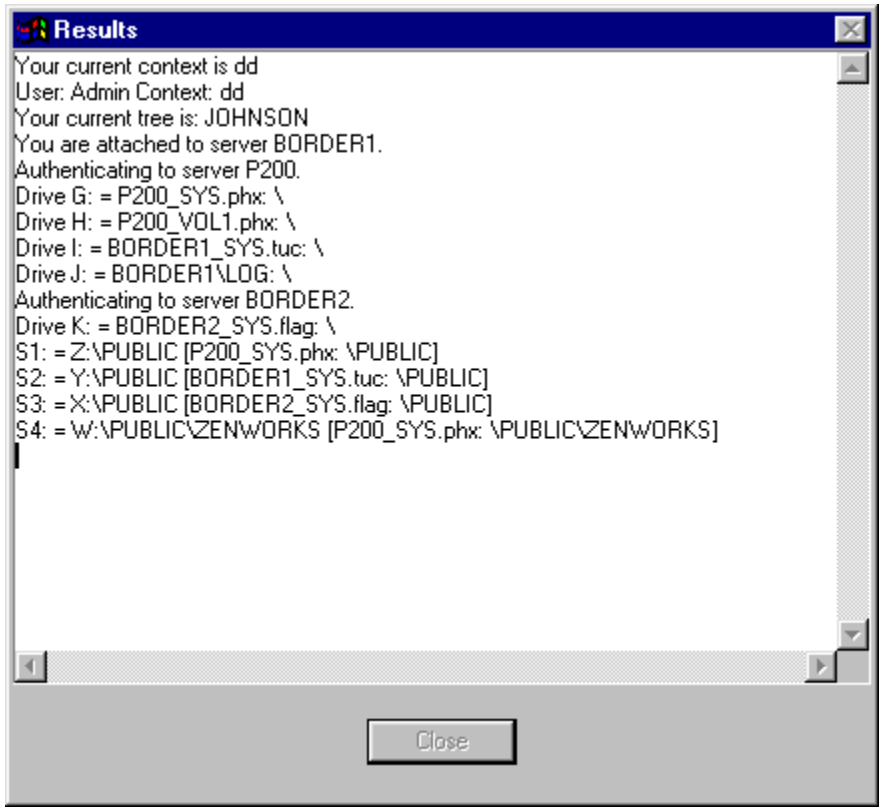
I knew that I might not have had the latest VPN client installed on my PC, and also that my PC had undergone extensive software installation and removal. Figuring that my VPN Client could have been corrupted or obsolete, I elected to reinstall the VPN client.

I reinstalled the VPN client using a version contained in patch BM3VPF08.EXE. (There are much later versions of the VPN client available now). There are certainly later versions available than the versions supplied by a standard (unpatched) BorderManager 3.0 installation!

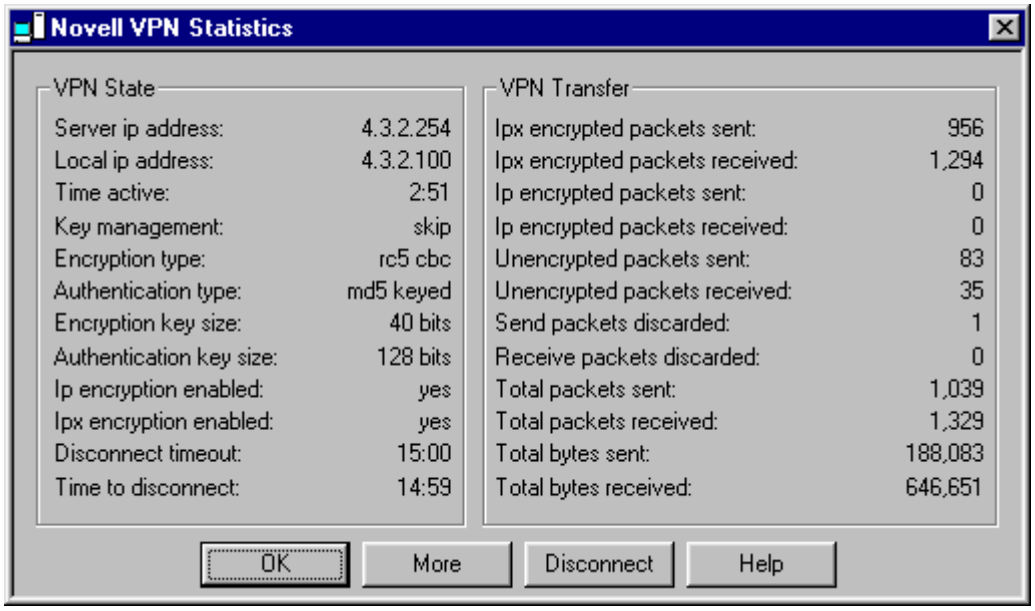
Once again, I launched the VPN client connection and established a VPN connection. I then launched Client32 on my PC, and checked for an NDS tree:



I was able to see my NDS tree after reinstalling the VPN client, and I was able to log in normally.



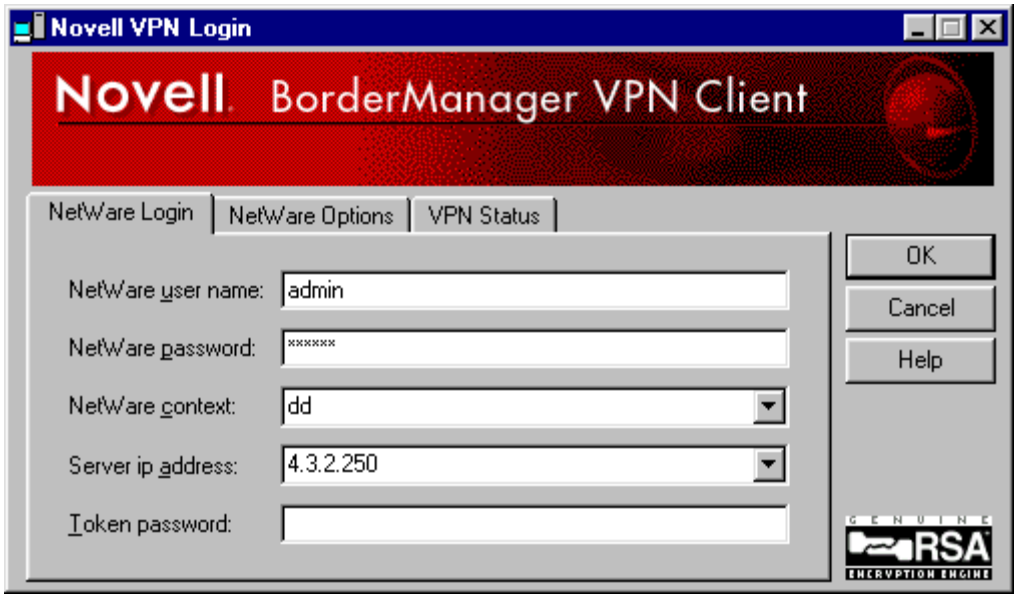
The example above shows my login script running through the Client-to-Site VPN connection.



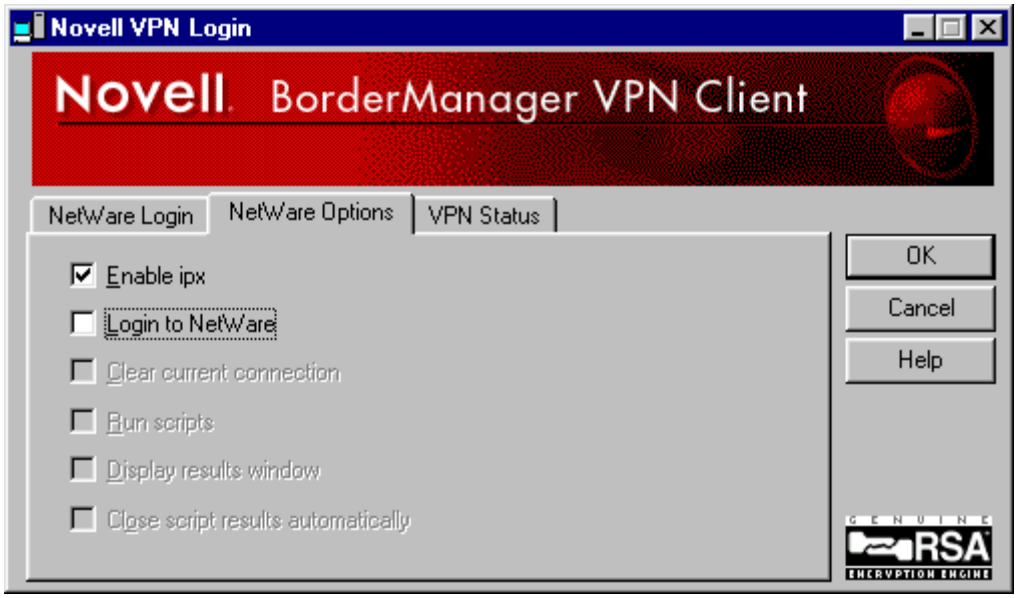
The VPN client connection statistics now showed plenty of encrypted IPX packets sent. Take notice of the **Total bytes received** value – **646,651 bytes**. If this were a slow dial-up connection, I would not have wanted to process the login script as it would have been extremely slow.

Step 4 – Try LAN VPN Client Connection to BORDER2

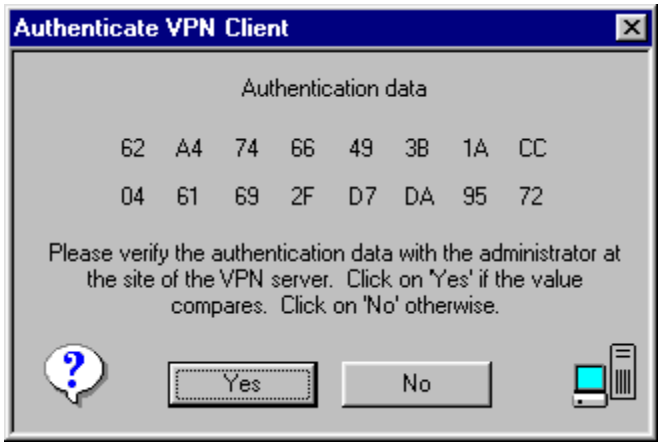
Now that I had successfully performed a Client-to-Site VPN connection to a BorderManager 3.0 server, I attempted to do the same to a BorderManager 3.5 server.



The example given above shows the NetWare Login settings used for the VPN client connection to BORDER2. The **Server IP address** was changed to the public IP address of the BORDER2 server: **4.3.2.250**.



Once again, I simplified the testing procedure by reducing the NetWare Options to the minimum. Only **Enable ipx** was selected.



When I began the VPN connection process, I immediately got a message digest display allowing me to verify that I was connecting to the correct VPN server. If the system administrator had provided the message digest information to me ahead of time, I would be able to check the values of the Authentication Data shown to the values supplied by the system administrator. (In my case, there could be no other server since I was on an isolated test network.)

Note I did not receive the same display in the test to BORDER1 only because I had previously tested a VPN connection to that server and accepted the Authentication Data. You should always get an Authentication Data displayed the first time you connect to a BorderManager VPN server.

I clicked on the **Yes** button to proceed to the authentication procedure.

A new problem was seen that did not exist for the BorderManager 3.0 server connection. My authentication was rejected because no authenticate policy was configured to allow my VPN access.

An investigation of the problem at the Novell Knowledgebase at http://support.novell.com indicated conflicting information. Some TID's claimed that a Login Policy might be required, while others claimed the opposite.

I know from experience that if you get the error message shown above, you either need to do one of the following:

If **not** using token authentication, delete the Login Policy Object (if one exists) and delete a file called LPOCACHE.DAT on the BorderManager server in the SYS:SYSTEM directory. I do not recommend this, especially with BorderManager 3.6 or later. Better to use the following steps to configure a Login Policy Object and be done with it.

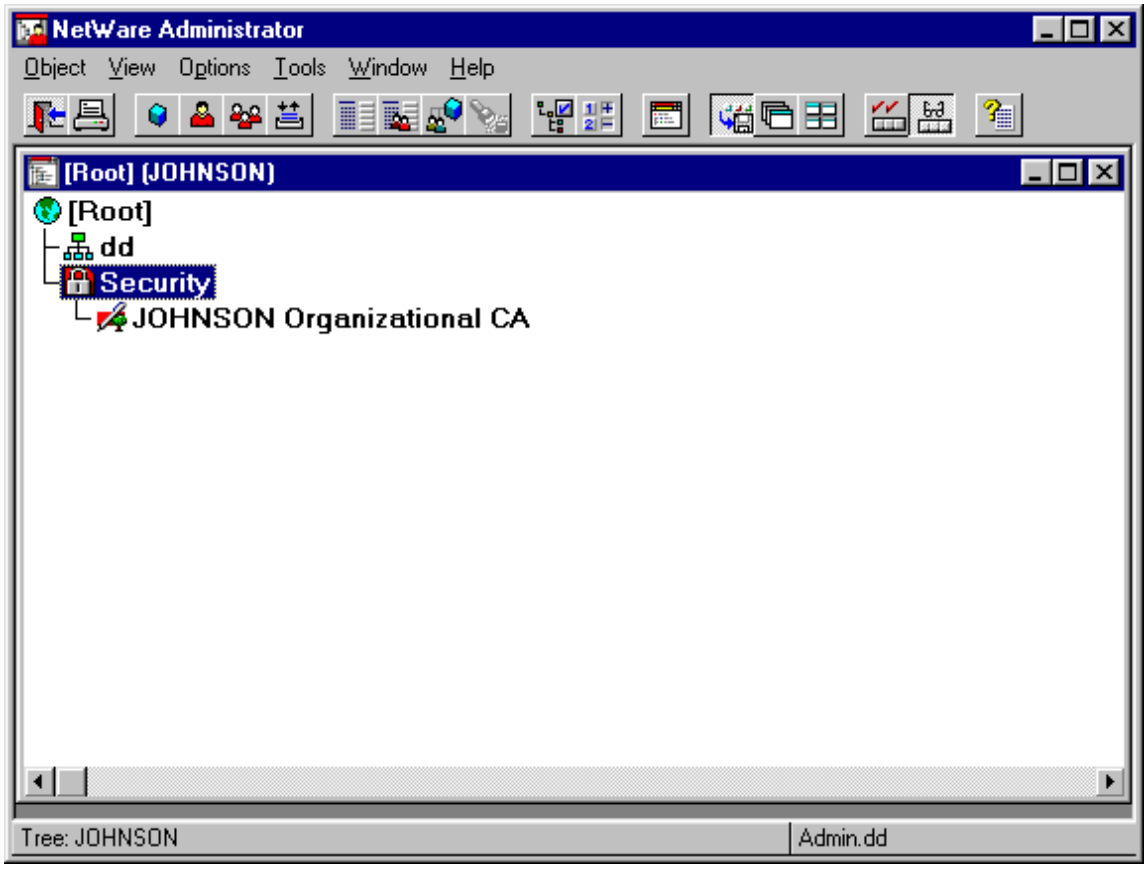
If you do want to use token authentication, you may need to first create a Login Policy Object, and within the Login Policy Object you must create an Authentication Method for VPN.

Note Important! Most people having the problem shown here should be able to simply delete any existing LPOCACHE.DAT files they find rather than go through the exercise shown next to set up a Login Policy Object. However, I recommend configuring an LPO, as it is used in many newer NetWare features, and you might as well just solve the root issue.

Step 5 – Create a Login Policy Object

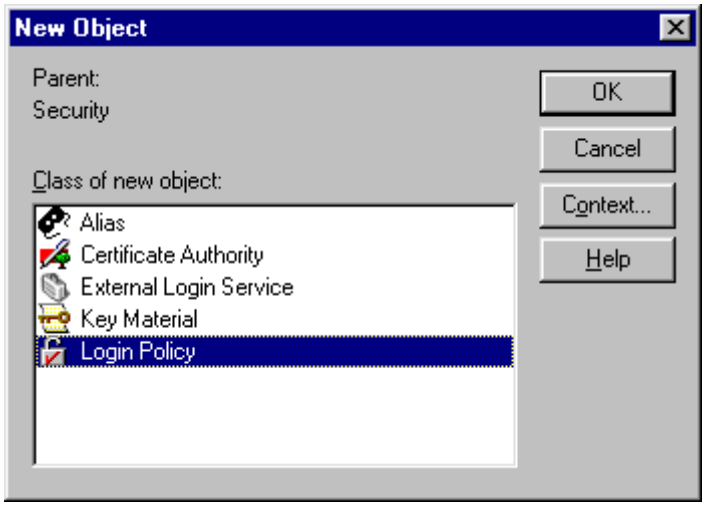
In order to create the Login Policy Object, you must launch NWADMN32 from a BorderManager 3.5 or later server in order to have the correct snapins. (The snapin required is called PKISNAP.DLL)

Note You cannot create the BorderManager login policy object rules with ConsoleOne snapins. You must use NWADMN32, with the PKISNAP.DLL snapin.

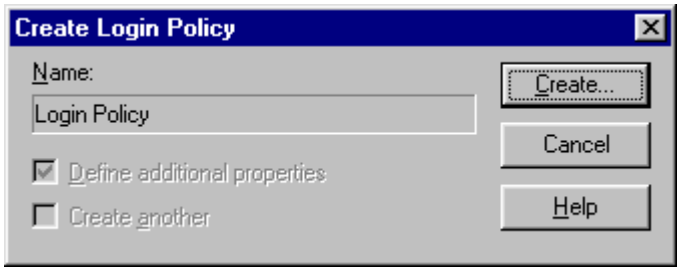


I launched NWADMN32 from the BORDER2 server, and opened the **Security** container. Note the absence of a Login Policy Object.

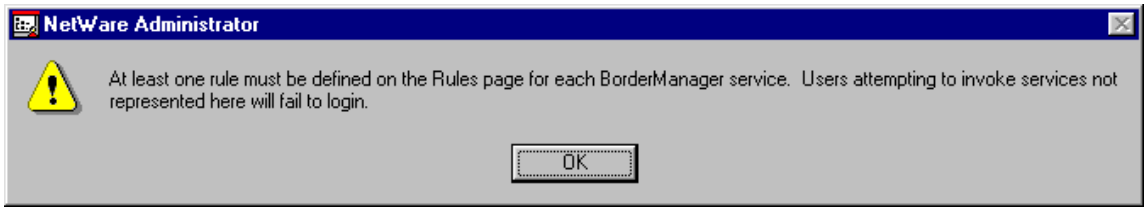
I pressed **Insert** to create a new object in the Security Container.



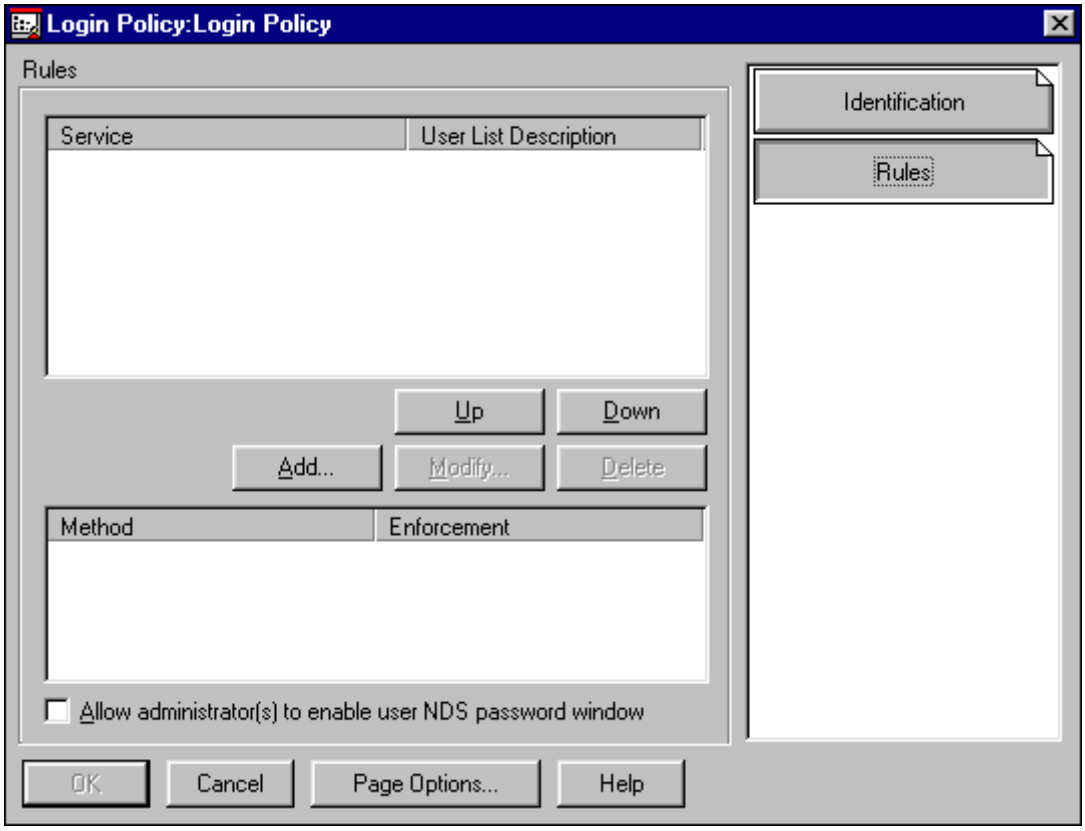
You now have to select **Login Policy Object**. If you do not have this option, you have the wrong snapins or the snapins required are missing. (You need PKISNAP.DLL, dated Feb 18, 1999).



Click on the **Create** button.



Once you create a Login Policy Object, you can no longer use certain BorderManager services without creating a Rule inside the Login Policy object. In this case, a Rule must be created for VPN authentication.



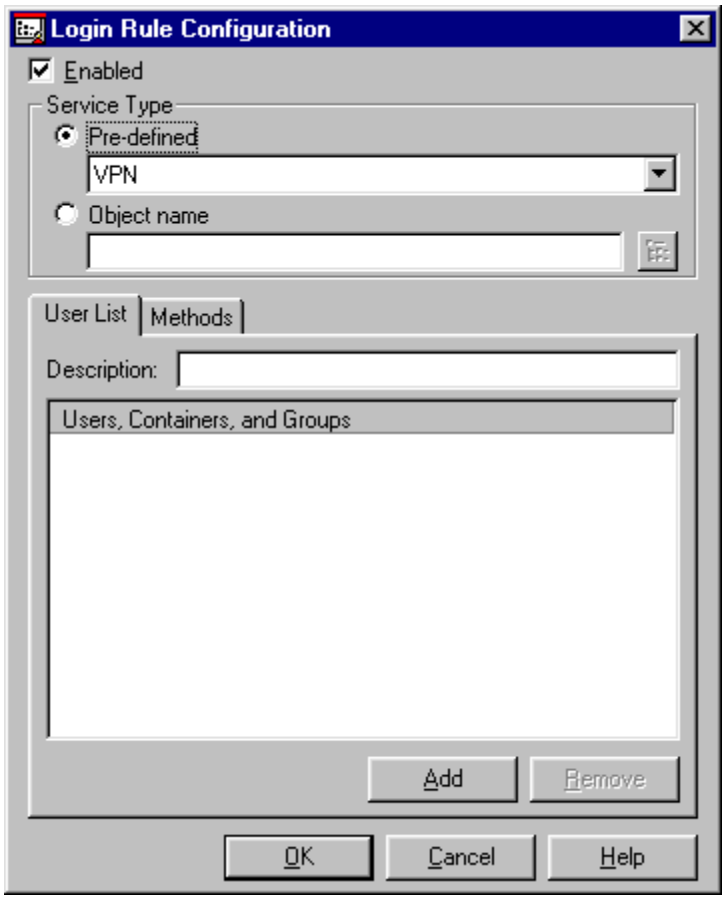
The initial Login Policy Object will not show any rules. You must now add a rule for VPN authentication.

Step 6 – Add Rule for VPN Authentication

Once you have created a Login Policy Object, I had to add a rule to enable VPN Authentication. This rule is different from an Access Rule, though an Access Rule is also required.

Other rules that can be created in the Login Policy object cover RADIUS, ActivCard and Dial services authentication, none of which are covered in this book. If NMAS is installed, many more policies can be configured.

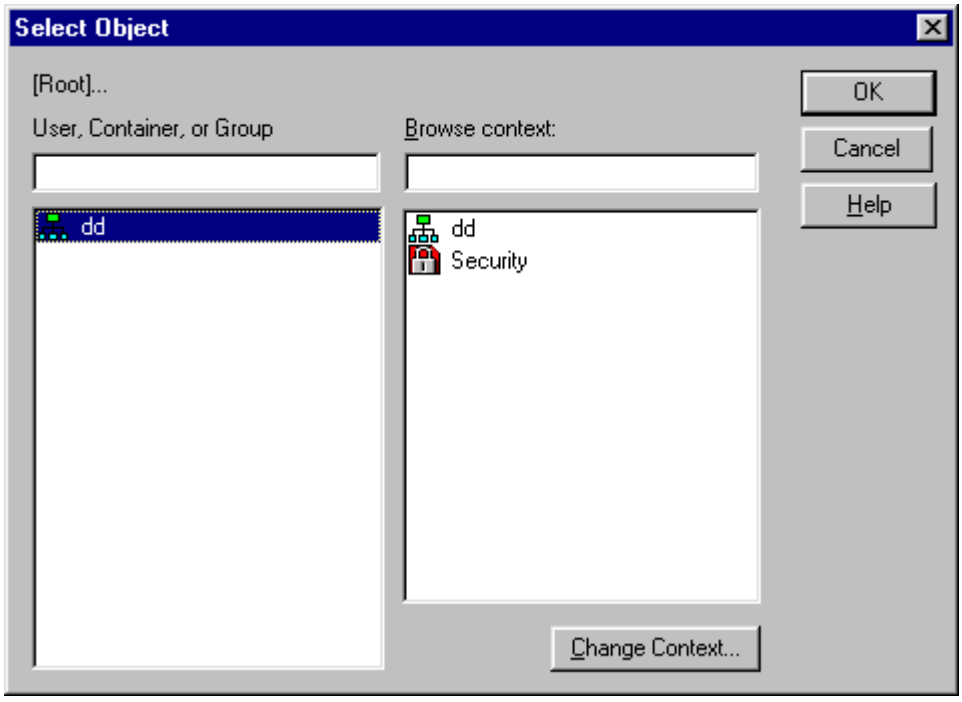
You click on the Login Policy Object to open it. Select the **Rule** tab, and then click on the **Add** button to begin creating an authentication rule for VPN access.



The **Enabled** field should be checked.

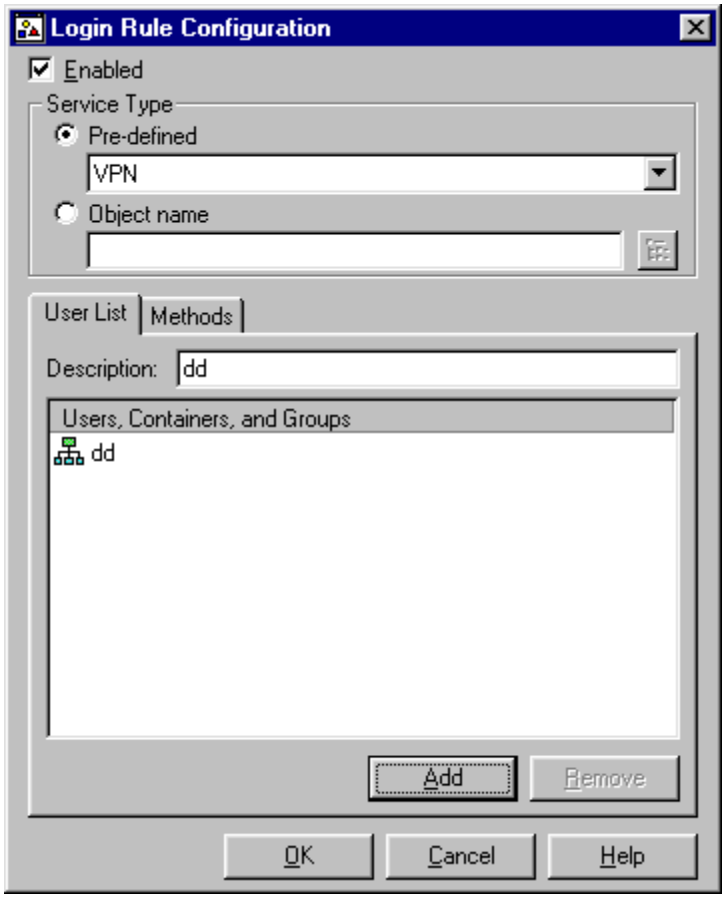
In the **Service Type** field, select **Pre-defined**, and select **VPN** from the drop-down list.

Click on **Add** to select users, groups or containers that the rule will apply to.



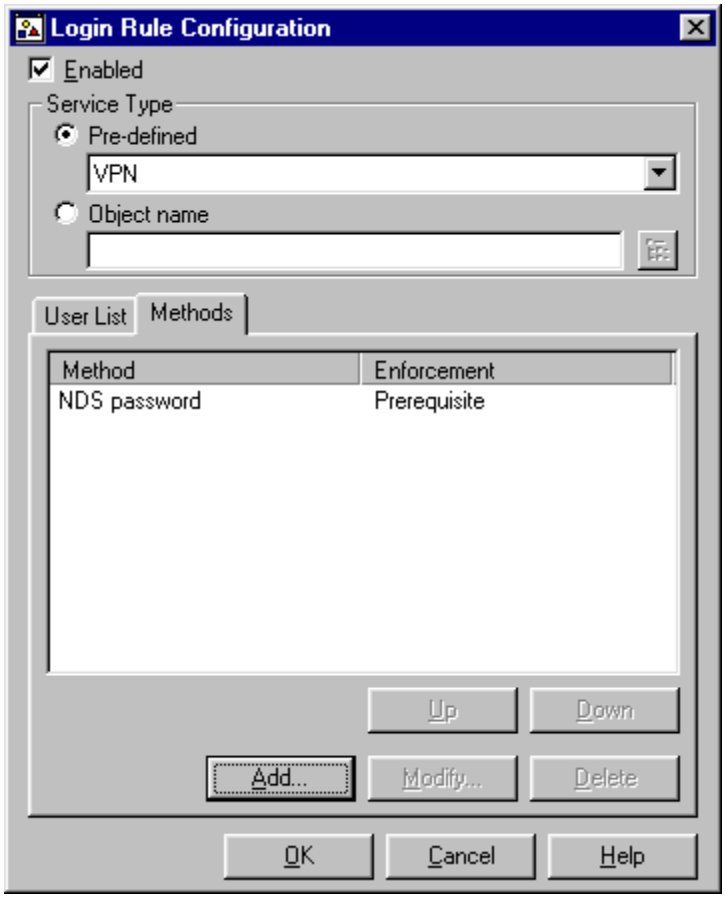
I wanted the VPN authentication to apply to the entire organization, so I selected the **DD container** at the top of my NDS tree.

Click on **OK** to accept the suggestion.



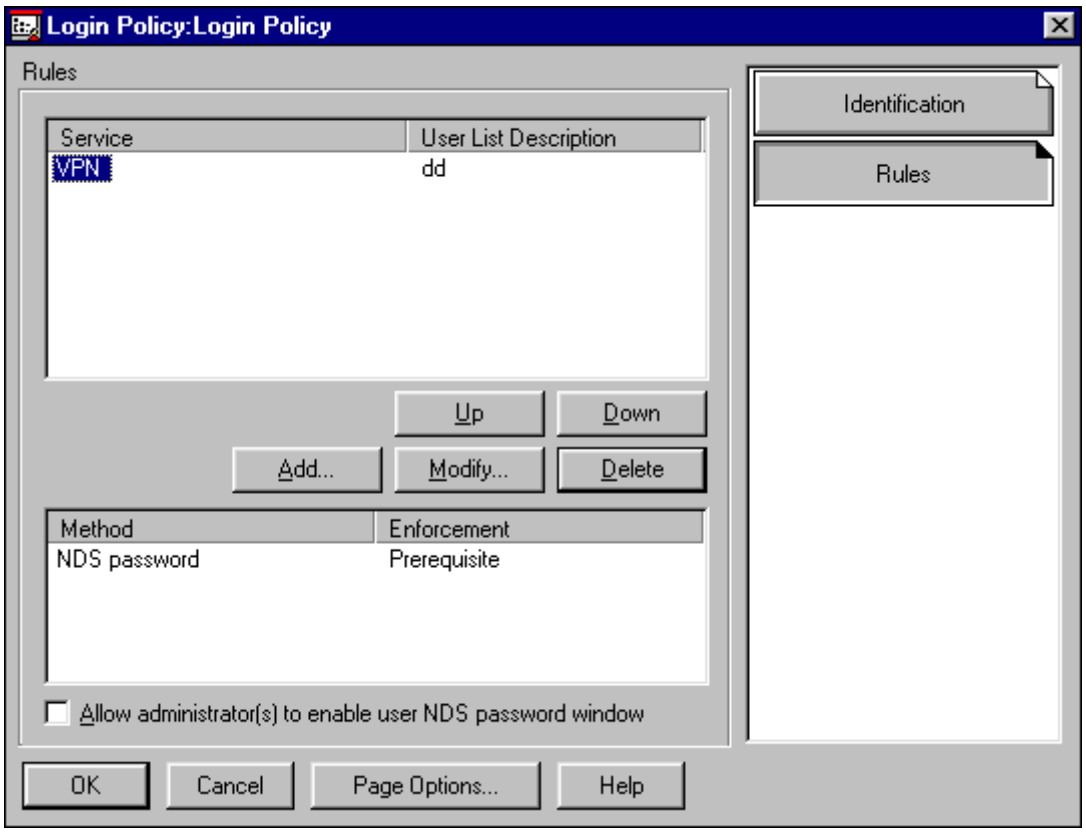
Now there is an entry in the **User List** for the DD container.

The next step is to select a Method, by clicking on the **Methods** button.



There should be a pre-defined method for using the NDS password to authenticate for the VPN rule.

Click on **OK** to proceed.



There is now a valid rule for VPN authentication in the Login Policy Object. Selecting **OK** saves the rule.

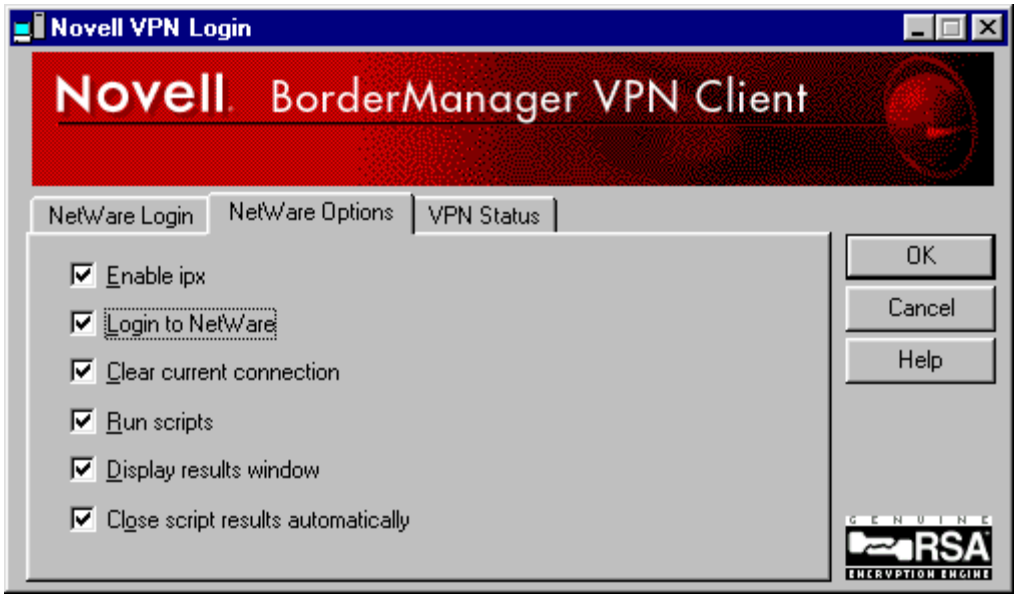
A message appears indicating that NDS rights are being assigned to all objects in the DD container to use the Login Policy Object. Clicking on **OK** completes the configuration procedure for the VPN authentication within the Login Policy Object.

The Client-to-Site VPN connection should now work for BorderManager 3.5, 3.6 or 3.7.

Step 7 – Try LAN VPN Client Connection to BORDER2 Again

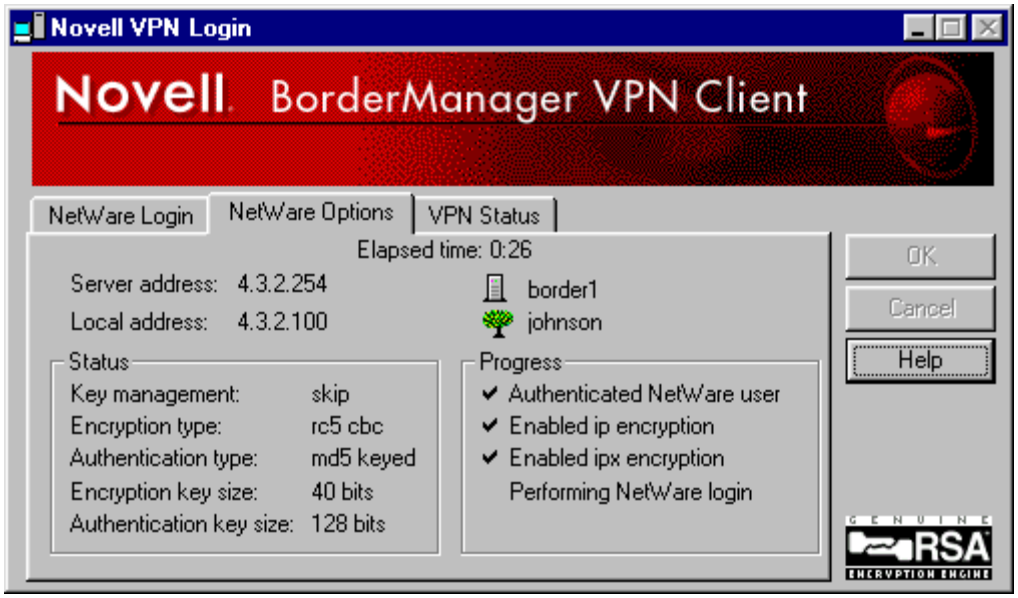
Now that a VPN authentication rule exists in the Login Policy Object, I was ready to try another Client-to-Site VPN connection test. Once again, I used a simple test, with only Enable IPX checked in the NetWare Login settings on the VPN client.

In my first test, I was able to connect to the BORDER2 server. I then was able to launch Client32 and log in to the BORDER2 server.



I next tried to use all of the NetWare Options in the VPN client settings.

To my surprise, I once again started getting an error message indicating that I an authentication policy needed to be configured to allow me to use the VPN!



To make a long story short, I ultimately had to **reboot** the BORDER2 server, after which it consistently allowed me to log in through the VPN connection.

Over this 10Mbps LAN connection to the server, the total time for me to establish the VPN connection, and run the entire login script, which included launching the ZENworks Application Explorer, was 49 seconds.

Client-to-Site VPN Using Pure IP Login

This section describes some issues related to using pure IP communications over a Client-to-Site VPN connection. The issues that come up will primarily consist of routing issues and name resolution (service location) issues.

Note Windows 2000 and Windows XP do not support IPX over Client-to-Site VPN.

Routing Issues

Pure IP communications to NetWare servers requires that the servers are either NetWare 5.x/6.x servers or NetWare 4.11 servers using the SCMD.NLM, coupled with a Novell Client32 installation using IP and IPX Compatibility Mode. The SCMD (server compatibility mode driver) module provides a means of encapsulating or de-encapsulating IPX packets inside of IP packets. **I was never able to configure a Client-Site VPN to work with SCMD**, and I do not think it is possible. This book will assume that if you are going to access NetWare 3.x and 4.x servers over your VPN connection, you will enable IPX on the VPN, and use a remote client that supports IPX over VPN (not Windows 2000 or XP).

Missing Default Route on Internal Hosts and Routers

In terms of connecting to NetWare 5.x/6.x servers using pure IP, one of the biggest issues found is either an incorrect or missing default route on the server or intervening routers. Even if the NetWare 5 .x/6.x servers have a proper default route, there are almost always issues with service location for logging in or mapping drive letters to them.

IP packets coming to internal hosts over a Novell legacy Client-to-Site VPN connection will have a source IP address of the remote client's public IP address. This means that the packets will appear to have come from the Internet. This means that the internal hosts will not know a route back to the remote client, and therefore the hosts must send the packet to a default route (or default gateway) entry. The default route must be present for ANY internal host to be accessed by TCP/IP, not just NetWare servers, including any intervening routers.

The classic symptom of a missing default route on a host in this case would be failure to send a return packet. If you use SET TCP IP DEBUG=1 on an internal NetWare 4.x/5.x/6.x server and ping it from a VPN connection, at the server console you would see ICMP

packets received, but no responses being sent. If the default route was missing (or incorrect) at some intervening router on the internal network, you would see responses sent, but those responses would never get back to the BorderManager server.

In most case, you would need to ensure that a default route (default gateway on PC's) is set, and that it points back through the BorderManager VPN server.

Incorrect Default Route on Internal Hosts and Routers

This is actually somewhat of a misleading heading. The default route may be perfectly fine, except for the VPN connection. If the default route is simply wrong on some host or router, then fix it. However, there is often a case where the default route MUST be set the way it is, because the normal path to the Internet is through a different host than the BorderManager VPN server.

In this case, you have a very limited option. The only way to get the Client-to-Site VPN to work is to have it set up as a **dedicated** Client-to-Site VPN server, and use dynamic NAT on the **internal** (private) IP address.

What happens in these cases is that packets get sent in through the VPN connection and are routed to the internal host. However, the return packets are sent back on a different path, and either never get back to the remote client, or worse, come back unencrypted. This is purely a routing issue due to default route concerns, and can be overcome with dynamic NAT.

If dynamic NAT is used on the private IP address of the BorderManager VPN server, all incoming Client-to-Site VPN traffic will be translated to have the BorderManager private IP address. Therefore, when the packets show up at the internal host, the internal host thinks they came from another internal host. The routing tables of any routers on the network between the BorderManager server and the internal host should have a route back to the BorderManager server. (If you can ping the BorderManager server private IP address from the internal host, you should be fine).

CAUTION *Using dynamic NAT on the private IP address of a BorderManager server should be done ONLY when the server is used as a dedicated Client-to-Site VPN server.*

Missing Encrypted Network on VPN Server

When setting up Client-to-Site VPN servers, you are prompted to enter protected networks. This option defines what internal hosts or subnets will be able to respond to the VPN requests. By default, Client-to-Site VPN is configured to 'Encrypt All Networks', which

should allow all internal traffic. (That option also results in ALL traffic from the remote client being sent through the encrypted VPN tunnel to the BorderManager server, and should be changed to Encrypt Only Networks Listed Below). If you have Client-to-Site VPN configured to encrypt only the networks listed, be sure you included the network or IP address of the host you are trying to access.

Issues with Client-to-Site over Site-to-Site Links

Larger networks using Site-to-Site VPN links, with Client-to-Site VPN capability at remote offices are likely to run into a routing / filtering issue. You will find Client-to-Site connections to one office cannot communicate over IP to any sites on the other side of a Site-to-Site WAN link. (The exception would be if a dedicated Client-to-Site server is being used that has dynamic NAT enabled on the internal IP address).

This issue is caused by the source IP address of the remote host packets. Incoming packets from the remote VPN client will have that client's public IP address as a source. As long as these packets stay within the local network, response packets will go to the default gateway (Client-to-Site VPN server), be encrypted and sent back to the remote host. However, when these packets are sent to another site across a Site-to-Site VPN link, they will appear to be packets trying to be routed to the Internet past the filters, and the filters will discard them. The reason is that the Site-to-Site VPN only 'protects' packets with a source IP address as configured in the VPN settings in NWADMN32. In other words, since the packet is seen as not coming from a host on a protected network, it is not sent through the (Site-to-Site) VPN tunnel.

There is little that can be done about this issue, other than to use a dedicated Client-to-Site VPN server with dynamic NAT enabled on the private IP binding. Such a configuration will force packets coming into the LAN from a remote VPN host to have an internal IP address, which should make the packets fully routable within the internal LAN. However, running dynamic NAT on the private interface will prevent most outbound communications, meaning that the server should be used only for Client-to-Site VPN.

A work-around is to make a 'local' Client-to-Site VPN connection to the office holding the servers that need to be accessed via IP protocol. In other words, make a Client-to-Site VPN connection to office 'A' if you want to access a server at office 'A', and make another Client-to-Site VPN connection to office 'B' if you want to access a server at office 'B'.

Note The problem above has been observed on my master VPN BorderManager 3.5 and 3.6 test servers, but not on my slave BorderManager 3.0 or 3.5 test servers. The slave test servers simply do not seem to forward the packets across the Site-to-Site VPN link at all. You may see either behavior in your environment, but the problem remains that traffic does not cross the Site-to-Site VPN link.

Issue with BorderManager 3.5 and 3.6 with Client-to-Site VPN and Dynamic NAT

Both BorderManager 3.5, 3.6 and 3.7 often do not let a VPN client access the private IP address of the VPN server if dynamic NAT is enabled on the public binding. (Strictly speaking, this is a NAT problem that tends to show up on BorderManager 3.5, 3.6 or 3.7, and some versions of NAT sometimes do not have the problem). To access the private IP address of the VPN server, add a static NAT mapping of the private IP address to itself on the BorderManager 3.5, 3.6 or 3.7 Client-to-Site VPN server. Afterwards, you should be able to access the private IP address over a VPN connection.

Name Resolution (Service Location) Issues

Using Pure IP communications to access NetWare 5.x/6.x servers over Client-to-Site VPN connections typically runs into name resolution (service location) issues. Because IPX is not being used, a different method of discovering NetWare services must be implemented. That method is normally SLP (Service Location Protocol), which usually works fine on an internal network. Setting up SLP is not within the scope of this book, but discussing the known problems and work-arounds is.

Making Use of SLP

The first issue is that SLP doesn't work automatically over a Client-to-Site VPN connection. Normally, multicast communications or unicast communications to and from the servers themselves or a Directory Agent is used on an internal LAN. Neither works over a Client-to-Site VPN connection without some special configuration being done, and even then, SLP does not work right away.

If you can log in to NetWare 5.x/6.x servers over the VPN connection, but only by using the server's IP address instead of the server name, then you have a service location issue.

The 'standard way' of making use of SLP over a Client-to-Site VPN is set up the remote Novell Client with a static entry for a Directory Agent so the Client can use unicast TCP/IP packets to query for services. Unfortunately, the Novell Client, up through at least version 3.3 for Win9x and 4.8 for NT, only makes an immediate

query for a Directory Agent when the Client32 software initializes. After that, periodic queries for the Directory Agent are done every five minutes. (Later versions of the Novell VPN client cause the SLPDA to be queried more often). What this means for the Client-to-Site VPN connection is that you may have to wait up to five minutes before the remote host contacts the Directory Agent and service location information gets to the remote host.

Note The latest VPN client, available for Windows 98 and later versions of Windows, in the BM37VPN2.EXE file (or later) has made improvements on how SLP functions with Client-to-Site VPN. If you are trying to get SLP to work with Client-to-Site VPN, it is essential to try the latest VPN client. As of this writing (October, 2003), the latest client is contained in the BM37VPN4.EXE patch. This client version also is the first VPN client to support the Intel Centrino chipset in newer laptops.

You can test the SLP Directory Agent response by using the SLPINFO.BAT file in the NOVELL\CLIENT32 directory. As long as the Directory Agent has not been queried, it will come back as 'unresponsive'. After some time elapses, SLPINFO should show the state changing to something else (such as 'unverified'), at which time a login using server names should work.

Using NWHOST Instead Of (Or In Addition To) SLP (Win9x Only)

Since most people don't really like waiting for up to five minutes for service location information to trickle into their PC in order to log in or authenticate to servers, map drives, etc, you may want supplement the SLP system with at least some locally-stored service location information. Specifically, you can configure the NDS tree and NetWare 5.x/6.x servers in the remote PC's NWHOST file, and the Novell Client32 will (if configured normally) make use of those entries.

The NWHOST file is contained in the C:\NOVELL\CLIENT32 directory. You should find a sample there with comments in it explaining how to add entries to the file.

Windows 9X PC's use the NWHOST file in the C:\NOVELL\CLIENT32 directory. Windows NT PC's look for it in the WINNT\SYSTEM32\DRIVERS\ETC directory.

You can add two types of entries in the NWHOST file: NDS tree names and server names. The NDS tree name should point to the IP address of the nearest NetWare 5.x/6.x server in that tree to the BorderManager VPN server. This will usually be the BorderManager server itself.

The format of the NWHOST entries is <name> <IP address>, with the entries separated by at least one space, and only one entry per line. A sample is shown below.

```
JOHNSON     192.168.10.250
ZEN01       192.168.10.250
BORDER1     192.168.10.252
```

The NDS tree name in this example is JOHNSON, and it points to the private IP address of the ZEN01 server. The other entries are server names.

With the NWHOST entries in place, the login process no longer runs into a 'Tree not found' or 'server cannot be located' error in the login script. All necessary information to locate the services is contained at the remote PC.

Using the HOSTS File (All Windows Platforms)

You may also add the internal IP addresses and server names in the local PC's HOSTS file. This file is usually located in:

- C:\WINDOWS\HOSTS on Win9x
- C:\WINNT\SYSTEM32\DRIVERS\ETC on NT 4.0
- C:\WINDOWS\SYSTEM32\DRIVES\ETC on Windows XP

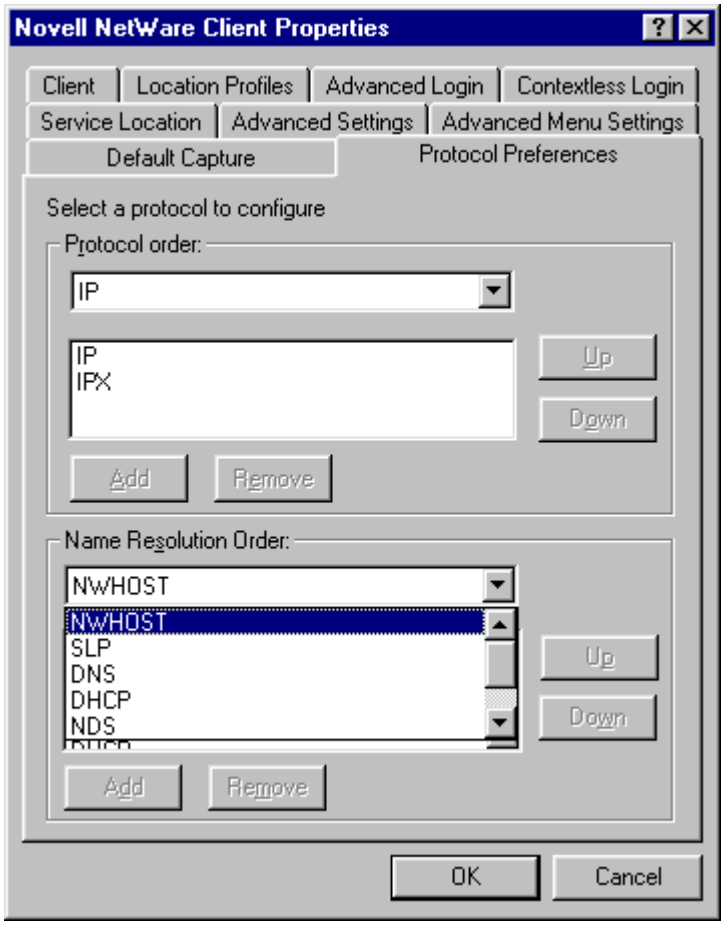
The use of the HOSTS file is basically the same as using the NWHOST file, and you can usually use either method on Win9x. The format is different from NWHOST.

```
192.168.10.250    JOHNSON ZEN01
192.168.10.252    BORDER1
```

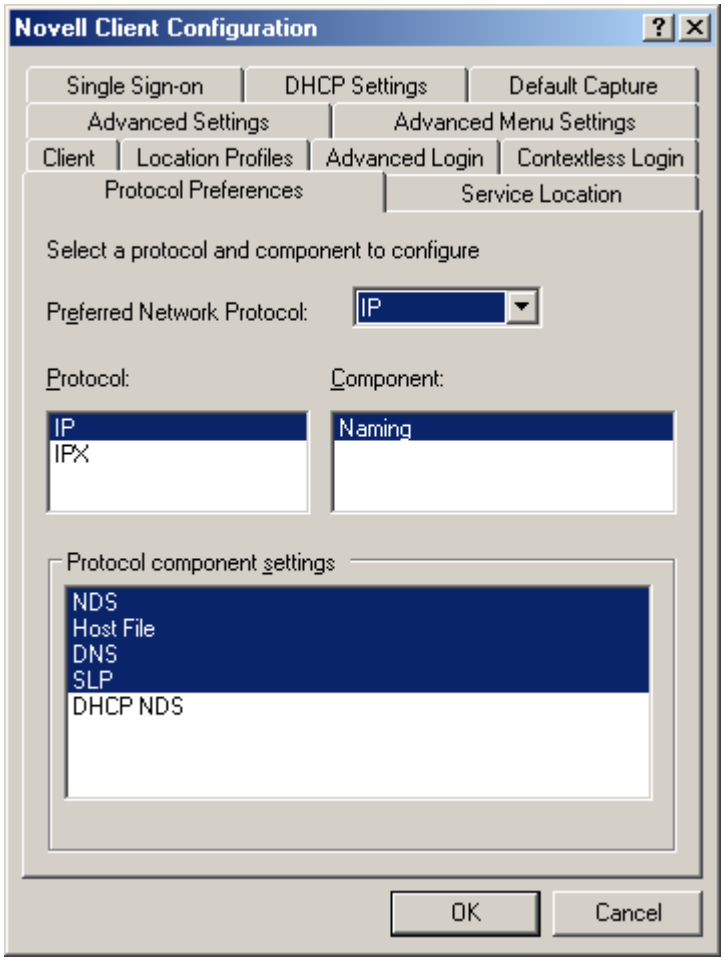
Note that the tree name (JOHNSON) is on the same line as one of the servers (ZEN01)

The Importance of Client32 Protocol Preferences

Whether or not you can use NWHOST, HOSTS, or even SLP depends on the settings you have for Client32 Protocol Preferences.



In the figure shown above, Client32 (for Windows 9x in this case) is set to use all possible methods under the **Name Resolution Order** menu. NWHOST has been configured at the top of the list so entries found in the NWHOST file will be used before any other method. Following that, SLP will be used, and following that DNS (which should include the HOSTS file). If you do not have an NWHOST entry, your NWHOST file will not be used. If you do not have a DNS entry, your HOSTS file may not be used.



The screenshot above shows Client32 version 4.83 (Windows 2000 & XP) Protocol Preferences. Service Pack 1 for Client32 4.83 was also installed.

The protocol preference selection methodology in this version of Client32 is rather odd. You must be sure that the selections desired are highlighted! If there is no highlighting, the option is not used. In the example shown, DHCP NDS will not be used for name resolution using the IP protocol.

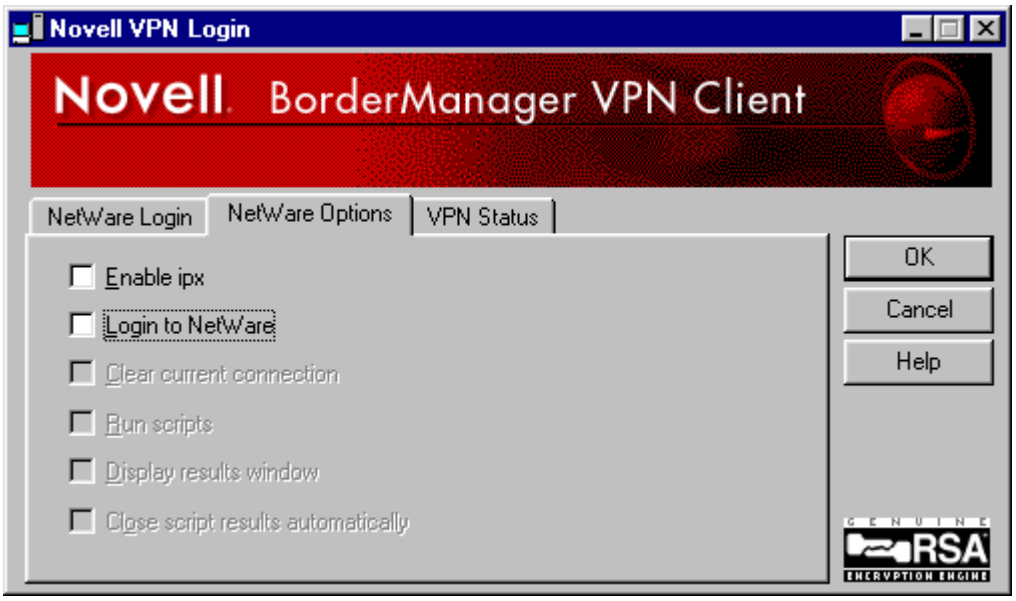
The Bottom Line

Most people will have the best success by **using a HOSTS file** on the local PC configured with all the server names and internal IP addresses of servers called out in the login script.

If the Client-to-Site VPN connection is to a BorderManager 3.5, 3.6 or 3.7 server and dynamic NAT is enabled on the public IP binding, add a static NAT mapping of the private IP address to itself. Otherwise you may not be able to access the private IP address of the BorderManager server.

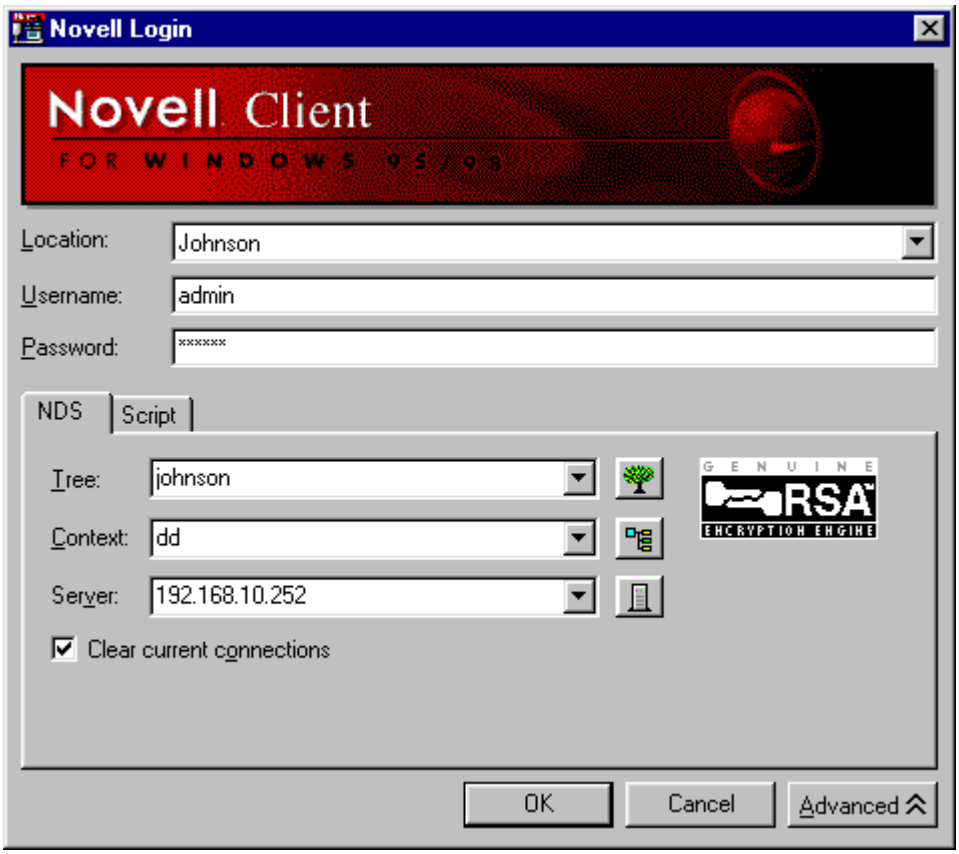
First, make a network connection to the Internet, using Microsoft DUN if necessary, or via a LAN connection (cable modem, DSL, etc.)

Second, make a VPN connection using the LAN VPN client, but do **not** check the Login to NetWare box.



The figure above shows a LAN VPN client set up for a pure IP login. **Enable IPX** is not checked. **Login to NetWare** is not checked.

Third, use the regular Novell Client32, with the internal IP address of a NetWare 5.x/6.x server in place of the server name in the advanced NDS menu.



The figure above shows Novell Client32 set up to log into a NetWare server at 192.168.10.252, once the VPN connection has been established.

A HOSTS file entry for all servers called out in the login script has been set up in the C:\WINDOWS directory. (This is for Windows 9x or XP).

Client-to-Site VPN Over NAT

You may have a remote client that is connected to the Internet through a NAT connection, perhaps via a DSL or Cable Modem connection. *BorderManager 3.0 and 3.5 servers cannot make a Client-to-Site VPN connection to those clients*, but BorderManager 3.6 servers can. The following components must be in place for the Client-to-Site VPN connection to occur:

1. A special version of TCPIP.NLM, included with BorderManager 3.6, must be in use. The version that ships with BorderManager 3.6 is 5.32z, dated August 30, 2000. Any later version with encryption should also work.
2. The latest VPN client software from BorderManager 3.6 must be used. The versions available for download for BorderManager 3.7 and 3.8 will also work to previous versions of BorderManager.
3. The usual default packet filter exceptions are required as before. If the default filters have been configured with BRDCFG.NLM, then the VPN client should work. VPN over NAT capability make particular use of UDP port 2010, so be sure that port is also allowed if you have customized your filter exceptions. (BorderManager 3.7 is a special case here, as some exceptions may have to be added manually in some circumstances. This subject is covered in my book on configuring BorderManager filter exceptions).
4. The ISP and any local router must be allowing UDP and TCP port 353, and UDP port 2010, and not be doing check-summing of the packets.

Note As of this writing, the BorderManager server itself must not be behind a NAT connection. Its public IP address must be a registered public IP address on the Internet. Only BorderManager 3.8 non-legacy VPN supports the BorderManager server being behind a NAT or port-forwarding router.

Disconnecting a Client-to-Site Connection

The VPN client should disconnect from the VPN as follows (for best results).

1. In Network Neighborhood, right-click the NDS tree and select Logout. This will log the user out of the NDS tree.
2. Right-click the VPN client icon in the toolbar and select Disconnect. This will break the VPN connection.

Chapter 19 – BorderManager 3.8 Site-to-Site VPN

This chapter covers the new IPSec-compliant, IKE-based VPN services provided in BorderManager 3.8.

While this chapter may seem quite long at first, there is much that you may not need to read. When setting up the VPN services, iManager will fill in many default values, for certificate names, trusted root objects, and trusted root container. I show examples for creating these objects manually, with both iManager and ConsoleOne, in case you want or need to create the objects yourself. But in the simplest case, where servers are in the same NDS tree and using a shared trusted root container, many of the objects can be automatically created for you. (This means you can possibly skip reading about half of this chapter! So it's not as long as you might think.)

Theory

This is VPN in a nice, short high-level description, in case you are not familiar with how a VPN works. A VPN, which is short for Virtual Private Network, uses encryption technology to secure data running over a public network, like the Internet. Instead of routing packets from point A to point B, the packets are first encrypted with some coding mechanism by one endpoint of a VPN connection. The packet header and the packet data are both encrypted as a unit. The result becomes a data packet that is place inside another IP packet. That packet is then routed to the other end point of a VPN connection.

The VPN connection between two VPN endpoints (where the data is encrypted, and then unencrypted) is called a VPN tunnel. To devices on each side of the tunnel, it looks like a convenient, short routing hop from one network to the other. In fact, the routing cost of the VPN tunnel is deliberately made low (as in '1 hop') so that packets are automatically routed (lowest cost route) through the tunnel by routers on either end of the tunnel.

The encryption and decryption is transparent to all but the VPN endpoints. But anyone intercepting the packets as they travel between the endpoints is not able to decipher the encrypted data.

It should be noted that VPN's are essentially an economic decision, using encryption technology to secure data across a cheap route (the Internet) between endpoints, as compared to setting up a private WAN link. In the past, private WAN links (remember 56k links between offices?) were used, and while they were secure, and reliable, they could be extremely expensive. Internet-based VPN's are as secure as the encryption technology, as reliable as the Internet connectivity between end-points, but generally much, much cheaper than dedicated WAN links. Also, Client-to-Site VPN's have largely replaced dedicated dial-up systems, where a company maintained a bank of modems, and not only had to pay for monthly telephone lines for each modem, but also typically had to pay for long distance charges for traveling employees. Again, a VPN is usually a cheaper alternative, since even if a traveling employee needs a modem connection to the Internet, it may be cheaper to provide a dial-up account to a local ISP than suffer continuous long-distance charges to dedicated phone lines.

Overview

If you are used to the older (legacy) version of BorderManager, this will be very different for you.

BorderManager 3.8 can support the old VPN services, but this chapter concentrates on the new VPN service, which uses IKE key exchange instead of SKIP. The new VPN has numerous features that are not available in the legacy VPN of previous versions of BorderManager. These new features include:

- Compatibility with non-Novell VPN clients and servers, as long as those VPN products are truly IPSec-compatible. That is, you can make a VPN connection between a Cisco VPN client or Cisco router and a BorderManager server now, or a Linux server, or many other VPN products. This chapter shows an example of a Site-to-Site VPN connection with an inexpensive Linksys VPN router.
- The VPN server can be located behind a NAT or port-forwarding router hop and work.
- A form of access rules can be used to restrict both the type of authentication available and the type of traffic allowed through the VPN.
- With Client-Site VPN, IP addresses are assigned to the VPN client, eliminating 99% of the routing issues seen with the legacy VPN. In addition to pushing an IP address to the

remote client, DNS Server and SLP Directory Agent addresses can be pushed at the same time, resolving many name resolution issues as compared to the legacy VPN.

- All VPN configuration is done using iManager 2.0. This is certainly an added complication, in that configuring iManager 2.0 can be complex, but at least the interface is very usable. (Unlike, in my opinion, the iManager interface for configuring filters).
- NMAS, Certificate and LDAP authentication methods are available. This means that there is a tremendously expanded capability to have different methods for authenticating VPN clients, as well as added complexity in getting those methods configured.
- VPN Monitoring is done with Novell Remote Manager (NRM), instead of inside NWADMN32.

This book will show examples only for a small subset of the VPN capabilities available. Specifically, this book will show Site-to-Site VPN between multiple BorderManager 3.8 servers (each in a different NDS tree), and Client-to-Site configuration using the Novell VPN client for BorderManager 3.8. I have also included one example of a Site-to-Site VPN connection to a non-BorderManager server, with a Linksys BEFSX41 router. Both Site-to-Site and Client-to-Site will be shown with one of the servers behind a static NAT (port-forwarding, actually) router hop. Authentication methods shown here include NMAS (NDS password), X.509 Certificate and LDAP (NMAS, with LDAP) methods. Some access rules to restrict the type and destination of VPN traffic will be shown. The following chapter, on monitoring VPN traffic, will show Novell Remote Manager monitoring BorderManager 3.8 VPN traffic.

I have included a chapter on installing and configuring iManager 2.0 (on Windows) for VPN configuration later in this book.

The capability of BorderManager 3.8 VPN is so vast, as compared to the legacy VPN, that I believe it requires a separate book dedicated to the subject, where additional NMAS methods can be shown, as well as non-Novell VPN connections, and additional access rules and troubleshooting information. I plan on writing such a book as soon as possible.

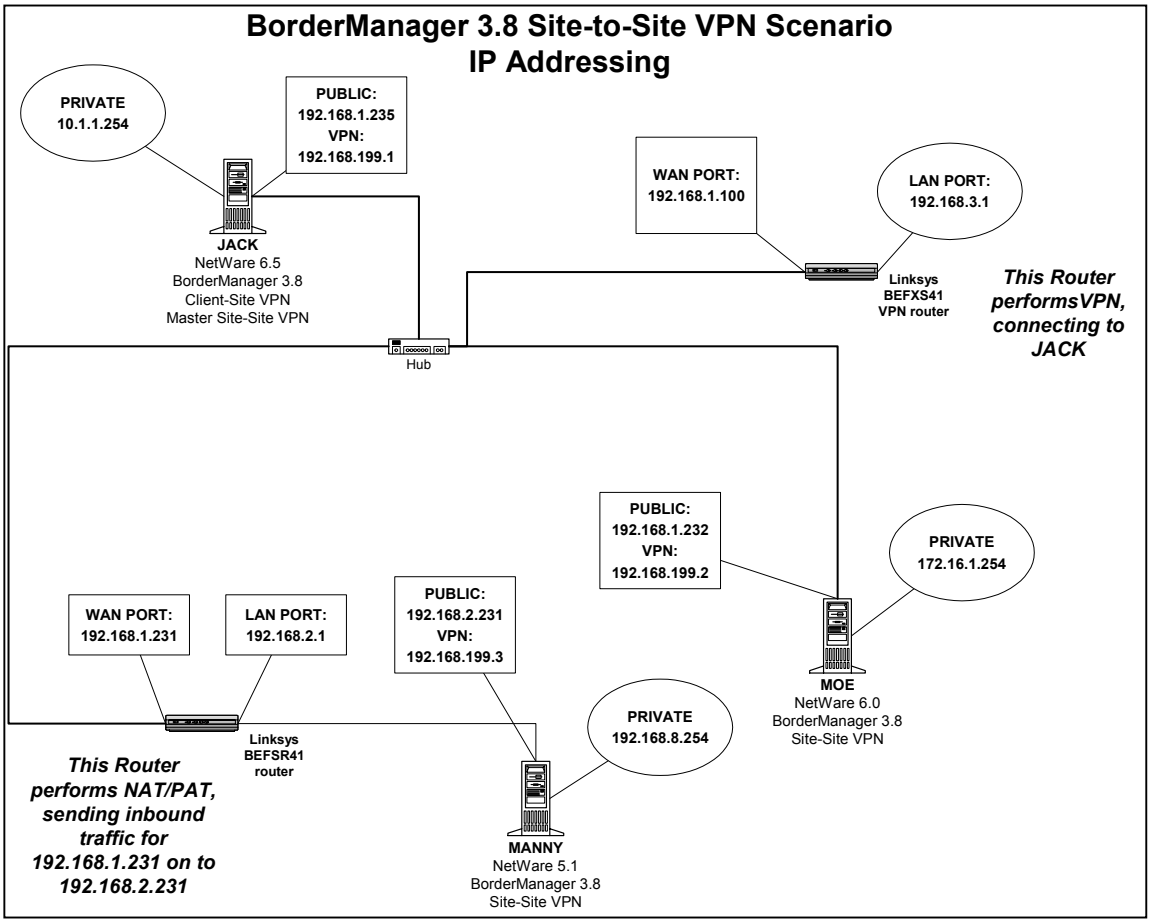
Upgrade Considerations

BorderManager 3.8 will still support earlier BorderManager 3.x VPN servers in a Site-to-Site VPN, but the master VPN server must be a BorderManager 3.8 server. All BorderManager 3.8 slave servers will connect to the master VPN server only in IKE mode, not

legacy mode. You will have to upgrade the existing master VPN server to BorderManager 3.8 first.

You could also set up a new BorderManager 3.8 master server, and begin adding new BorderManager 3.8 slaves to it, replacing the old slave servers one-by-one. In this case, you will lose a fully-meshed VPN configuration during the upgrade transition, but with proper use of static routes, you can maintain network connectivity between old and new VPN systems.

Network Diagram



This graphic shows a network diagram of the test network used in this book. *The reader might get confused by the fact that I did not use actual public network addresses*. Please be aware that the concepts are the same, even if your public IP addresses are really public, and not the 192.168.1.x or 192.168.2.x addresses I show here.

In the diagram above, three BorderManager 3.8 servers are configured in a Site-to-Site VPN. One non-BorderManager VPN router, a Linksys BEFXS41, is also included.

Each server is in a separate NDS tree.

The Master VPN server is JACK, which is a NetWare 6.5 server. JACK is in a NDS tree called REDWOOD. JACK has public IP address 192.168.1.235, and private IP address 10.1.1.254. JACK's VPN tunnel IP address is 192.168.199.1

A VPN slave server called MOE is in the NDS tree MAPLE. MOE has public IP address 192.168.1.232, and private IP address 172.16.1.254. MOE's VPN tunnel IP address is 192.168.199.2.

A VPN slave server called MANNY is in the NDS tree OAK. MANNY's only access to the other servers is through a small Linksys BEFSR41 router performing dynamic NAT for outbound traffic, and port forwarding for inbound traffic. MANNY has public IP address 192.168.2.231, and private IP address of 192.168.8.254. MANNY's VPN tunnel address is 192.168.199.3. MANNY's default route is 192.168.2.1.

A Linksys BEFXS41 router makes a Site-to-Site VPN connection to JACK, using preshared key mode. The Linksys router tunnels traffic to 10.1.1.0 (behind JACK), and

Prerequisites

- You must have installed BorderManager 3.8.
- You must have installed the special version of TCP/IP on the NetWare server that supports the new VPN. (This means the version of TCP/IP supplied on the BorderManager 3.8 Companion CD.)
- You must have installed and configured iManager 2.0 with the BorderManager 3.8 snapin components, on either a Windows 2000 or XP system, or on NetWare 6.5. A chapter later in this book covers installing iManager 2.0 on a Windows PC, in order to manage BorderManager 3.8 on NetWare 5.1 or 6.0, in an environment where no NetWare 6.5 servers are available. The Troubleshooting chapter also includes some instructions on getting iManager 2.0.1 running on a NetWare 6.0 server.

Site-to-Site VPN

You must begin by creating at least one Master VPN server. All other VPN servers that will connect to the master VPN server will be slave servers. All configuration is done using iManager 2.0. In this chapter, the Master VPN server is called JACK.

Understanding Certificates and VPN

The BorderManager 3.8 Site-to-Site VPN relies on X.509 certificate authentication for encryption. This means that you must manually configure, and export, custom certificates for each server involved. I find this to be one of the trickiest aspects of the new VPN if you are used to a legacy BorderManager VPN configuration. With the legacy VPN, you never had to create a certificate and export it. (Actually, you did that using VPNCFG, but it was a lot simpler, and the details were hidden from you).

Custom Server Certificates

You can actually have BorderManager create certificates for you, if you let it use default values when you configure the VPN for the first time. However, I will show the process of creating a custom certificate, and exporting it. You should know that you cannot get the VPN to work if you simply use the default certificate creation method – you must specify some non-standard settings. You can use either iManager 2.0 or ConsoleOne to create the certificates.

The concept here is that you create a certificate to be used on the server to encrypt the data when it is sent to another VPN host.

If your servers are not in the same NDS tree, you must then export the trusted root certificate (in a .DER file), to be used by the other VPN host to verify and decrypt the VPN data. Therefore, you have two steps to complete:

1. Create a custom certificate for use by VPN, making a note of the Public Key Subject Name.
2. Export the Trusted Root Certificate to a .DER file. You will have to use that file to create a TRO on the other server (if making a VPN connection between two BorderManager 3.8 servers).

Thankfully, you only need to export the slave certificate to the master VPN server – it will automatically push the certificate details from one slave to all the others. You will have to create a TRO for the master, from the master's certificate export, on each slave when first configuring the slave. (This is done manually if you the slave

VPN servers are in a different NDS tree than the master VPN server).

One of the critical pieces here is that you need to know the exact subject name of the server certificate. The subject name you want is the Public Key Certificate Subject Name, which is found in the properties of the certificate. You will have to type it when configuring the Site-to-Site VPN later, if the VPN servers are not in the same NDS tree. I recommend you screenshot the Public Key Certificate menu that shows you the subject name so that you will not have to be guessing later.

User Certificates (for Client-to-Site VPN)

A special type of certificate called a user certificate is required (for each user) if using Client-to-Site VPN with certificate authentication method. There is more detail on this in the chapter on BorderManager 3.8 Client-to-Site VPN later in this book.

Trusted Root Containers

If you are using BorderManager 3.8 as a VPN server, it must have one or more trusted root objects for other VPN members. These certificate objects are stored only in a special NDS container called a Trusted Root Container (TRC). iManager can create the TRC for you when you configure the VPN for the server. Alternatively, you can create a TRC manually with iManager or ConsoleOne.

When you configure the BorderManager 3.8 VPN, you will tell it the name of the Trusted Root Container. Once the server knows the name of the container, it will always look there to find trusted root objects.

Site-to-Site VPN - Summary of Major Steps

This is a very basic checklist of the steps that must be completed in order to configure a Site-to-Site VPN between two Novell BorderManager 3.8 servers. Some of the steps can be done automatically by iManager when you first configure the server as a VPN server.

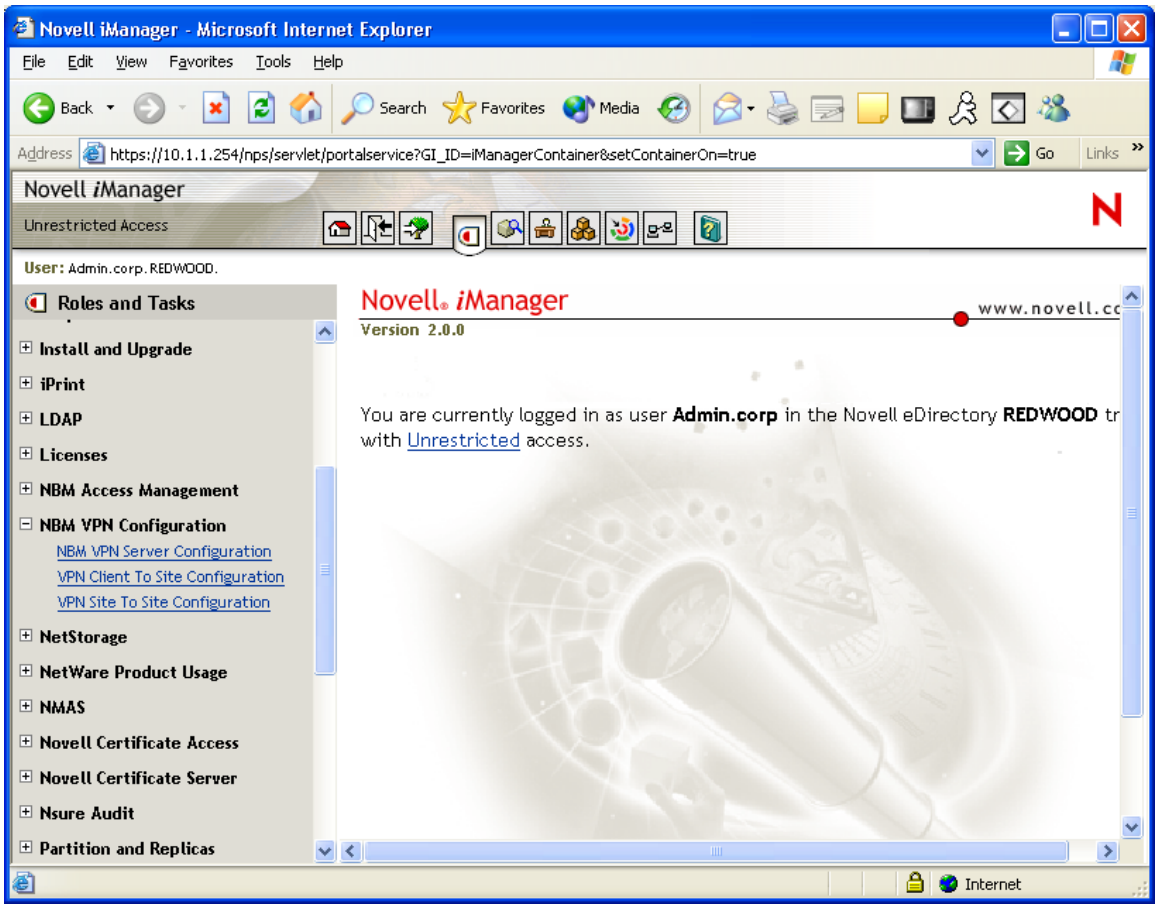
1. Each server (master and all slaves) must have a Trusted Root Container (TRC). iManager will create these for you if you allow it.
2. Each server (master and all slaves) must have a (custom) server certificate. iManager will create these for you if you allow it.
3. The master server must have a Trusted Root Object (TRO) for itself within its trusted root container. IManager will create this for you if you allow it.

4. The master server must have a Trusted Root Object (TRO) for each slave server to be added as a VPN member. If the slave server is in another tree (or in the same tree but not using the same trusted root container), you must manually create the TRO. You manually create a TRO from a .DER file. You manually create a .DER file by exporting the Trusted Root Certificate from the VPN certificate.
5. Each slave server must have a Trusted Root Object (TRO) for the master server. If the slave server is in another tree (or in the same tree but not using the same trusted root container), you must manually create the TRO. The slave servers do not have to have TRO's for themselves or other slave servers in their TRC.
6. You must configure each server as a VPN server. To do this you need to configure a custom server certificate, select the public IP address, and select a VPN tunnel IP address. You also need to know what IP addresses (hosts or networks) behind the each server will need to be accessed over the VPN.
7. You must configure each server as a master or slave server. You can have only one master in a VPN. (You can have multiple VPNs in a tree).
8. You must add each slave server as a VPN member, at the master. To do this, you need the name of the slave server, the Public Key Certificate Subject Name of the slave server certificate used for VPN, the Issuer (slave TRO), the slave server's public IP address, the slave server's VPN Tunnel IP address, and the IP addresses (hosts or networks) behind the slave server to be accessed over the VPN.
9. You may need to add access rules to the Master VPN server defining the traffic to be allowed over the VPN. (By default, everything is allowed).
10. You need the proper filter exceptions on each VPN server to allow the VPN traffic to the public IP address. The default exceptions should already allow this.

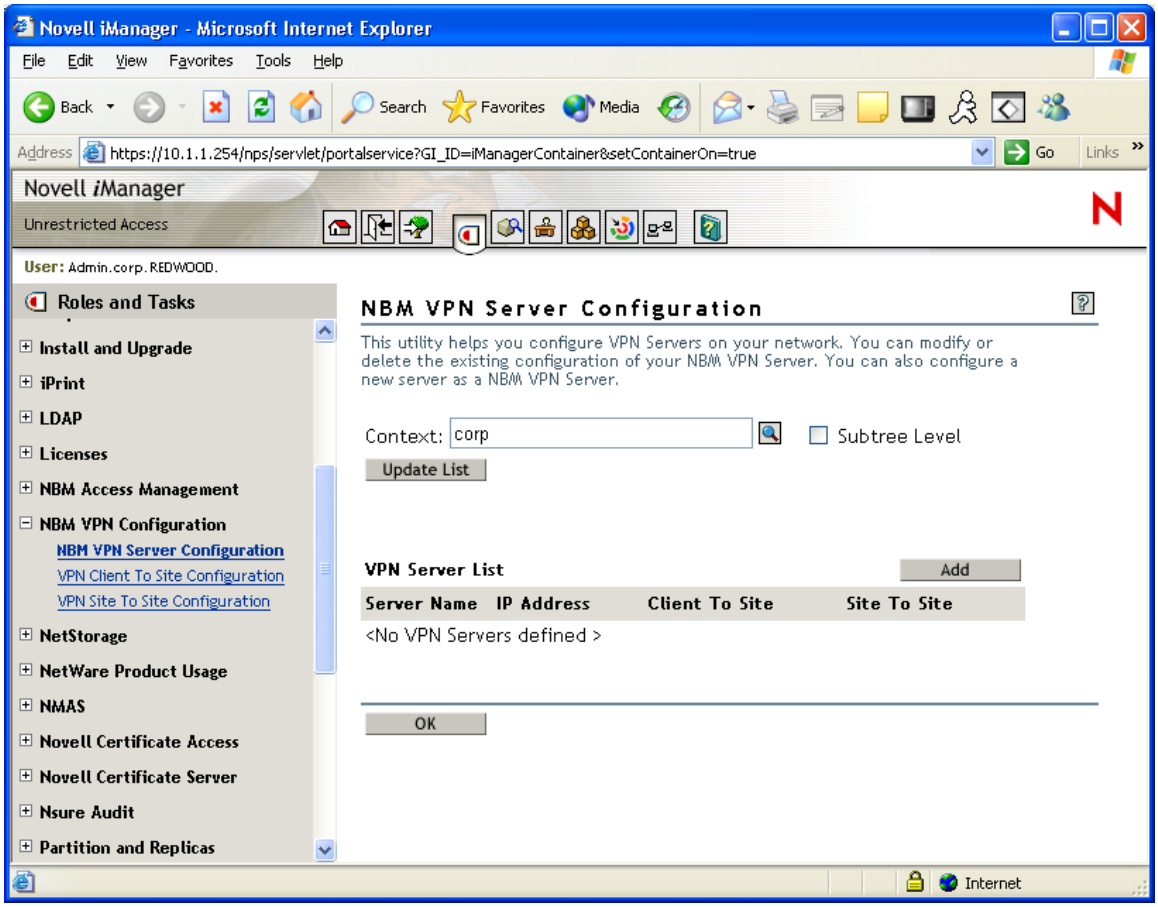
Configure JACK as a VPN Server

JACK will become the VPN master server. In this step, it will simply be defined as a VPN server.

Start by logging in to iManager in the master VPN server's NDS tree.

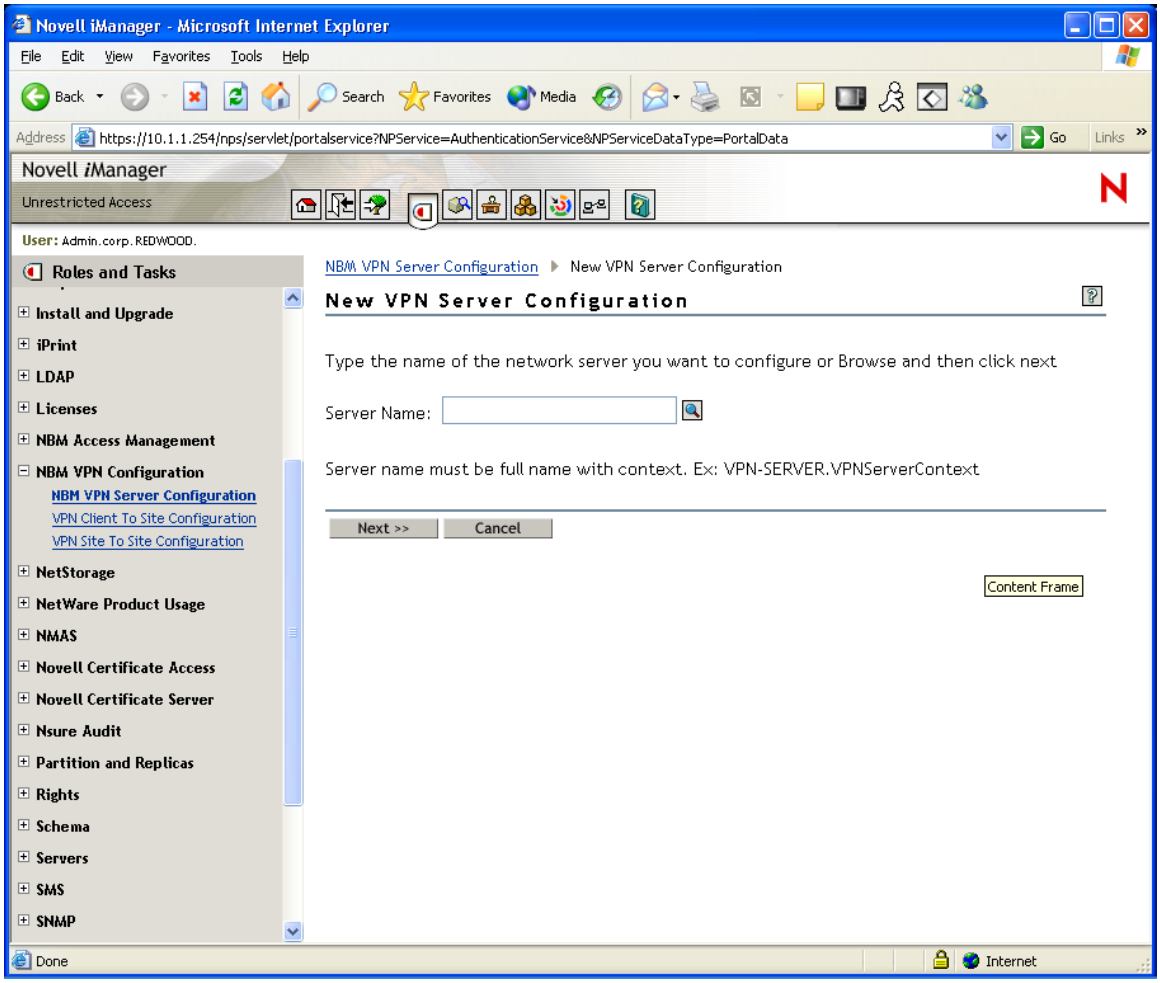


Expand the **NBM VPN Configuration** option.

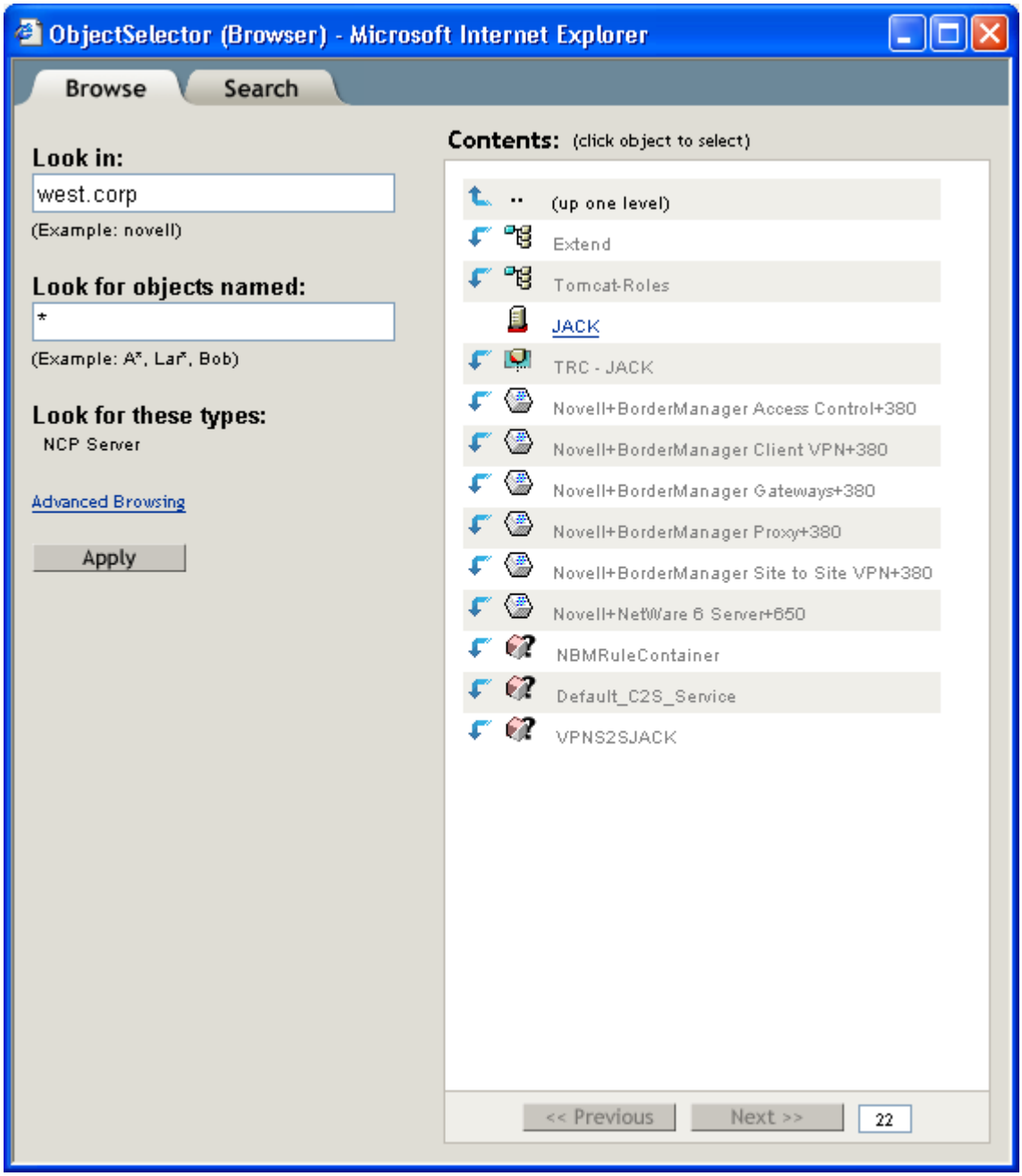


Since I know there is no VPN server in this tree yet, I will not search for one.

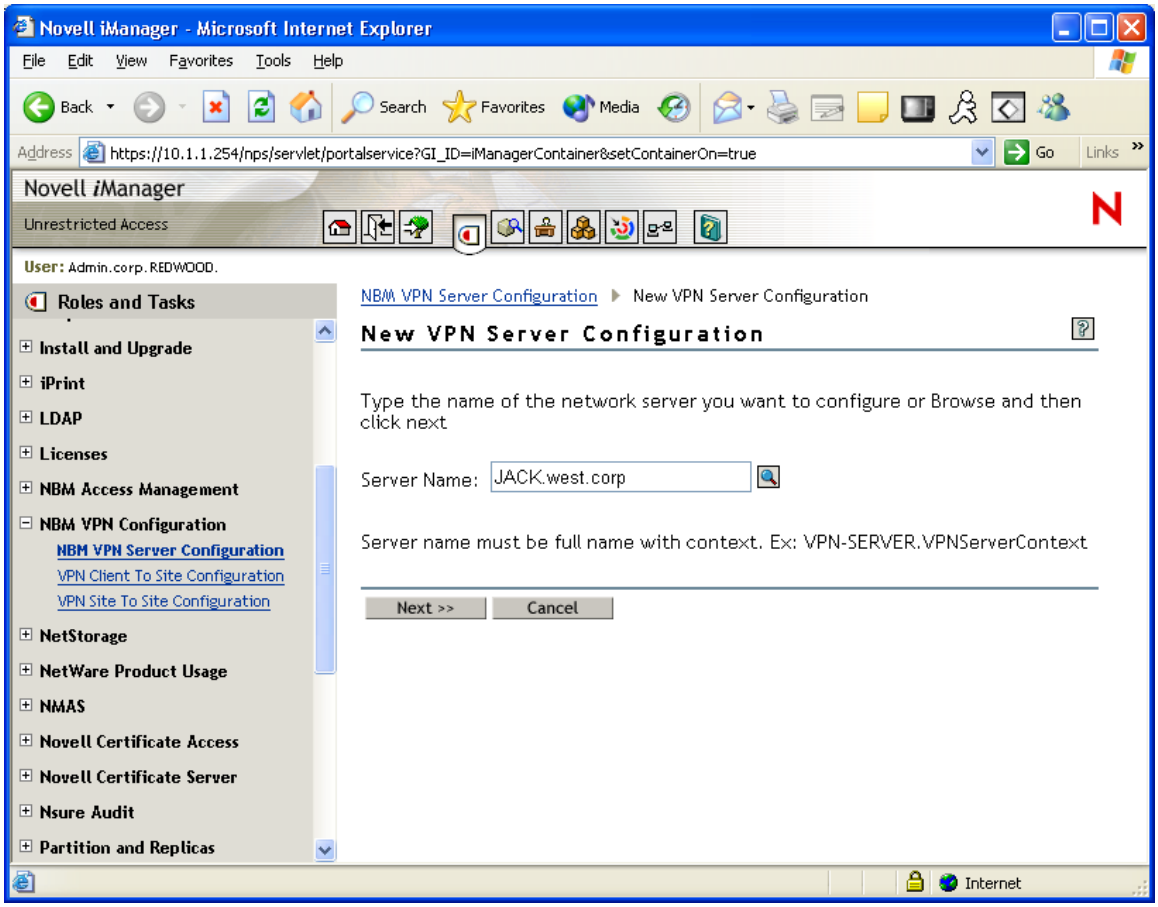
Click on the **Add** button to add JACK to the list of VPN servers.



Click on the **browse icon** to search for the server.

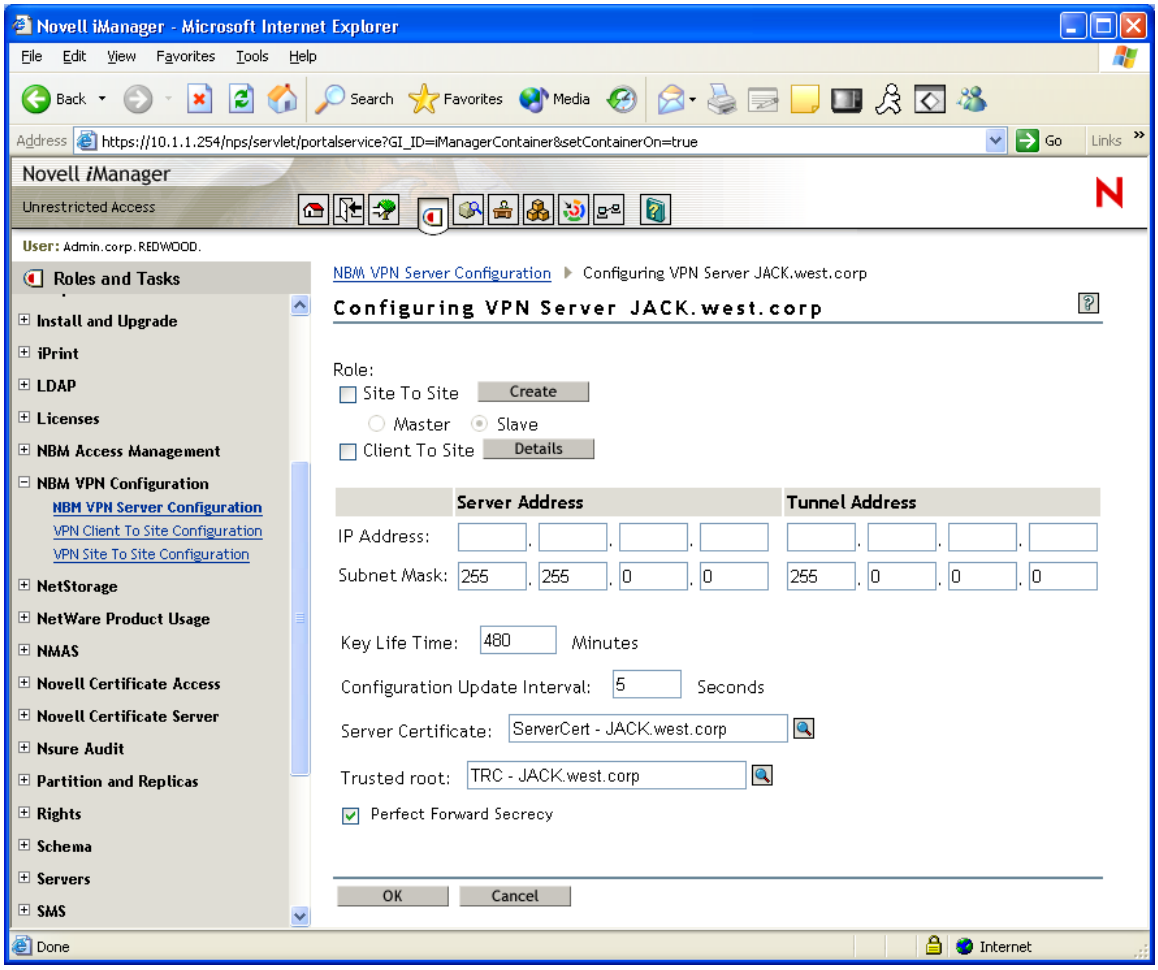


Locate the server in the tree, and select it. In this example, **JACK** is selected.



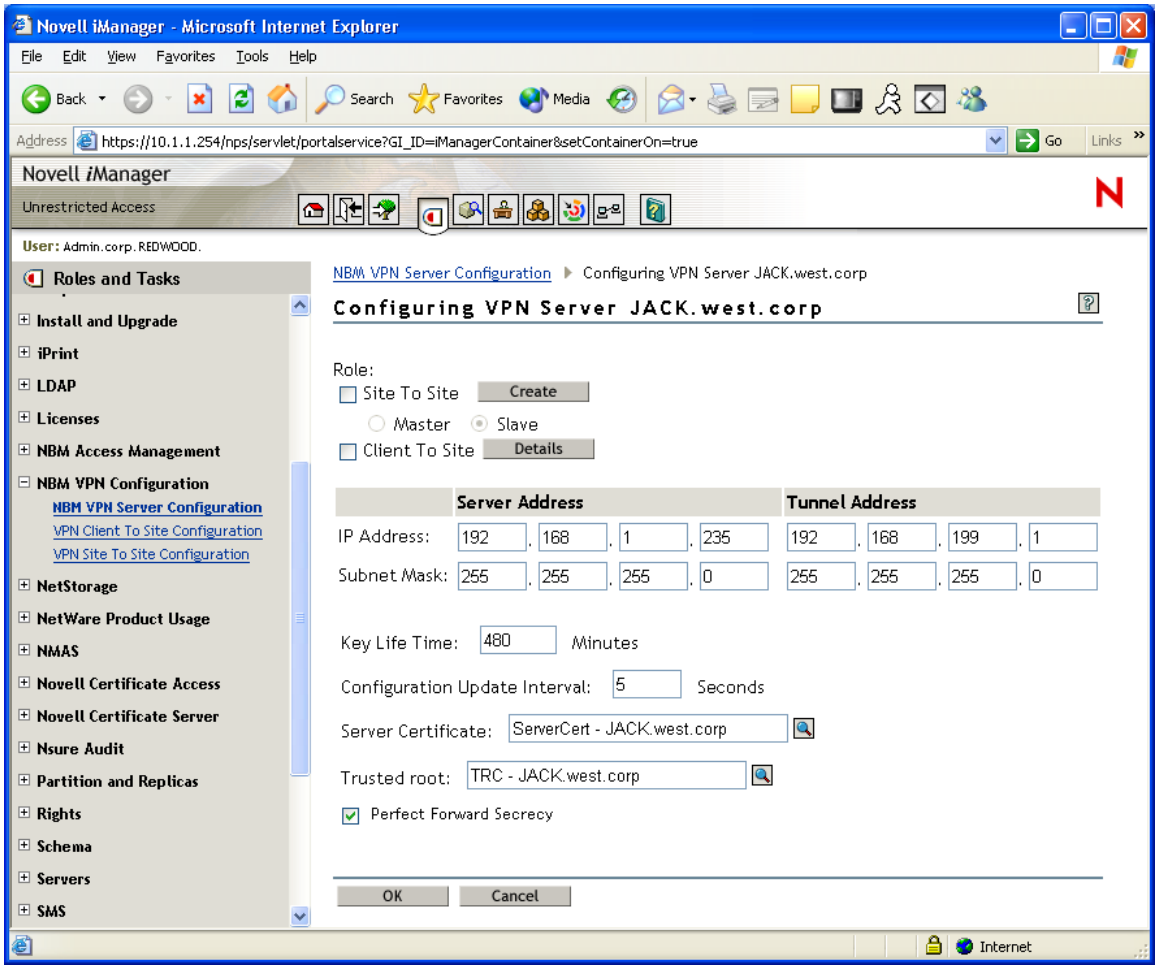
When you have selected the server to be configured as a VPN server, click **Next**. In this case, **JACK.west.corp** in the REDWOOD NDS tree will be configured as a VPN server.

JACK's role as a master or slave server will be defined a bit later in the process. The first step is to define it as a VPN server and give it basic settings.



Notice at this point that the **Server Certificate** and **Trusted root** fields are already filled in – with objects that do not yet exist. This is where iManager will automatically create such objects for you, with the proper settings. These objects will be created in the VPN server's NDS container.

For this example, I will allow iManager to create those objects (a server certificate called **ServerCert- Jack**, and a trusted root container called **TRC - JACK**) for me.

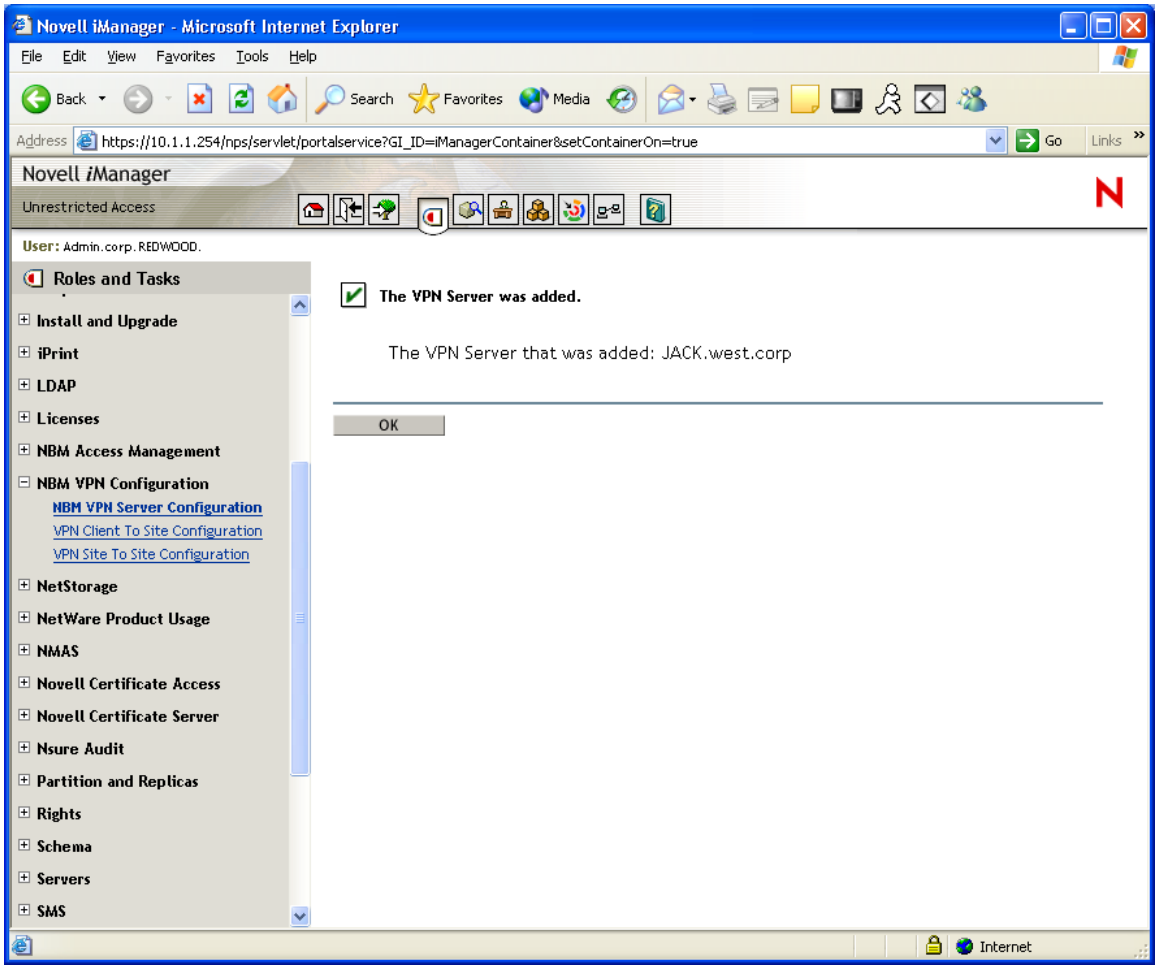


Refer to the network diagram at the beginning of this chapter for IP addressing used in this example.

In the **Server Address** field, fill in the Public IP address to be used by other servers for a VPN connection. The **Server Address** is the PUBLIC IP address of the server. If the server is behind a NAT hop, you would put the public IP address of the static NAT pair here. (I show an example of this later in the chapter for the server MANNY).

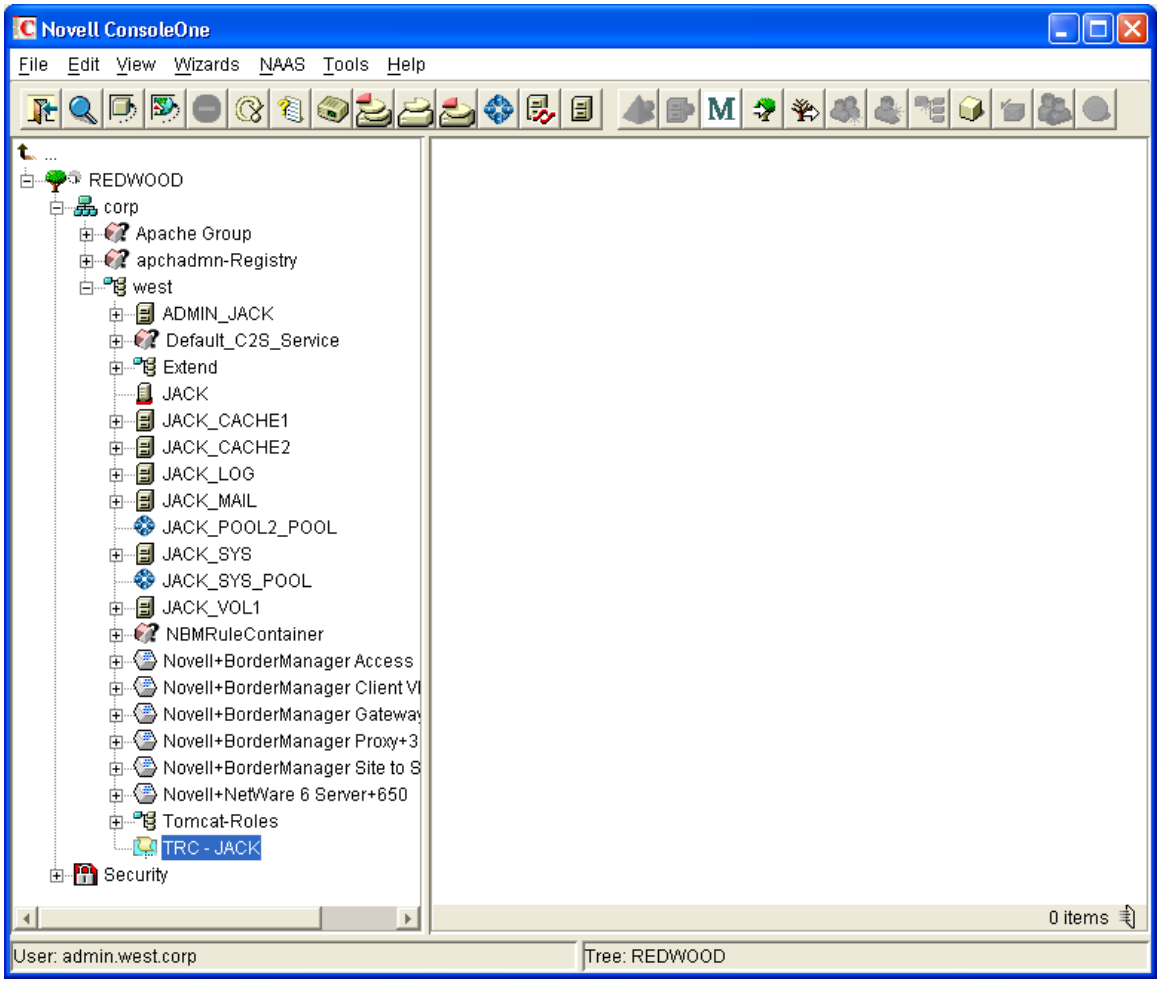
In the **Tunnel Address** field, fill in the VPN tunnel IP address of this server. The Tunnel Address is an address that should not be in use anywhere on the private network, on any VPN slave server networks to be connected, or on any private home networks to be connected with Client-to-Site VPN. This is quite important, as it means you have to be careful to avoid any address in common use. Do NOT use 192.168.0.x or 192.168.1.x – these are very common default values for many home networks or small routers. I chose 192.168.199.0 as the VPN tunnel network because it is not likely to conflict with anything else.

Leave **Perfect Forward Secrecy** enabled, and click **OK**.



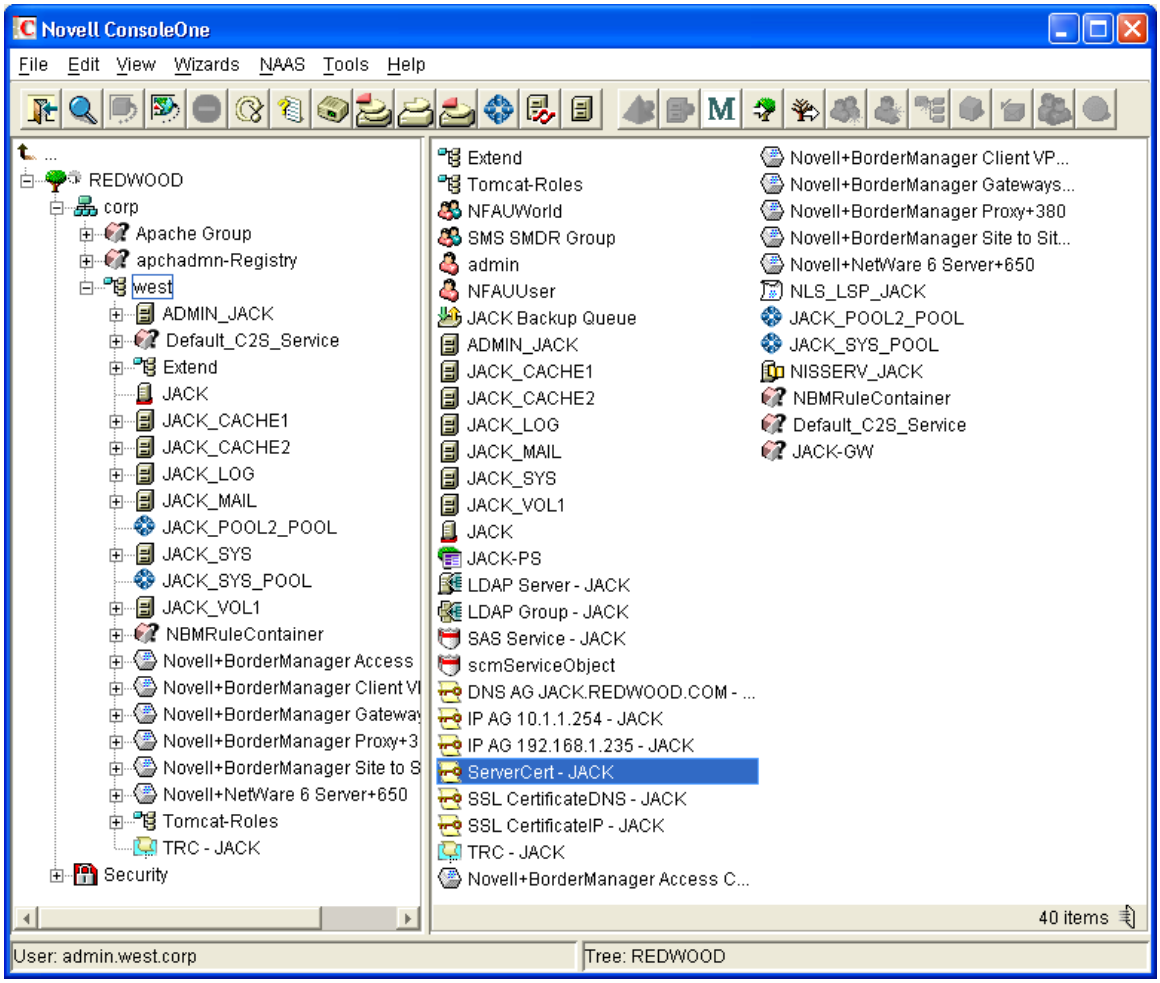
You should see a success message if all went well. Click **OK**.

Now let's look at NDS, using ConsoleOne, to see what objects were created for us.



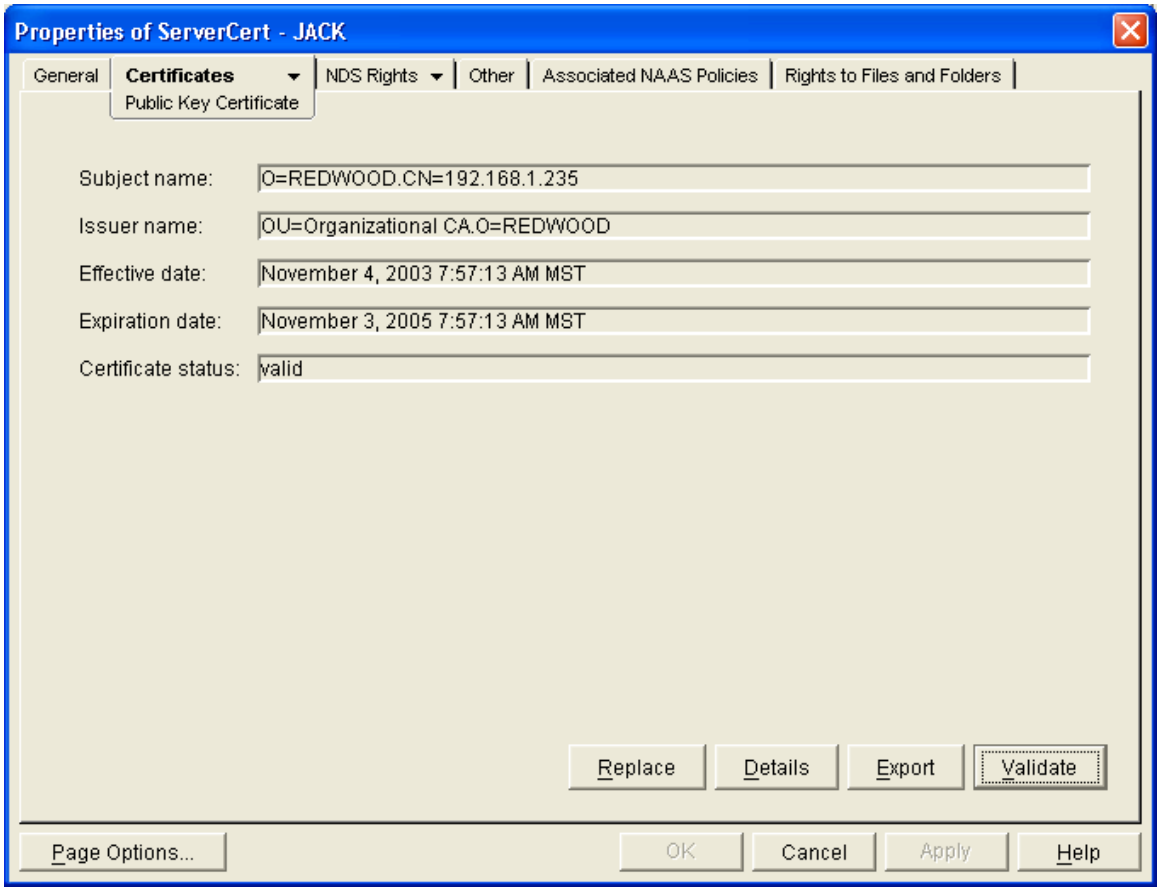
There is now a **TRC - JACK** object in the same container as the server object. This is the Trusted Root Container (TRC). There are no objects within the TRC container yet.

When we add slave servers that are not in the same tree as JACK, we must create Trusted Root Objects (TROs) for each slave server into this trusted root container so that JACK can validate the slave server VPN certificates when establishing an encrypted link.



There is now a **ServerCert – JACK** certificate (key material) object in the same container as the VPN server.

When JACK makes a VPN connection to other VPN devices, JACK will present this certificate for encryption purposes. The remote devices will have to have a trusted root object (TRO) to validate this certificate.



Looking at the **ServerCert – JACK** certificate properties, we can see that the **Subject name** created for the Public key certificate is **O=REDWOOD.CN=192.168.1.235**.

CAUTION *You want the Subject Name for the Public Key Certificate here, not the subject name for the Trusted Root Certificate!*

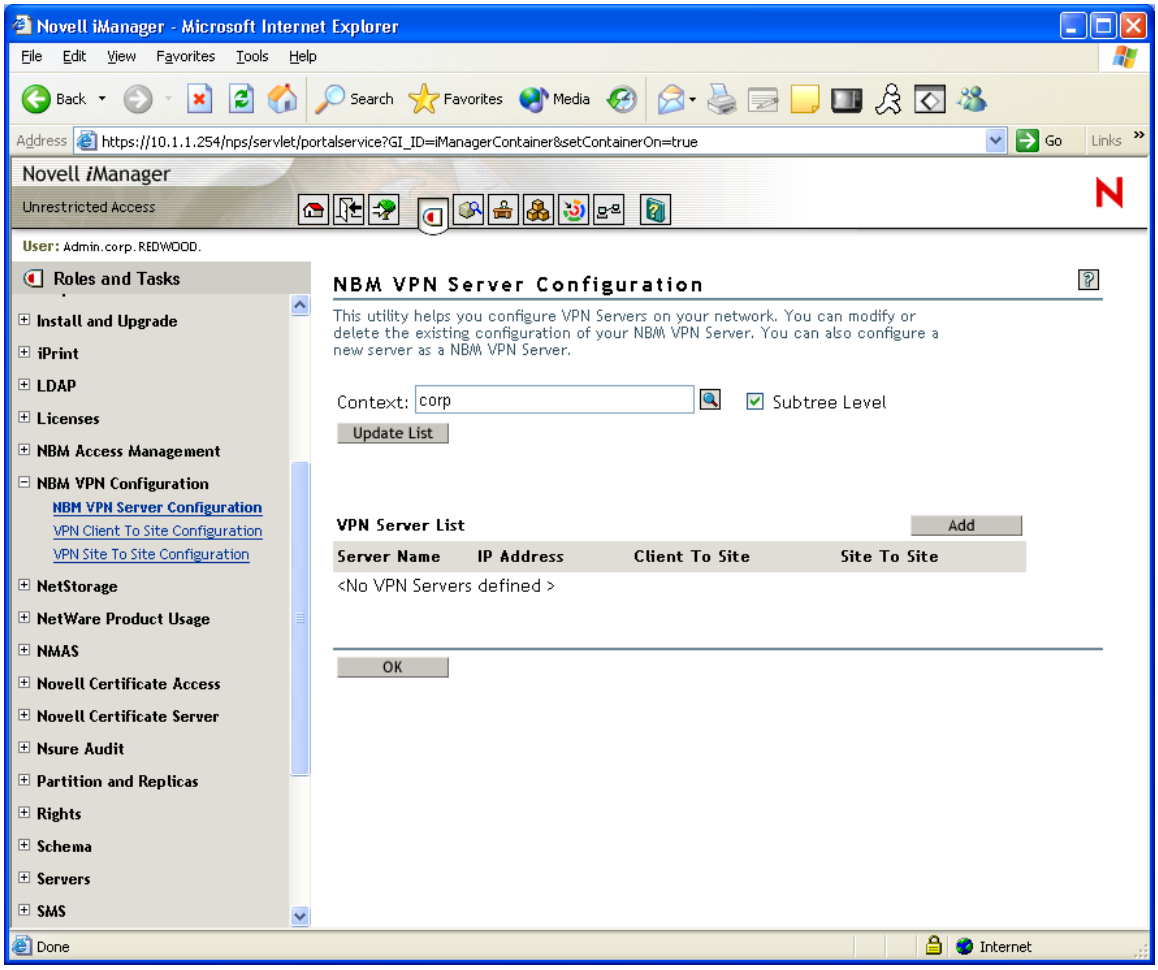
This is important, because we will later need to type in this exact text on the slave VPN device. We must also export this certificate to a .DER file to import to the remote VPN device at some point in the future. (That operation will be shown later).

It is important to note that the VPN certificate created here was not created with default values if you simply were to create a server certificate in either iManager or ConsoleOne. The procedure and settings to be used for manually creating a VPN server certificate are shown later.

Configure JACK as the Master Site-to-Site VPN Server

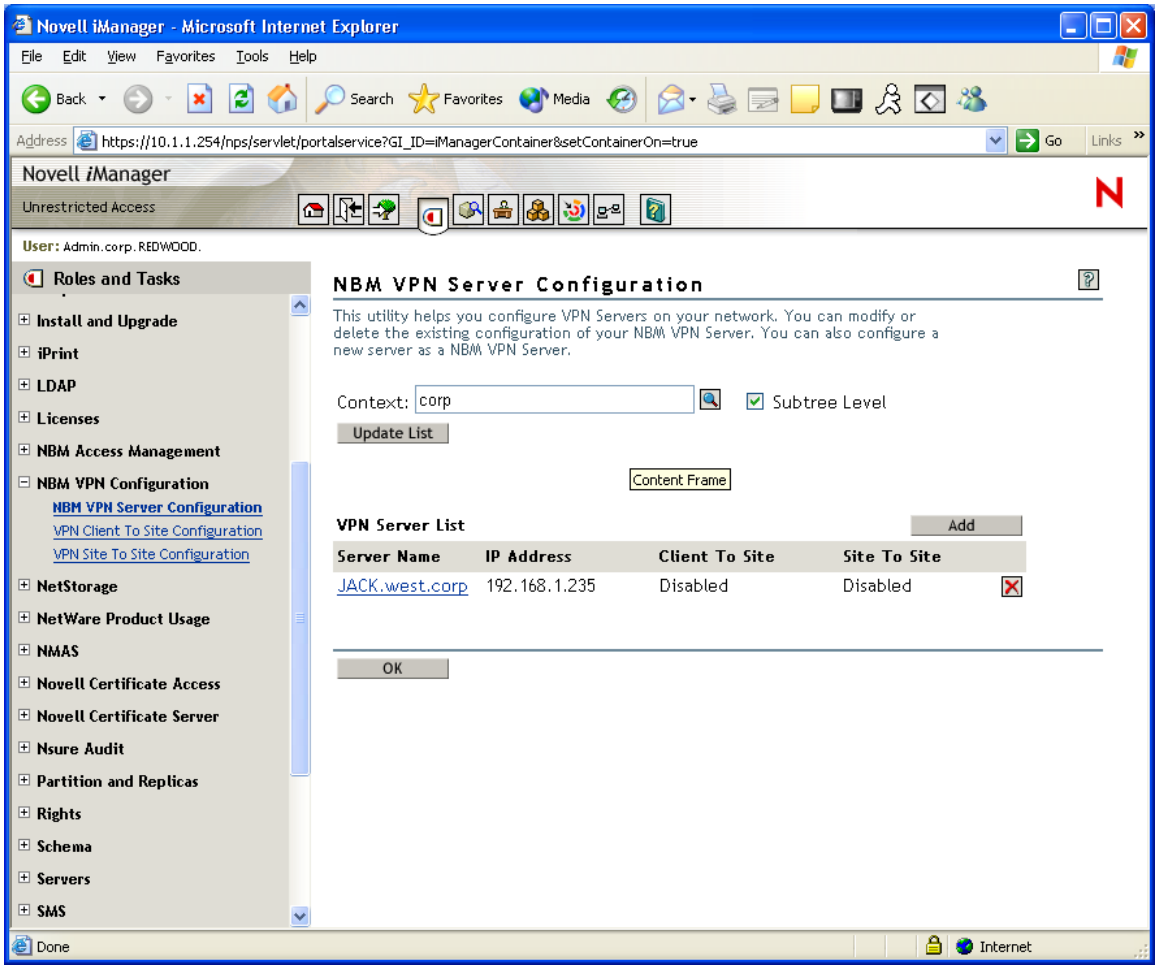
VPN Server Configuration

In this section, server JACK in NDS tree REDWOOD will be configured in the role of Master Site-to-Site server. Start by logging into iManager in the server's NDS tree, and expand the **NBM VPN Configuration** link.



Select **NBM VPN Server Configuration**, and then select **Subtree Level**. Click on **Update List**. This should result in the display of any VPN servers in the corp context or below.

Or, simply browse to the context holding your VPN server and select it.



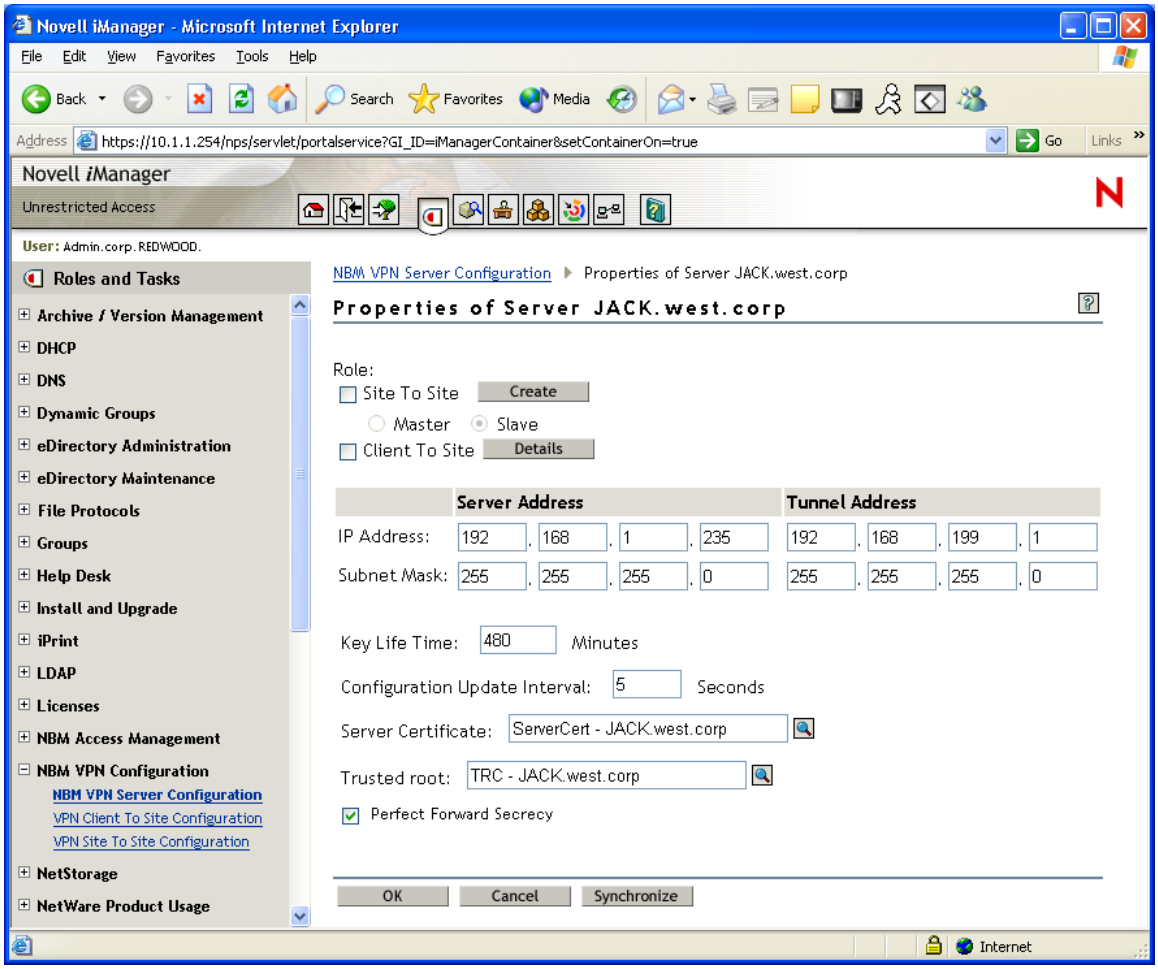
Now that JACK has been defined as a VPN server, it shows up as a an entry in the VPN Server List.

At this point, both **Client To Site** and **Site To Site** services are **disabled**.

Click on the **link to JACK** under the **Server Name** field.

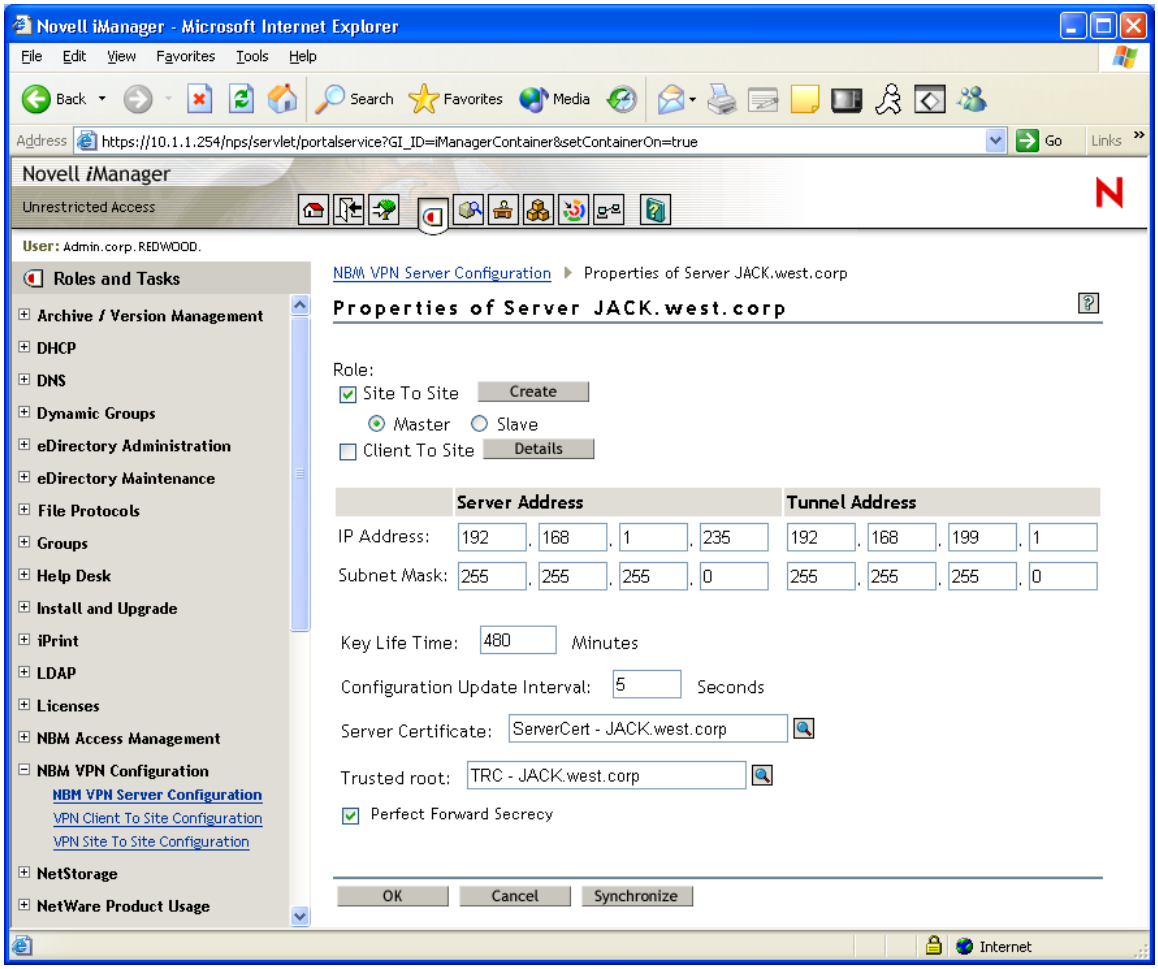
Configure Site-to-Site VPN Service

You should now be at the VPN Server Configuration menu.

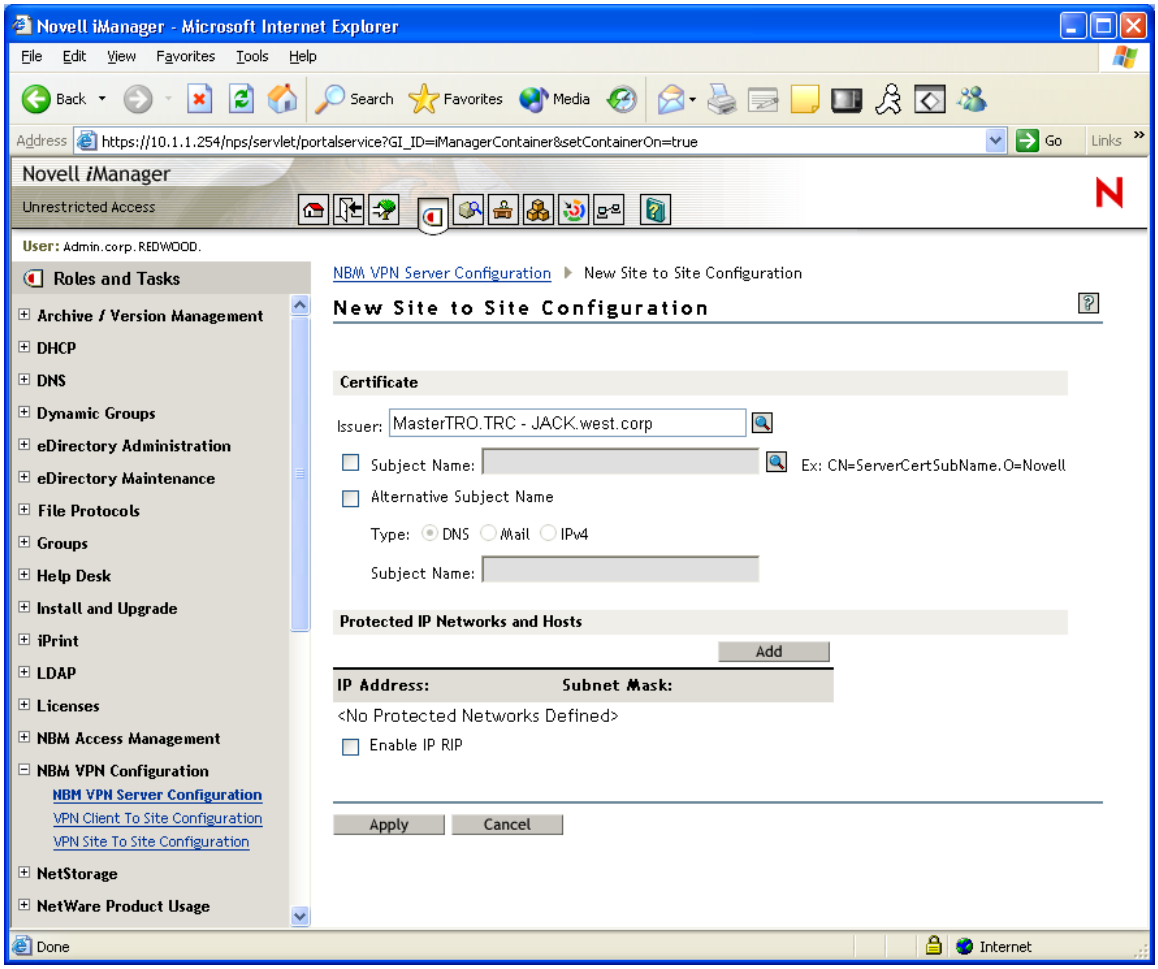


We are back to the VPN server properties page for JACK. We now want to set this server up as a master Site-to-Site server. (Client-to-Site is shown later).

Check the **Role box for Site To Site**, and select the **Master** option.



With the **Site To Site Role** checked, and the option set to **Master**, click on the **Create** button.



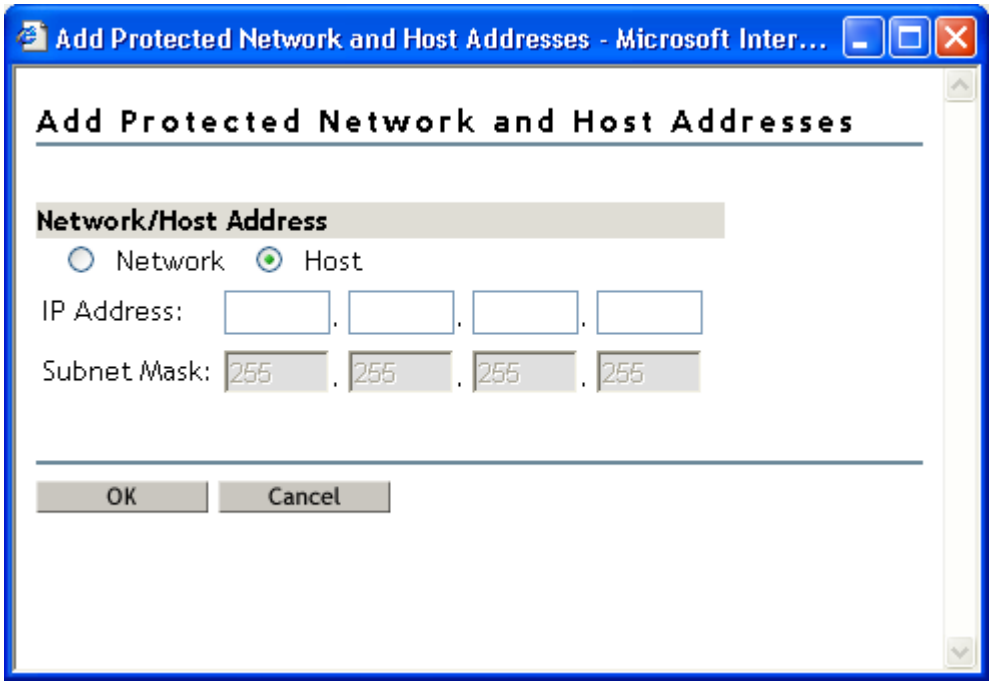
Again, we come to a menu where a value has been filled in without the actual object having been created yet. The **Issuer** field is set to **MasterTRO.TRC – JACK.west.corp**.

iManager will create a new Trusted Root Object (TRO) with the name **MasterTRO** in the Trusted Root Container (TRC) previously created for JACK in JACK's NDS container. We will accept the default.

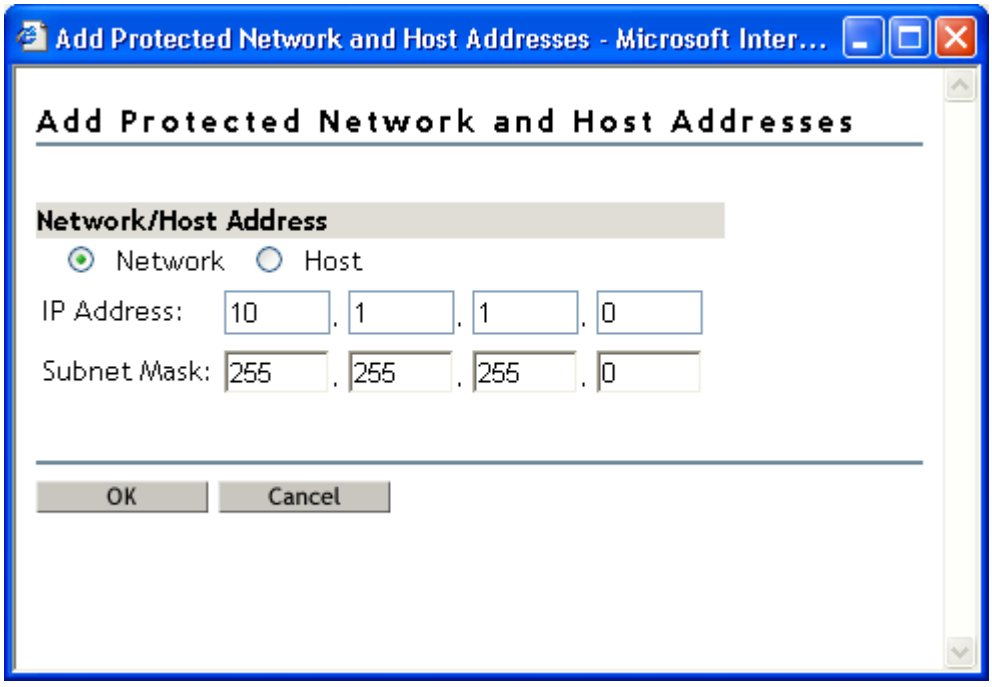
If you do not accept this default, you must previously have created a TRO in the TRC so that you can browse to it and select it.

The TRO is an object that tells the server some details about a Trusted Root, for the purposes of validating certificates. In this case, the TRO will provide details on the Certificate Authority (trusted root) of the REDWOOD NDS tree.

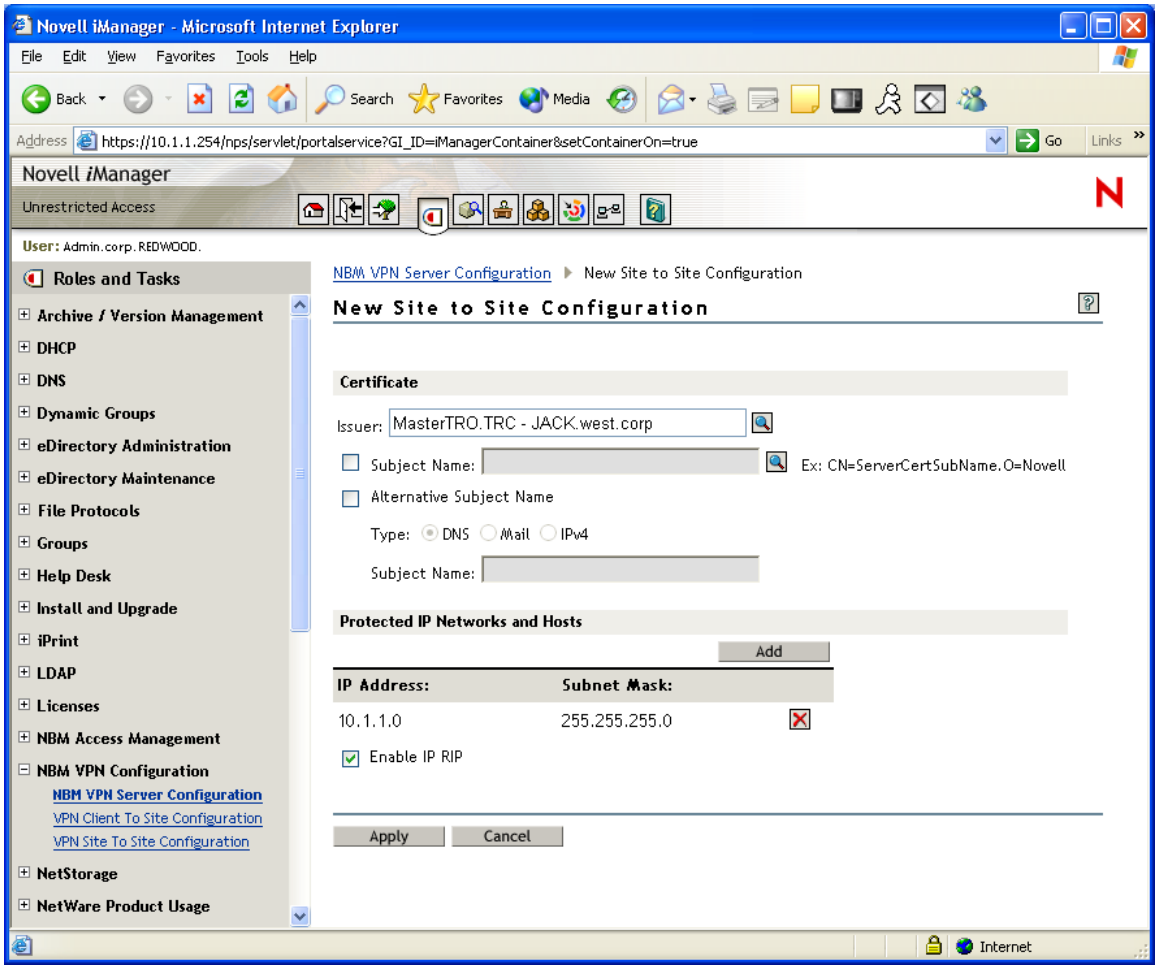
Accept the defaults, and click on the **Add** button to specify the **Protected IP Networks and Hosts**.



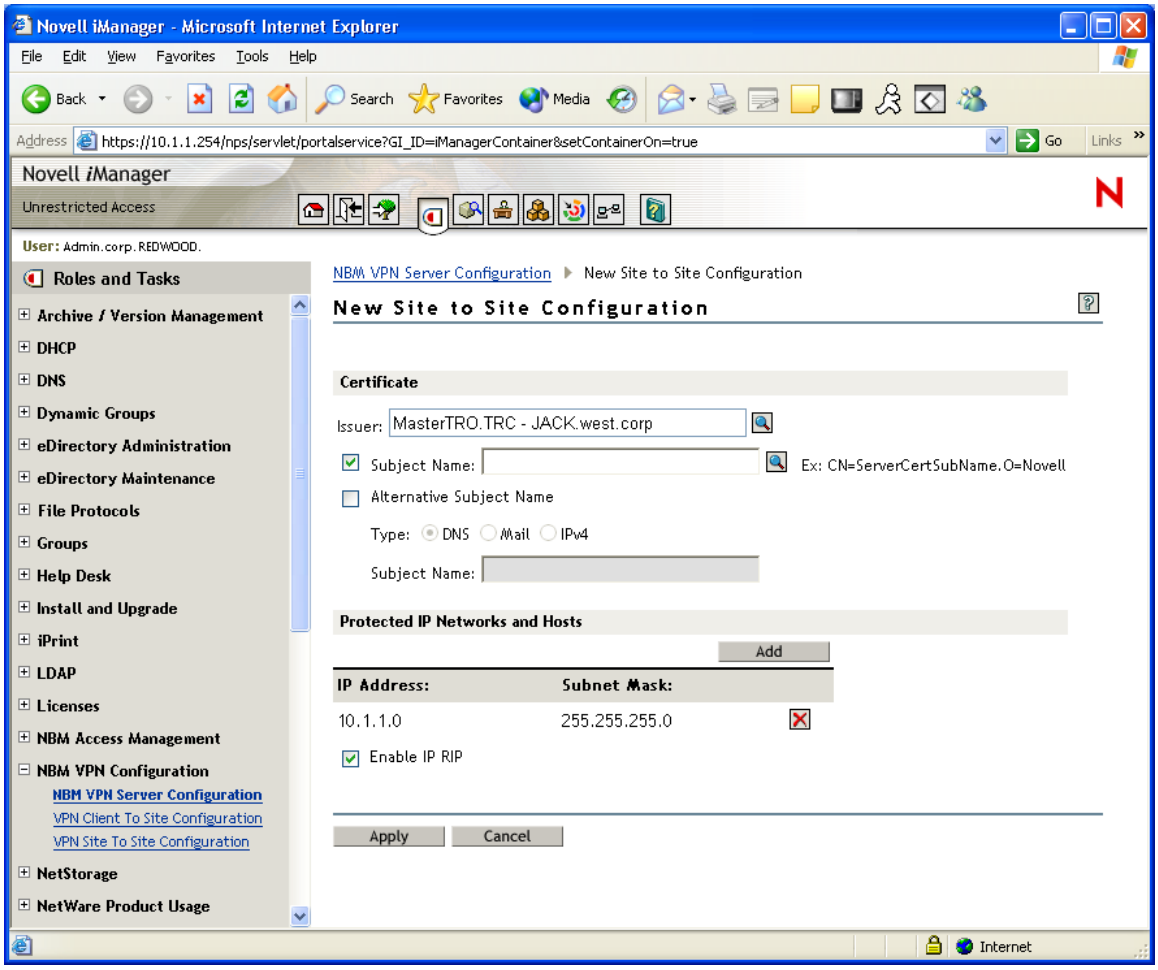
You should see a browser window to add a network or host address.



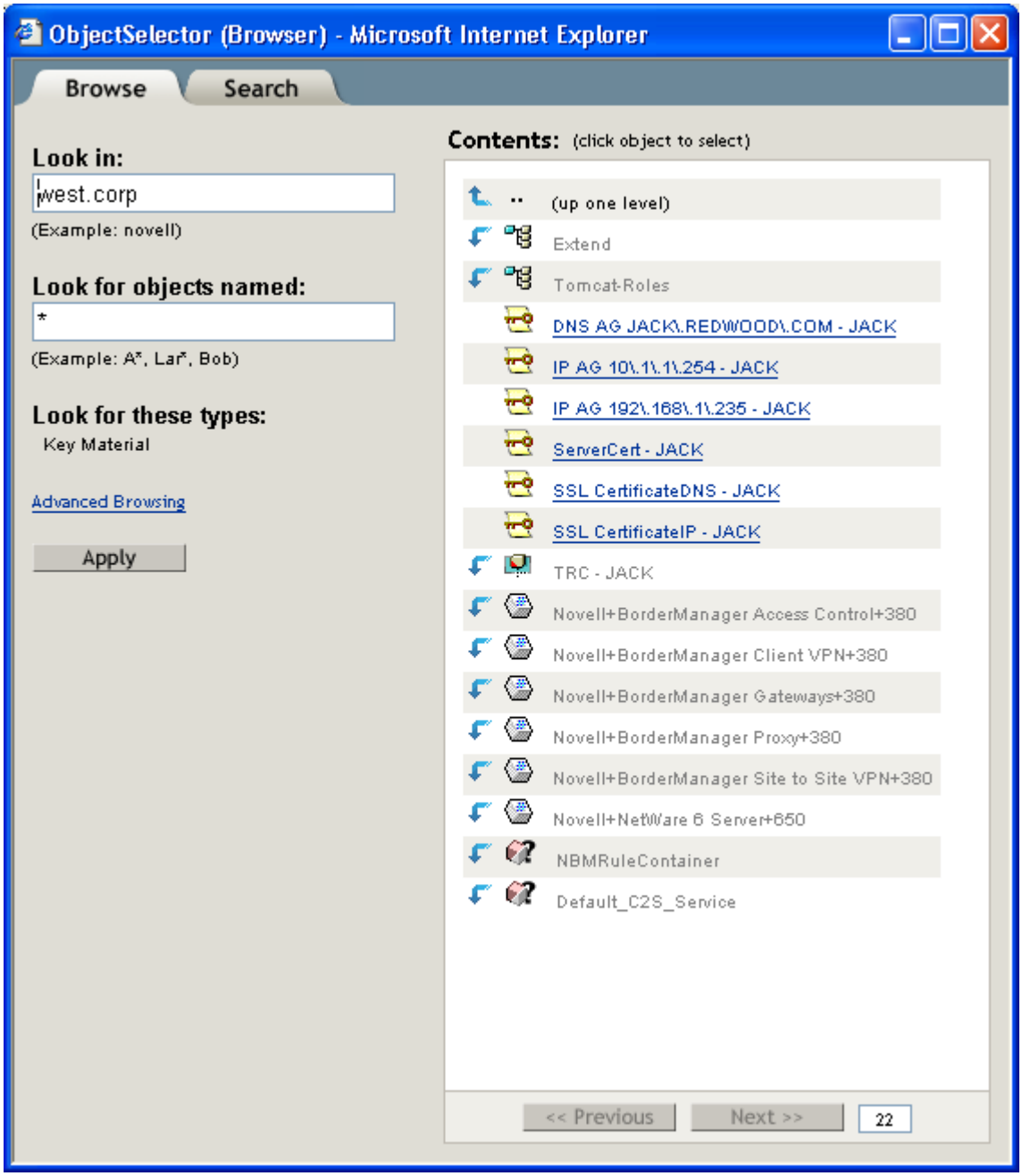
Fill in the **private network address and subnet mask**. This assumes you want to provide full Site-to-Site VPN access to the entire subnet. You can also specify a single host, or some limited subnet range. You can repeat this step to add multiple hosts or networks. Then click **OK**.



Enable IP RIP if you want the protected networks and hosts entries automatically pushed to the VPN slaves later. (Normally you want this option enabled!)

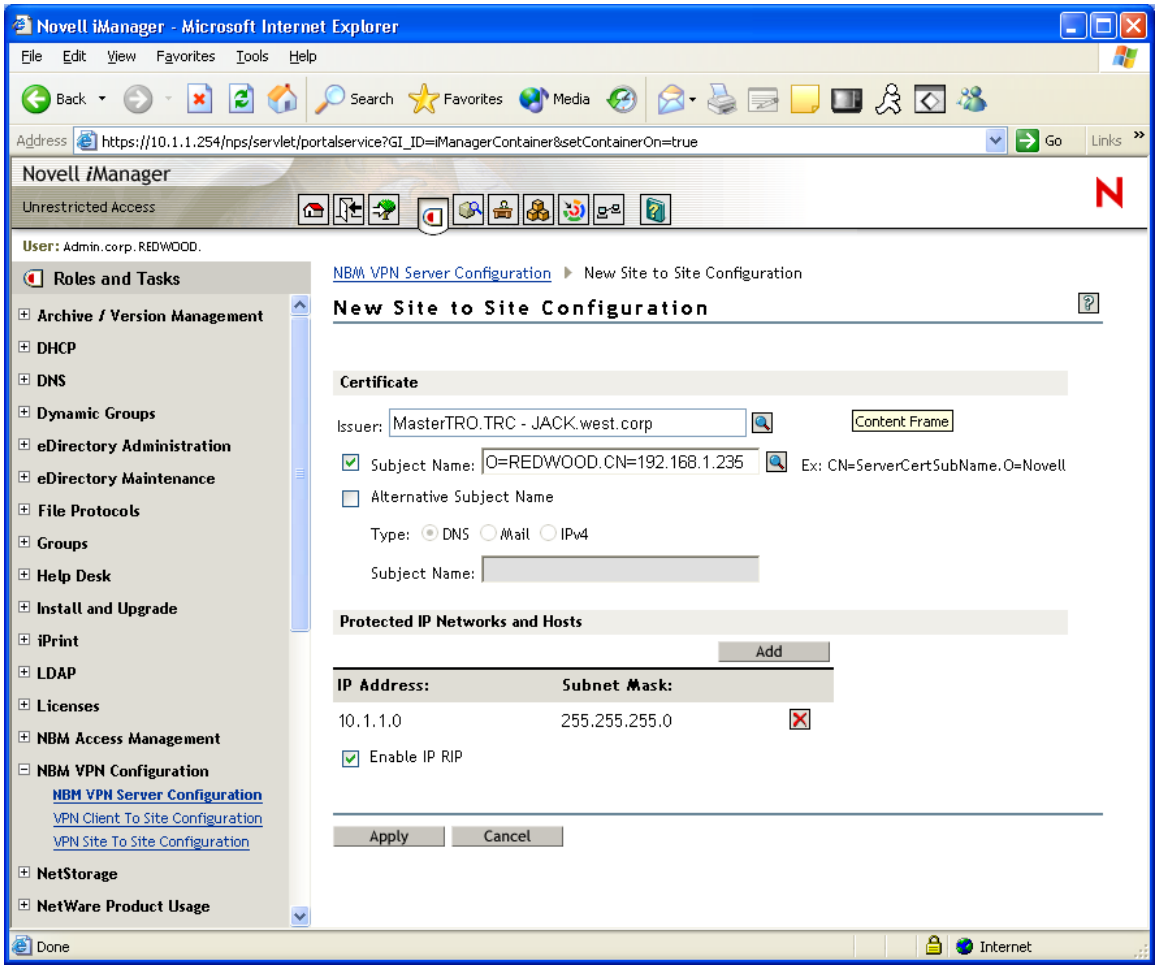


Select **Subject Name**. Click on the **browse icon** next to it to browse to the server's VPN certificate.



Select the **ServerCert – JACK** certificate created earlier by iManager, unless you have manually created a custom certificate for the VPN.

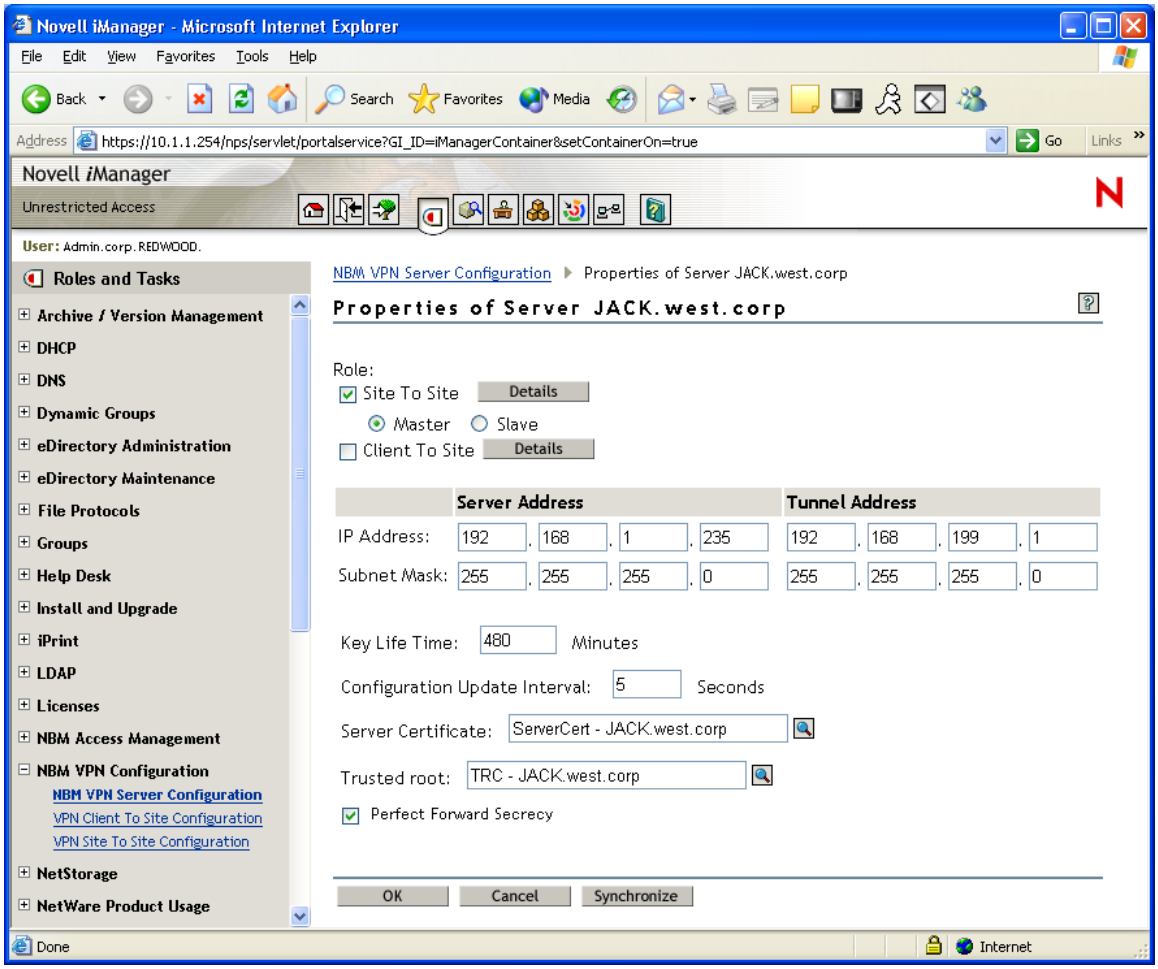
Click **Apply**.



Notice that the **Subject Name** is filled in automatically for us in this case. It could also have been typed in manually.

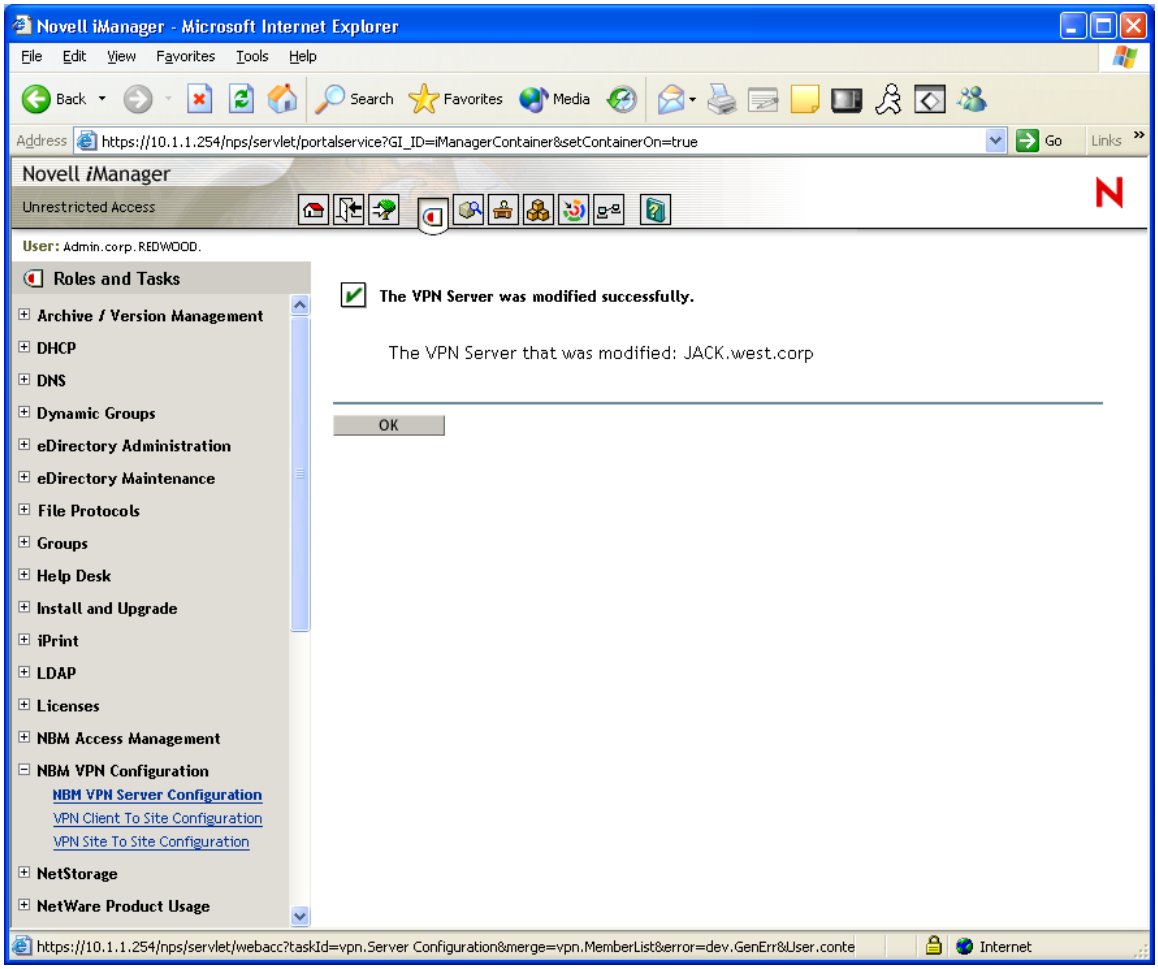
If you examine the ServerCert – JACK Public Key Certificate Subject Name (with ConsoleOne or iManager), you will see the same subject name here. This is not the subject name that shows up on the Trusted Root Certificate menu in the ServerCert – JACK properties.

Now click on **Apply** at the bottom of the screen.



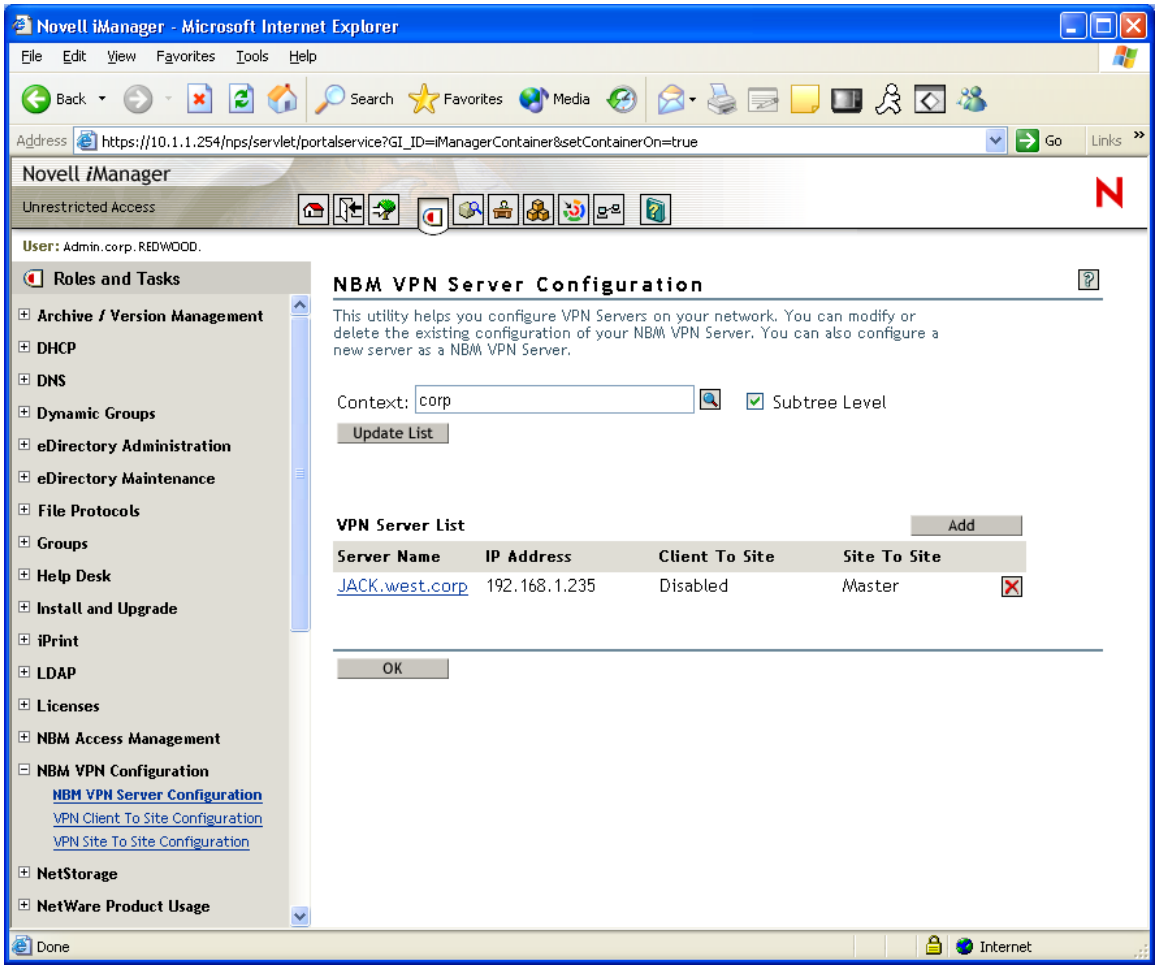
We are brought back to the VPN server properties screen now that we have created the Master VPN configuration, but **we have not saved** that Master VPN configuration for this server yet.

Click on **OK** at the bottom of the screen.



You should see a success message. The server is now modified to be a master VPN server.

Click **OK** to close this window.



Server JACK now shows up as a **Master Site To Site** VPN server.

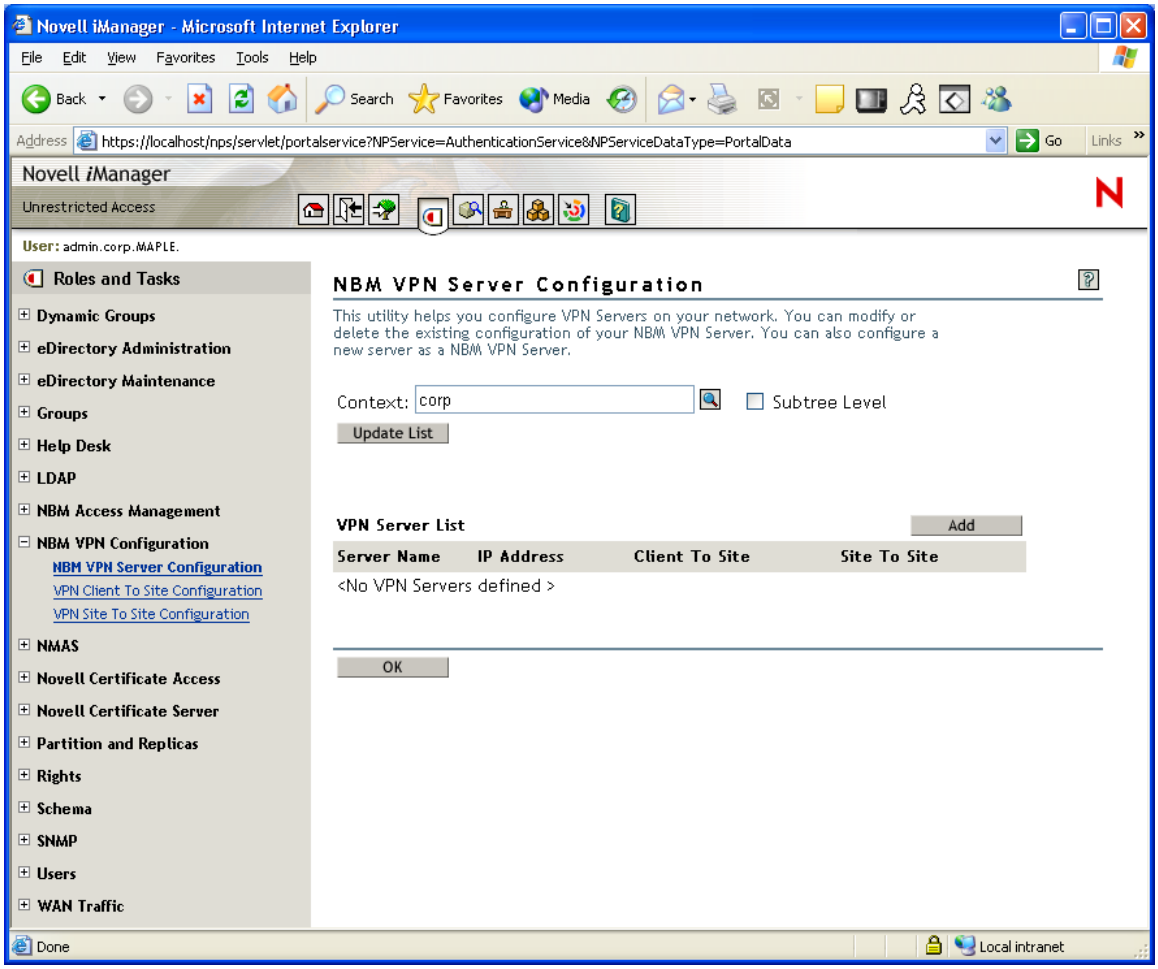
Next, you need to add other servers as Site-to-Site slave members. This procedure is shown next.

Configure MOE as a VPN Server

In this section, we define MOE as a VPN server. In the next section, we define MOE as a Site-to-Site VPN slave server. The steps are basically identical to the previous section configuring JACK as a VPN server, except that MOE is in a different NDS tree and will not use the same Trusted Root Container (TRC) as JACK.

Because MOE is a NetWare 6.0 server, and does not have iManager 2 installed, you must use either iManager 2.0 from a NetWare 6.5 server, or a local Windows iManager 2.0 installation to configure the VPN services. In this case, there is no NetWare 6.5 server available that can connect to MOE, so a local Windows iManager 2.0 server was used. (iManager 2.0 installed on a Windows XP Professional workstation).

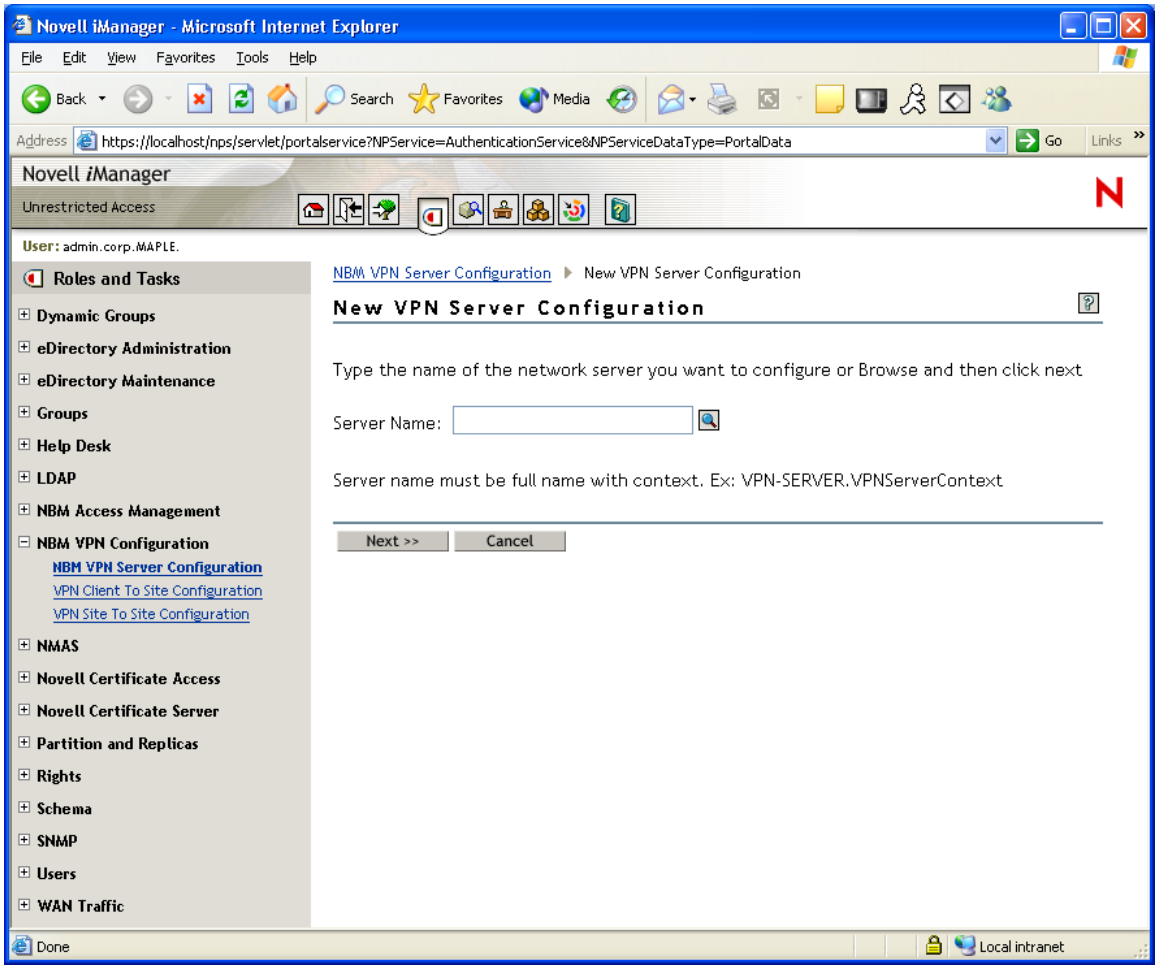
Note This section will configure a server up that is using the public IP address as the VPN IP address. An example later (for slave server MANNY), will show the configuration for a VPN server that is behind a NAT router hop, where the VPN address is NOT the server's public IP address.



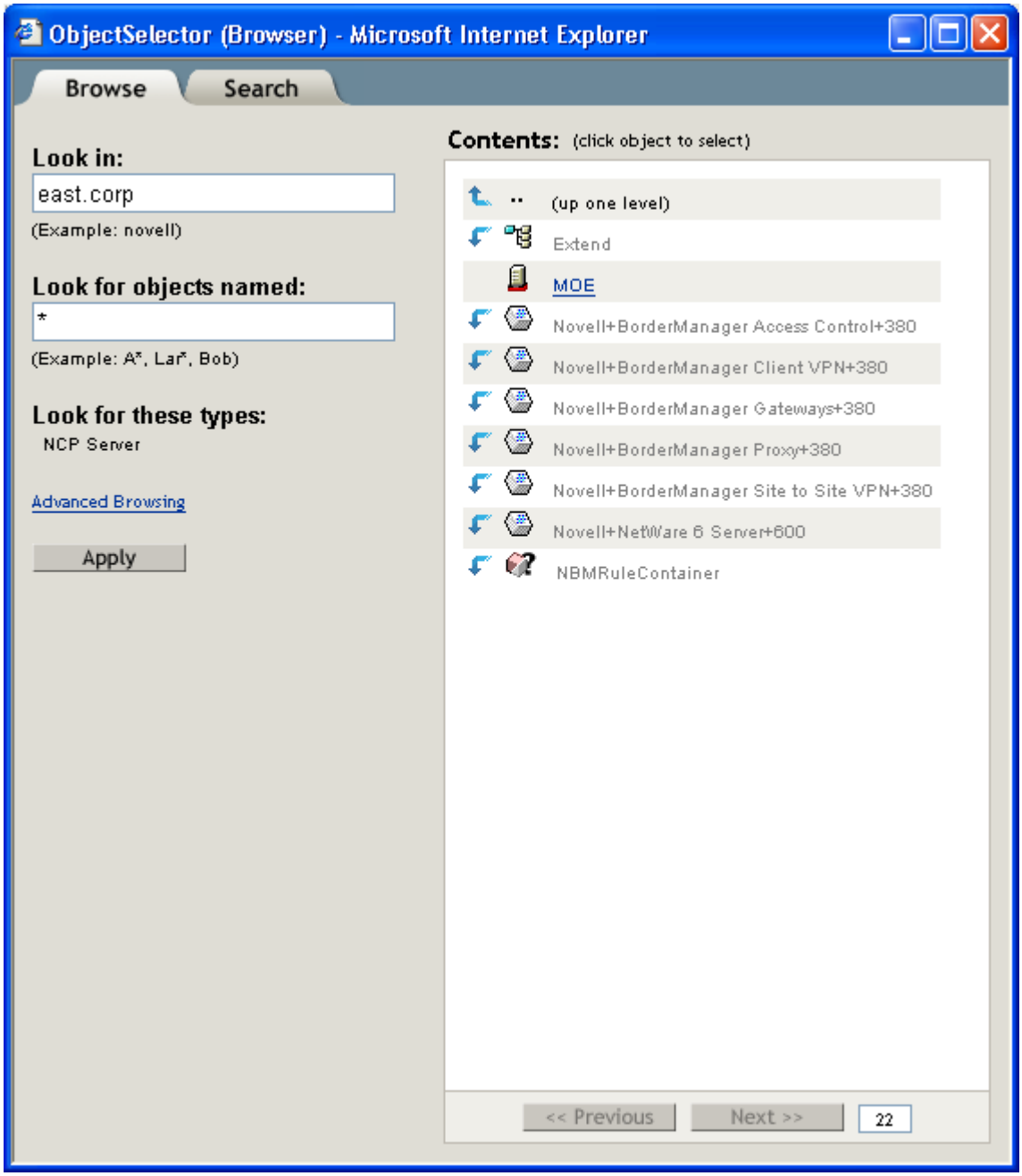
Log in to iManager in the same NDS tree as MOE, expand the **NBM VPN Management** link and select **NBM VPN Server Configuration**.

In this case, we know there are no VPN servers defined in the tree yet, so there is no use in searching for one.

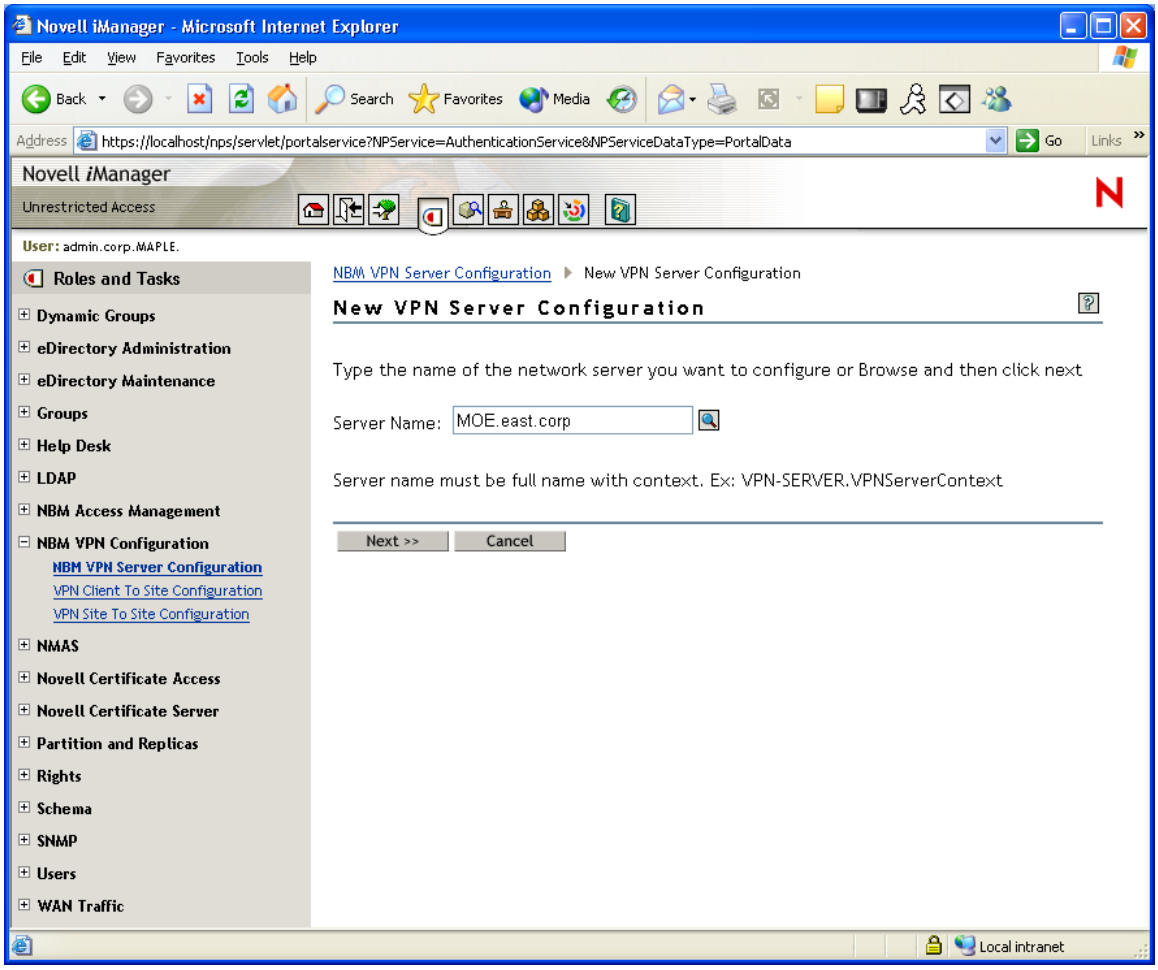
Click the **Add** button in the **VPN Server List**.



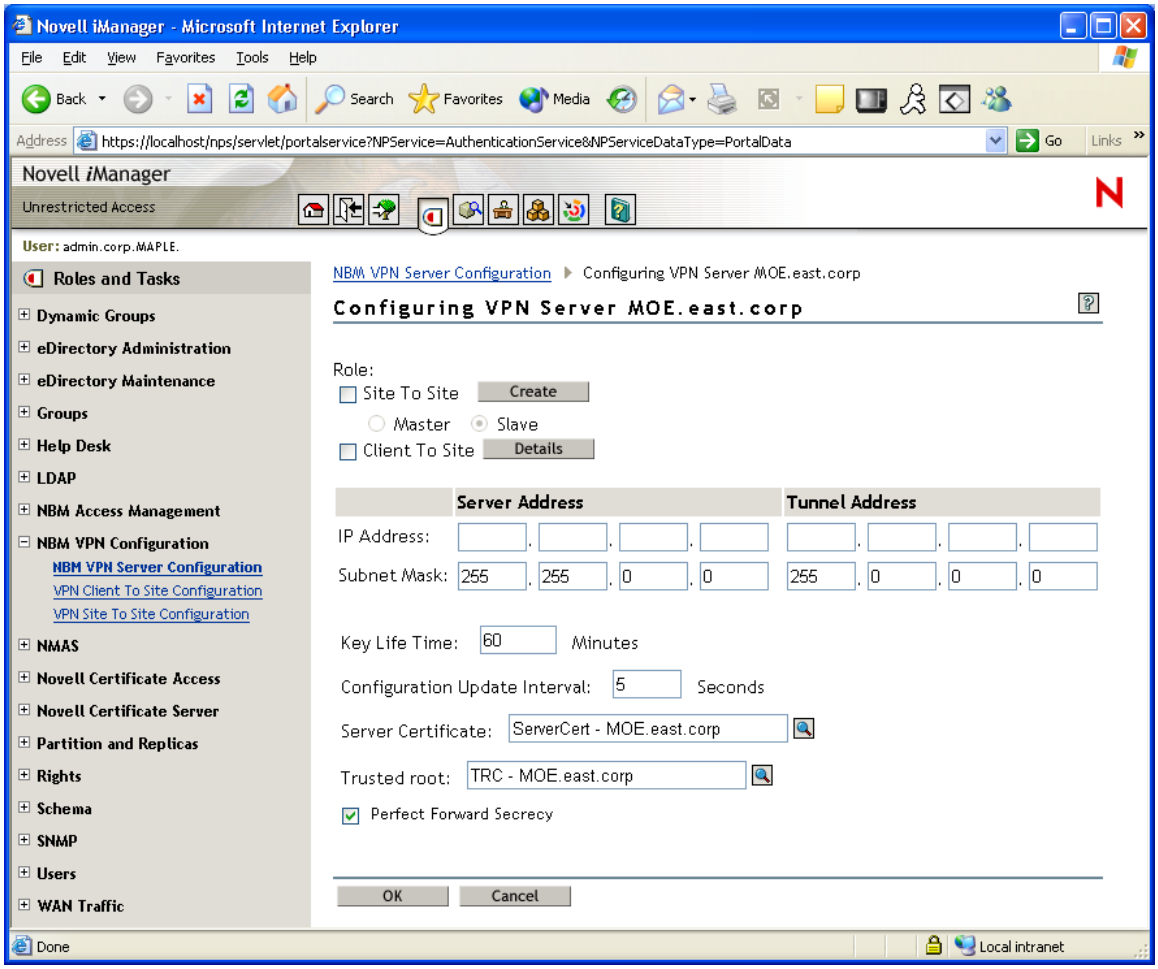
Browse to the server to be configured, in this case MOE. Click on the **browse icon** next to the **Server Name** field.



Browse to, or search for, servers, and select the server to be defined as a VPN slave server, in this case **MOE**.



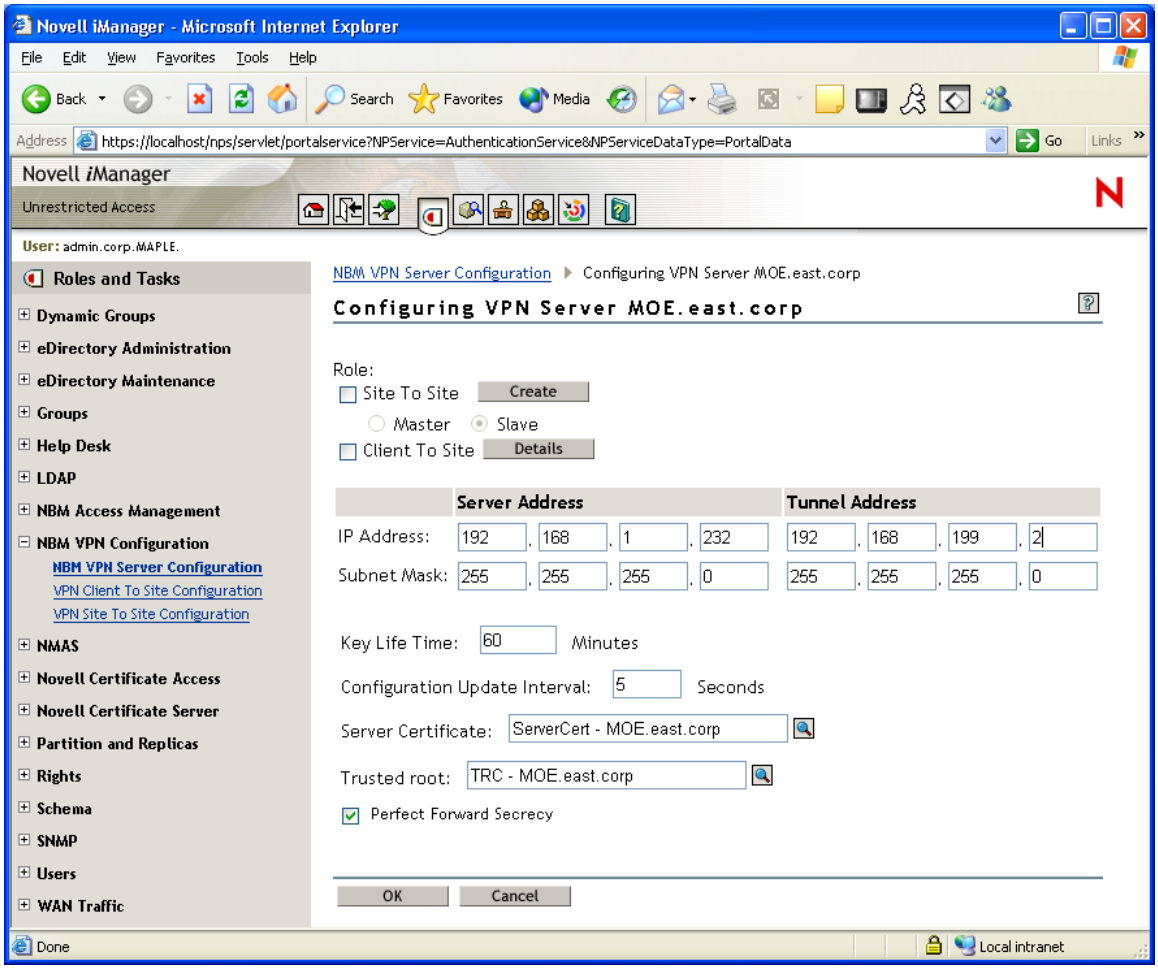
With the proper server to be configured as a VPN server selected, click **Next**.



As in the case with the Master VPN server, there are entries added here for **Server Certificate and Trusted Root** that do not yet exist. iManager will create these objects for us.

Note If you wish to manually create the server certificate, trusted root container, and trusted root objects, refer to the section later in this chapter that describes those operations.

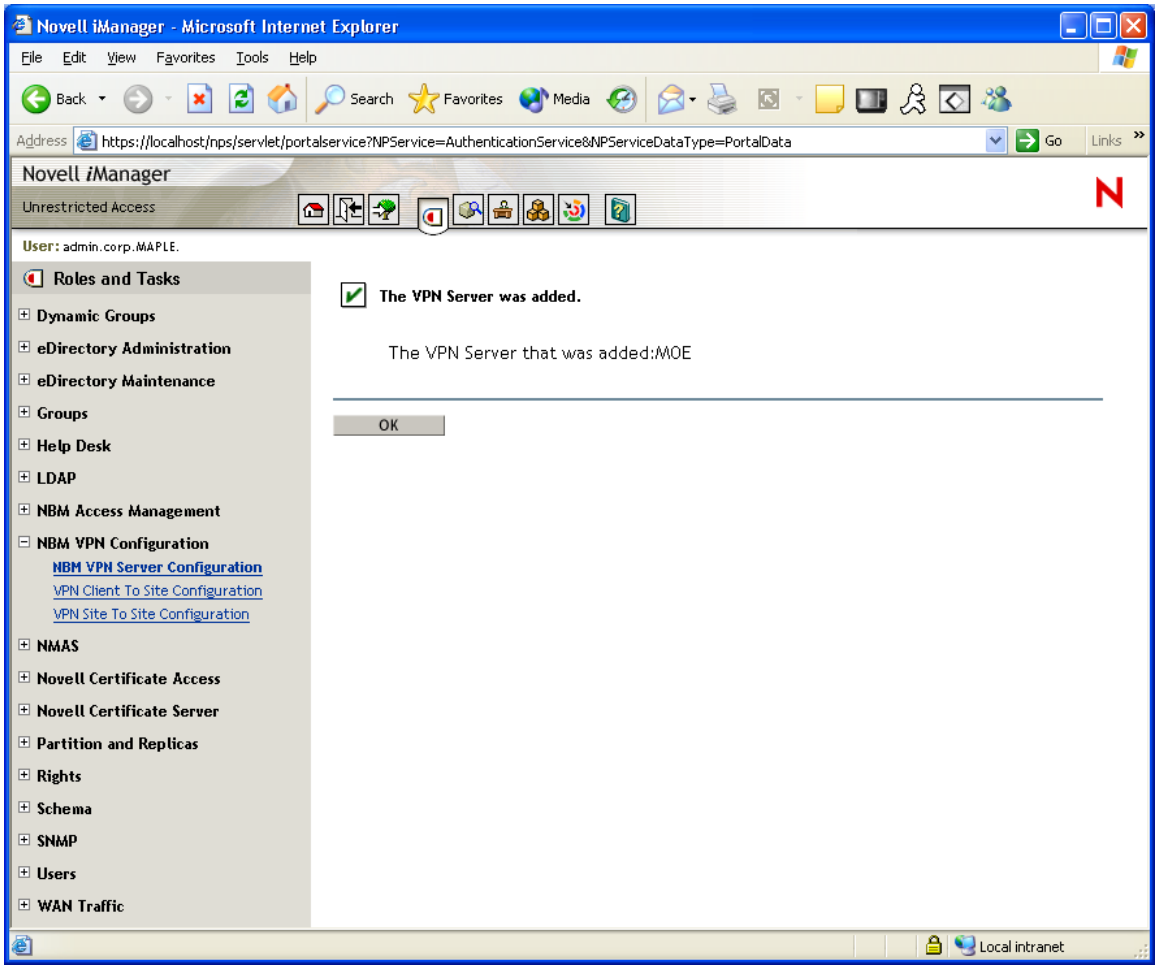
If this server is in the same tree as another VPN server, you can also browse to the location of an existing Trusted Root Container (TRC) and select that as the Trusted Root. This example uses a server that has its own TRC.



In the **Server Address** field, fill in the **PUBLIC IP Address** of the server. Refer to the network diagram at the beginning of this chapter for IP addressing assigned to the servers for this example. The public IP address of MOE is **192.168.1.232**.

Note If MOE was to be used behind a static NAT or port-forwarding router hop, the public IP address of the router or NAT pair would be configured as the Server Address here. An example of such a configuration is given later in this chapter when configuring the slave server MANNY.

Click **OK** when the desired values are configured.



You should see a screen indicating that the server was added as a VPN server. You can now configure it as a master or slave VPN server.

Click **OK**.

Configure MOE as a Site-to-Site VPN Slave Server

Prerequisites

Before you start – this example skips over the creation of the trusted root objects (TROs) required for each server. If you are creating a VPN with servers in the same NDS tree, you can simply browse to the location of the TRO as needed, since it should already have been created by iManager.

In this example, the servers are in different NDS trees, and the TROs had to be configured manually. **The examples for doing that are shown later in this chapter**. Examples are shown using both ConsoleOne and iManager. You can choose either tool as you like, but the TRO's need to exist before you continue with the next steps as you will have to select them in the following steps.

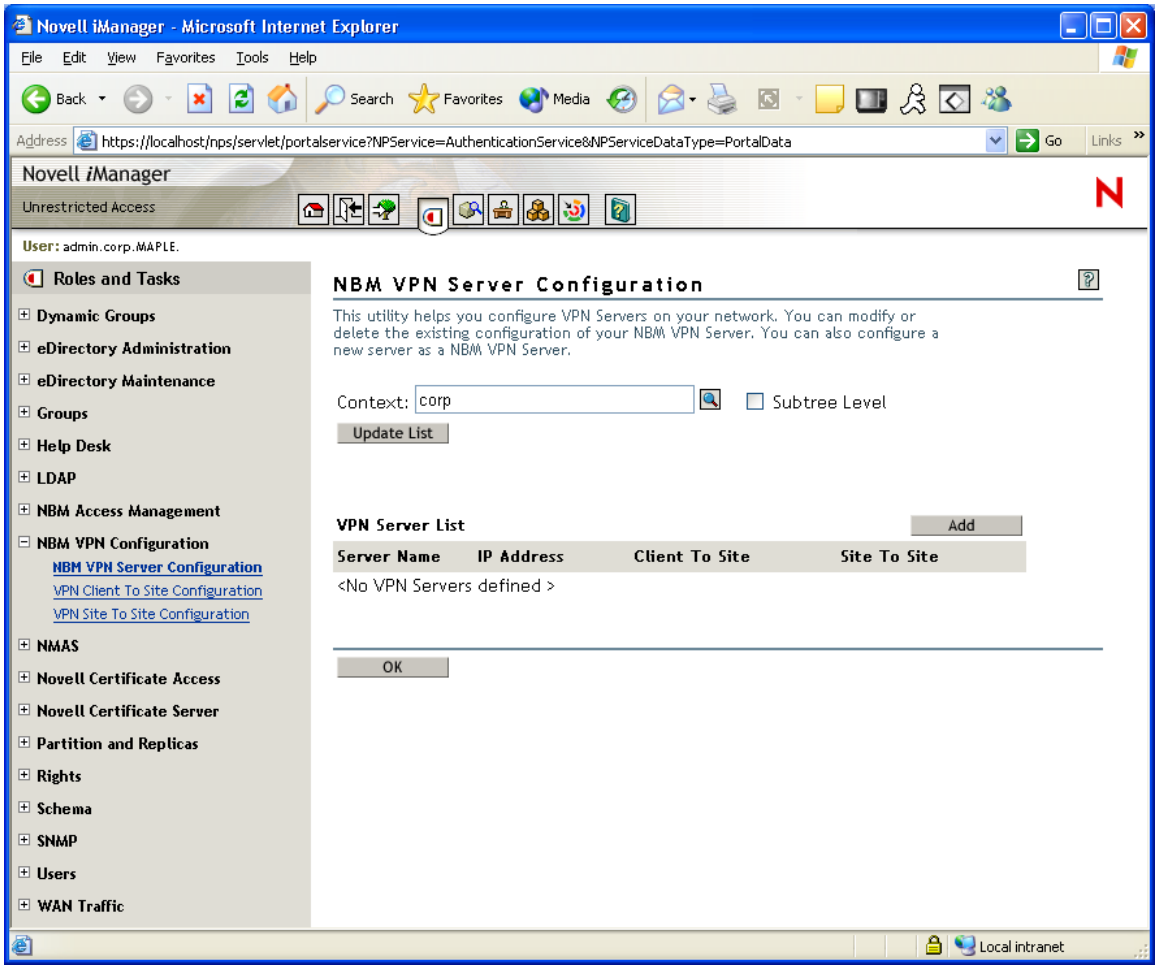
In order to configure MOE, you will need to have a TRO in MOE's NDS tree for JACK.

In order to add MOE as a VPN slave server to the VPN member list, you will have to have a TRO in JACK's NDS tree for MOE.

You will also need the Public Key Certificate Subject Name for both MOE and JACK's VPN certificates.

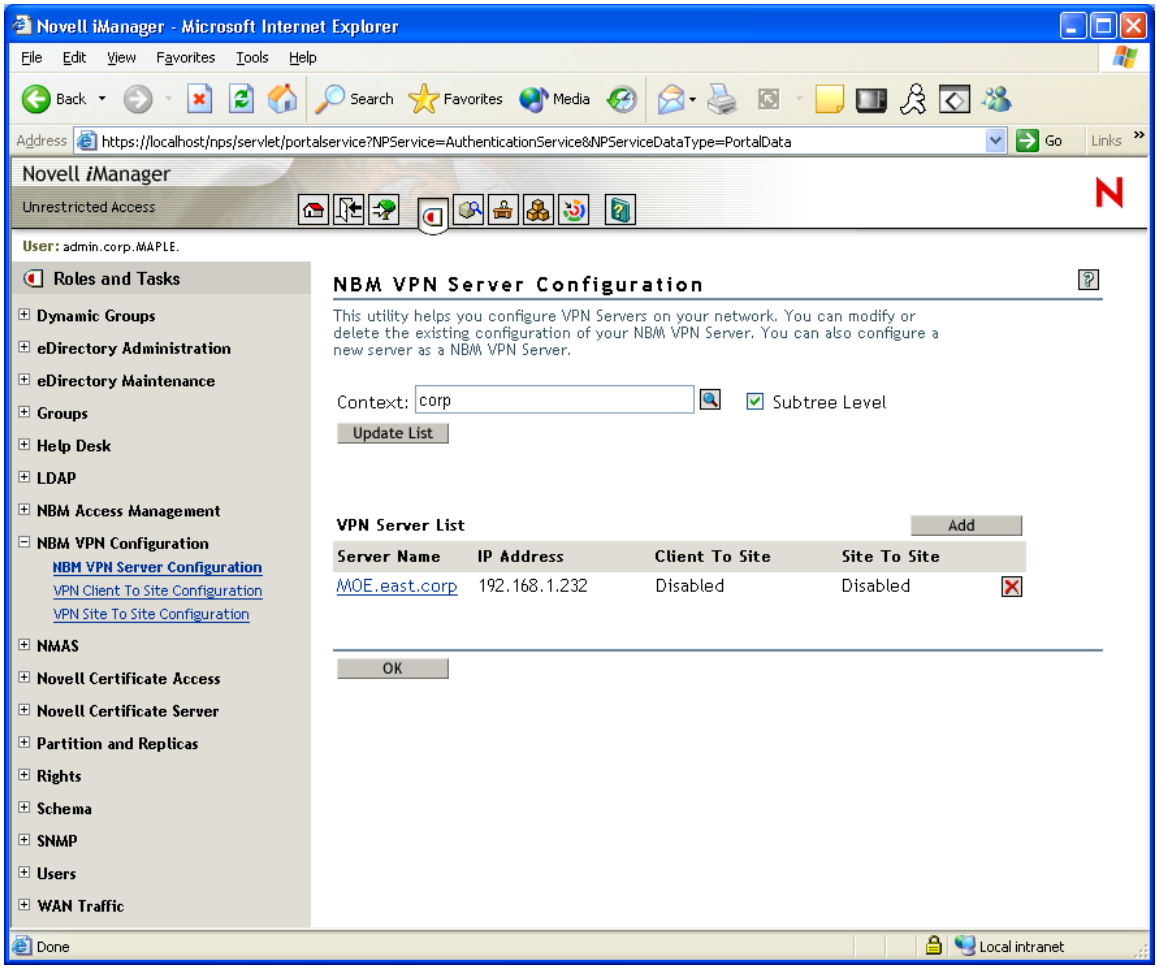
Configuring MOE

The menu shown below appears at the end of the previous step, or if you log into iManager in server MOE's NDS tree and select **NBM VPN Server Configuration** from the frame on the left of the screen.



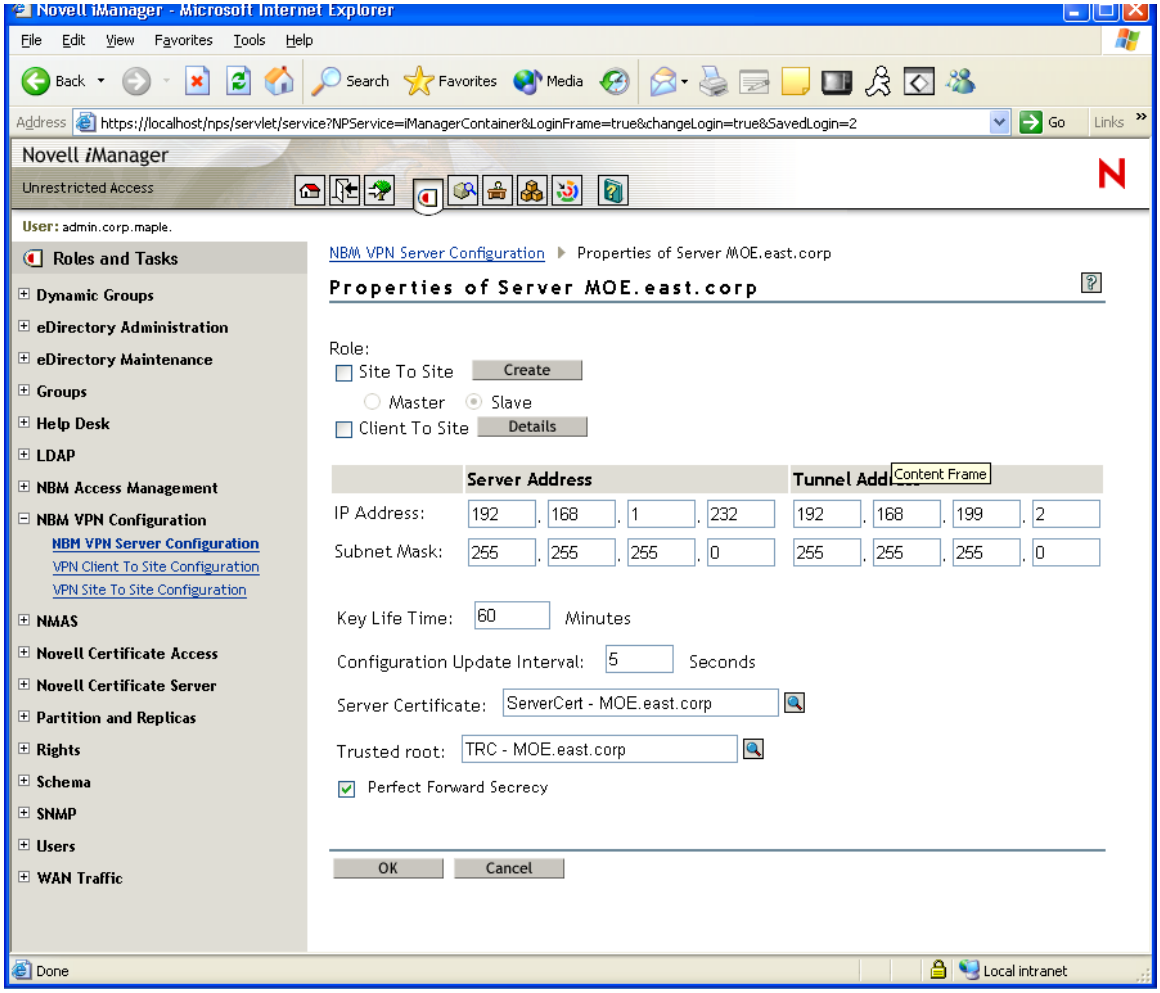
You should now be at the main **NBM VPN Server Configuration** menu. You can now browse to the VPN server to continue the configuration.

Select the **Subtree Level** option and click on **Update List** to have iManager search for VPN servers from the designated Context on down through the tree, **or manually browse** to the VPN server.



MOE is shown as a VPN server, with both **Client To Site** and **Site To Site** disabled.

Click on the **MOE.east.corp** server link to select it.

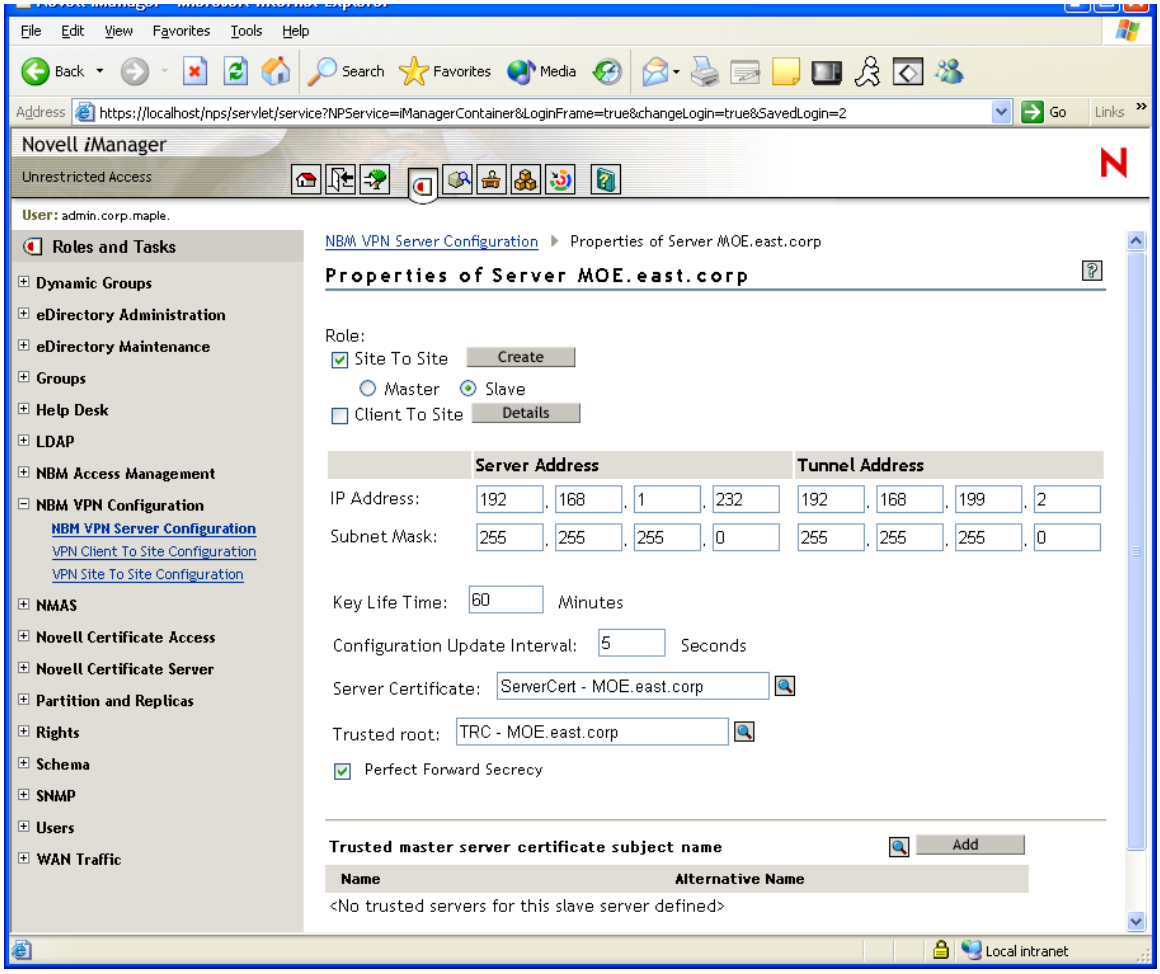


In order to add MOE as a VPN slave server, we will require a Trusted Root Object (TRO) to be created for the master VPN server JACK. Since MOE and JACK are not in the same NDS tree, we will have to manually create a Trusted Root Object (TRO) in MOE's Trusted Root Container (TRC). In order to do that, we will have to export the master server's VPN certificate's public key to a .DER file, and use that file to create the TRO.

You can export the certificate using either iManager 2 or ConsoleOne. **Examples of doing that are shown later in this chapter**. *This example assumes the export of the .DER file, and the creation of the TRO have already been done.* This example assumes that you already know the Subject Name of the master server's VPN certificate.

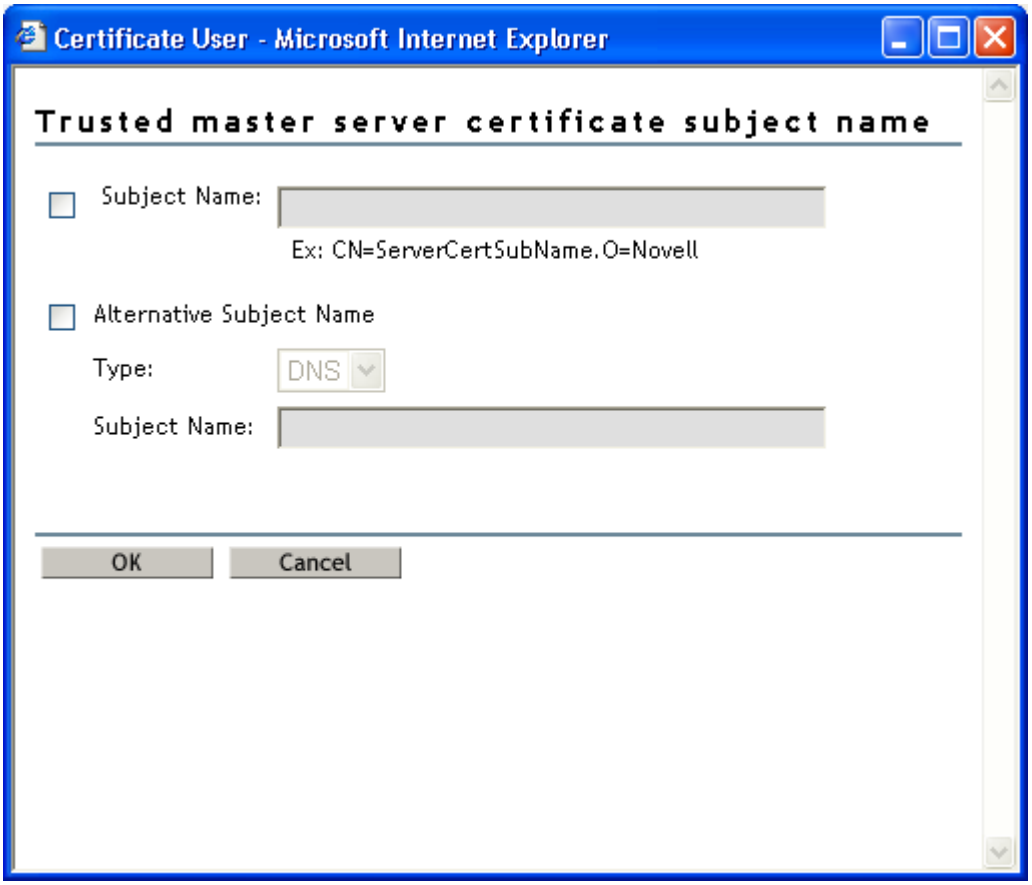
In order to add this server to the master VPN server's list of slave servers, you will also have to export this server's VPN certificate to a .DER file, and import it at the master.

Click on the **Site-to-Site Rule** option, while leaving the **Slave** option selected.



Entries at the bottom of the menu appear, as previously defined.

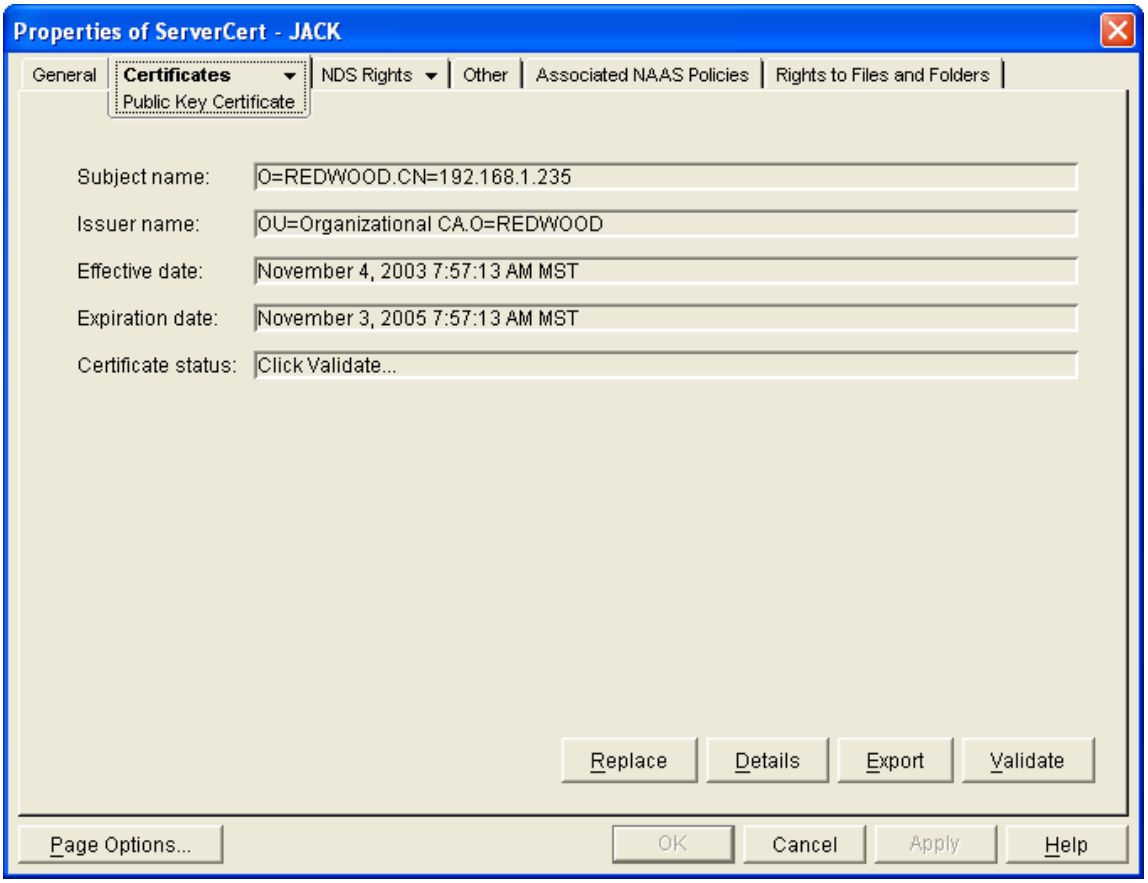
We now need to add data for the **Trusted master server certificate subject name**. Near the bottom of the menu, click on the **Add** button.



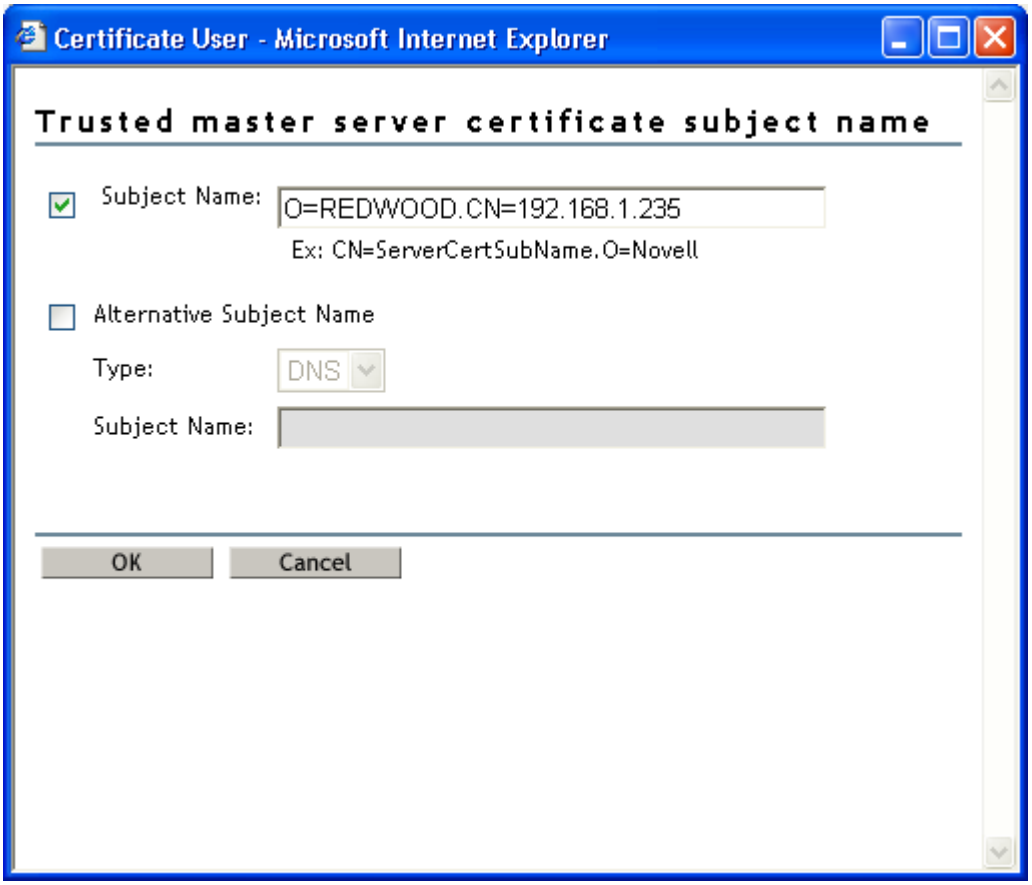
A menu appears. We must fill in the **Subject Name**.

Alternative subject name is not supported at this point.

The following screenshot is taken from ConsoleOne, and shows properties of the VPN certificate for JACK, created automatically by iManager when master VPN server JACK was configured. **The screenshot is shown here so that the reader will see where to find the subject name of the certificate to be filled in as the Trusted master server certificate subject name**. All slave servers in the same Site-to-Site VPN will use the same subject name when configuring the Trusted master server certificate subject name.



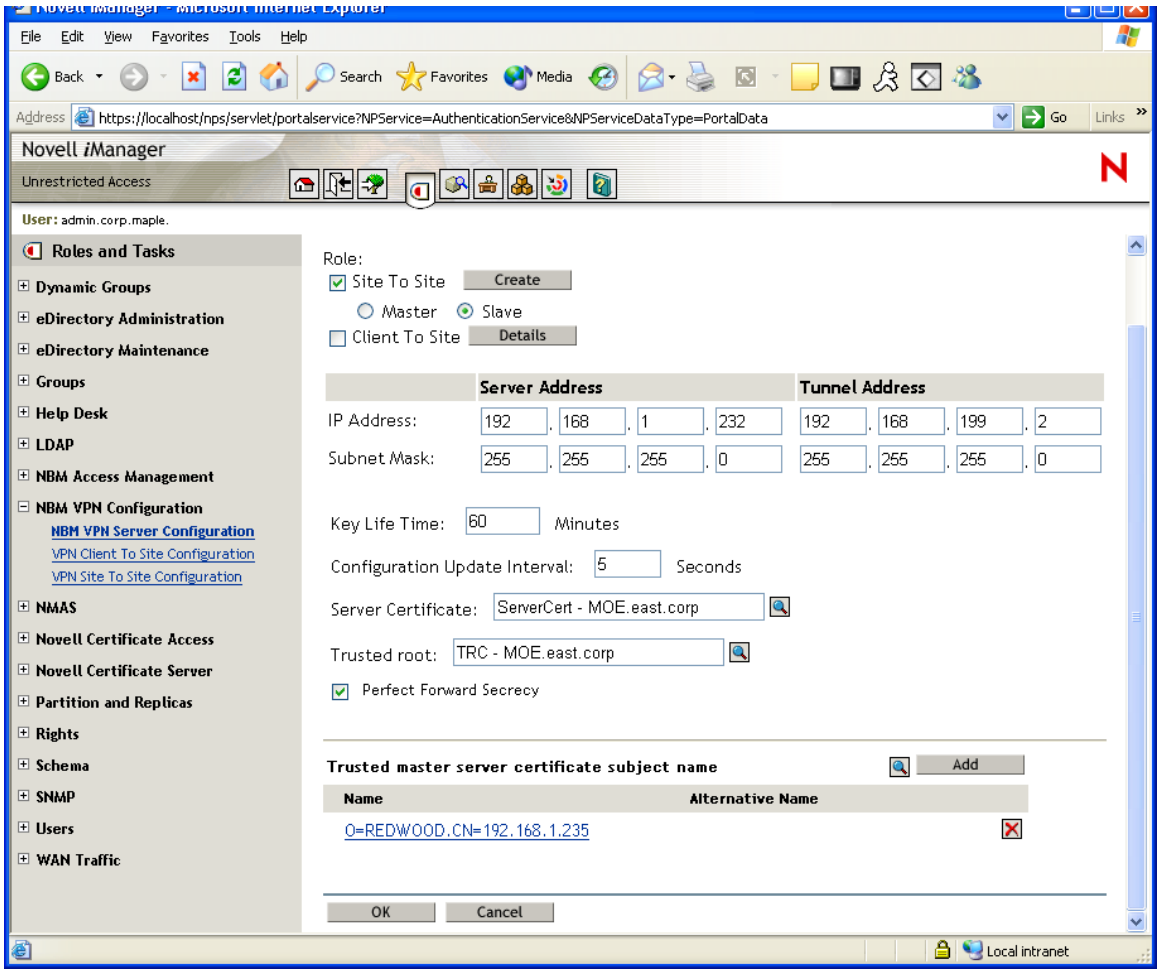
The screenshot above shows properties of the NDS object ServerCert – JACK. Note that the Certificates tab is set to Public Key Certificate in the drop-down menu. The subject name is O=REDWOOD.CN=192.168.1.235.



Type in the **Public Key Certificate Subject Name** for the master VPN server's VPN certificate (ServerCert – JACK has been configured earlier).

In this case, the subject name for JACK's VPN server certificate is **O=REDWOOD.CN=192.168.1.235**.

Click **OK**.

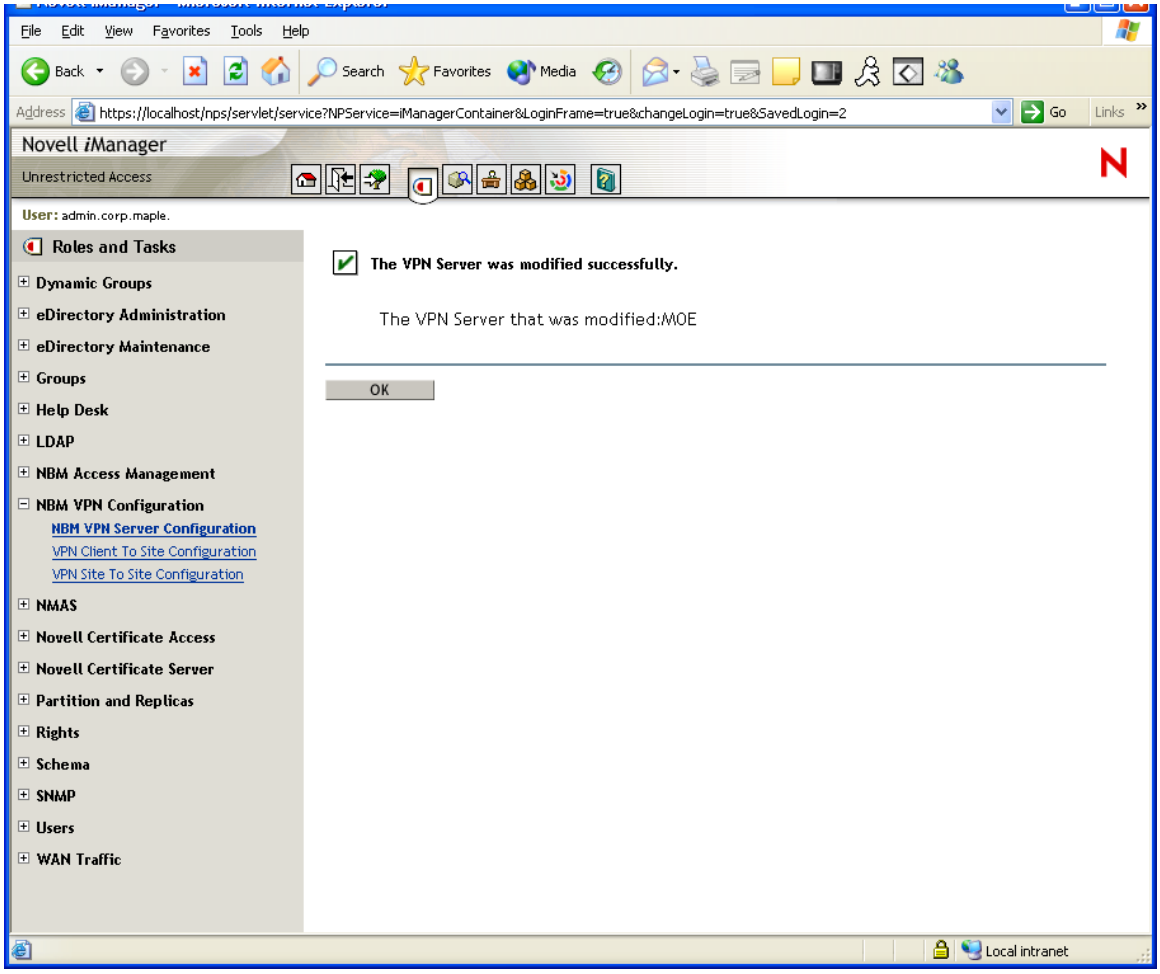


The VPN server configuration menu for a slave server appears, with the **Trusted master server certificate subject name** configured.

As a slave VPN server, MOE only needs to have its VPN public IP address, VPN tunnel IP address, and the subject name for the master server's certificate configured, in order to join the VPN. The master server will contact the slave server and push down the configuration data to the slave. Once the master has configured the slave, the slave server will know how to contact the master, and any other slave servers it may need to.

In order for the slave server to know that it is being contacted by the master, it has to verify the master's VPN certificate, using both the subject name of the master's certificate (entered here), and a Trusted Root Object (TRO) for the master. The master's TRO must be located in the slave's Trusted Root Container (TRC). If your VPN slave is not in the same NDS tree as the master, or is not using the same TRC as the master, you must configure the master's TRO manually, as shown later in this chapter.

Click **OK** to save the changes.



You should see a success menu. Press **OK** to continue.

If the Master VPN server were already configured for MOE as a slave, the servers should begin setting up a Site-to-Site VPN link within 15 minutes.

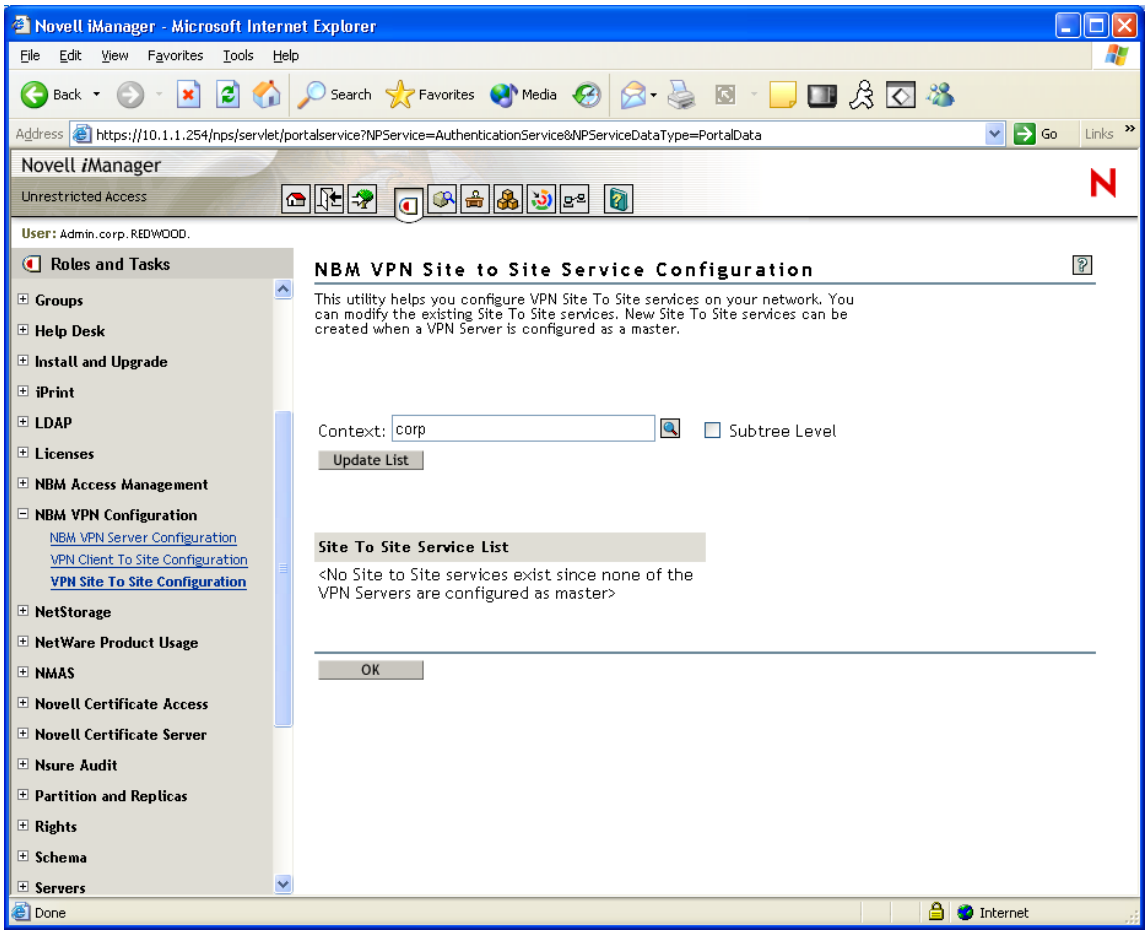
If you want to force the process to start more quickly, you can try using the commands STOPVPN and STARTVPN on the master VPN server.

You can also use the Synchronize All command in the VPN Monitoring section of Novell Remote Manager for the Master VPN server to try to force VPN connectivity to start.

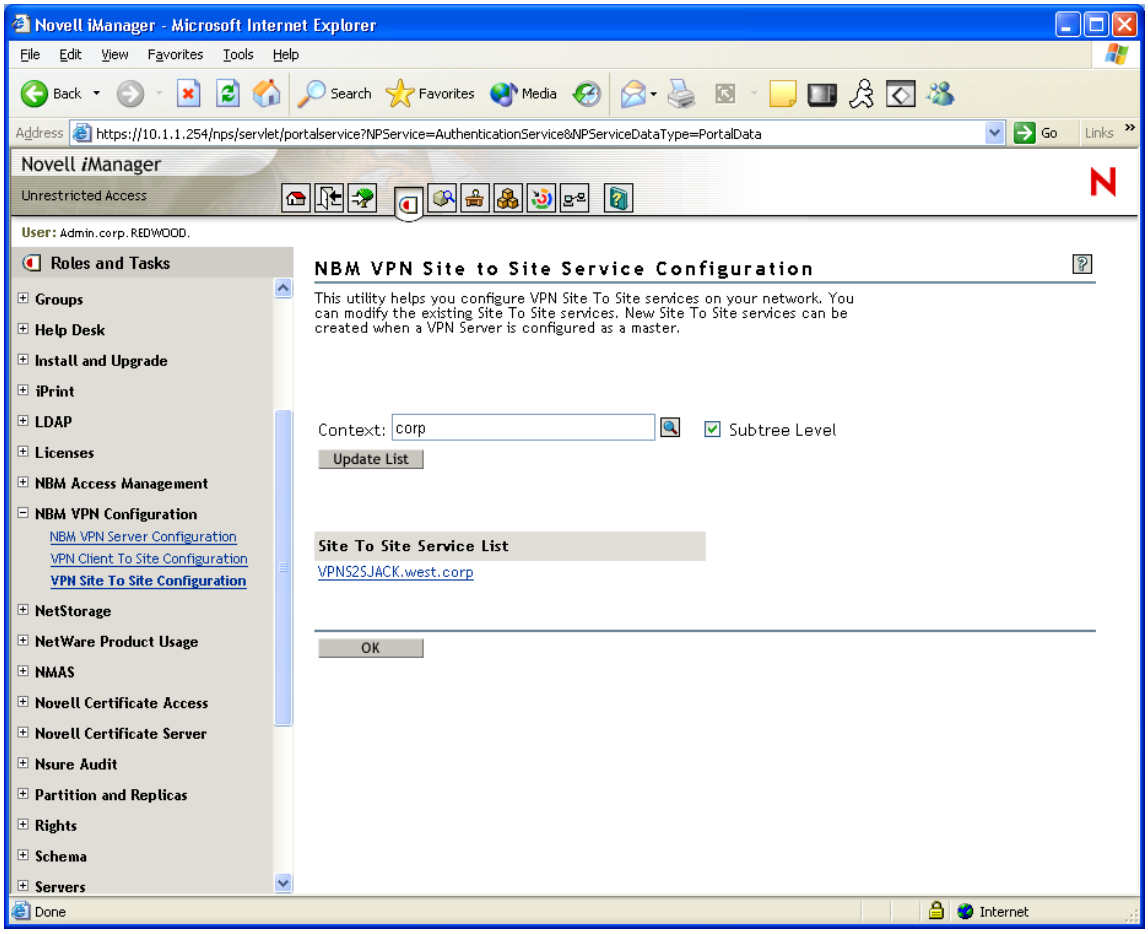
Adding MOE as a VPN Slave Server to the VPN

When you have configured a server as a Master VPN server, you can add slave servers to its Site-to-Site VPN member list. Now that MOE has been configured, we can add it as the first VPN slave server.

In iManager for the master server (JACK), expand the **NBM VPN Configuration** link in the left panel.



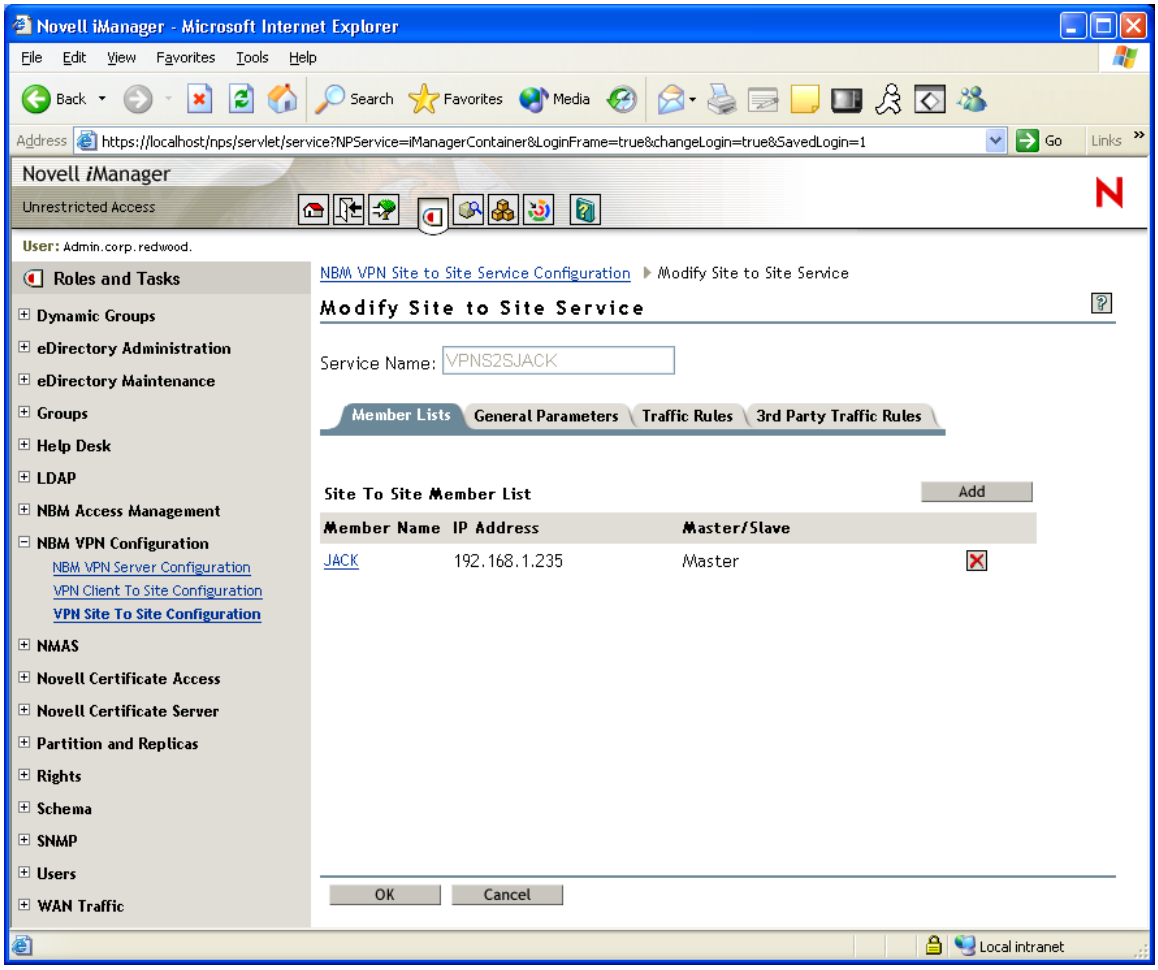
Select **VPN Site To Site Configuration**



Either allow iManager to search out a Site-to-Site VPN service, by clicking **Update List** button with **Subtree Level** option enabled, or browse to the service.

Because JACK was configured as the Master Site-to-Site VPN server earlier, a **VPNS2SJACK.west.corp** object appears in the **Site To Site Service List**.

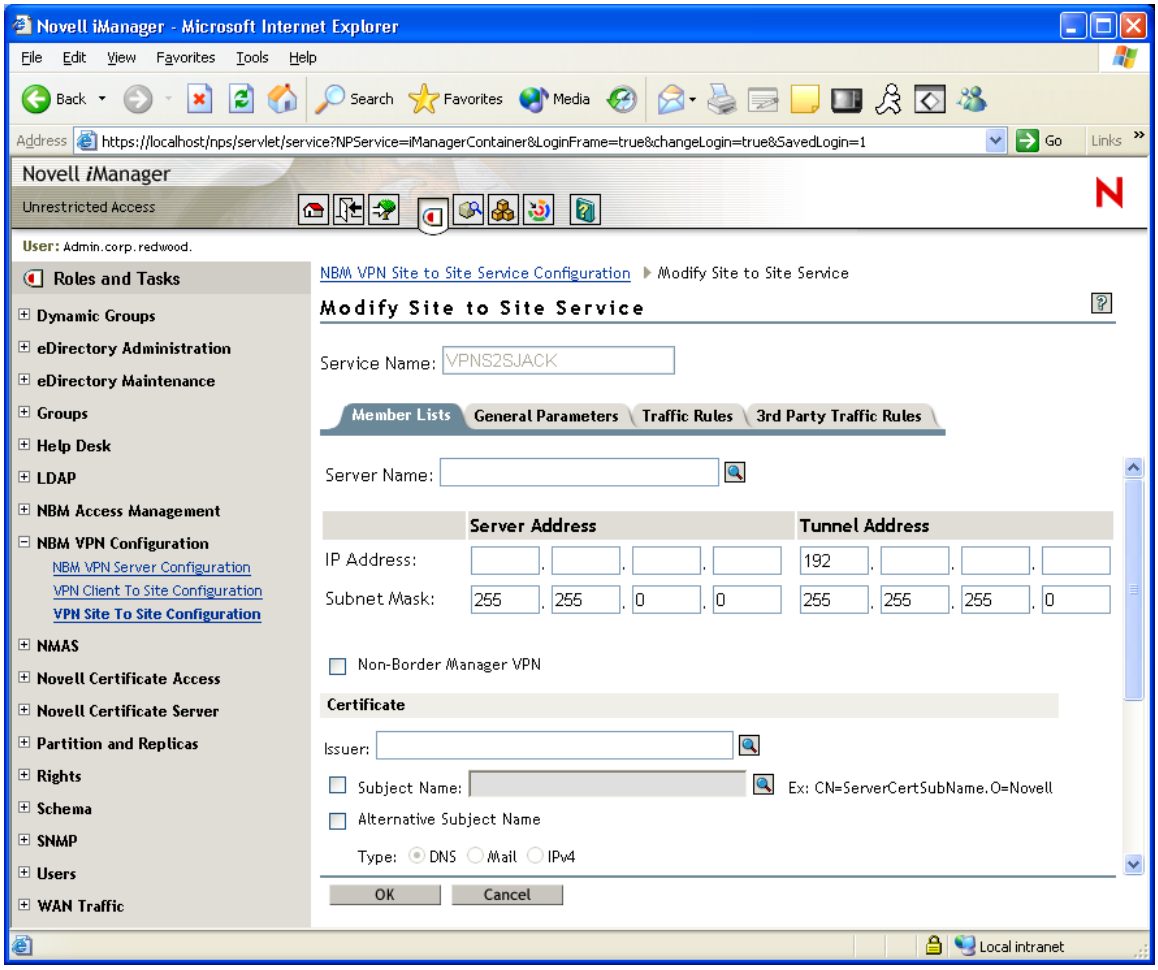
Click in the **VPNS2SJACK.west.corp** link.



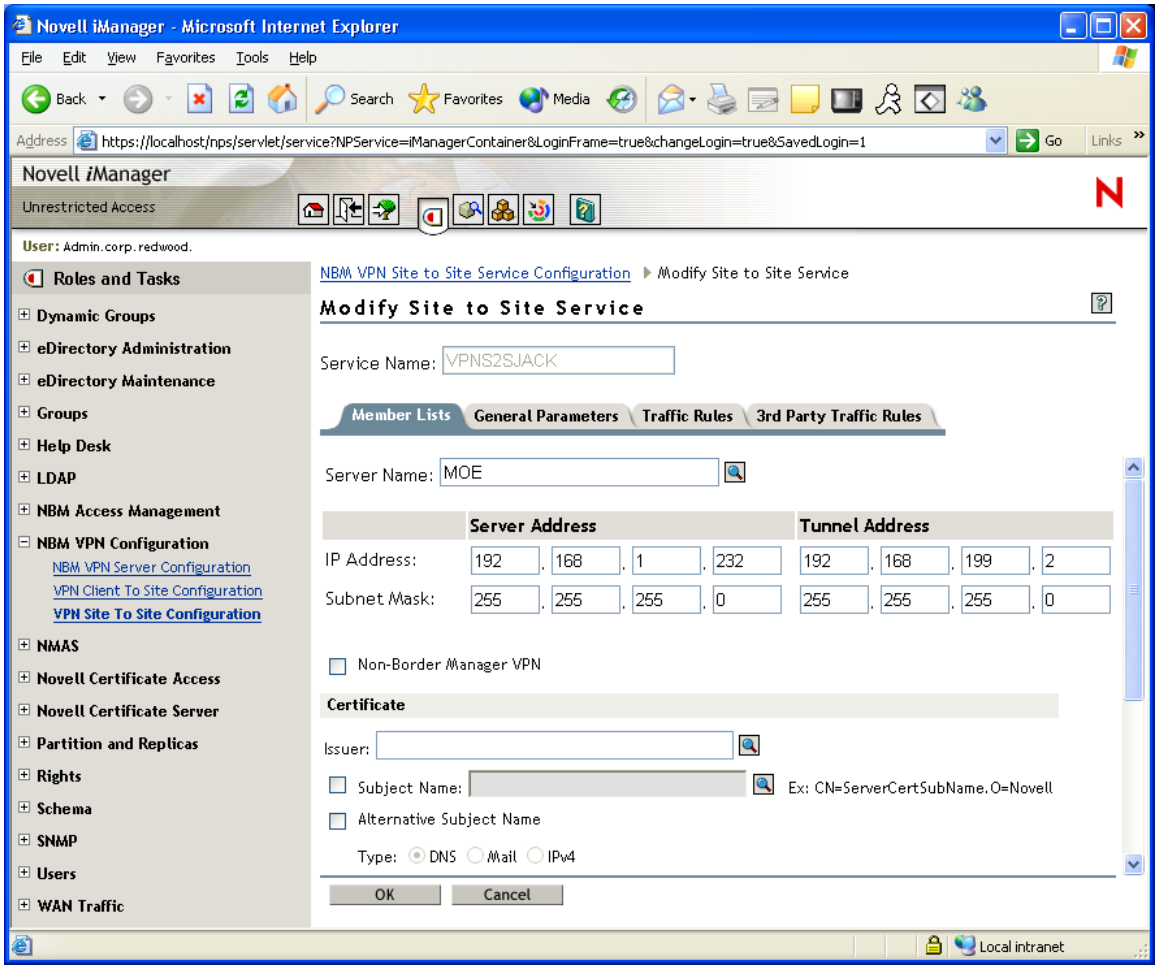
At this point, we simply have a Master VPN server in the **Site To Site Member list**. We want to add a slave server (MOE), and also set various parameters.

First we will add MOE as a slave server. Click on the **Add** button.

Note A TRO for MOE has already been created, as shown in examples later in this chapter.



If MOE were in the same NDS tree, we might be able to browse to it. Since it is in another tree, we must type in the server name.



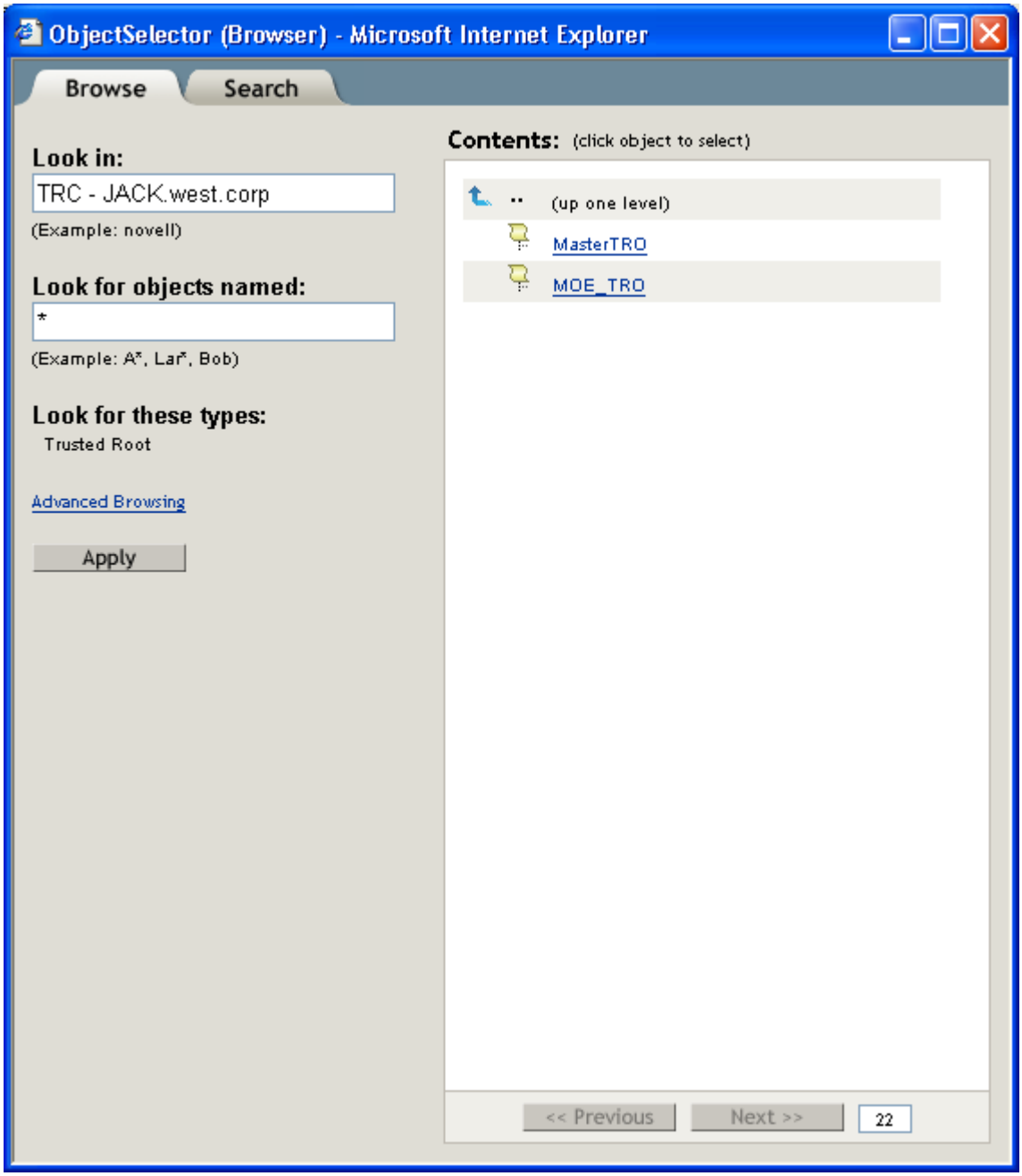
In the **Server Name** field, type in the slave server name (MOE)

Refer to the network diagram at the beginning of this chapter for IP addressing used in this example.

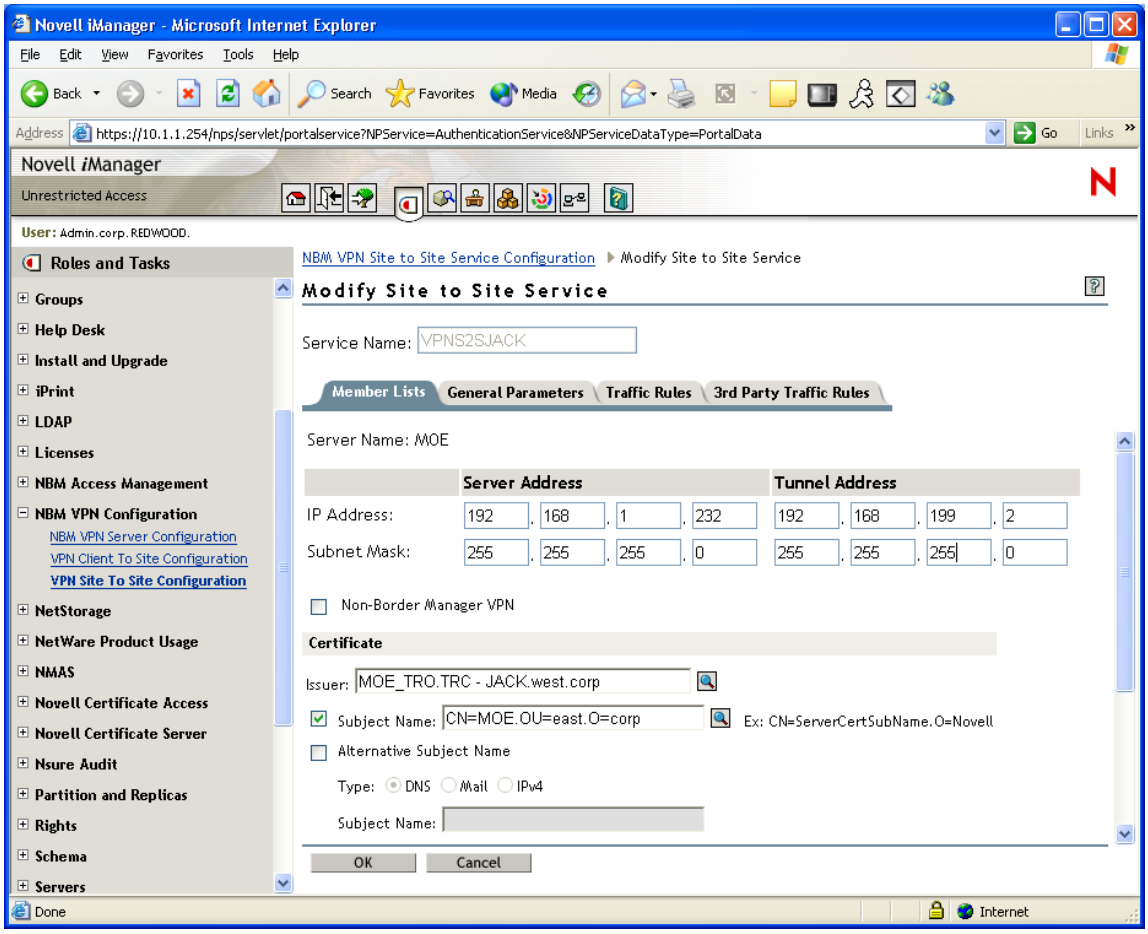
In the **Server Address** field, type in the MOE's public IP address to be used for VPN communications (192.168.1.232 here)

In the **Tunnel Address** field, type in the IP address to be used by the slave server as a VPN tunnel IP address (192.168.199.2 here). The VPN tunnel address must be an address within the same subnet as the VPN tunnel address configured on the master VPN server, and all other slave servers to be in the same VPN tunnel.

Now we must enter the certificate data for MOE. Click on the **browse icon** for the **Issuer** field and browse to JACK's Trusted Root Container. In that container, we have already created the Trusted Root Object for MOE's VPN certificate. The TRO from MOE is the **Issuer**. (Examples of creating TROs are shown later in this chapter).



Select the Trusted Root Object (TRO) for the MOE slave server. In this example, we use **MOE_TRO**.

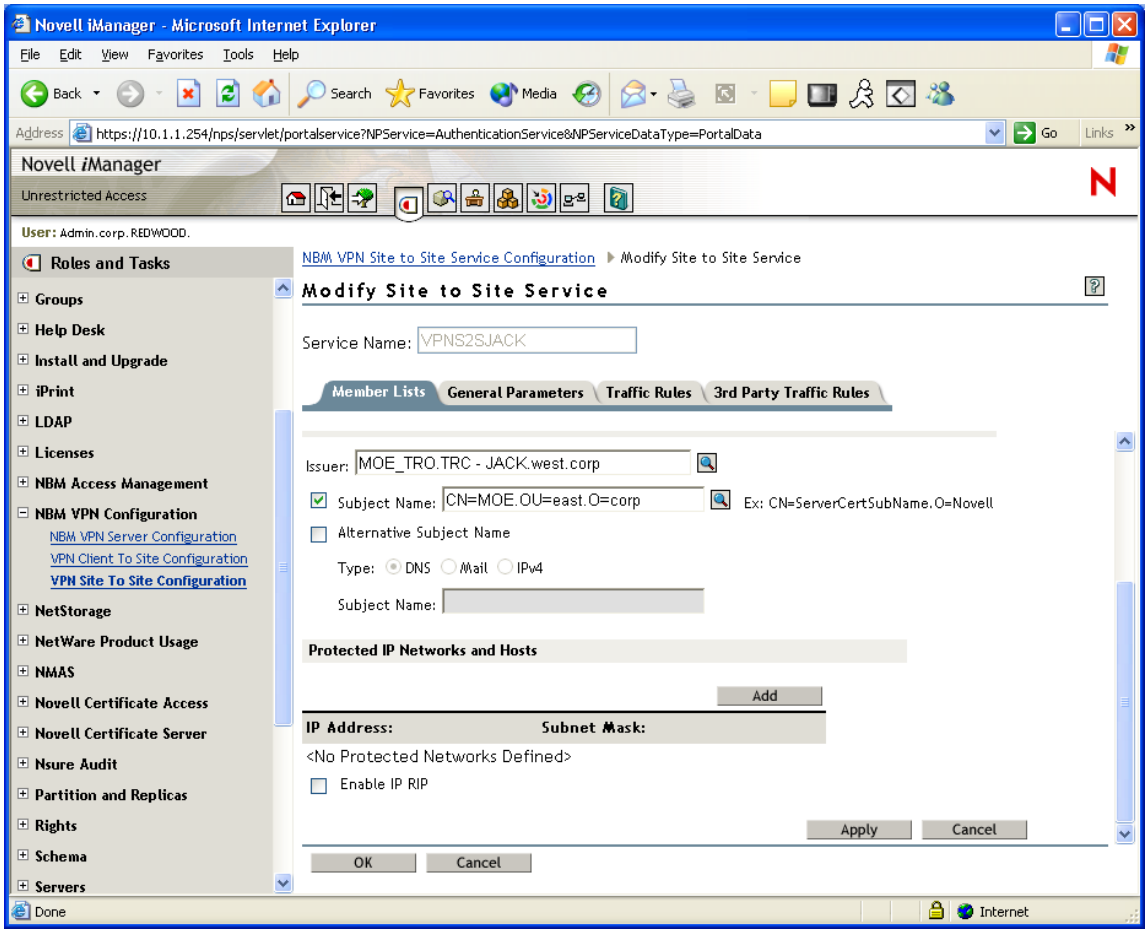


Next, select the **Subject Name** box, and type in the Subject Name for the MOE VPN certificate. (The Subject Name is in the Public Key Certificate field of the ServerCert – MOE certificate in MOE's NDS tree.)

In the example shown, the Subject Name is **CN=MOE.OU=east.O=corp**.

Note If MOE were in the same tree, we could browse to the certificate instead of having to type in the subject name.

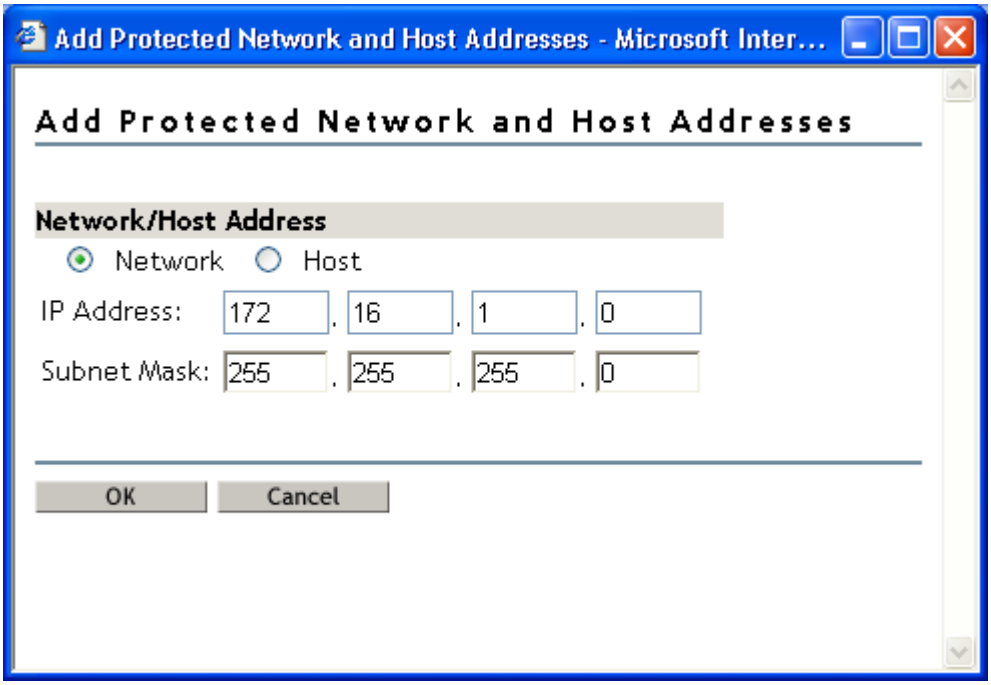
Now, in case you cannot see the entire field, scroll the Member List window up to see additional fields to fill in.



We need to enter the **Protected IP Networks and Hosts** next.

While we could set up the VPN to only allow traffic for particular hosts on the slave VPN network, for this example we want to allow VPN traffic to any internal IP address on the MOE network.

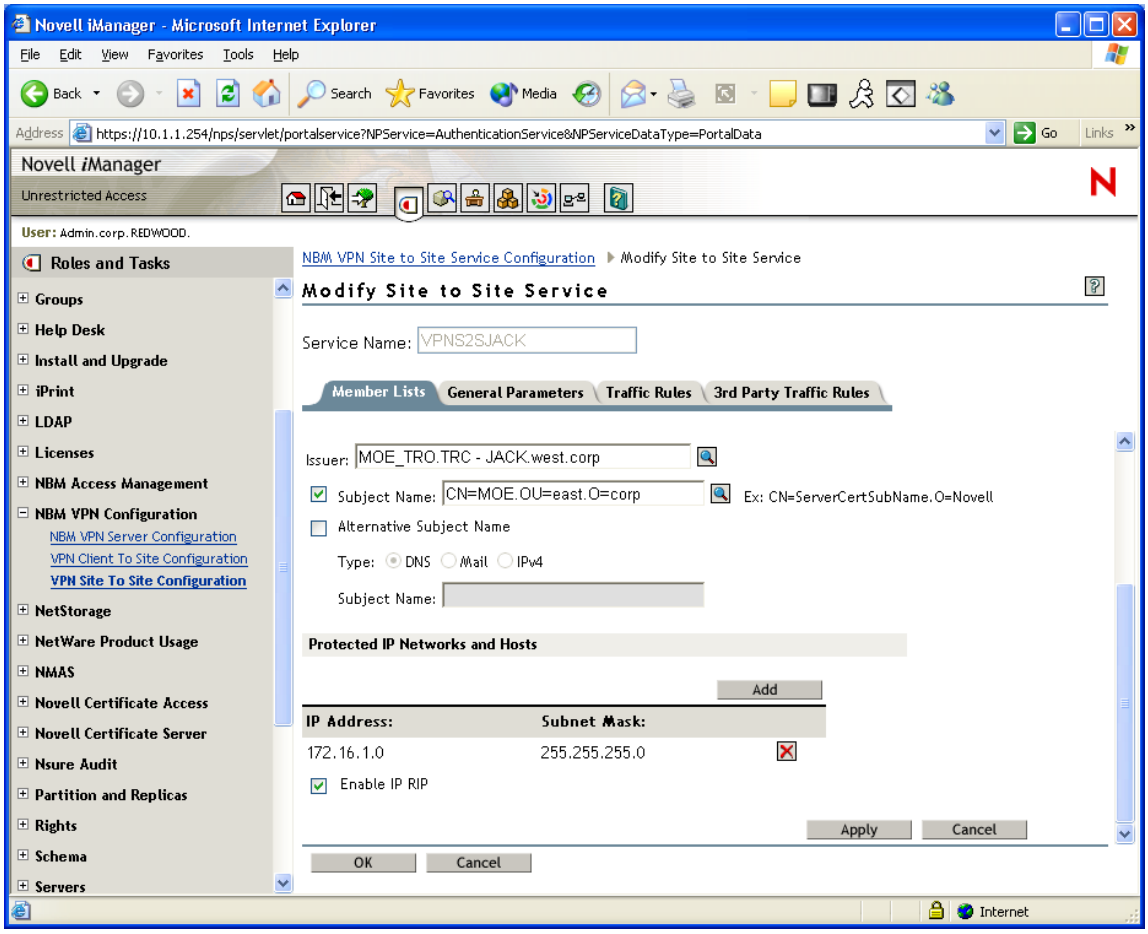
Click on the **Add** button for **Protected IP Networks and Hosts**.



Fill in the **network address** and **subnet mask** of the private LAN behind the VPN slave server MOE. These addresses will be accessible from the other side of VPN Site-to-Site links.

In this example, a network address of **172.16.1.0** and subnet mask of **255.255.255.0** is being used.

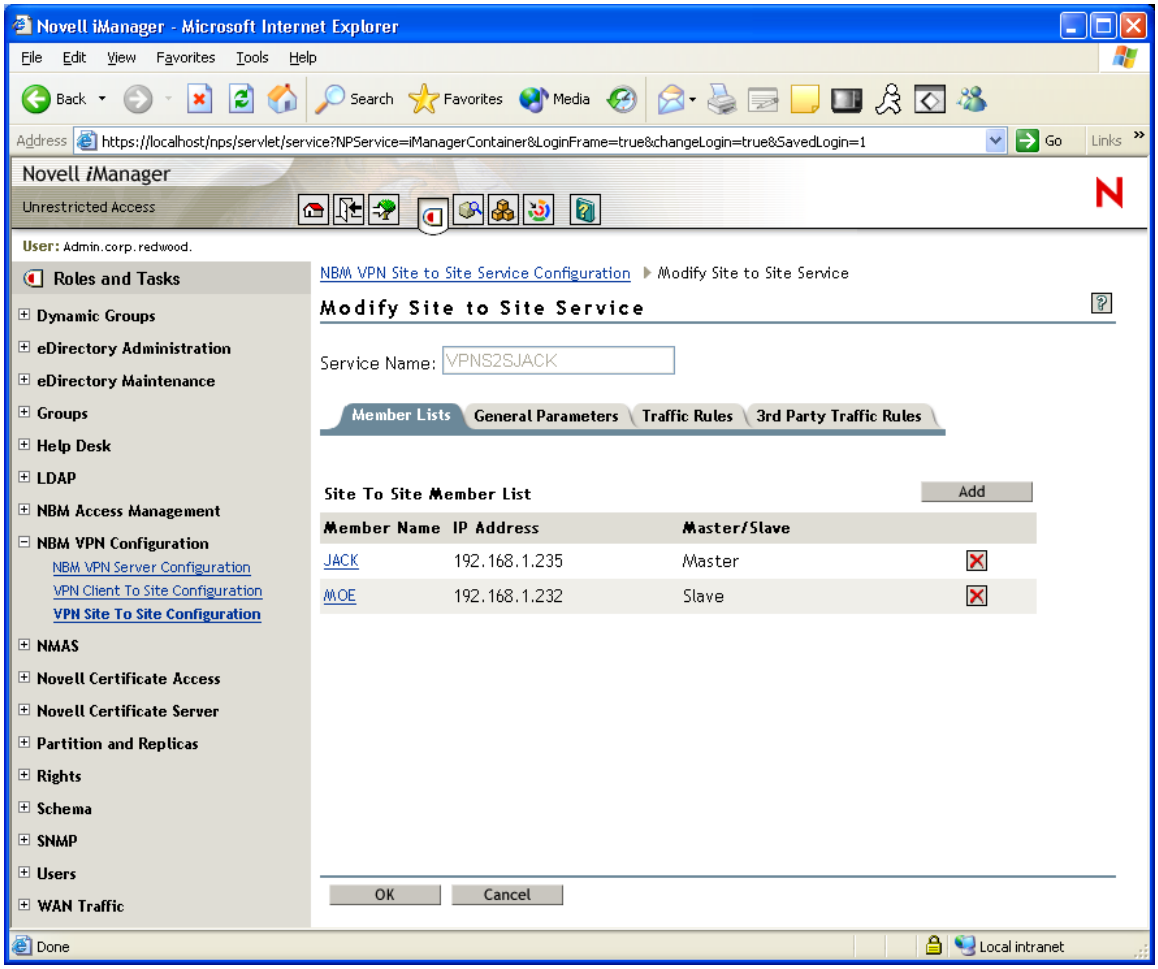
Click on **OK** when done entering both address and mask.



The IP address(es) you entered now show up on the Protect IP Networks and Hosts list.

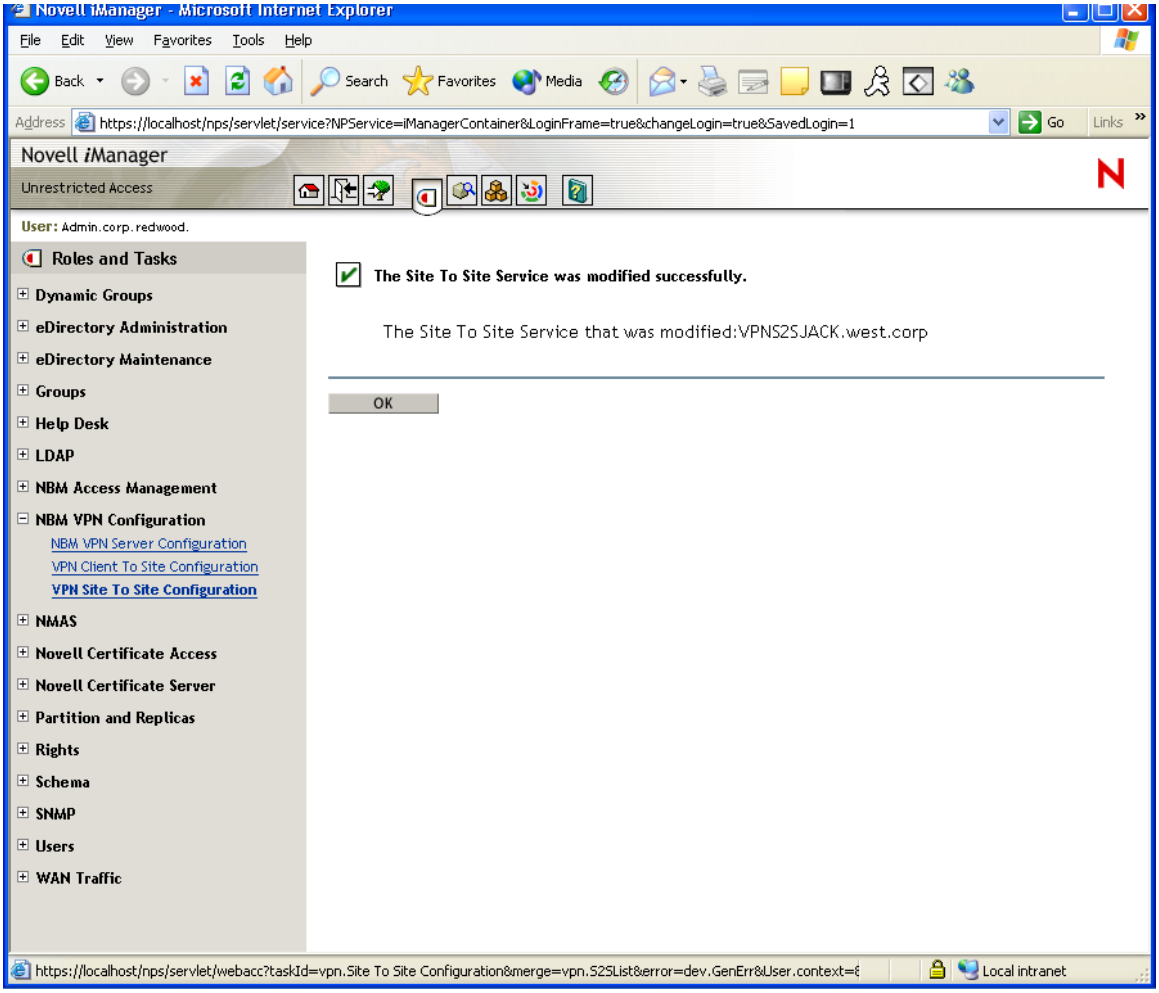
Select the **Enable IP RIP** option to have the protected network address(es) automatically configured for the master VPN server, and any other slave VPN servers.

Click on **Apply** to save these changes.



MOE is now added as an entry in the **Site To Site Member List**.

Click **OK** to save settings.



You should see a success message. Click **OK**.

At this point, the Site-to-Site VPN service on JACK should be trying to contact MOE. (Assuming MOE was already configured as a Site-to-Site VPN slave server).

Configuring Site-to-Site VPN Parameters

In the previous section, we configured two servers in a Site-to-Site VPN. However, we did not change any of the default parameters for VPN communications.

Once you have defined Master Site-to-Site VPN server, you have the option of setting various parameters that will apply globally across the VPN links.

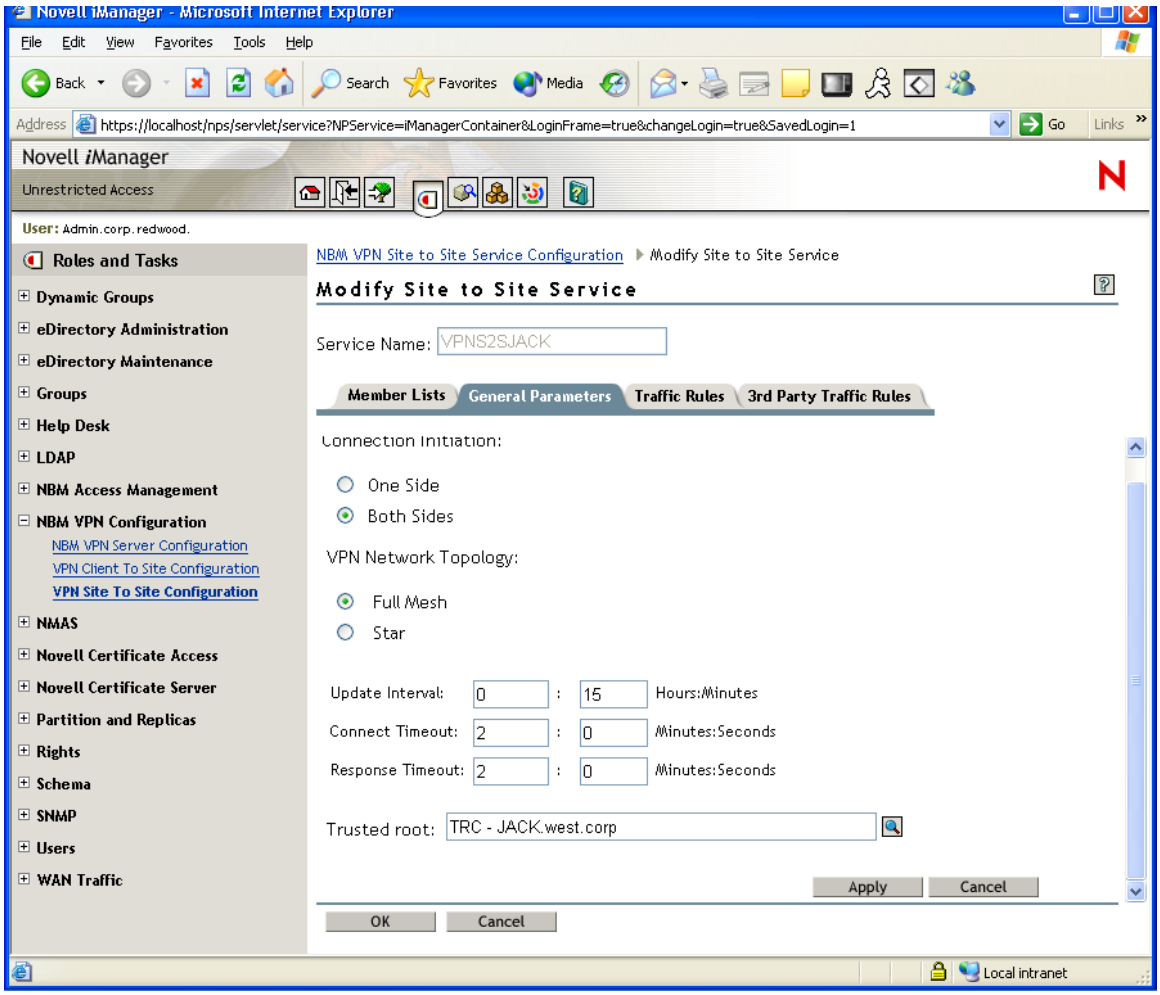
You can configure **general parameters**, including whether the VPN uses a star or mesh configuration, whether one side only or both sides can initiate a connection, etc.

You can configure **traffic rules**, which can allow or deny certain kinds of traffic across the VPN.

You can configure **third-party traffic rules**, which apply to non-BorderManager servers, or BorderManager servers defined as non-BorderManager server. Third-party traffic rules are similar to BorderManager server rules.

From the **Modify Site To Site Service** menu in iManager on the Master VPN server, click **on General Parameters**.

General Parameters



In this example, we leave the settings at default values.

Either VPN server in the network can contact the other server to begin VPN communications.

Full Mesh topology means that slave servers will be able to talk directly to each other, without having to communicate to the master VPN server.

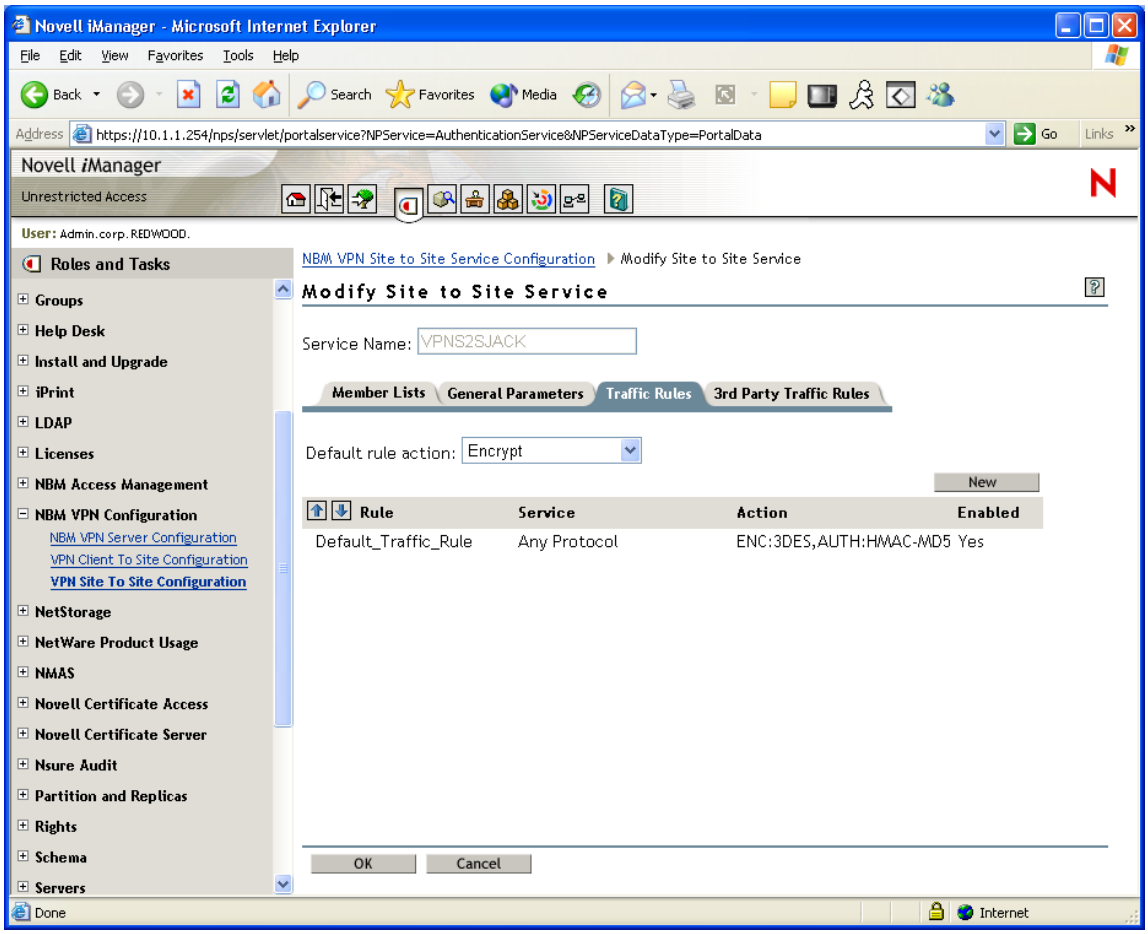
The update interval is set to the default value of 15 minutes, which is how often the VPN master server will attempt to verify connections or reconnect as needed to reconfigure a slave server.

The Connect Timeout and Response Timeout values are both set to the default of 2 minutes.

If you change any of the parameters, click Apply before proceeding.

Click on **Traffic Rules**.

Traffic Rules

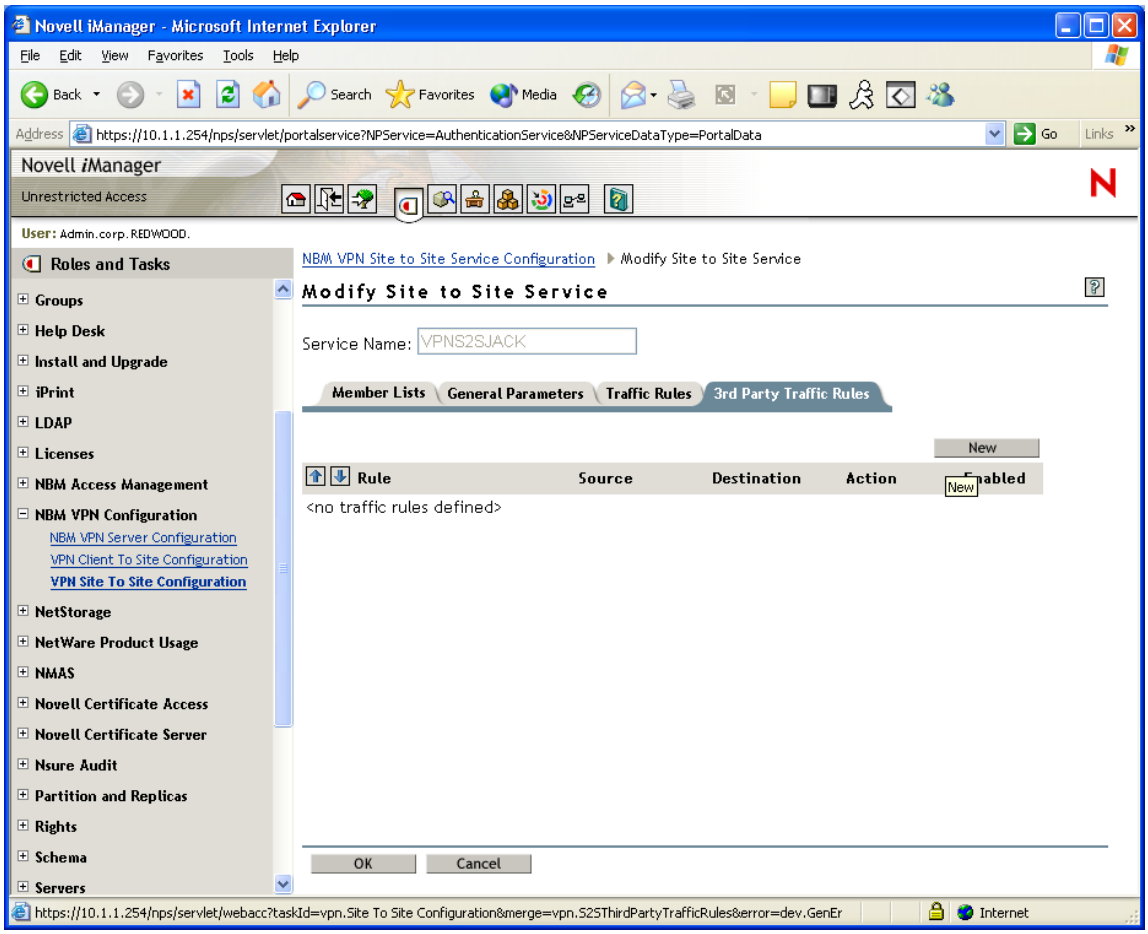


The default value for Site-to-Site VPN traffic is to allow all traffic and encrypt it. For a Site-to-Site VPN between networks in a single corporation, this is highly desirable.

However, there are circumstances where not all traffic should be allowed over a VPN. Perhaps only HTTP should be allowed between VPN servers, in a case where a Site-to-Site VPN is being used to link client networks to your network, but you only wish the clients to be able to access a particular web server. In that case, the protected networks behind the master server might limited to a single host, and an new traffic rule could be create that allows, and encrypts, only HTTP, while denying all other traffic.

It is important to note that these rules are read in sequence from top to bottom, like proxy access rules in NWADMN32. Therefore, if we put a Deny HTTP port 80 higher in the list than the default All Any rule, that traffic will be denied while everything else will be allowed. We could also configure the VPN to allow only some particular traffic, and deny everything else, which might be suitable for a VPN connecting another corporations to yours.

3rd Party Traffic Rules



Third-party traffic rules are used for non-BorderManager servers. Use of third-party traffic rules is out of the scope of this version of this book.

This subject may be covered in more depth in the non-beta version of this book, or in a book dedicated to BorderManager 3.8 VPN.

Configure MANNY as a VPN Server Behind NAT

In this example, a NetWare 5.1, BorderManager 3.8 server called MANNY is configured as a VPN slave server while located behind an inexpensive router doing NAT.

Refer to the network diagram at the beginning of this chapter for the IP addressing used.

Configuration Steps Performed

- A custom VPN certificate was created for server MANNY, using ConsoleOne, and the same settings shown in examples of configuring certificates manually later in this chapter.
- The Trusted Root Certificate from MANNY's VPN certificate was exported to a .DER file using ConsoleOne, per procedures shown later in this chapter.
- A Trusted Root Object in MANNY's Trusted Root Container was created, using ConsoleOne, from the .DER file exported from master VPN server JACK's VPN certificate.
- A Trusted Root Object in JACK's Trusted Root Container was created, using ConsoleOne, from the .DER file exported from slave server MANNY's VPN certificate.
- A Linksys router was configured to perform NAT and DMZ forwarding, and sits between MANNY and the rest of the network connections. All inbound traffic addressed to the WAN port of the Linksys router is forwarded to MANNY's public IP address. This is equivalent to static NAT with no filtering being performed. All outbound traffic is being NAT'd by the Linksys router so that it appears to have a source IP address of the WAN port of the Linksys router. This is equivalent to either dynamic NAT, or a static NAT pair between MANNY's public IP address and a public IP address on the Linksys router.

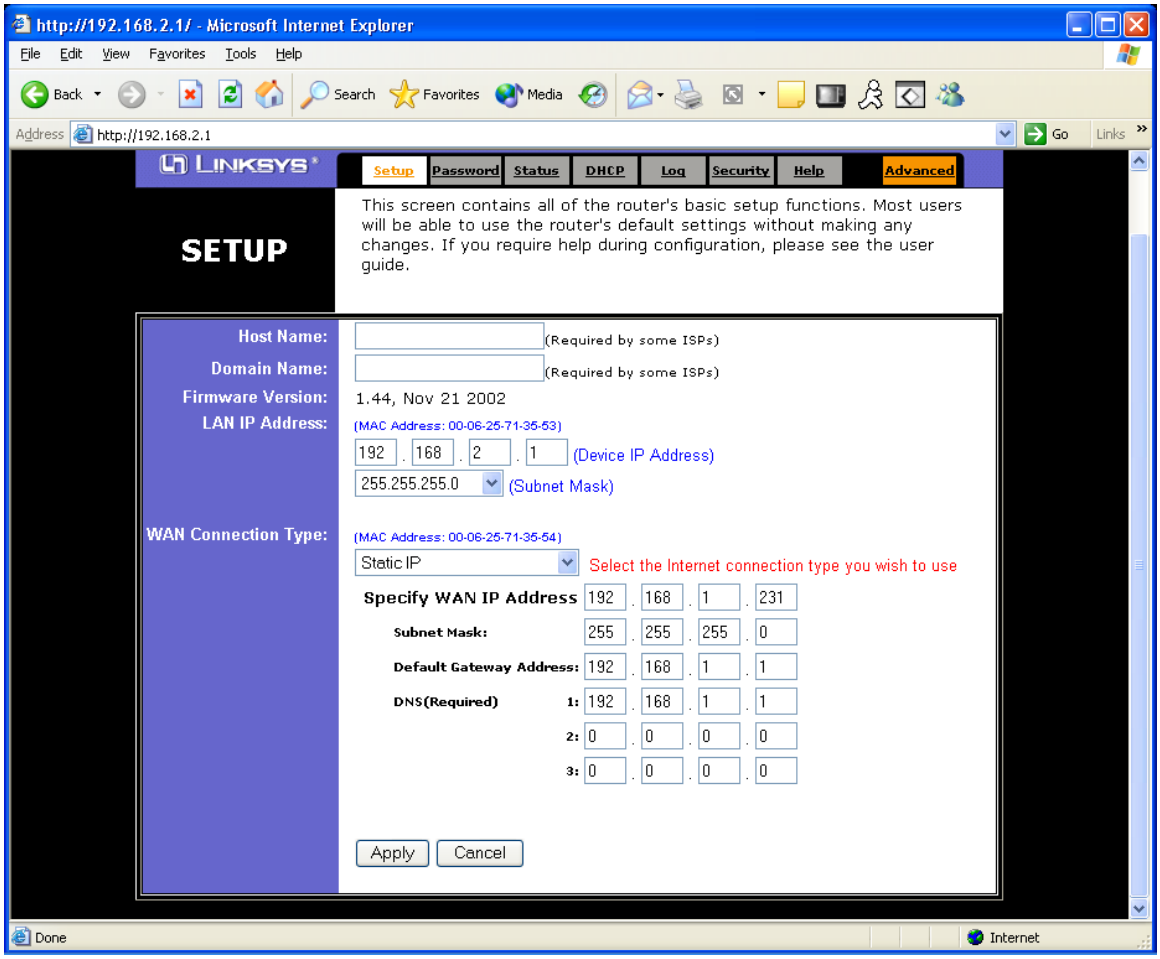
Linksys Router Configuration (NAT Configuration)

The router (Linksys BEFSR41) used in this example can be purchased for as little as $40USD new. Many similar inexpensive routers exist, and the configuration options on them are similar, though may have different titles or wording. The private side of the router is called the LAN port, while the public side is called the WAN port. A typical use for this sort of router is connecting to a cable modem or DSL modem.

Linksys calls dynamic NAT 'Gateway Mode'. All traffic passing from the LAN side through the WAN port is translated to have a source IP address of the WAN port.

Because this router cannot add a second IP address to the WAN port, it cannot really perform static NAT. Instead, routers like this do port-forwarding, where traffic addressed to the WAN port is instead forwarded to an IP address on the LAN port side. This router has a typical feature called DMZ mode, where all inbound traffic is forwarded. In addition, specific port numbers can be forwarded to particular IP addresses. However, this router can only selectively port-forward UDP or TCP traffic, and BorderManager VPN requires additional protocols. Therefore, DMZ mode is used on this router, so that the IKE protocols will be forwarded as needed.

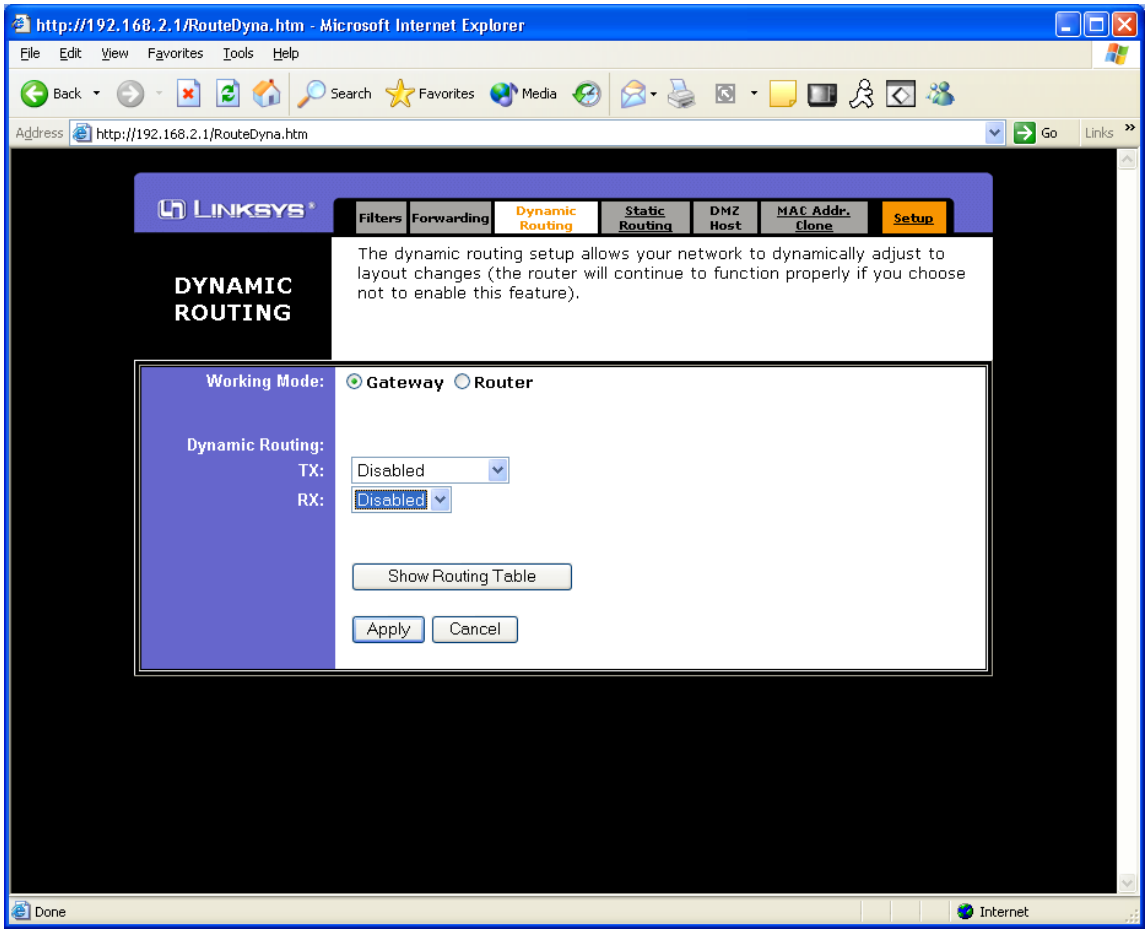
Router IP Addressing



This menu shows that the Linksys router is configured with **a LAN IP address** (private side address) of **192.168.2.1**. Server MANNY has a default route set to 192.168.2.1.

The **WAN IP address** (public side address), which is set to static, is configured as **192.168.1.231**, with a subnet mask of 255.255.255.0. Traffic intended to come to MANNY from outside MANNY's LAN must point to 192.168.1.231, where the router will forward it to MANNY.

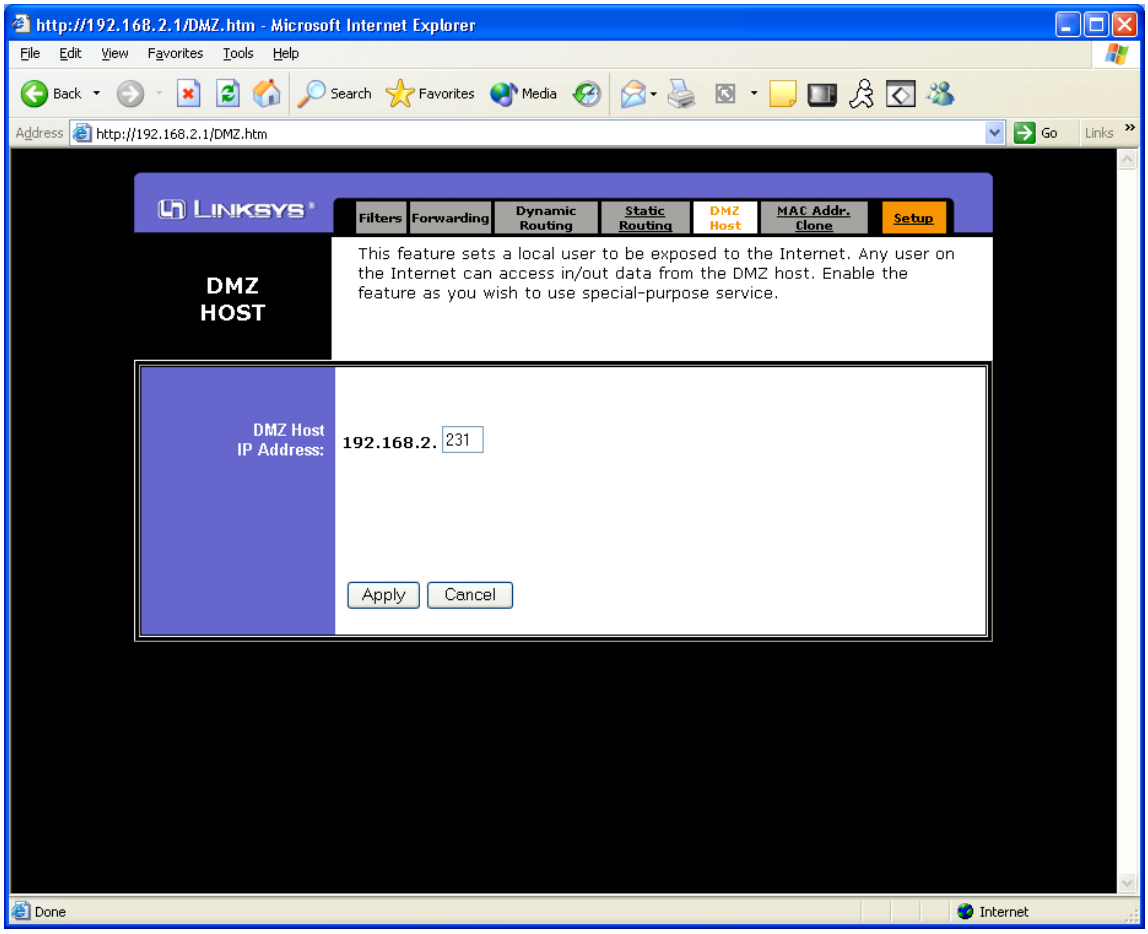
Router NAT



The Linksys router is set to **Gateway** in **Working Mode**.

Note On a Linksys BEFSR41 router, Gateway Mode is equivalent to dynamic NAT. Router mode would simply route packets without a network address translation happening.

Router Port Forwarding

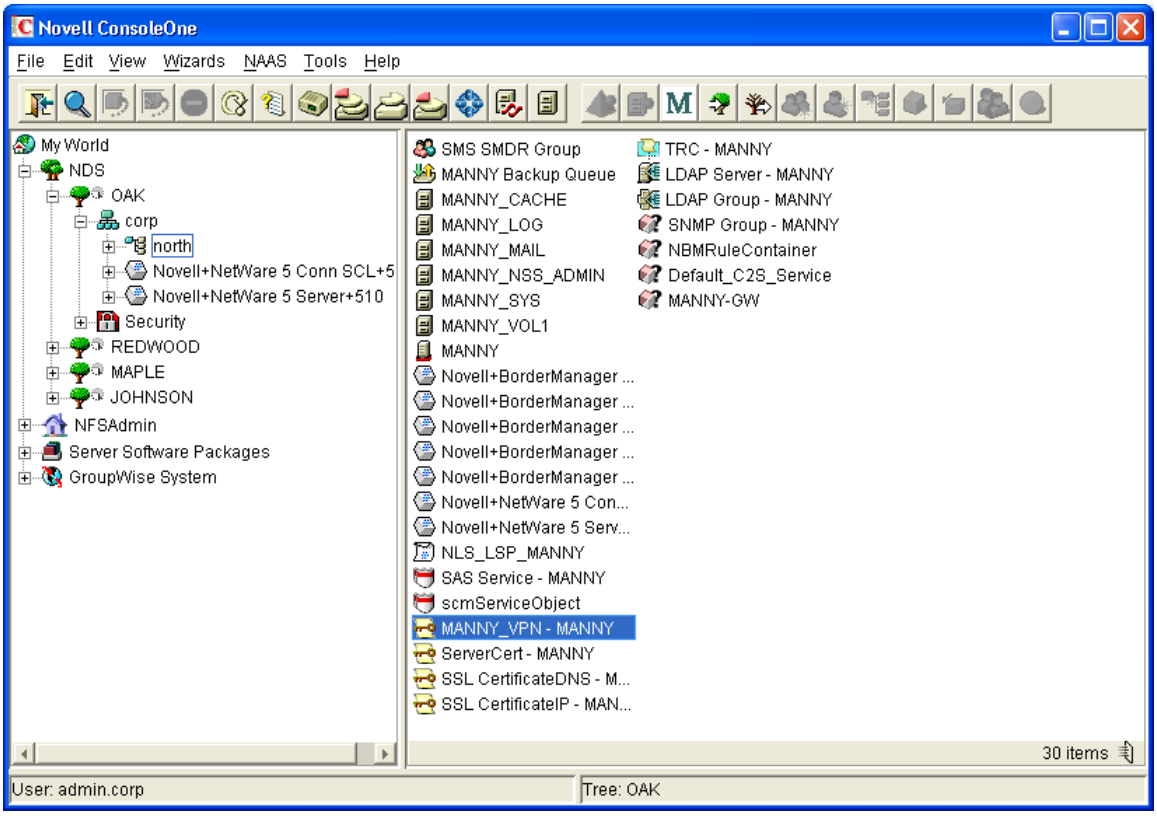


A **DMZ host IP Address** of **192.168.2.231** has been configured on the Linksys BEFSR41 router. **IP address 192.168.2.231 is the public IP address on server MANNY.**

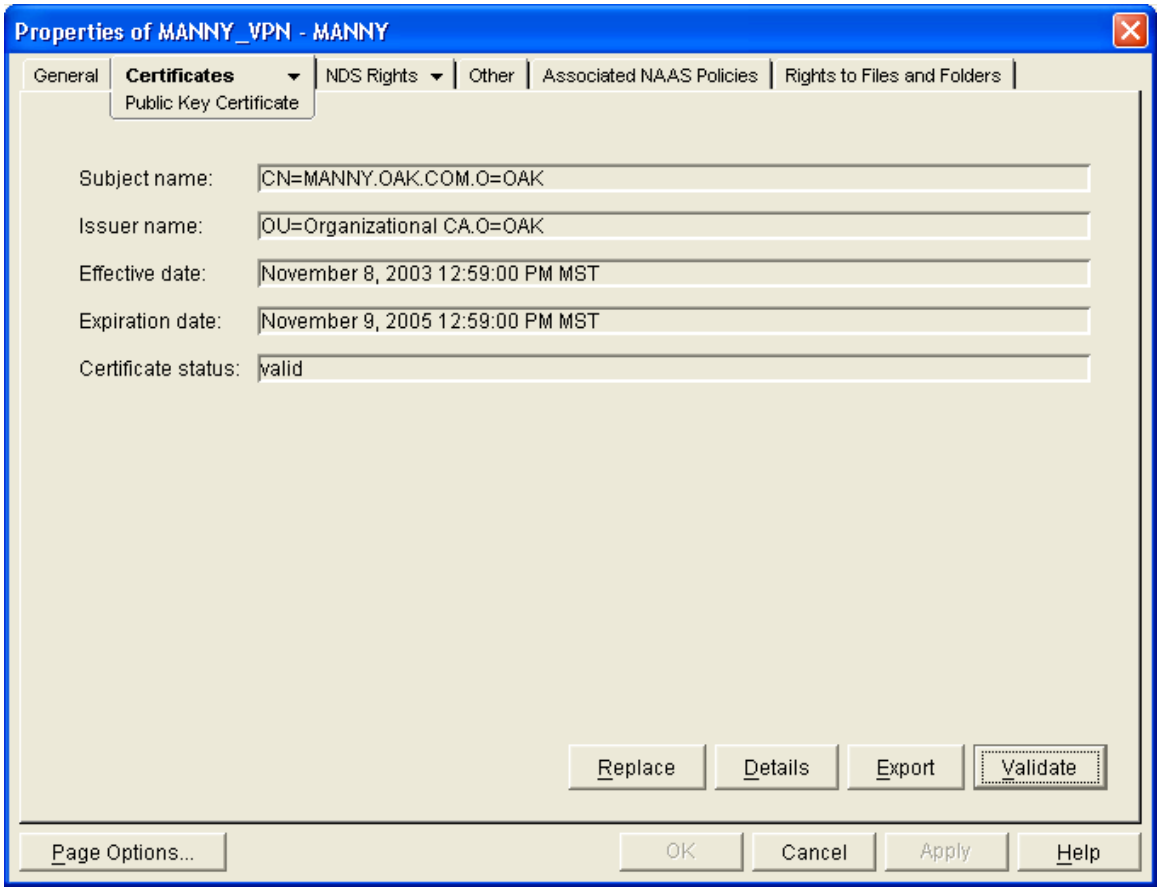
All traffic from the WAN port side of the router (Internet) addressed to the router's WAN port address will be forwarded to IP address 192.168.2.231 on the LAN port side.

Configuring a DMZ Host on this router is similar to configuring static NAT.

VPN Certificate Details

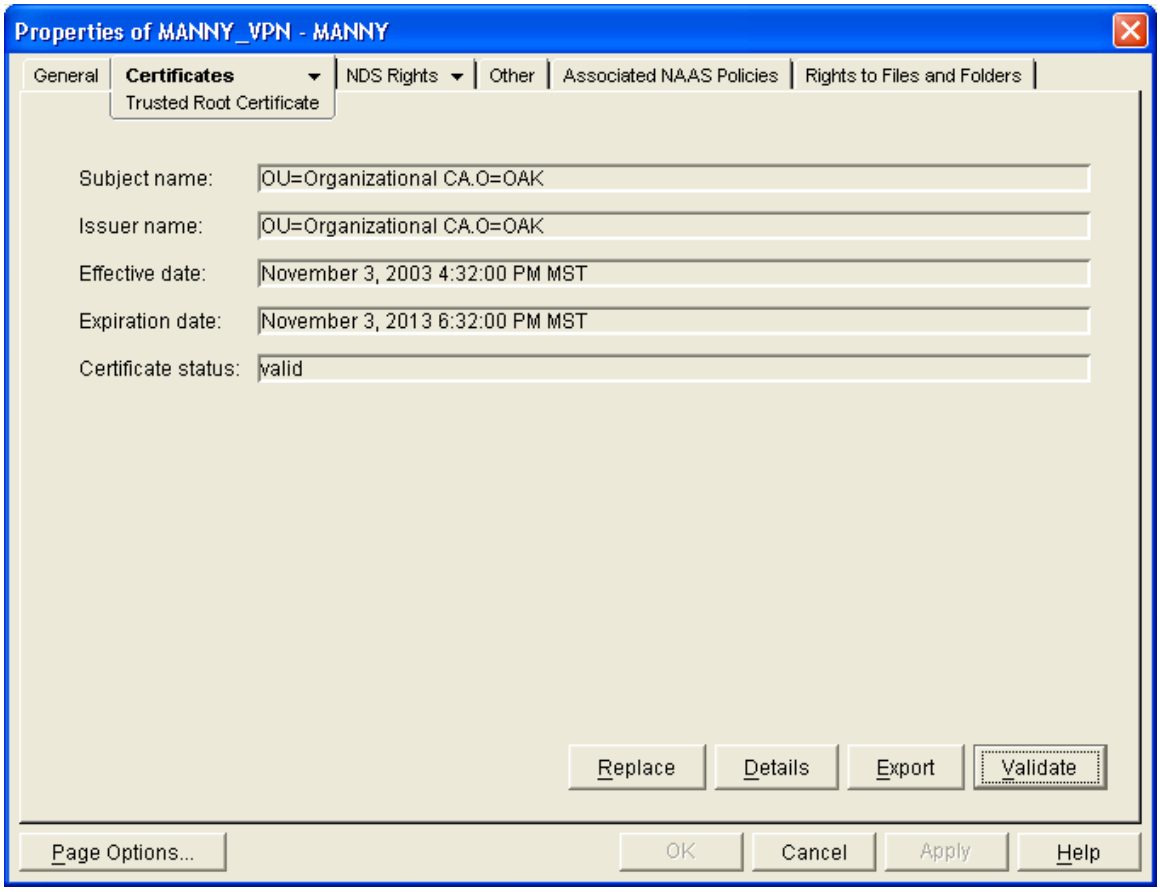


MANNY is using a custom VPN certificate called MANNY_VPN, configured in ConsoleOne, using settings shown in examples later in this chapter.



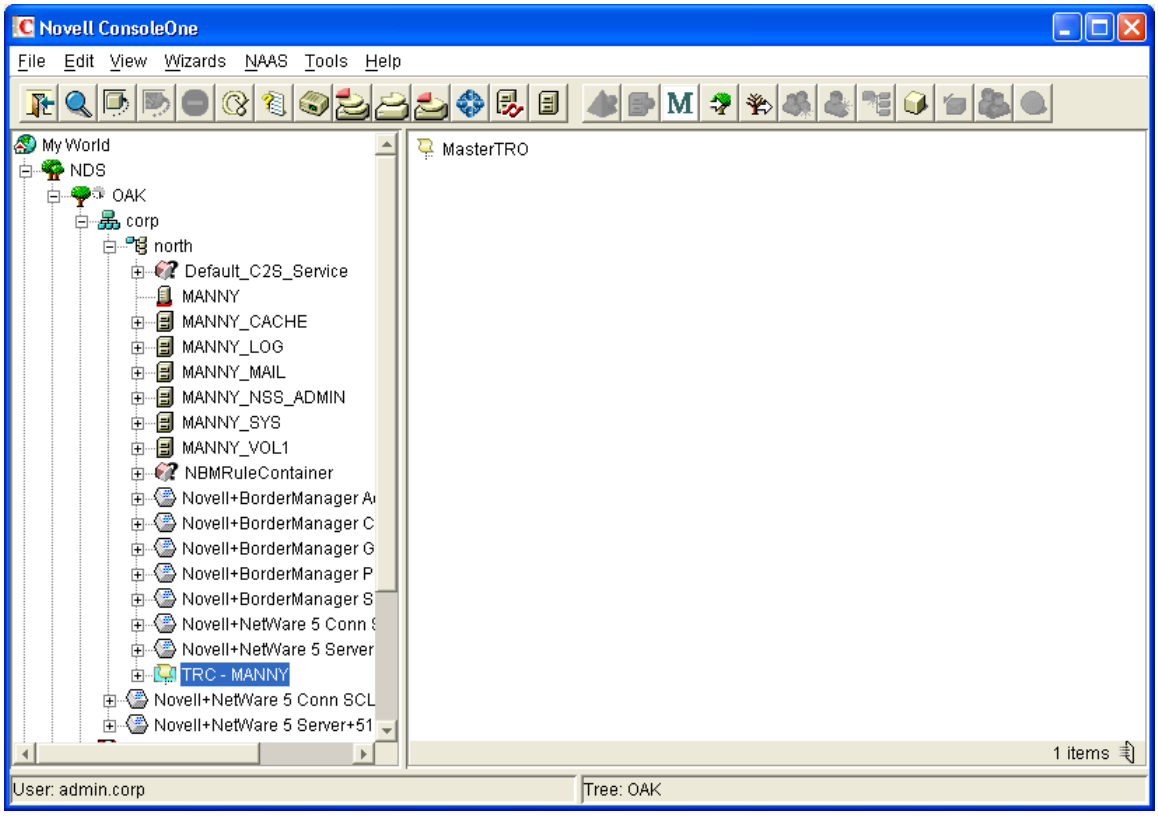
MANNY's VPN certificate has a **Public Key Certificate Subject Name** of **CN=MANNY.OAK.COM.O=OAK**.

This is the subject name that must be entered in the VPN configuration in the Site To Site Member List in iManager on the master VPN server.



The screenshot above shows the Trusted Root Certificate in the properties of MANNY_VPN certificate. This is the menu where the export of the certificate to a DER file was done.

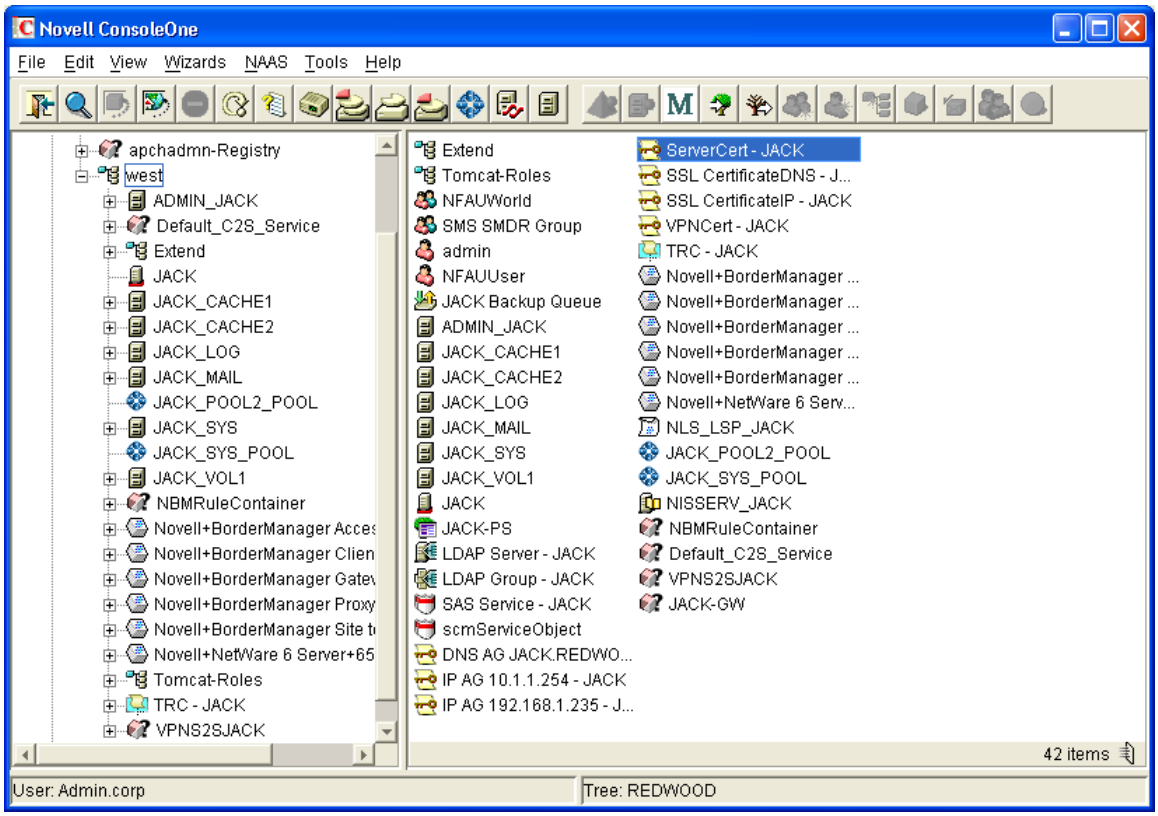
Trusted Root Object in Slave Server NDS Tree



The screenshot above shows the Trusted Root Object (TRO) created in server MANNY's Trusted Root Container in MANNY's NDS tree.

The TRO was created from a .DER file, which was exported from the master server's VPN certificate using ConsoleOne.

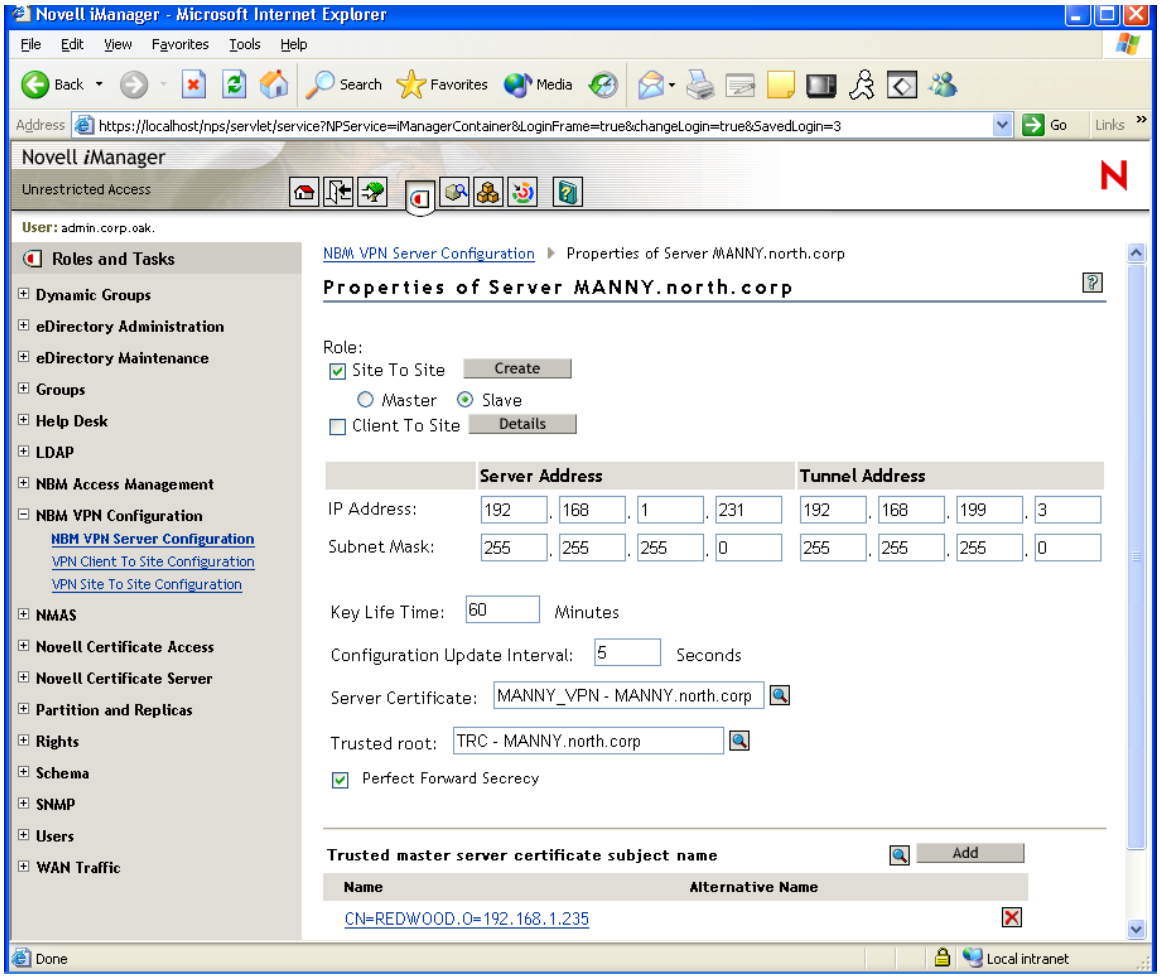
Trusted Root Object in Master Server NDS Tree



The screenshot above shows the Trusted Root Object (TRO) created in server JACK's Trusted Root Container in JACK's NDS tree.

The TRO was created from a .DER file, which was exported from the slaver server's VPN certificate using ConsoleOne.

Slave Server MANNY VPN Configuration



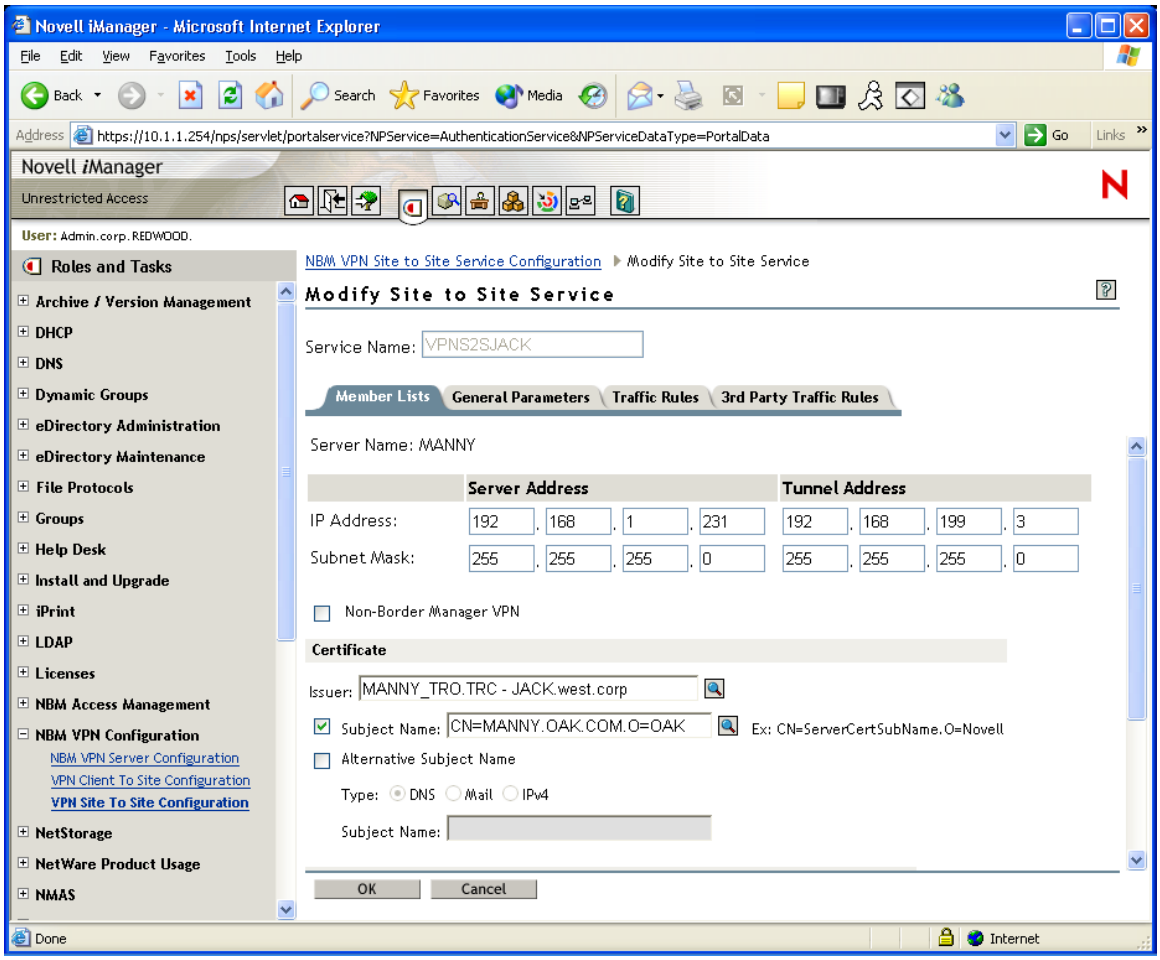
The VPN slave server MANNY's **Server Address** has been set to **the public address of the router**, not to MANNY's public binding. The Server Address is the address that other servers will use to connect to MANNY, and that should be the address that is being static NAT'd or port-forwarded.

MANNY has two network interfaces, PUBLIC and PRIVATE. The IP address of PRIVATE is 192.168.8.254. The IP address of PUBLIC is 192.168.2.231. The IP address 192.168.1.231 is on the Linksys router WAN port. (Refer to the network diagram at the beginning of this chapter for network addressing used in this example).

MANNY is using custom certificate **MANNY_VPN – MANNY** for VPN.

MANNY is configured as a slave server with the **Trusted master server certificate subject name** configured as **CN=REDWOOD.O=192.168.1.235**.

Configuration of Slave Server MANNY on Master VPN Server



When adding MANNY as a slave server on the master server, the following parameters are configured.

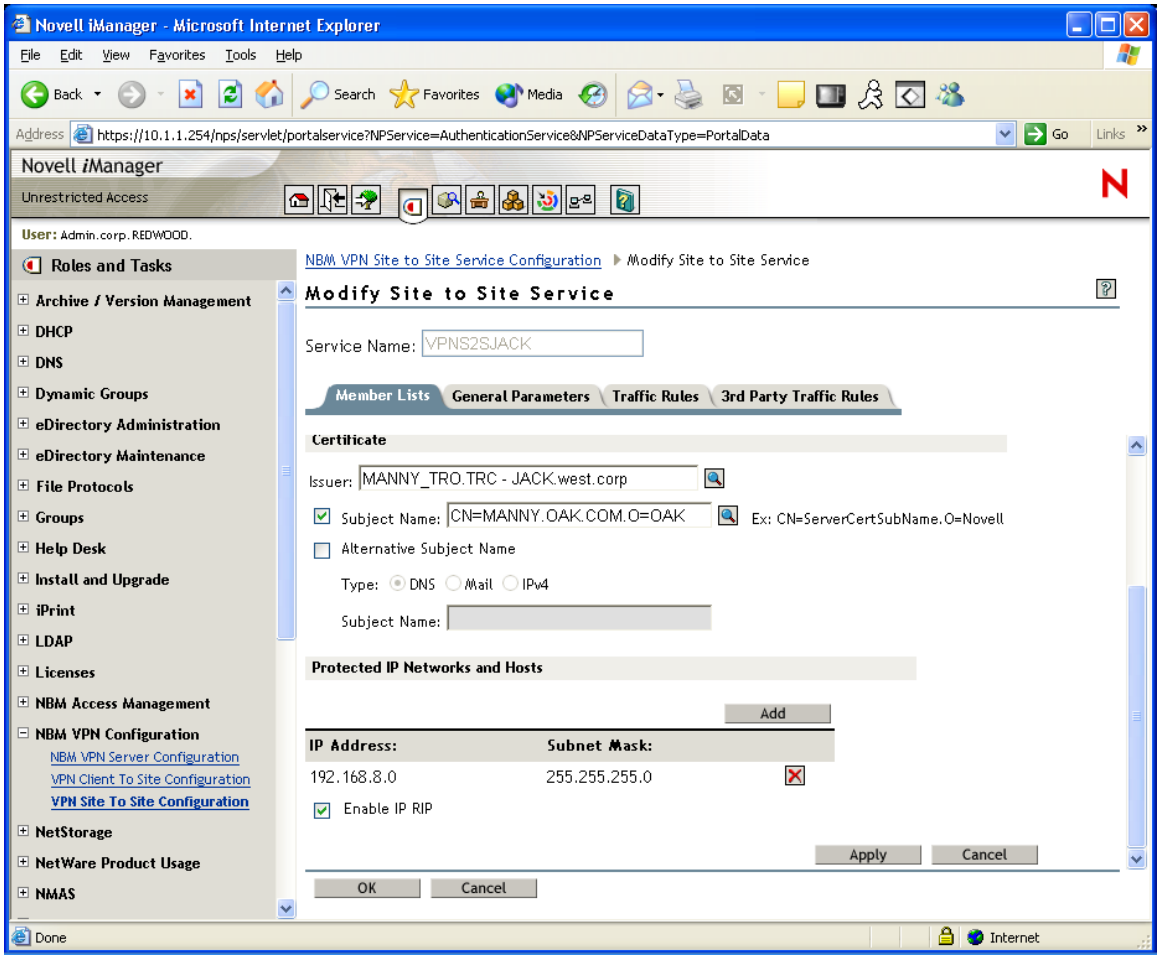
Server Name: **MANNY**

Server Address: **192.168.1.231** (this is the **router** WAN port address where port forwarding is being done, and would be the static NAT public IP address if static NAT was being used on a router).

Issuer: **MANNY_TRO.TRC – JACK.west.corp**. (This is the TRO for MANNY that was created in JACK's trusted root container from a DER file from MANNY's VPN certificate).

Subject Name: **CN=MANNY.OAK.COM.O=OAK** (This is MANNY's VPN certificate Public Key Certificate Subject Name, as shown earlier).

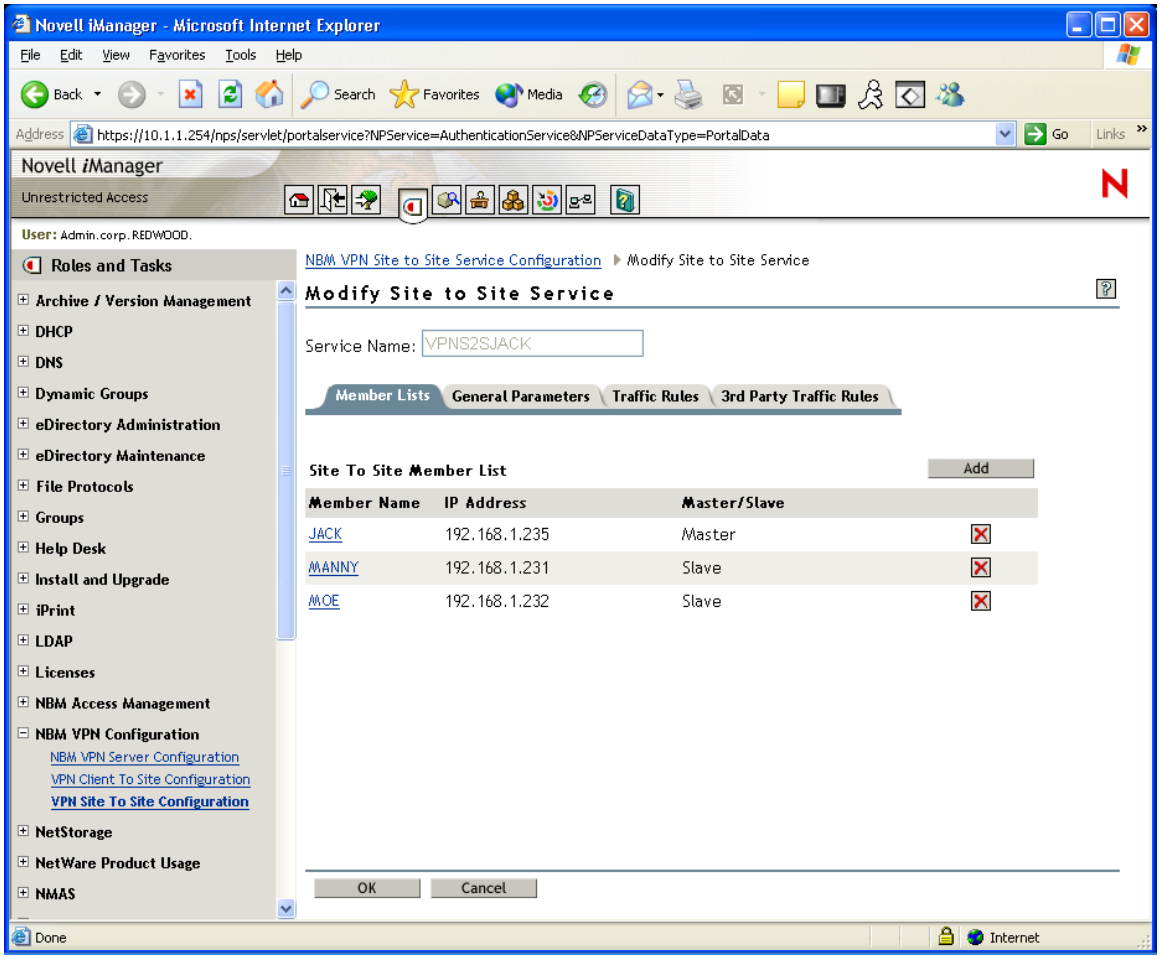
In order to see additional details, the browse must be scrolled down.



With the browser scrolled down, you can see the **Protected IP Networks and Hosts** menu entries.

The IP network **192.168.8.0**, subnet mask **255.255.255.0** is configured as a protected network for slave server MANNY.

Enable IP RIP is checked, so that the protected network address will be automatically pushed by the master VPN server to all other servers in the VPN.



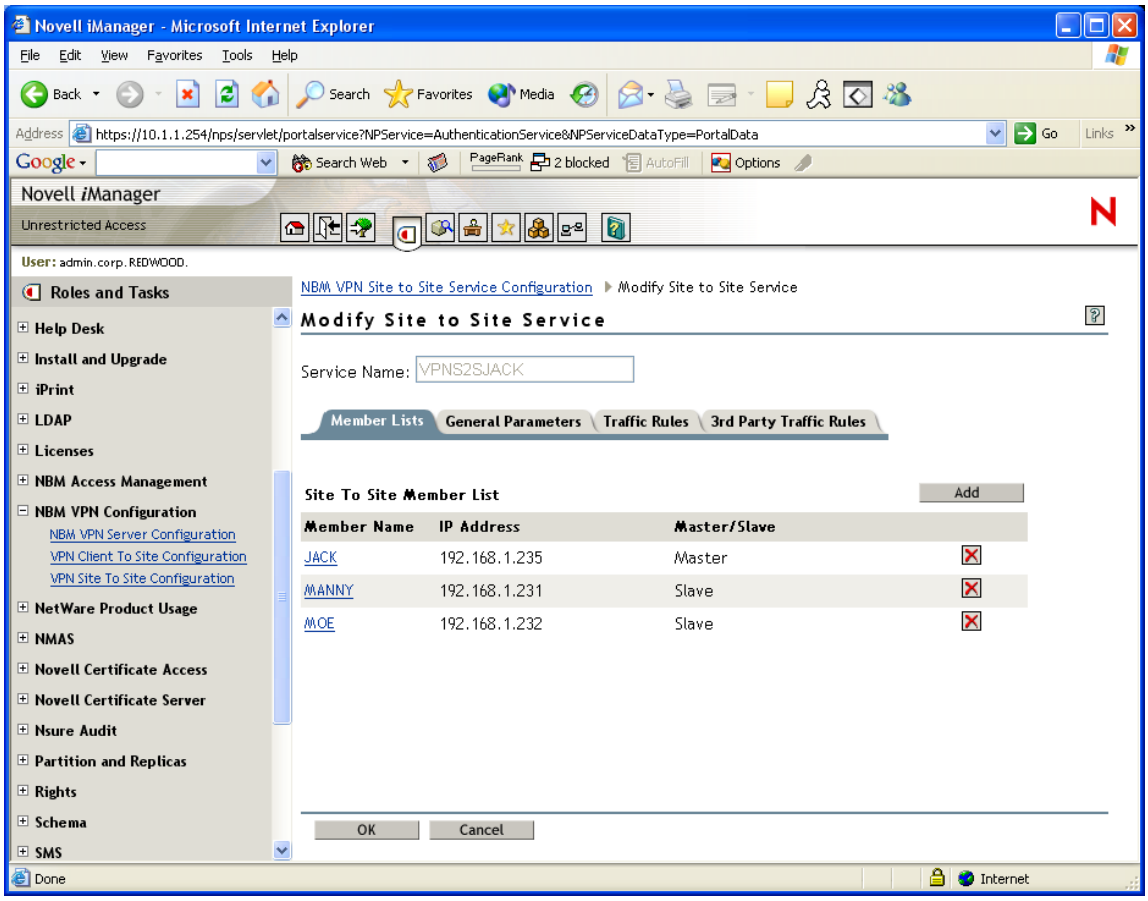
When configured, MANNY shows as an entry in the VPN **Site To Site Member List.**

Configure a Non-BorderManager Server as a Site-to-Site VPN Link

Add the Non-BorderManager VPN Server

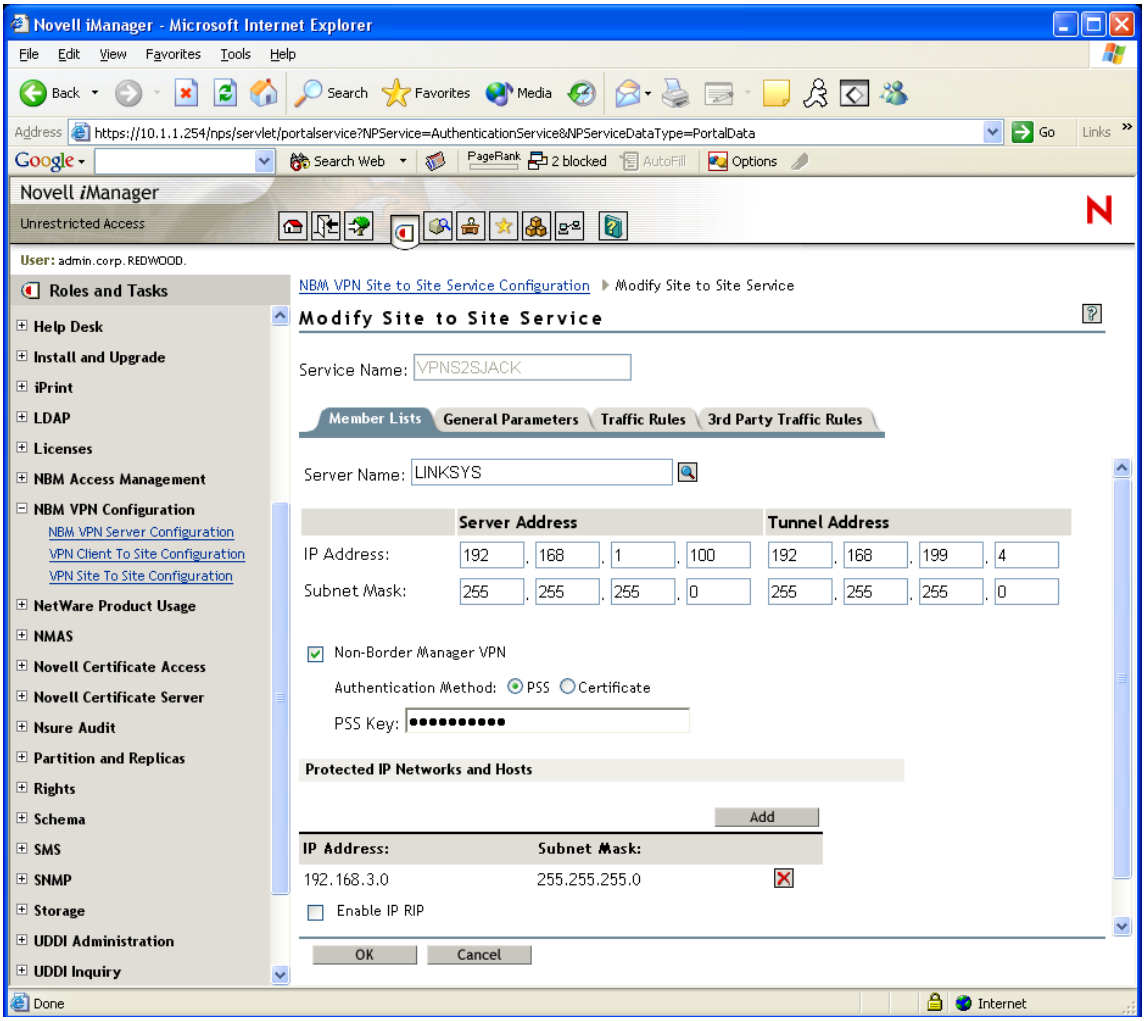
In this example, A Linksys BEFXS41 VPN router will become a VPN slave server, able to connect PC's behind it to JACK's private network. The Preshared Secret method will be used, since the VPN router has no way to store a certificate from the BorderManager server.

Due to limitations of the Linksys router, only one network can be configured for access behind the BorderManager server. The Linksys only has the option to enter a single IP network address, host or range of addresses. The Linksys can also only tunnel one network address connected to it on it's LAN side – again a limitation of the Linksys router, not BorderManager.



Connect to iManager and select the VPN Site-to-Site service already configured.

Click **Add** to add another VPN server.



Fill the **Server Name** – LINKSYS is used here.

Fill in the **Server IP address** of the public (WAN port) side of the Linksys router.

Configure a **Tunnel Address** for the Linksys router. On a non-BorderManager server, this address is not configured. It is only used for routing purposed on the BorderManager side. It needs to be in the same subnet as the other Site-to-Site VPN server addresses.

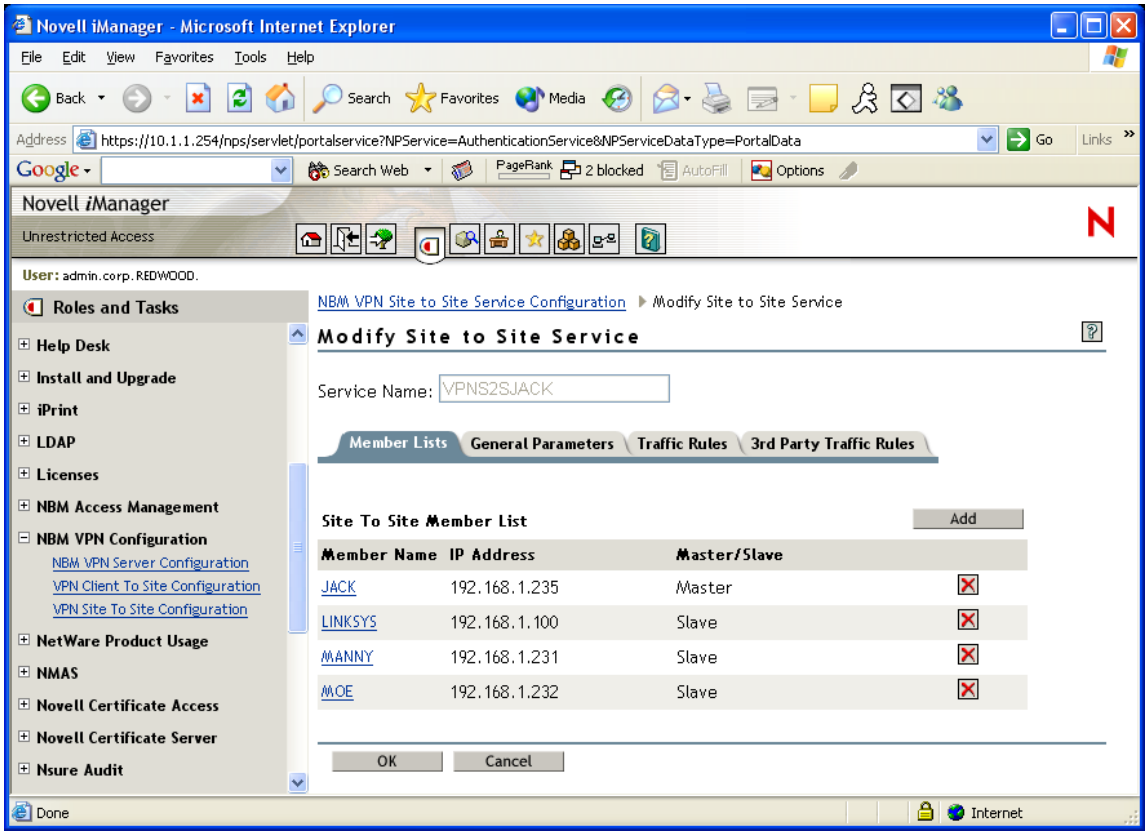
Check the box **Non-Border Manager VPN**. The menu entries below it will change.

Select **PSS** (PreShared Secret) as the Authentication Method. Type in the same **PSS Key** that was used on the Linksys. (Here it was 1234567890)

Click **Add** and configure the network connected behind the Linksys router.

Do not **Enable IP RIP**. That would push the subnet address to the other VPN servers, and they would be unable to connect directly to the Linksys router. The Linksys can only be connected to one of the VPN servers at a time.

Click **Apply** to save the configuration.



You now have a non-BorderManager server (Linksys) as part of the Site-to-Site VPN.

Since we have a non-BorderManager server, we can make use of 3rd Party Traffic Rules.

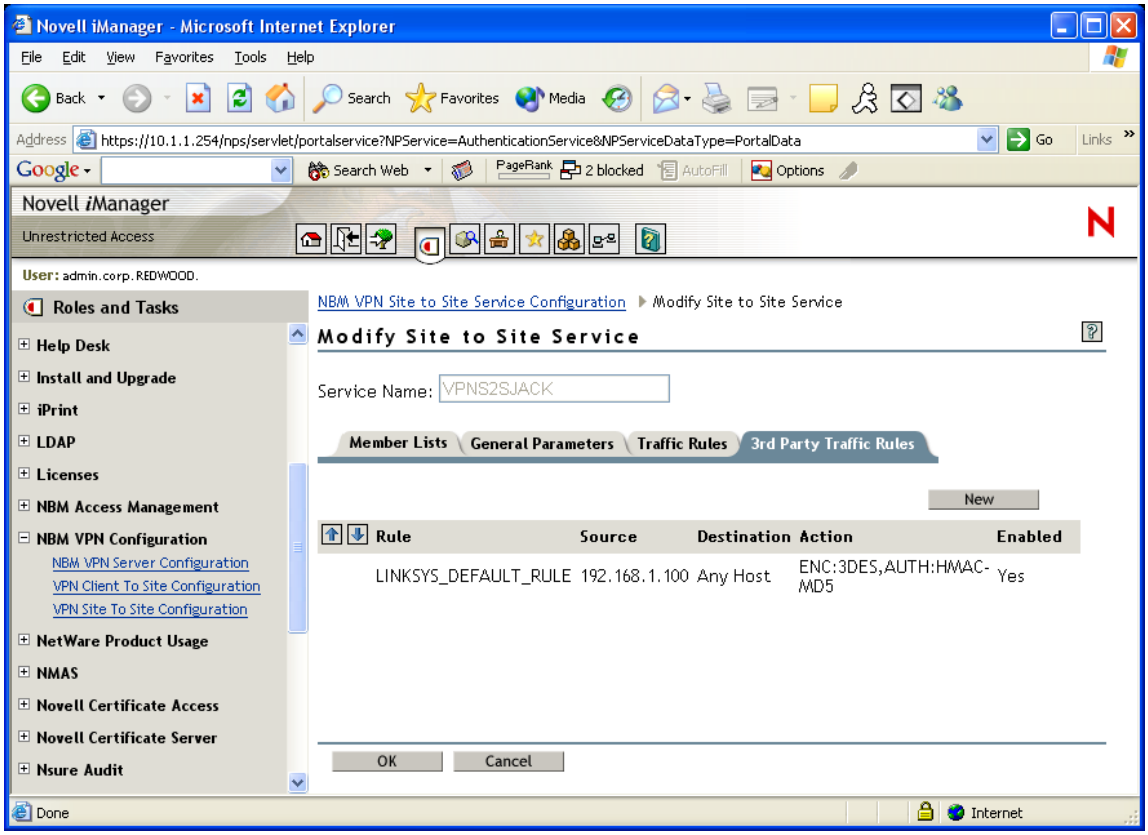
Select the 3rd Party Traffic Rules tab.

Configuring 3rd Party Traffic Rules

Note The BorderManager 3.8 default 3rd-party traffic rule changed from Encrypt All to Deny All traffic at a certain patch level. (This is desirable). An unpatched BorderManager 3.8 server may require you to add your own Deny All traffic rule below your desired allow all rule, depending on the traffic you wish to allow. The example in this section shows screenshots of both default rules.

3rd Party Traffic rules affect traffic flowing from the remote VPN server to your BorderManager VPN server. The 3rd Party VPN Server Configuration menu defines what addresses behind the 3rd party VPN server are allowed to send data to the BorderManager server. The 3rd party VPN server generally will have a way to control traffic in the other direction. The NBM Protected Server Network List defines which hosts behind your BorderManager server are accessible from the remote VPN site.

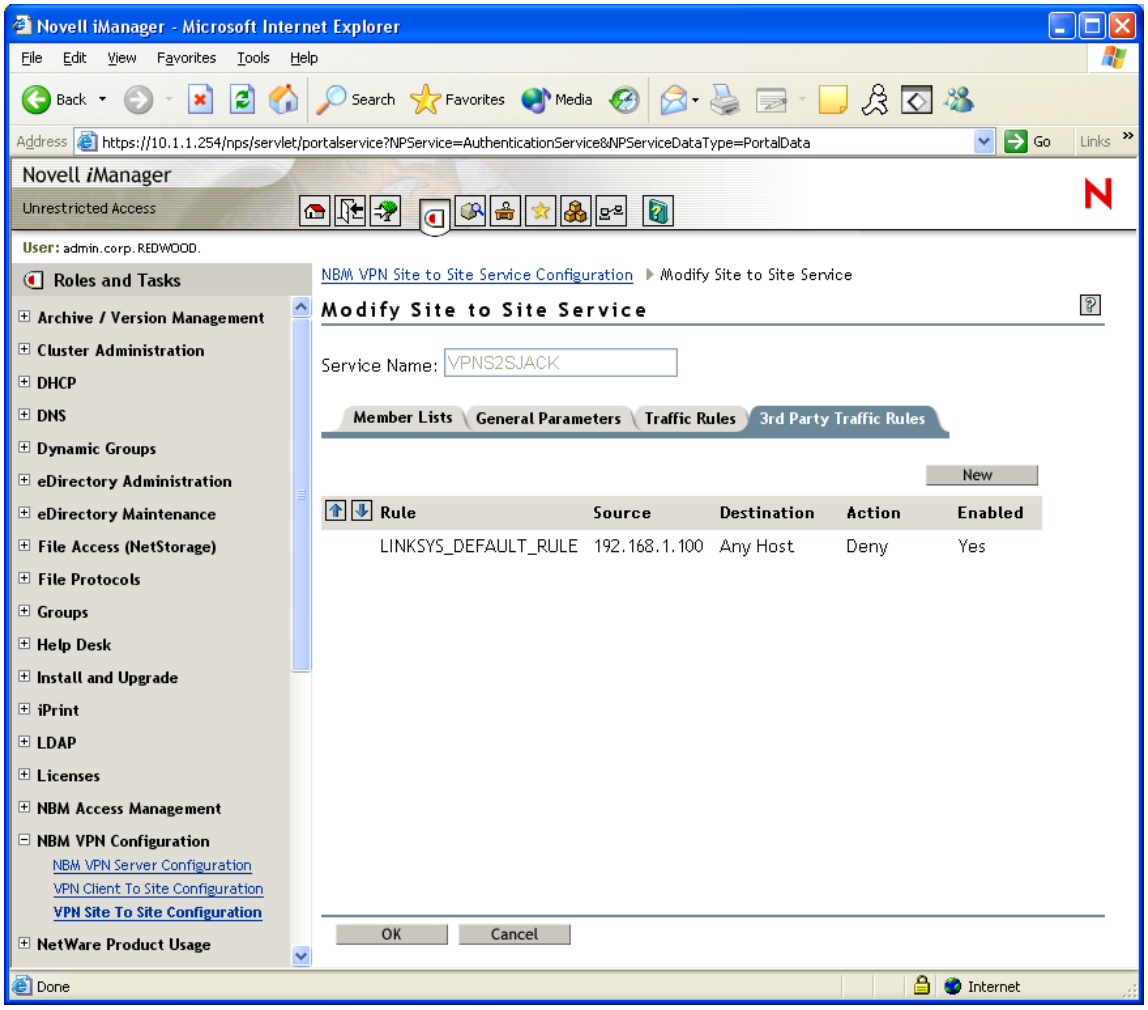
Default Allow Rule



In the **3rd Party Traffic Rules** menu, we MIGHT see that there is a default rule for the Linksys router already configured. In the example above, the default rule, taken from a BM38SP1 server, shows the default as encrypting any host. This default changed at BM38SP2. This rule encrypts the traffic from the public address of the Linksys router. This rule may be present depending on the patch level of your BorderManager 3.8 server. This rule can present a problem as it has the effect of sending different information to the remote VPN server than you want, if you wish to allow only a specific restricted subnet.

Should you see a default rule similar to the above (encrypting any destination), you should override it with your own custom rules, one which allows the traffic you want, and another which denies everything else. One reason for this is that a BorderManager patch might change the action of the default rule from encrypting all to denying all.

Default Deny Rule

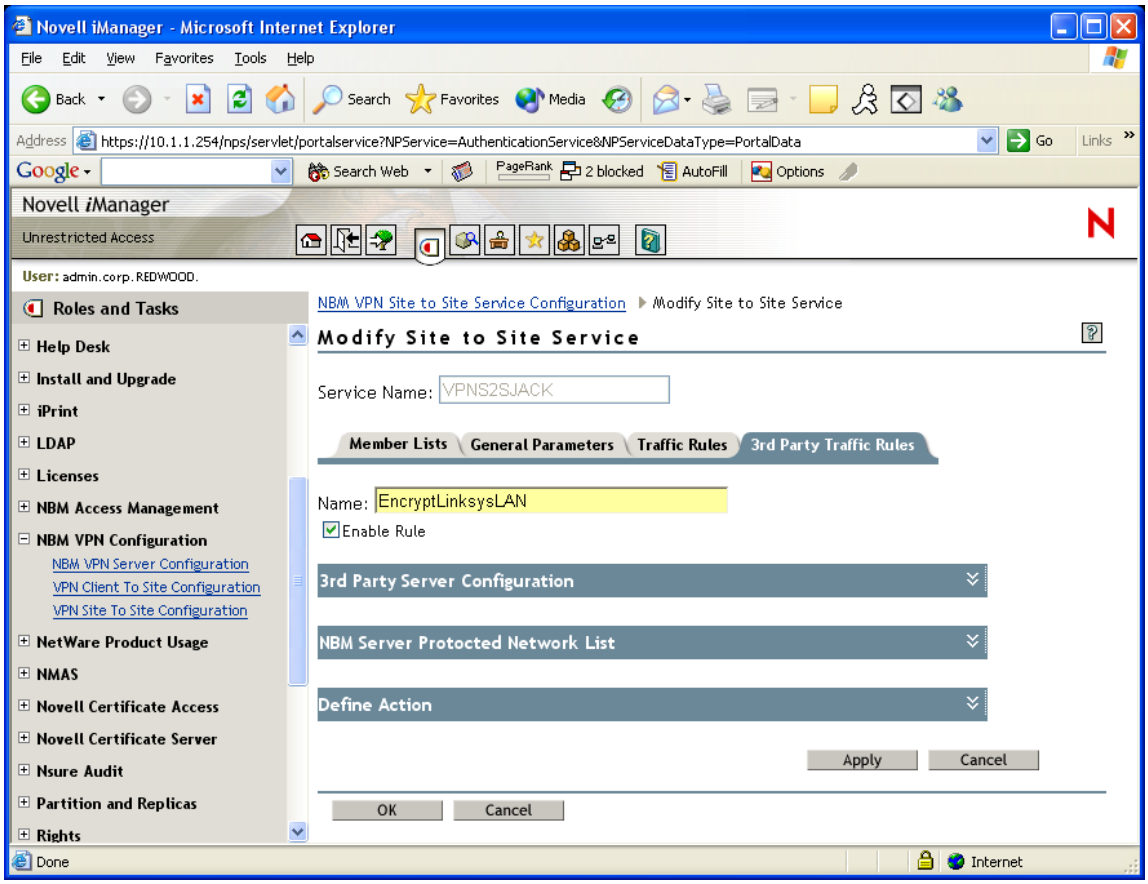


Compare the screenshot above to the previous screenshot. In this example, taken from a BorderManager 3.8 service pack 2 (beta) server, the default rule is changed to deny traffic.

Encrypt Selected Traffic Rule

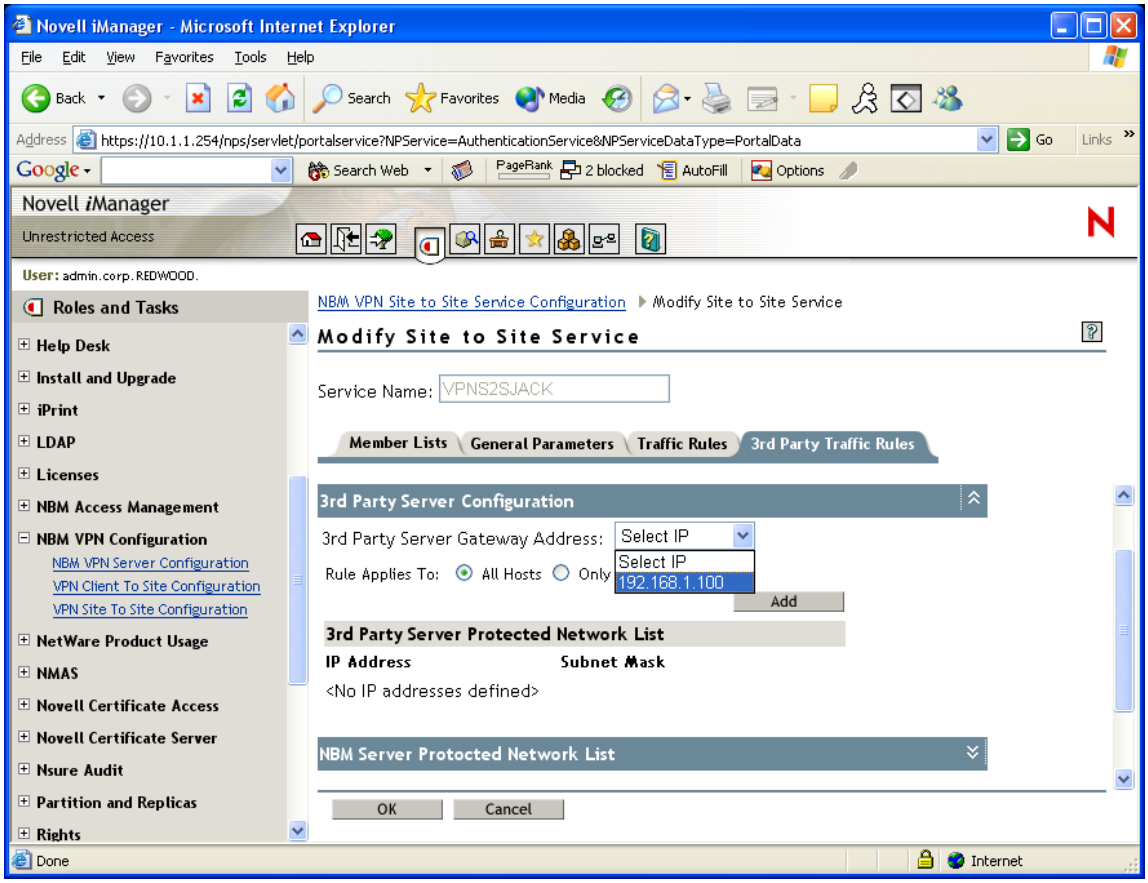
We wish to add a traffic rule to allow only certain traffic between the VPN endpoints.

Click **New** to add a new traffic rule.



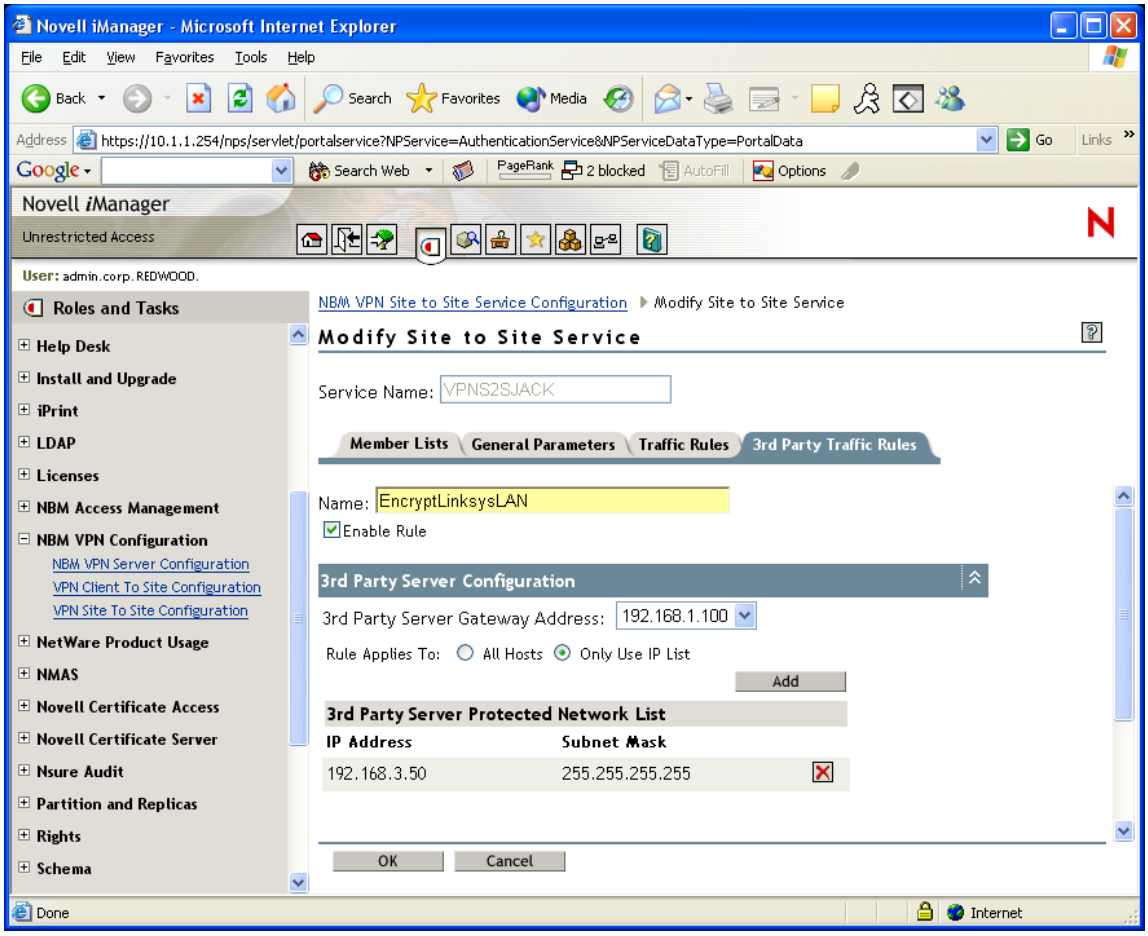
Give the new rule a name **EncryptLinksysLAN**.

Expand the 3rd Party Server Configuration section.



From the drop-down list for **3rd Party Gateway Address**, select the **public IP address** of the Linksys router.

If you want to allow/deny any particular IP addresses behind the Linksys, you can add the desired IP addresses next. As an example, we will limit VPN traffic to the single IP address 192.168.3.50.



Choose **Only Use IP List**.

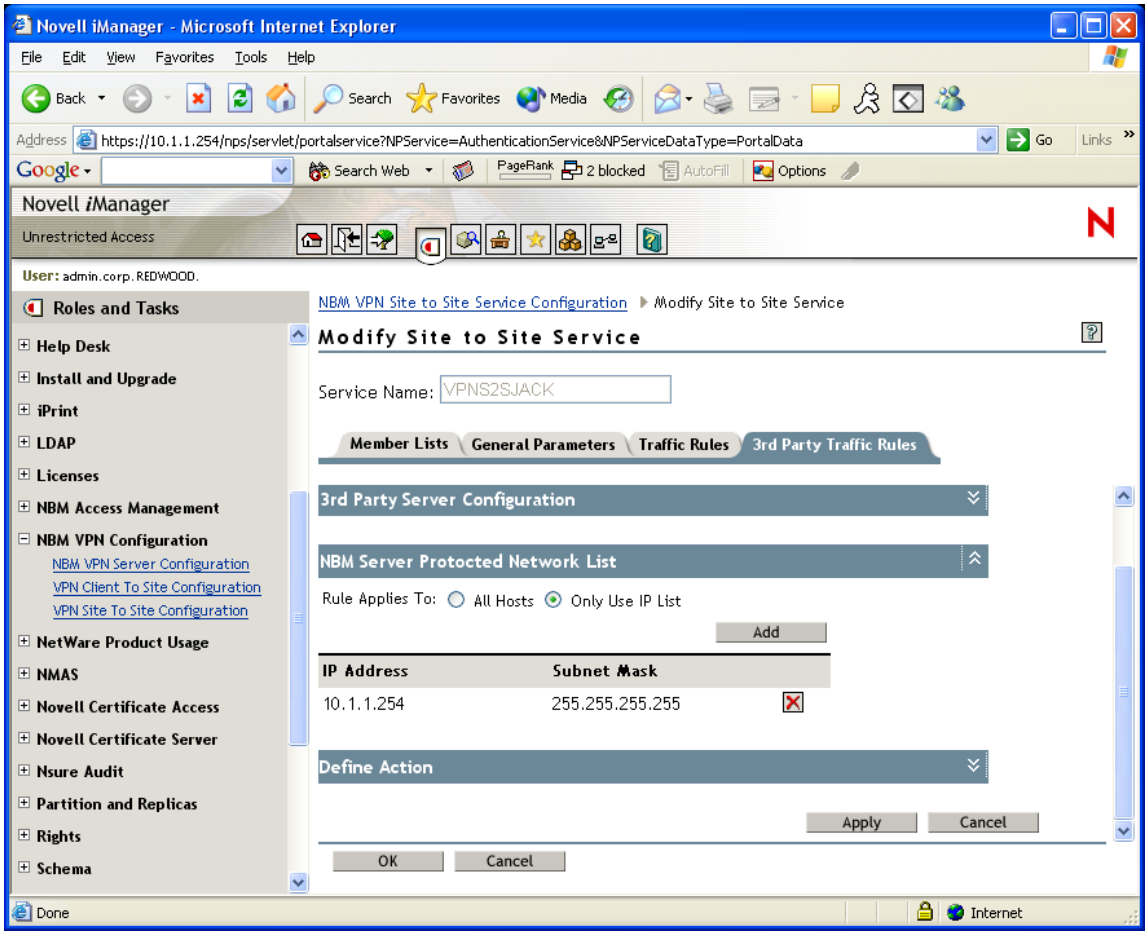
Click **Add**.

Add the single IP address **192.168.3.50** and click **OK**.

Expand the **NBM Server Protected** [sic] **Network List**

Choose **Only Use IP List**.

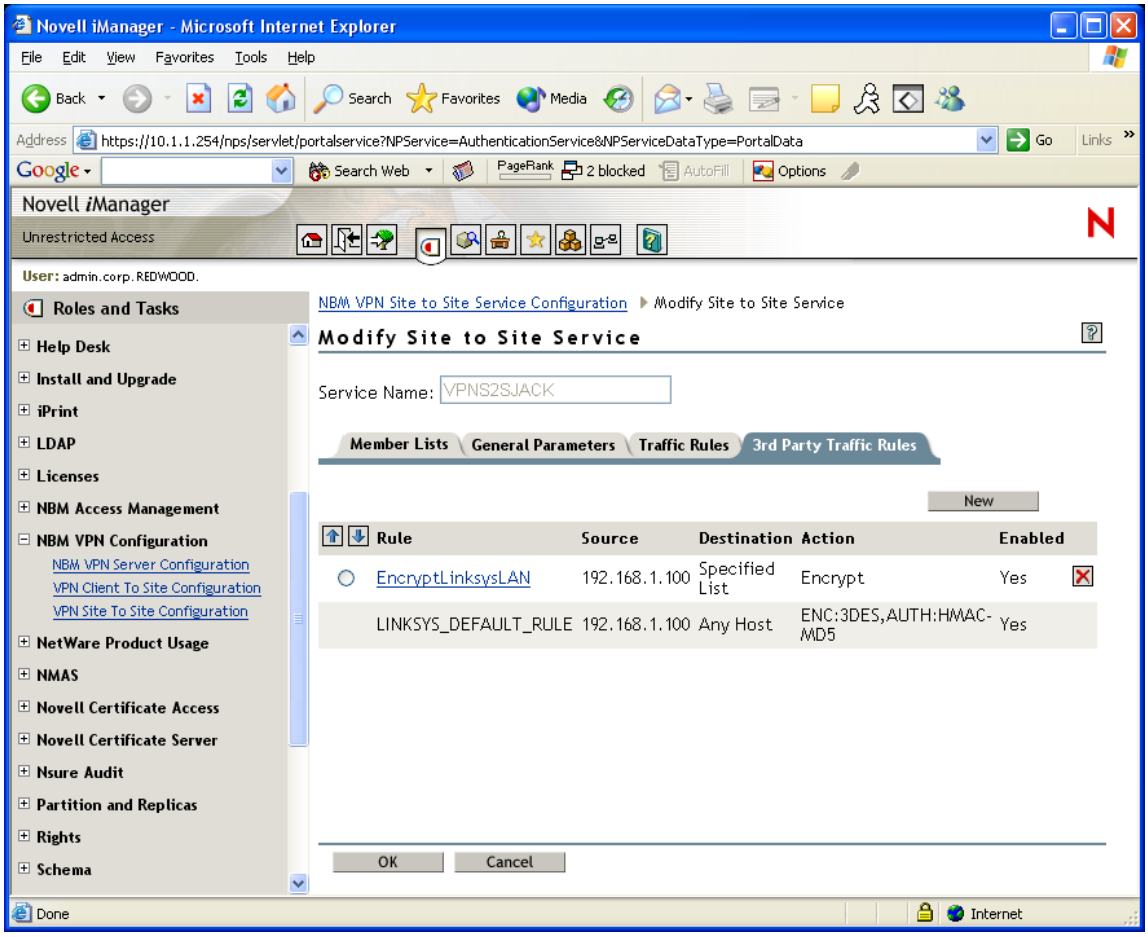
Click **Add**.



As an example, we will only allow one IP address behind the BorderManager network to be accessed across this Site-to-Site VPN link. Configure the host IP address **10.1.1.254**, and click **OK**.

The Define Action default setting is to encrypt all IP traffic, and that is fine for this example.

Click **Apply**.

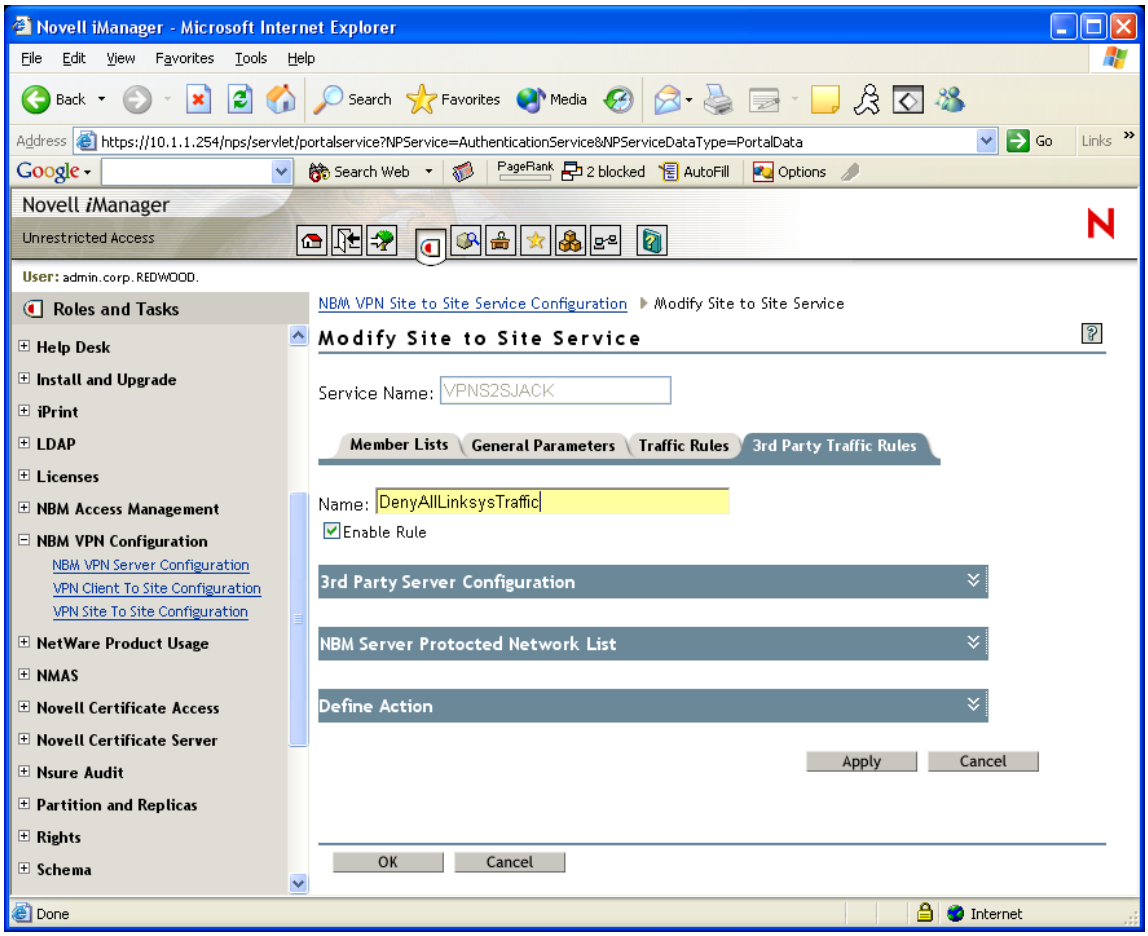


Now we see a traffic rule for the Linksys Router. If we leave this setting, we will still have more traffic allowed, since the default rule shown for the particular server (depends on patch level) encrypts all hosts behind the Linksys router public IP address.

Deny All Other Traffic Rule

Depending on the default traffic rule in your server, you may need to add a Deny rule above the default Encrypt Any rule. As of this writing, a 3rd-party (non-Novell) VPN server may not work if you leave the default rule in place, because the configuration of protected networks on each side of the VPN may not match. At this point you want to deny all other traffic.

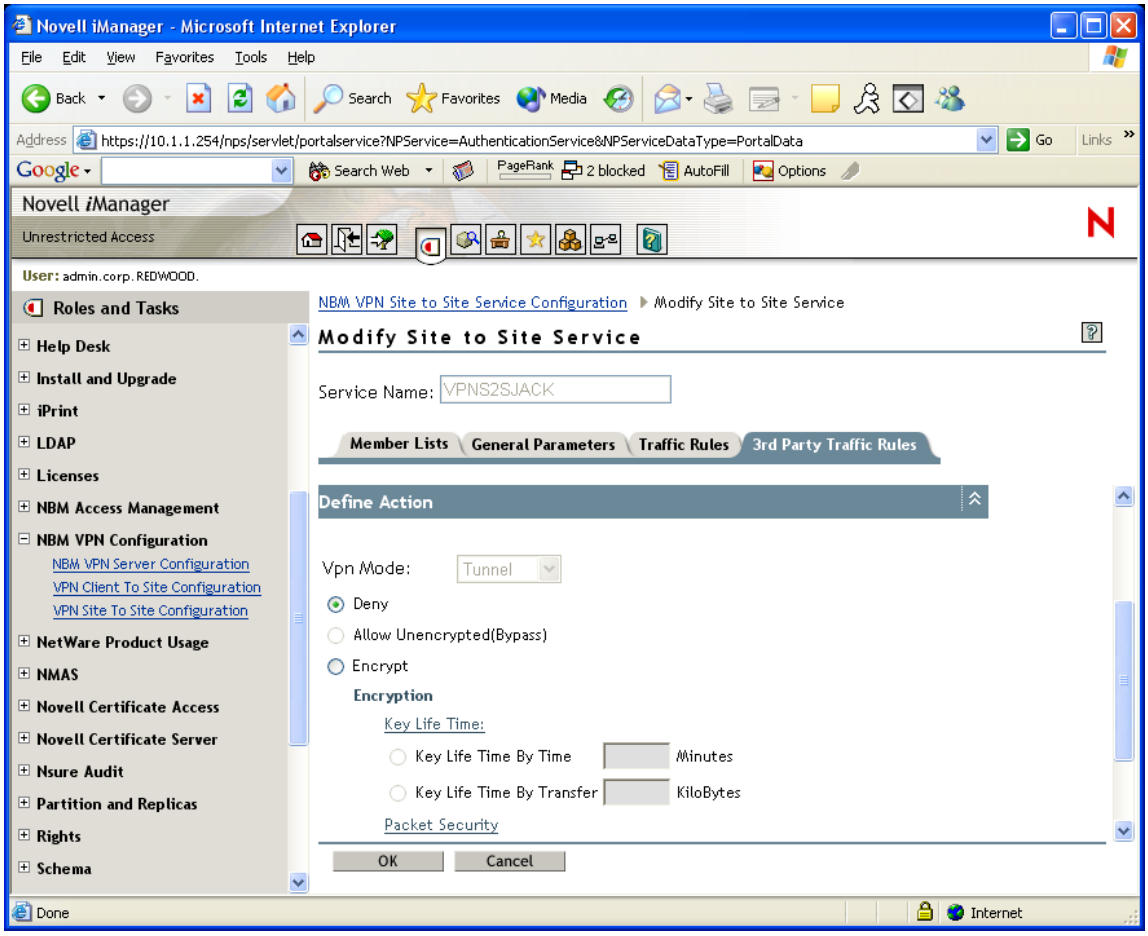
If you have a default traffic rule that denies all traffic, you will not need this rule.



Click **New**, and name a new rule **DenyAllLinksysTraffic**.

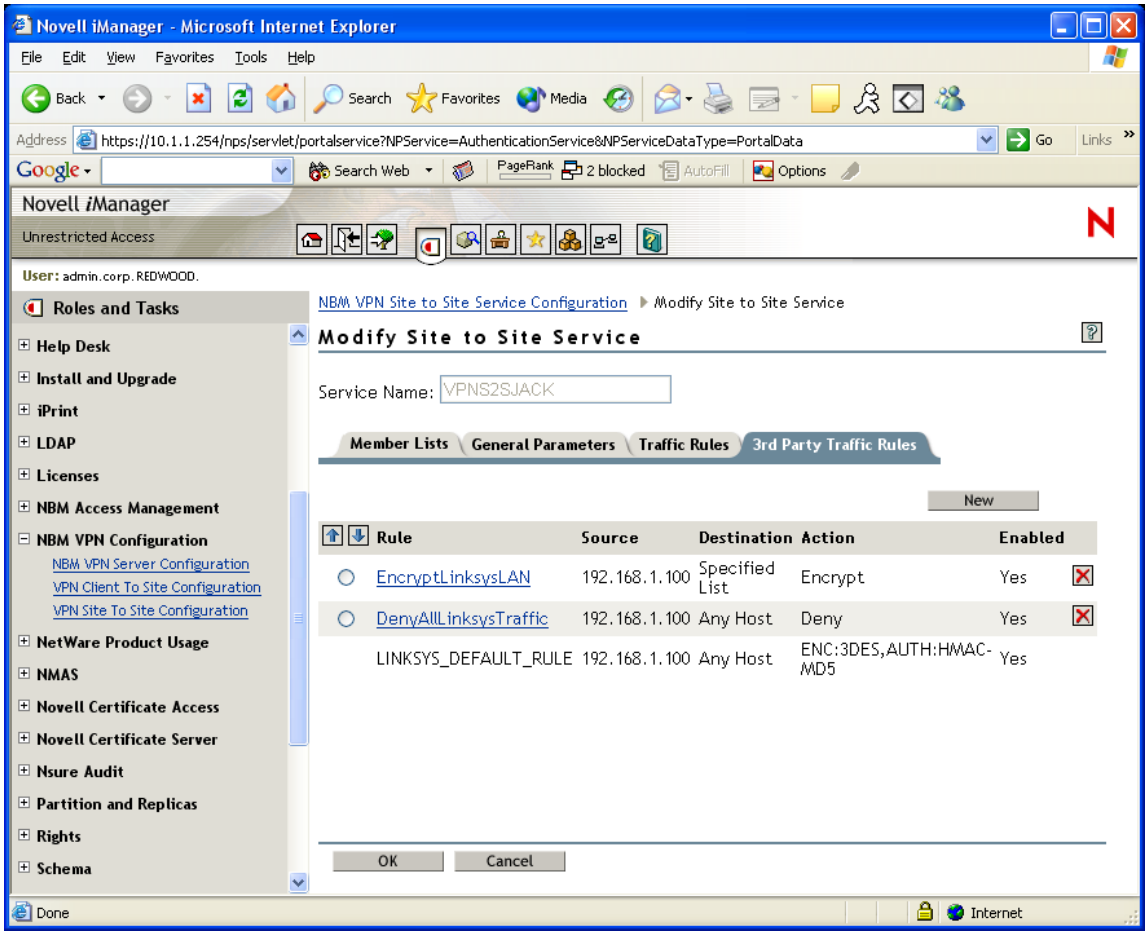
Under **3rd Party Server Configuration**, select the **IP address of the WAN port of the Linksys router**. Leave the rest of the settings in that menu section and in the NBM Server Protected Network List at the default values.

Expand the **Define Action** section.



Select **Deny**.

Scroll down and click **Apply**.



Now we have rules that should allow traffic through the Linksys Site-to-Site VPN router link only for 10.1.1.254 to and from 192.168.3.0. The screenshot shown above was taken from a BorderManager 3.8 server which was at a patch level that did not deny 3rd-party traffic by the default rule.

Click **OK** to save the settings.

Check the IKE screen for activity involving the Linksys WAN port IP address.

Check the Linksys configuration menu – you may have to manually tell the router to Connect.

Configure a Linksys Router as a VPN Server

A Linksys router, model BEFSX41, has limited VPN capabilities. It can only establish a VPN connection in Shared Secret mode, can only protect a single network (connected to its LAN ports), and can only tunnel to a single network (connected to the BorderManager server's private side). These limitations are within the router, not the BorderManager server.

Linksys Settings

Local Secure Group: The IP address or network that will be accessible through the VPN on the LAN port side of the Linksys router. In this example, it is configured for a single IP address of 192.168.3.100. A PC at this address will be able to use the VPN, but other addresses behind the Linksys will not.

Remote Secure Group: The IP address of network that will be accessible through the VPN on the private side of the BorderManager server. In this example, it is configured for the IP network of the master BorderManager server's private side, 10.1.1.0 (255.255.255.0).

Remote Secure Gateway: The public IP address of the BorderManager server.

Encryption: The encryption type to be used. In this example it is set to 3DES

Authentication: The authentication type to be used. In this example it is set to MD5.

Key Management: The kind of key management method to be used. In this example it is set to IKE.

PFS (Perfect Forward Secrecy): A method for improving security. In this example, PFS is enabled.

Pre-Shared Key: The alphanumeric string used to both authenticate and encrypt data between the VPN end-points. This value must match the value configured in the BorderManager Site-to-Site VPN Member List entry for the Linksys router. In this example, it is set to 1234567890.

Key Lifetime: The length of time a key is used before new keys are exchanged. In this example it is set to 3600 seconds.

Linksys Advanced Settings

The Linksys route has some additional settings that can control the phase 1 and phase 2 VPN session parameters in more detail. The values

Phase 1 Operation Mode: **Main Mode**

Proposal 1:

Encryption: DES

Authentication: SHA

Group: 768-bit

Key Lifetime: 3600 Seconds

Phase 2

Proposal

Encryption: 3DES

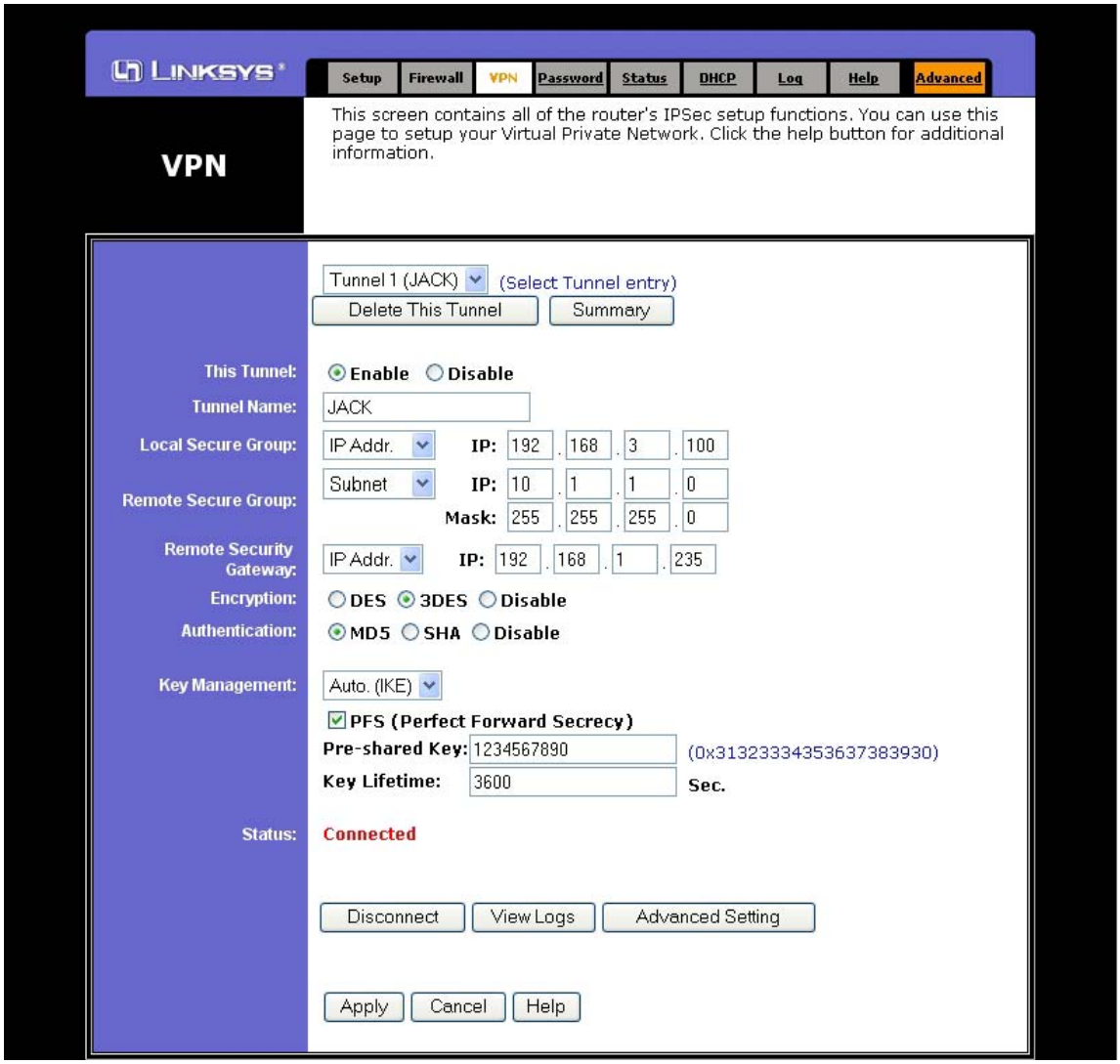
Authentication: MD5

Group: 1024-bit

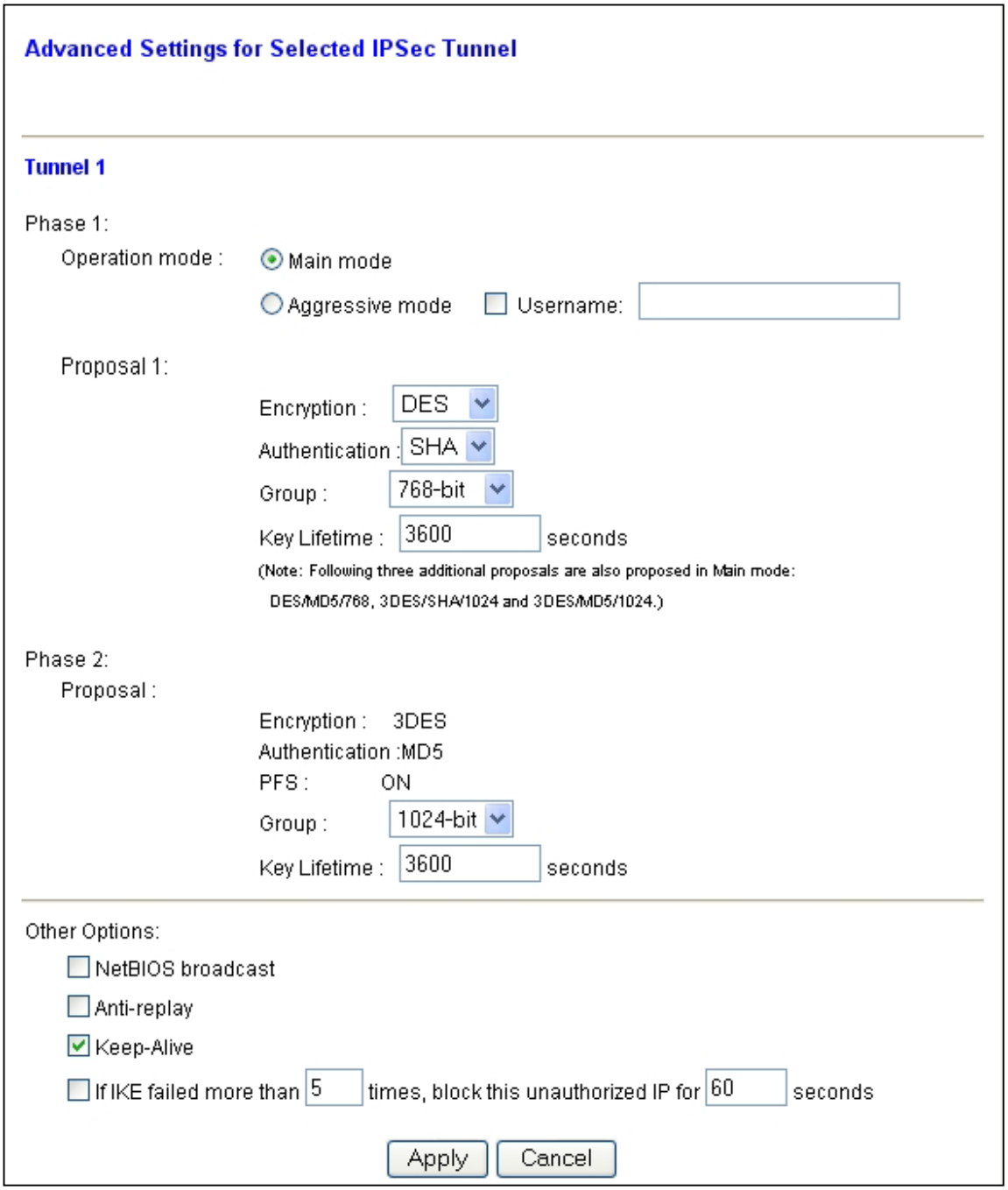
Key Lifetime: 3600 Seconds

Other Options

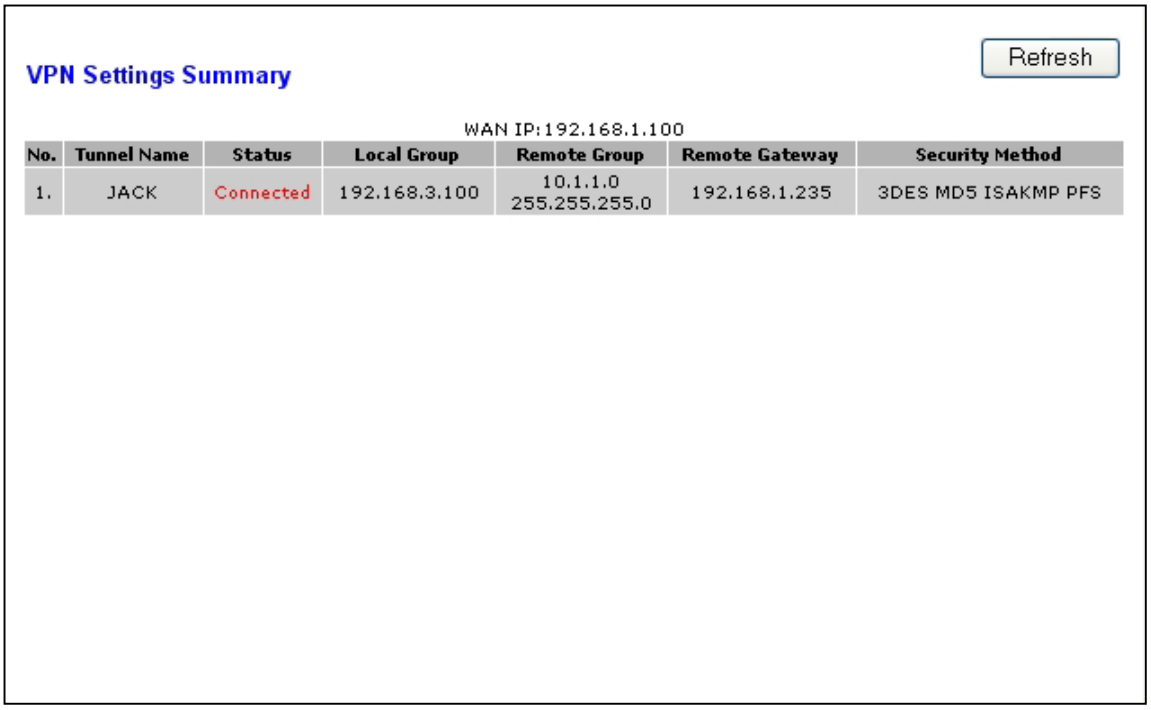
Keep Alive: Enabled



The screenshot above shows the Linksys Router VPN configuration menu, after the VPN connection has been established. If the Linksys router has been rebooted and brought up before the BorderManager server, you may have to manually start the VPN connection. If the router is not already connected to the VPN, the Disconnect button shown above will be a Connect button instead.



The screenshot above shows the Linksys router configuration accessed by the Advanced button.



The screenshot above shows the VPN Settings Summary as accessed from the Summary button on the Linksys VPN menu.

Creating VPN Objects with ConsoleOne and iManager

The remainder of the chapter shows how to manually create VPN objects such as Trusted Root Objects, Trusted Root Containers, and VPN certificates. Both ConsoleOne and iManager methods are shown.

Manually Creating A Trusted Root Object (TRO), Using ConsoleOne

This section shows the procedure for manually creating a Trusted Root Object (TRO) for a server using ConsoleOne.

All operations will be done in JACK's NDS tree.

Two procedures are shown:

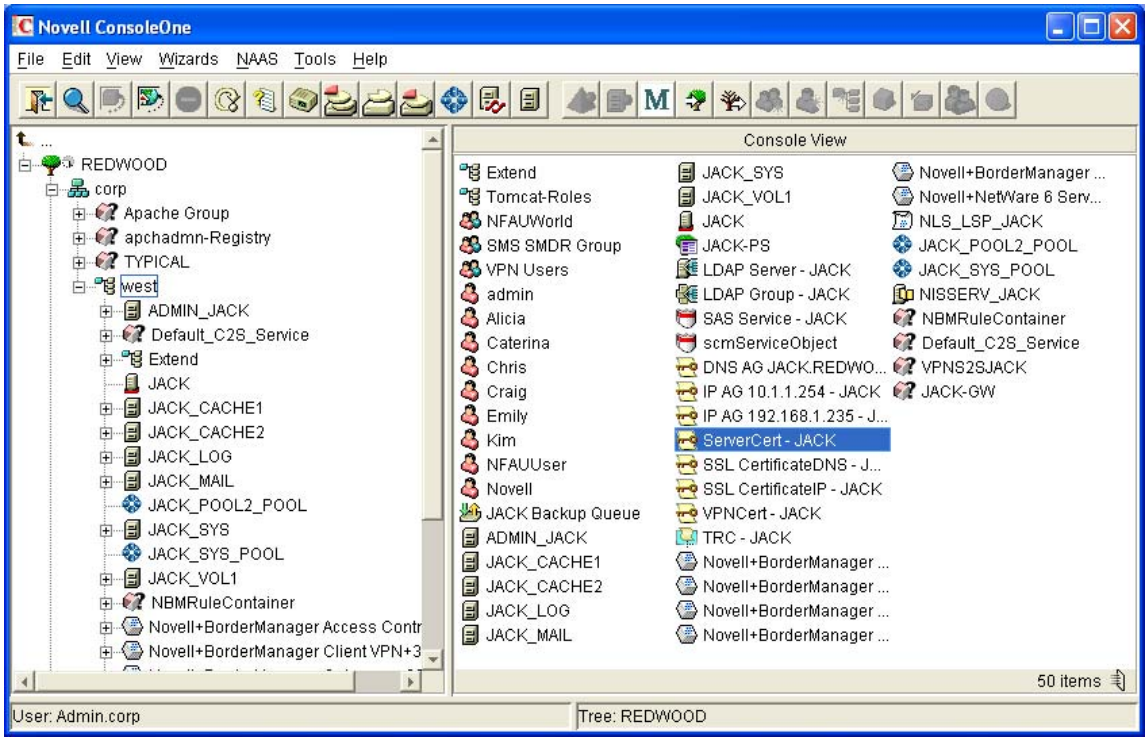
- Exporting JACK's VPN server certificate to a .DER file. This file will be used by MOE to create a TRO for JACK.
- Importing MOE's exported server certificate file into JACK's trusted root container (TRC) to create a TRO for MOE.

The same procedures can be done using iManager, and those procedures are shown later in this book. You have the choice of using iManager or ConsoleOne, and this book is simply showing a procedure for either method.

The TRO shown is for the server MOE, and is necessary in order to add MOE as a slave server. The manual creation procedure is necessary because MOE is in a different NDS tree than JACK.

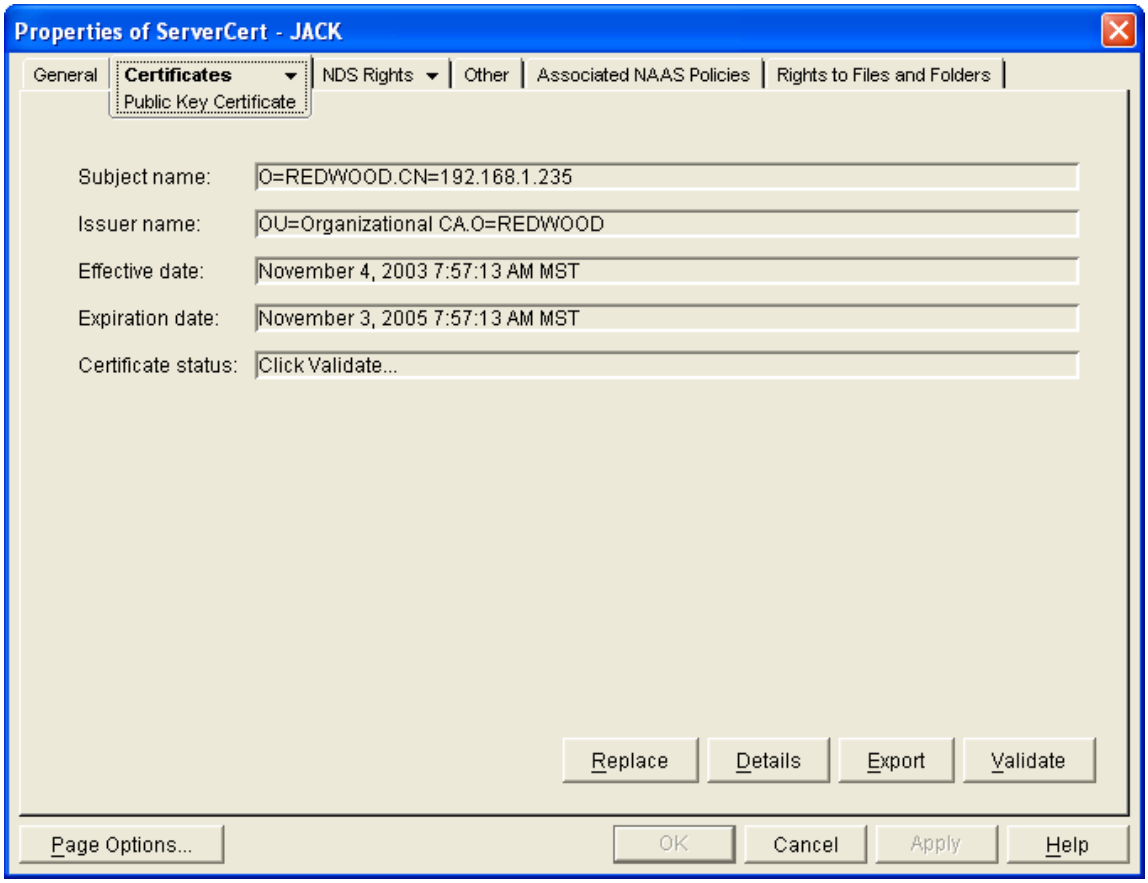
Exporting JACK's VPN Certificate to a .DER File using ConsoleOne

The first step in manually creating a Trusted Root Object for a server is to export the trusted root certificate to a .DER file. The trusted root certificate is contained within the server certificate.



Using ConsoleOne, browse to the container holding the server, and select the server certificate to be used for the Site-to-Site VPN.

Double-click on the VPN certificate, here **ServerCert – JACK**.

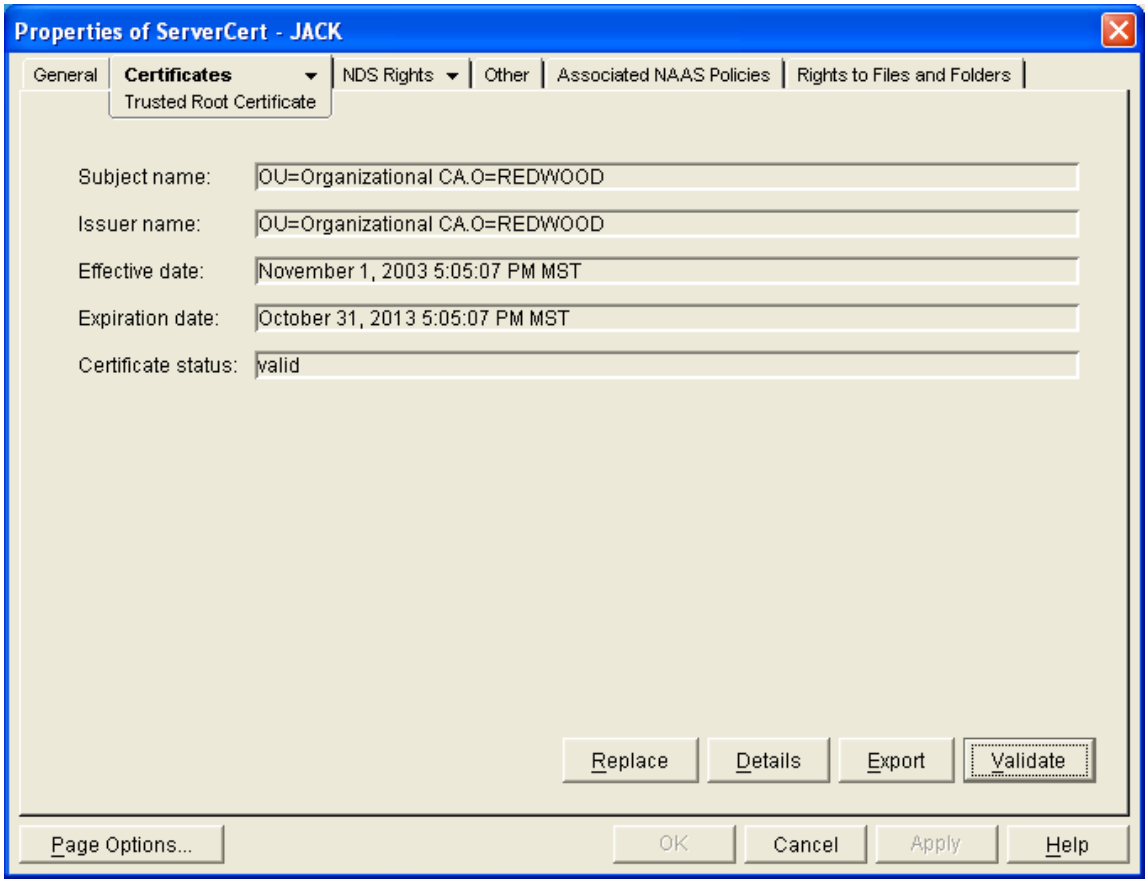


First, select the **Public Key Certificate** from the **Certificates** drop-down menu.

Make a note of the **Public Key Subject Name** as you will need it later when you create a Trusted Root Object from the exported certificate trusted root certificate. You might want to have a screenshot of this menu handy.

The Subject Name here is **O=REDWOOD.CN=192.168.1.235**.

Now select the Trusted Root Certificate tab from the **Certificates** drop-down menu.

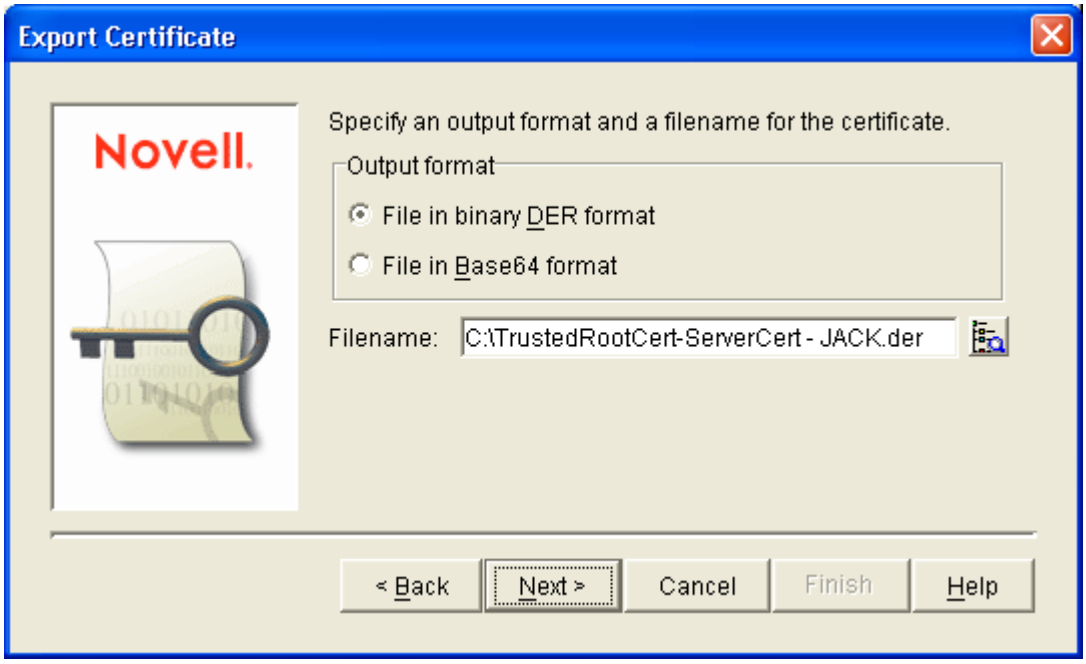


You should be looking at the **Trusted Root Certificate**, from the **Certificates** drop-down menu.

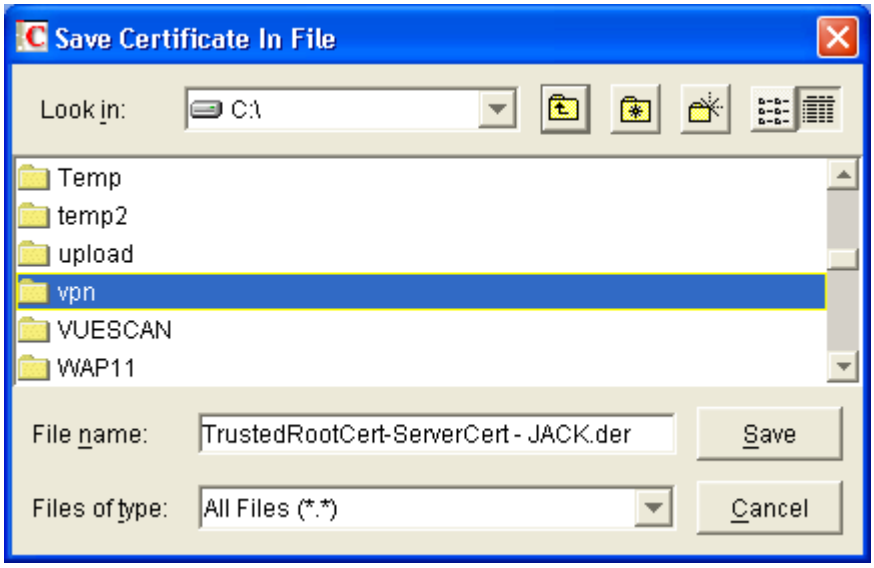
Click on **Export**.

Do not export the private key.

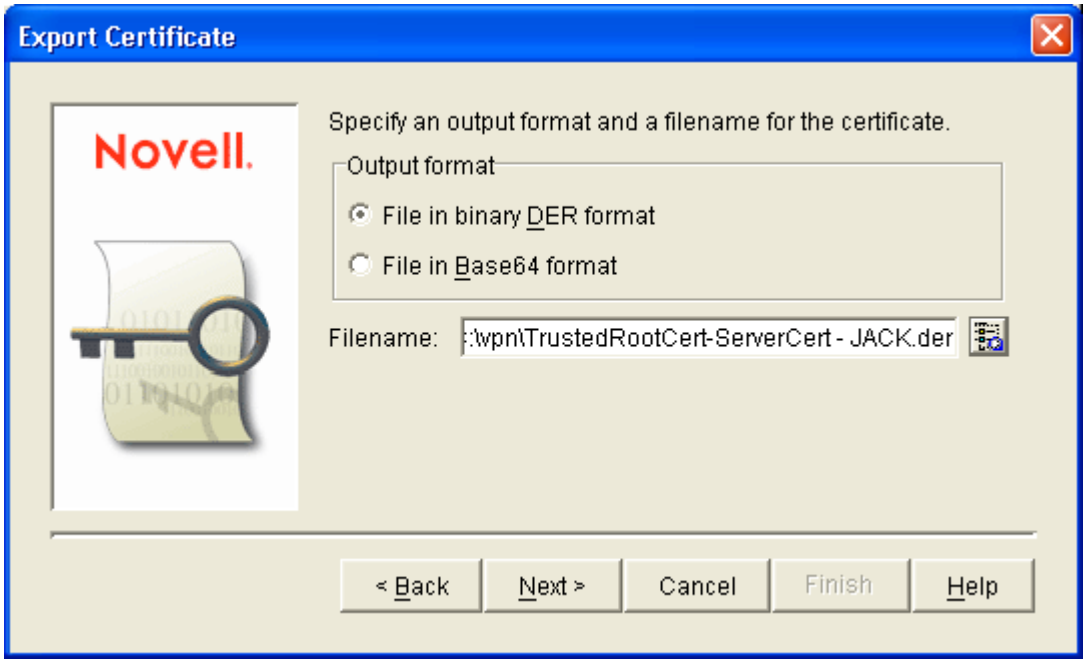
Click **Next**.



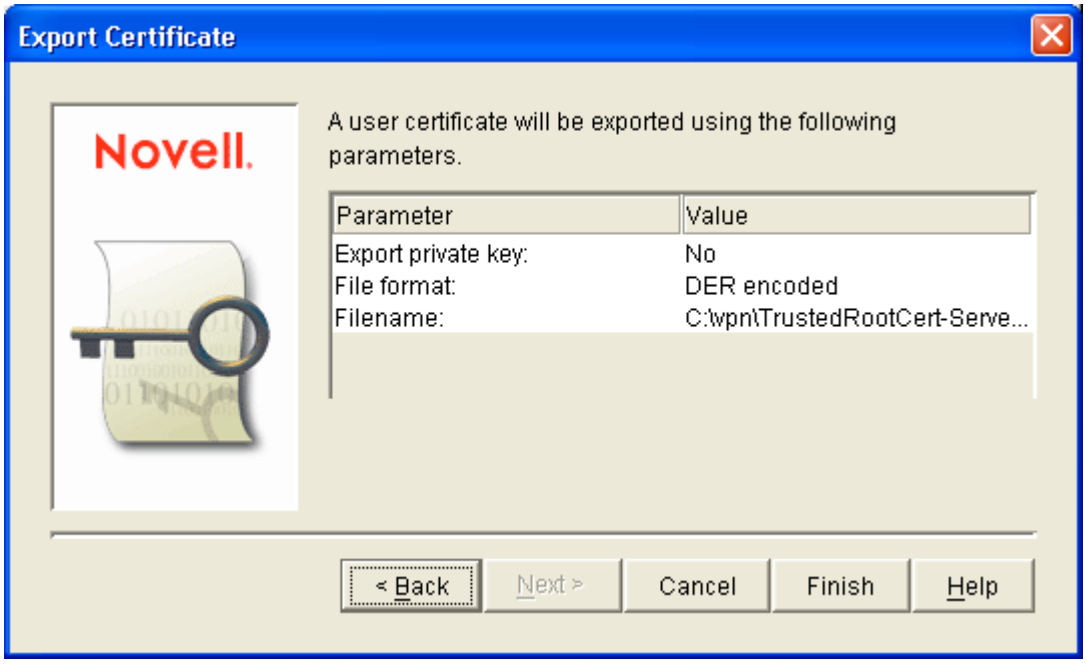
Export the key in DER format. Instead of using the default file location, you may want to browse to a more convenient directory.



In this case, I have created a subdirectory on the C drive of the local PC called VPN to use for storing the .DER files.



Click **Next** when the file name and location are to your liking.

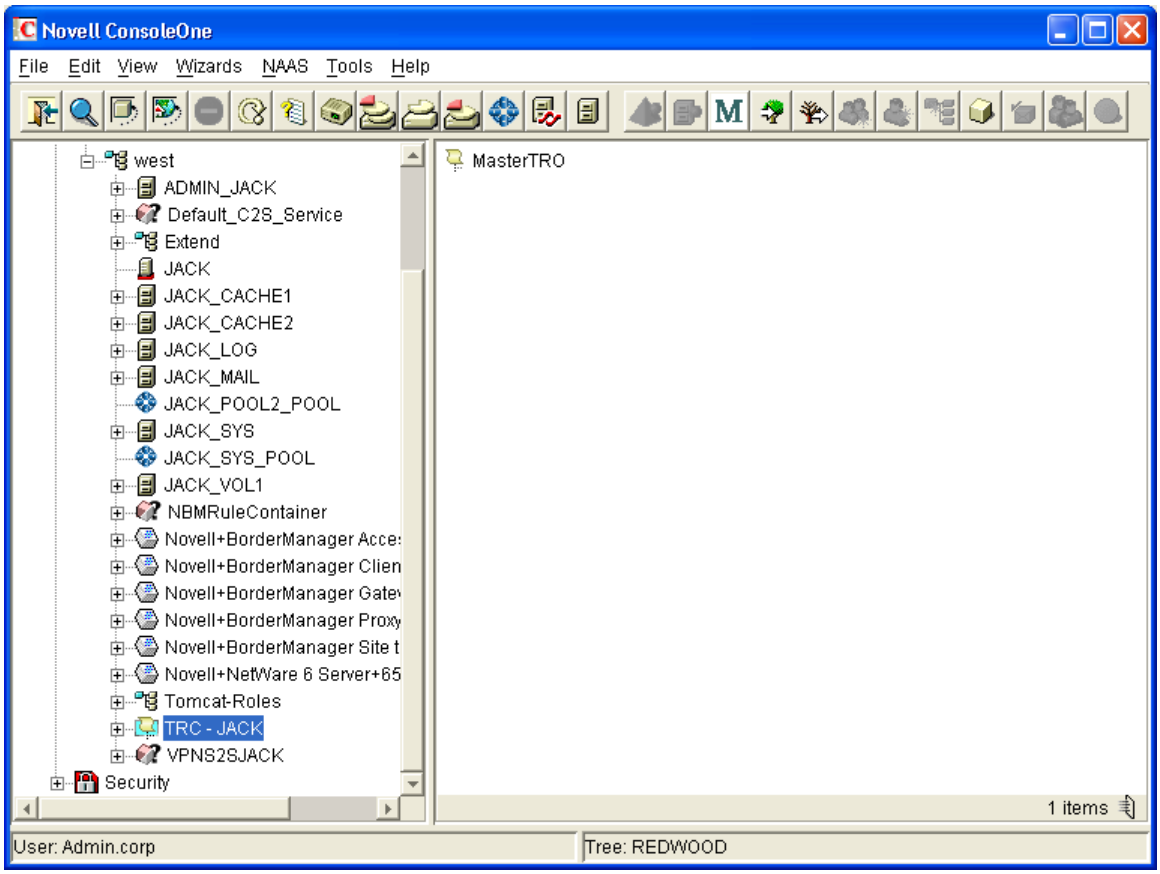


Click **Finish**.

Create MOE's Trusted Root Object from a .DER File Using ConsoleOne

This example shows how to create a TRO from a .DER file, using ConsoleOne. The TRO will be created in JACK's Trusted root container. The .DER file to be used was exported from slave server MOE's ServerCert – MOE certificate. That certificate is configured on MOE as the certificate to be used for VPN.

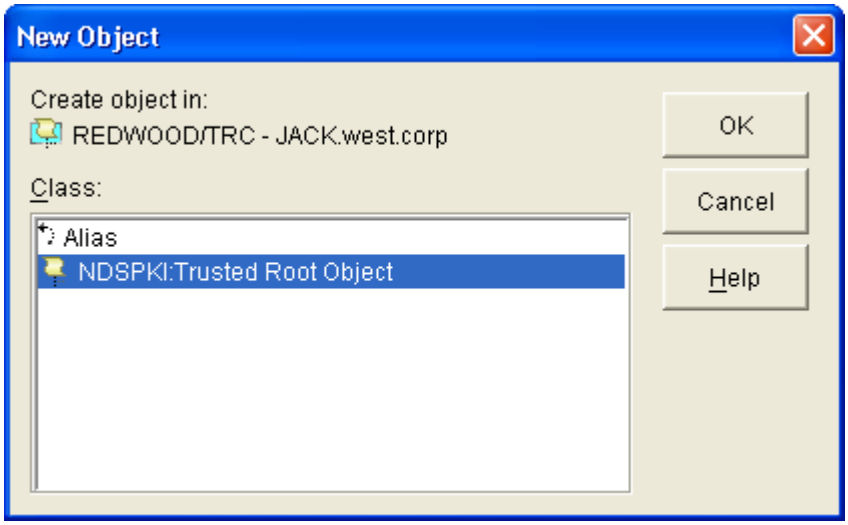
An example later in this chapter shows this operation being done with iManager, creating a TRO in MOE's tree from a .DER file exported from JACK's VPN certificate.



Go to the Master VPN server's Trusted Root Container (**TRC - JACK**) and open it in ConsoleOne.

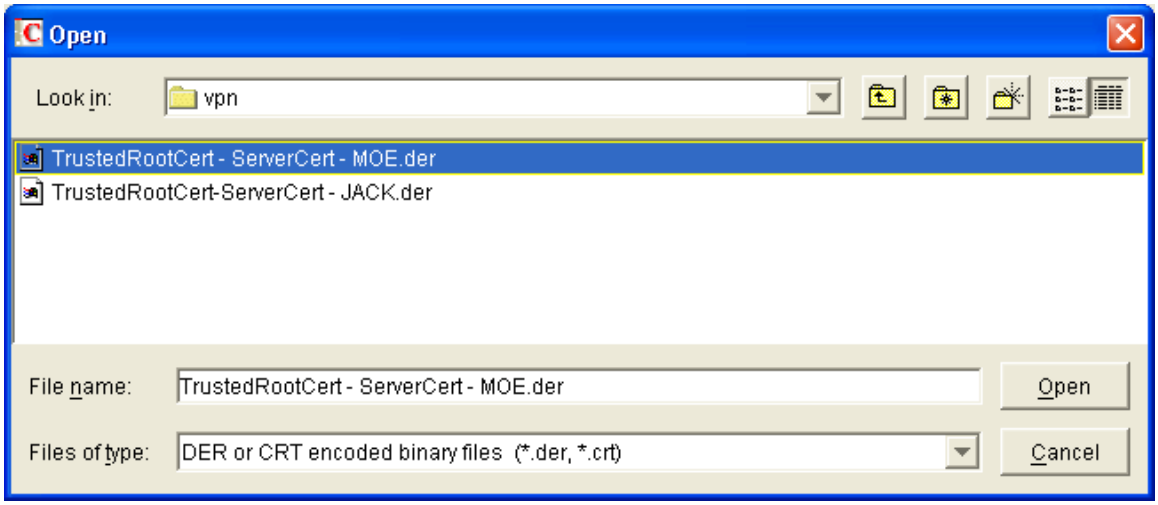
You should see the **MasterTRO** Trusted Root Object (TRO) created automatically by iManager when the server was configured as a VPN server. (The name of the TRO may be different than that shown in this example, if you configured a TRO manually).

Click on the button to add a new object.



Select **NDPSKI:Trusted Root Object.** Click **OK**.

You will have to browse to the location of the slave server's .DER file, exported earlier. (The procedure used to do that is shown later in this chapter, under the iManager example for exporting a certificate to a .DER file).

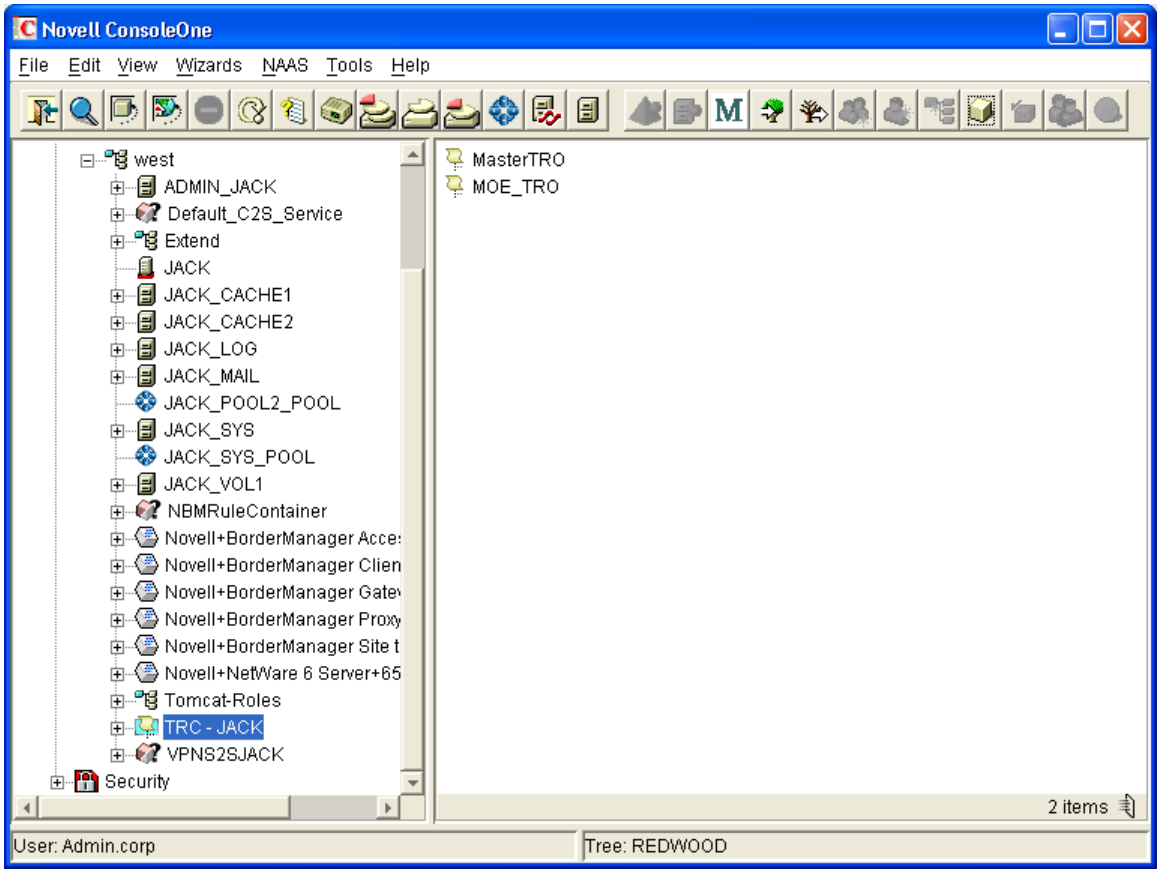


Select the .DER file from the slave server's exported VPN certificate, and click on **Open**.

Add a descriptive name in the **NDS Object Name** field.

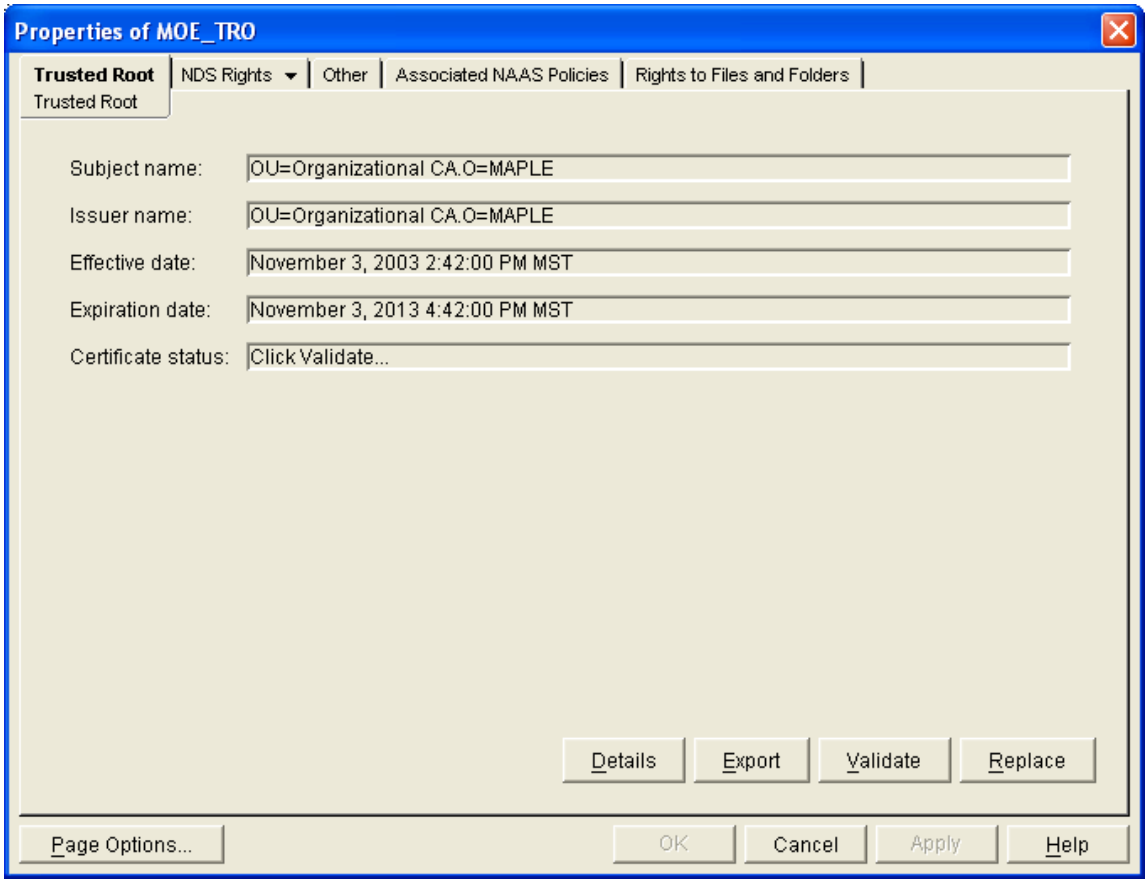
This name will become the name of the TRO for the slave server, and it should suffice to validate any VPN certificate issued by the certificate authority in the slave server's NDS tree. Therefore, the name might best describe the slave server's NDS tree rather than the slave server itself. However, any suitable name will do.

When the name of the NDS object has been entered, click **Finish** to have ConsoleOne create the TRO.



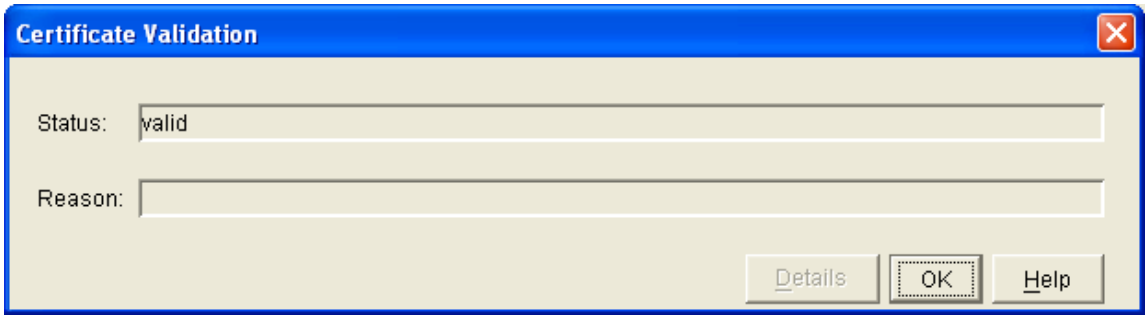
The Master VPN server now should be able to validate/decrypt the slave server MOE's VPN certificate, by looking up a trusted root object for Moe in JACK's Trusted Root Container.

Double-click on MOE's TRO (MOE_TRO) to look at the properties of the object.



An important step here to save troubleshooting time later is to be sure that the TRO you created is actually valid. Notice that the Certificate Status field says **Click Validate**…

Click on the **Validate** button to check the validity of the Trusted Root.



If you see anything other than Valid, you should check the entire procedure of configuring the server certificate, exporting it to a .DER file, and importing the .DER file to create a TRO. If the trusted root is shown to be invalid on this check, the VPN will not make a connection to the server involved.

Manually Creating A Trusted Root Object (TRO), Using iManager

This section shows the procedure for manually creating a Trusted Root Object (TRO) for a server using iManager.

All operations will be done in MOE's NDS tree.

Two procedures are shown:

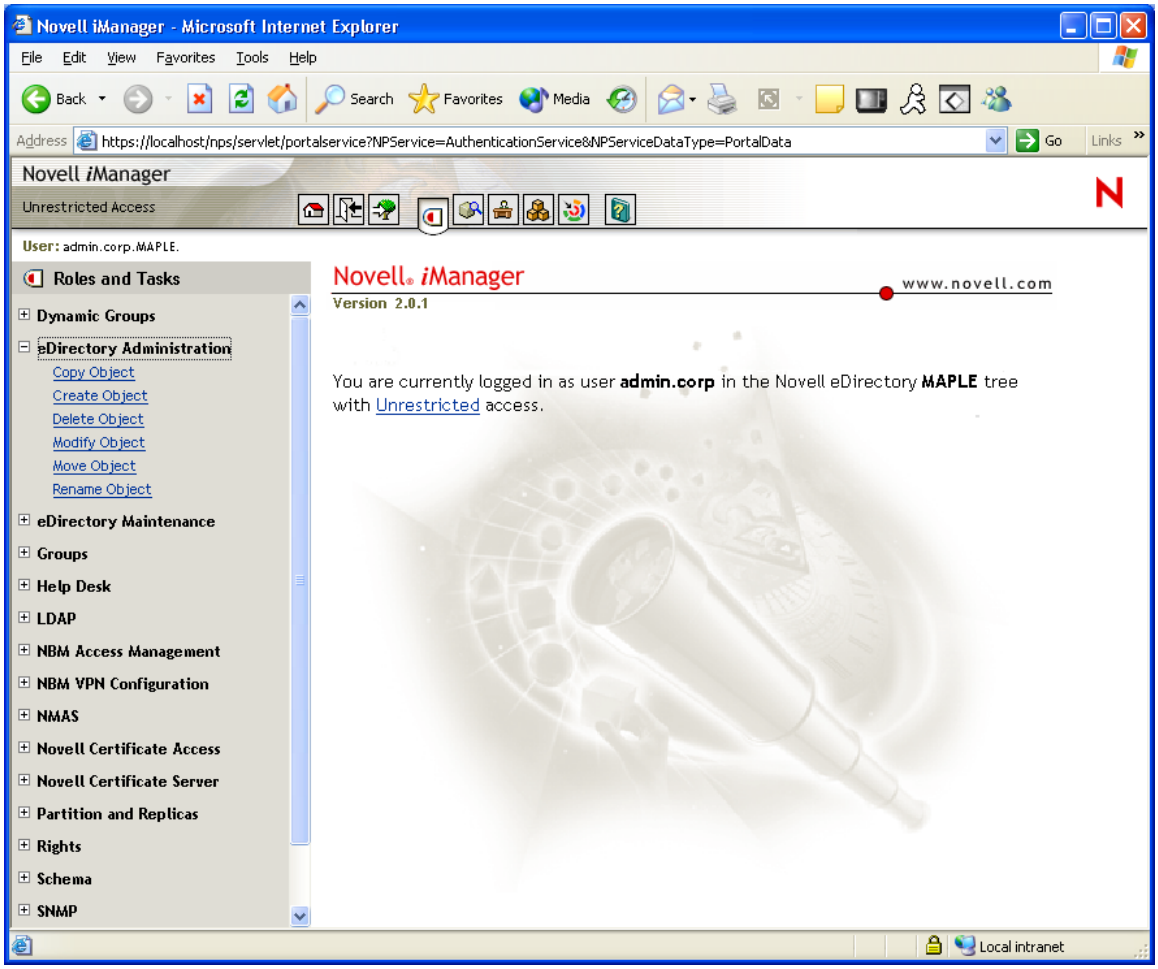
- Exporting MOE's VPN server certificate to a .DER file. This file will be used by JACK to create a TRO for MOE.
- Importing JACK's exported server certificate file into MOE's trusted root container (TRC) to create a TRO for JACK.

The same procedures can be done using ConsoleOne, and those procedures are shown earlier in this chapter. You have the choice of using iManager or ConsoleOne, and this book is simply showing a procedure for either method.

The TRO shown is for the server JACK, and is necessary in order to add JACK as the master server for each slave server. The manual creation procedure is necessary because MOE is in a different NDS tree than JACK.

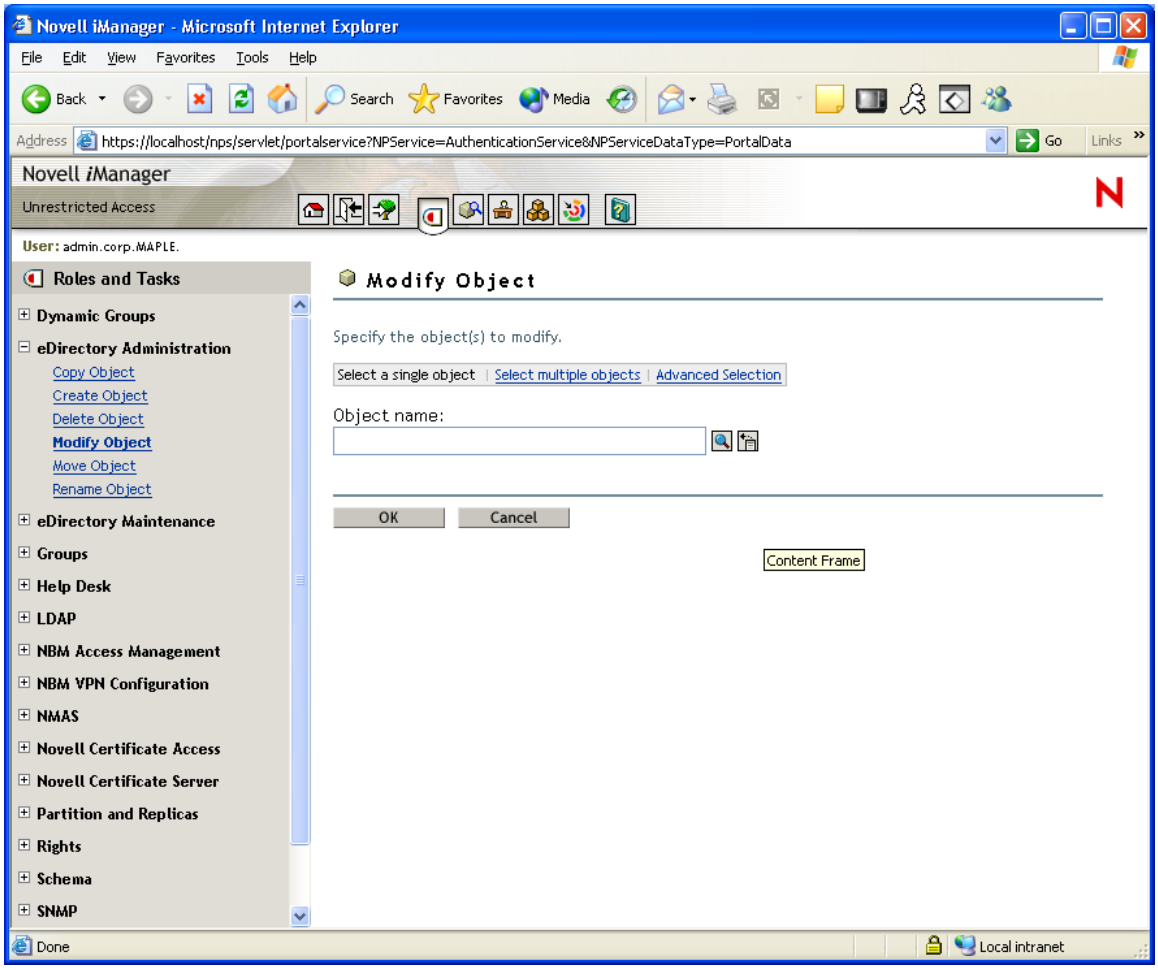
Exporting MOE's VPN Certificate to a .DER File using iManager

Start by logging into the slave server's NDS tree in iManager.

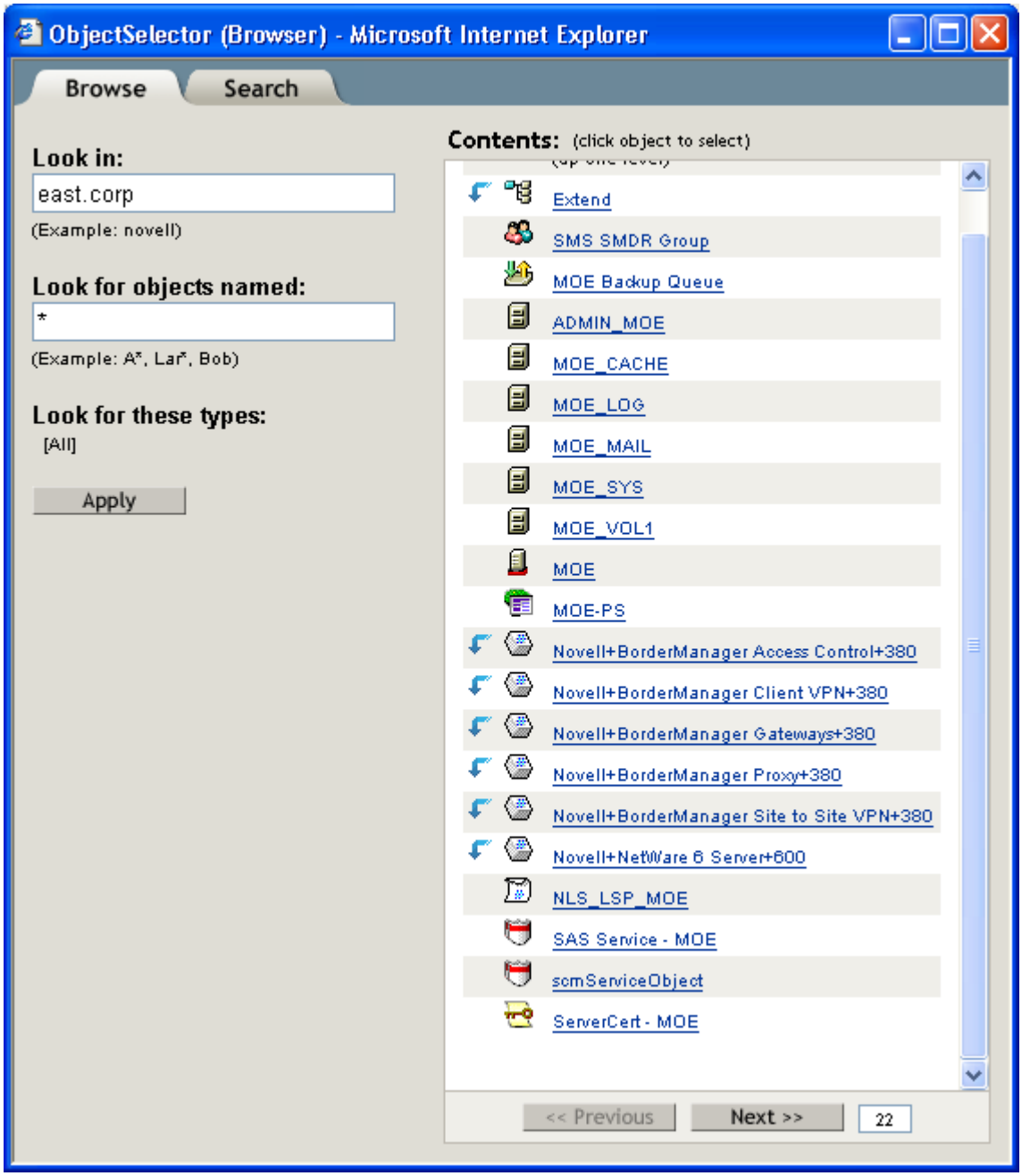


In iManager, expand the **eDirectory Administration** link.

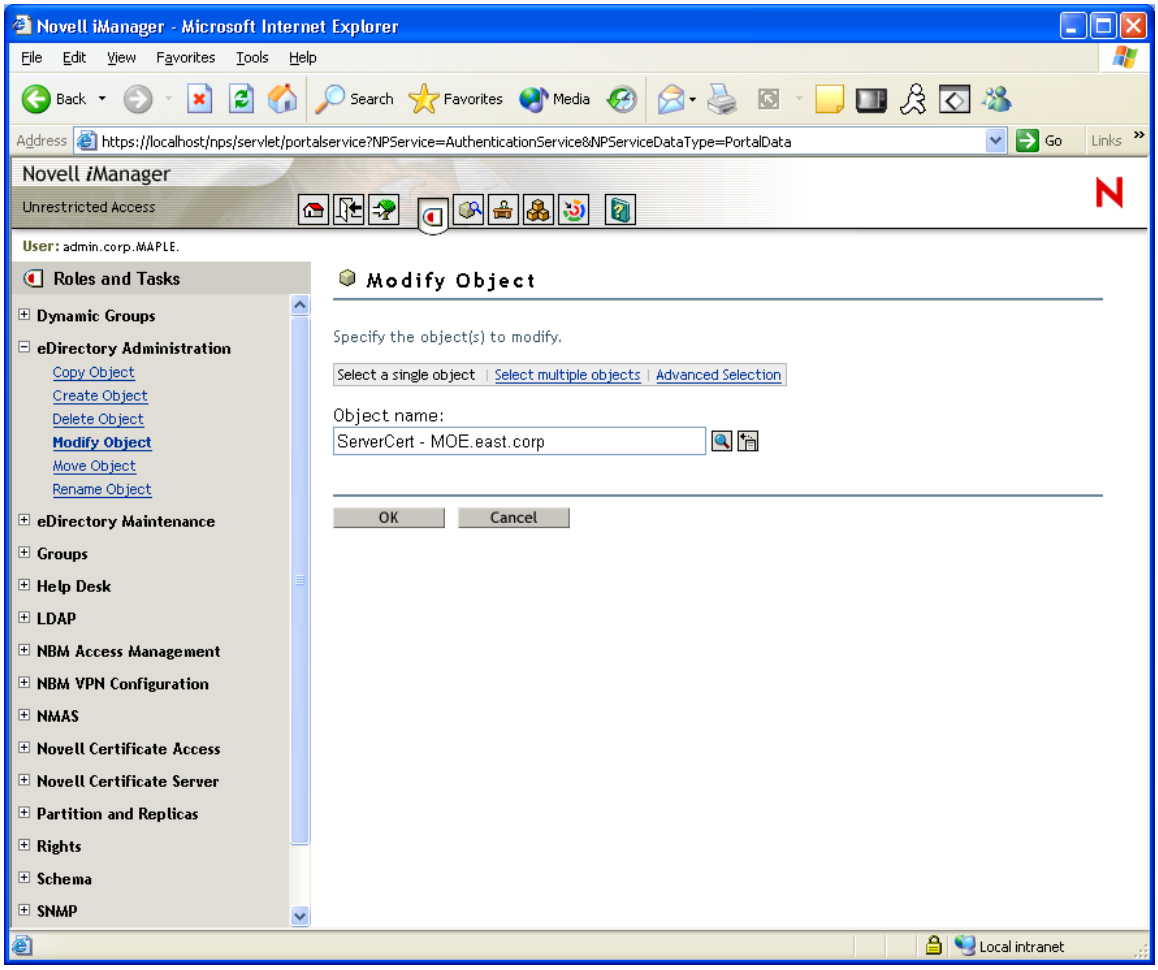
Select **Modify Object**.



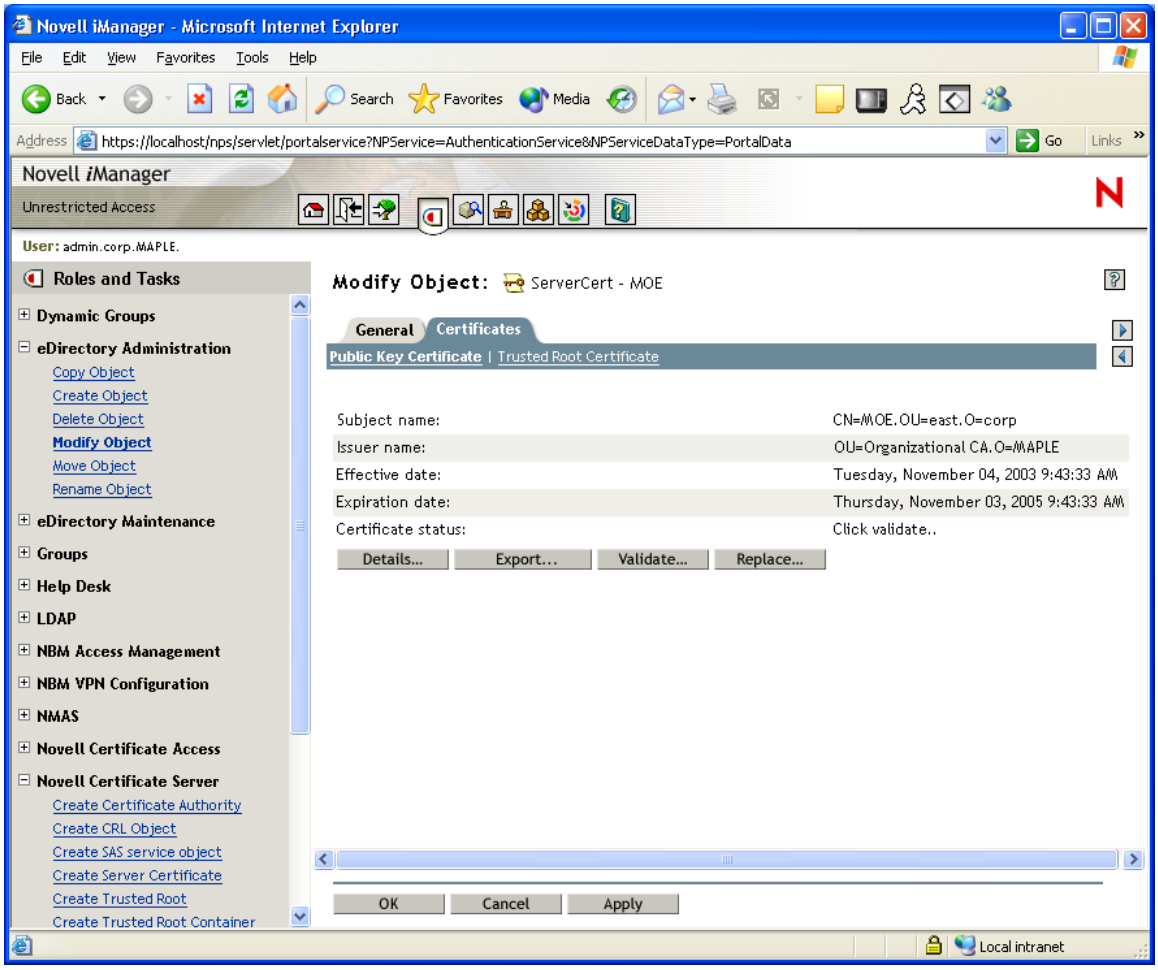
Click the **Browse** icon.



Find and select the VPN server certificate, in this example **ServerCert – MOE**.


Novell iManager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://localhost/nps/servlet/portalservice?NPService=AuthenticationService&NPServiceDataType=PortalData
Go Links
Novell iManager
Unrestricted Access
User: admin.corp.MAPLE.
Roles and Tasks
Dynamic Groups
eDirectory Administration
Copy Object
Create Object
Delete Object
Modify Object
Move Object
Rename Object
eDirectory Maintenance
Groups
Help Desk
LDAP
NBM Access Management
NBM VPN Configuration
NMAS
Novell Certificate Access
Novell Certificate Server
Partition and Replicas
Rights
Schema
SNMP
Modify Object
Specify the object(s) to modify.
Select a single object | Select multiple objects | Advanced Selection
Object name:
ServerCert - MOE.east.corp
OK
Cancel
Local intranet

Click **OK**.

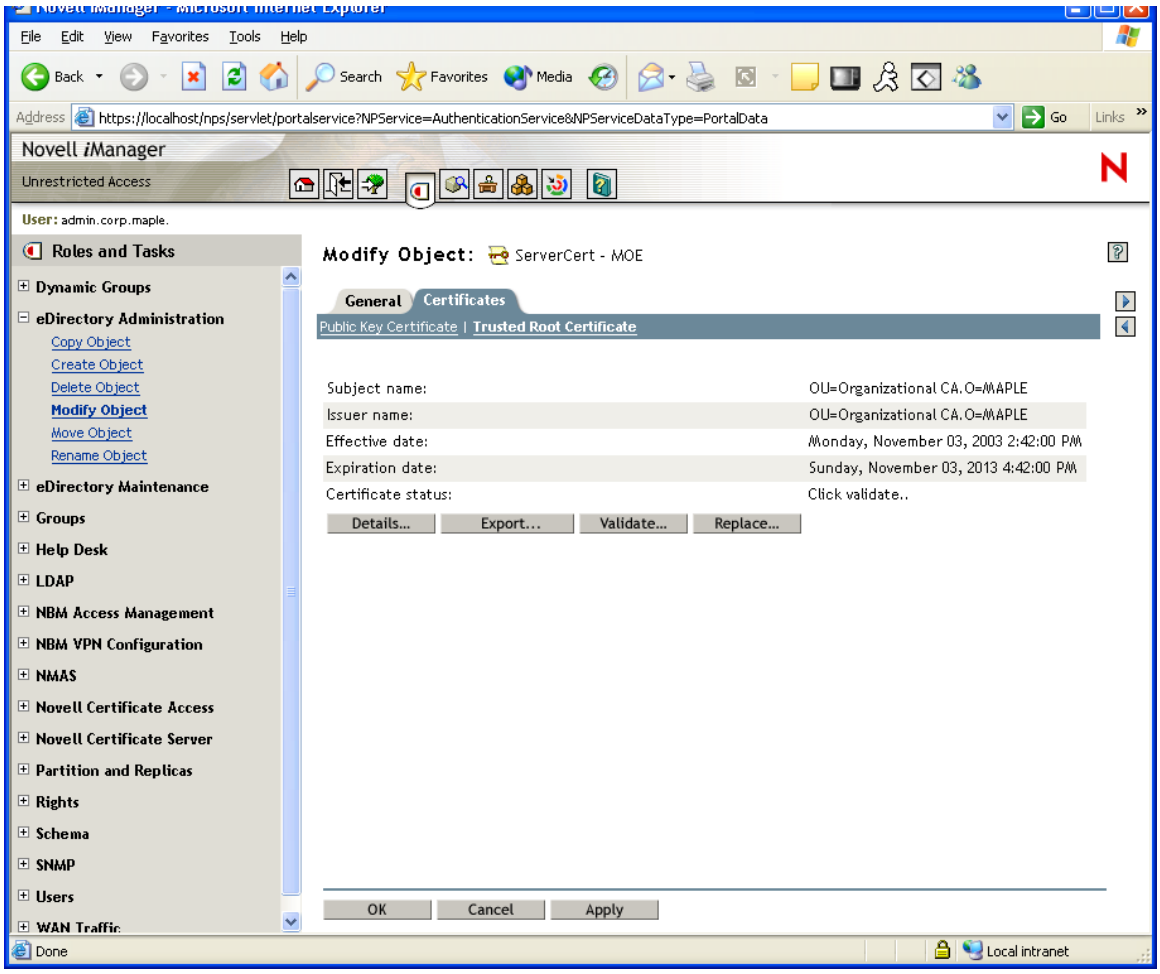


Click on the **Certificates** tab. Click on the **Public Key Certificate** tab.

Make a note of the **Subject Name** here. You will need it when importing the certificate into the master VPN server. You might want to screenshot this menu to a document.

In this example, the **Public Key Subject Name** is **CN=MOE.OU=east.O=corp**.

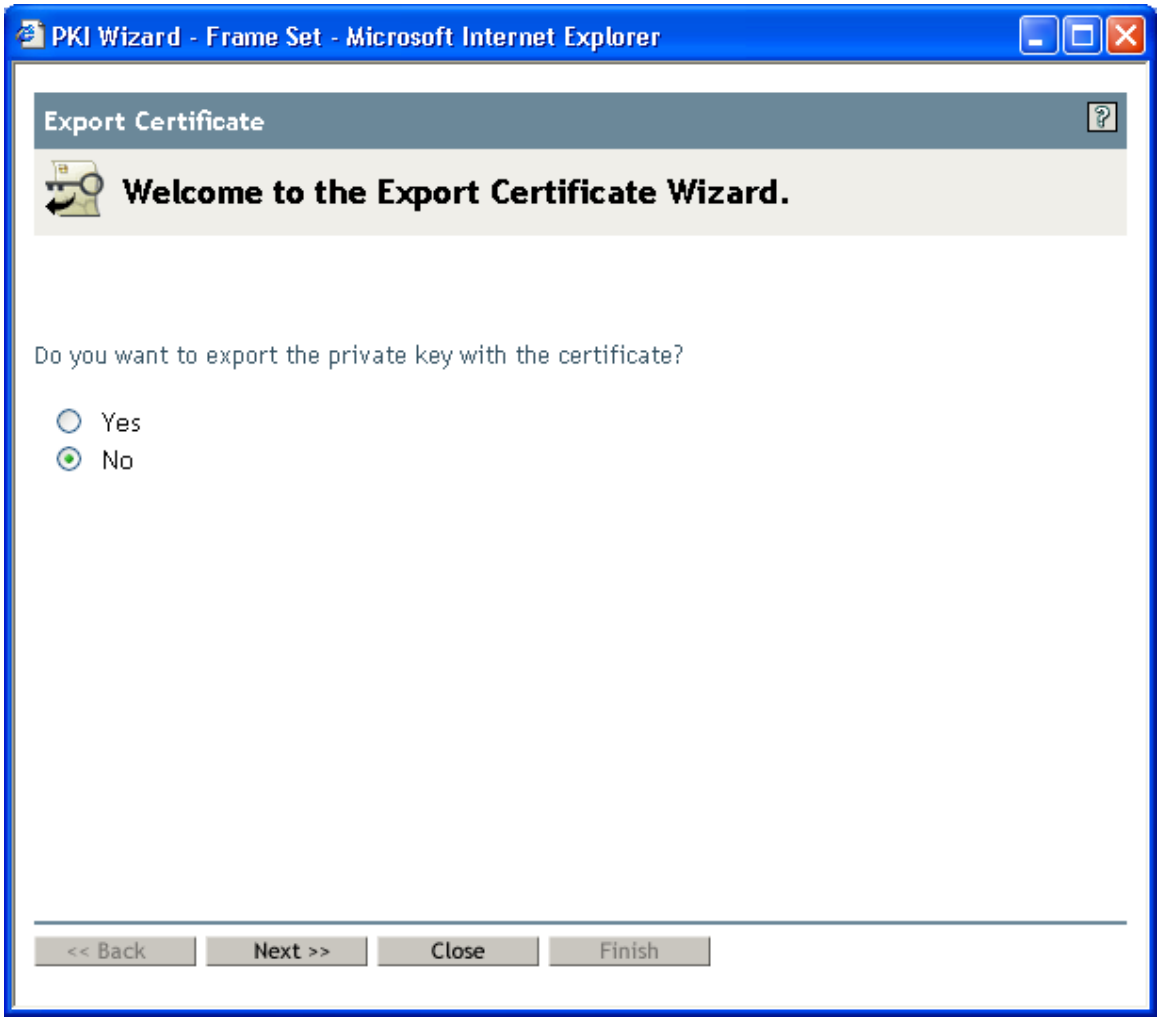
Do not export the certificate from this menu.



Now select the **Trusted Root Certificate** tab.

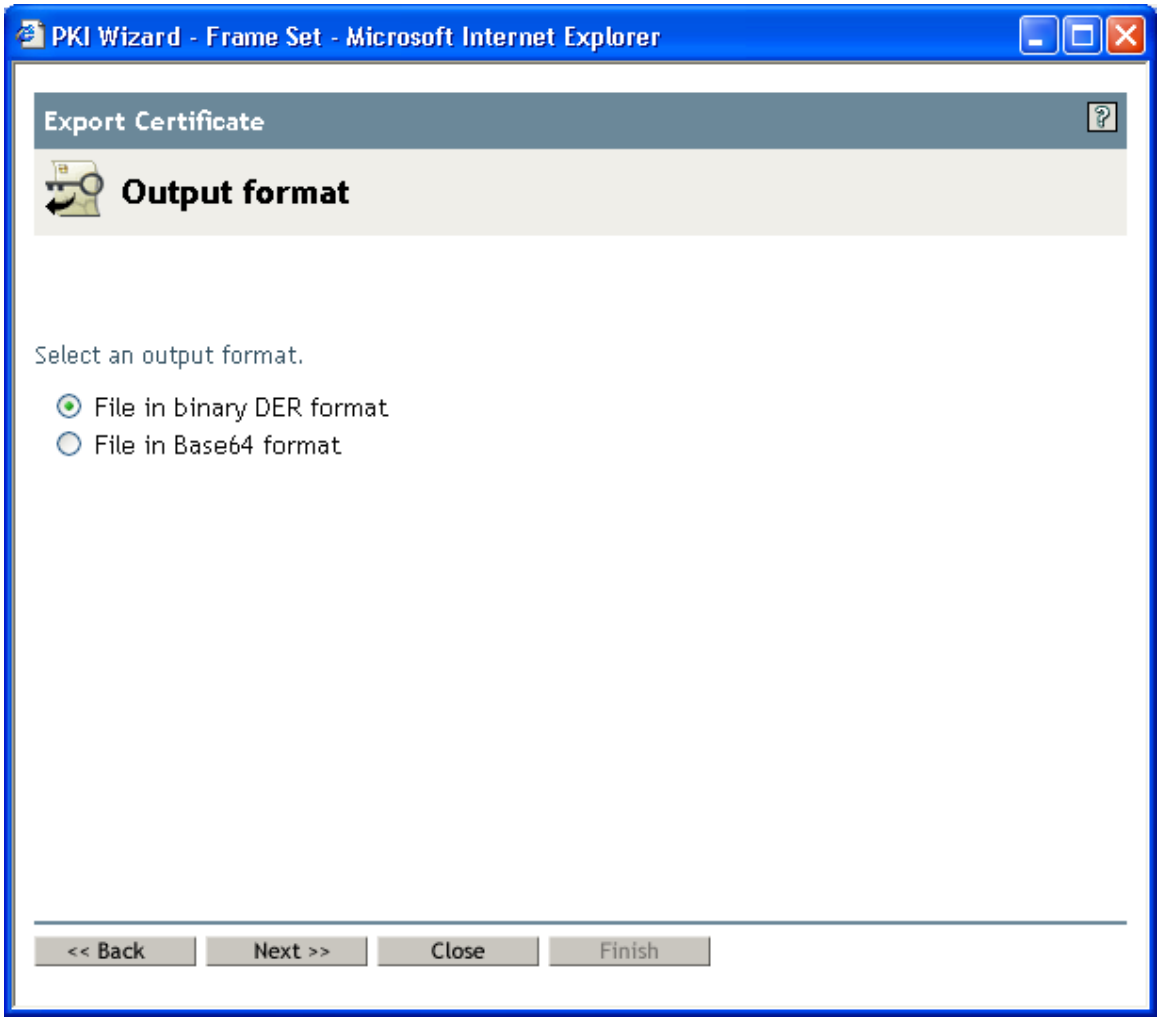
This is what we want to export to a .DER file.

Click on **Export**.

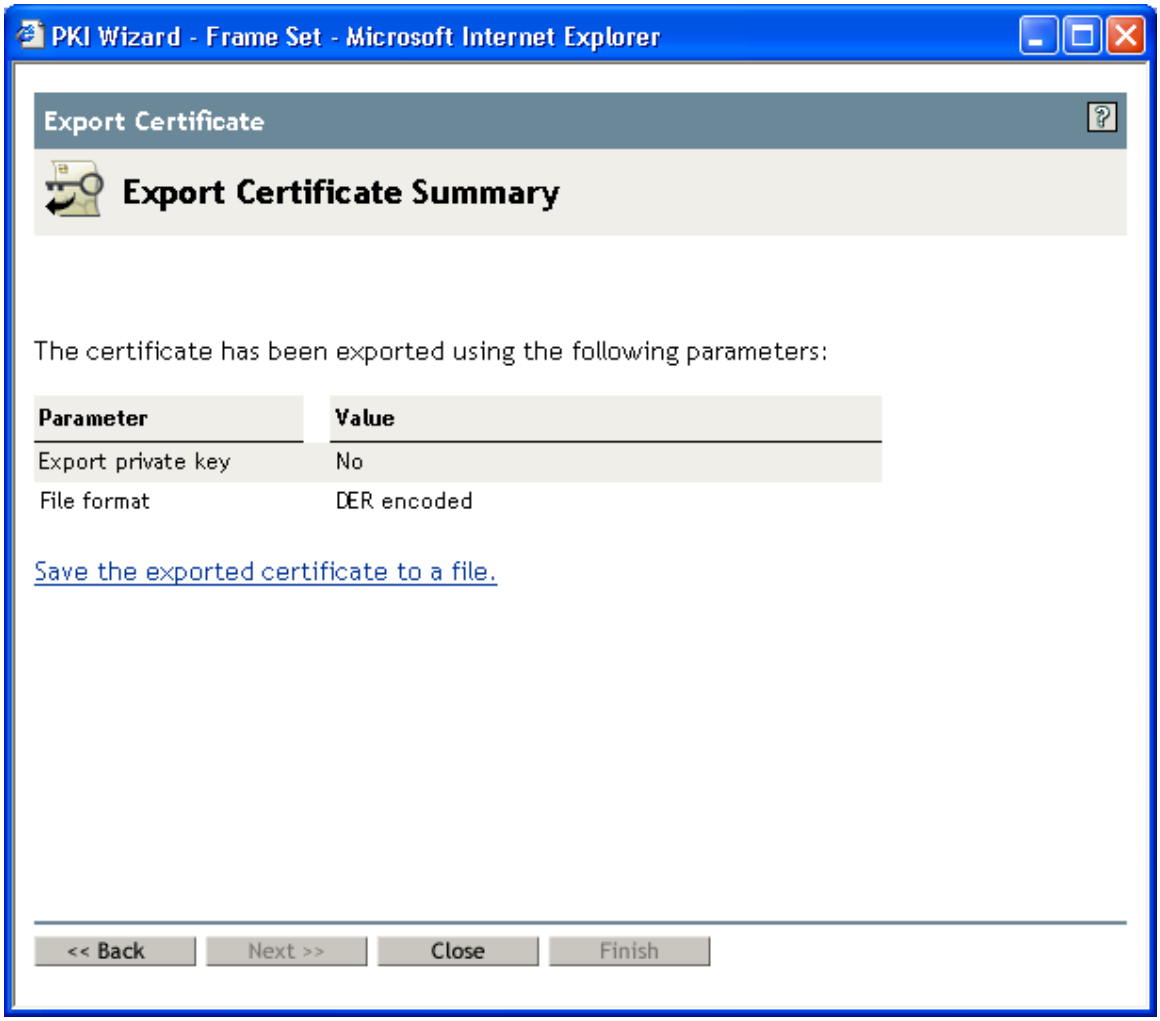


Select **No** – you do not want to export the private key.

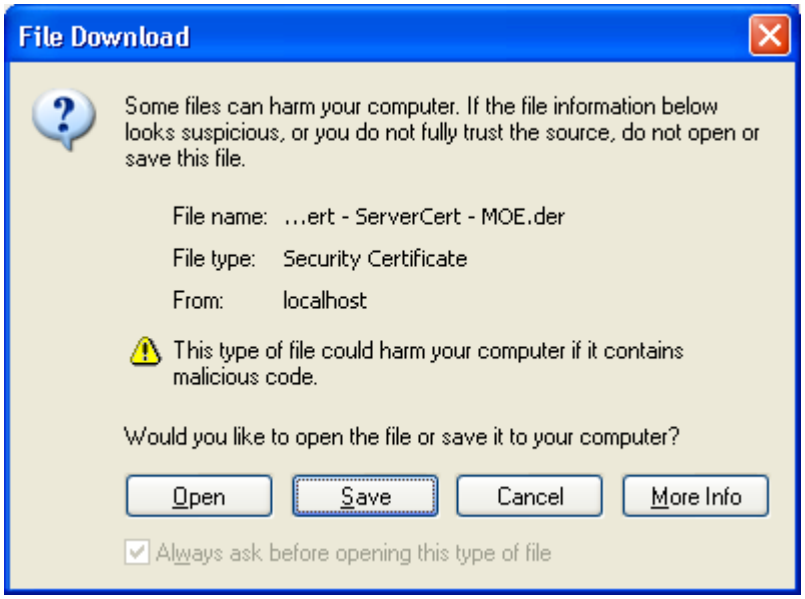
Click on **Next**.



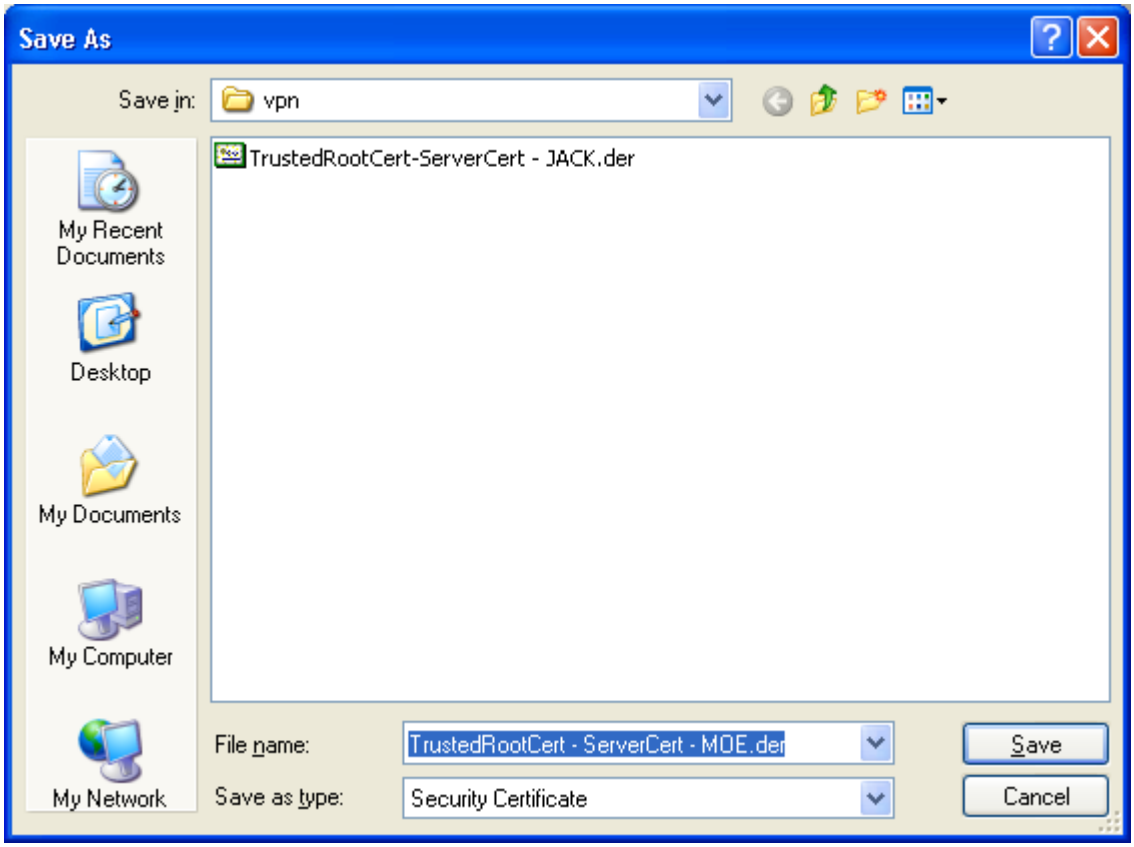
Select **File in binary DER format**, and click **Next**.



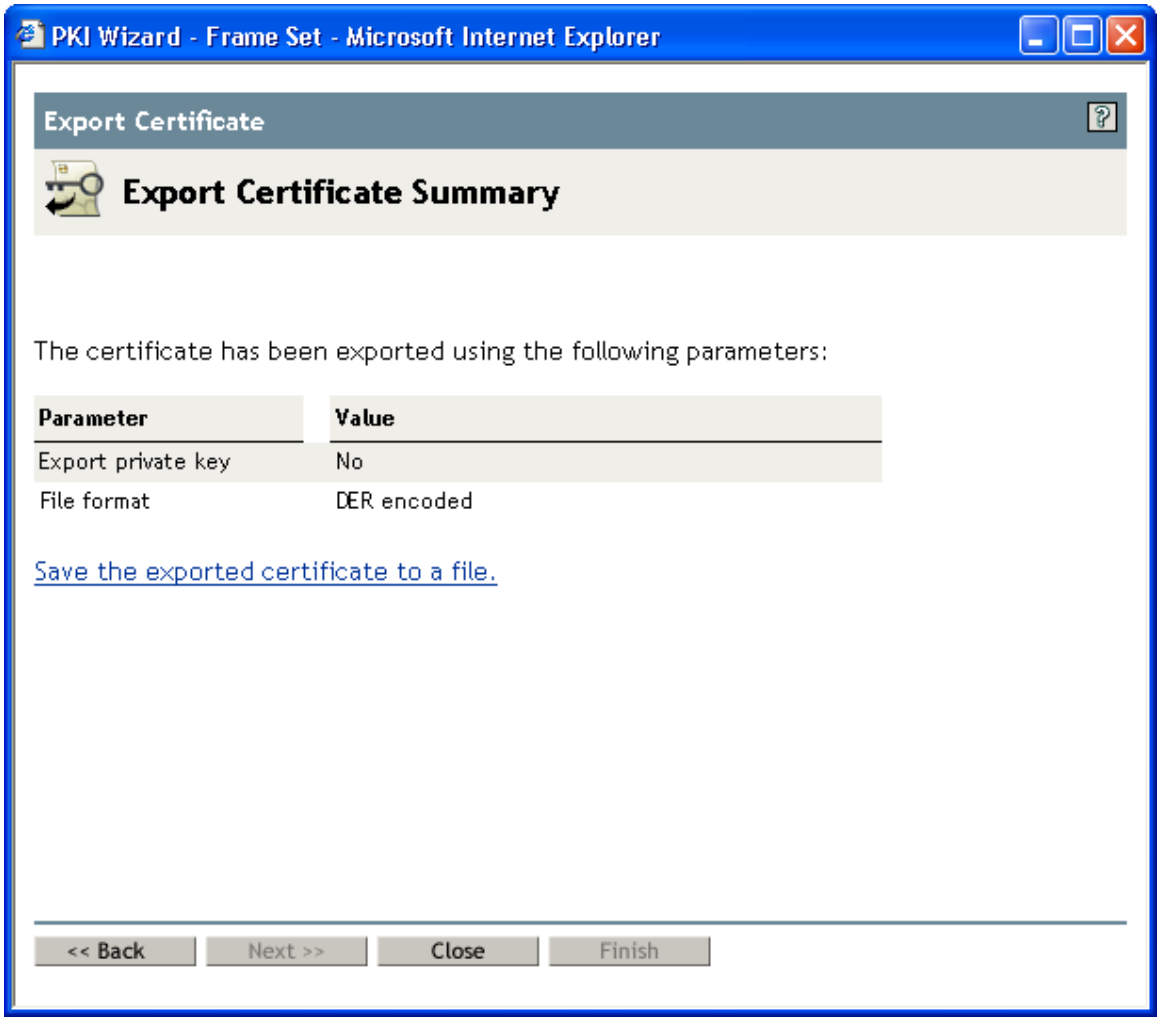
Click on **Save the exported certificate to a file**.



Your browser may give you a warning message. If you get such a warning, click **Save**.



Save the file to some convenient location where you can easily retrieve it later. You will need the file to be available in iManager or ConsoleOne later on when working in the master server's NDS tree.



You should be take back to the previous browser window. When the file has been saved, click **Close**.

Create JACK's Trusted Root Object from a .DER File Using iManager

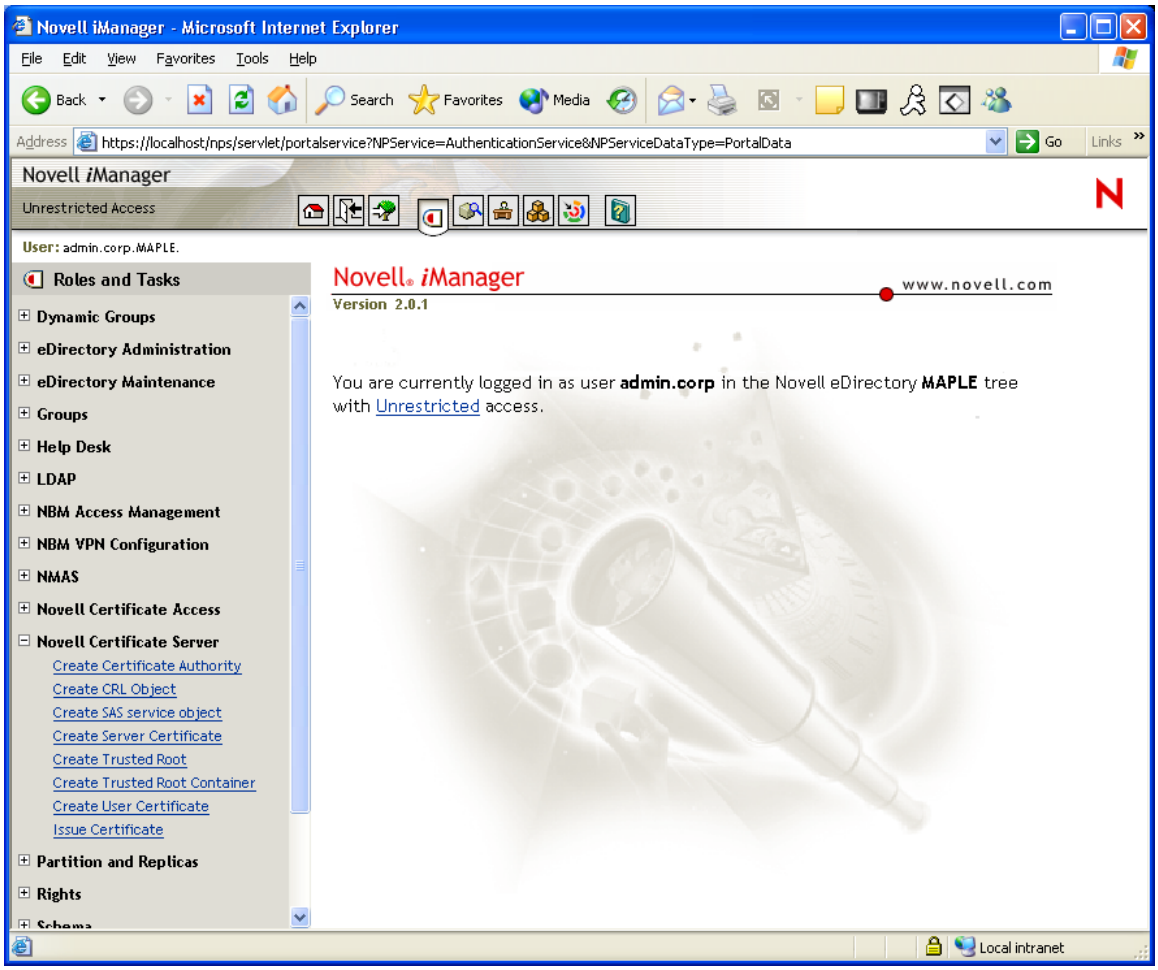
If master and slave VPN servers are not in the same NDS tree, you have to manually create a Trusted Root Object (TRO) for each server in the other server's Trusted Root Container (TRC).

The master server needs a TRO for each slave server. The TRO is created from a .DER file exported from the slave server VPN certificate, if the slave and master are not in the same NDS tree. (If the servers are in the same tree, the process is simpler because you do not have to export and import .DER files). The slave server TRO's are created in the master server's TRC.

The slave server only needs a TRO from the master server, not from all of the other slaves in a multi-server Site-to-Site VPN. The master VPN server takes care of pushing encryption information about each slave to the other slaves automatically. The master server TRO is created in the slave server's TRC.

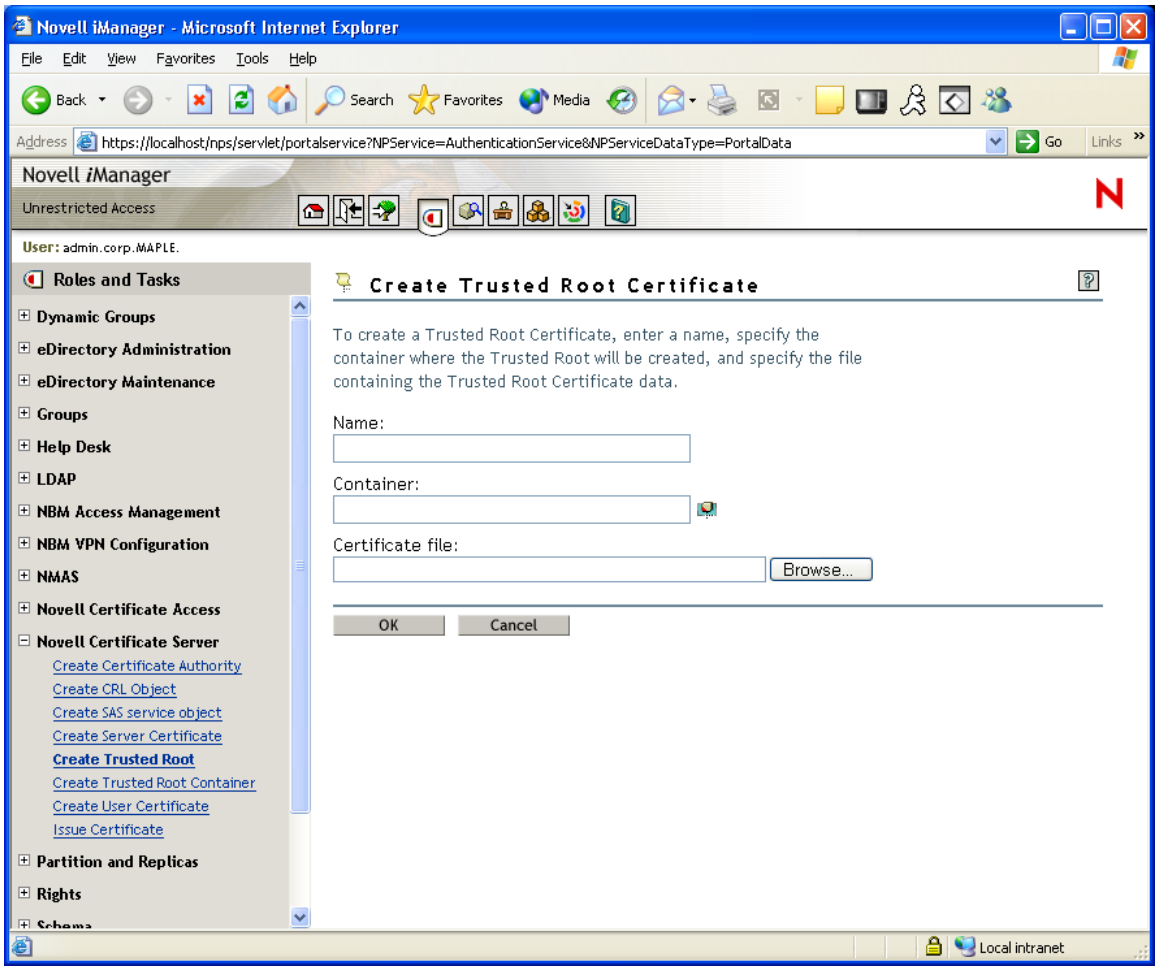
Manually exporting certificates and creating TRO's by importing .DER files can be done in either iManager or ConsoleOne. iManager is shown here, but an example using ConsoleOne is given earlier in this chapter.

Before starting, you must have already exported the master server's VPN certificate public key to a .DER file, and have the .DER file available to you.

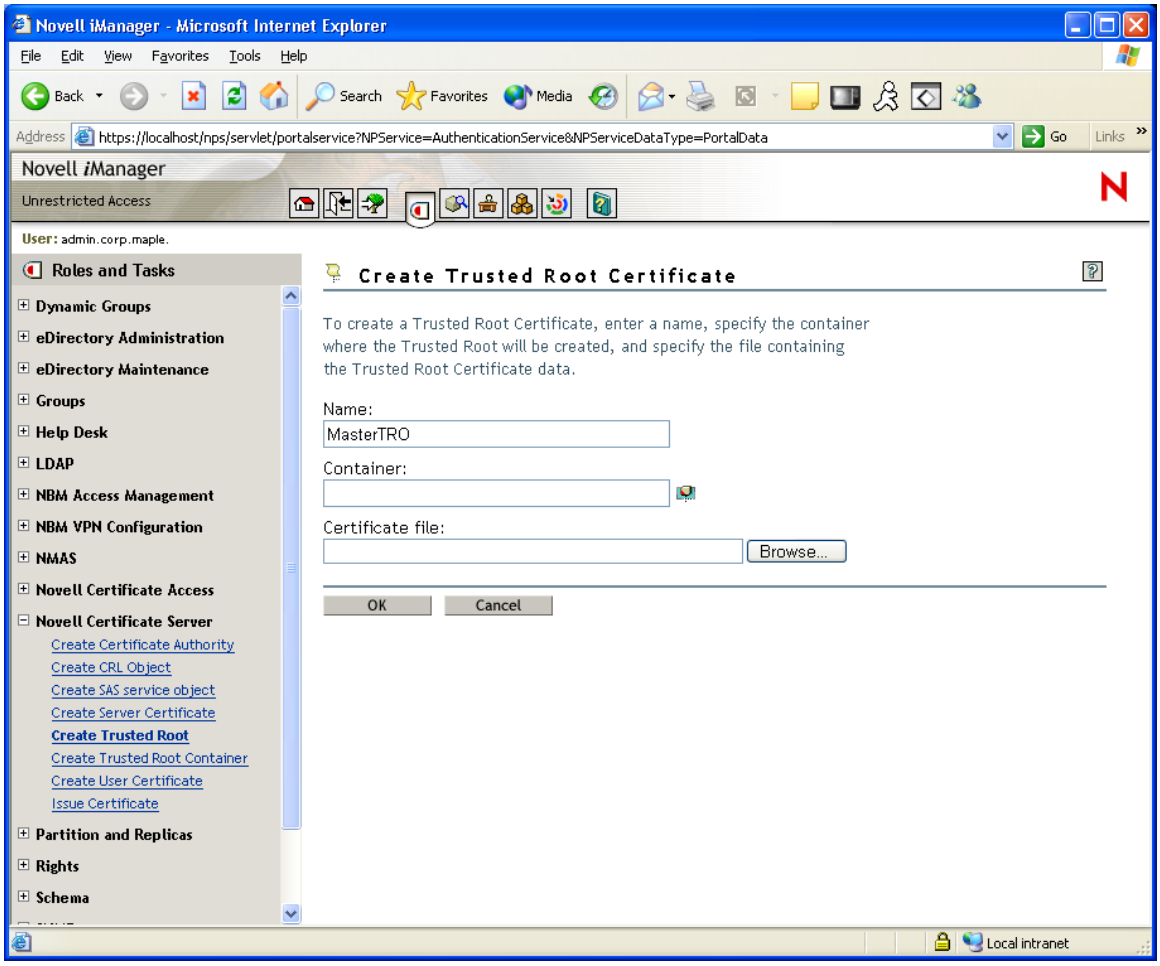


Expand the **Novell Certificate Server** link.

Click on **Create Trusted Root**.



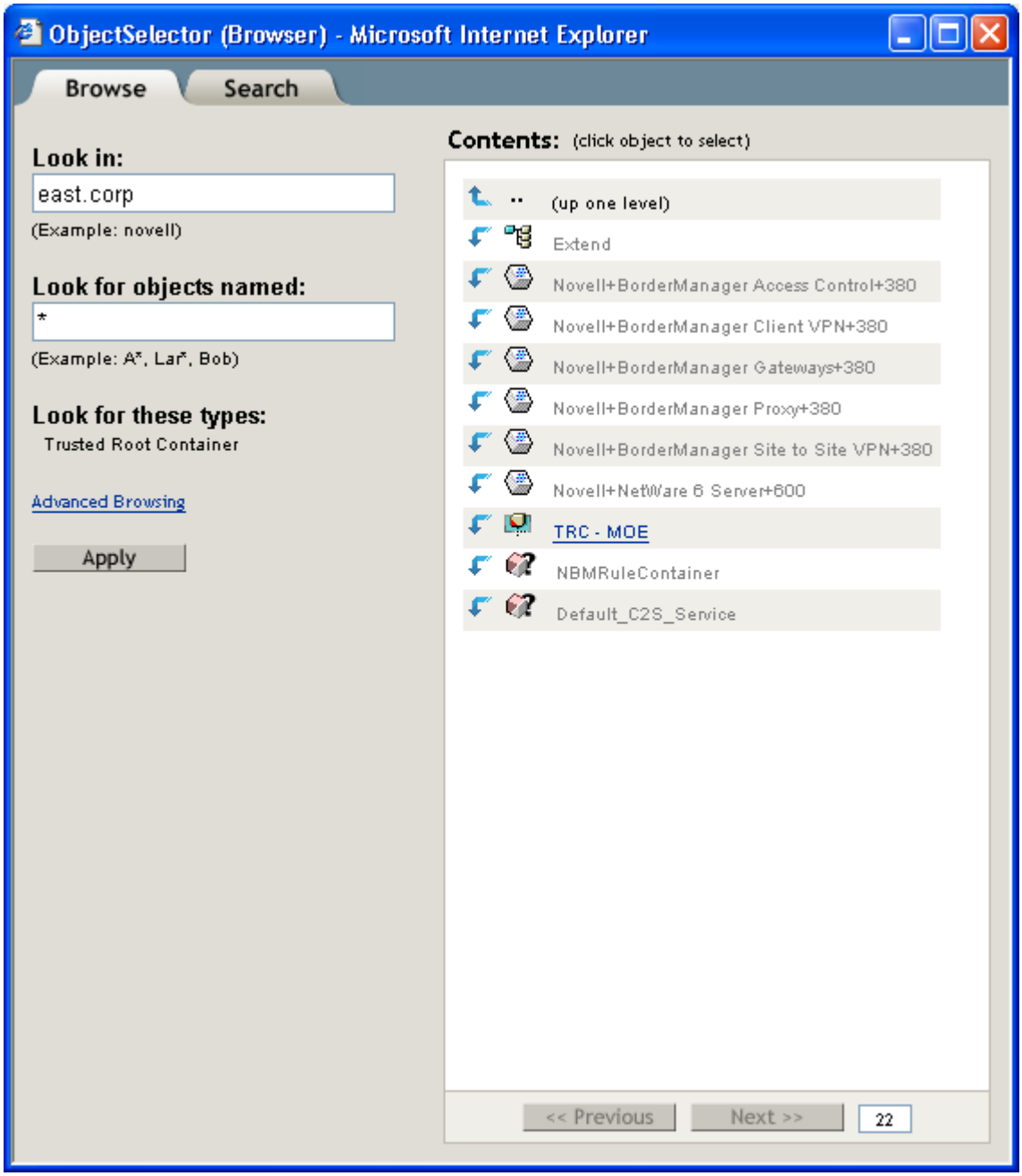
The menu for creating a Trusted Root Certificate should appear. This is the same as creating a Trusted Root Object (TRO).



Add a descriptive name in the **Name** field to be given to the TRO for JACK's exported certificate.

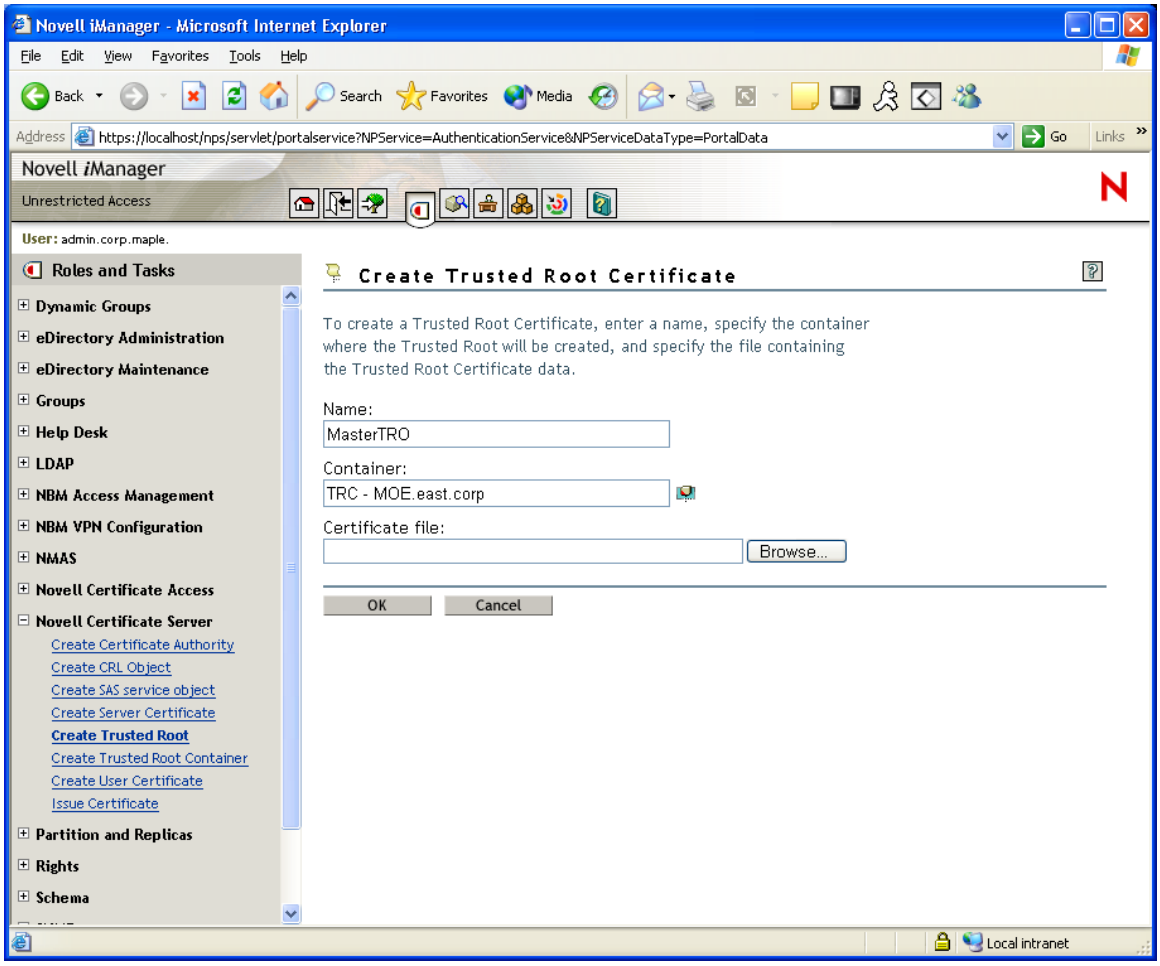
In this example, the TRO will be called **MasterTRO**.

Then browse to the Trusted Root Container in MOE's NDS tree container by clicking on the browse icon next to the Container field.



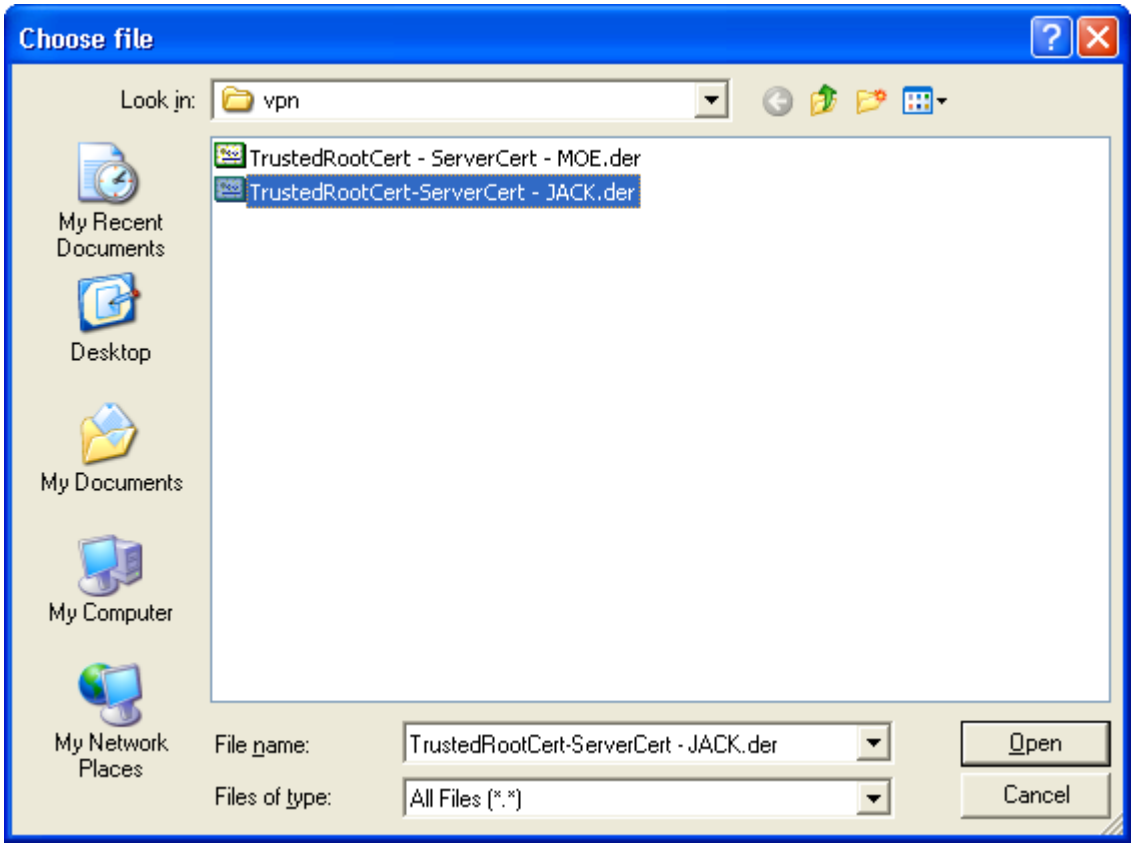
Next, you need to select the **Trusted Root Container (TRC)** where you intend to create a Trusted Root Object.

In this example, the TRC for MOE is called **TRC – MOE**, and was created in the same NDS container as MOE.



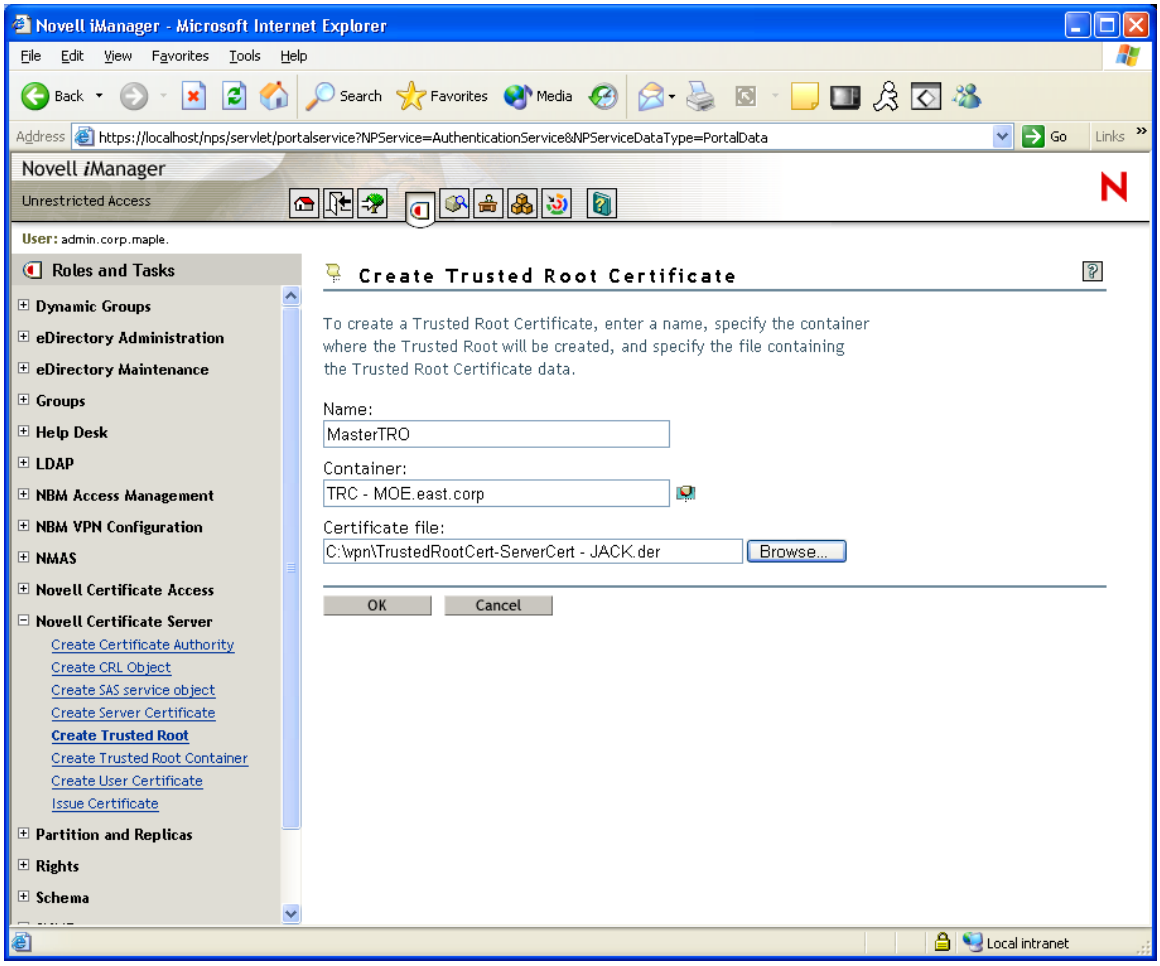
Next, you need to import the .DER file from JACK's VPN server certificate in order to create the TRO.

Click on the **Browse** button next to the **Certificate file** field.

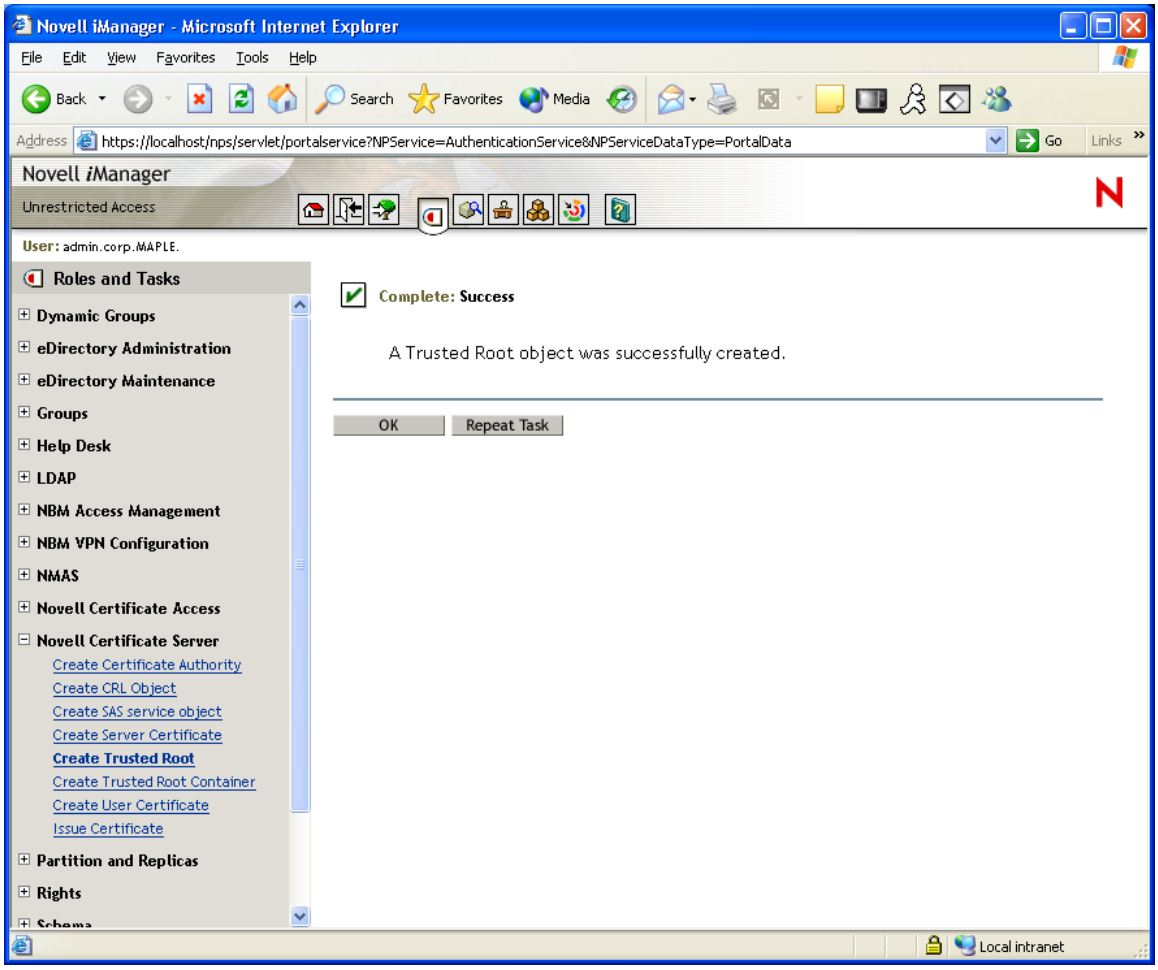


Select the correct .DER file (pick the one for the master VPN server) and click on **Open**.

In this example, we select the **TrustedRootCert-ServerCert – JACK.der** file.



When all the fields are correctly filled-in, click **OK**.



You should now have a TRO for JACK's VPN certificate, allowing slave server MOE to validate/decrypt JACK's VPN certificate.

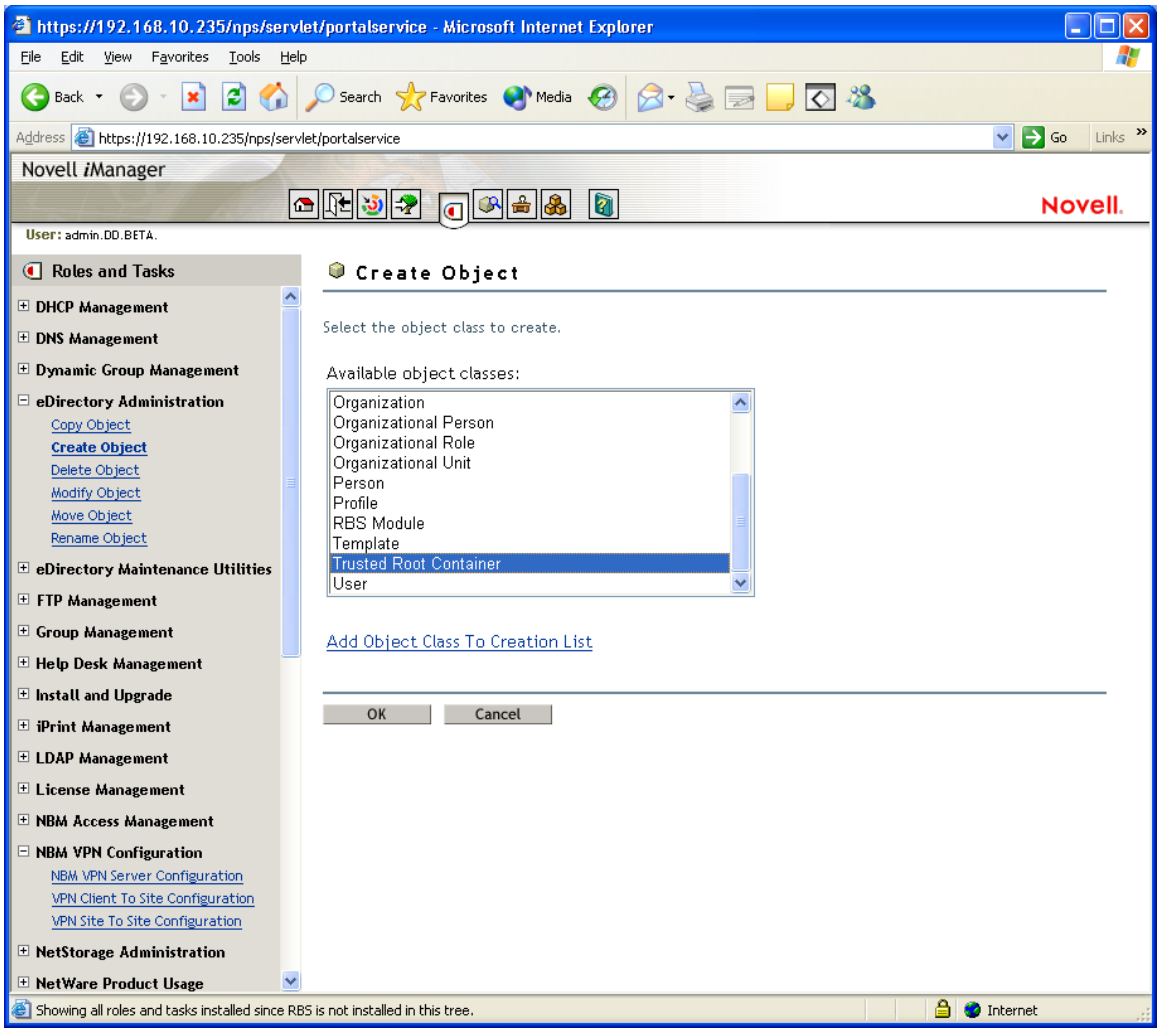
Click on **OK** when you see a Success message.

Manually Creating a Trusted Root Container (TRC)

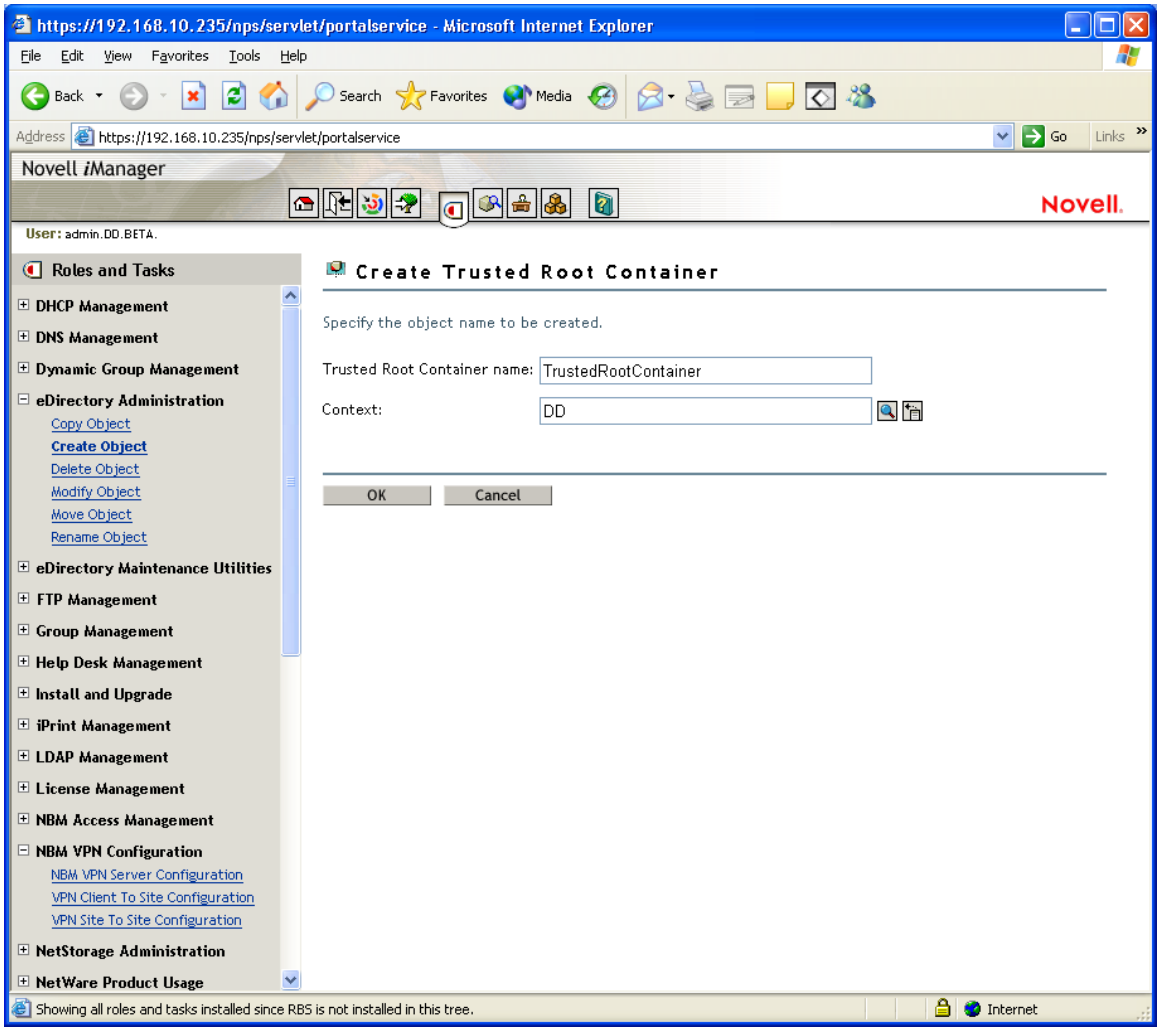
In case you want to manually create a Trusted Root Container, instead of using iManager defaults when setting up a VPN server, this section shows how. You can use iManager or ConsoleOne. The iManager procedure is shown here.

Log into iManager in the NDS tree where you want to create a Trusted Root Container.

Using iManager 2.0



Under **eDirectory Administration**, select **Create Object**, and select **Trusted Root Container** from the available object classes.

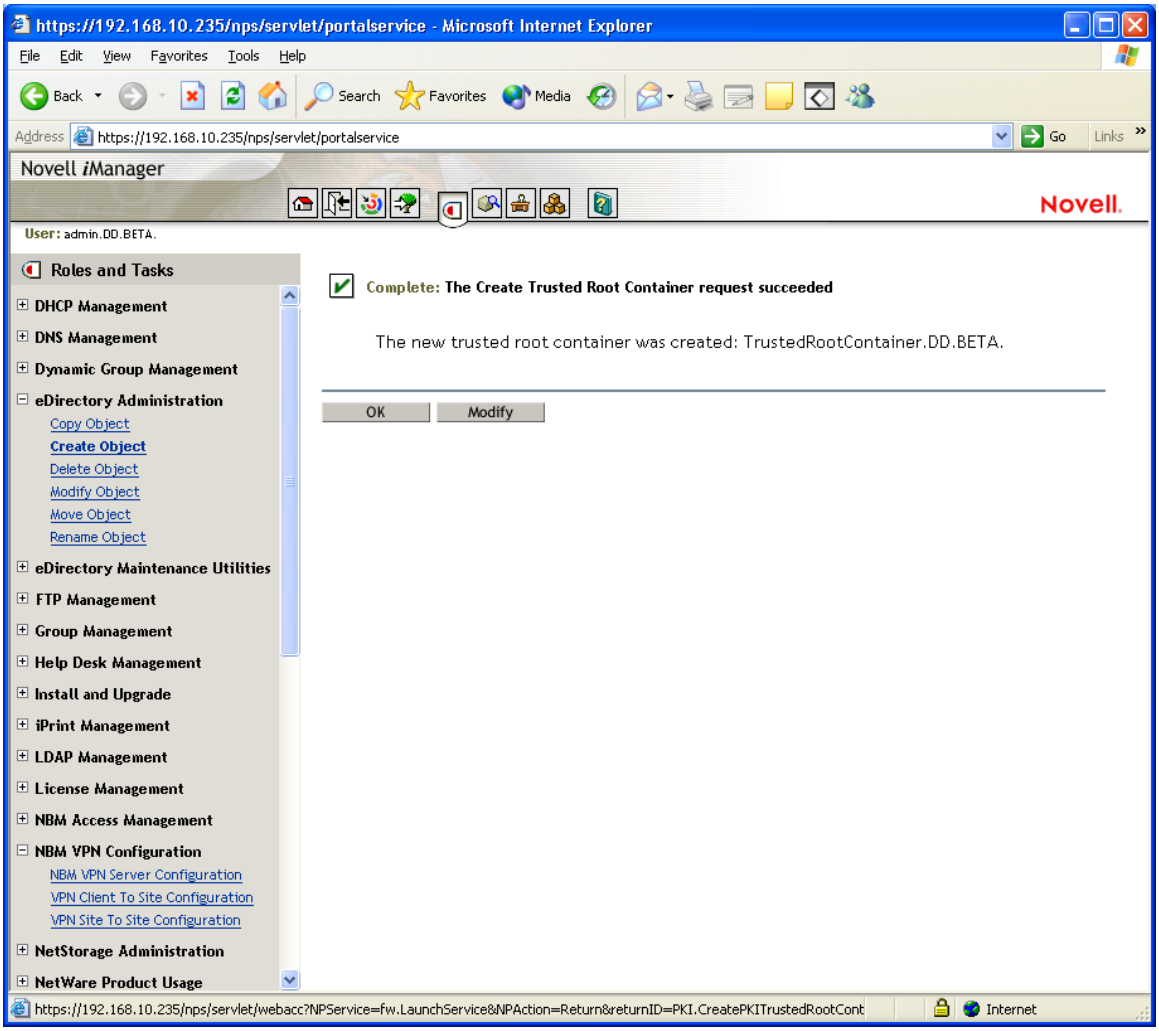


Give the container object a descriptive name, and **select the context** in which the context will be created. The context can be anywhere in your NDS tree, but is normally placed in, or near, the container holding the VPN server object.

In this example, the trusted root container was called **TrustedRootContainer**. (The default name created by iManager is TRC).

Click **OK** to create the **Trusted Root Container** (TRC) object.

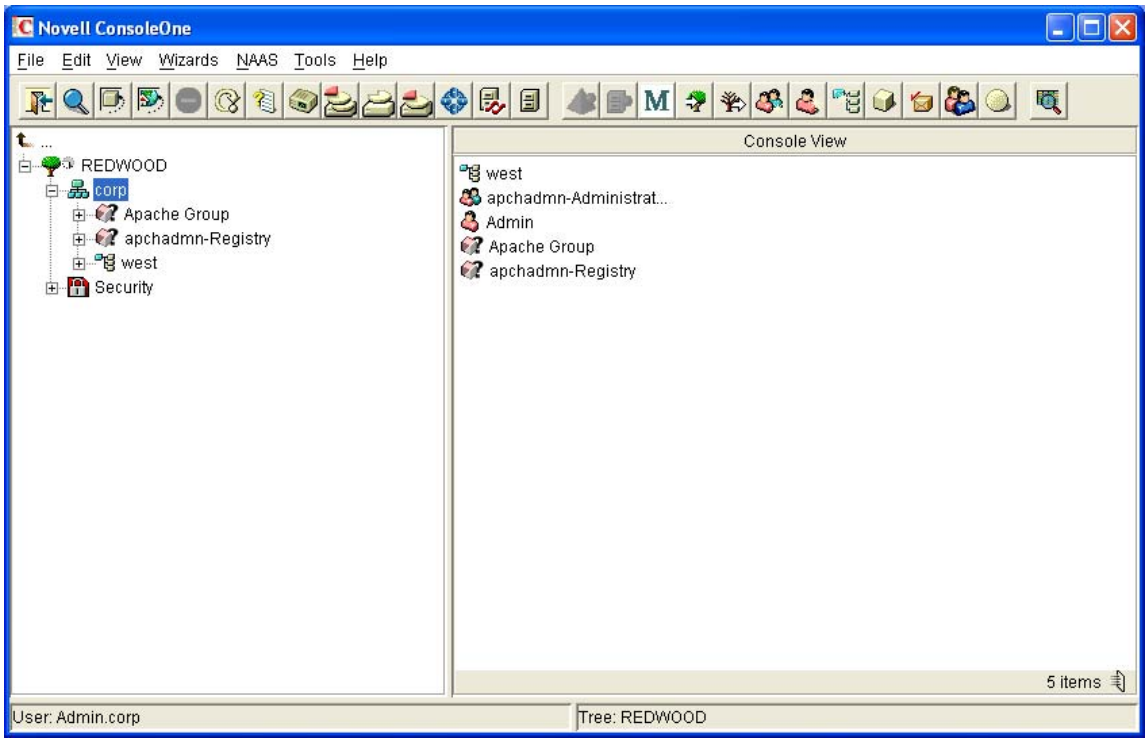
Note This example shows the creation of a TRC that was not used in the VPN example shown elsewhere in this chapter. The purpose of this section is simply to show the reader how the object can be created with iManager.



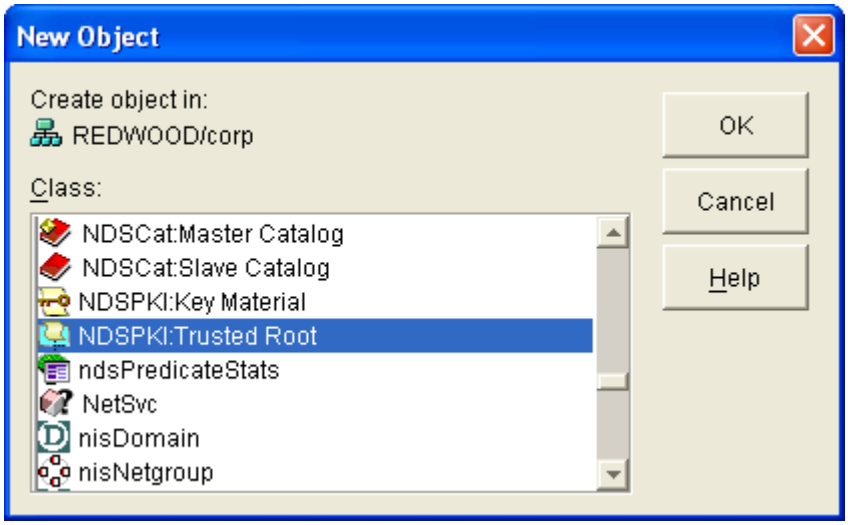
You should now see a successful completion dialog. Click on **OK.**

Using ConsoleOne

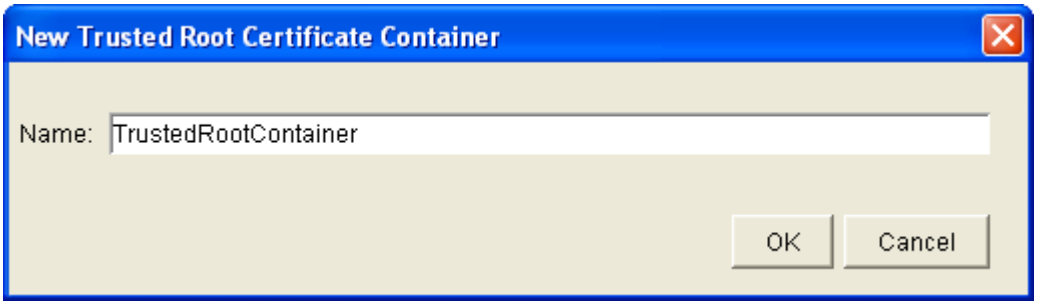
The procedure to add a Trusted Root Container in ConsoleOne is similar to iManager. Launch ConsoleOne, and browse to the NDS container where you wish to create a Trusted Root Container. The context can be anywhere in your NDS tree, but is normally placed in, or near, the container holding the VPN server object.



Click on the icon to add a new object, or press the Insert key.



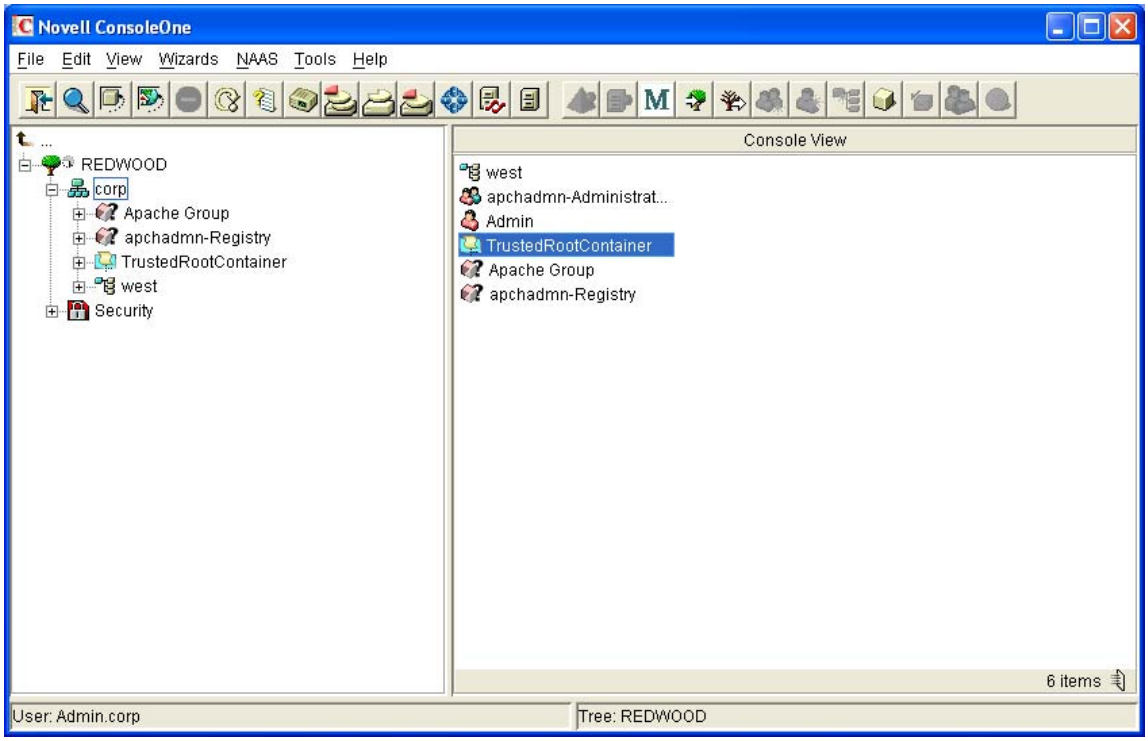
Select **NDSPKI:Trusted Root**, and click **OK**.



Type in a descriptive name for the TRC. In this example, the name is **TrustedRootContainer**.

Click **OK**.

Note This example shows the creation of a Trusted Root Container that was not used in the VPN example shown elsewhere in this chapter. The purpose of this section is simply to show the reader how the object can be created with ConsoleOne.



The Trusted Root Container, called **TrustedRootContainer** in this example, is created.

You can now place Trusted Root Objects in this container.

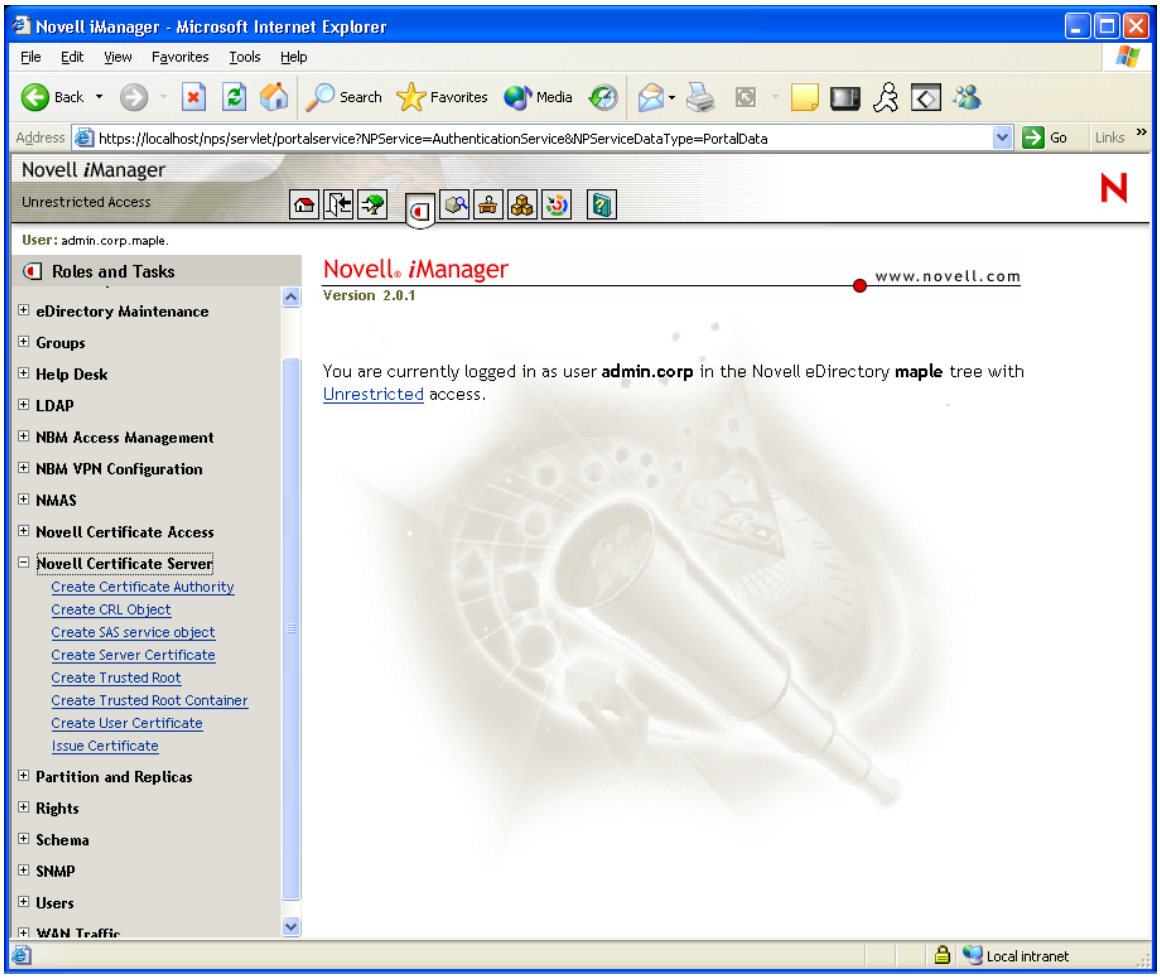
Manually Creating a VPN Server Certificate

This section shows two how to create a custom server certificate that can be used with BorderManager 3.8 Site-to-Site VPN. Both iManager and ConsoleOne methods are shown.

You normally would allow iManager to automatically create the VPN server certificates when you configure the VPN server. However, should you need to create VPN server certificates manually, follow the steps shown in either of the two examples.

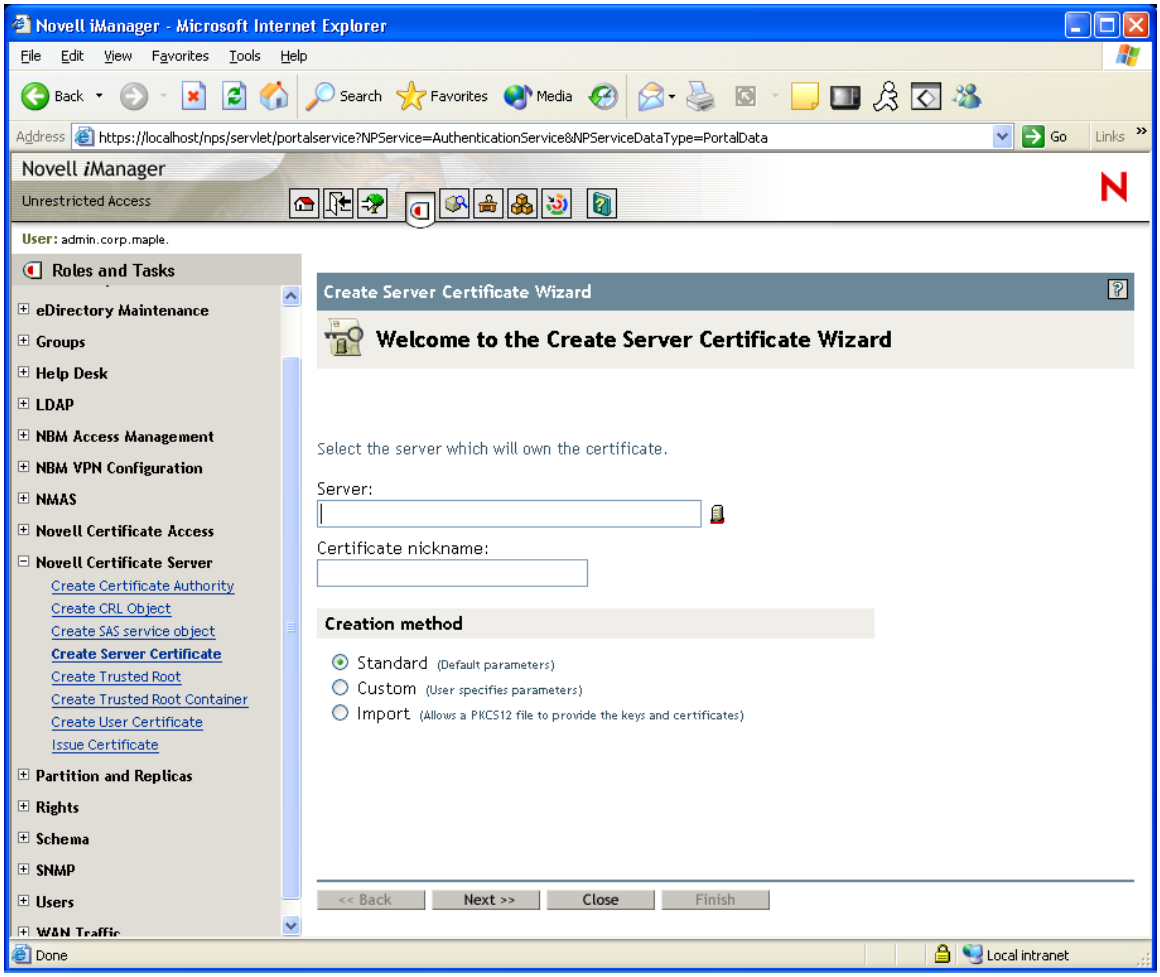
You cannot use a standard server certificate for VPN – the settings must be configured as shown in this chapter.

Using iManager



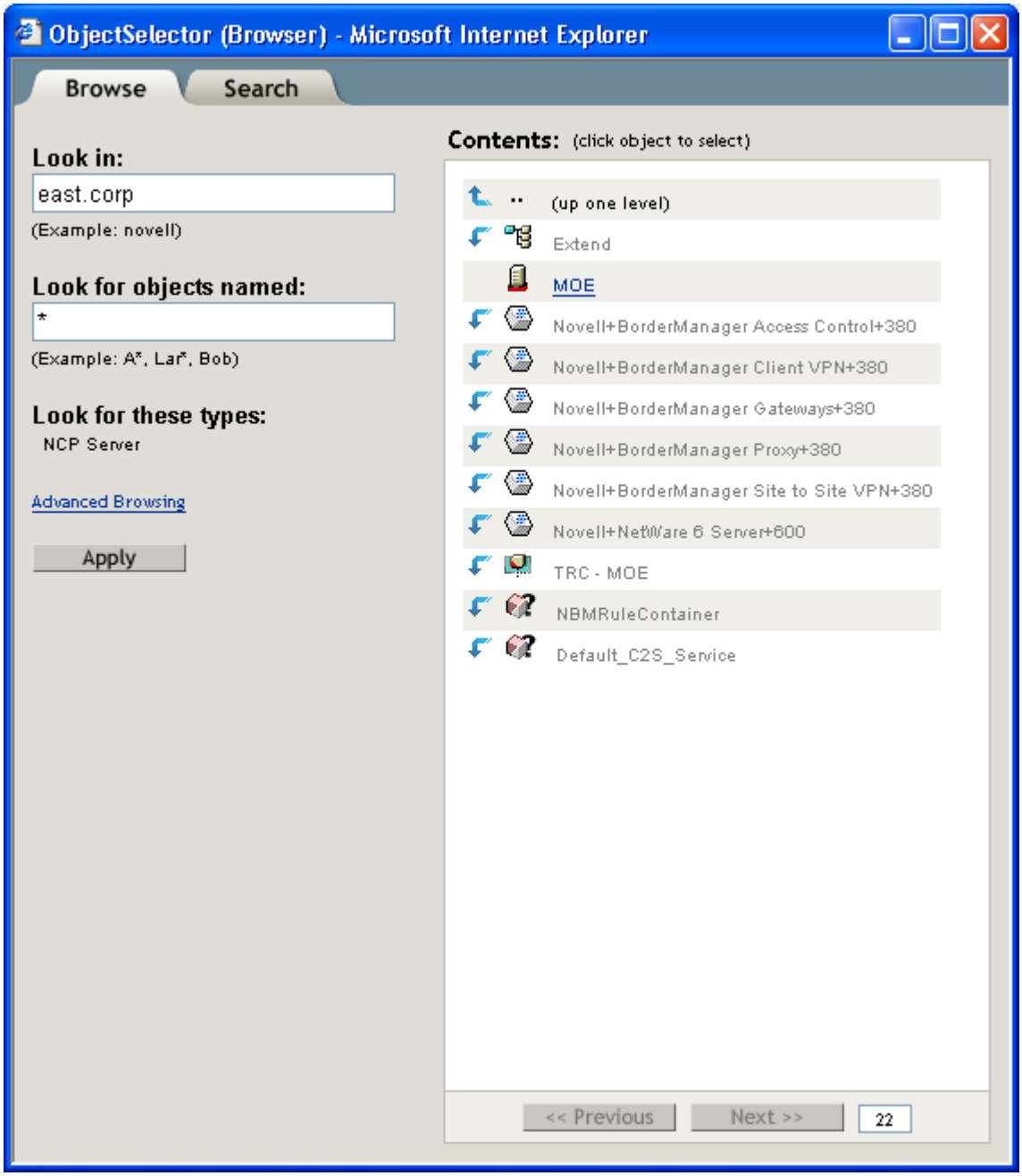
Log in to iManager 2.0 into the NDS tree where you want to create a VPN server certificate.

Expand the **Novell Certificate Server** link in the left panel. Click on **Create Server Certificate**.



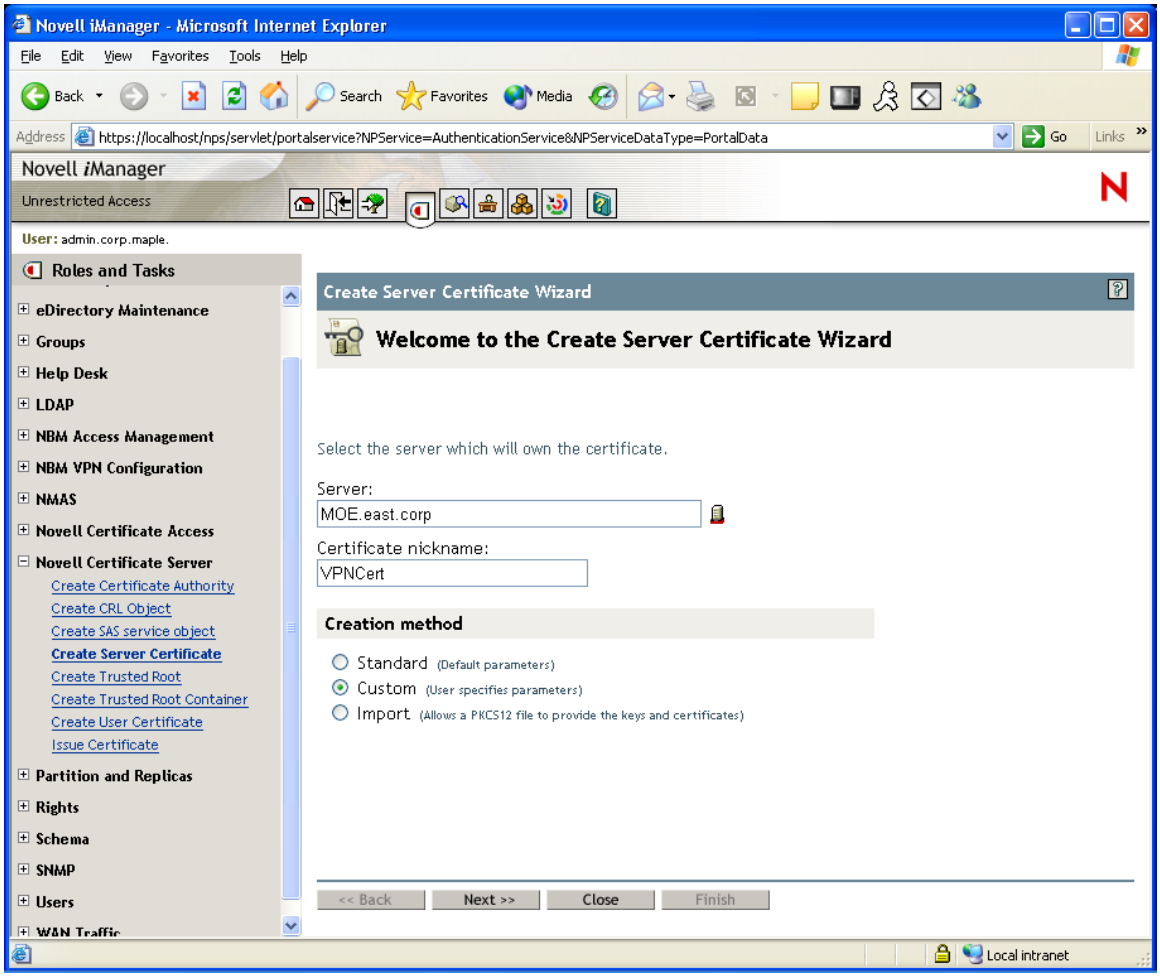
The **Create Server Certificate Wizard** appears.

Click on the server icon to the right of the Server field to browse to a server that will hold the certificate. This should be a server that you want to use as a VPN server.



Browse, or search, your NDS tree until you locate the server to hold the certificate. In this example, server **MOE** is to be used.

Click on the server to be used.

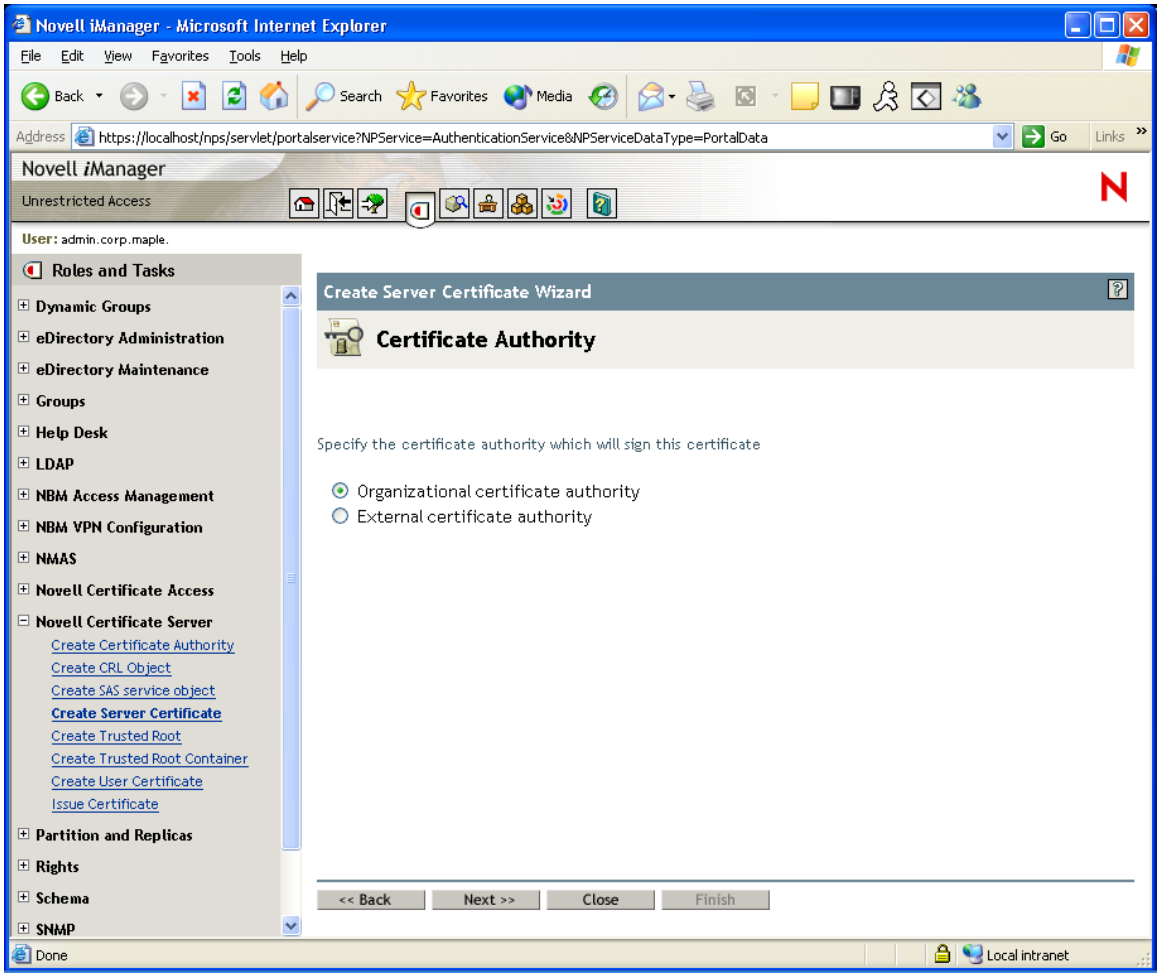


The server name is now filled in.

Enter a **descriptive NDS name** for the server certificate, in the **Certificate nickname** field. In this example, the name is set to **VPNCert**.

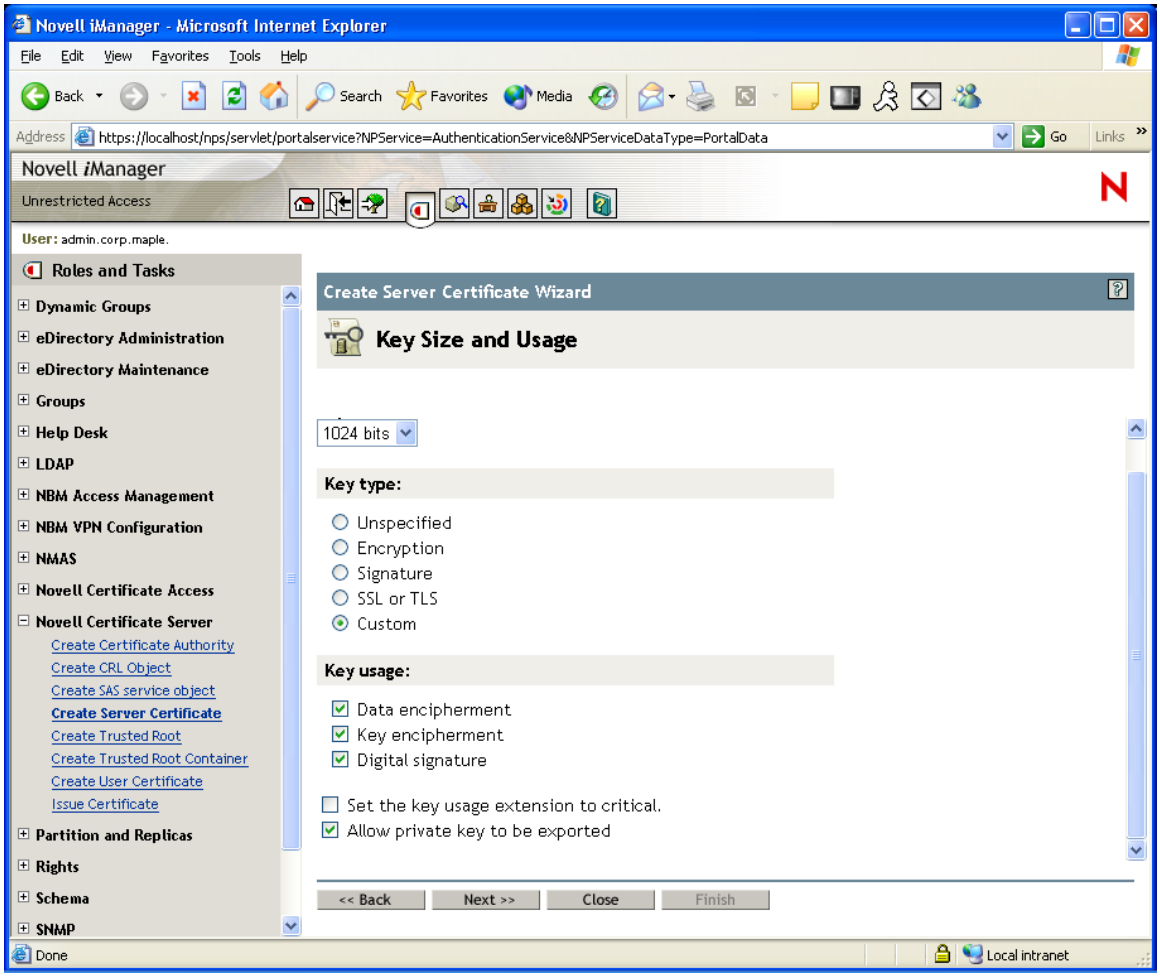
Choose **Custom** for the **Creation Method**.

Click **Next**.



Unless you have a reason to do otherwise, select the default value **Organizational Certificate Authority** for this certificate.

Click **Next**.



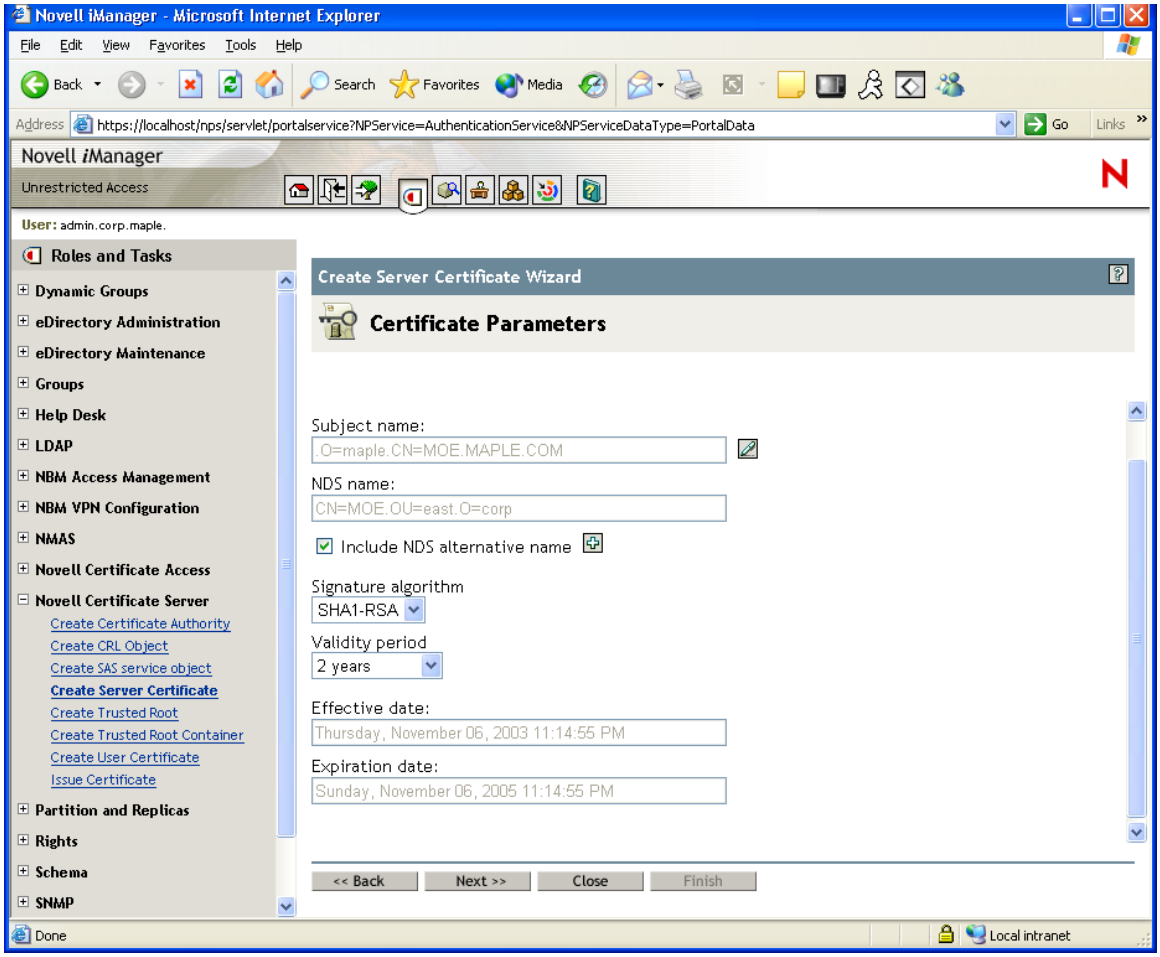
You must make several changes in the next menu.

Change the key size to **1024 bytes** in the drop-down menu.

Set the **Key Type** to **Custom**.

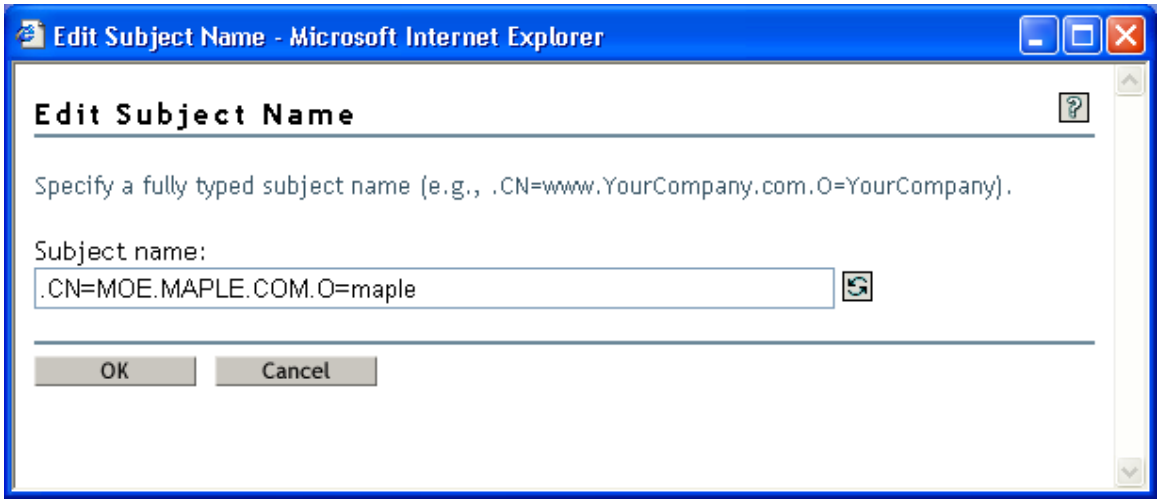
Check all three options under **Key usage**. (Enable **Data encipherment**, **Key encipherment** and **Digital signature**).

Click **Next**.



The Certificate Parameter menu appears. Again, a number of changes need to be made, although if you used the default values here, at least the certificate should work.

Click on the button to the right of the **subject name** field.

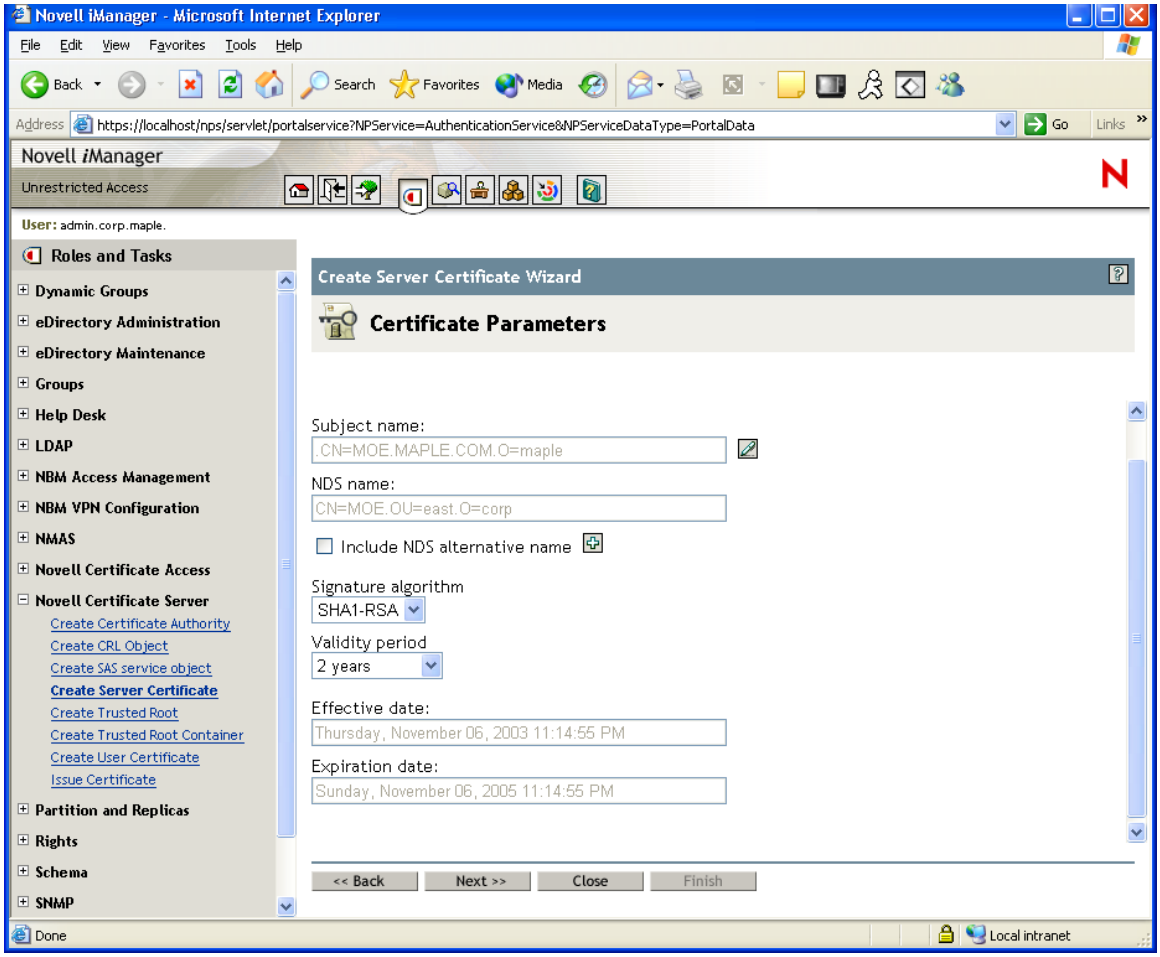


The subject name consists of an O and a CN entry. I like to reverse the order so that the CN comes first. This is just a cosmetic change, but it makes more sense to me to see the format in the usual NDS left-to-right manner.

You cannot simply type in any name you want, unfortunately. You can only reverse the O and CN entries. Click on the **arrow button** to the **right of the Subject name field**, and the subject name will be 'reversed'

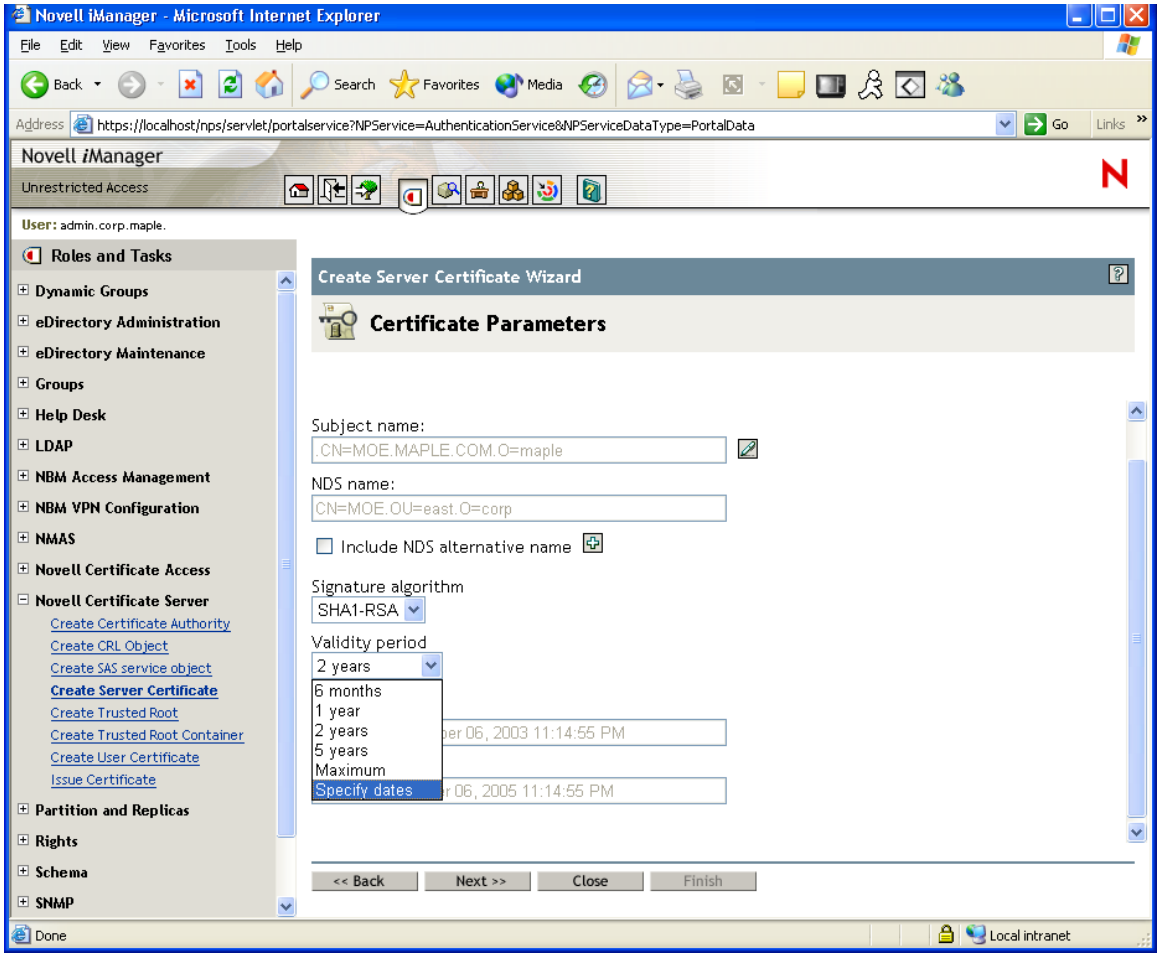
In this example, I wanted the subject name to end up as **CN=MOE.Maple.Com,O=maple**.

Click **OK**.

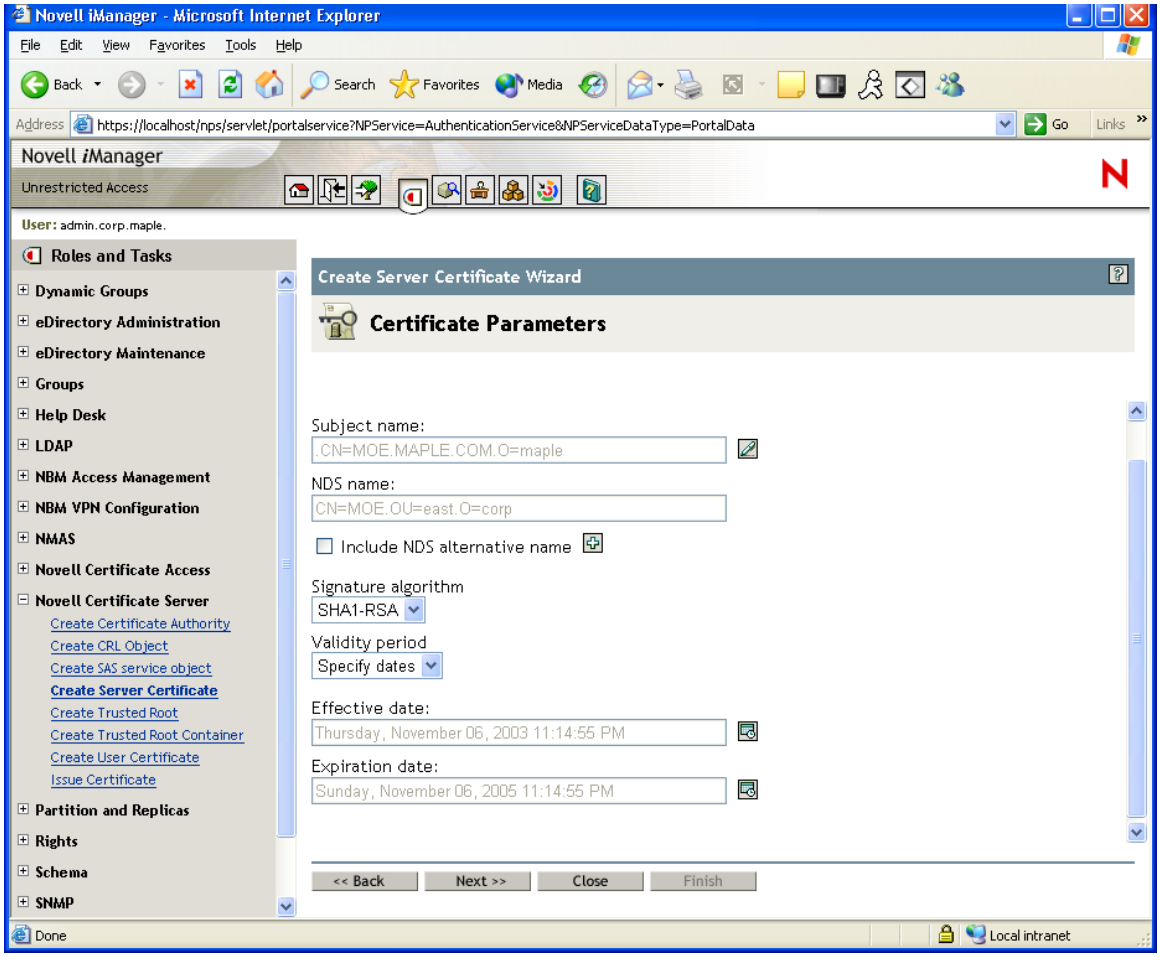


Next, **uncheck** the **Include NDS alternative name** field to **disable** that feature. That feature is not supported in BorderManager 3.8 VPN, and disabling it here will avoid a cosmetic error message from showing up in the VPN audit logs.

Now you need to change the **Validity period** from two years, to a specified value.



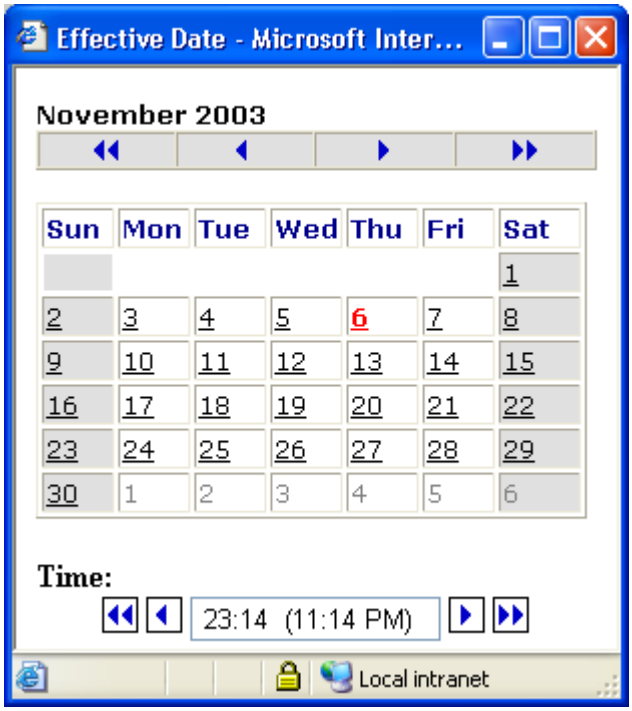
Click the drop-down menu in the **Validity Period** field, and just the value **Specify Dates**.



With **Specify Dates** selected, the fields for **Effective Date** (starting date) and Expiration Date become available for change.

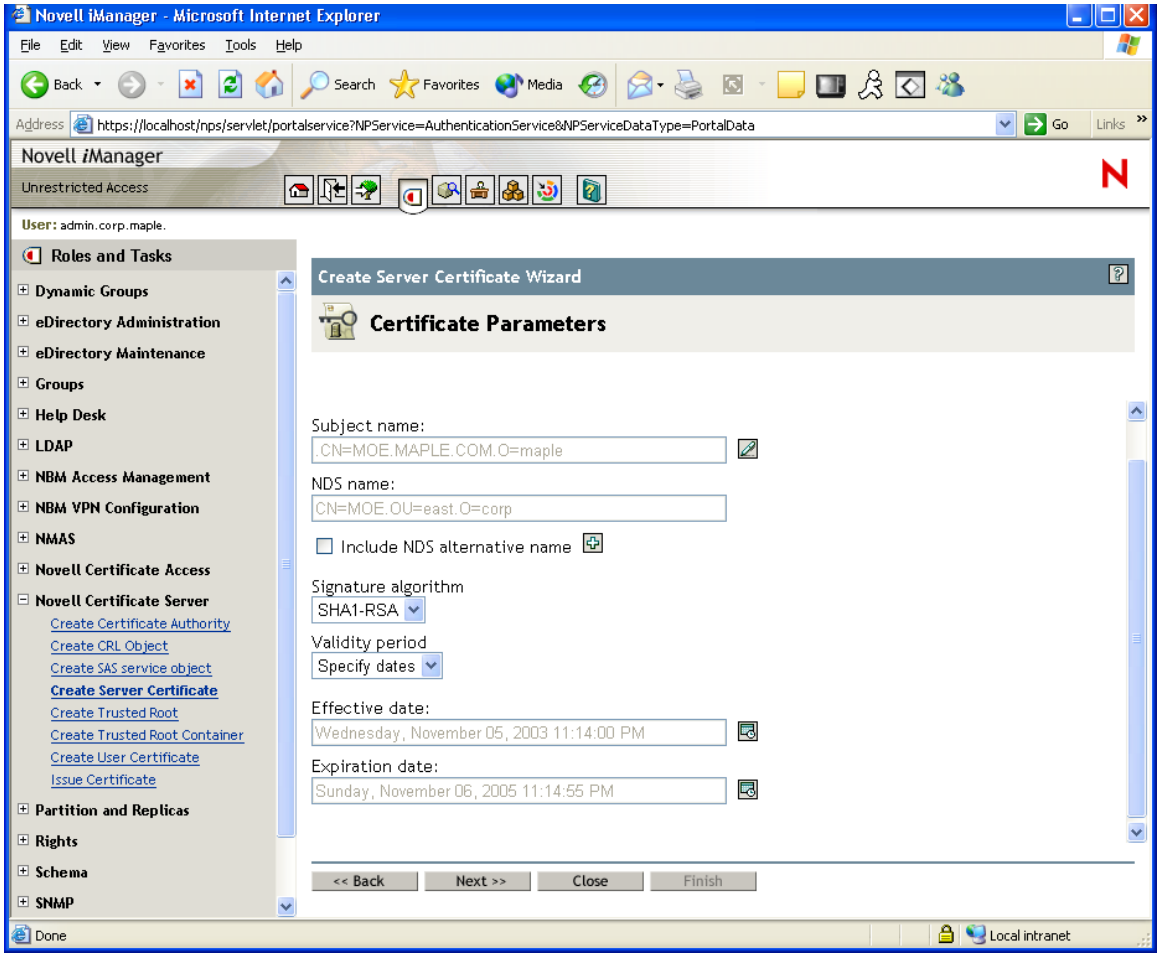
We want to change the starting date to yesterday, so that the certificate will be effective immediately upon creation. Otherwise, you may have to wait a few hours before the VPN will actually be able to use the certificate.

Click on the **icon** to the right of the **Effective Date** field.



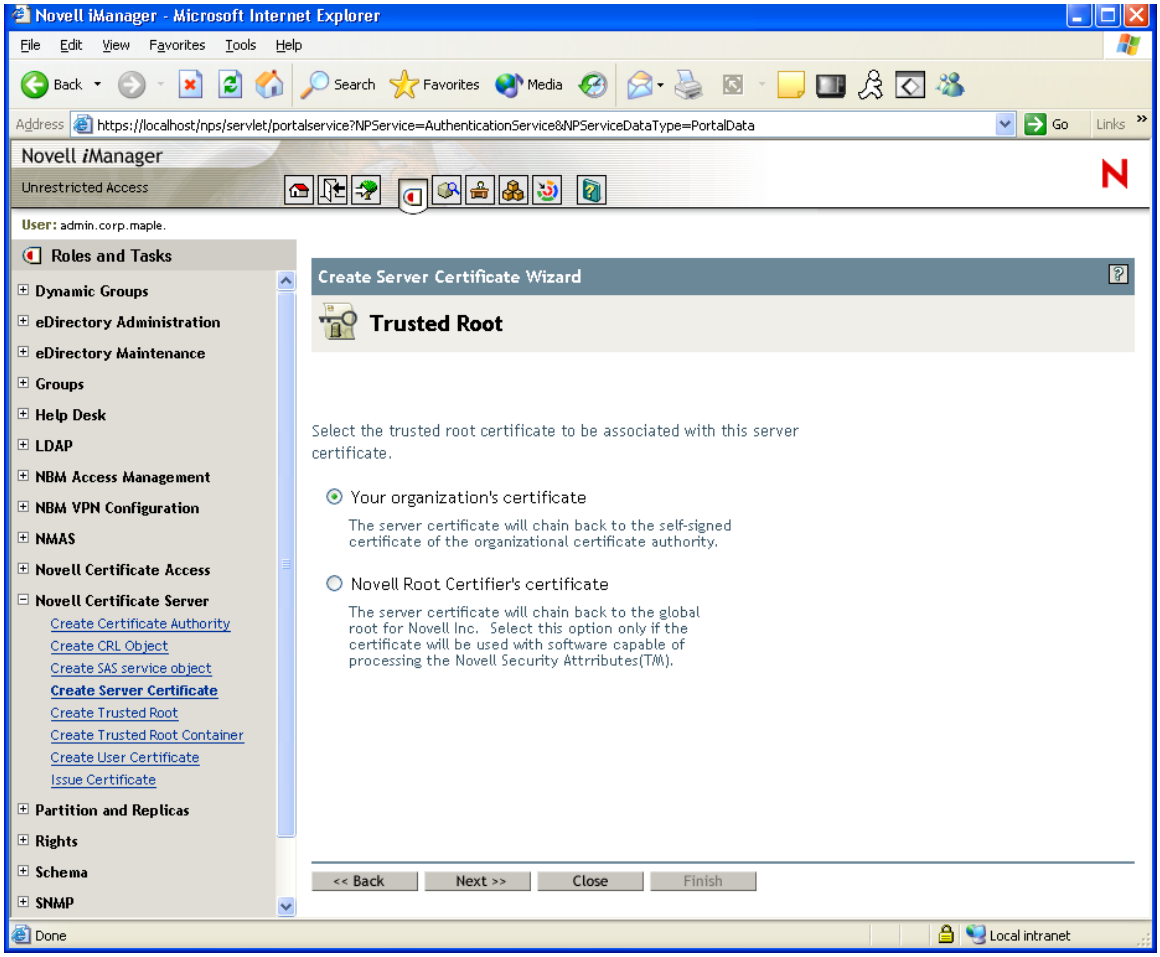
A calendar appears, with the current time and date selected.

Click on **yesterday's** date, to set the Effective Date to some time in the past, so that the certificate is already effective by date.



The certificate parameters now show the changed Subject Name, disabled Alternative NDS subject name, and an effective date slightly in the past.

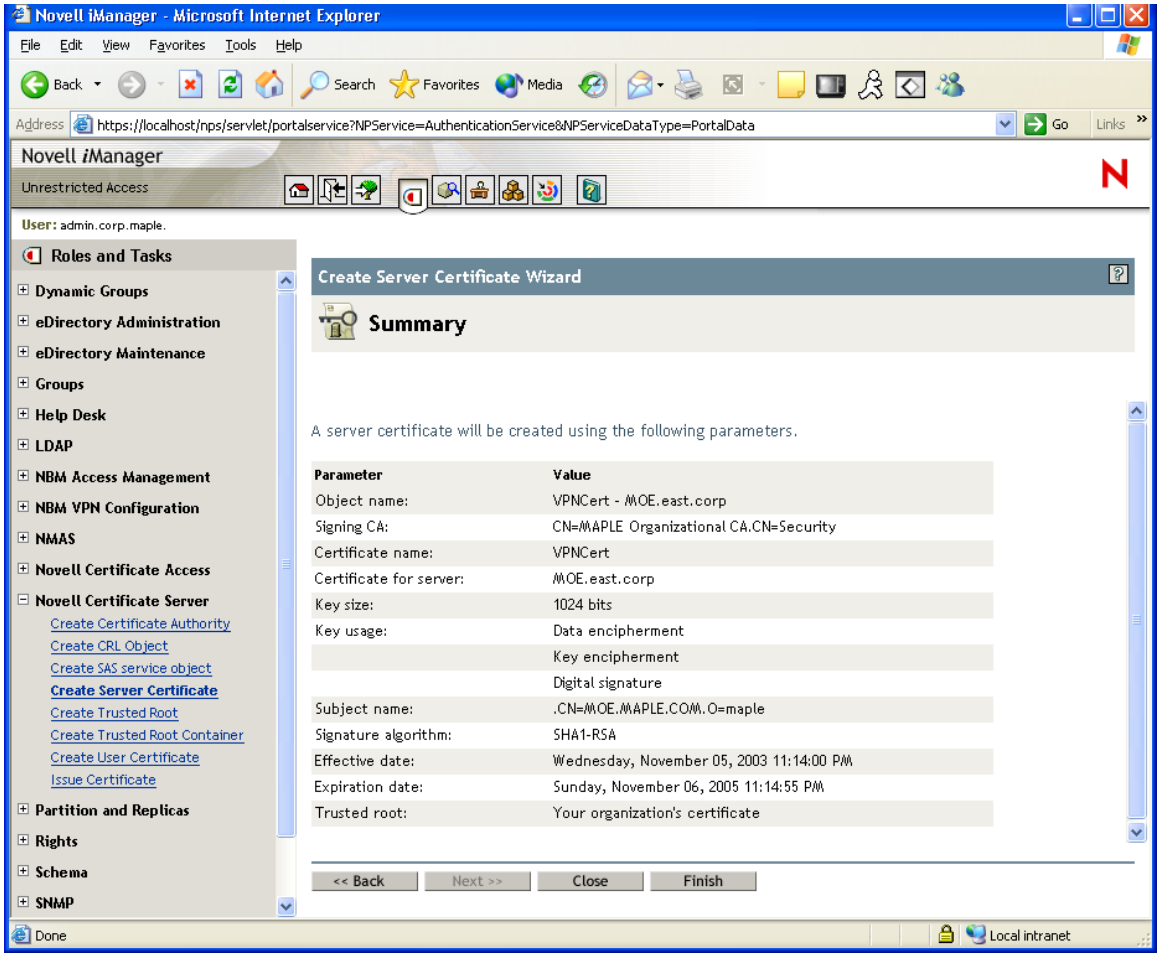
Click **Next**.



The **Trusted Root** menu appears.

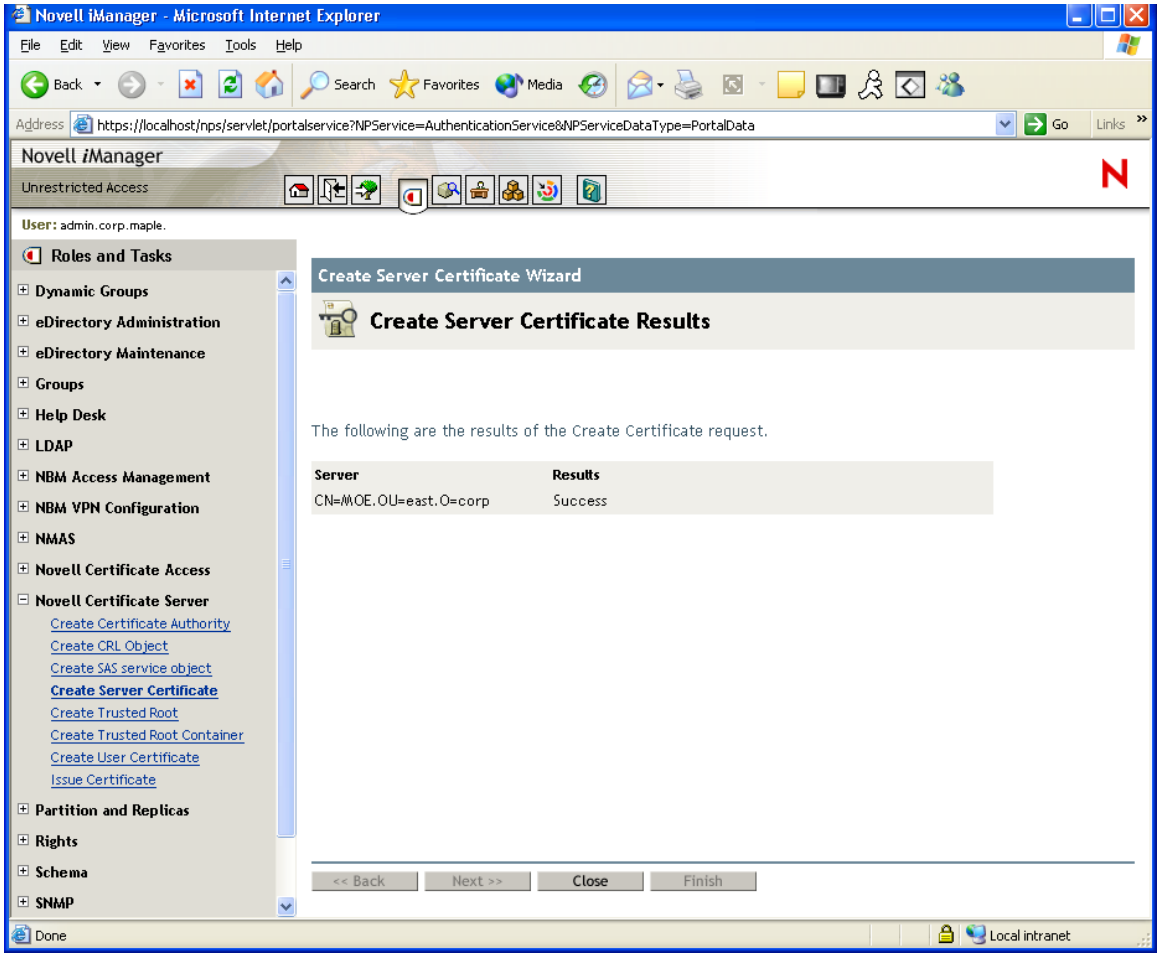
Leave the selection at the default value, **Your organization's certificate**.

Click **Next**.



A **Summary** menu screen appears.

Click **Finish** to create the VPN server certificate with the desired settings.



If all went well, the server certificate was created, and a successful result is seen.

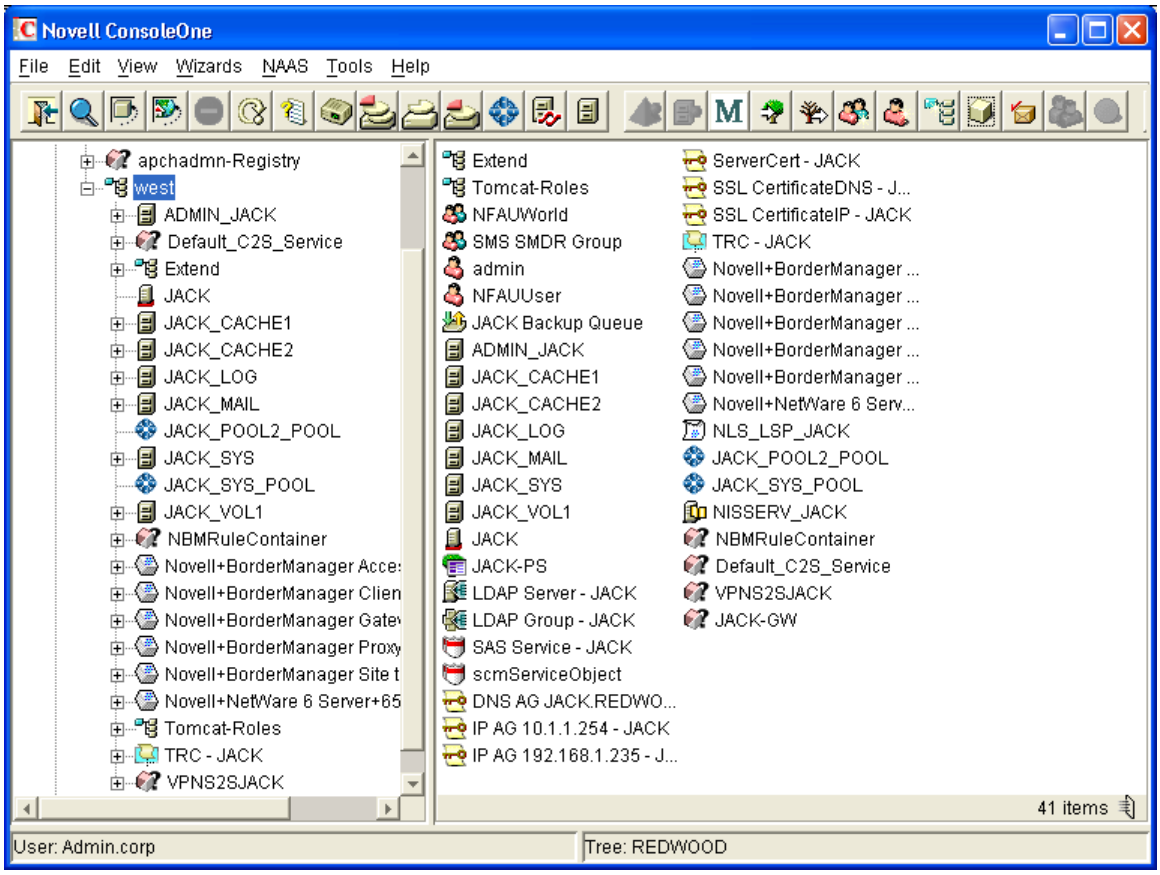
Click **Close**.

Using ConsoleOne

This section shows how to use ConsoleOne to create a custom server certificate that can be used with BorderManager 3.8 Site-to-Site VPN.

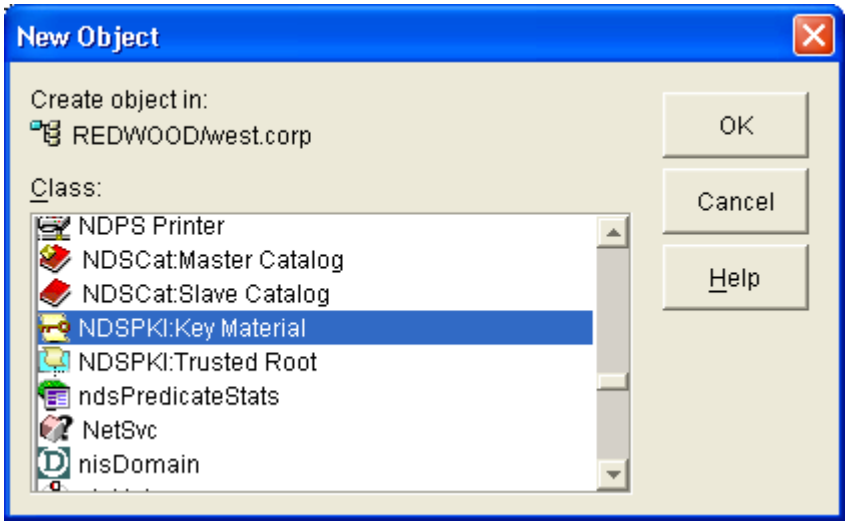
Launch ConsoleOne from the BorderManager 3.8 server. If you have any error messages about security-related snapins, you may need to download and install a newer version of NICI from Novell to your PC.

In this example, a custom VPN certificate is created for the NetWare 6.5 server JACK.

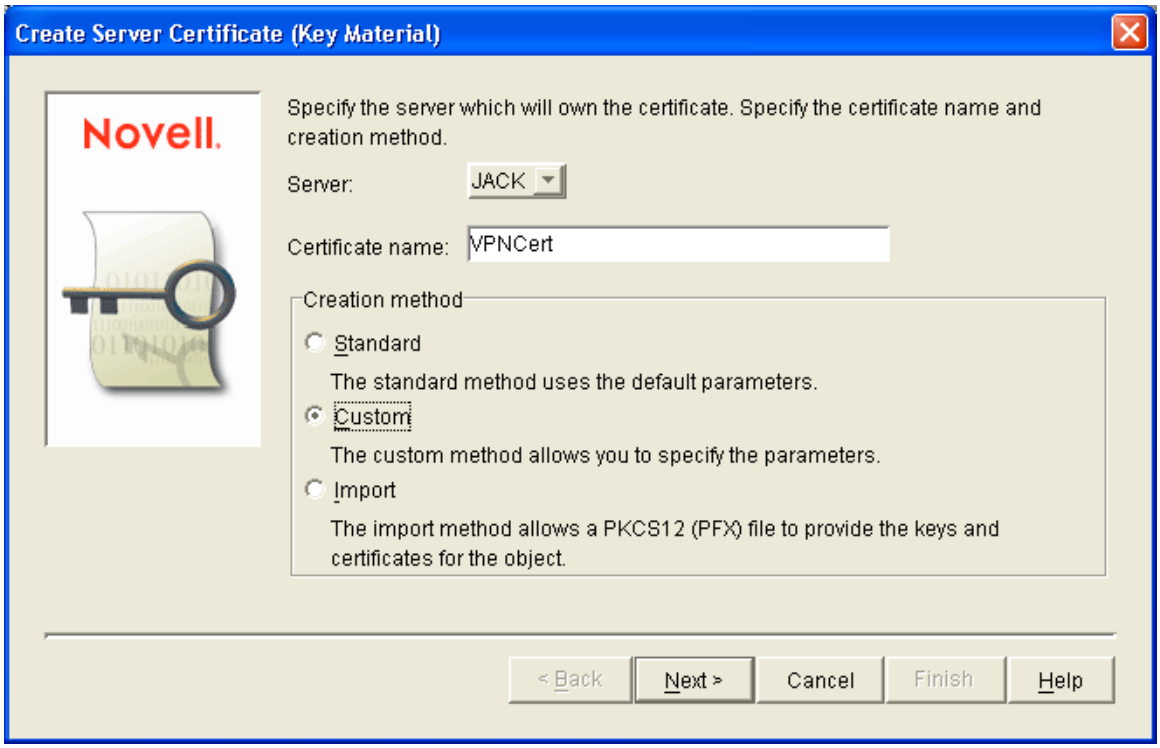


In ConsoleOne, go to the NDS container holding the VPN server.

Click on the icon to create a new object, or press the Insert key.



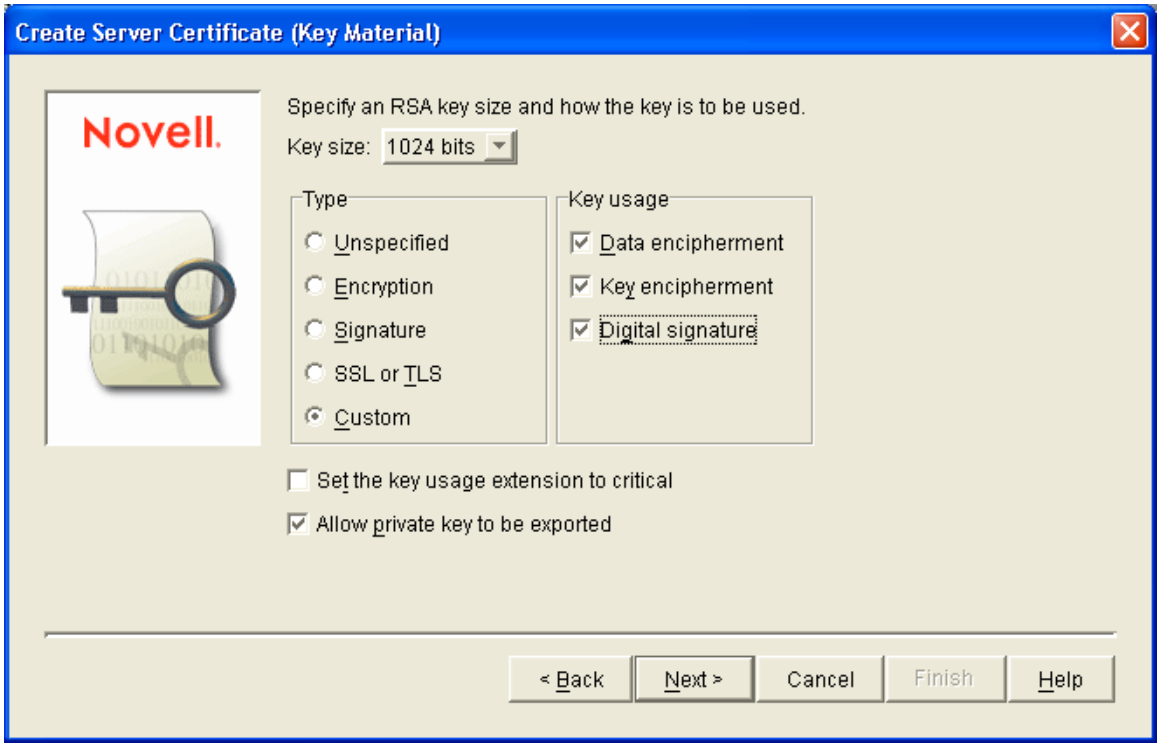
Choose **NDSPKI: Key Material** to create a certificate, and click **OK**.



You will need to create a Custom certificate. A standard certificate will not work. Select **Custom**, and type in a descriptive Certificate Name. In this example, the name **VPNCert** is used. Click **Next**.

Unless you want to use an external certificate authority, select the **Organization certificate authority**.

Click **Next**.



You will have to make a number of changes to the menu that comes up next.

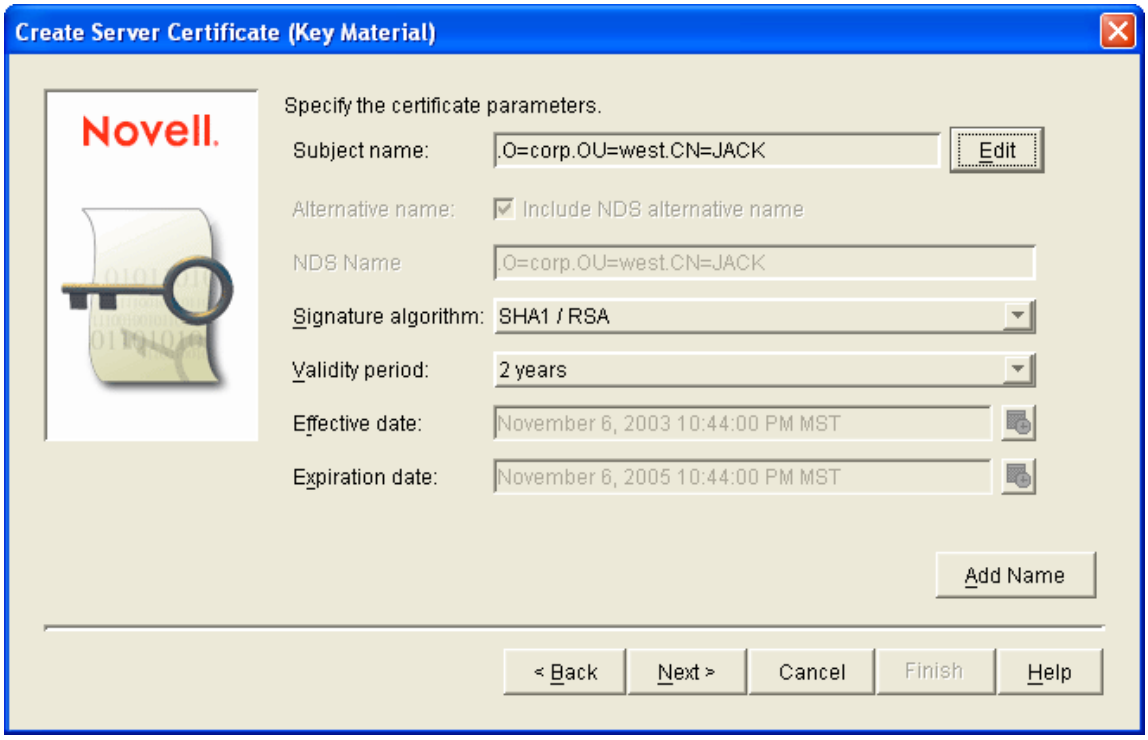
The **Key size** needs to be changed to **1024 bits**.

The **Type** needs to be set to **Custom**.

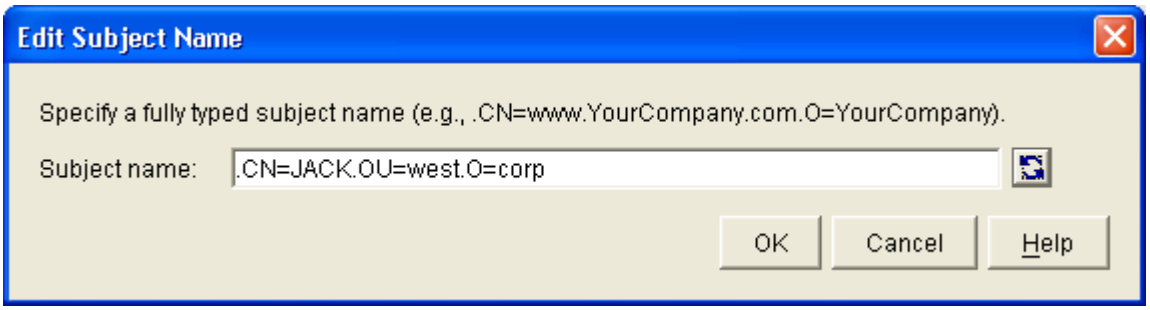
All the **Key Usage** fields need to be checked – that is, enable **Data encipherment**, **Key encipherment** and **Digital Signature**.

You can leave the other fields at default values.

Click **Next** to continue.



On the next menu, you could actually leave the default settings, but they may cause some issues if you are trying to get the VPN up immediately. I recommend changing the **Subject name** (slightly, for a 'more standard' appearance), and the **Effective Date**, so that the certificate will be applicable immediately.

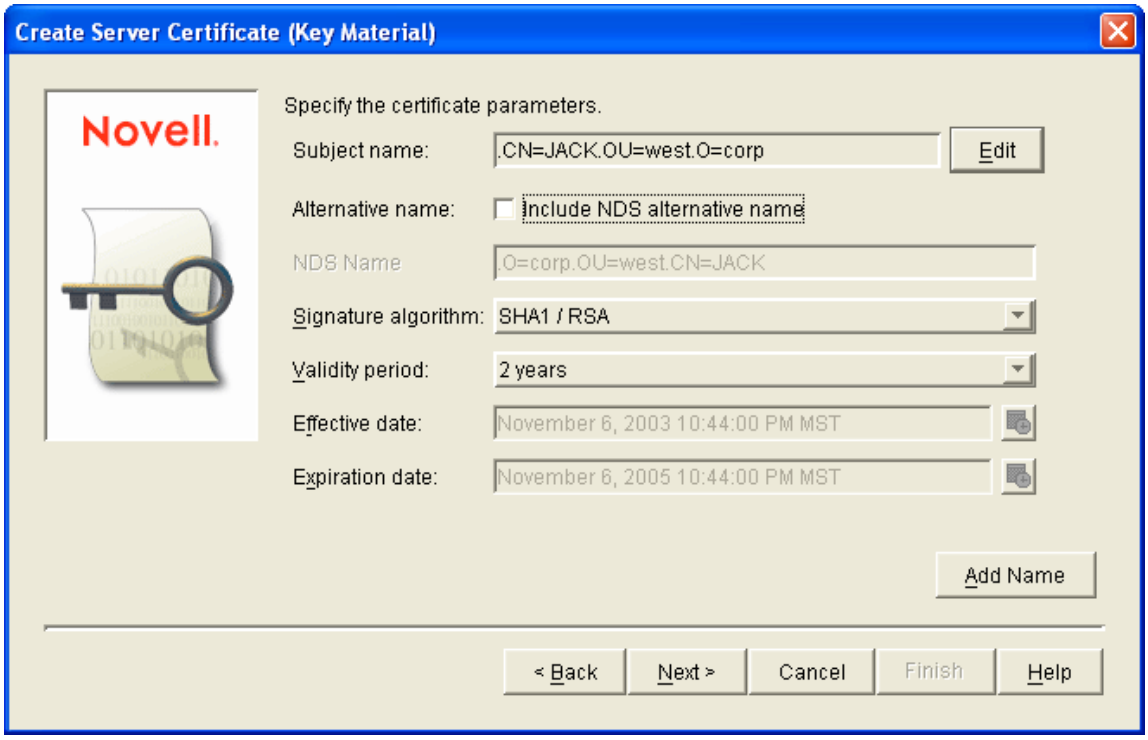


Click on the **Edit** tab next to the **Subject Name** field.

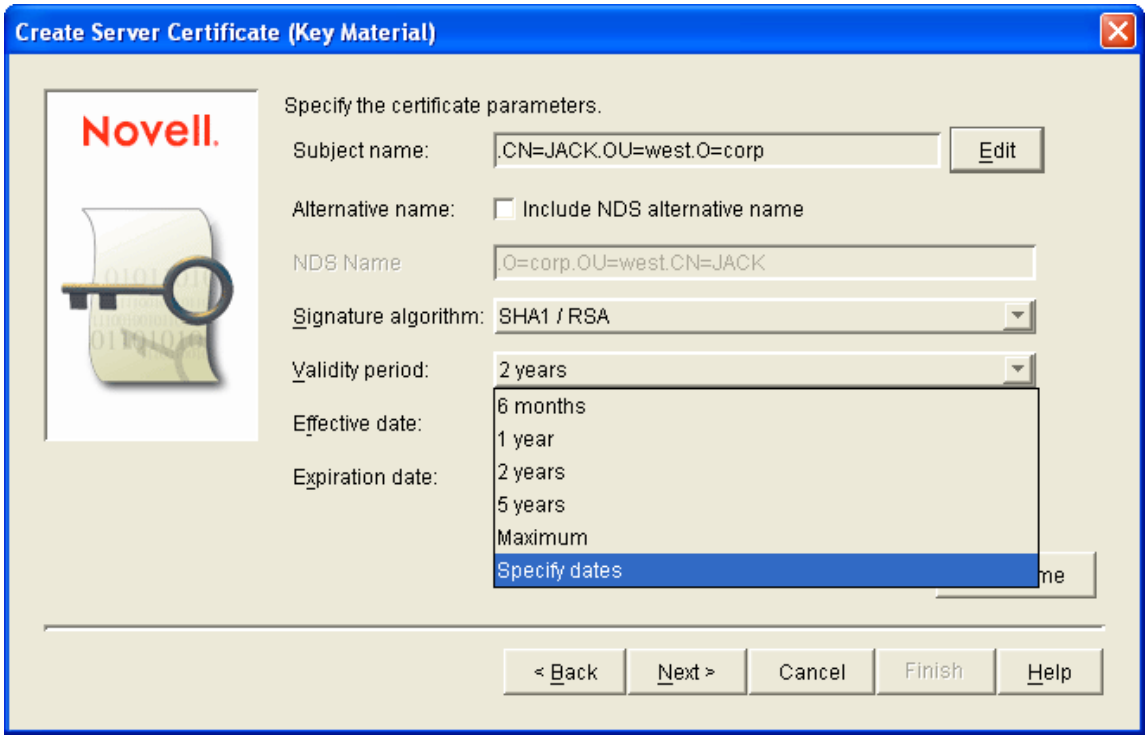
The only change to be made here is to reverse the CN and O entries. (You should not try to type in another name). Simply click once on the arrow button to the right of the Subject Name field, and the existing entry should be re-ordered so that the CN comes first.

This is essentially a cosmetic change, but I think it is easier to remember when having to type in the subject name.

Then click **OK**.



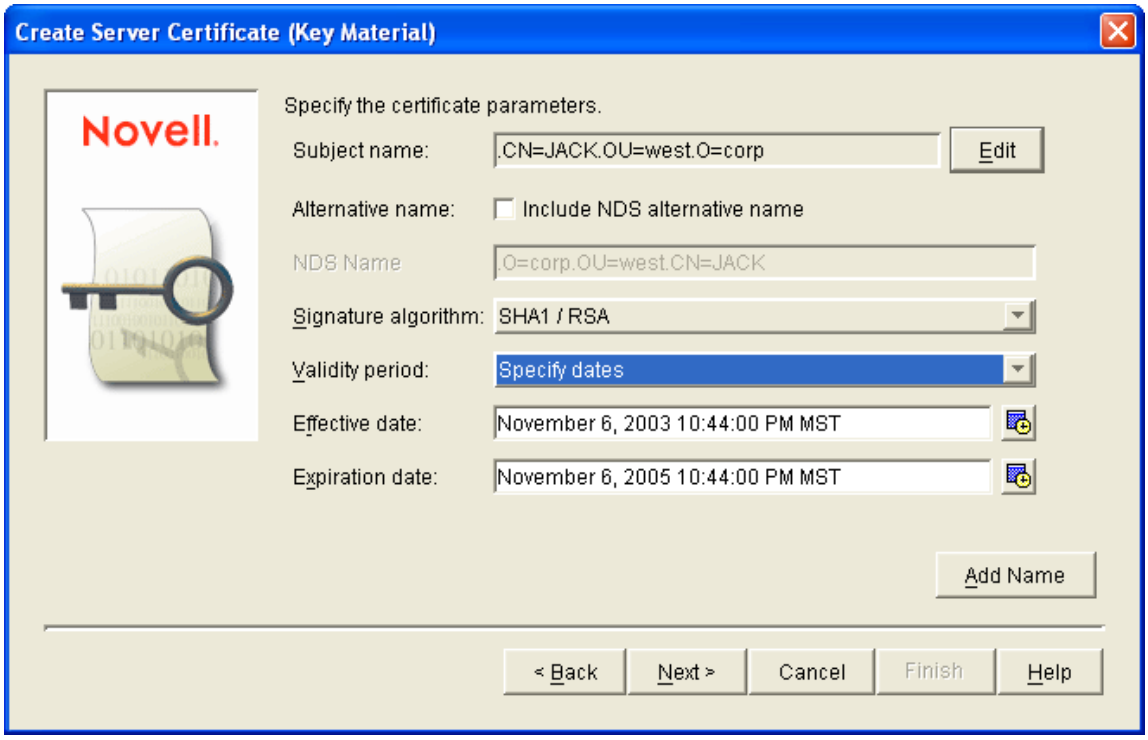
Next, **uncheck** the option to **Include NDS alternative name**. You do not want to include the alternative name.



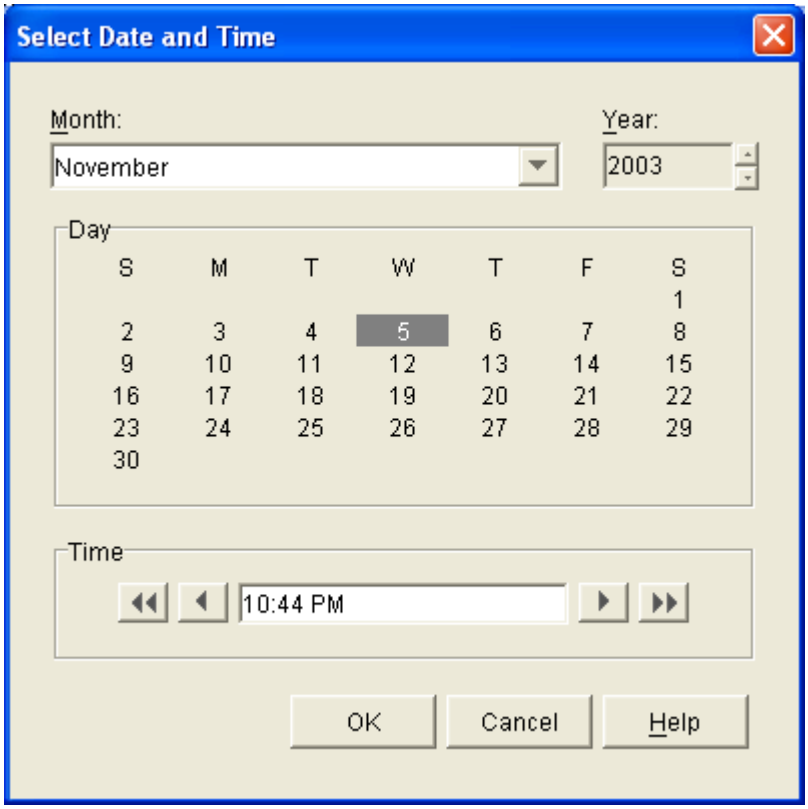
The next step is necessary to have the certificate be valid immediately, or you may have to wait several hours before it can be used. You need to change the start date to yesterday's date. (You can make the end date as late as you desire.)

Click on the **Validity period** to show the drop-down menu.

Select the option to **Specify Dates**.



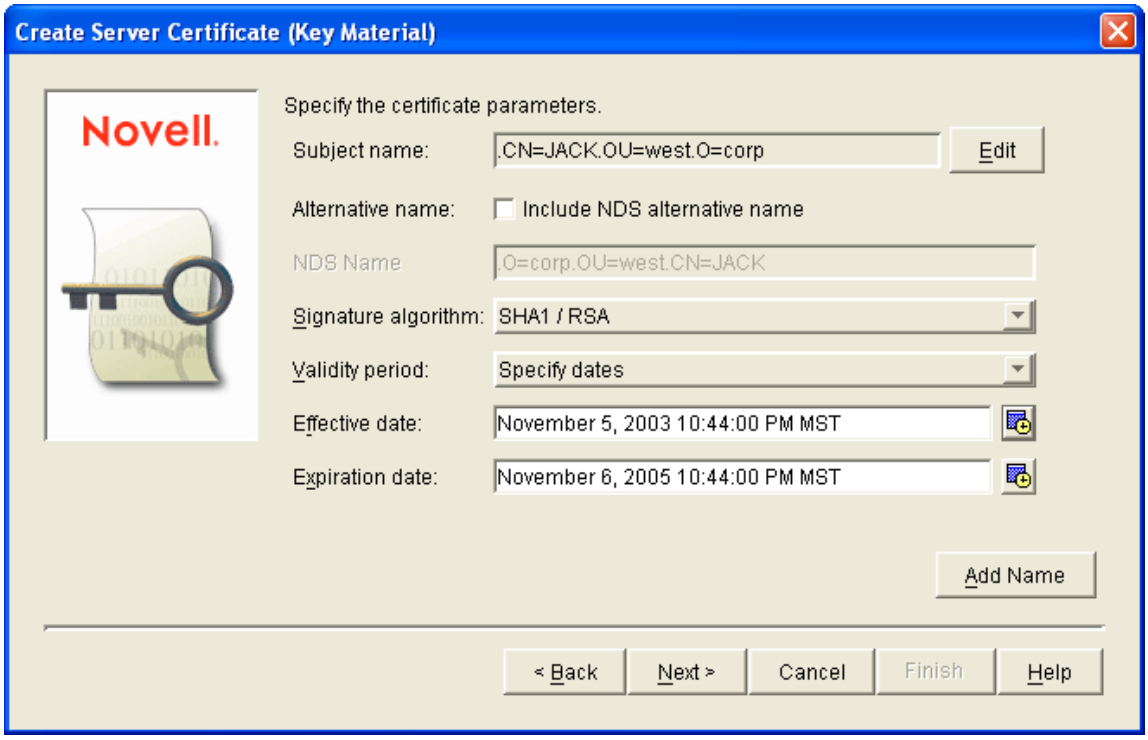
Then select the button to the right of the **Effective Date** field to set the starting date.



A calendar will appear. Select yesterday's date. In the example above, the time was 10:44pm on November 6th, 2003. I chose an effective date of November 5th by clicking on the 5.

Click on a date that is **earlier than the current date**.

Click **OK**.

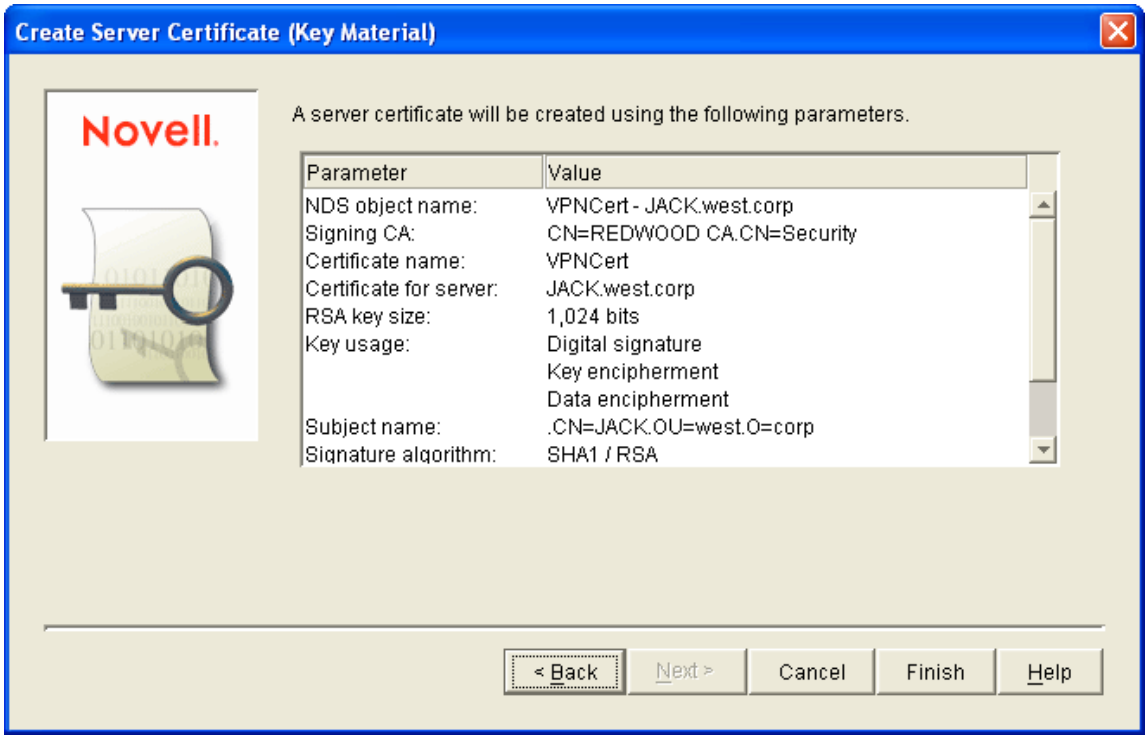


You should now see a menu filled in with the altered subject name, and dates that are effective from yesterday to some period of time in the future. Include NDS alternative name is not enabled.

Click **Next**.

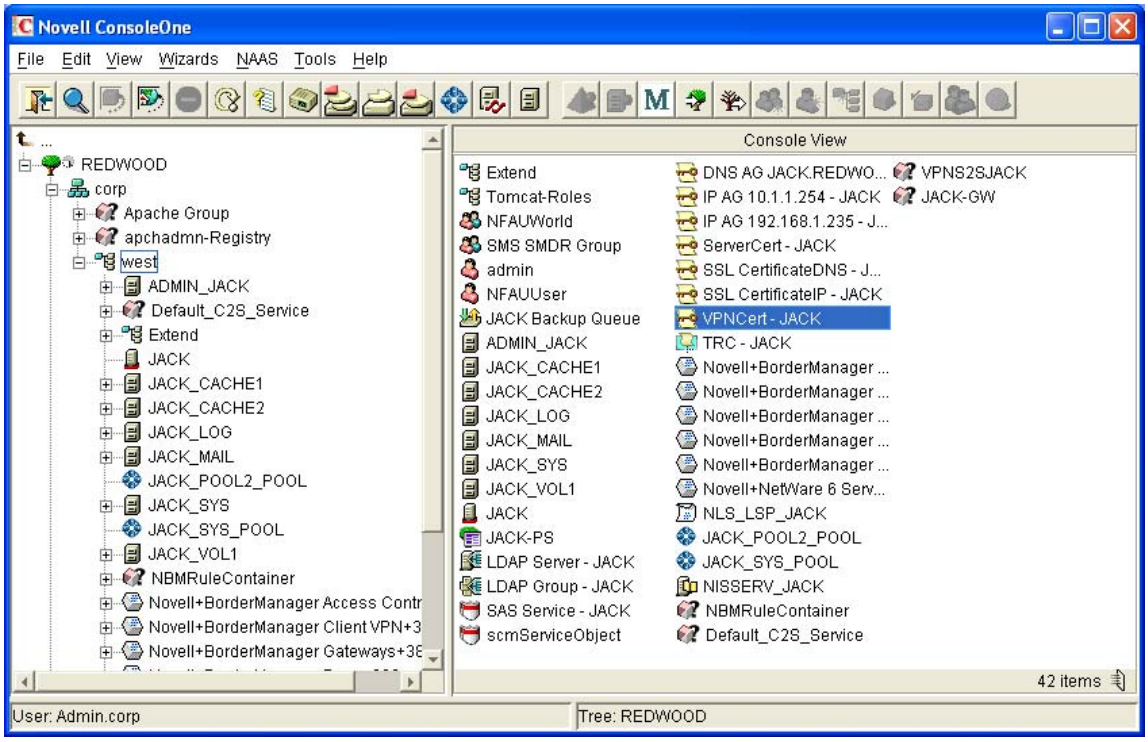
Use the **default value** of **Your organization's certificate** to specify your organization's certificate for **the trusted root certificate associated with this server certificate**.

Click **Next**.



You will see a summary screen of your settings.

Click **Finish**.



Your new server certificate should now appear in the same NDS container as the VPN server. The server's name will be appended to the end of the name that you chose for the certificate.

<This page intentionally left blank. This is to facilitate putting in chapter tabs in a ring binder for double-sided printing. The main chapters should start on an odd-numbered page.>

Chapter 20 - BorderManager 3.8 Client-to-Site VPN

In order to configure Client-to-Site VPN, you must first have configured the server as a VPN server.

Unlike previous versions of BorderManager, you have many more options to configure with BorderManager 3.8. The server can be located behind a static NAT or port forwarding router. You can specify different methods of authentication. You can specify particular protocols to allow, and you can allow those protocols to be sent over the VPN or not sent over the VPN. Perhaps best of all, you can specify IP addresses to be pushed to the remote client, which eliminates most of the routing issues inherent to previous versions of BorderManager Client-to-Site VPN. You can also push DNS server addresses and SLP Directory Agent addresses as well, greatly simplifying name resolution issues.

However, all of these options increase the complexity of the system configuration. If you want to make things as simple as possible, configure NMAS authentication method, allow and encrypt all protocols to all internal addresses, and push a range of private IP addresses to the clients. Certificate authentication method will allow a much wider range of potential clients (meaning non-Novell VPN clients), but takes more work to configure. Preshared secret (PSS) mode can also be used with a wide range of VPN clients, but is really intended only for testing for Client-to-Site VPN.

The following example will show a VPN configured to allow NMAS authentication (using NDS password) and Certificate authentication. Traffic will be restricted to both particular destinations and particular protocols. Only the Novell VPN client will be shown – non-Novell VPN clients are beyond the scope of this book.

Quick Summary

- You must have iManager 2.0 installed, with the BorderManager 3.8 snapins. You cannot administer BorderManager 3.8 VPN with any other tool. If BorderManager 3.8 is installed on NetWare 6.5, this should happen by default. Otherwise, install iManager 2.0 on the

local workstation, from the Companion CD. You can also install iManager 2.0.1 from the Companion CD to a NetWare 6.0 server.

- Create a Certificate for the server using the public IP address of the server in the Certificate subject name.
- Create a trusted root container in the same OU as the server.
- Create a trusted root object in the trusted root container, from the ROOTCERT.DER file.
- Create a VPN server.
- Create a VPN Client-to-Site Profile, in the VPN server's NDS container.
- Assign the VPN Client-to-Site Profile to the VPN server.
- Many of the above options will be created for you automatically in iManager if you accept default values.

Limitations

As of this writing (BorderManager 3.8sp1a released), I have found the following limitations. You should look at them closely, as some of them are surprising, and some are severely limiting.

NDS Context

- You must create the Client-to-Site service in the same context as the VPN server. Unless you happen to be in that context, changing to the context is not obvious. In iManager, you have to type in the correct context and click the Update List button. If you see a Default_C2S_Service show up, you should be in the correct container.

Traffic Rule Limitations

- If you are authenticated via Certificate, you can only make use of individual certificate user entries for subject name, or 'All Users'.
- In the Define Services section of Traffic Rules, you cannot enter more than four digits as a port number, meaning that you cannot allow/restrict on common iFolder or Netstorage ports like 51080 or 52080.
- You can only specify port numbers for TCP protocol in Traffic Rules.

Authentication Rule Limitations

- When using NMAS authentication, leave the minimum allowed authentication grade as 'Logged'. Other settings may not work.

LDAP Configuration

- LDAP authentication did not work for me over port forwarding, but is supposed to work over NAT.
- I have seen a number of cases where my changes related to LDAP did not seem to work, until I used the command STOPVPN and STARTVPN on the VPN server. Of course this takes down Site-to-Site VPN temporarily, and so it is not advisable to do. Perhaps if I waited for some longer period of time, the changes would have taken affect.
- In my testing, I found LDAP authentication to be case-sensitive for both user name and password.

DNS/SLP Configuration Limitations

- Pushing the DNS and SLP addresses to Windows 2000 and XP clients requires the user logged into Windows to be at least a Power User.
- Pushing the SLP addresses to remote clients requires Client32 4.90 or later.

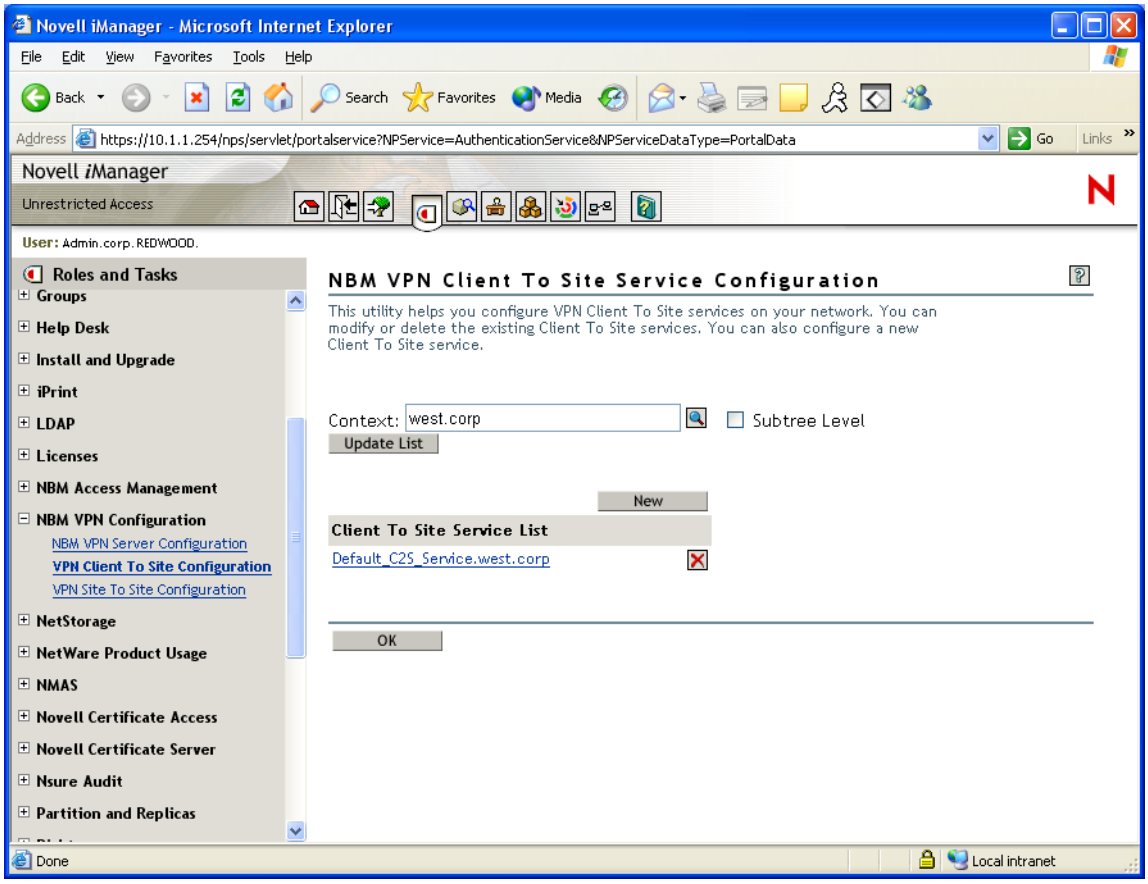
Configure A Server for Client-to-Site VPN

In the example shown below, the server has already been configured as a VPN server, as shown in the Site-to-Site VPN chapter.

Configure General Parameters

Use iManager 2.0 to select a BorderManager 3.8 server and configure it for Client-to-Site (C2S) service.

Log in to iManager in the VPN server's NDS tree.



Expand **NBM VPN Configuration**, and select **VPN Client To Site Configuration**.

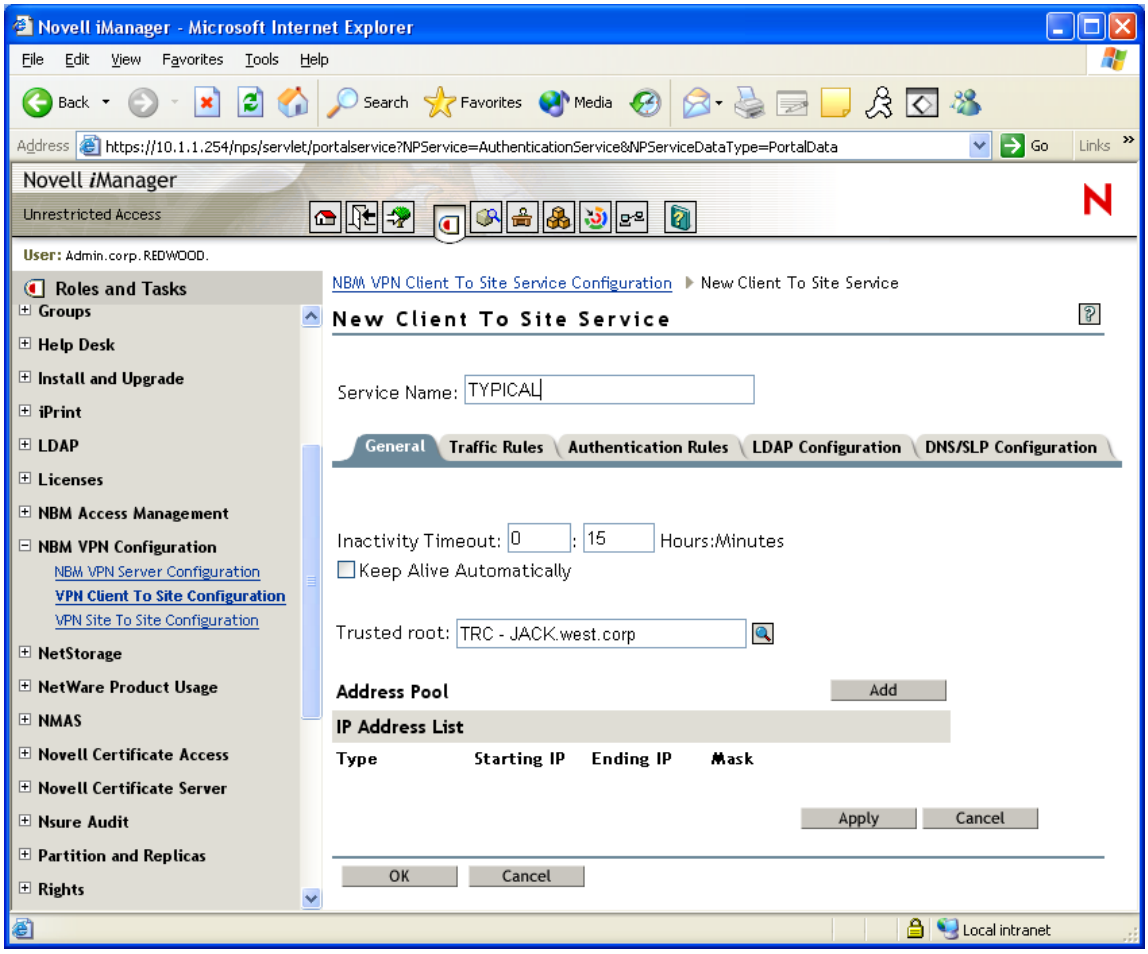
Important: *Change the context to the context of the server! Type in the context, and then click the* ***Update List*** *button.*

You should always see a default Client-to-Site service if you have changed to the context of the VPN server. If you do not configure your Client-to-Site service in the VPN server's container, it will not be able to use the service.

You can use the default Client-to-Site service and edit the default entries. To show how it is done, this book will create a new service.

You can have multiple Client-to-Site VPN services, though only one can be active on a VPN server at one time. This may be useful in a testing situation.

Click **New** to add a new Client-to-Site service.



Enter a **Service Name** for your Client-to-Site VPN service. This name will be stored in NDS as an object that contains the various Client-to-Site parameters to be applied to a VPN server. In the example shown above, the name used is **TYPICAL**.

You could have multiple Client-to-Site servers in your tree, each one using a different service and allowing different access privileges or connectivity options. However, each service must be created in the same container as the BorderManager server.

Browse to the Trusted Root Container (TRC) and select it, to fill in the **Trusted root** field. We already have a Trusted Root Container (TRC) in the NDS tree because the server was configured as a Site-

to-Site VPN server in the previous chapter. In this example, the TRC is called **TRC – JACK**.

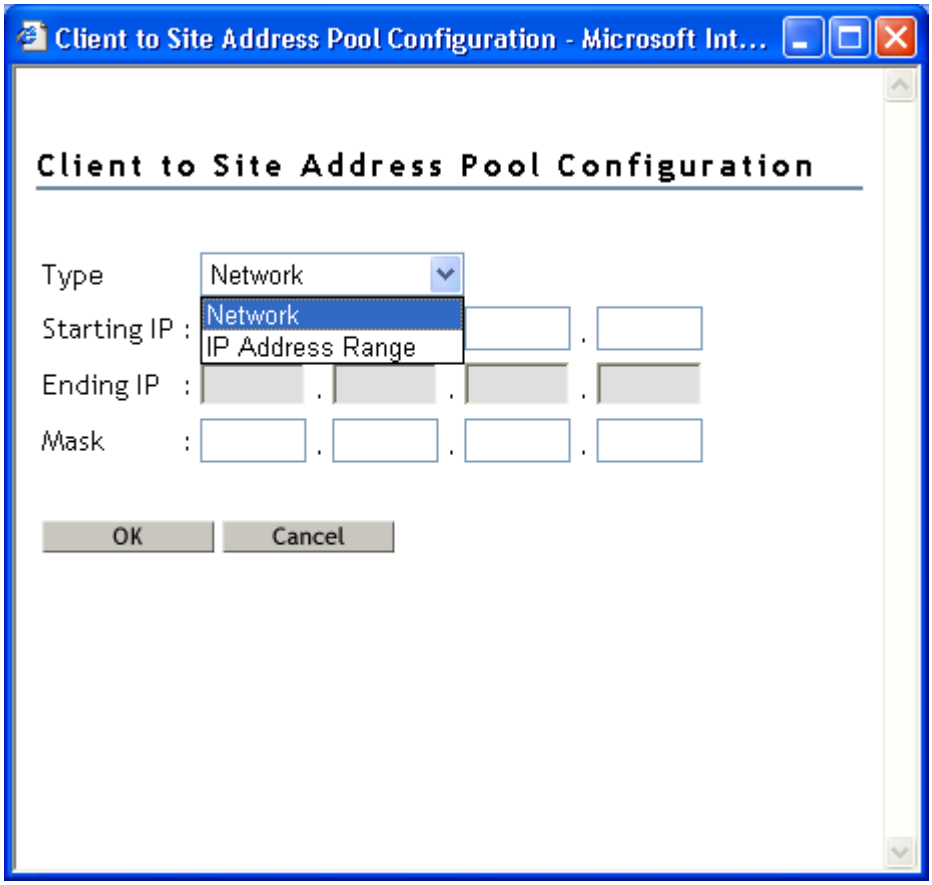
Select the TRC.

Next, you must define an **Address Pool**.

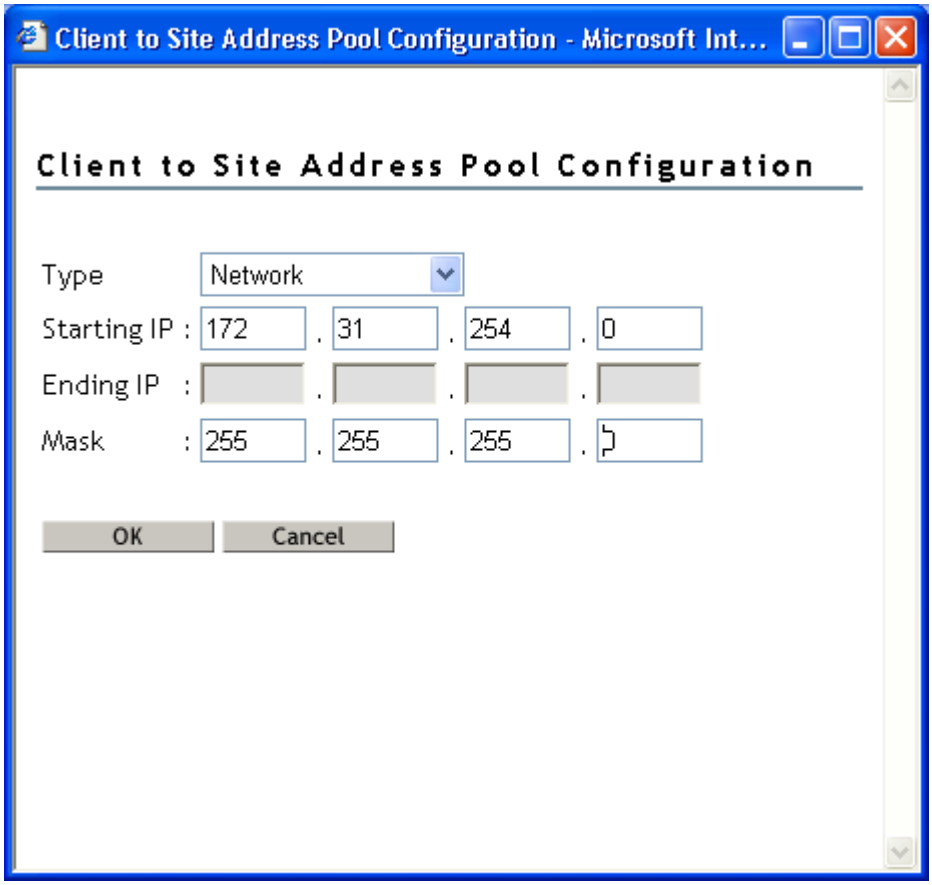
Unlike BorderManager 3.7 and earlier versions of Client-to-Site VPN, BorderManager 3.8 allows/requires you to push a VPN address to the remote client PC for VPN communications. This option solves a tremendous number of routing issues, since you can then configure static routes on your internal network to route traffic back to the VPN clients, even if the BorderManager VPN server is not the default gateway for internal hosts.

You must choose a VPN client Address Pool that does not conflict with any other network addresses on your network, on your remote clients' networks, or other networks connected to yours with VPN or WAN links.

Click on **Add**.



You have the option of adding a network address, or just a range of addresses within some network.

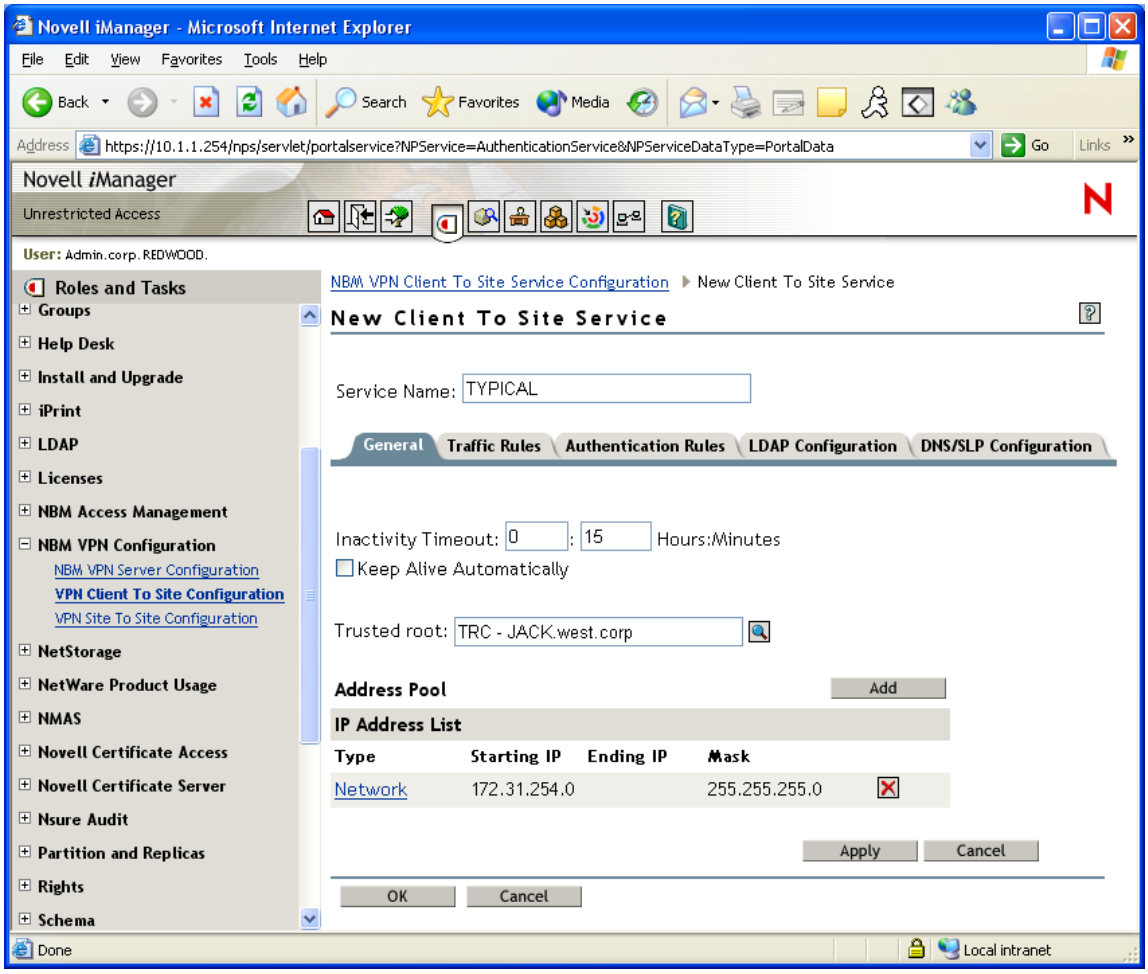


In this example, we will use the private IP network **172.31.254.0**, with subnet mask **255.255.255.0**. This selection will allow up to 254 simultaneous remote clients, with IP addresses starting at 172.31.254.1 and ending at 172.31.254.254.

A class B or even class A network could be configured as well. Additional networks or address ranges could be added to the address pool later should the configured network not allow enough addresses.

Internal routers will need to know how to route packets to the 172.31.254.0 address. If they have a default route that goes to the BorderManager 3.8 VPN server, there should be no problem. If they cannot be configured with a default route that takes packets to the VPN server, then they need to have a static route configured for the 172.31.254.0 network, with a next hop chosen to eventually get packets to the VPN server. This is quite different from previous versions of BorderManager, when an IP address was not assigned to the client.

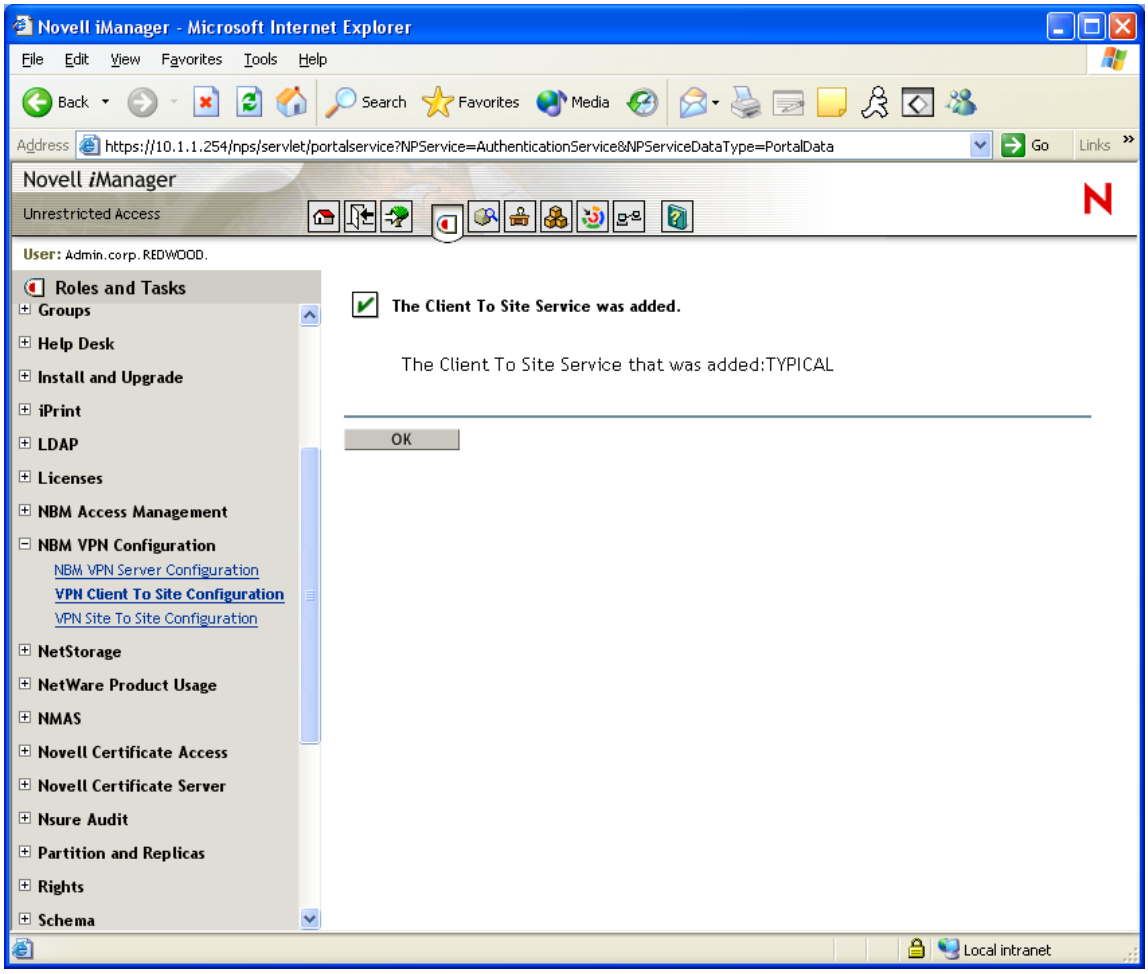
Click **OK** when done configuring a VPN network address or range.



Each subsection under **New Client To Site Service** must be saved individually using the **Apply** button near the bottom of the screen before you leave the menu.

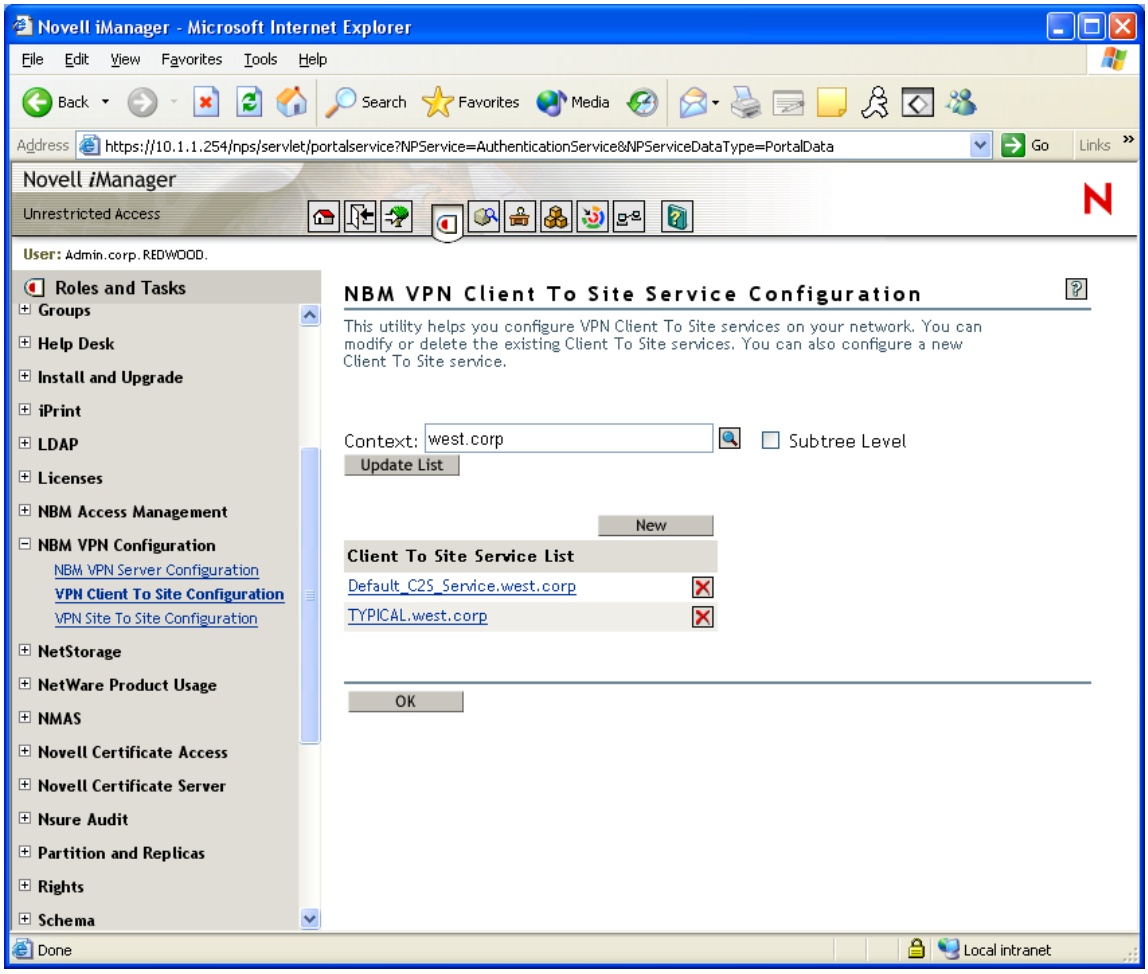
Click on **Apply.**

CAUTION *I recommend that you also then click on OK, to save all the settings to NDS, and then go back in to this point in the menu. I have found that iManager sometimes quits working properly if used for a long time. If iManager quits working, all of the configuration you have entered up to that point could be lost. The rule is,* ***Save Early, Save Often****.*



If you want to be safe, rather than sorry, click **OK** to save the service with settings configured so far. You will edit those settings later.

Now click on **OK**.



You should now be back at the Client To Site Service list for the VPN server's context. You should see your new service, and the default service.

Click on your new service so that it can be configured further.

Configure Traffic Rules

Next, click on **Traffic Rules**.

BorderManager 3.7 and earlier did not allow configuration of rules that limited the types of traffic allowed over a VPN connection, or the destination address within the protected network. BorderManager 3.8 does provide a great deal of control over such traffic. You have three choices of what to do with network traffic from the remote VPN client:

1. Encrypt it – which means send it over the VPN tunnel.
2. Do not encrypt it – which essentially means allow the traffic from the remote PC, but do not send it over the VPN tunnel.
3. Deny it – which means do not allow the traffic either over the tunnel or allow it out from the remote PC.

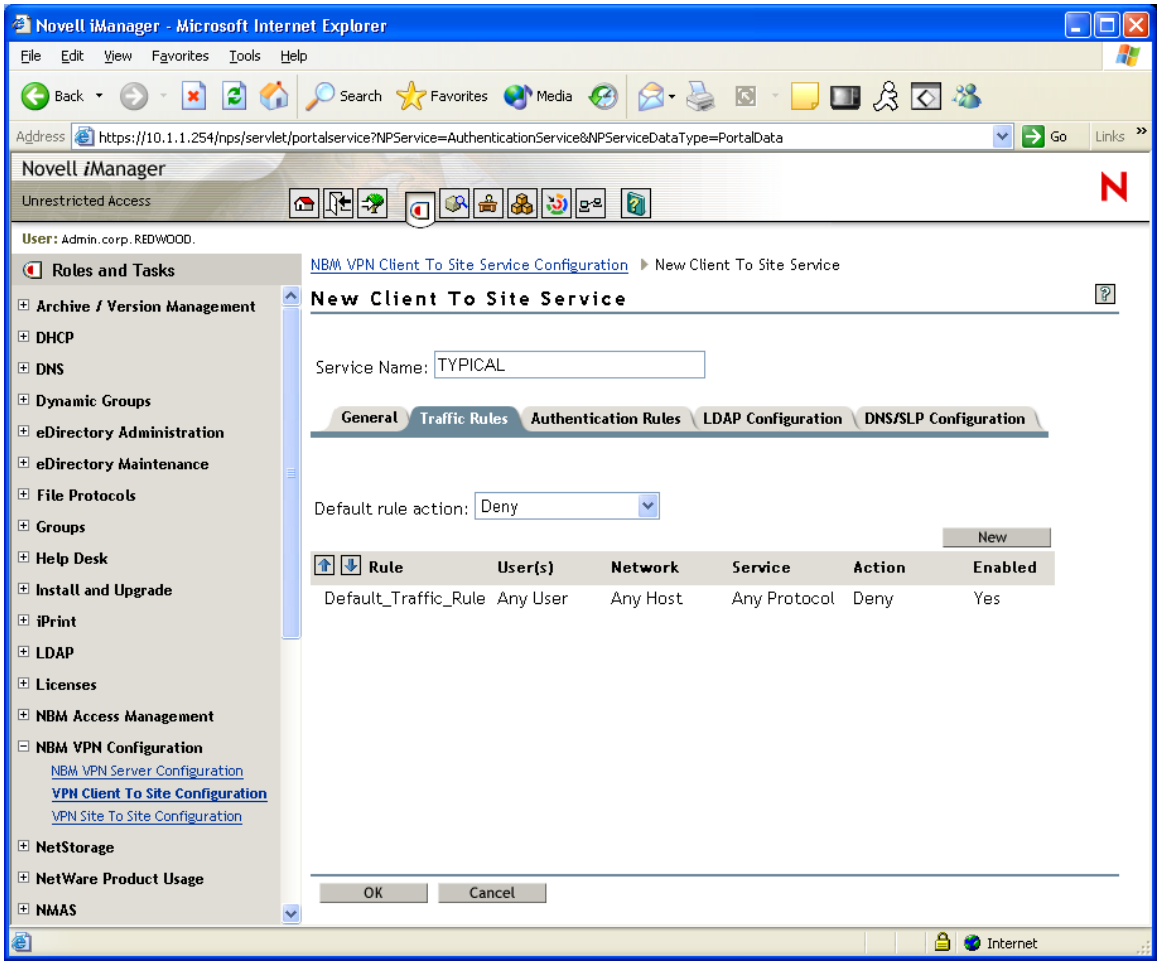
In previous versions of BorderManager, the Client-Site VPN automatically tunneled traffic any network that was encrypted ('protected'), and by default it encrypted all networks. That had the effect that even local traffic from the remote VPN client to a host on the same LAN as the remote VPN PC was sent over the VPN connection, resulting in loss of communications between the remote PC and anything not on the network behind BorderManager. The equivalent situation in BorderManager 3.8 will also occur, based on the default traffic rule that denies all traffic. In order to NOT send traffic over the VPN, you must allow traffic to be unencrypted in a traffic rule.

If you want to allow a remote PC to browse the Internet at the same time as it is connected to the VPN, you will need to have a traffic rule at some point that allows all traffic, unencrypted, below the traffic rules designed to encrypt traffic into your BorderManager network(s).

BorderManager 3.8 uses a set of access rules, much like access rules controlling proxies in NWADMN32. There is also a default rule to Deny Any, meaning that even if the VPN were configured and working now, all traffic through it would be denied. It is necessary to add at least one traffic rule to allow some desired traffic through the VPN connection. All other traffic will be denied.

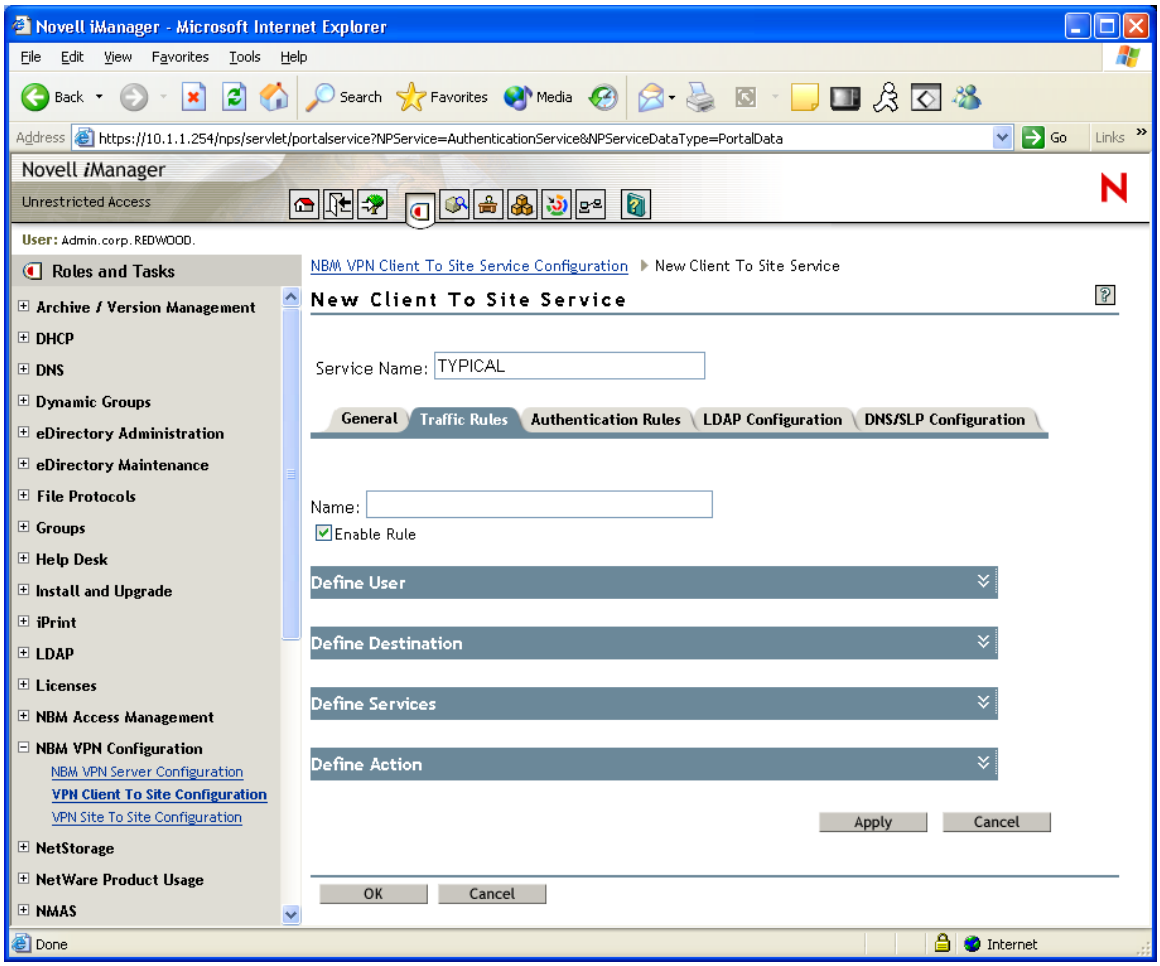
Traffic rules also apply to the type of authentication being used. You must have different traffic rules for the following types of authentication:

- NMAS (NDS)
- LDAP
- Certificates



The VPN access rules, like those for proxies, are read from top to bottom. The first rule (allow or deny) that matches the type of traffic seen on the VPN is used.

Click on **New** to add a new traffic rule.



You must next enter a **name** for the rule. You can have many rules in your rule list, an each will be listed by the name you enter here. The name should be short, but reasonable descriptive. Within this rule, you will have the choice of defining a user (or all users), a destination (or all destinations), a service (or all services) and an action (allow or deny, encrypted or not).

Let's decide first what we want to accomplish with the access rules. We want to start with NDS authentication, not worrying about certificates and LDAP methods. (Examples of that will be shown later).

- First, we want the Admin user of the tree to be allowed to go to any destination inside the BorderManager server, and use any protocol.
- Next, we want a VPN Users group to be allowed to go to any destination **except** a sensitive internal server at IP address 10.1.1.50.
- Next, we want any user in the NDS tree to be allowed to go to an internal web server at IP address 10.1.1.100, but only

be able to use ports 80 and 443. The traffic must be encrypted.

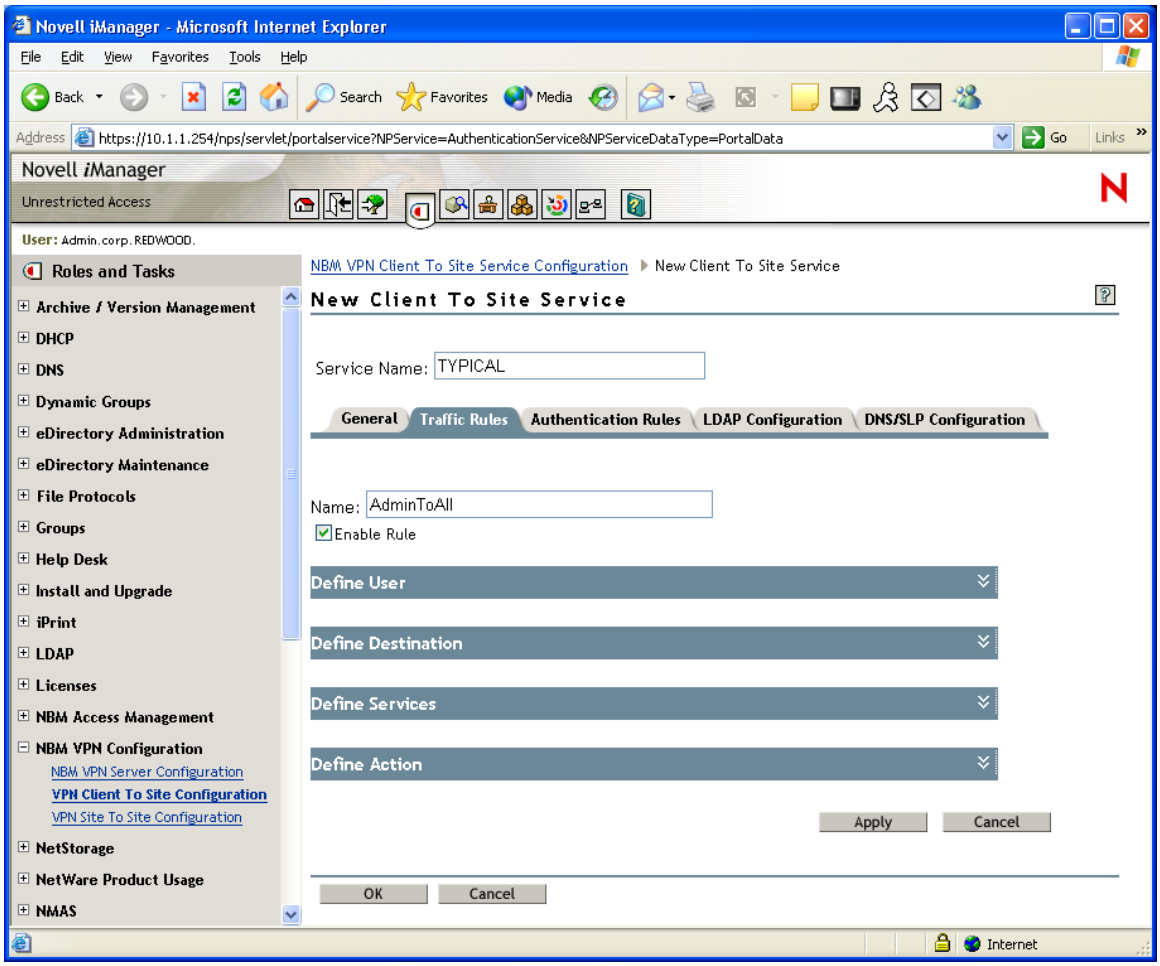
- Next, we want to allow any user in the NDS tree to be allowed to go to an iFolder web server at IP address 10.1.1.101, using ports 52080 and the traffic should not be encrypted, since the iFolder data is already encrypted.
- Next, we want remote VPN users to be able to browse to the Internet while connected to the VPN, as well as be able to communicate with other hosts on their own local network.
- Finally, we want to deny all other traffic, which will be taken care of by the default rule.

With this set of criteria, we can put together a set of access rules that will allow us to do what we want.

We will have to configure multiple rules, and place them in a sequence that gives the desired results.

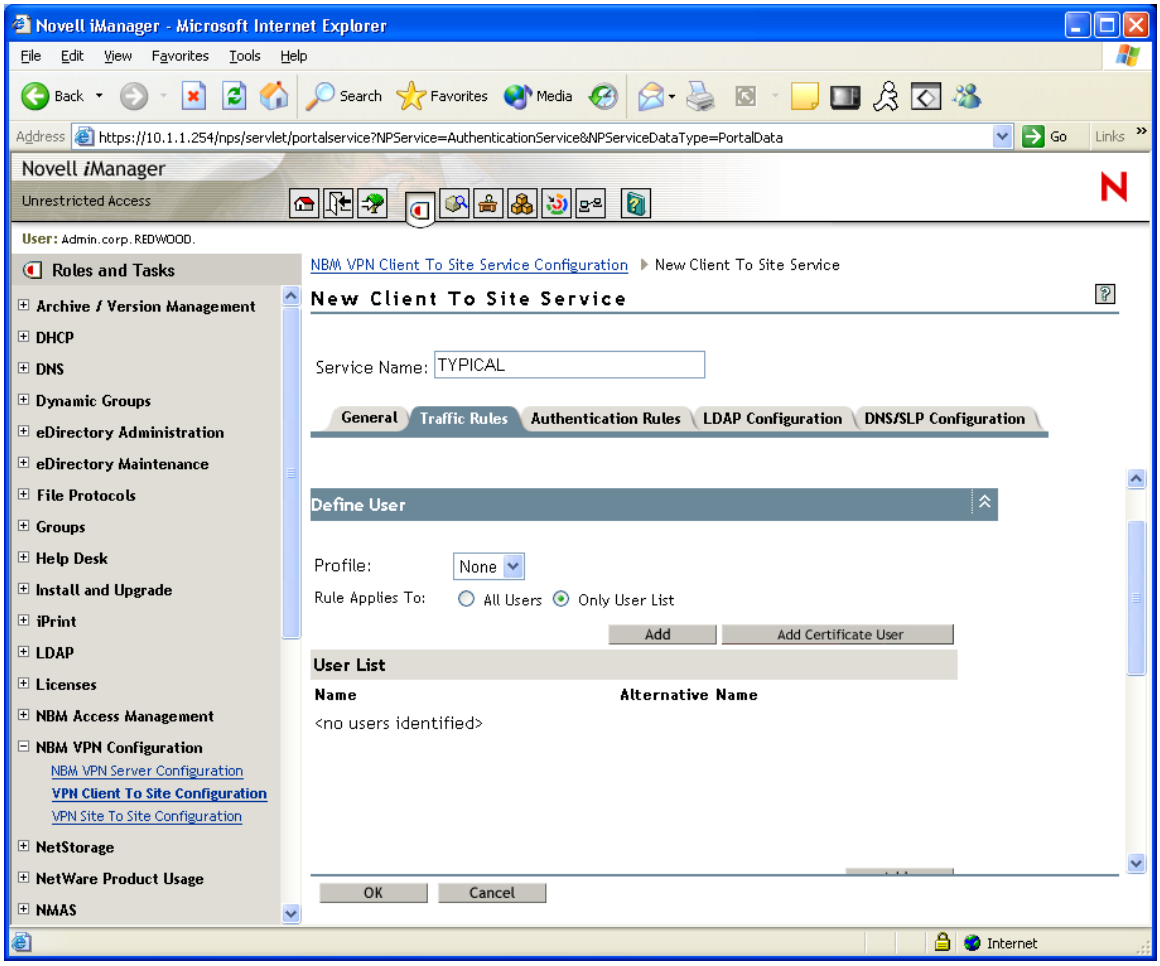
You may wish to review the section called **Limitations** near the very beginning of this chapter before planning your own access rules.

Traffic Rules – Allow Admin User to All Internal Hosts



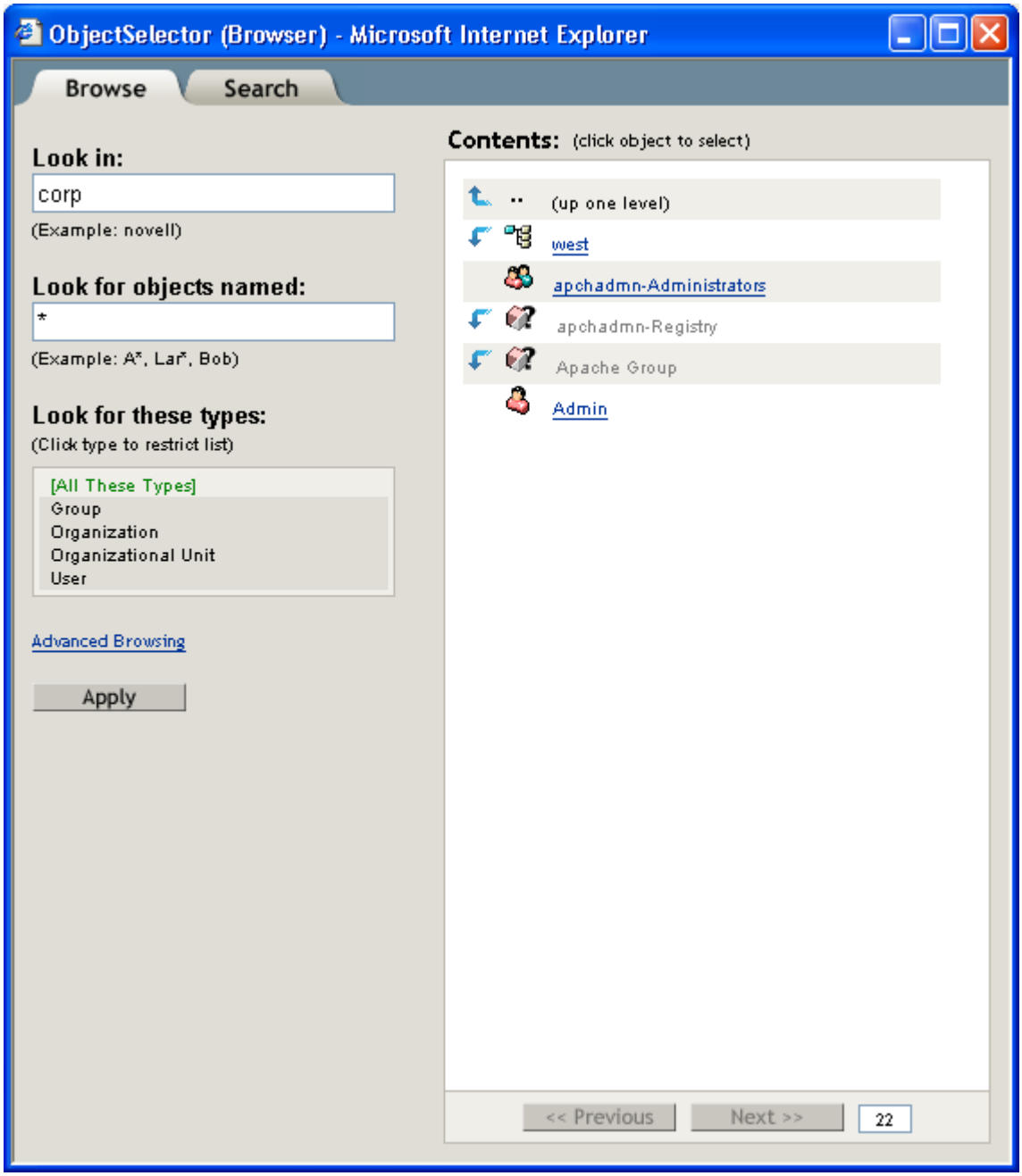
Start with a rule to allow the Admin user ID full access. We will give this rule the name **AdminToAll**.

Next, expand the **Define User** section by clicking on the **arrows** at the far right of the Define User bar.

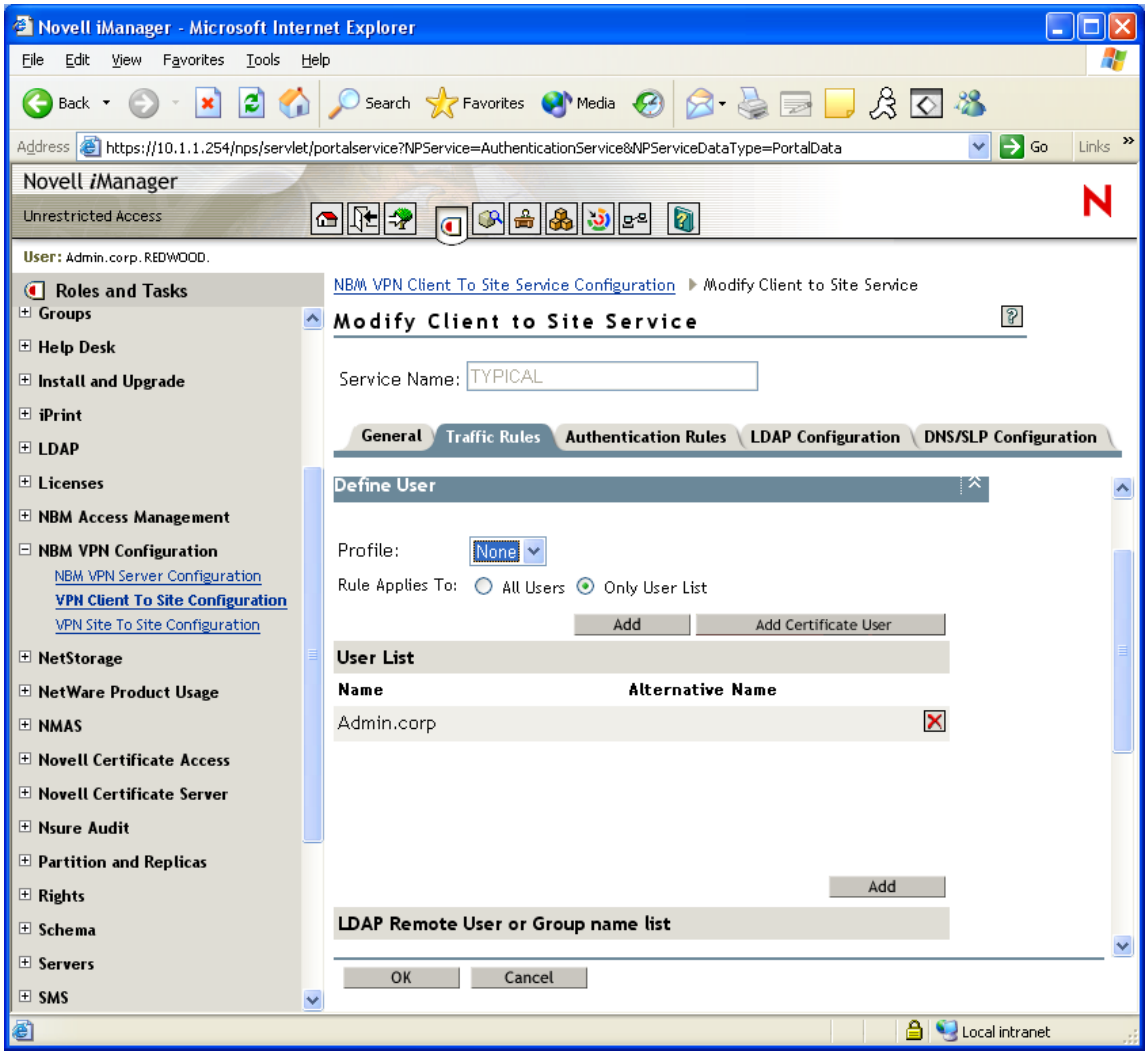


The section expands to reveal details.

Select **Only User List**, and click **Add**.



Browse to the **Admin user account**, and select it.

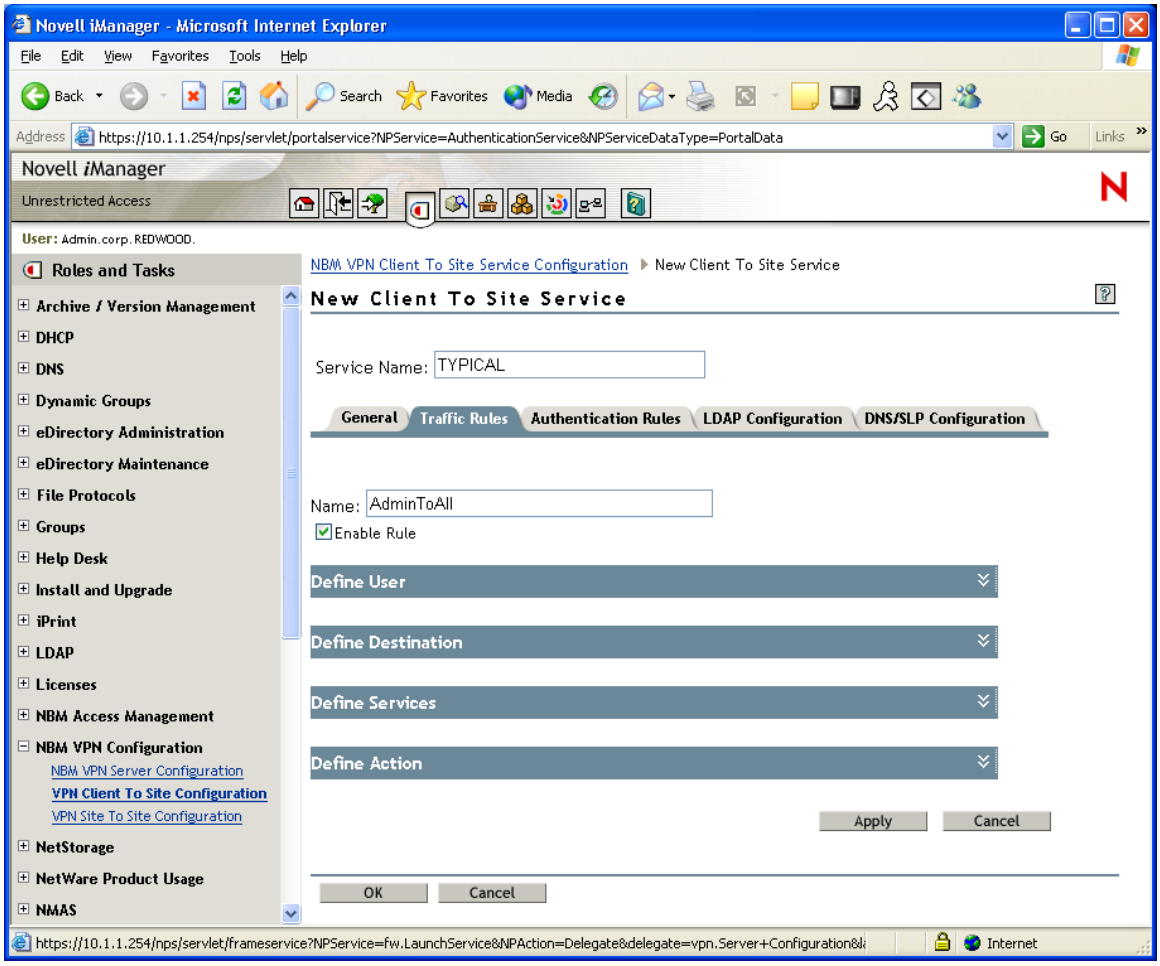


The **admin.corp** user ID is added to the **User List**.

Add Certificate User is used to allow users based on X.509 certificates rather than NDS accounts. There is an example for certificate-based authentication later in this chapter.

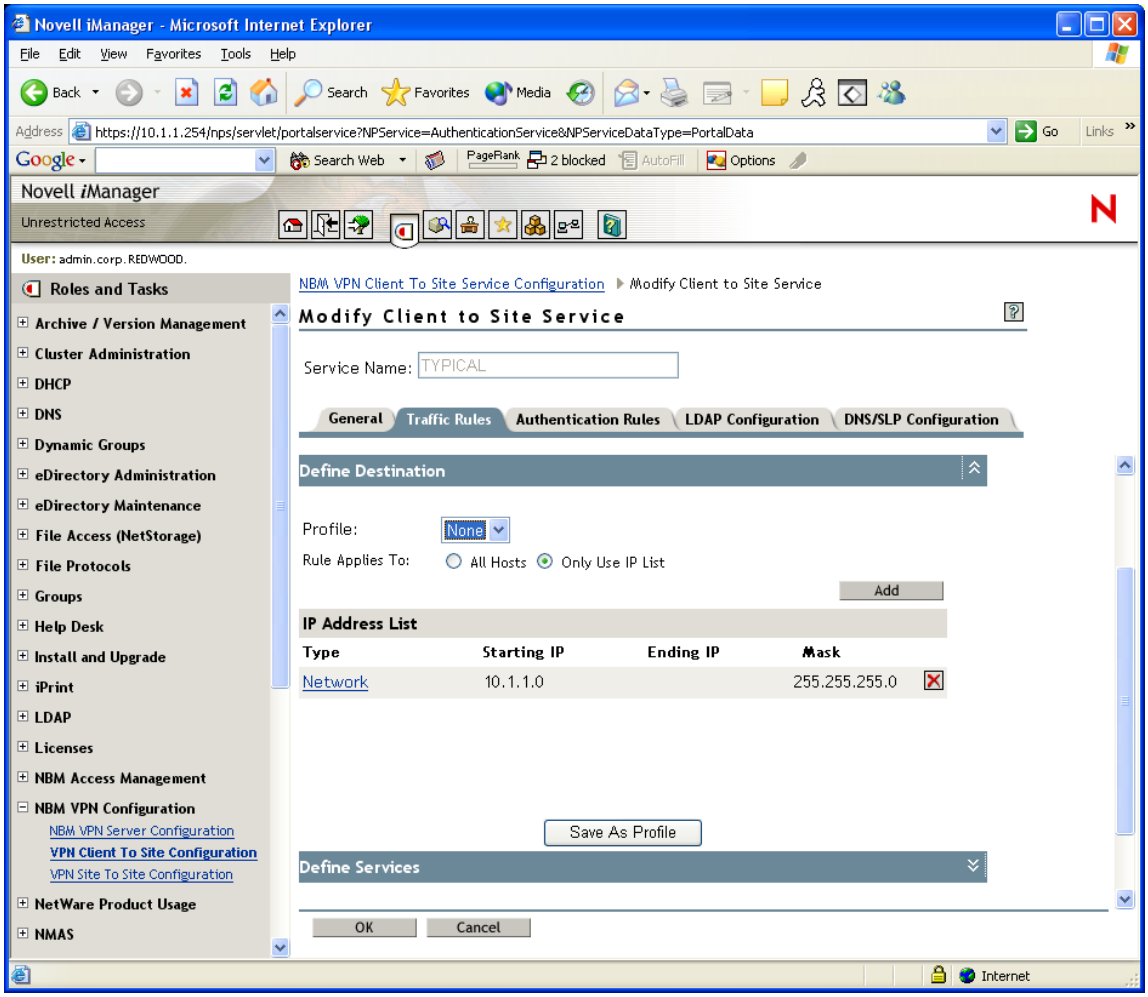
If you scroll down a bit, you will also see an option for **LDAP Remote User or Group name list**. In that section, you can define LDAP users or groups for traffic rules. There is an example for LDAP-based authentication later in this chapter.

For now, we do not wish to add any more users to this list, so click on the **arrows** in the Define User bar to close that section.



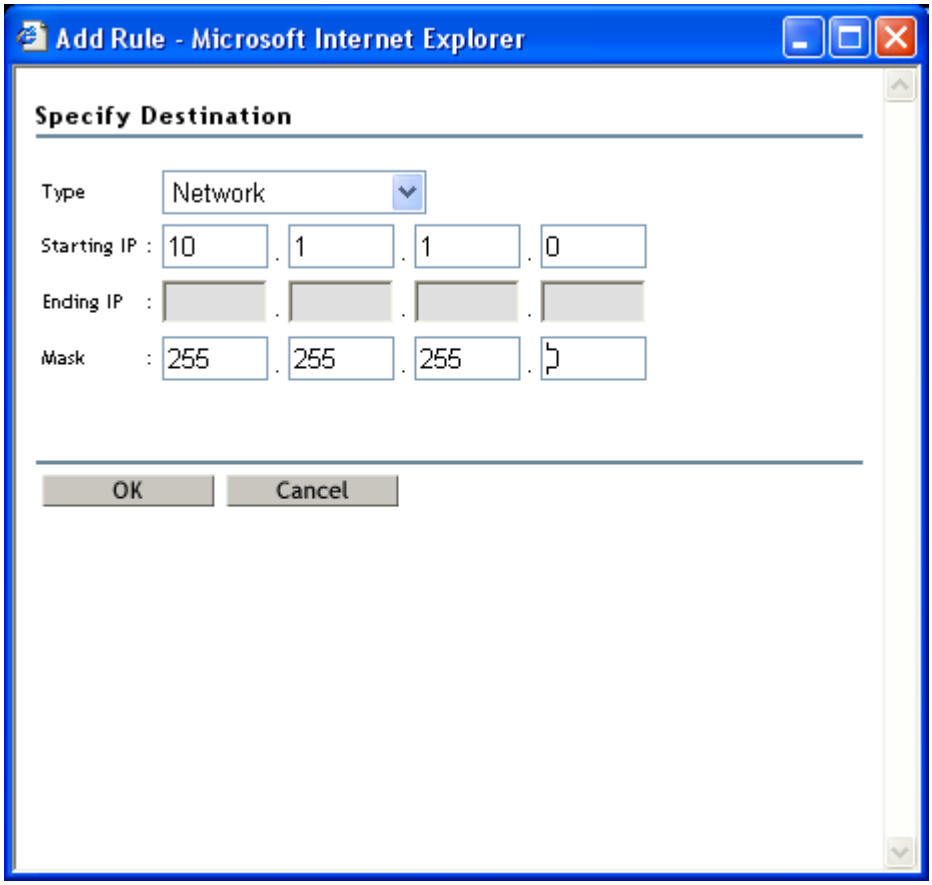
Now click on the arrows in the **Define Destination** bar to expand that section.

The default value applies to all hosts. This is not what we want, because it would also force Internet browsing traffic over the VPN, so we need to specify the LAN addresses behind the BorderManager server.



Expand the **Define Destination** bar by clicking on the arrows in the bar.

Select **Only Use IP List** and click on **Add**.



Enter the **network address** of your internal LAN (behind the BorderManager server). If you have multiple subnets inside your LAN, you will need to add each network address separately. In this example, only network 10.1.1.0 (255.255.255.0) is being made available by VPN.

Click **OK** in the Specify Destination window..

Collapse the Define Destination section by clicking on the **arrows** in the bar.

Expand the **Define Services** section.

The default choice calls out all services, and since this is what we want to allow, we do not need to change anything.

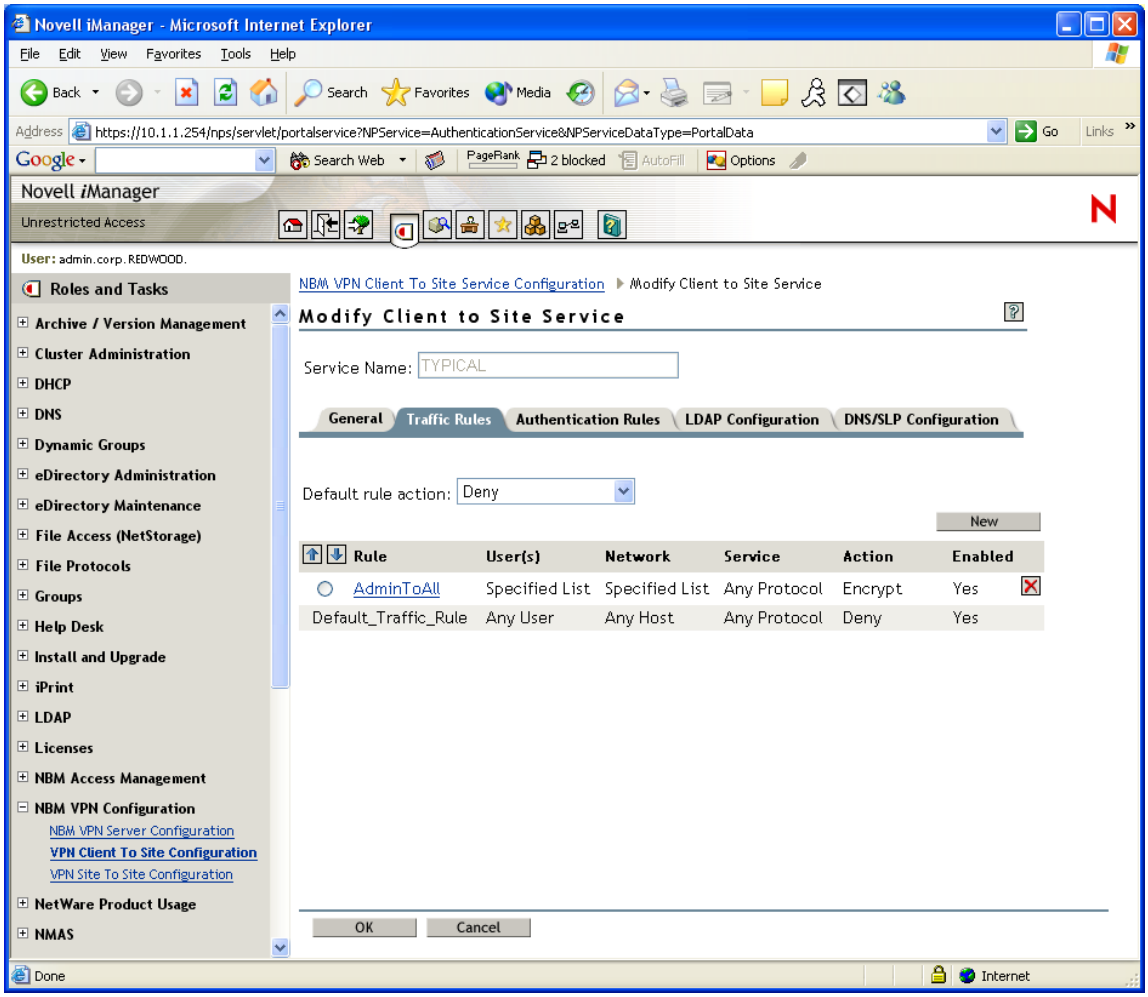
Collapse the Define Services section.

Expand the **Define Action** section.

The default action allows and encrypts all services. Again, this is what we want, so we do not need to change any settings.

Collapse the define action section.

Click on **Apply** to save this traffic rule.



Now we have at least one traffic rule, which is designed to work only when the Admin.corp user in the VPN server's NDS tree is authenticated.

With this traffic rule, if the Admin user authenticates by NMAS (NDS user ID and password), that user will be able to go to any host in the 10.1.1.0 network over the VPN. If no more traffic rules were added now, the Admin user would not be able to browse the internet or connect to any other remote hosts while connected to the VPN.

Next, we need to add additional traffic rules, as defined in the following pages.

Click **New** to add the next rule. It will be placed at the bottom of the rules list. You can move it up or down in the rules list later.

Traffic Rules - Allow VPN Users to All Hosts Except 10.1.1.50

We can make an access rule much like the allow rule for the Admin user, to access all hosts, but how do we prevent those users from getting to one particular host?

We will have to use **two rules** – one to deny access to 10.1.1.50 (for all users), and one to allow access to any host for the VPN Users group. The rule order is critical when we are done.

The Allow AdminToAll rule must be at the top of the list.

Next, we need a rule to **deny access to 10.1.1.50**.

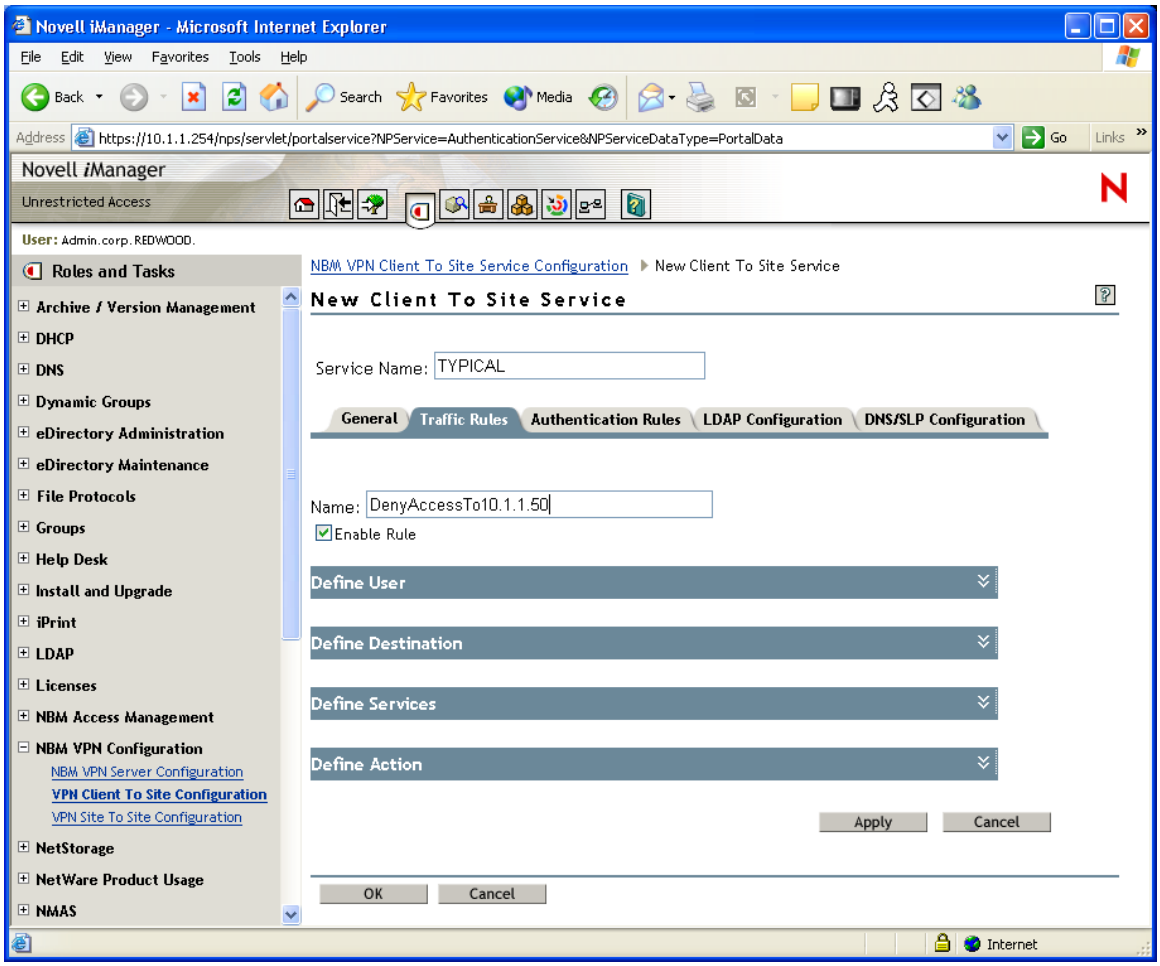
After that, we can put in a rule to **allow the VPN Users group to get to any host in the 10.1.1.0 network**.

If a VPN Users group member tries to access 10.1.1.50 through the VPN, that access will be denied because the deny rule for 10.1.1.50 is higher in the rules list than the rule that allows the user to get to any host.

Only those sections where a change from the default settings is needed will be shown in all following screenshots.

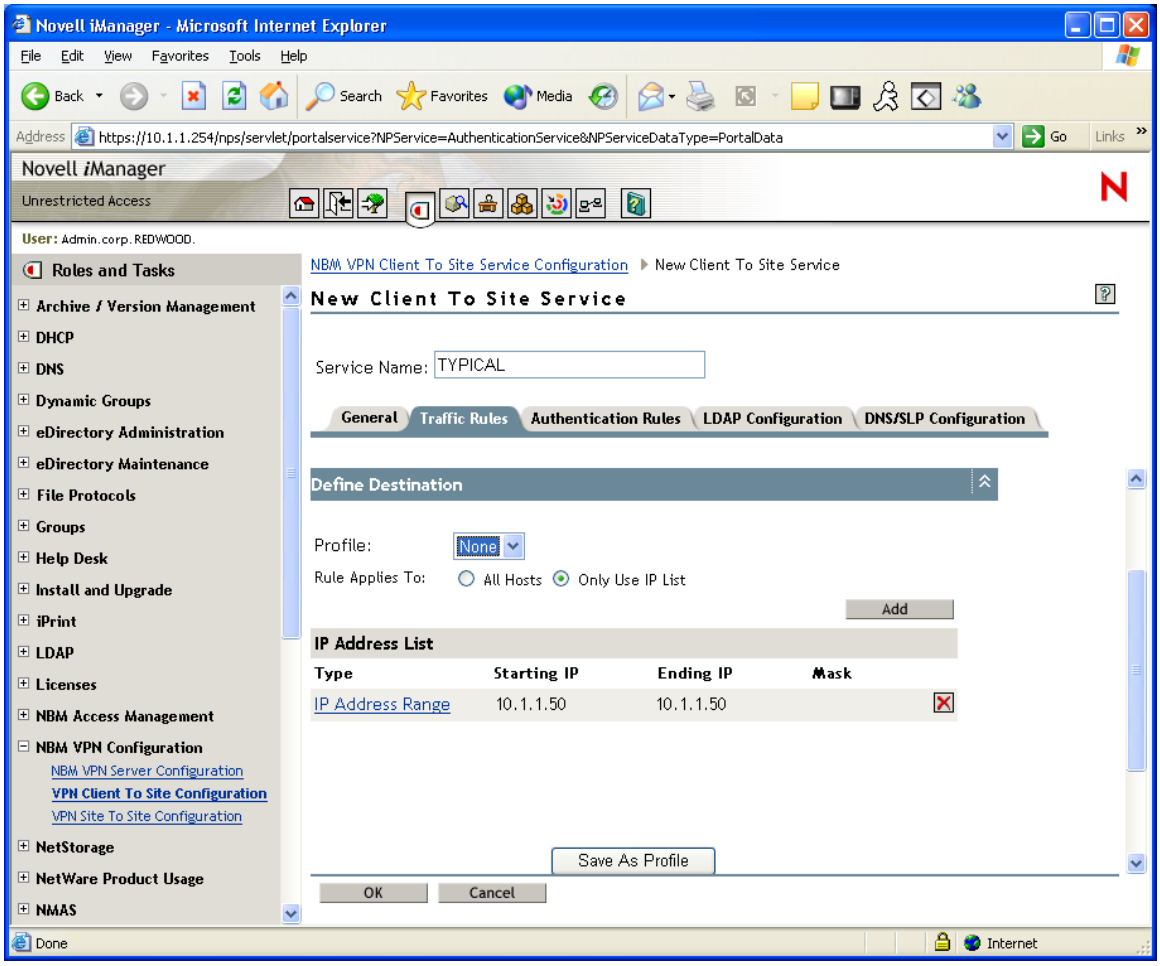
Deny All Access to 10.1.1.50 Rule

Click on **New**, in the **Traffic Rules** menu.



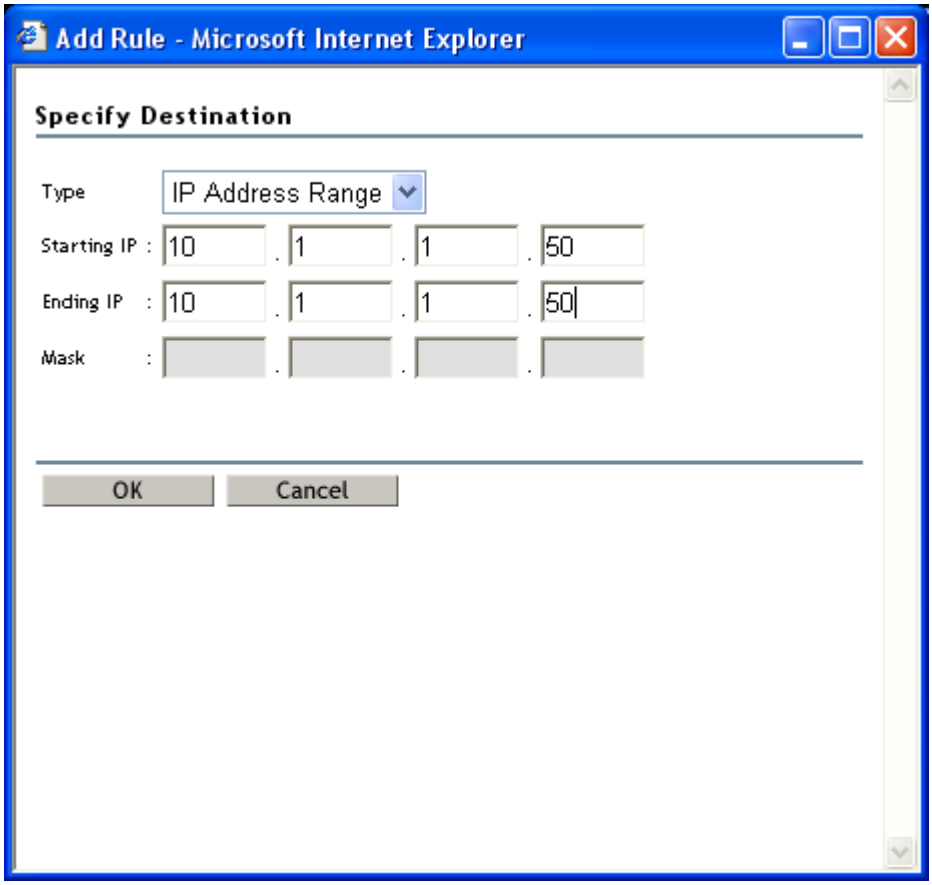
Name this rule **DenyAccessTo10.1.1.50**.

Expand the **Define Destination** section.



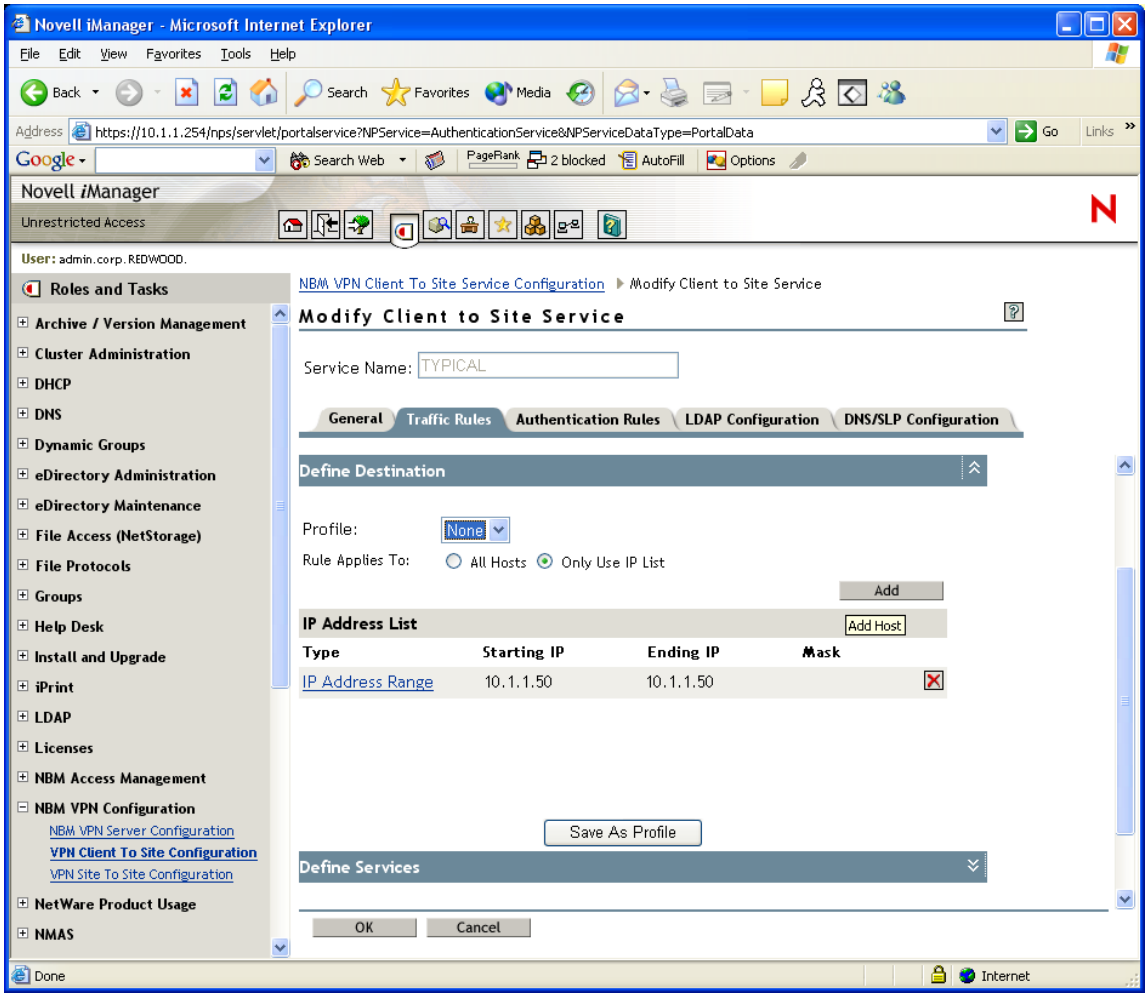
In the **Define Destination** section, choose **Only Use IP List**.

Click on the **Add** button.

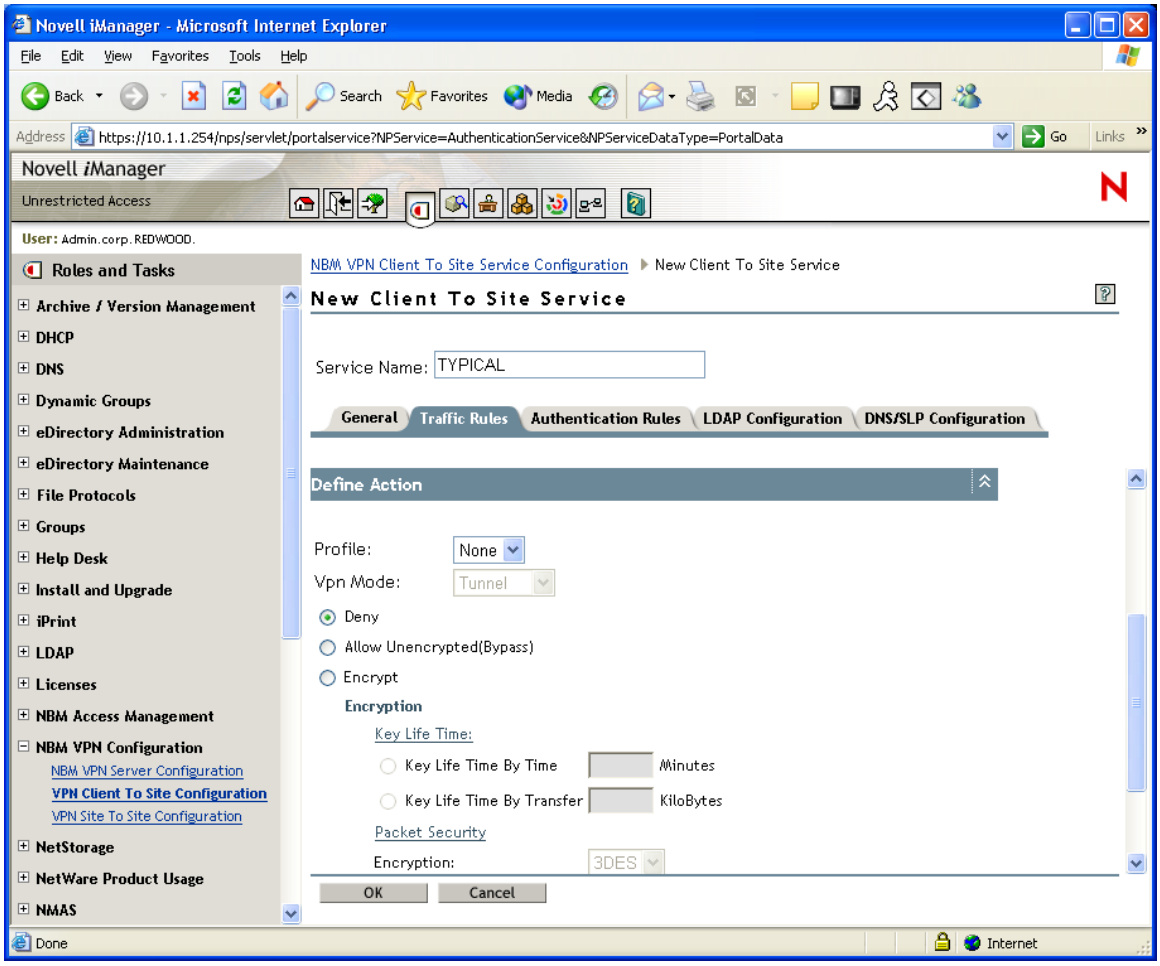


Add a **IP address range** of **10.1.1.50** to **10.1.1.50**.

Click **OK**.



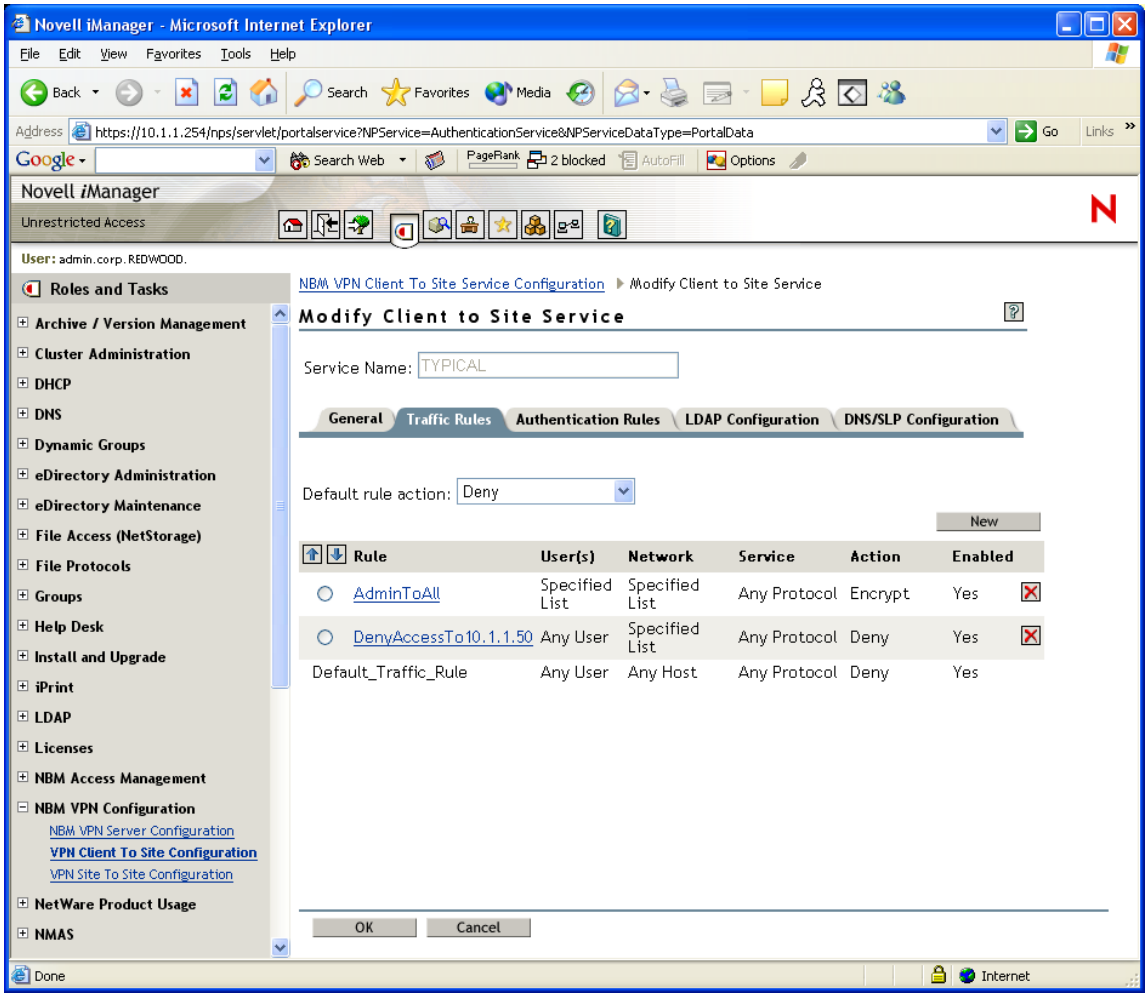
Next, **Collapse the Define Destination section**, or scroll down, and expand the **Define Action** section.



In the **Define Action** section, choose **Deny**.

Collapse the section, or scroll down until the Apply button can be seen.

Click on **Apply** to save this rule.

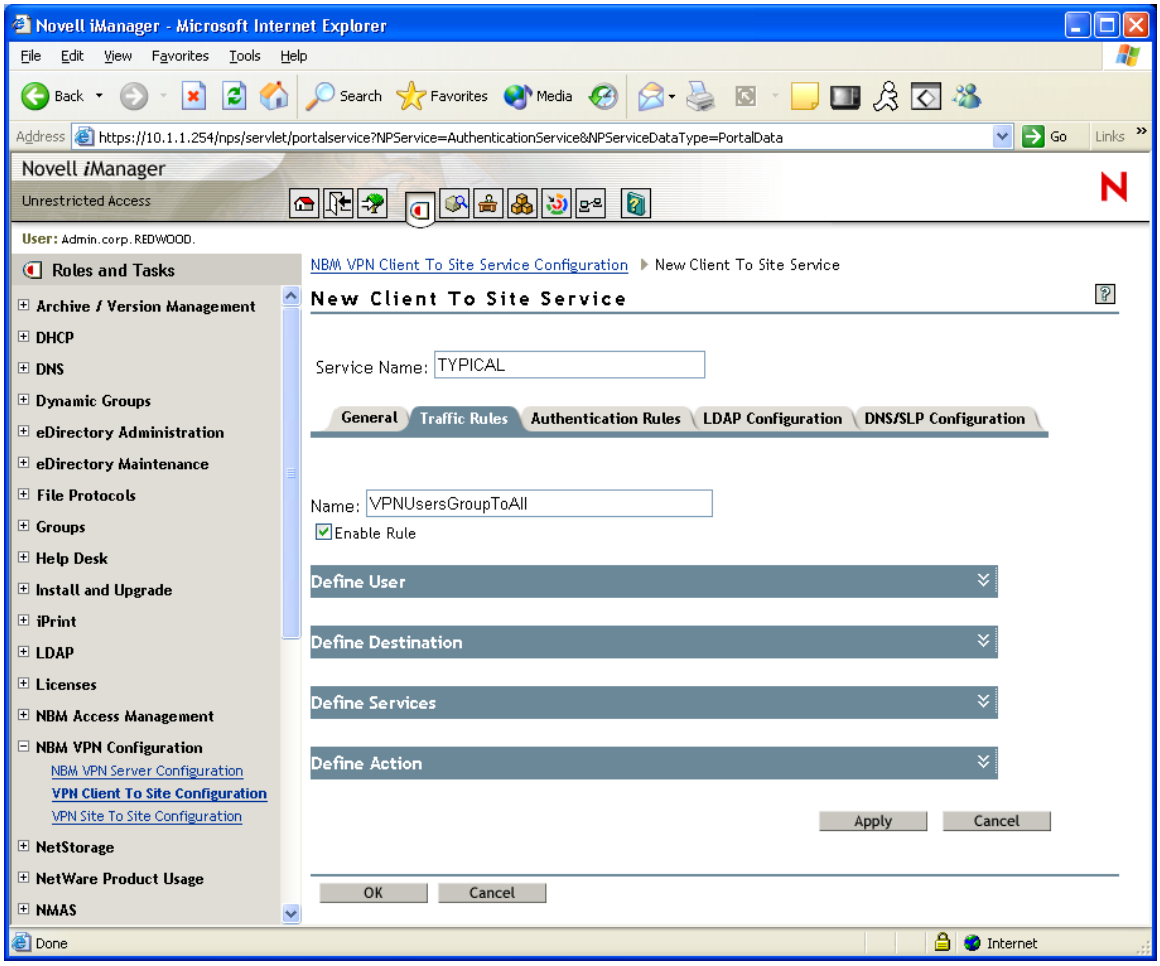


We can now see that we have a rule after the AdminToAll rule that will deny access to the 10.1.1.50 for anything added after it in the rules list.

Now we can add a rule under it to allow the VPN Users group to all internal hosts.

Click on **New**.

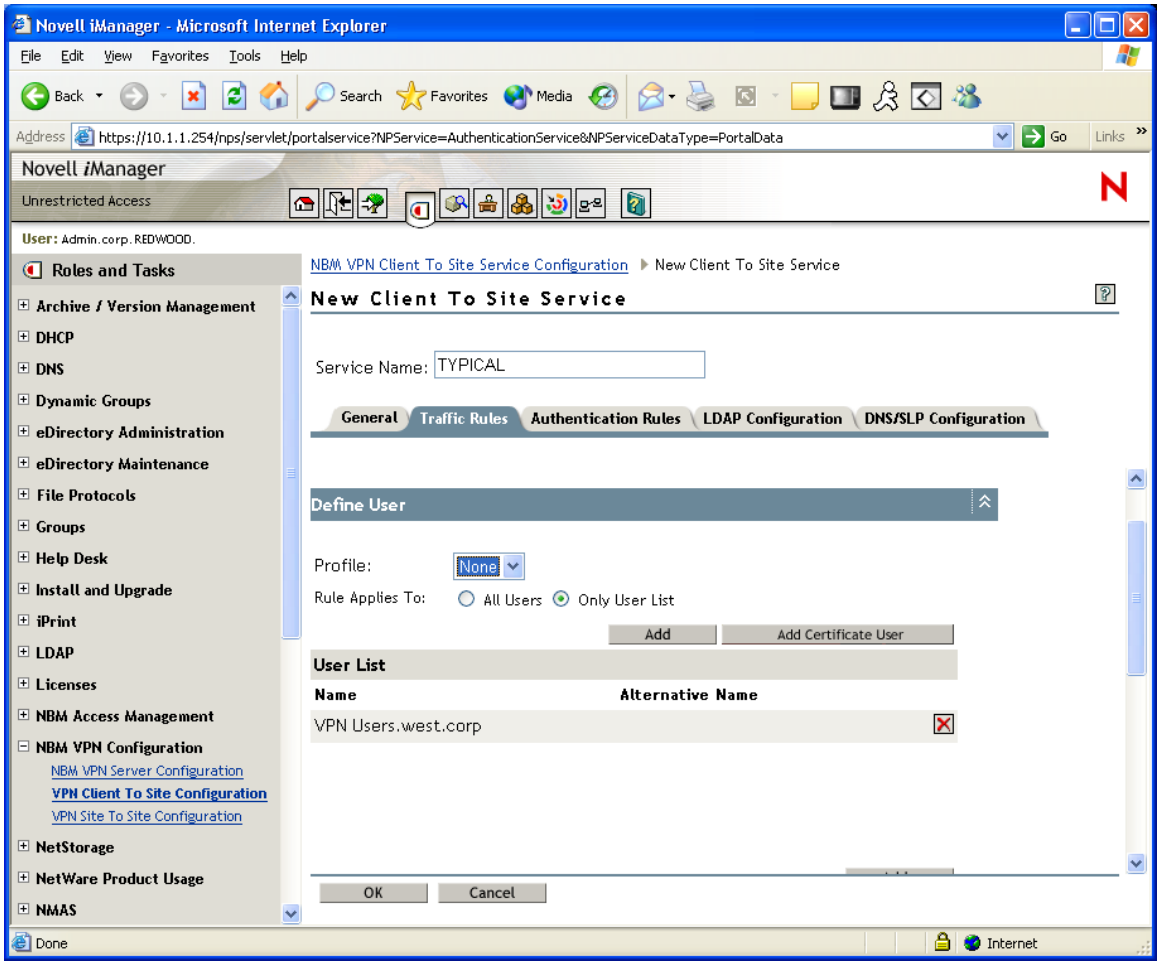
Traffic Rule - Allow VPN Users Group to All Internal Hosts



Give the new rule a descriptive **name**, such as **VPNUsersGroupToAll**.

The only non-default settings we will need for this rule is to define the user as the VPN Users group, and specify the internal network(s) as the destination.

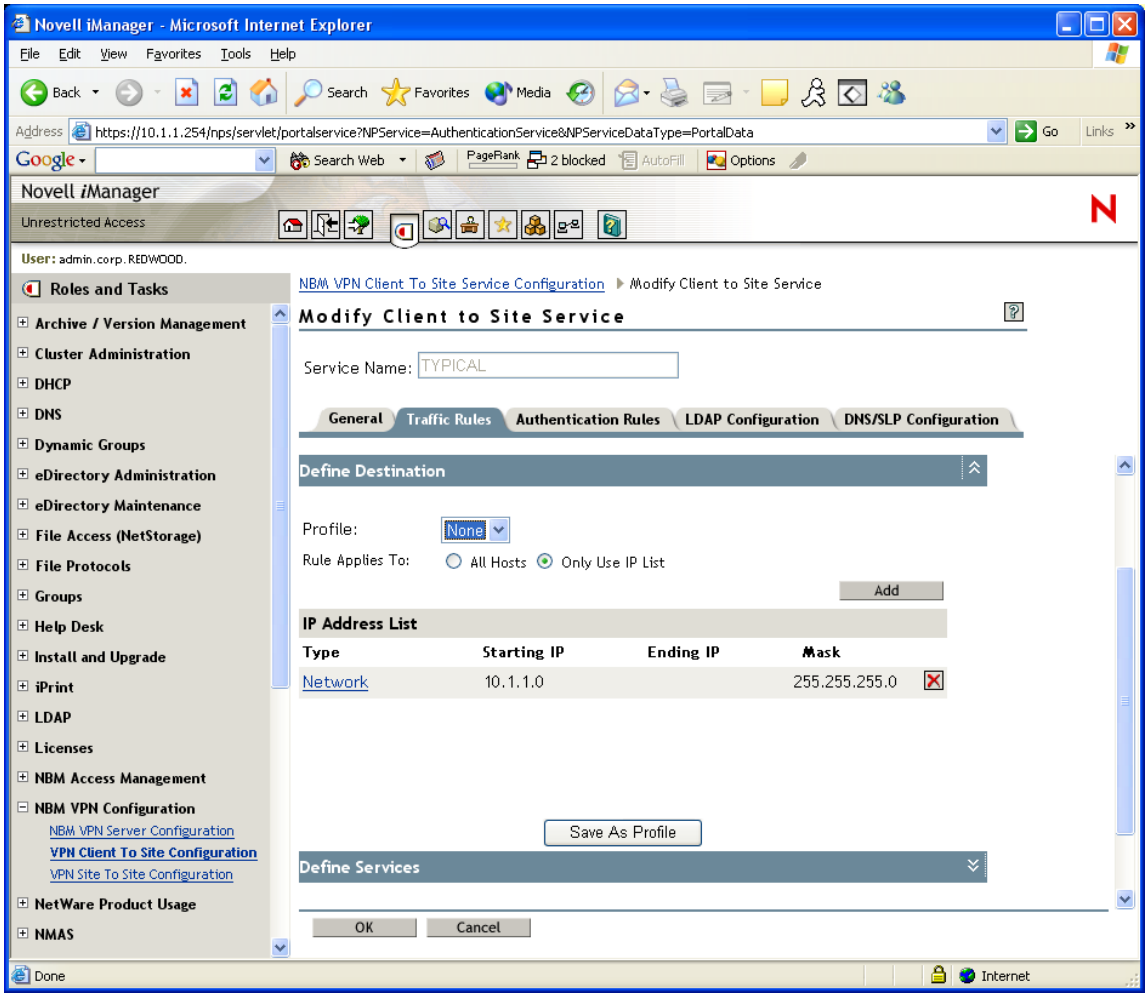
Expand the **Define Users** section.



In the **Define Users** section, select **Only User List**, and **browse** to the **VPN Users** group.

Select the **VPN Users** group.

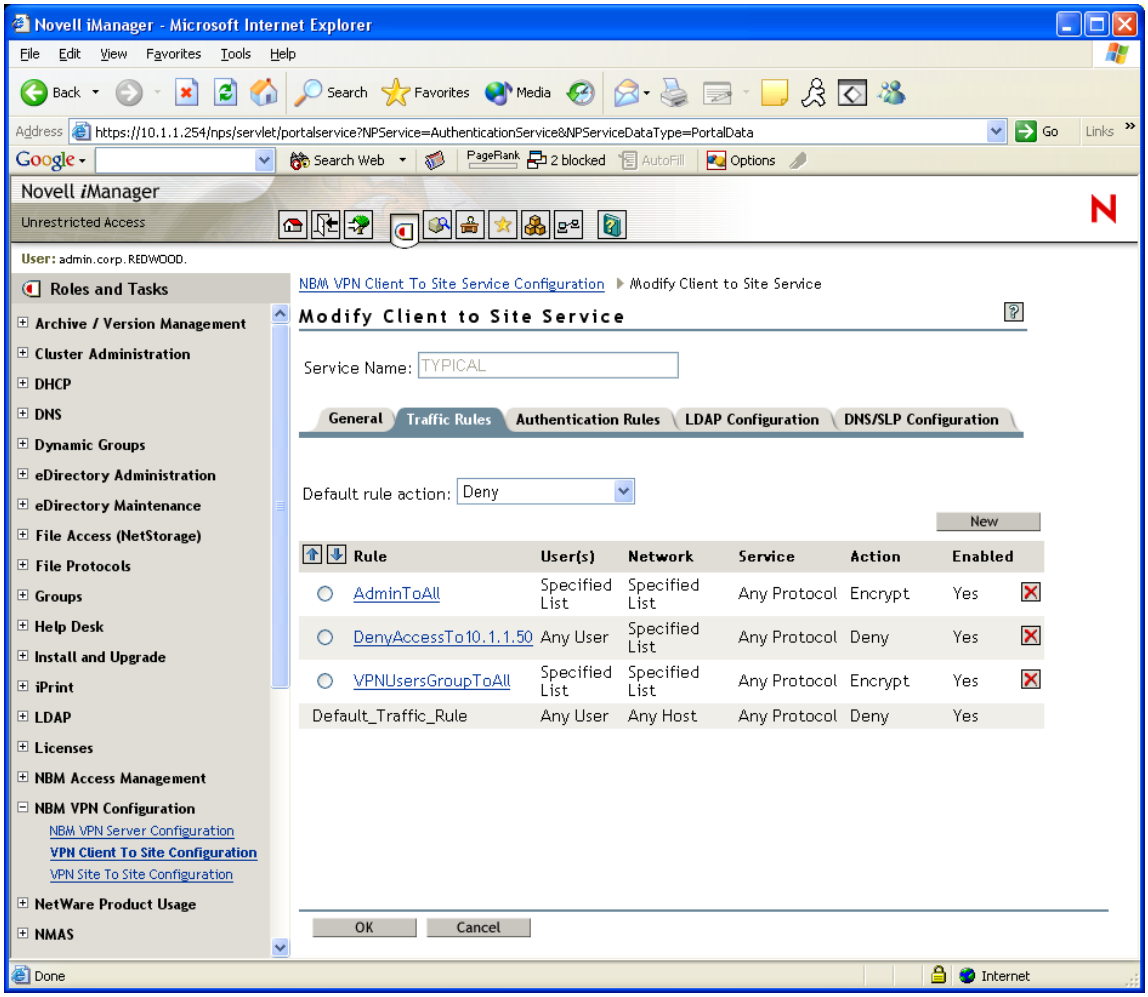
Collapse the **Define User** section, and select the **Define Destination** section.



Select **Only Use IP List** and click **Add**.

Add a **network address** of 10.1.1.0, with subnet mask 255.255.255.0. Click **OK**.

Scroll down and click on **Apply**.

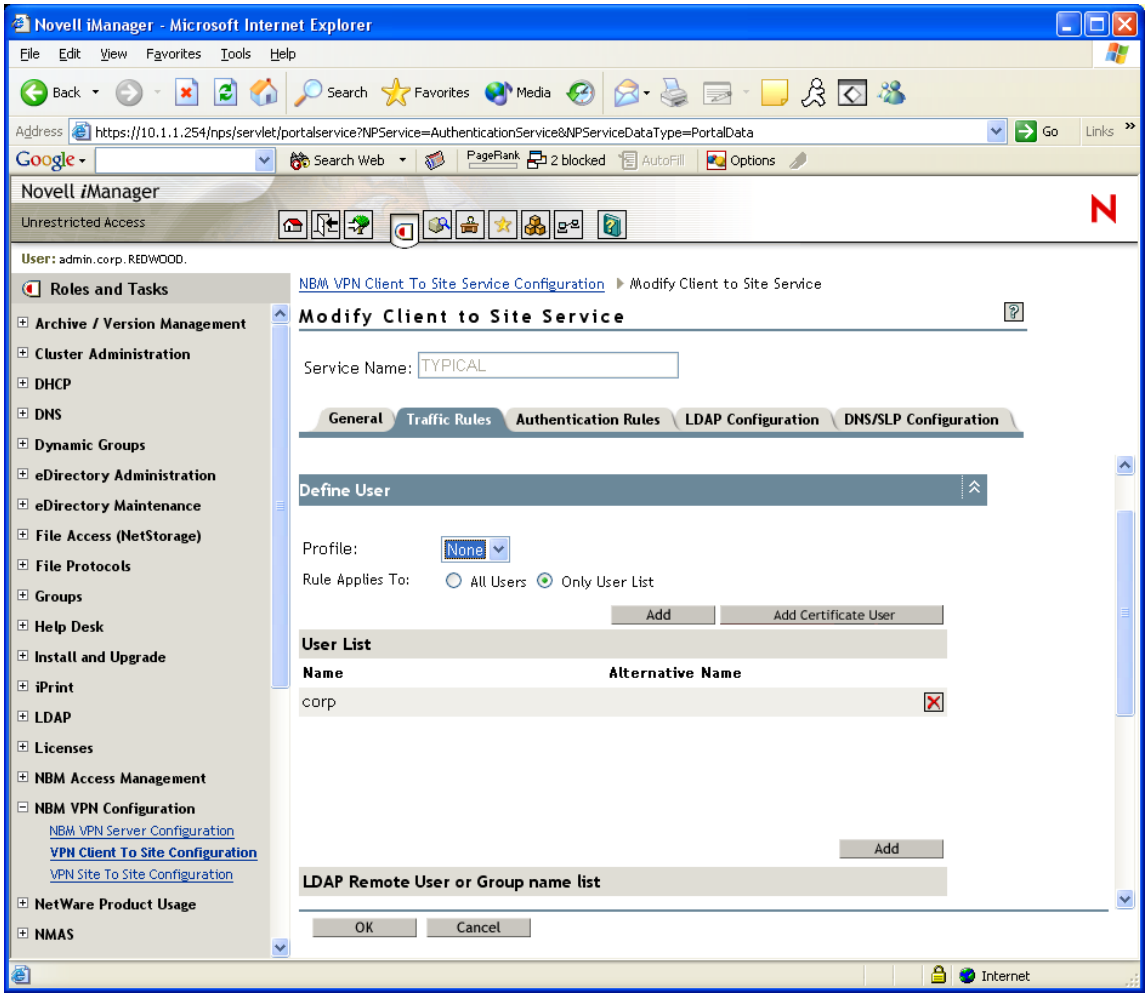


We have now allowed the **VPN Users** group to get to anything accessible via VPN except that denied by a rule higher in the rules list.

Click on **New**.

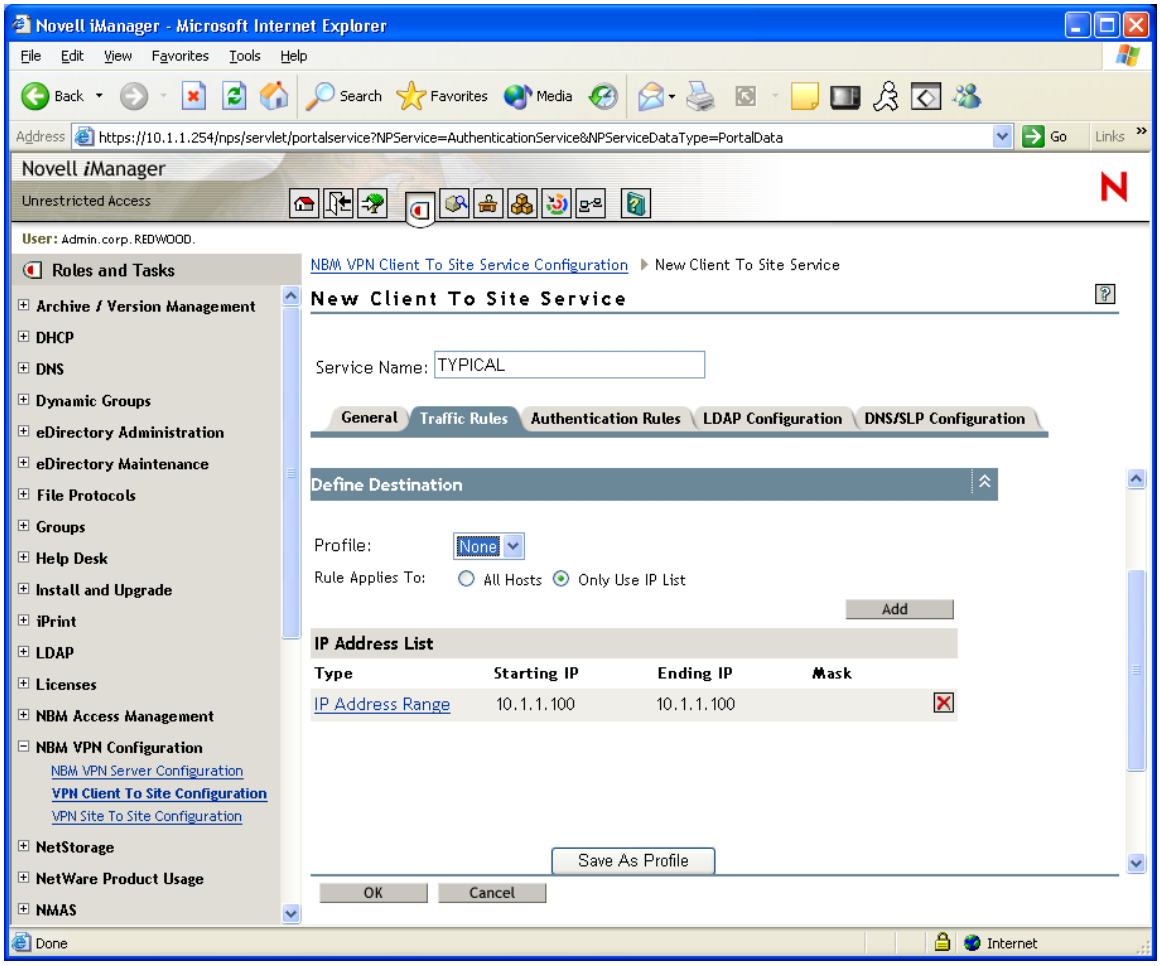
Traffic Rule - Allow All Users in NDS Tree Access to 10.1.1.100

Add a new rule, and call it **AllowUsersTo10.1.1.100_Port80**



Expand the Define User list, select **Only User List**, and browse to the top of the NDS tree. Select the Organization container at the top of the tree. Click **OK**.

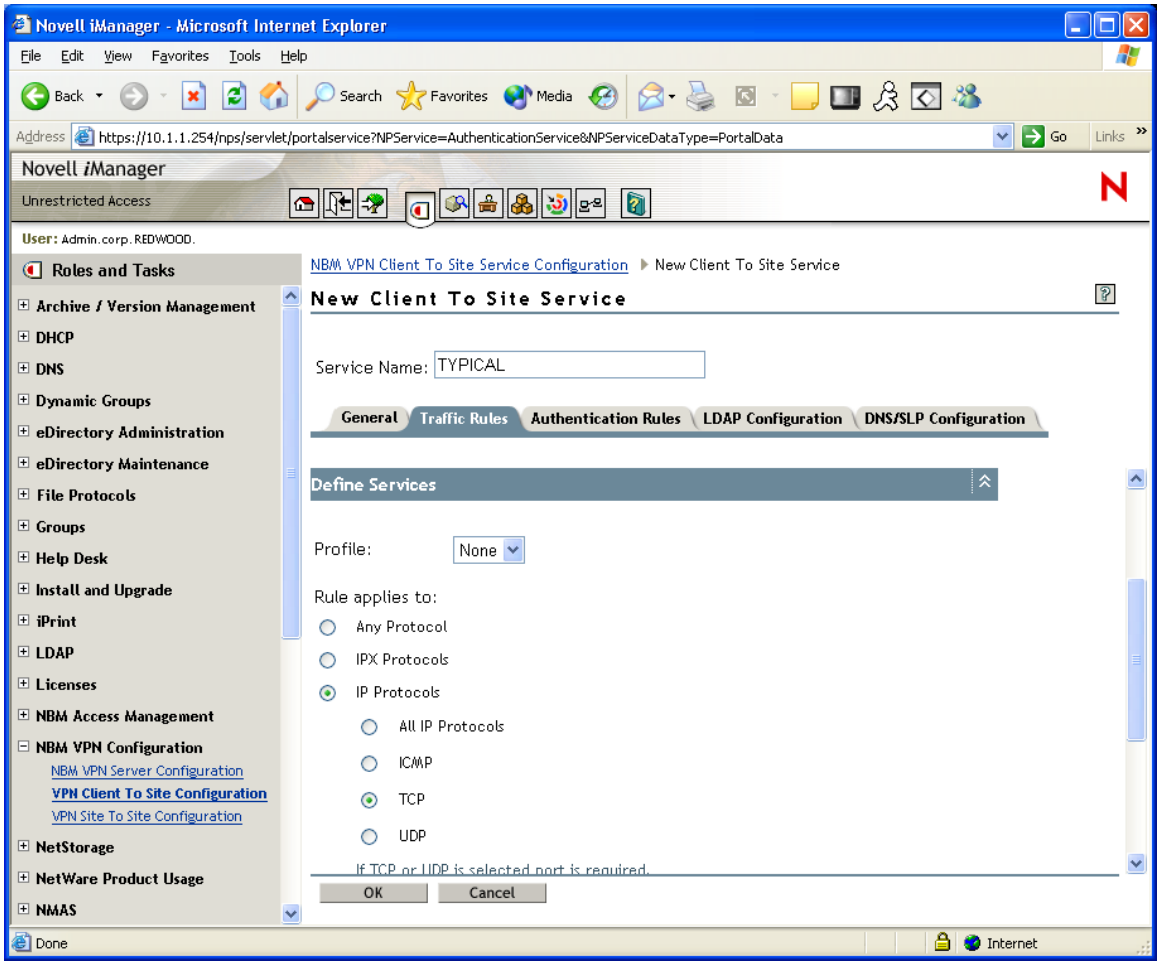
Collapse the **Define User** section.



Expand the **Define Destination** section.

Select **Only Use IP List** here, and add an **IP address range** of **10.1.1.100 to 10.1.1.100**.

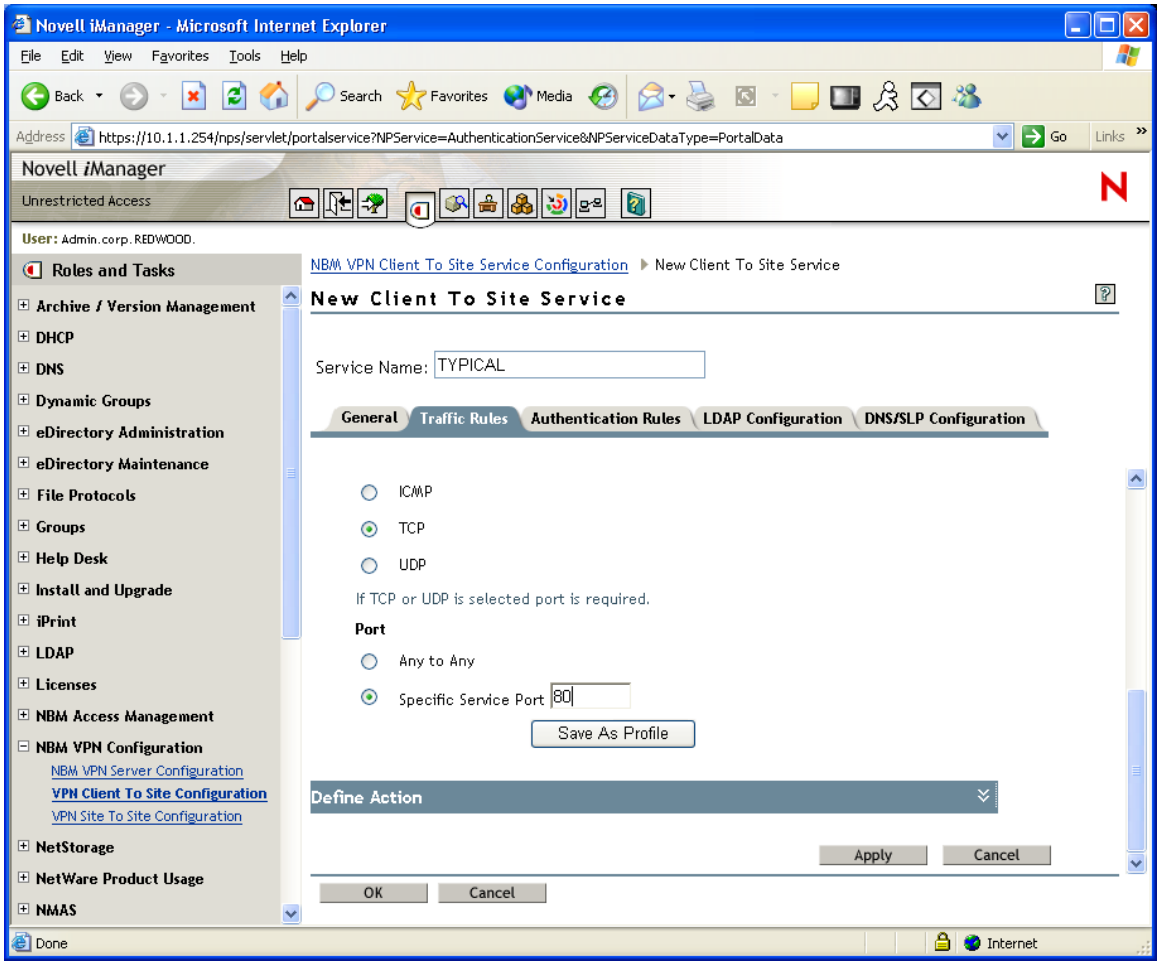
Expand the **Define Services** section next.



Here we must specify ports **80** and **443**.

Select **IP Protocols** and then **TCP**.

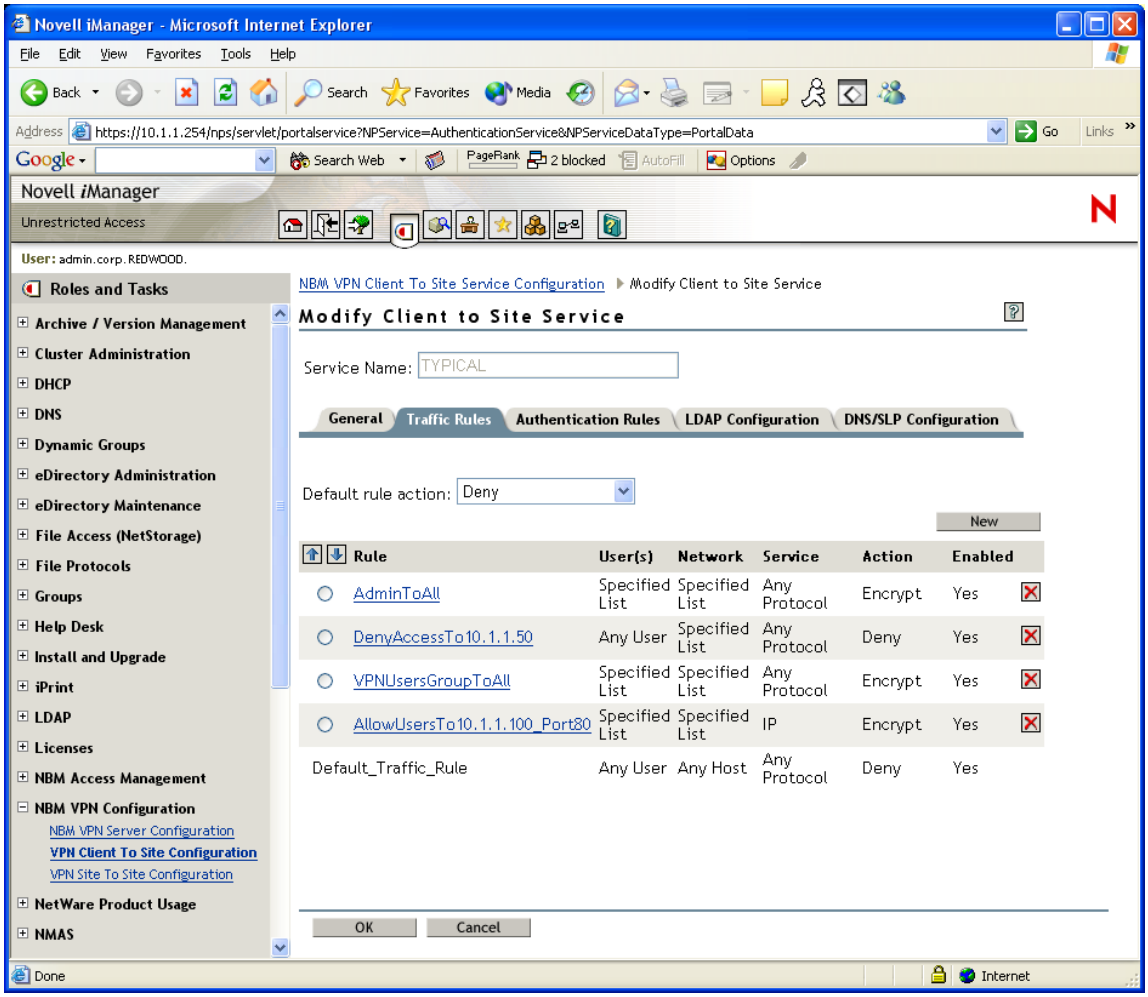
Scroll down farther in the window.



Note You can only enter one port number in the Port field. To allow access to ports 80 and 443, we will have to add two separate rules.

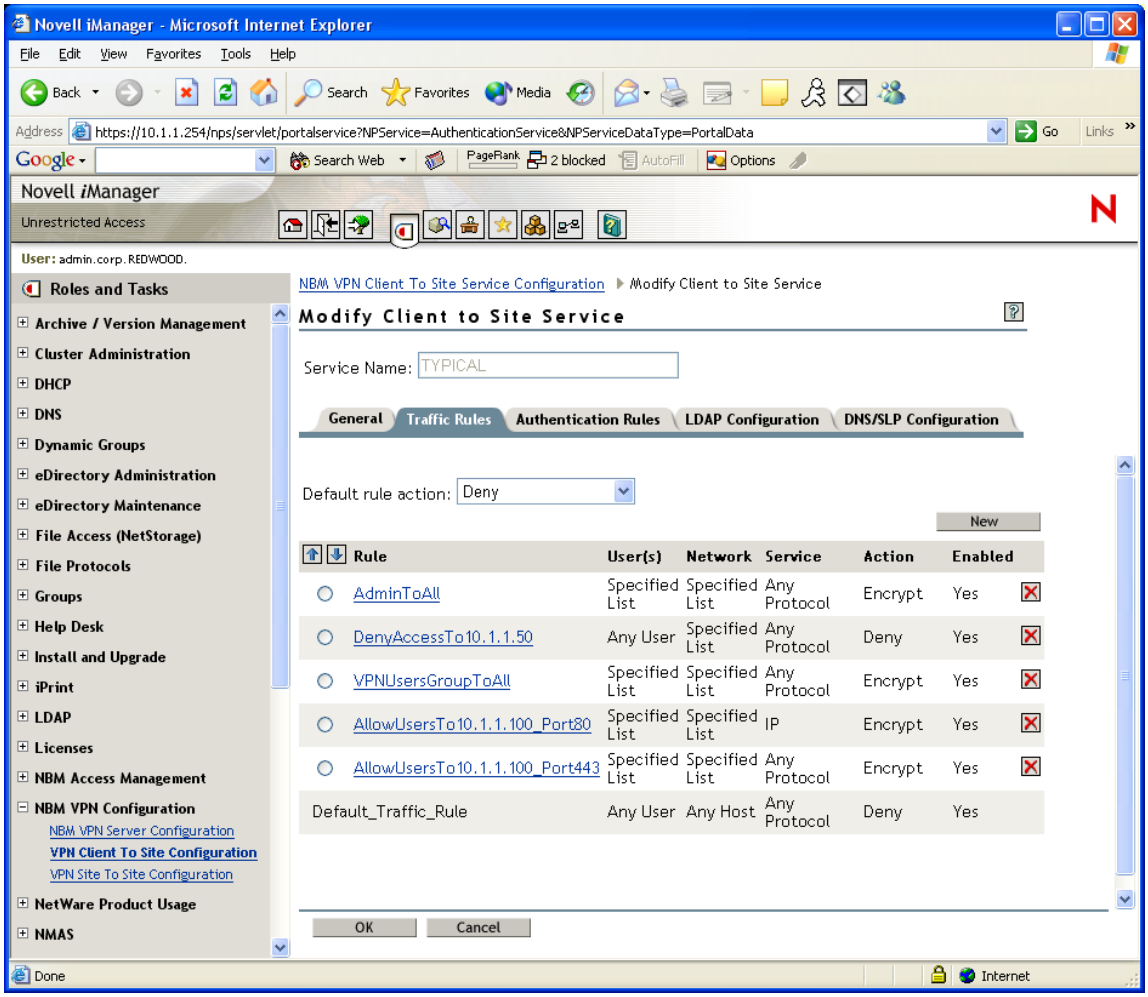
Under **Port**, enter port **80** in the **Specific Service Port** field.

Click **Apply**.



We have now allowed port 80, but need to allow 443 as well.

Add another rule in the same manner as the previous example. (The procedure is not shown here).

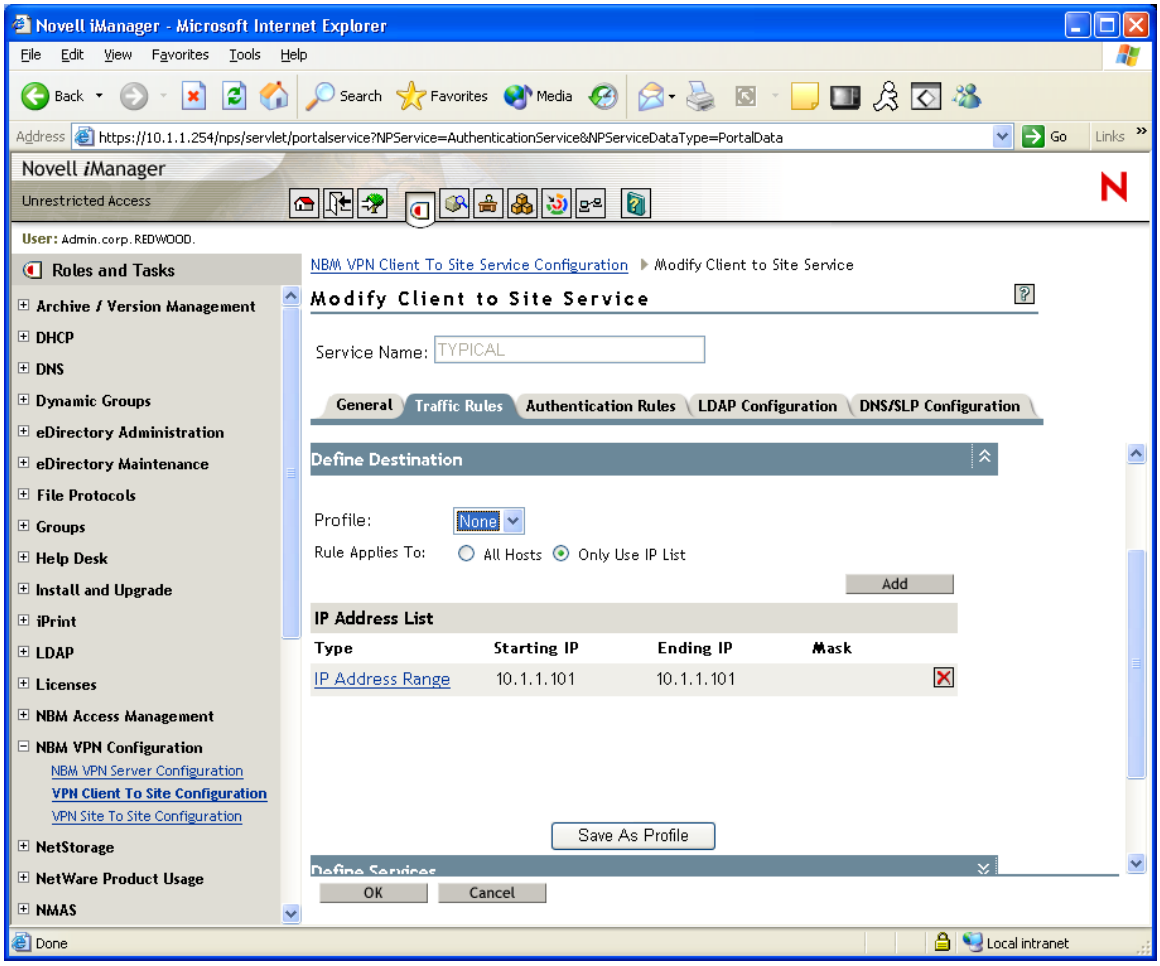


After allowing port 443 to 10.1.1.100, click **New** to add one more rule, for iFolder traffic.

Traffic Rule – Allow Any User to iFolder Server

Add another new rule, and name it **AllowAnyone2iFolder**. Or something else nice and descriptive!

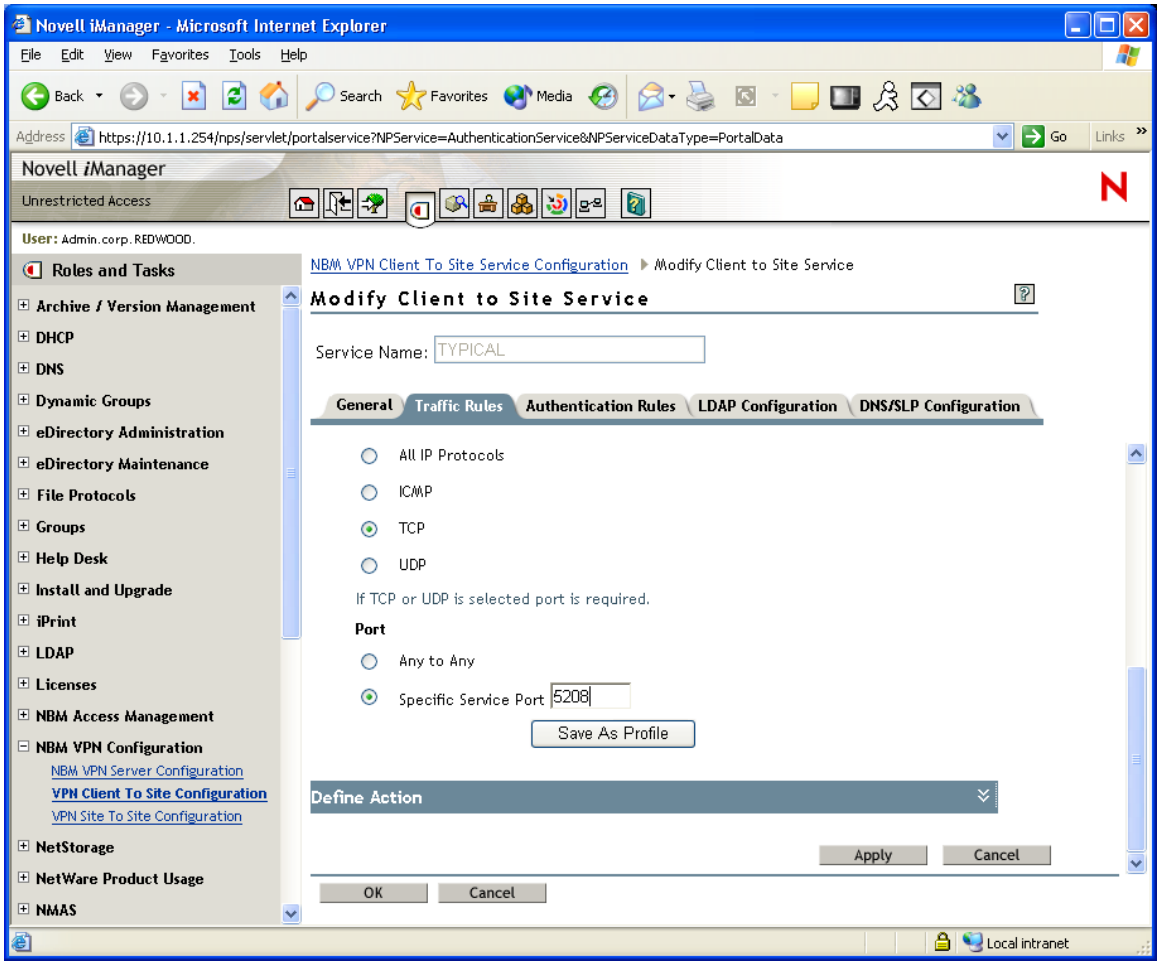
Expand the **Define Destination** section.



Select **Only Use IP List**.

Click **Add**, and add an **IP address range** of **10.1.1.101 to 10.1.1.101**.

Collapse the Define Destination section, and expand the **Define Services** section.



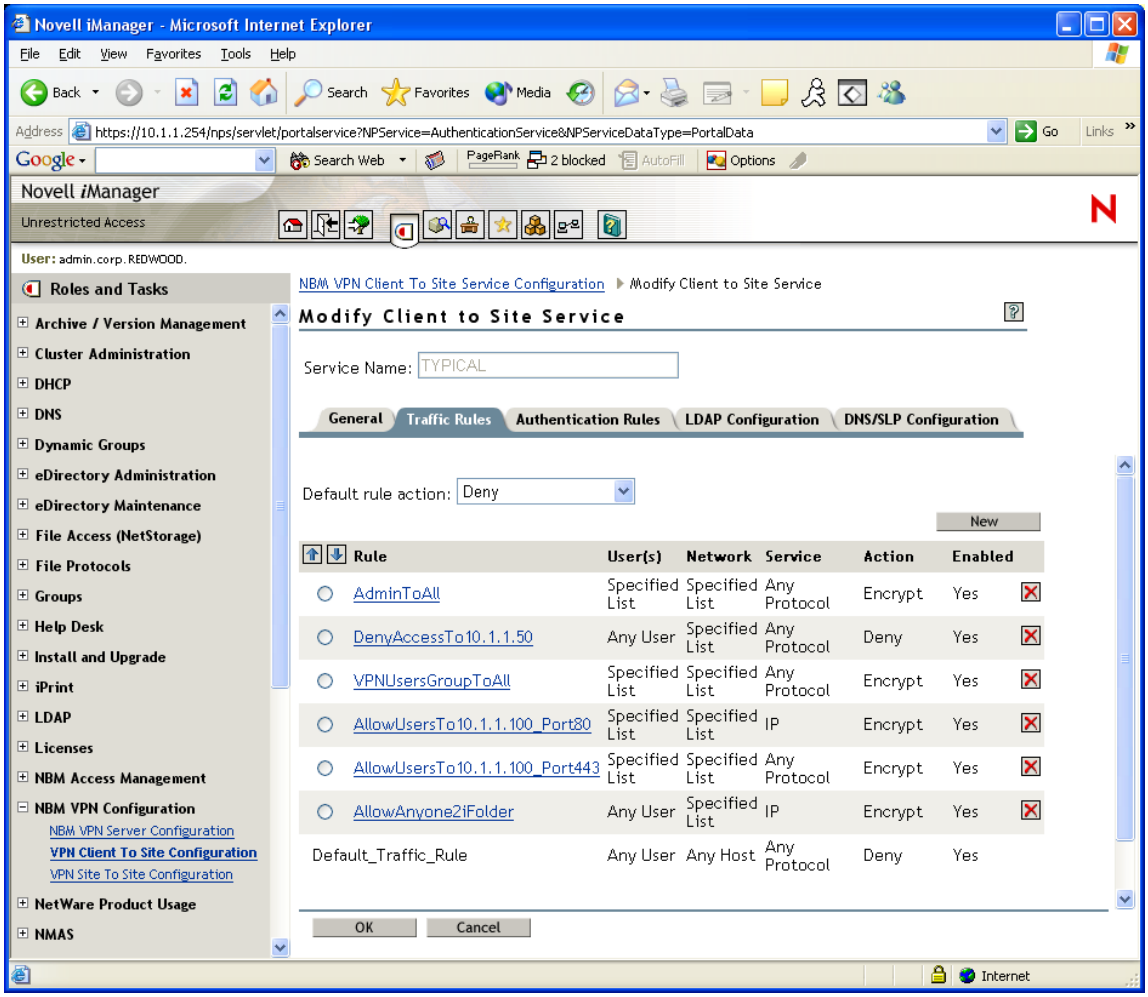
Here we find a limitation. You cannot configure more than 4 digits in the Specific Service Port field! This means that the idea of allowing only port 52080 and 52443 cannot be done at this time.

As of this writing, there are no patches out for BorderManager 3.8 that change this behavior. Novell TID

For now, you have a choice of choosing all TCP ports or allowing even more protocols to the server. (Or consider reconfiguring the iFolder server to listen on a secondary IP address on ports 80 and 443.)

For now, choose **Port, Any to Any**.

Click **Apply**.



We now have all but one of the traffic rules in place, in a sequence that will work.

If you do not want remote users to be able to connect to any other hosts besides the ones allowed in your traffic rules (meaning: they cannot browse the Internet, or access hosts local to their network), you can click OK and use these traffic rules.

Since we want to allow remote users to browse the Internet while connected to the VPN, we need to add another traffic rule.

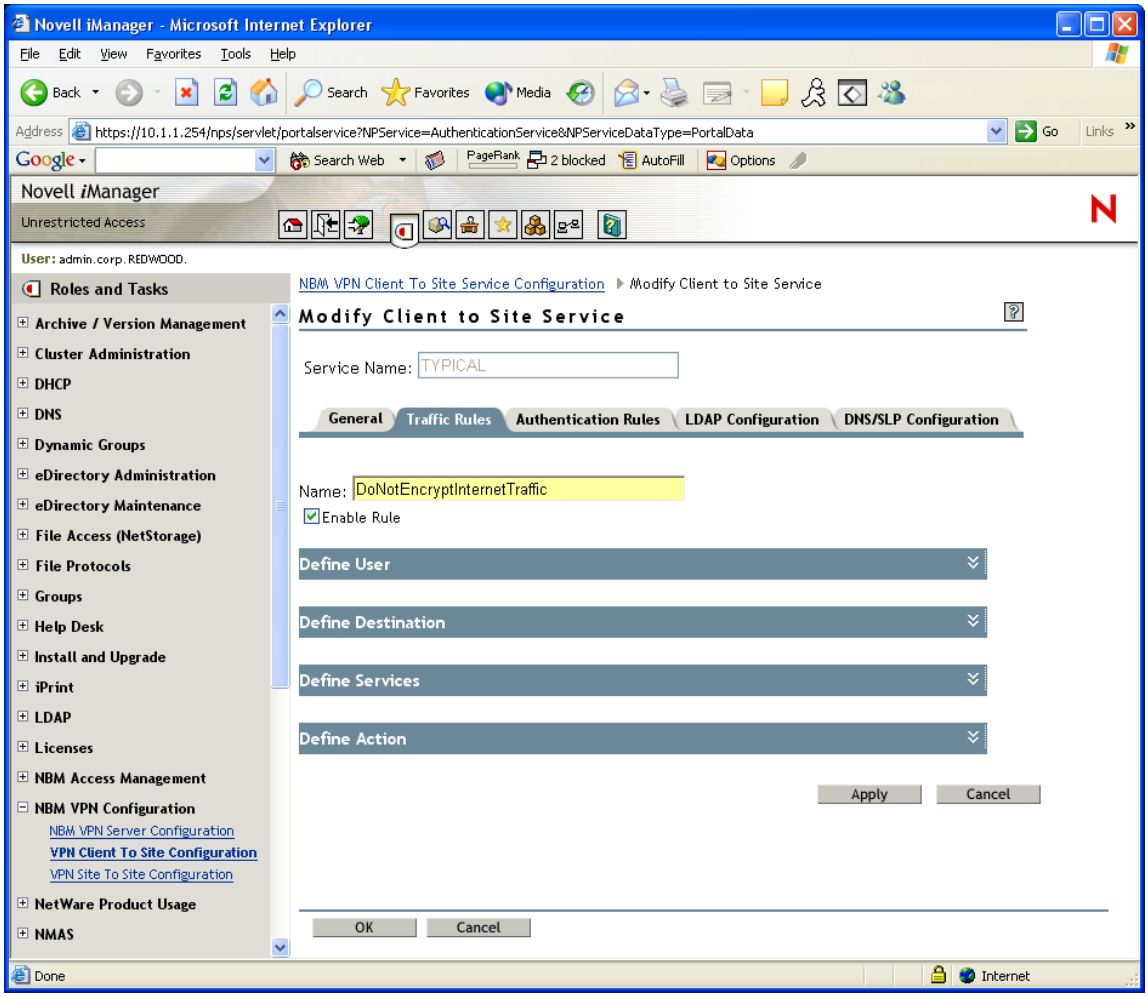
Click **New**.

Optional Traffic Rule – Do Not Deny Non-VPN Traffic

The purpose of this rule is to allow remote VPN clients to be able to access hosts (local, or Internet) that are not behind the BorderManager VPN server. This is the equivalent of the 'protect only networks listed below' in the legacy Client-to-Site configuration.

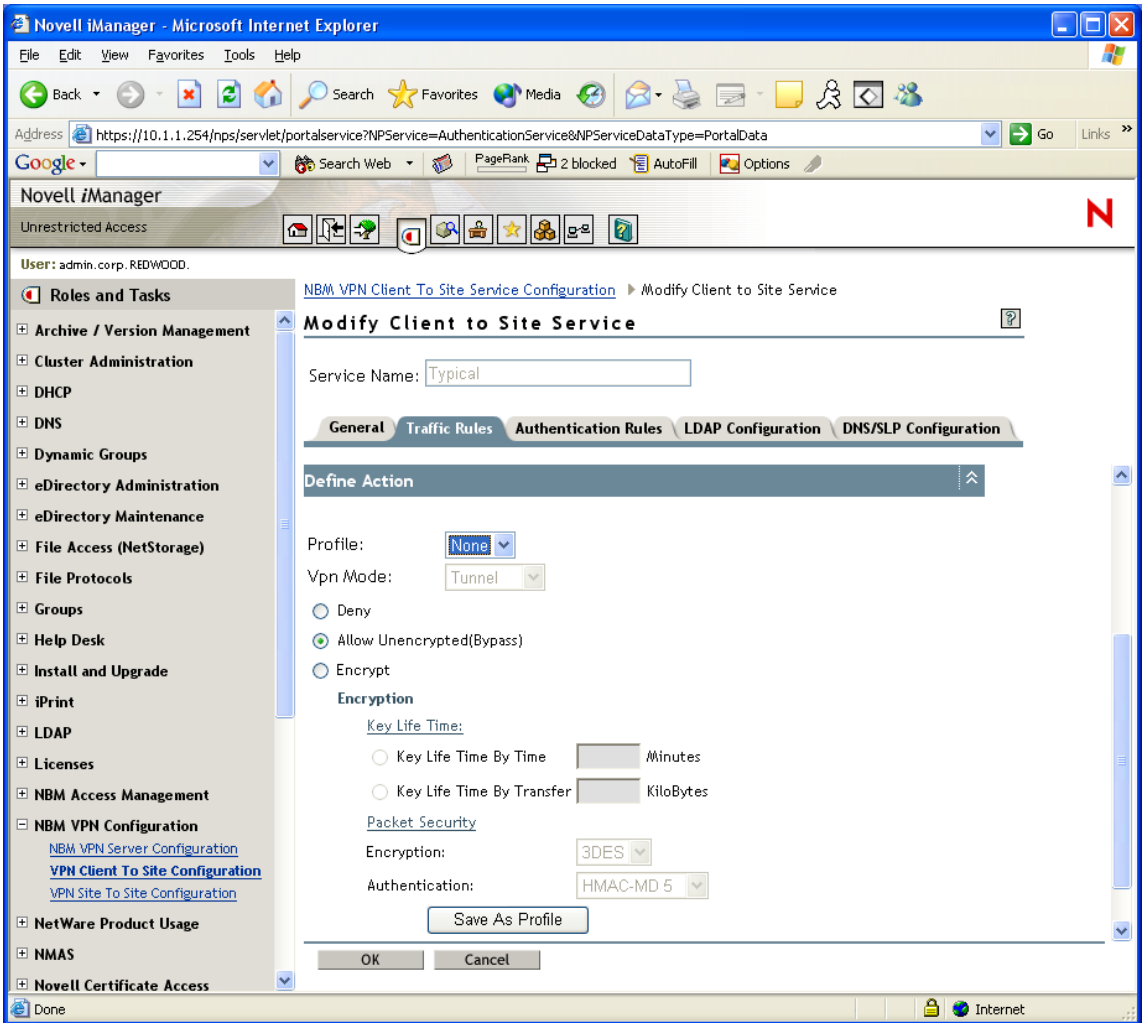
If you make a VPN connection that includes a few rules to encrypt traffic to your internal network, all other hosts will be denied by the default traffic rule. This has the effect that traffic to Internet hosts, or local area network hosts gets denied until you disconnect the VPN connection. While this is a good security feature, it also can be a problem, especially if the remote client needs to have access to a server on his/her local network while connected to the VPN.

The solution to this problem is to add a traffic rule just above the Default rule to not encrypt IP traffic. (This is also known as a 'bypass' rule). You must have structured the rules above it to only specify the networks behind the BorderManager server – not All Addresses.



Give the rule a descriptive name.

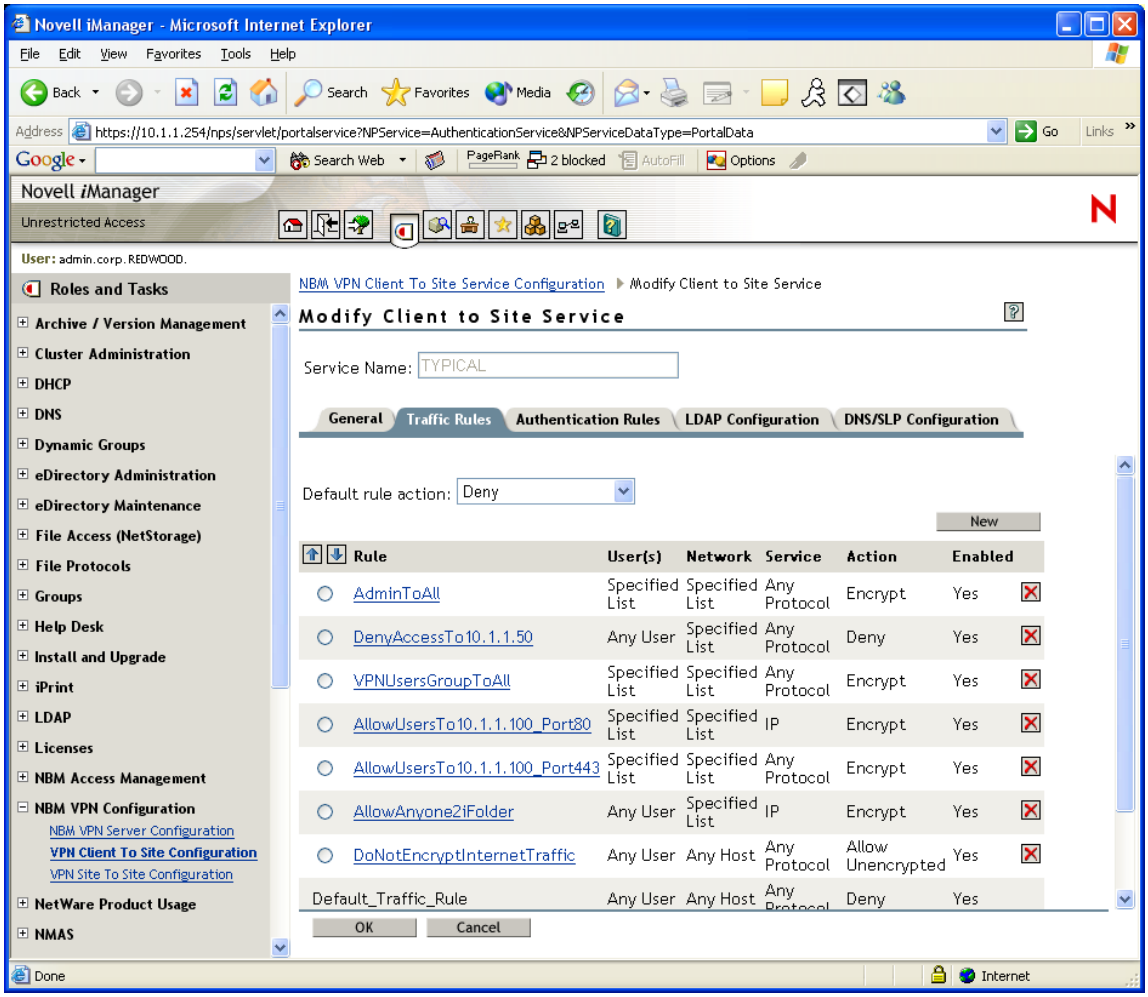
In the example shown here, a rule is created called **DoNotEncryptInternetTraffic.**



The only non-default setting in this traffic rule is shown above in the **Define Action** section of the Traffic Rule.

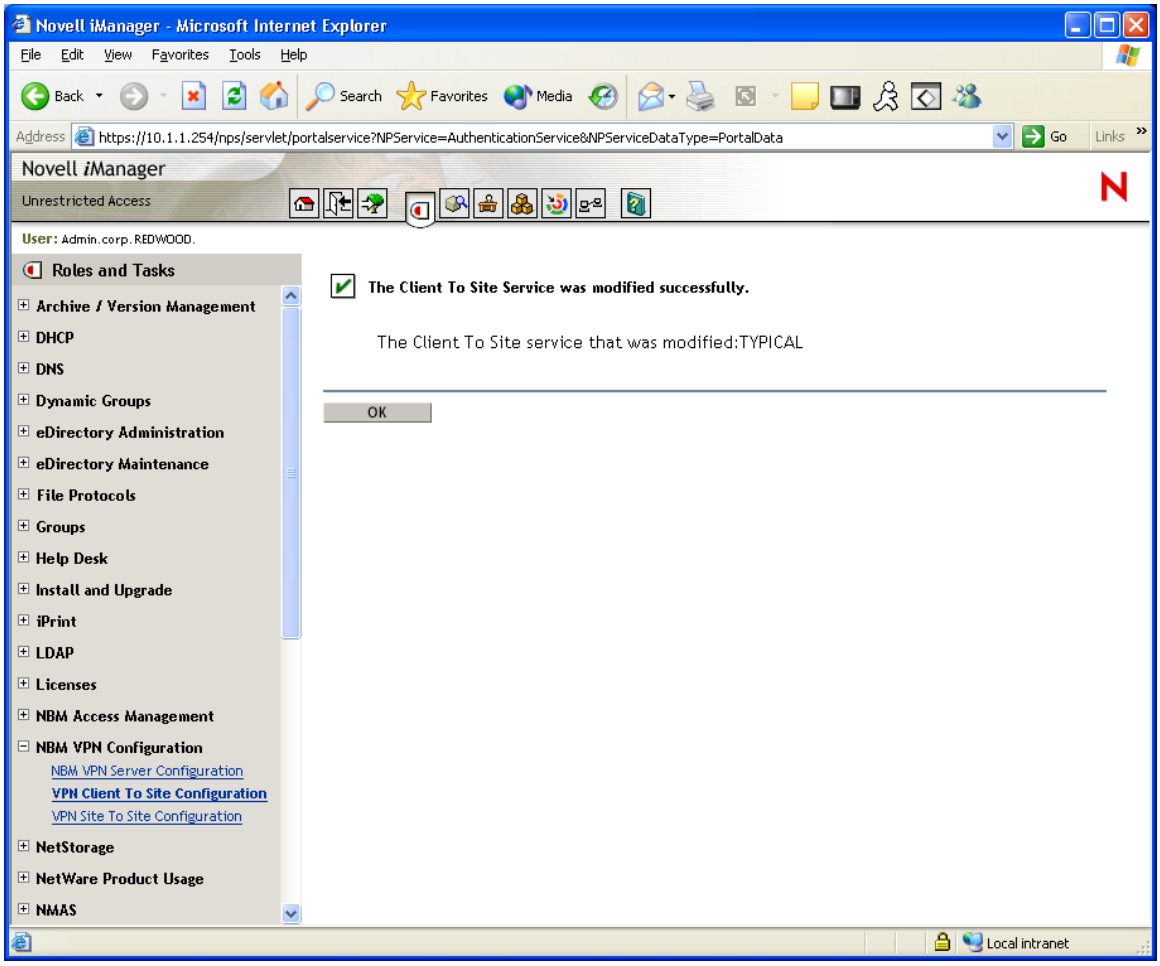
Select **Allow Unencrypted (Bypass).** Any traffic not already affected by a rule above this one in the list will bypass the VPN. That is, it will not be sent over the VPN.

Scroll down and click **Apply**.



Now we see all of our traffic rules, in the order (top to bottom) that they should apply. Note that several rules will apply only to NMAS-authenticated users, while others (the ones that do not specify a user list), will apply to LDAP- or Certificate-authenticated users as well.

Click **OK** to save these changes to the VPN.



If you have not saved the configuration before this point, you should see a message that a new service was saved.

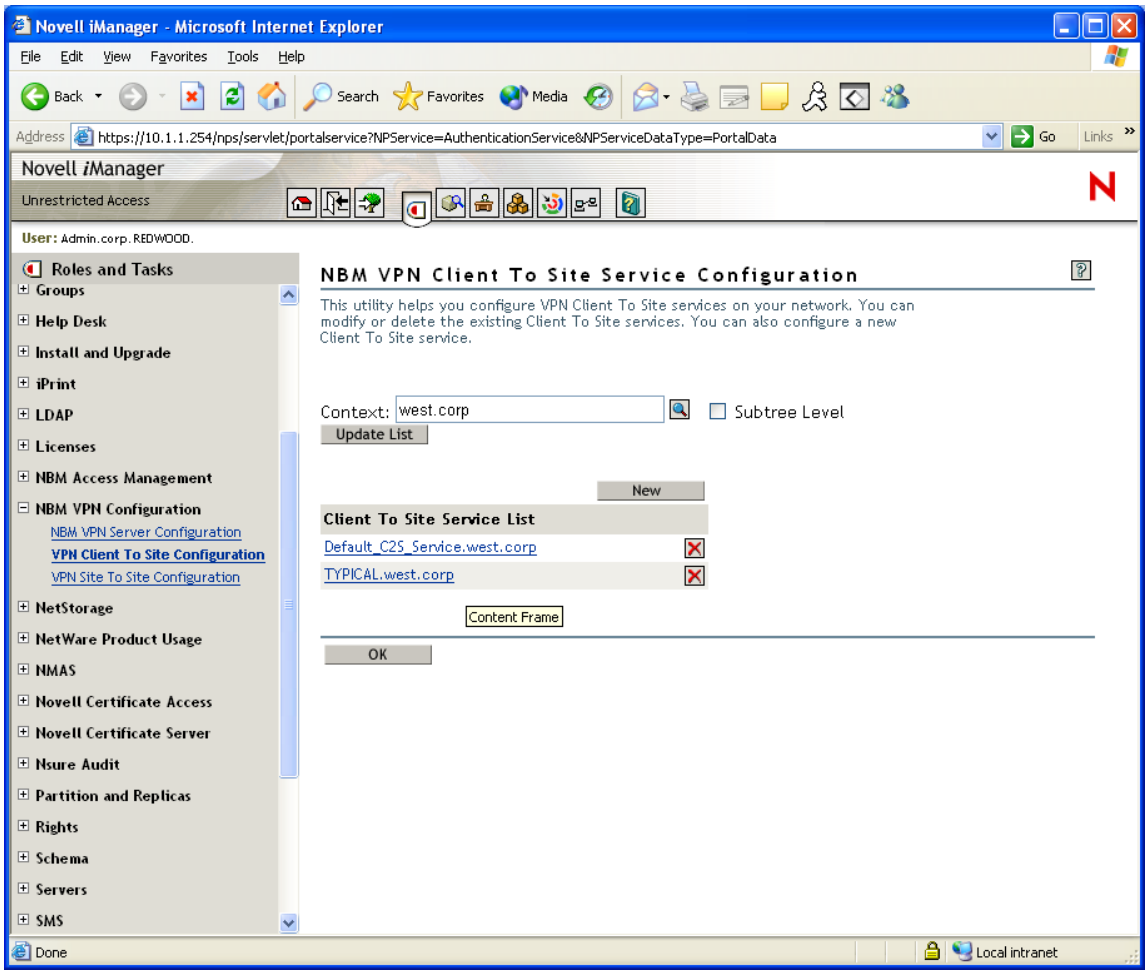
If you have saved the configuration previously, you should see a message that the client-to-site service was modified, as in the example shown above. The changes are saved to service called TYPICAL.

Click **OK**.

Configure Client-to-Site Authentication Rules

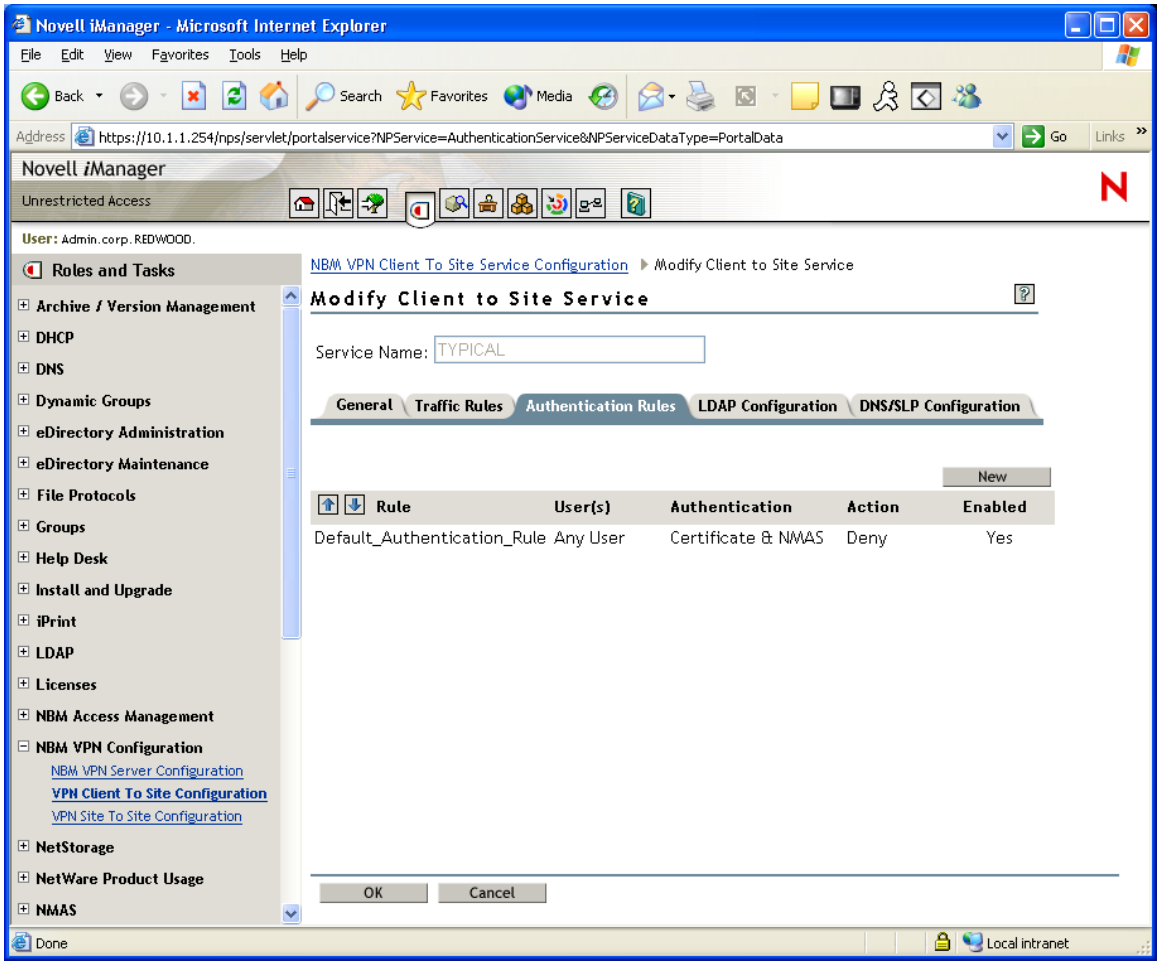
We have configured some Traffic Rules, but not any Authentication Rules. The Authentication rules are necessary to determine who can authenticate to the VPN. Once authenticated, the traffic rules apply.

Go back to the VPN Client-to-Site Configuration in iManager and bring up the **Client To Site Service List**.



Select our new Client-to-Site service called **TYPICAL** from the service list to continue with the configuration.

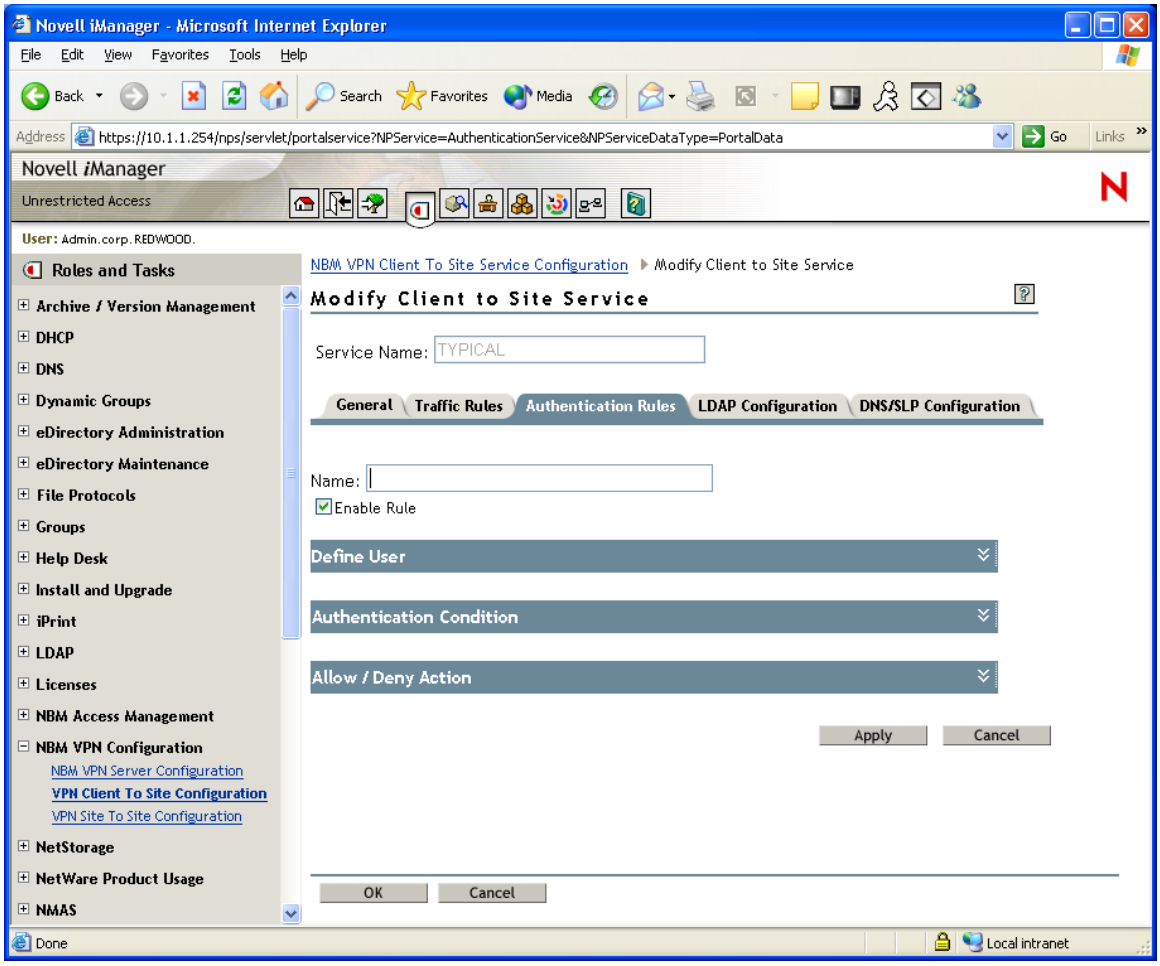
Select the **Authentication Rules** section.



There is a default Deny rule, to prevent any user from having access unless you specifically add a rule to grant some sort of access. If we do not add another rule here, no one can authenticate to the VPN.

The **Traffic Rules** defined what could happen once the VPN connection was made. The **Authentication Rules** define who and how someone gets to authenticate.

Click the **New** button to add a new rule.



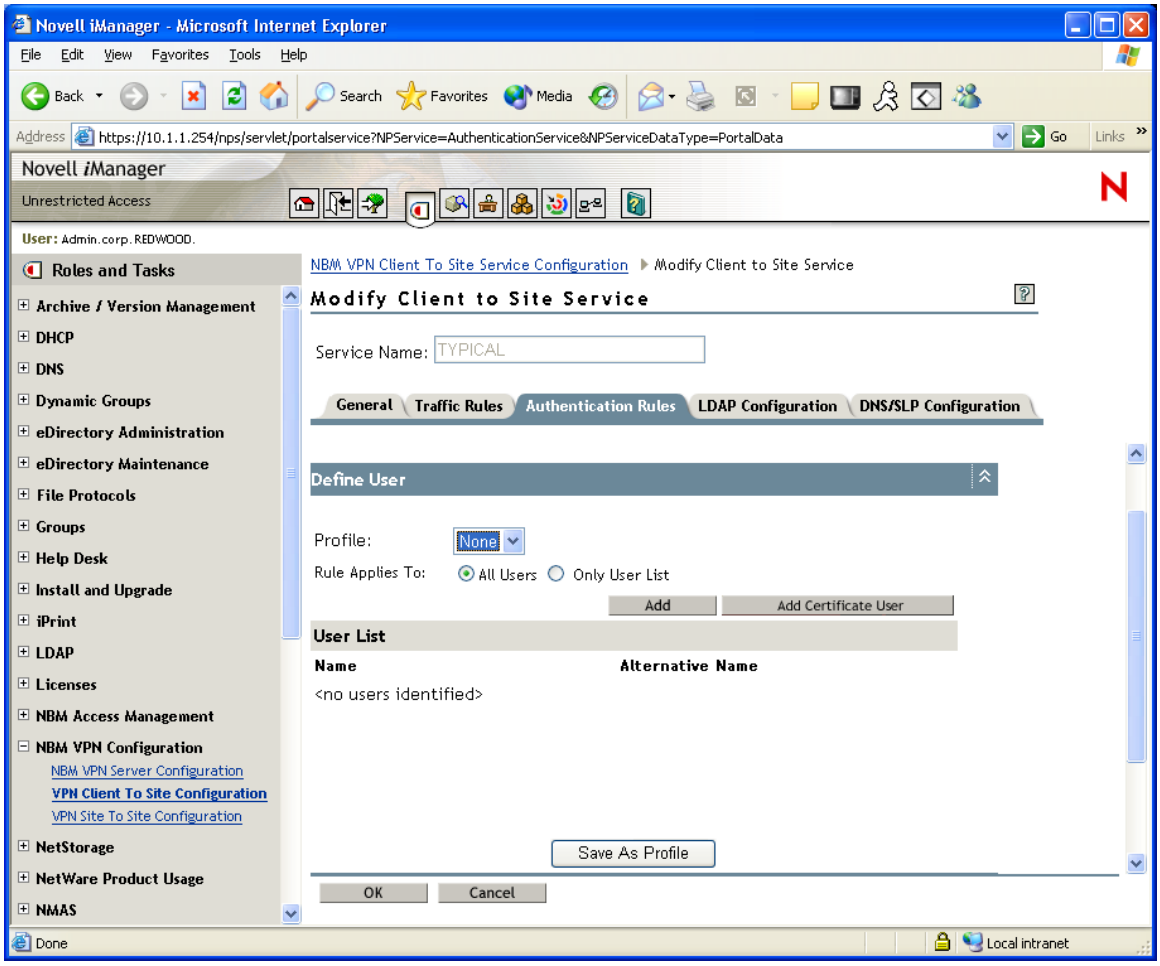
We must name the rule (naturally), and then we will be able to specify particular users or groups in the Define User section and what sort of authentication method those users can use in the **Authentication Condition** section.

The **Authentication Condition** essentially gives a choice of **NMAS** or **Certificate** methods for authenticating a user to the VPN. For this example, we wish to allow NMAS only. An example of allowing certificate access is shown later in this chapter. The simplest form of NMAS authentication is an NDS password.

The **Allow/Deny Action** does what you might expect – allow or deny a user to use some authentication method.

Name the rule **AllowNMAS**.

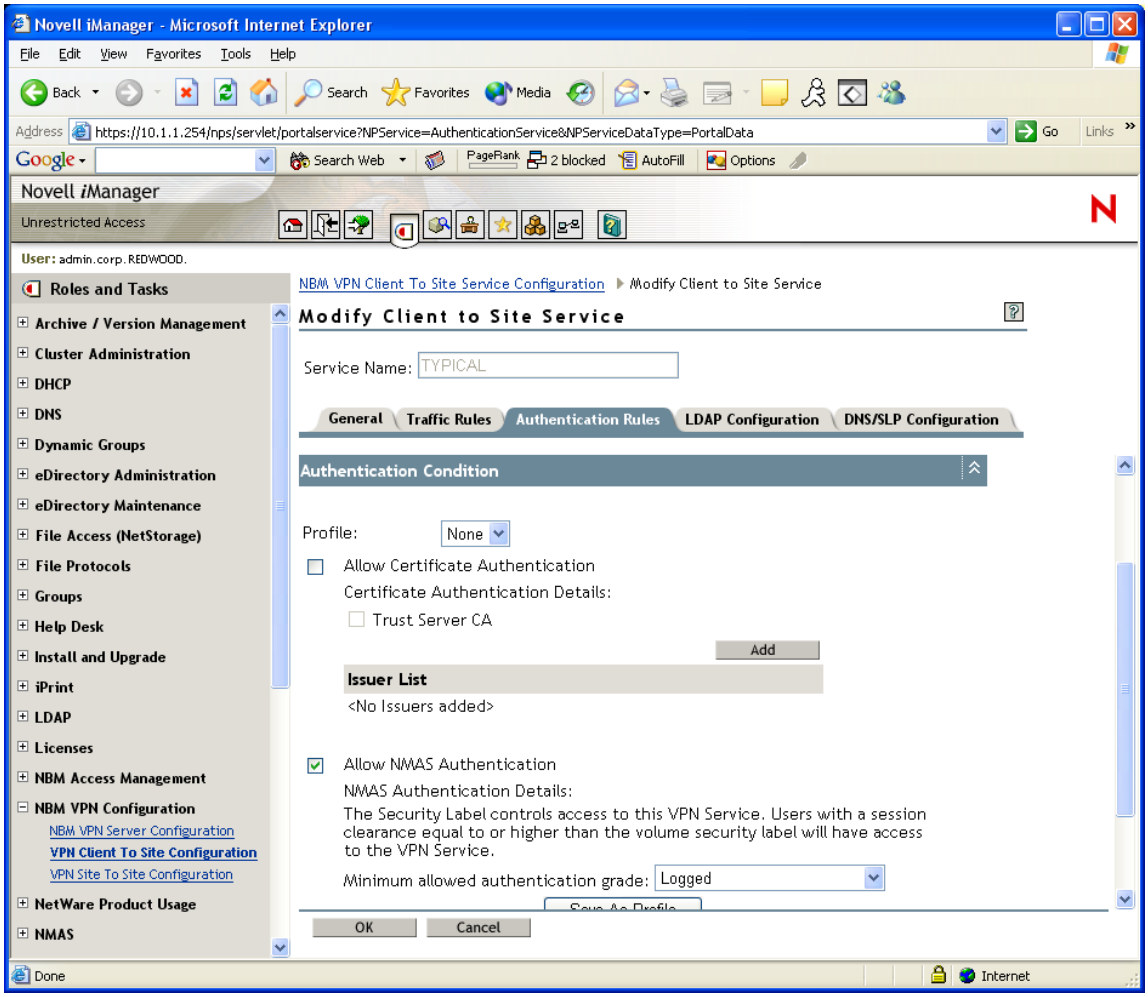
Expand the **Define Users** section.



We can authenticate all users, selected users, a group, or we can authenticate by means of a user certificate. (I show an example of certificate user later in this chapter.)

For now, we want to cover as many users as possible by as many methods as possible, so we will leave the default setting in place. This will allow anyone in the same NDS tree as the VPN server to authenticate.

Expand the **Authentication Condition** section.



There are options to **Allow Certificate Authentication** and **Allow NMAS Authentication**.

Certificate Authentication does not require that the user have an NDS user account in the server's NDS tree. An example of certificate-based authentication is shown later in this chapter.

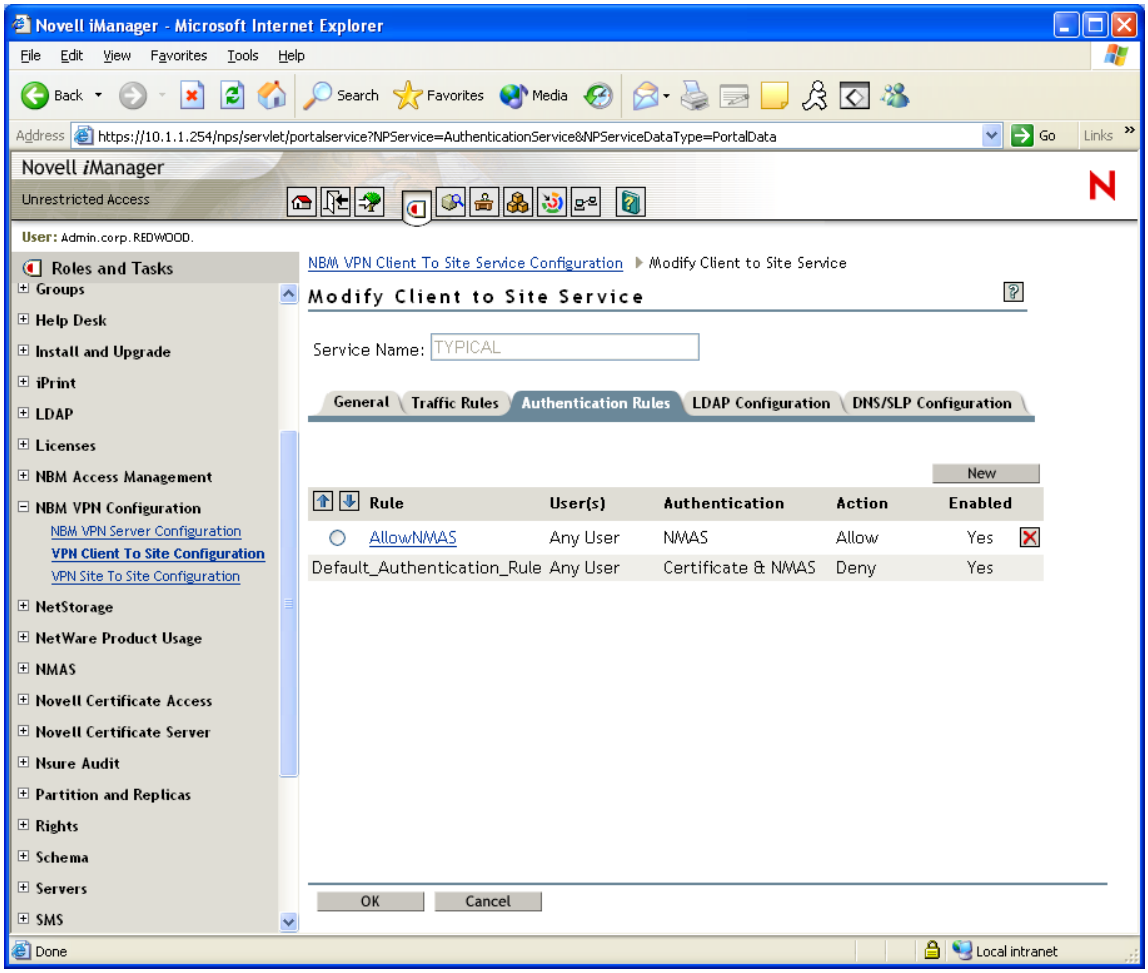
NMAS Authentication implies that the client has some sort of Novell NMAS client, and logs into the VPN server's NDS tree. There are various NMAS authentication methods available, but the simplest one is NDS password. Only NDS password is covered in this book.

Select the **Allow NMAS Authentication** option to allow authentication of VPN clients using an available NMAS method.

Since we want to make things easy to start with in authentication methods in this example, leave the **Minimum Allowed Authentication Grade** to **Logged**. As of this writing, BM38SP1A is the latest BorderManager patch, and selecting the NMAS authentication grade method of Password causes the VPN client to

fail with an error. Later patches may fix this issue, but you should test changes before allowing production use.

Click **Apply** to save the changes.

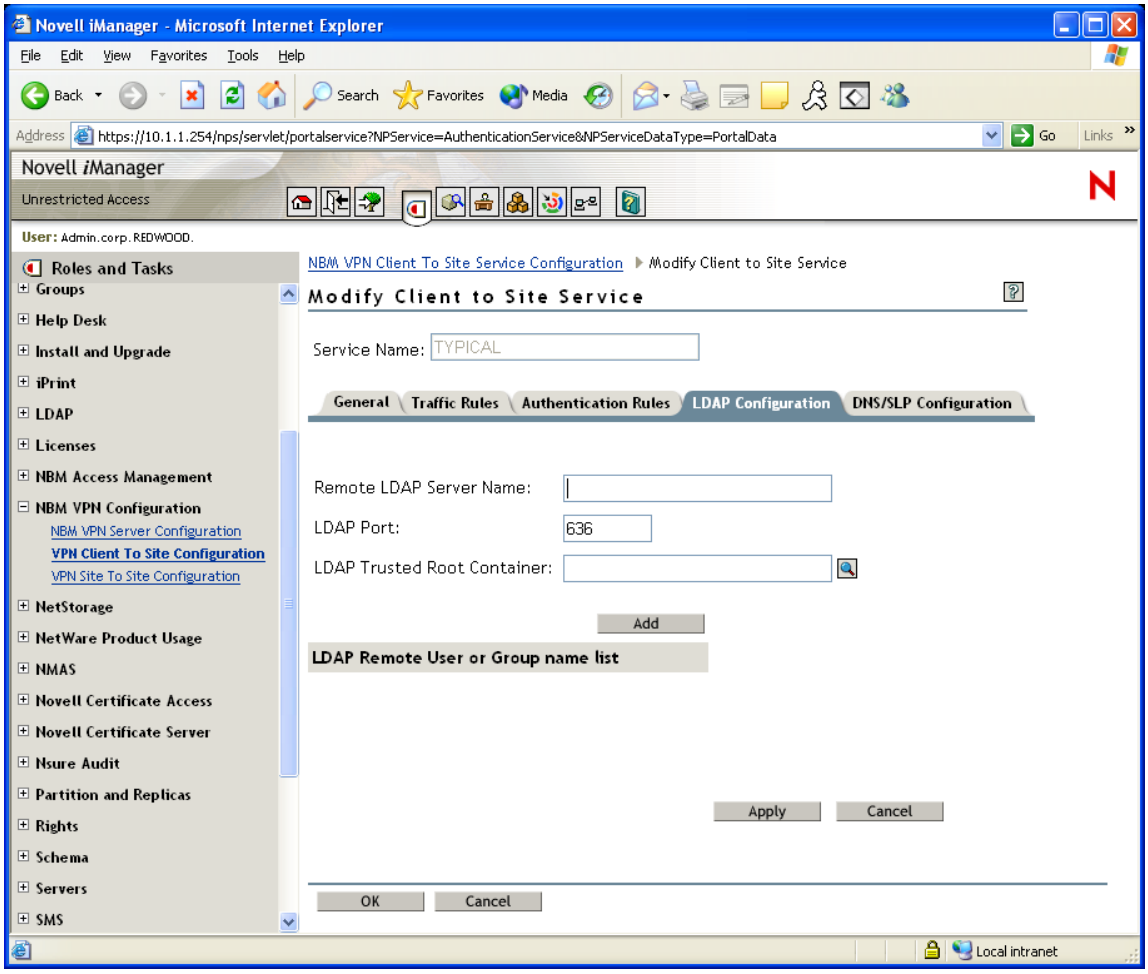


At this point most of the critical settings are in place to use NMAS authentication (simple user ID/password login) for the VPN client.

If you click on OK now, the settings would be saved, but we would still be missing some useful parameters.

Click on **LDAP Configuration** to look at that menu.

LDAP Configuration



The LDAP Configuration menu is used to allow remote VPN users to authenticate to a different server than BorderManager, using LDAP queries.

This option provides a means to authenticate users in another directory service, since they do not have to be members of the same NDS tree as the BorderManager server.

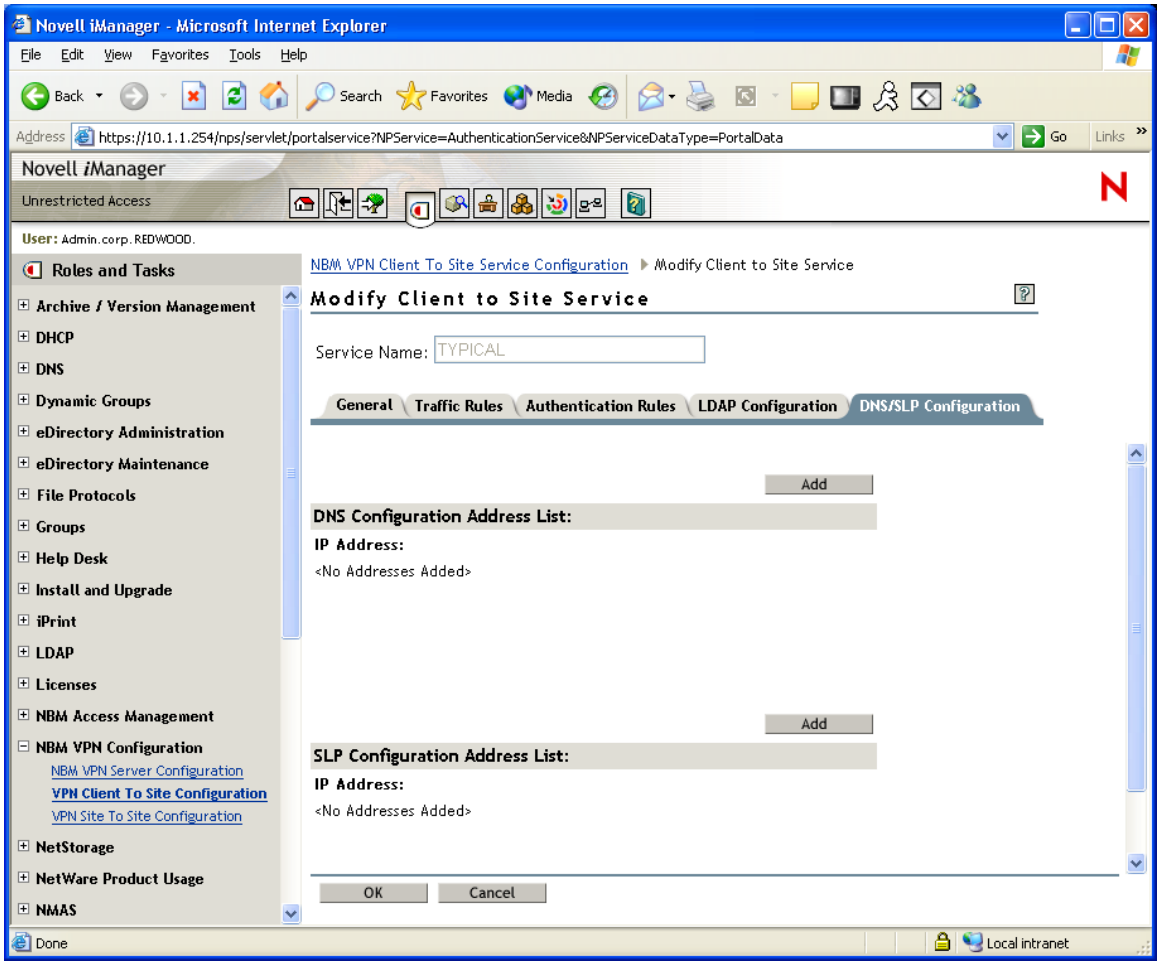
LDAP authentication can be used to authenticate VPN users to other NDS trees, Active Directory, or any LDAP-compliant directory. However, there are noticeable limitations in how you can apply both authentication and traffic rules. See the Limitations section at the beginning of this chapter.

LDAP configuration examples are shown later in this chapter.

Click on **DNS/SLP Configuration**.

DNS/SLP Configuration

Now we come to the final bits of the configuration we need to make a useful Client-to-Site VPN service definition. In a small network, these settings could be ignored, or may be optional. In larger networks, they become essential.

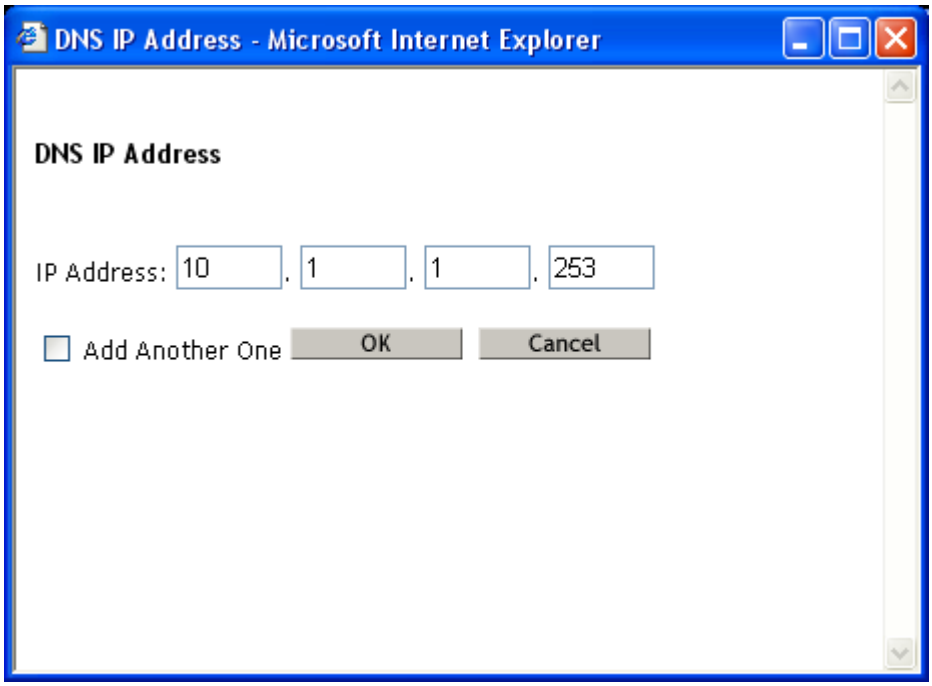


With the DNS/SLP Configuration options set, you can push your internal DNS server addresses to be used by the VPN client while the VPN connection is up, giving the remote client the ability to do name resolution using your internal DNS servers. This allows the VPN user to connect to internal web sites by URL, among other things.

The SLP configuration option allows you to push Directory Agent settings to the client, for the duration of the VPN connection, giving the remote client the ability to do name resolution using your internal SLP directory agent. This makes it much easier to log into NetWare servers by name.

These options provide a tremendous improvement compared to previous versions of BorderManager in terms of being able to resolve internal web server addresses and log in to NetWare servers, using SLP name resolution.

There are some limitations to these features, as described in the beginning of this chapter. You should review them. You should also review the Troubleshooting chapter for some issues seen with these features as of this writing.

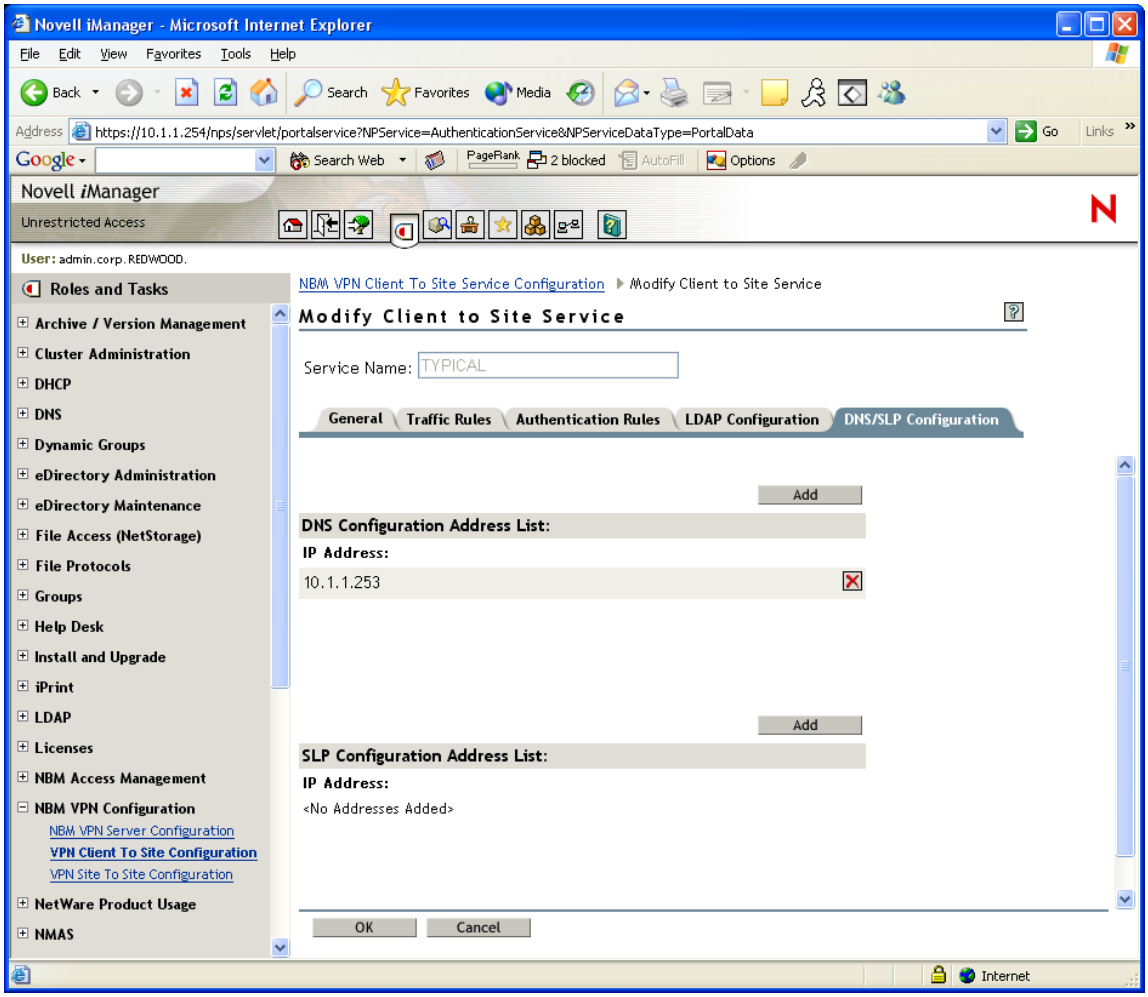


Click the **Add** button in the **DNS Configuration Address List** section to add a DNS server IP address. The IP address of an internal DNS server is added.

In this example, the address is that of the VPN server itself. That server must be running NAMED or DNS Proxy.

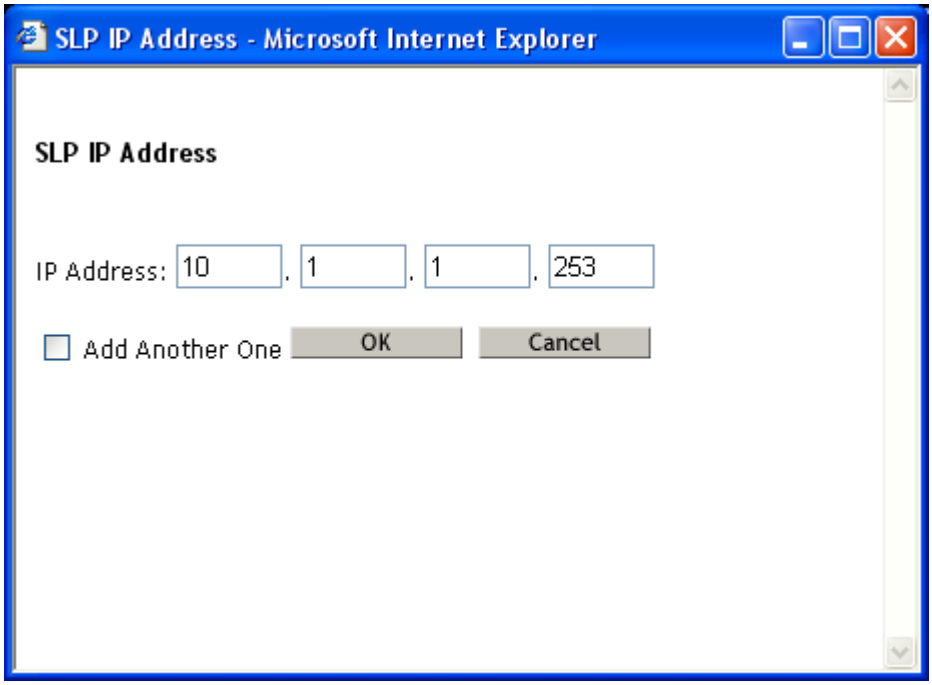
Be sure you have traffic rules that allow these hosts to be accessed!

Note As of this writing, with BM38SP1A, NW65SP1, and TCP654REV2 patches applied to the BorderManager server, there is a bug that prevents me from accessing the primary private IP address of the BorderManager server through the Client-to-Site VPN, if NAT is enabled on the server. Novell is working on a fix, but the old trick of static NATing the private IP address to itself does not work. For now, I have a simple work-around: instead of connecting to the primary private IP address, I add a secondary IP address (10.1.1.253) to the private side of the BorderManager 3.8 server, and then I use that value instead of the primary address for proxy, DNS, SLP DA, or logging into the server over the VPN connection.



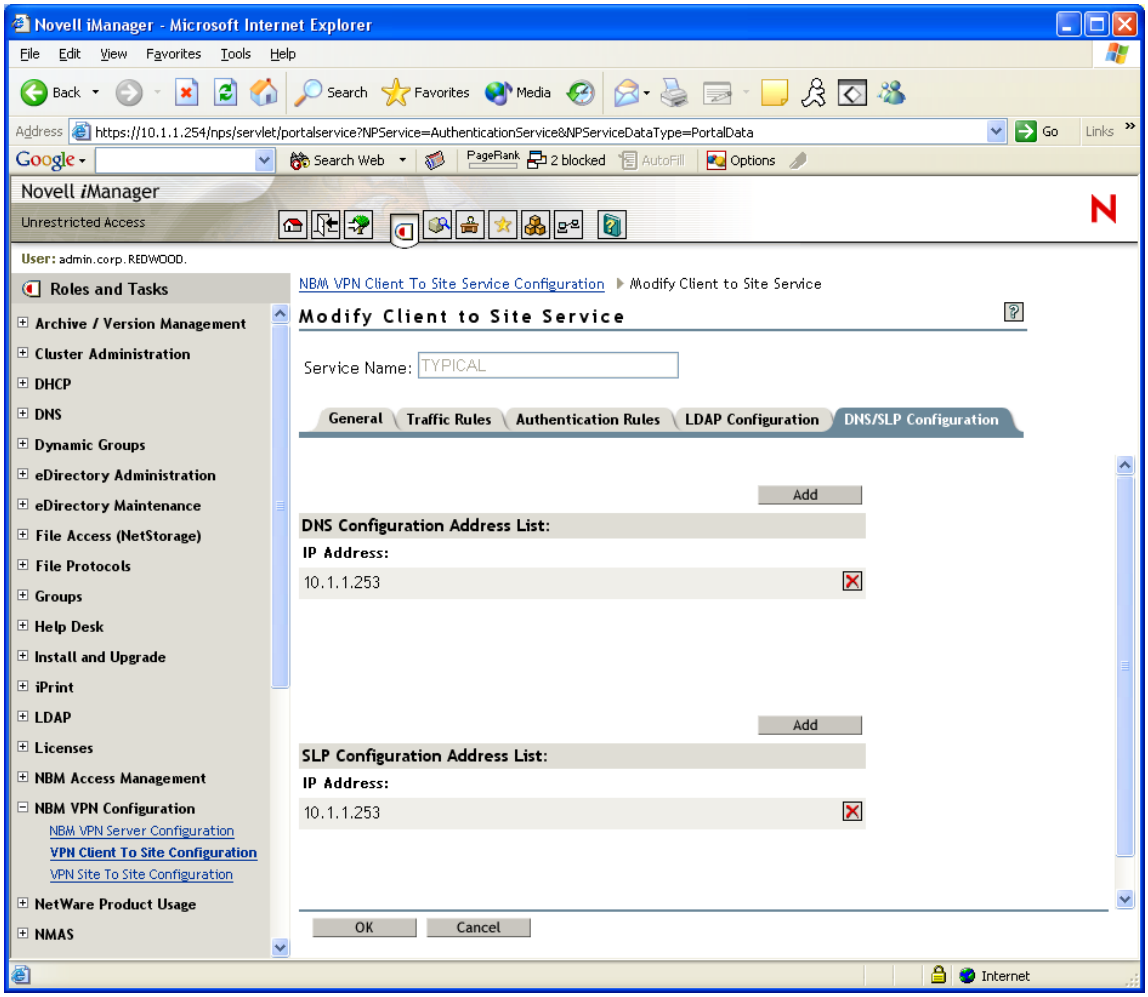
Note A DNS server IP address is added.

Click **Add** in the **SLP Configuration Address List** section to add a SLP Directory Agent IP address.



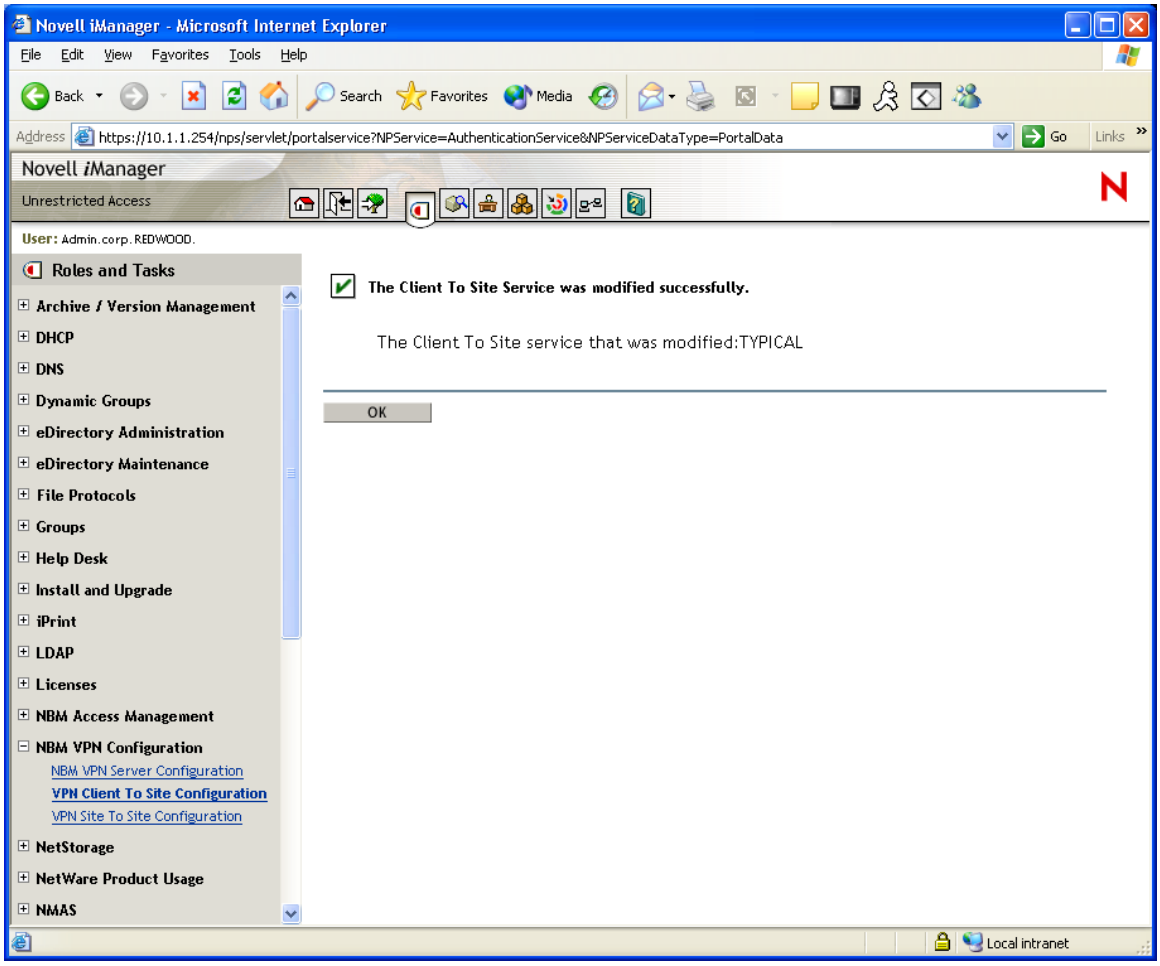
Configure the IP address of a **SLP Directory Agent**.

In this case, the internal IP address of the VPN server is used. That server must be running SLPDA.



In this example, the internal IP address of the VPN server is used for both choices.

Click **OK** to save the settings.

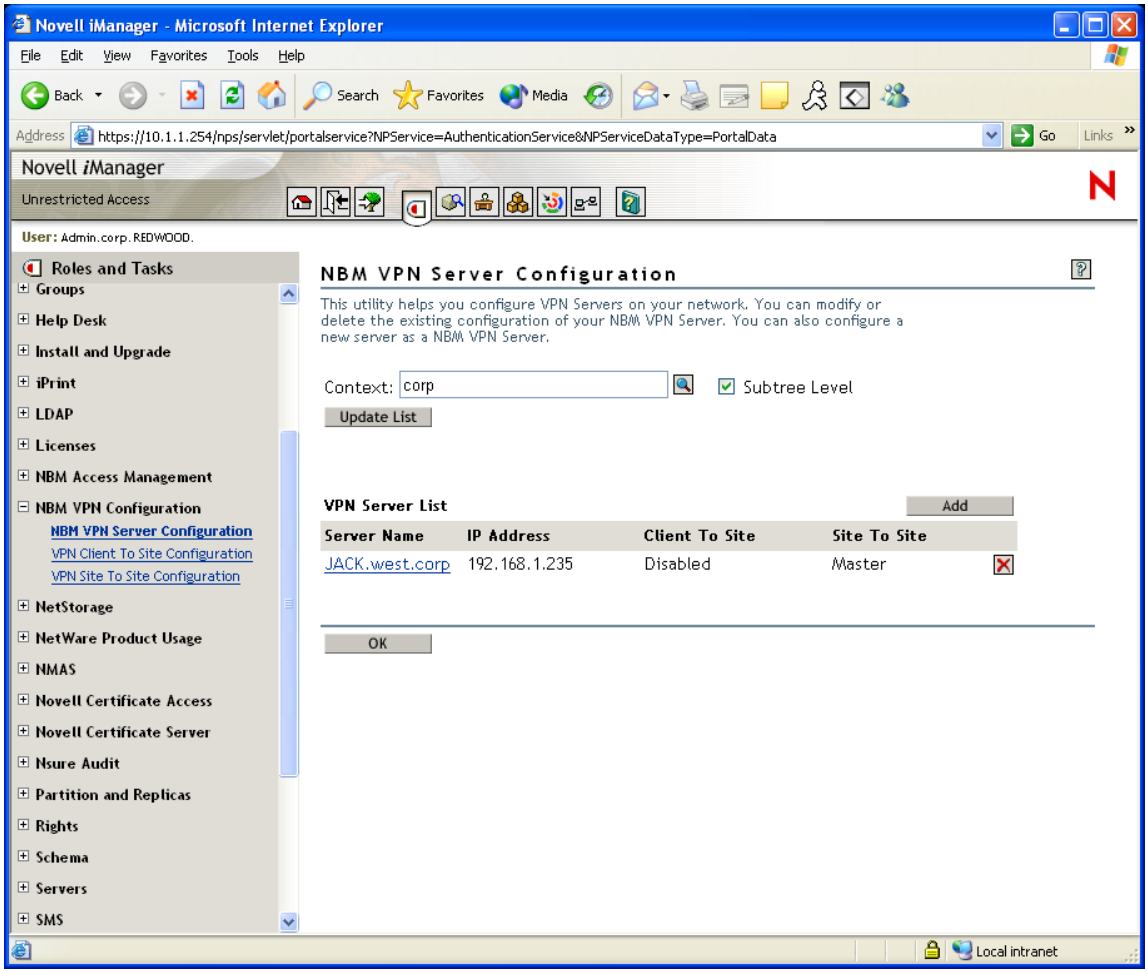


Client-to-Site VPN is now ready to be assigned to the VPN server.

Remember that up to this point, the VPN server JACK is not configured for Client-to-Site VPN.

Assign the Client-to-Site VPN Service to VPN Server JACK

Once the Client-to-Site VPN service has been configured, we need to assign it to a server.

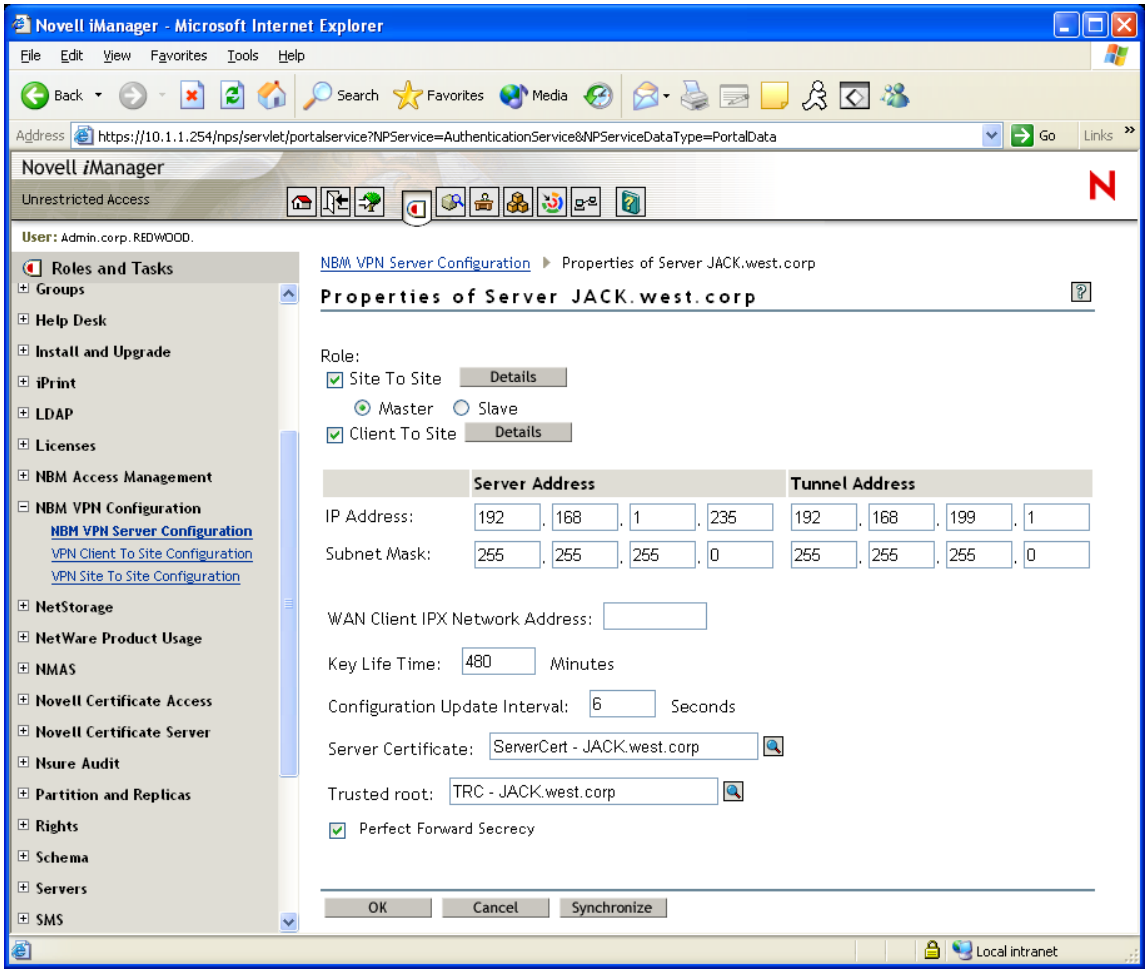


Open the **NBM VPN Server Configuration** link inside the **NBM VPN Configuration** option in iManager.

Select **Subtree level** and click **Update List** to see the VPN servers below the starting context.

Notice that **Client To Site** is **Disabled** for server JACK.

Select the VPN server **JACK**.

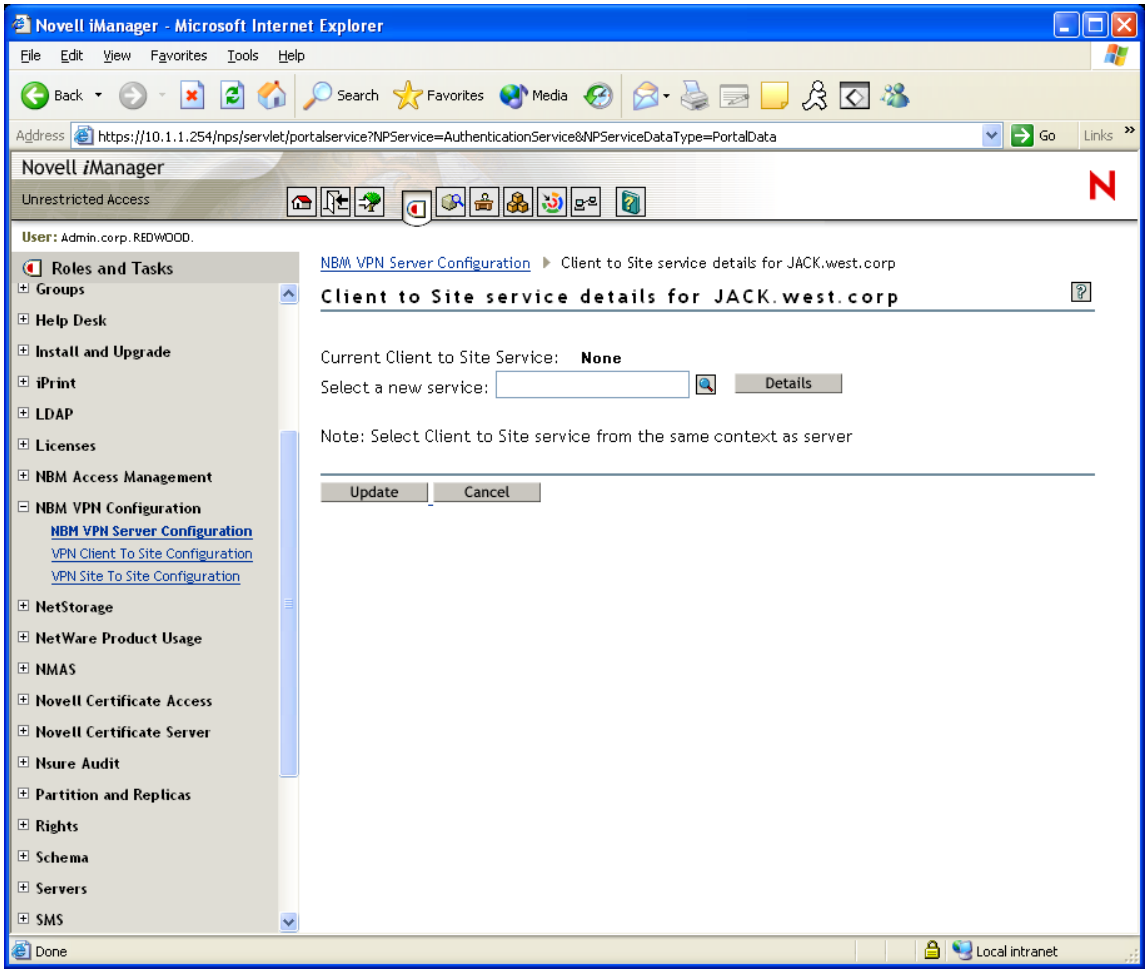


Select **Client To Site** in the Role section at the top of the menu.

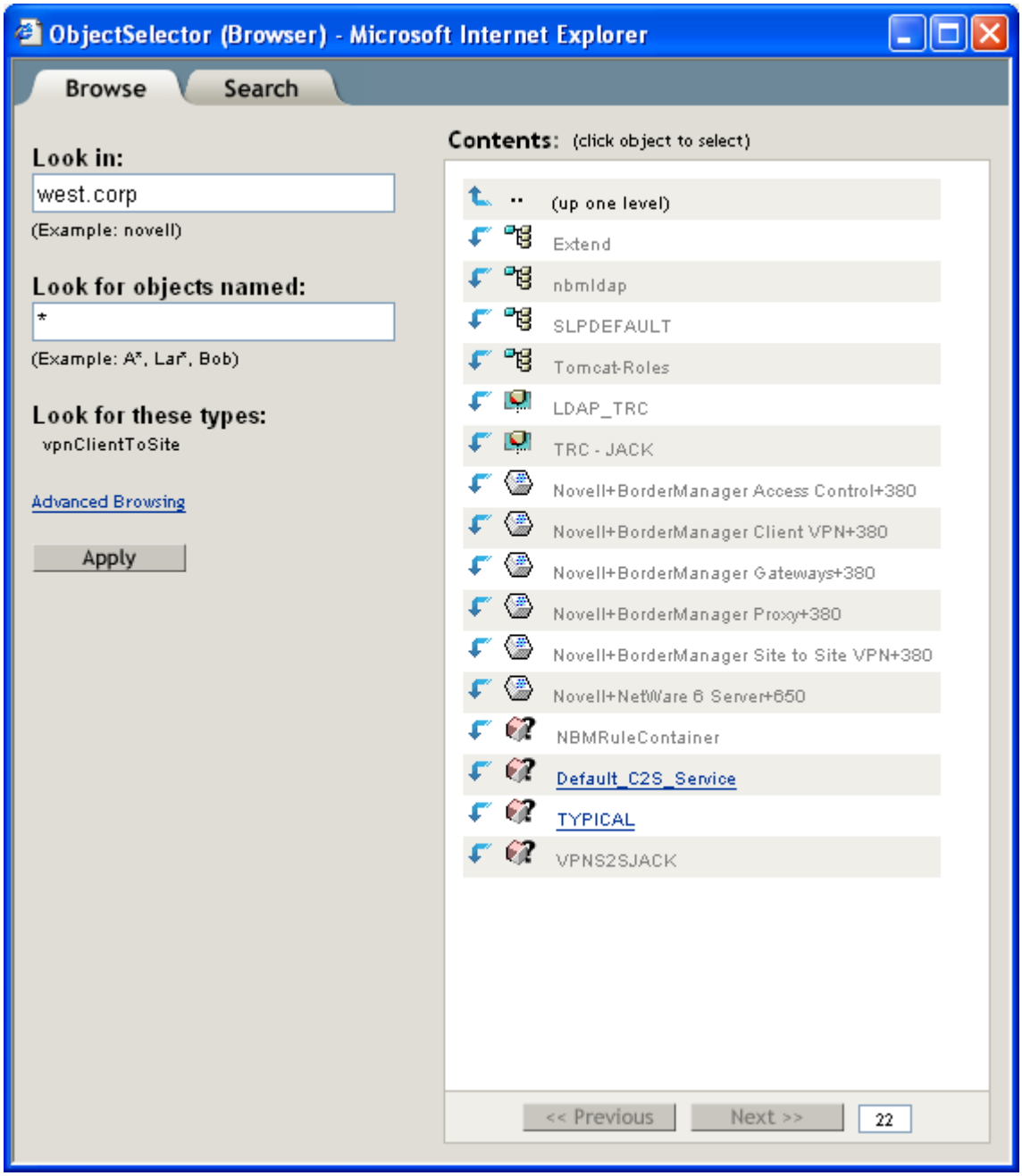
A warning message comes up that you need to now click on the Details button and select a Client-to-Site service. Or create a new one.

Click **OK**.

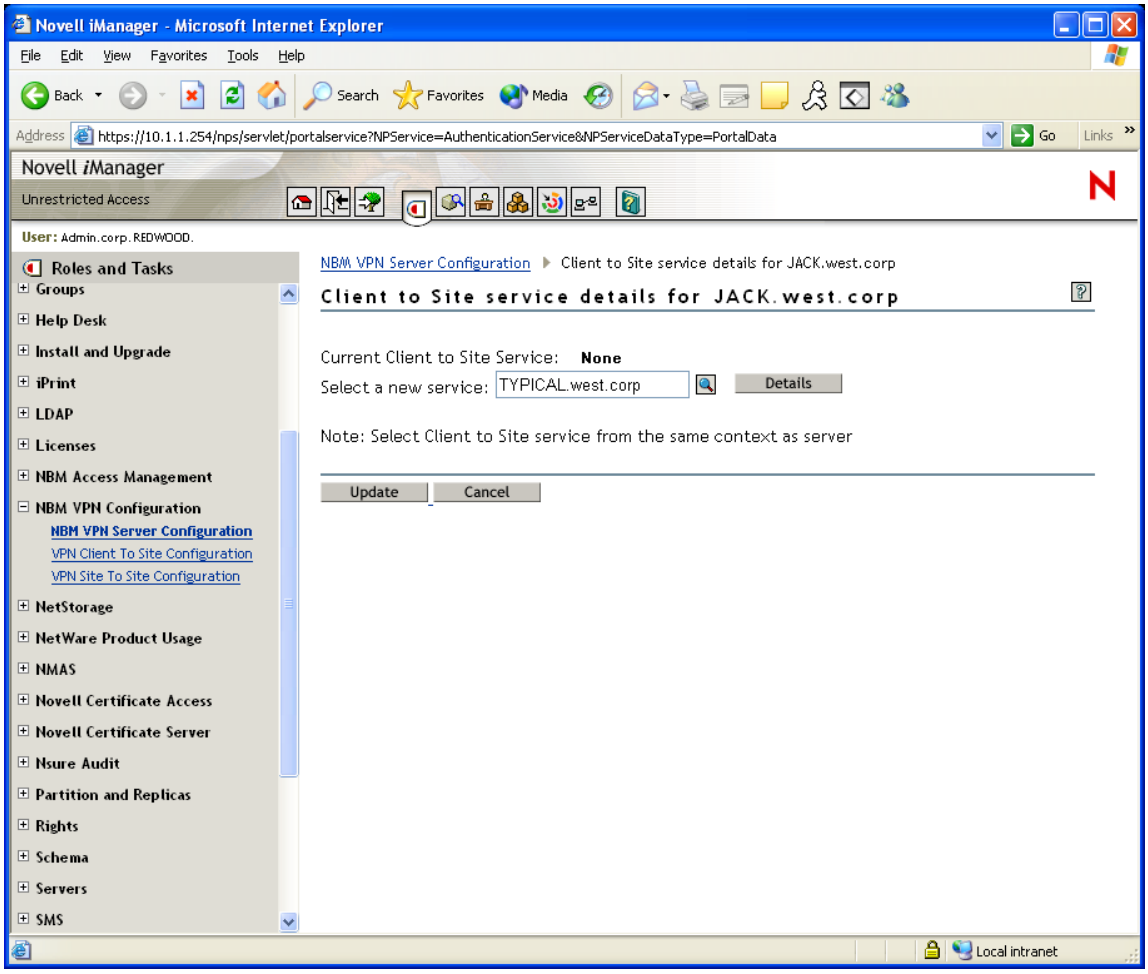
Now click on **Client To Site Details**.



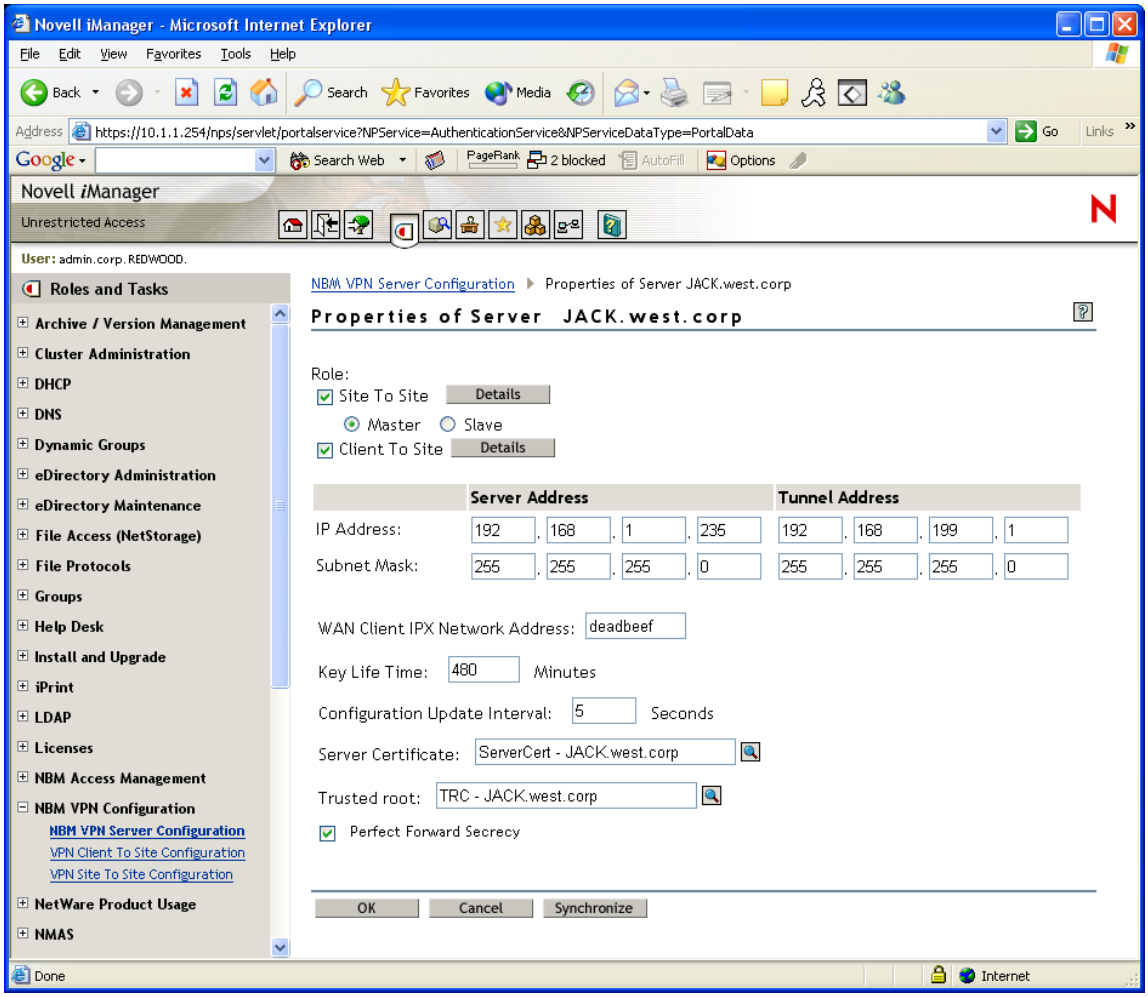
Click on the **browse icon** next to the **Select a new service** field.



Select the Client-to-Site VPN service that has just been configured. In this example, that service is called **TYPICAL**.



Click the **Update** button to assign the Client-to-Site service to the VPN server and make it take effect.



You are taken back to the VPN server configuration menu.

You now have a **WAN Client IPX Network Address** field. Even if you do not expect to have IPX clients, you should put in a valid **IPX network address**. (In this example, the hexadecimal address deadbeef is used).

Note The Novell client for WindowsME, Windows NT, Windows 2000, Windows XP does not support IPX over VPN.

Click **OK** to save all the settings.

You should see a message that the VPN server was successfully modified, and Client-to-Site VPN should begin working almost immediately.

Novell VPN Client Installation And Configuration

Security Considerations – Use A Personal Firewall and Anti-Virus Software

When a user connects to your network using Client-to-Site VPN, they become a node on your network, and are able to access whatever resources on your LAN that you have made available with traffic rules. Especially if you have configured rules to allow remote clients to browse the Internet while connected with VPN, your network is vulnerable to viruses and Trojan horse programs infecting the remote client. For this reason, you should insist that any remote VPN client be configured with a personal firewall and up-to-date antivirus software.

Novell supplies a personal firewall with BorderManager 3.8 called Novell Client Firewall (NCF). This software is based on the Agnitum Outpost Pro personal firewall. You are allowed to install as many copies of the personal firewall software as you have BorderManager 3.8 licenses. The software can be found in the BorderManager 3.8 product CD, in the CL_INST\NCF directory. The software is good, and it also defaults to automatically updating itself with newer versions from Novell.

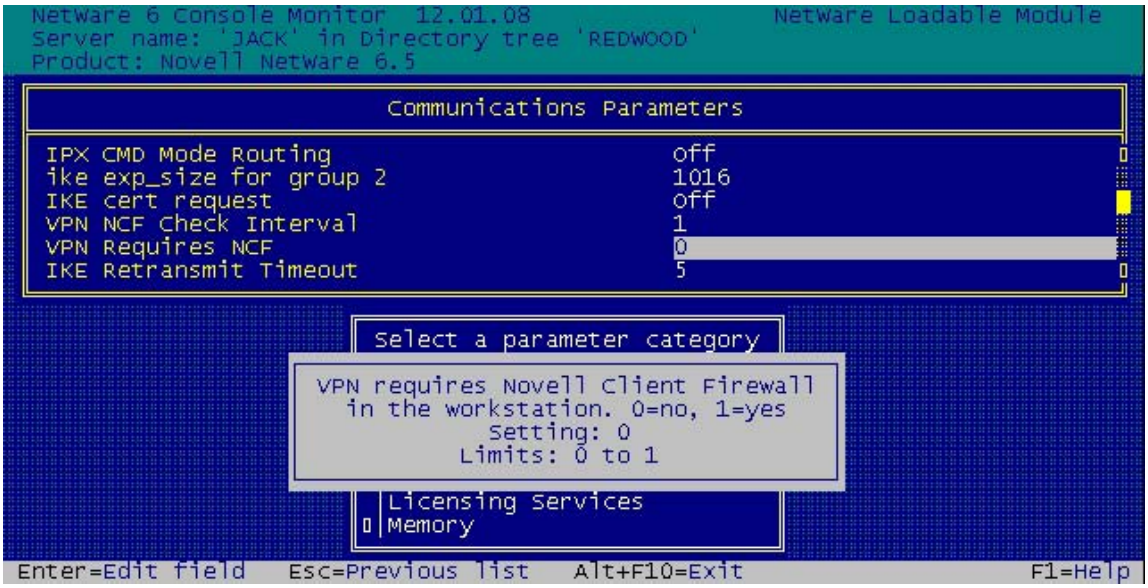
The installation and use of personal firewalls (and anti-virus software) is out of the scope of this book, but here a few typical features you may see in a personal firewall.

- Learning mode – personal firewalls should have a mode of operation where they alert you when inbound or outbound traffic is seen, and allow you to temporarily or permanently allow that traffic from the particular program sending or receiving it. Novell's NCF defaults to this mode, and you will want to Always Allow traffic from the VPN client software the first time you make a VPN connection.
- Intrusion Logging – personal firewalls should log traffic being denied for later review. This feature not only allows you to see if someone is trying to hack into your system, it also allows you (or an administrator) to go back to the logs and see if you denied some traffic needed for a legitimate application to function. Novell's NCF has good logging capability.

Force Novell Client Firewall for VPN Connections

BorderManager 3.8 can be configured to require the Novell Client Firewall to be running to make a Client-to-Site VPN connection. This is done with a setting on the BorderManager 3.8 VPN server in **Monitor, Server Parameters, Communications**.

Change the setting VPN Requires NCF from 0 to 1.



Alternatively, use a SET statement:

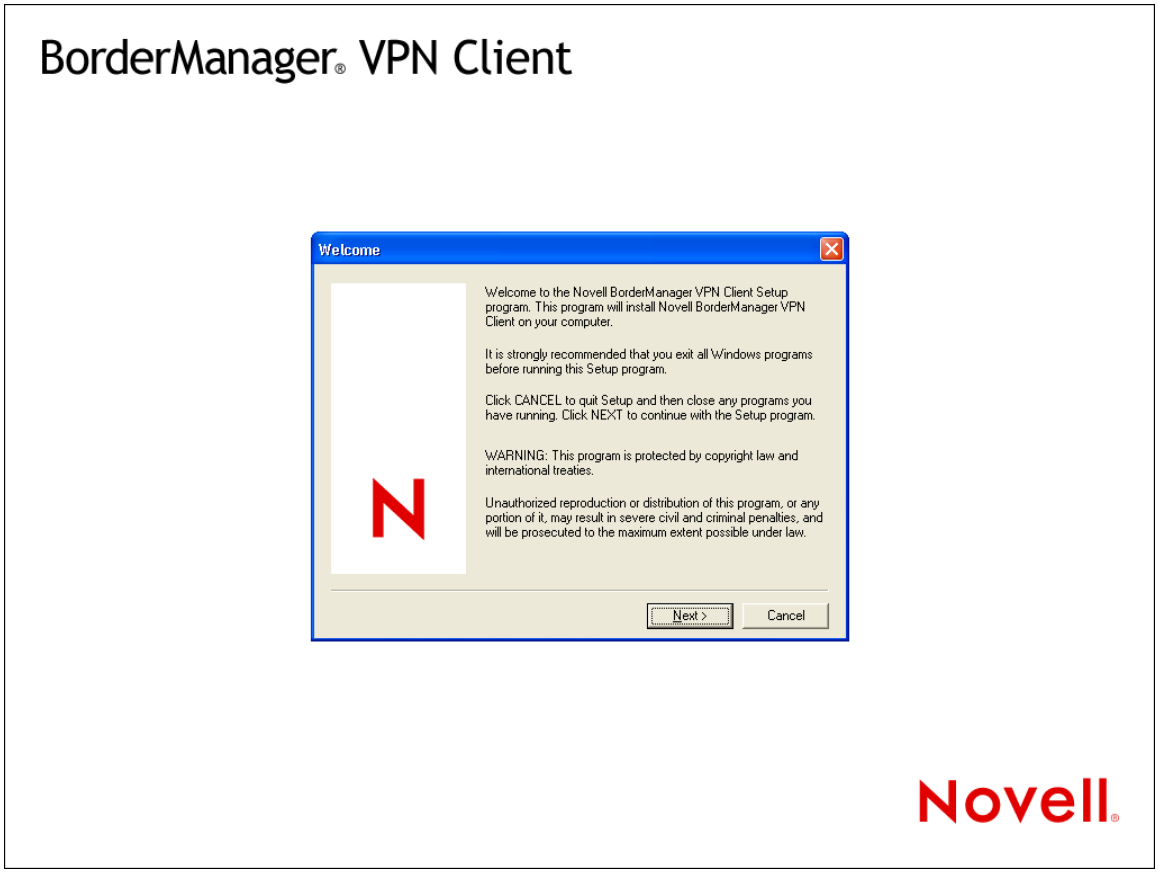
SET VPN REQUIRES NCF=1

Installing the Novell VPN Client

The VPN client is located in the BorderManager SYS:\PUBLIC\BRDRMGR\VPN\DISK1 (or EXES) directory. Newer versions, with many bug fixes, are available by download from Novell.

You should install Client32 on the PC before installing the VPN client if you intend to log in to a NetWare server over the VPN. If you install Client32 after the Novell VPN client is installed, the VPN client will not have full integration with Client32.

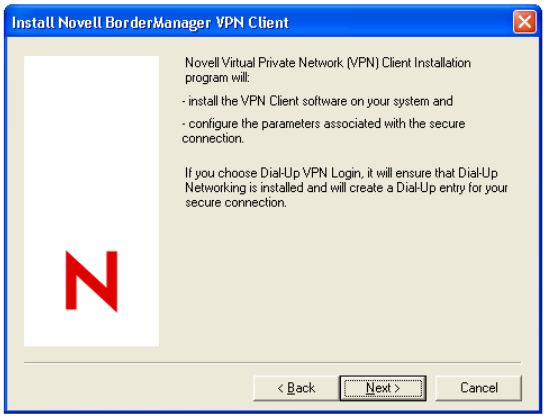
Clicking on the SETUP.EXE program in that directory begins the BorderManager 3.8 VPN client installation. The VPN client can be installed in Silent mode, with some limitations. See the VPN client readme.txt file in the installation directory.



Launch the VPN client installation program.

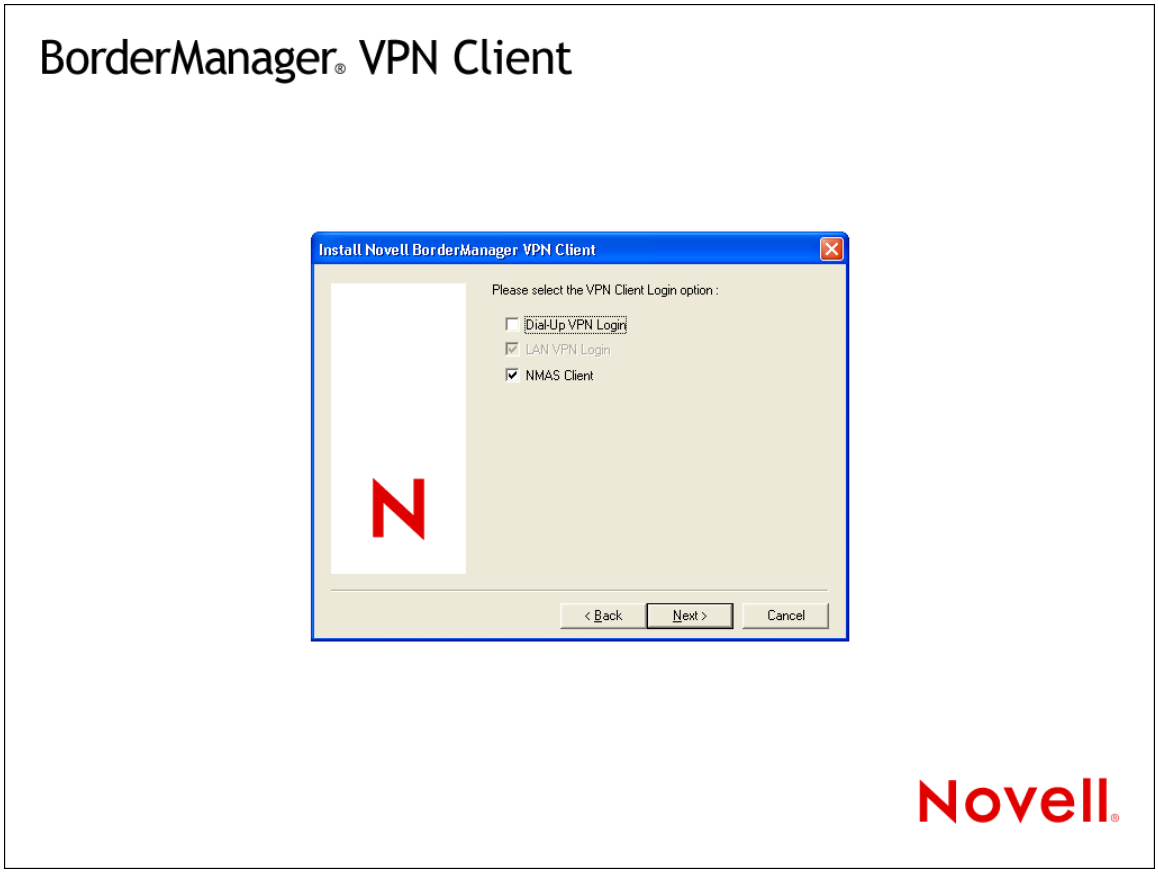
Click **Next**.

BorderManager® VPN Client



Novell®

You will be given a few installation messages. Press **Next** when you come to these.



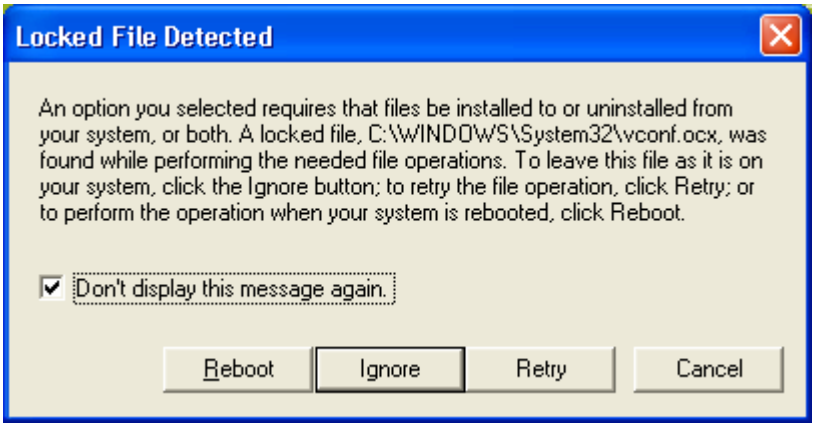
I chose not to install the DialUp VPN Login, and choose to install the NMAS Client. The VPN client may overwrite Client32-supplied NMAS with this choice, and depending on the version of the VPN client, this could actually back-rev your NMAS component. It is a good idea to check the version of NMAS before and after the VPN client installation by looking at the Windows installed programs list in Control Panel.

Selecting Dial-Up VPN Login simply puts an icon on the desktop that attempts to integrate the dial-up networking settings already present into a convenient menu option with a VPN connection. I have had problems with that working, and so I choose to launch my dial-up connections separately, then use the LAN VPN client connection to make the VPN connection over the dial-up link.

Make your desired selections and click **Next**.

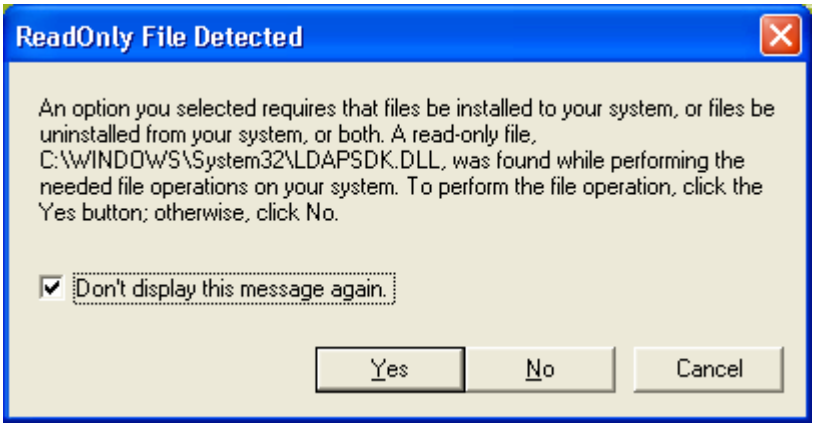
You should get an information message that you may need the Windows CD or the Novell Client32 software. Click **Next.**

You may have some existing component that needs to be updated, resulting in a message. This is particularly likely if you have a previous VPN client installed.



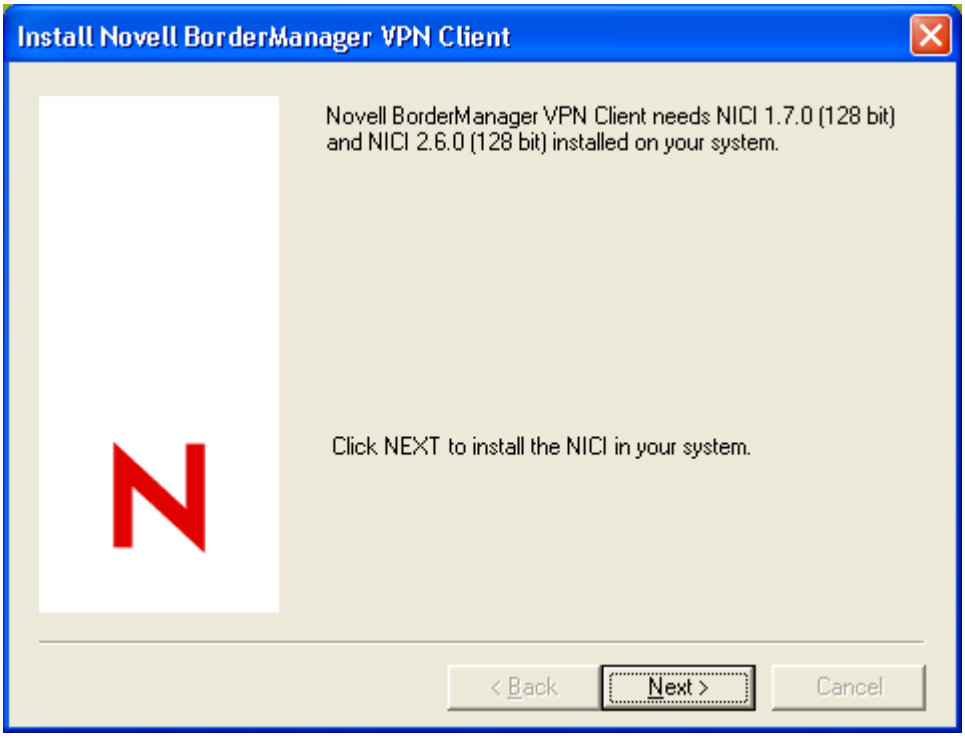
In my case, I had software running that could only be updated following a system reboot.

I chose the **Reboot** option.



I also had some read-only files that needed to be overwritten.

I chose the **Yes** option.

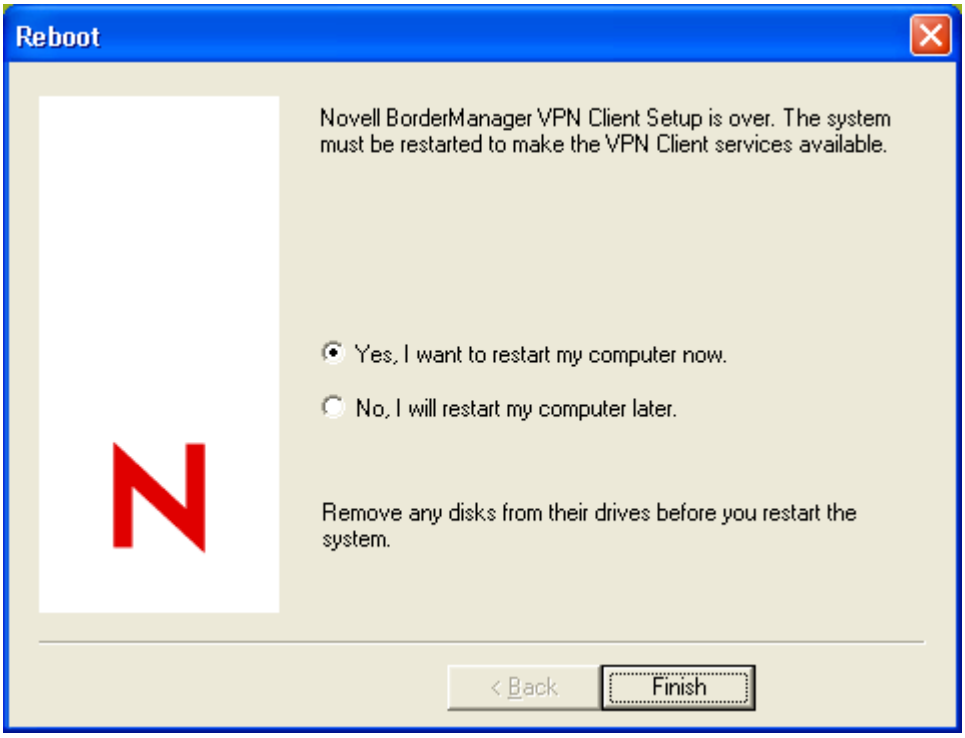


BorderManager 3.8 VPN requires both NICI 1.5.7 and 2.6.2 to be installed on the workstation. If either NICI version is missing or out of date, the VPN client installation will install it for you. The VPN client will also upgrade 56-bit versions of NICI to 128-bit.

NICI is used to encrypt data for the VPN connection.

If a later version of NICI needs to be installed on your system, the VPN client will do that for you automatically.

You should get a prompt to view the Readme file after the NICI install is completed. I recommend that you read that file.



When finally complete, you will probably need to reboot the PC for the software to complete its installation.

Choose the appropriate option and click on **Finish**.

When the PC reboots, it is a good idea to go to the network properties for your local area network, and check the TCPIP properties. In Windows XP, you should have a check box next to the Novell Virtual Private Network option. If that check box is not enabled, no TCP/IP traffic will flow over the VPN adapter.

Using BorderManager 3.8 VPN Client – Backwards Compatibility Mode

The BorderManager 3.8 VPN client can easily be used to connect to BorderManager 3.0 through 3.8 Client-to-Site VPN. You must configure the VPN client to use Backwards Compatibility mode to connect to versions prior to 3.8. The server must also have been configured as described in the legacy VPN chapters (or upgraded in place from a 3.6 or 3.7 VPN server).

Note There is one difference between the configuration of legacy mode in a 3.8 server and that shown in the legacy VPN chapters – the VPN configuration menu and access rule in NWADMN32 are no longer used. Instead, configure a simple NMAS authentication rule for users, groups or containers, and traffic rules for NMAS identities in iManager 2.0. The traffic rules applying to the user being authenticated should show up in the VPN policies on the client.

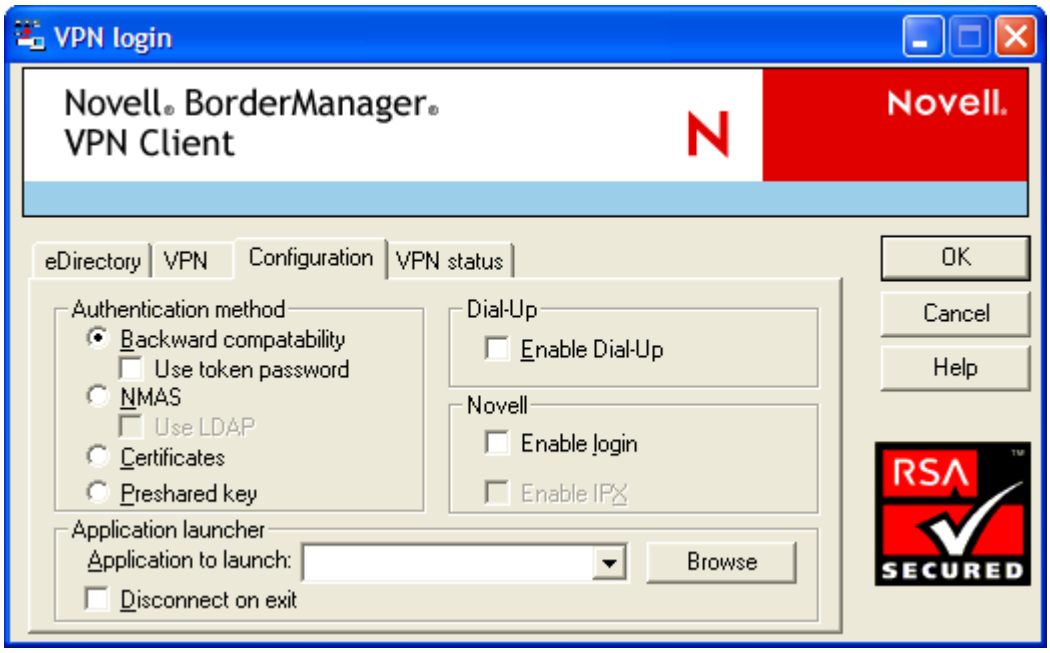
Essentially the same settings are available in the new client as in previous versions when Compatibility Mode is used, although the menu entries are different.

When the VPN client has been installed on your PC, and the PC has been rebooted, you are ready to begin configuring its settings.

In this example, Novell Client32 is also installed on the PC. A Novell client is only needed if you need to log in to a NetWare server over the VPN. If you do not need to log in to a NetWare server, you can install just the Novell VPN client, but some menu options shown in the following examples will be grayed out and inaccessible.

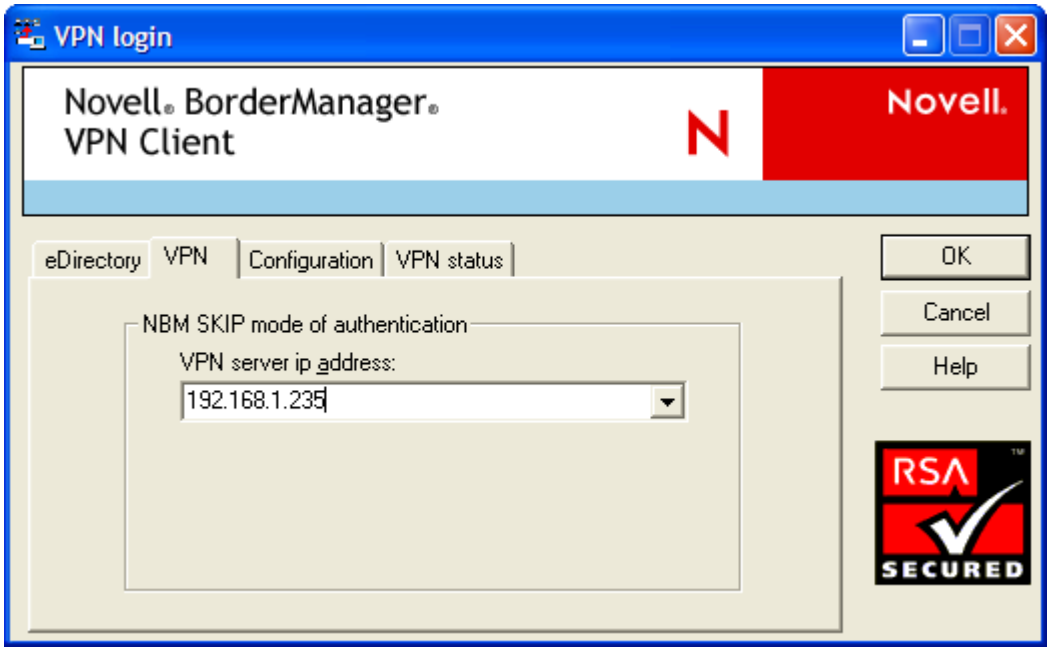
Configuring the BorderManager 3.8 VPN Client

Launch the VPN client, and select the Configuration tab.



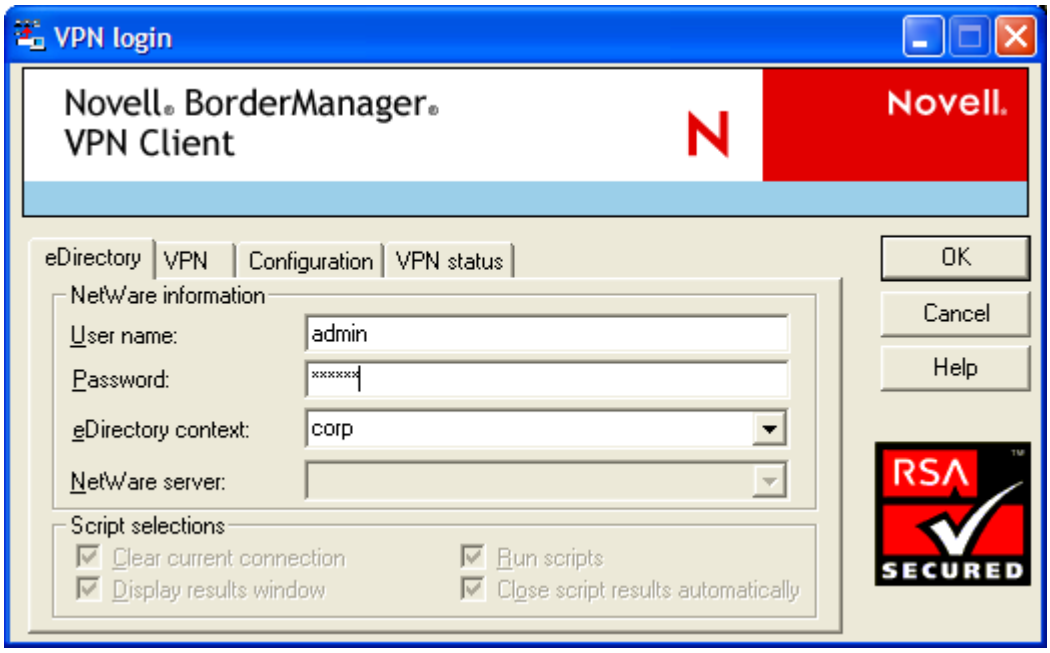
Select **Backward compatibility**. The new VPN client will now function in the same way as the older VPN client, described in the Legacy VPN chapters.

Select the **VPN** tab.



Enter the **public IP address** of the BorderManager VPN server in the **VPN server ip address field**.

Select the **eDirectory** tab.



Enter the **user name**, **password** and **eDirectory context** on the eDirectory tab. These are the fields used to authenticate to the VPN server.

If Enable Login is enabled on the Configuration tab, you may have additional options enabled, if Client32 is also installed. However, you will have more control of login using Client32 after a VPN connection. Review the legacy Client-to-Site VPN chapter.

Click **OK** to make the VPN connection.

Connecting to a BorderManager 3.8 Server in Backwards Compatibility Mode

Connecting to a BorderManager 3.0 through 3.7 server is just like the description given in the legacy VPN chapters. However, there is a difference when connecting to a BorderManager 3.8 server in backwards compatibility mode.

In a BorderManager 3.8 server, the old Client-to-Site VPN settings in NWADMN32 are not used, including both the VPN configuration tab and any access rules for VPN client. If you upgraded an older VPN server in-place, the old rules and Client-to-Site configuration details should have been automatically migrated into the closest equivalent settings in iManager. If you are configuring a new BorderManager 3.8 server to be used with backwards compatibility mode, you will need to be aware of the following:

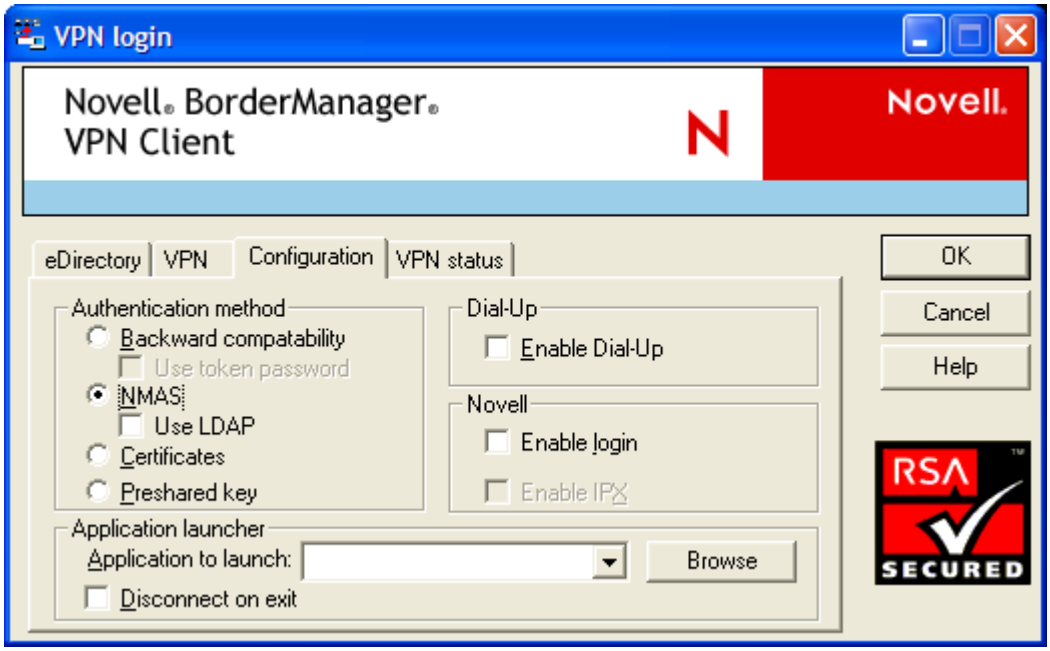
- You will first need to LOAD VPNCFG.NLM on the BorderManager 3.8 server. Go to Master Server Configuration (if on the Master VPN server) and Generate Encryption Information. For the slave server, you probably will not have to do that.
- In the legacy mode VPN chapter for Client-to-Site VPN, you had to configured protected/encrypted networks to control which networks were accessed through with VPN client connections. With BorderManager 3.8, that is done with NMAS Traffic Rules.
- legacy mode VPN chapter for Client-to-Site VPN, you had to configure an Access Rule for the VPN client connection to determine who was allowed to make a VPN connection. With BorderManager 3.8, that is done with NMAS Authentication Rules.
- While you can control who can make a VPN connection and what networks are available using iManager rules, you cannot control by port number, or have rules apply from top to bottom, or use a deny traffic rule.

Using BorderManager 3.8 VPN Client – NMAS Authentication Mode

NMAS Authentication mode allows the VPN client to make use of various NMAS-compatible authentication methods, which could be as simple as an NDS password, or as complex as using a combination of passwords, tokens and biometric NMAS methods such as retina scans or fingerprint scans.

In this example, I show only the simplest case, and the easiest to configure – NMAS NDS Password. The goal is that a user only needs to log in by specifying the correct NDS user ID and NDS password, as in the previous versions of BorderManager Client-to-Site VPN.

VPN Client Configuration for NMAS

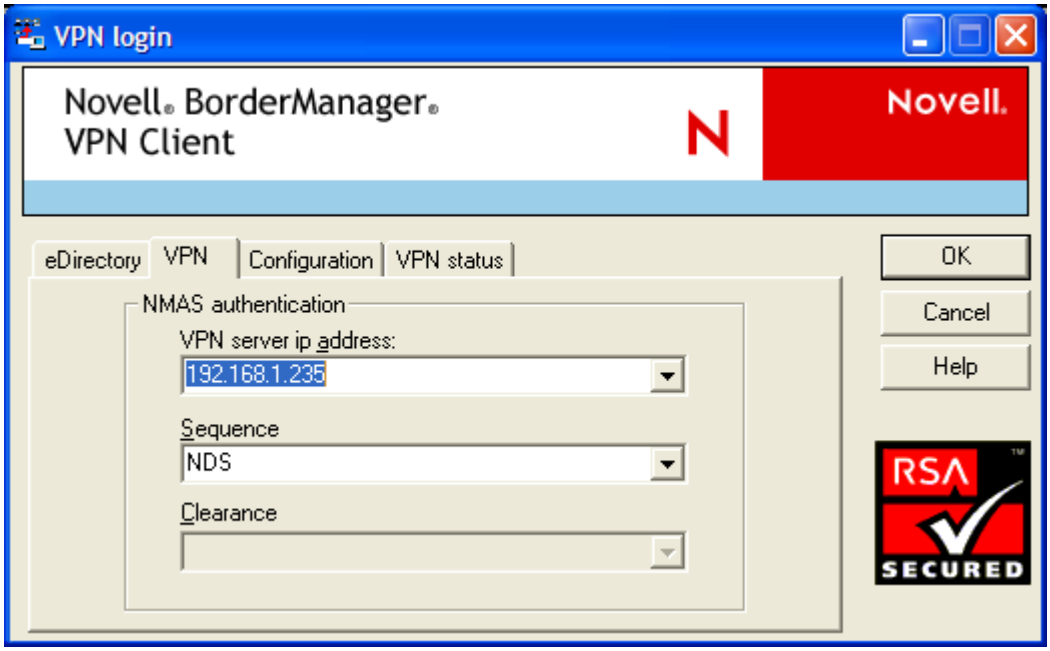


Launch the VPN client, and select the **Configuration** tab.

Select **NMAS**.

Especially if you are just starting to test Client-to-Site VPN, I recommend that you do not enable login here.

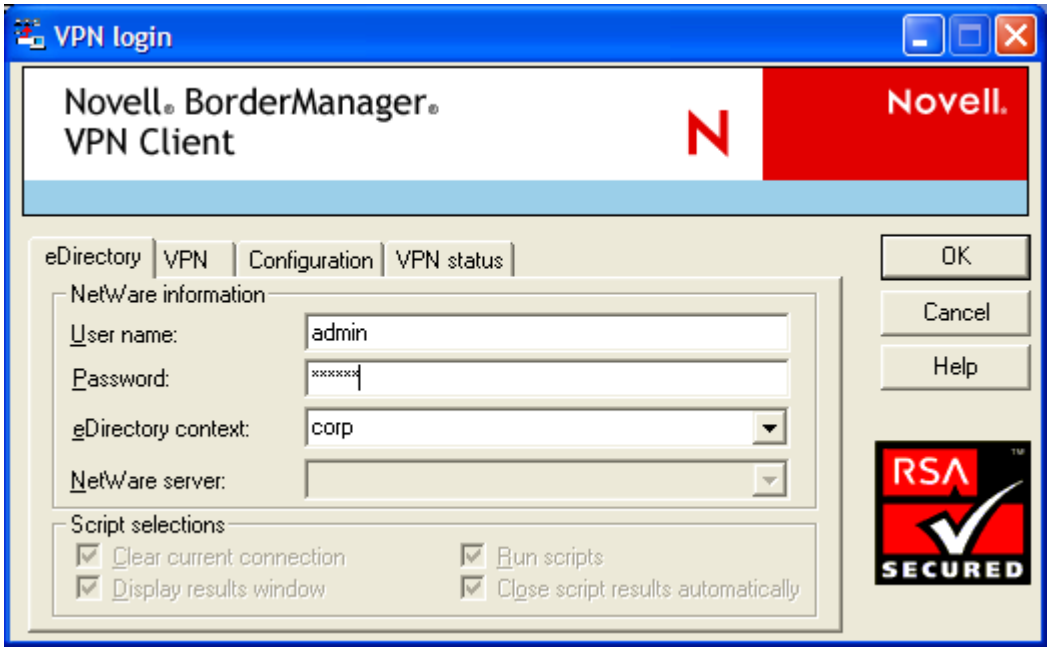
Note You should verify that you can ping the internal NetWare servers by both IP address and server name (with the VPN connected) before you try to login with either the VPN client or Client32.



Select the **VPN** tab.

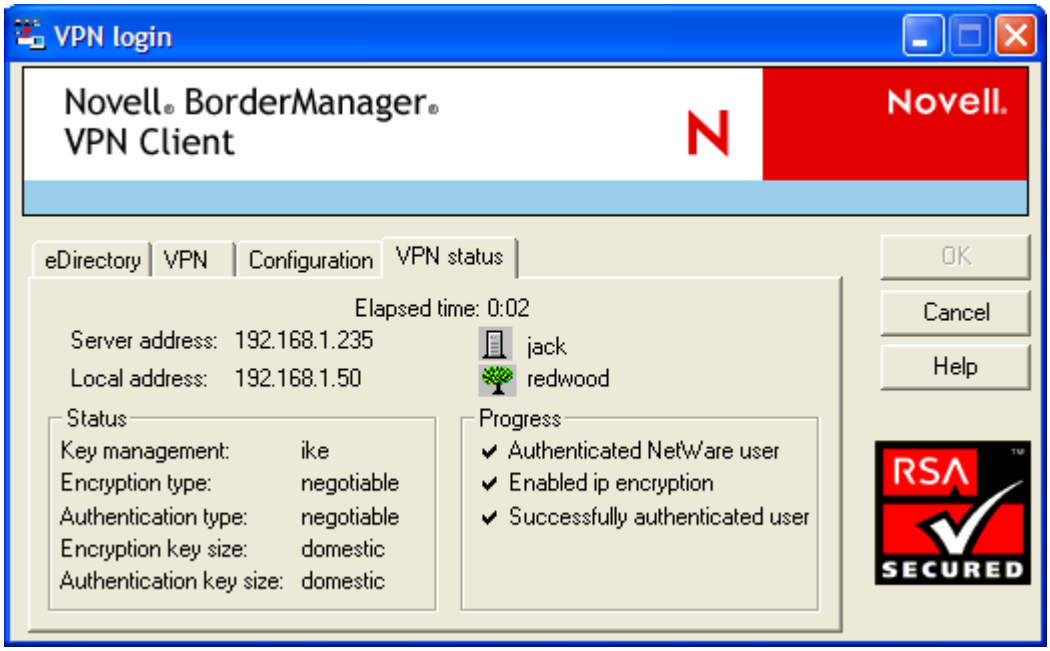
Enter the **public IP address** of the VPN server that you want to use for a VPN connection in the **VPN server ip address** field.

In the **Sequence** field, enter **NDS**.



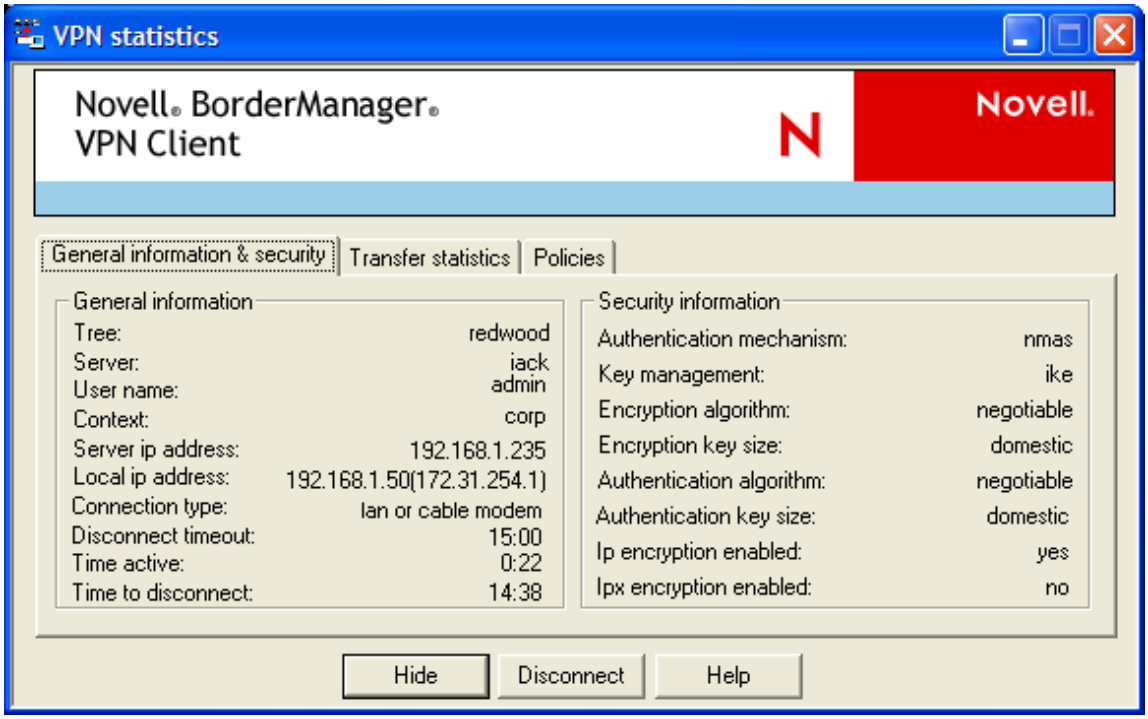
Select the **eDirectory** tab, and fill in the **User name**, **Password** and **eDirectory context** fields.

Click **OK** to make a VPN connection, using NMAS Password method.



Once authenticated, the client should set up the connection. If you are not logging in to a server, the connection should complete quickly.

If logging in to a Novell server, and running a log script, over a dial-up connection, the entire process could take a long, long time…



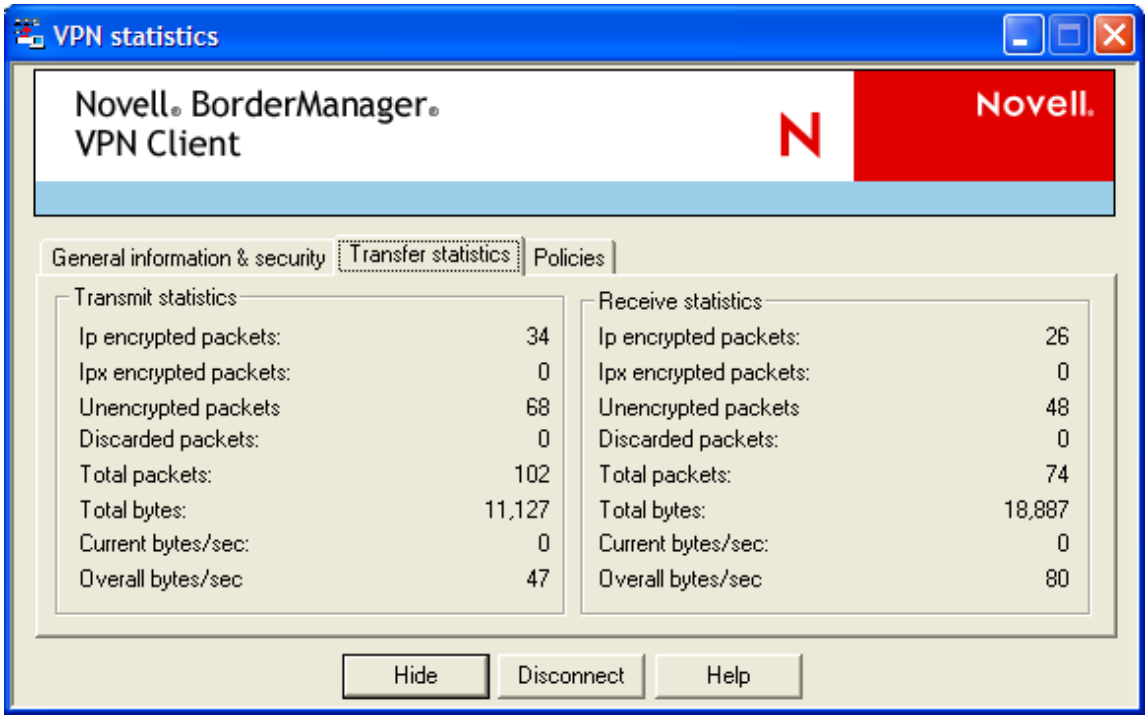
Once connected, you can see some important statistics on the VPN client **General information & security tab**. (Double-click on the VPN client icon in the system tray when connected to the VPN to see these statistics).

As can be seen from the example show, the user **Admin** in context **corp** is logged into NDS tree **redwood**. The VPN server address is **192.168.1.235**.

Of somewhat more interest is the **Local ip address: 192.168.1.50 (172.31.254.1).**

The PC's local IP address is **192.168.1.50**. The PC's VPN tunnel IP address (assigned by BorderManager 3.8) is **172.31.254.1**.

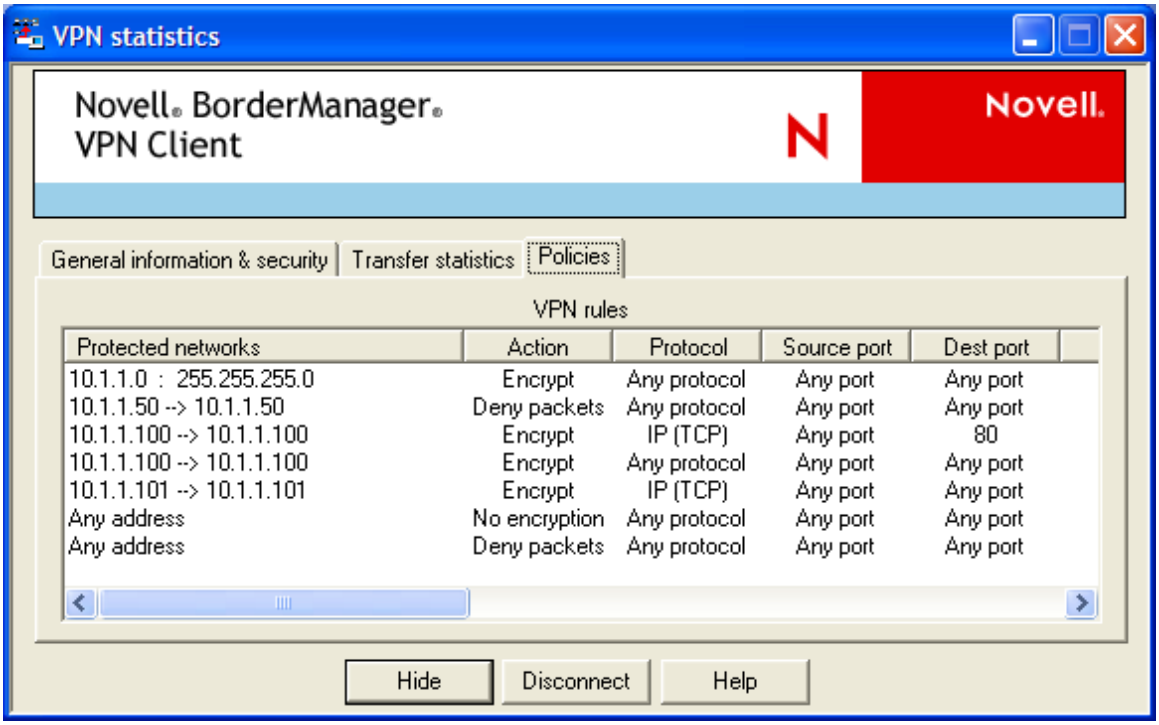
In order for this PC to be able to communicate using TCP/IP to a host inside the BorderManager 3.8 network, those hosts must have a way to route packets back to the 172.31.254.0 network, either by default routes that go back through the VPN server, or by static routes for the VPN-assigned subnet.



The VPN client **Transfer statistic**s tab shows some useful statistics for IP and IPX traffic seen at the client.

Not all traffic reported in this screen is VPN traffic!

Only the encrypted packets are packets that have gone through the VPN. And depending on the traffic rules, there could be some non-encrypted packets allowed as well.



The **Policies** tab shows which networks are available after applying Traffic Rules for the VPN-authenticated user.

When troubleshooting VPN client connection issues (once the connection has been established), it is very important to know what policies are seen at the VPN client.

The protected networks shown in the Policies tab should exactly match up with the traffic rules applied to the user.

Important! Disconnect the VPN connection by right-clicking the VPN client icon in the system tray and selecting **Disconnect**. If you do not disconnect cleanly from the VPN, you run the risk that any internal DNS server settings pushed to the remote client are not removed, and the remote user will not be able to resolve DNS names afterward.

Using BorderManager 3.8 VPN Client – NMAS/LDAP Authentication Mode

The NMAS/LDAP mode is a special case of NMAS mode. In this mode, the user ID is authenticated using LDAP calls to a remote LDAP server. This generally means that the user being authenticated does not have to have an account in the VPN server NDS tree.

Prerequisites

You must first configure a dedicated Trusted Root Container (TRC) for LDAP, and a Trusted Root Object (TRO) for the server being accessed through LDAP. You can create the TRC in the same way that you do for a TRC for VPN, using ConsoleOne or iManager. See the examples at the end of the Site-to-Site VPN chapter. I recommend you use a different TRC than the VPN TRC, so that the VPN server does not try to read the LDAP Trusted Root Object (TRO) as a VPN TRO. The settings for an LDAP TRO and a VPN TRO are not the same.

Create a LDAP TRO in the LDAP TRC (using ConsoleOne or iManager) by importing the ROOTCERT.DER file from the SYS:\PUBLIC directory of the server to be used as the LDAP Remote Server.

Configure LDAP Authentication

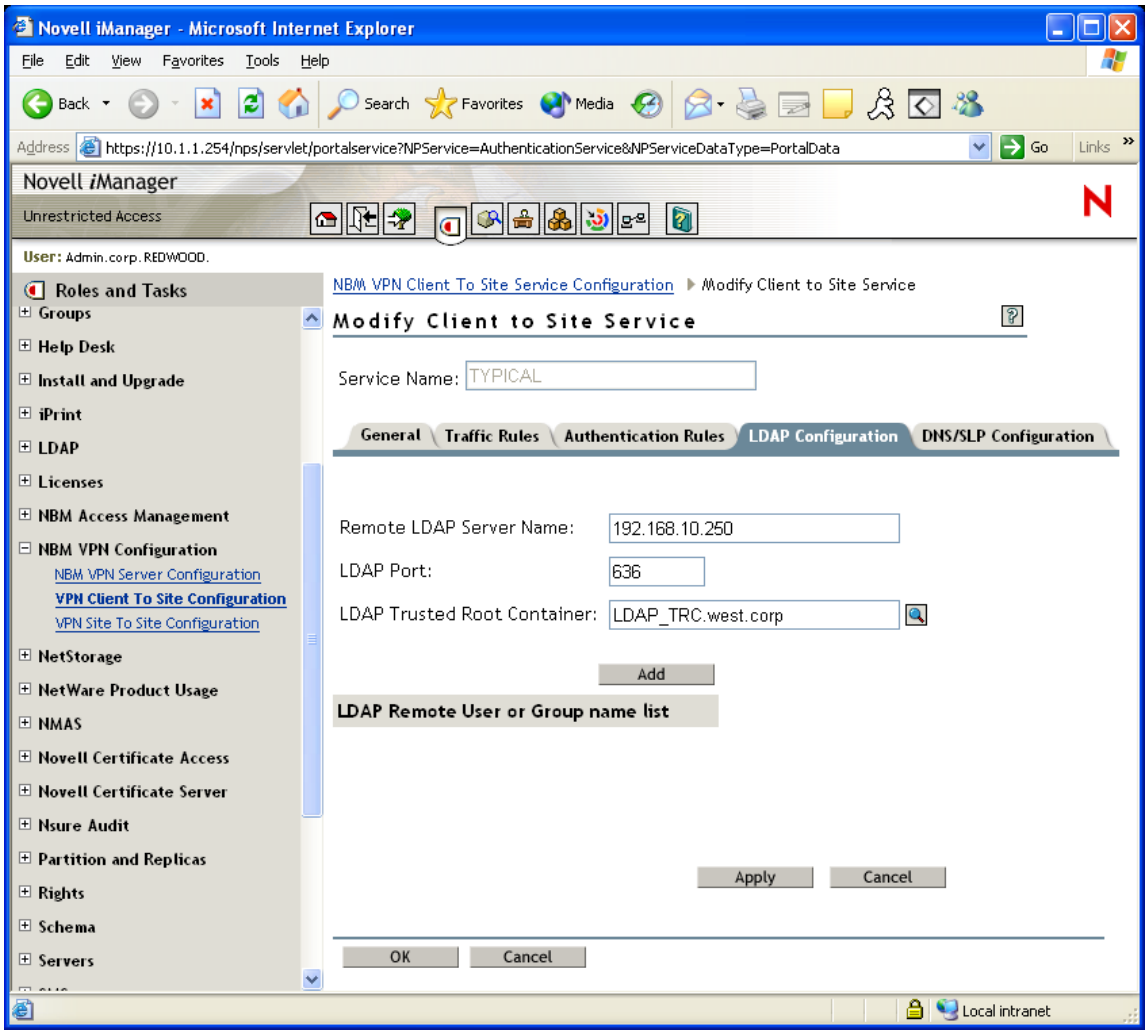
LDAP Authentication is controlled by settings in the LDAP Configuration menu of the Client-to-Site service. You can point BorderManager 3.8 to another server that will reply to LDAP user ID/password queries. You must specify an LDAP Trusted Root Container that holds a Trusted Root Object for the remote server. If the remote server is a NetWare server, create the Trusted Root Object by using ConsoleOne or iManager to import that servers ROOTCERT.DER file from SYS:\PUBLIC.

You have three ways to configure LDAP authentication:

- Any – any valid account in the remote directory will be able to authenticate.
- LDAP User Account – one or more valid LDAP usernames, in fully-qualified LDAP syntax, can be used to specify particular LDAP users that may authenticate
- LDAP Group - one or more valid LDAP groups, in fully-qualified LDAP syntax, can be used to specify particular LDAP users that may authenticate

LDAP Configuration within the Client-to-Site VPN configuration is used to allow authentication of a VPN client by LDAP protocol to a server. This option would normally be used to authenticate a user to another NDS tree, or to another directory service that supports LDAP queries, such as Active Directory.

Go to the Client-to-Site Service, and expand the **LDAP Configuration** tab.



Fill in the IP address for the **Remote LDAP Server Name**, the **LDAP Port** number (typically **636**), and browse to an **LDAP Trusted Root Container (TRC)** in the same tree as the VPN server.

Use ConsoleOne or iManager as described in the previous chapter to create a dedicated TRC for LDAP.

You must have a Trusted Root Object (TRO) for the remote LDAP server in the LDAP Trusted Root Container. Use ConsoleOne or iManager as described in the previous chapter to create a TRO for the LDAP server. When creating the TRO, use the remote LDAP server's ROOTCERT.DER file.

Click on the **Add** button to add LDAP users or groups.

Add the name of an LDAP user, or group, in LDAP syntax.

You have the following choices:

- Any – allows any user in the remote LDAP directory to authenticate to the VPN. I suggest you try this first, to test to see if LDAP is working. Once you get it working, remove this entry and put in more specific authentication rules.
- LDAP Group – allows any user contained in the LDAP group in the remote LDAP directory to authenticate to the VPN.
- LDAP User – Allows a specific user in the remote LDAP directory to authenticate to the VPN.

In this example, I will add all three types, to show the syntax. The Any user will of course override the other two entries.

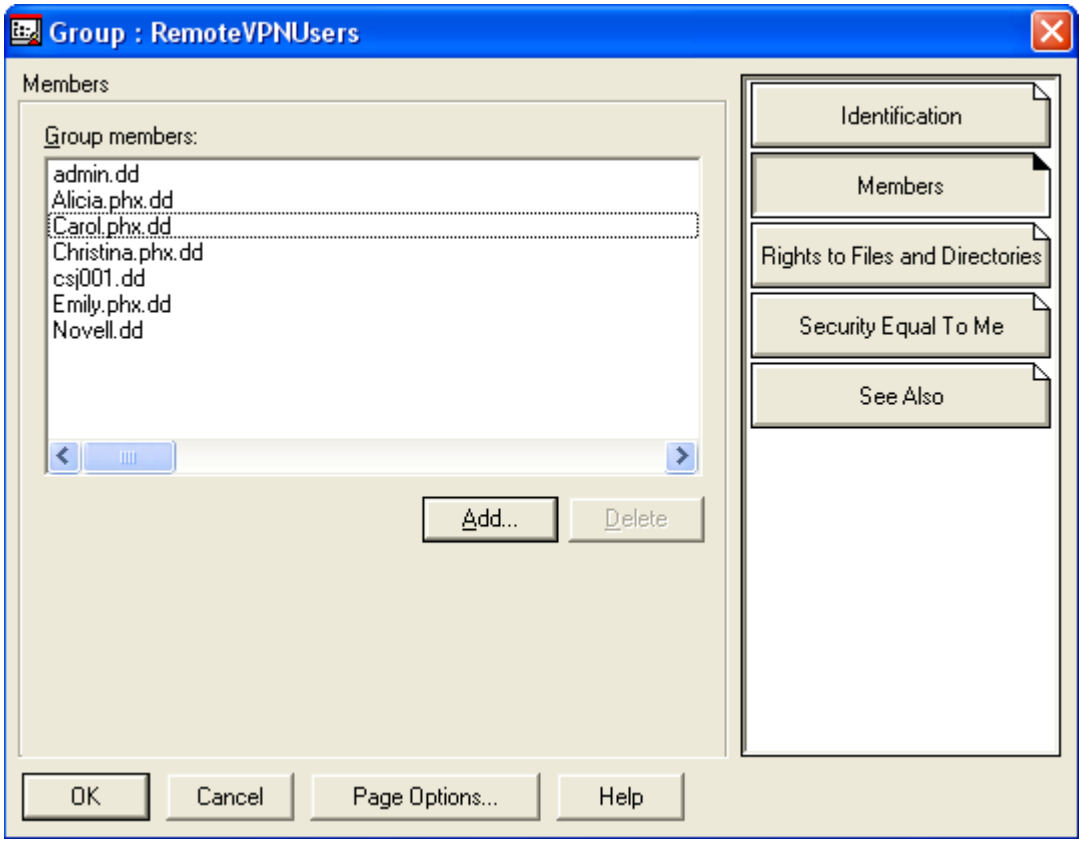
It is important to note that the Traffic Rules will have control over what an LDAP-authenticated user can do over the VPN connection.

The entries to be added in this example are:

- CN=Craig,OU=phx,O=DD
- CN=RemoteVPNUsers,OU=phx,O=dd

CAUTION *LDAP syntax uses commas, not periods, between containers. LDAP is also case-sensitive.*

You cannot specify a container name in the LDAP rules, but you can use the entry Any, and authenticate any user in any container of the remote LDAP directory.

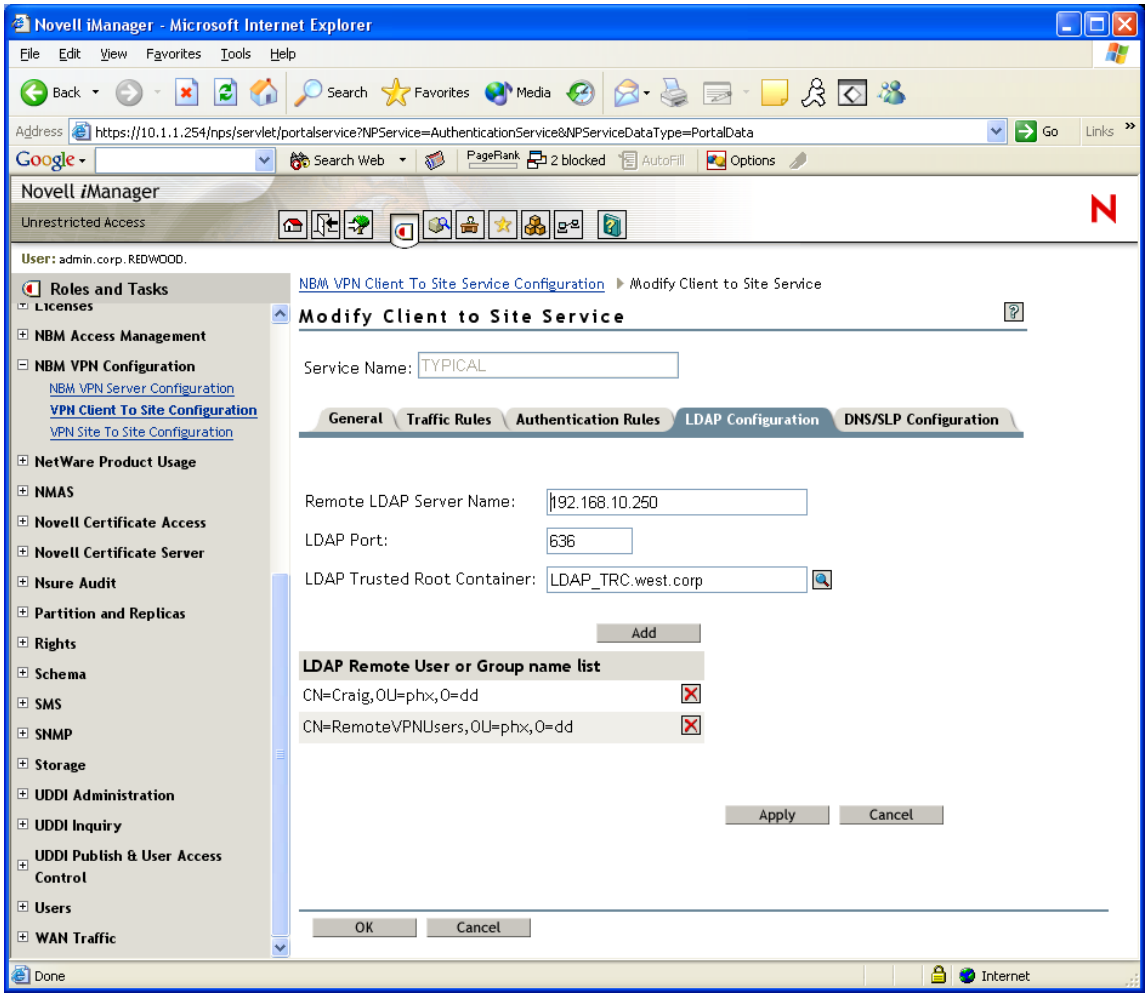


The screenshot above shows the group membership list of the RemoteVPNUsers group in the other NDS tree. Note the case of the users names because the VPN users must enter their login names in the same upper and lower case combinations.

In the example show in the next few pages, notice that Craig.phx.dd is not in this group. Separate traffic rules will be used for the group and the Craig user.

The remote LDAP directory is a separate NDS tree (shown in Scenario 9b at the beginning of this book). An important point to note here is that the users never need to be granted access to the remote LDAP server via a Traffic Rule. The BorderManager 3.8 VPN server itself needs to have network access to the remote LDAP server, using the configured LDAP ports, but the users do not.

Note that the IP address used in this example is not a protected IP address for the VPN server. It happens to be accessible via some static routes on the VPN server, and was chosen to demonstrate that the LDAP authentication is not directly between client and LDAP server, but instead is passed from client to LDAP server by the VPN server.



In the example shown here, the VPN server is configured to allow a VPN client to use LDAP authentication to a remote LDAP directory for one user and one group in that directory.

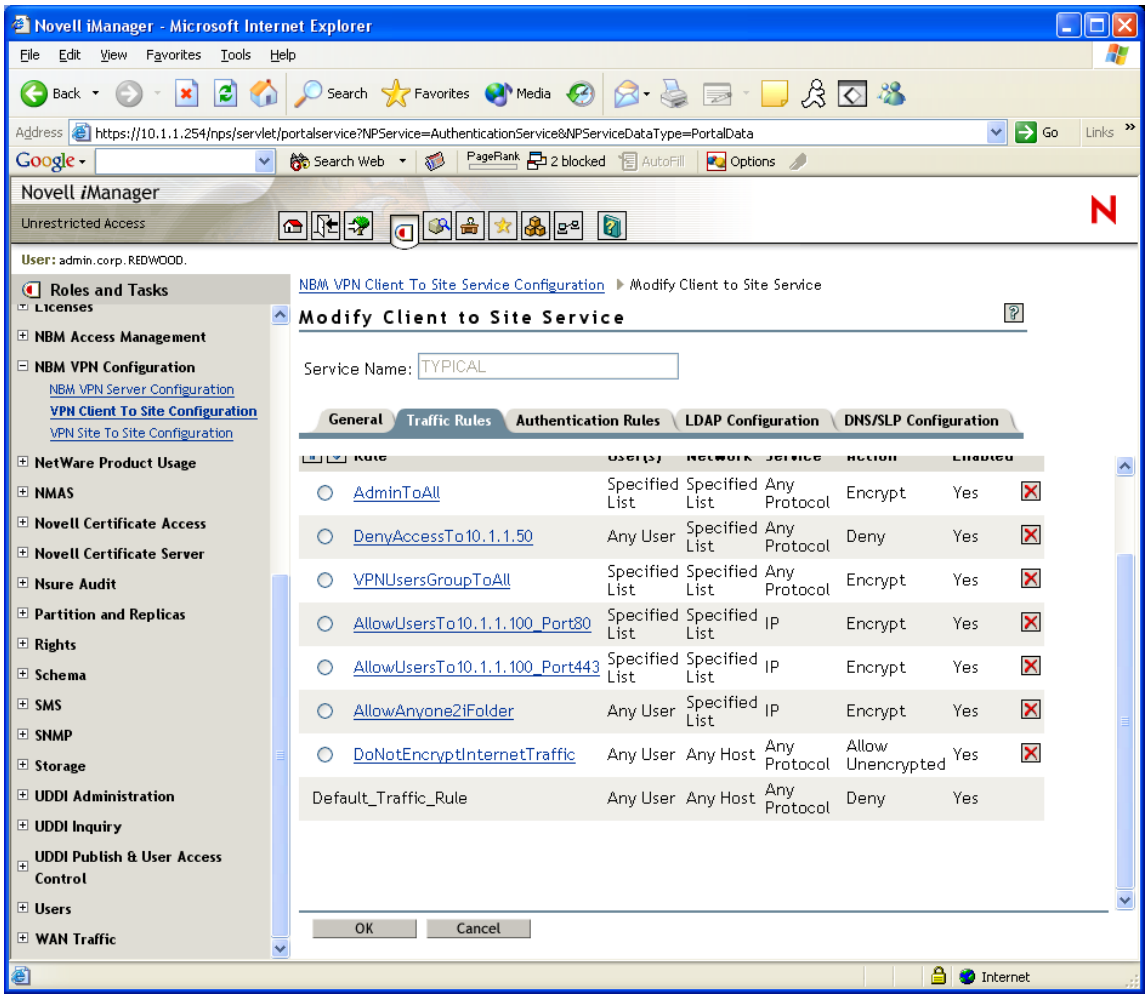
Note When setting up LDAP Authentication, try using **Any** as a test entry for LDAP remote users before trying to get more specific with LDAP users and groups. Once you are sure LDAP authentication itself is working, you can get more complicated with specific user authentication entries.

Click **Apply** to save the changes.

Click **Traffic Rules** to make a new rule to apply to LDAP users.

Configure LDAP Traffic Rule

We have previously configured a number of rules for NMAS authentication.



Some of the existing (NMAS) rules will apply to All Users, including those users that authenticate via LDAP. Specifically, the LDAP users should be able to get to 10.1.1.100 using port 80 and 443, and should be able to get to the iFolder server using the ports configured in that rule. LDAP-authenticated users should be denied access to 10.1.1.50, and should also be denied access to any other sites besides 10.1.1.100 and the iFolder server by the default deny rule at the bottom of the list. This is if we add no additional rules for LDAP.

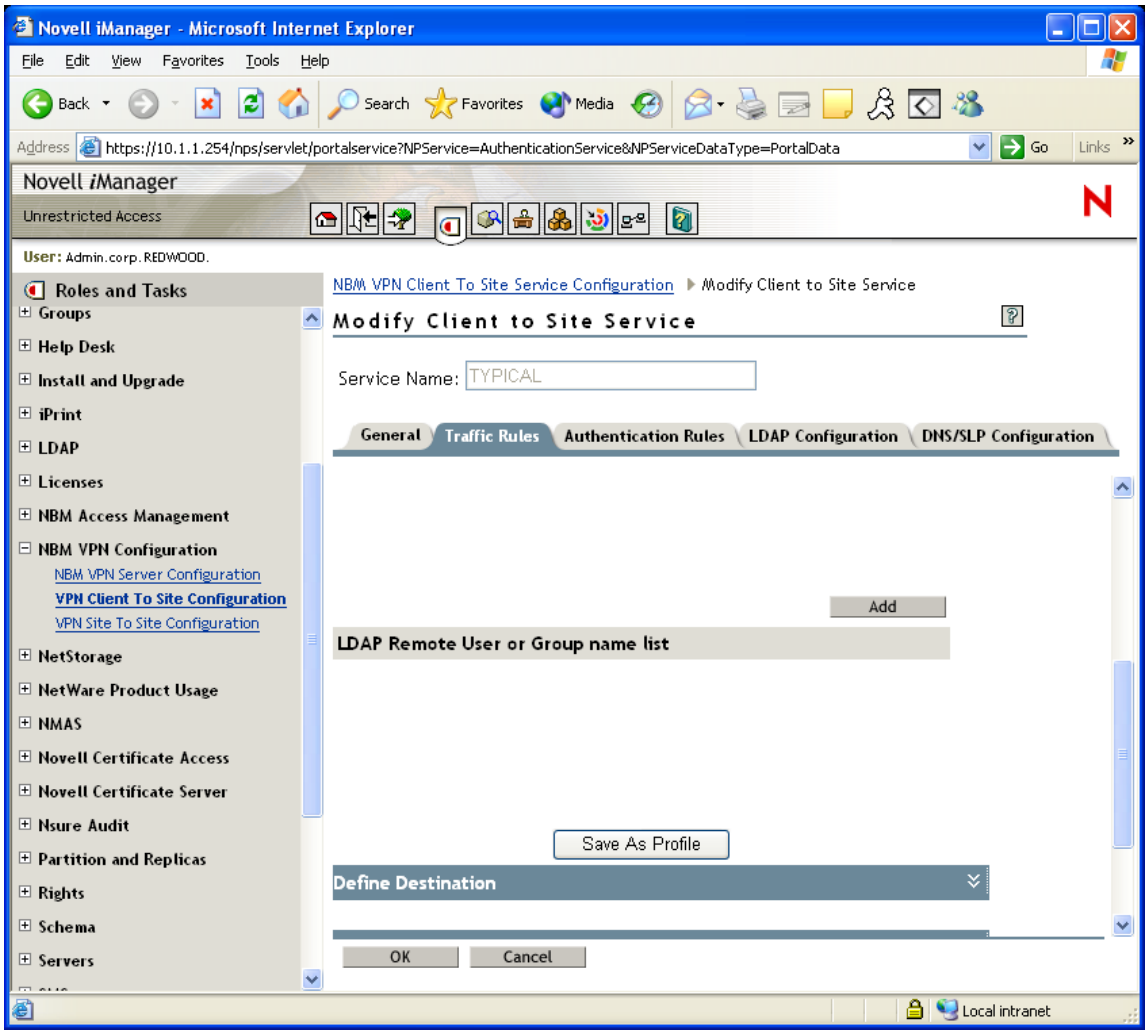
Let's say that we want a subset of LDAP-authenticated users to have HTTP access to a web server at IP address 10.1.1.20. We must make a traffic rule that calls out that IP address as a destination, and which also specifies port 80. In order to limit the access to a

particular subset of users, the traffic rule must call out a LDAP Group as a defined user, or a list of individual LDAP users.

For the sake of convenience, I have created a RemoteVPNUsers group in the NDS tree being accessed via LDAP. Several user accounts were put into that group, but not Craig.phx.dd. The Craig user and the members of the RemoteVPNUsers group in the remote LDAP directory can authenticate to the BorderManager 3.8 VPN server JACK, but only the users in the VPNUsersGroup will be able to route packets to 10.1.1.20.

Click **New** to add a new Traffic Rule.

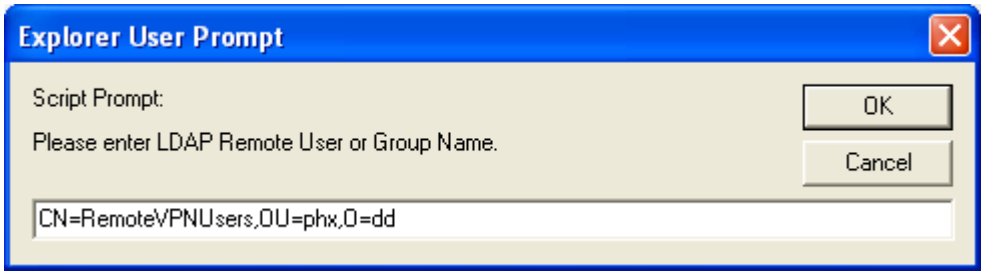
Name the rule **RemoteVPNUsersTo10.1.1.20_LDAP**.



Expand the **Define User** section.

Select **Only User List.**

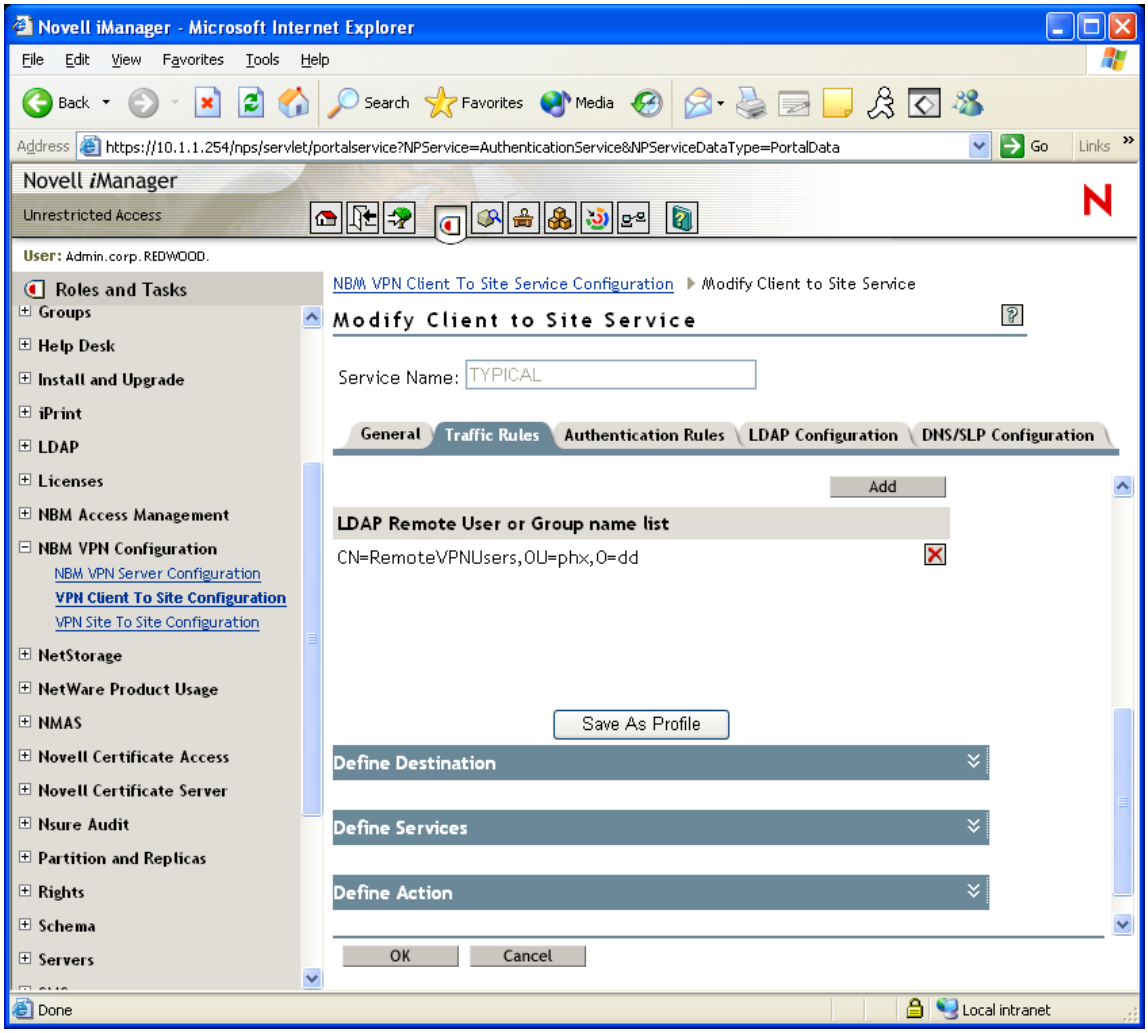
Scroll down slightly to see the **LDAP Remote User or Group name list**.



Click the **Add** button just above the **LDAP Remote User or Group name list**.

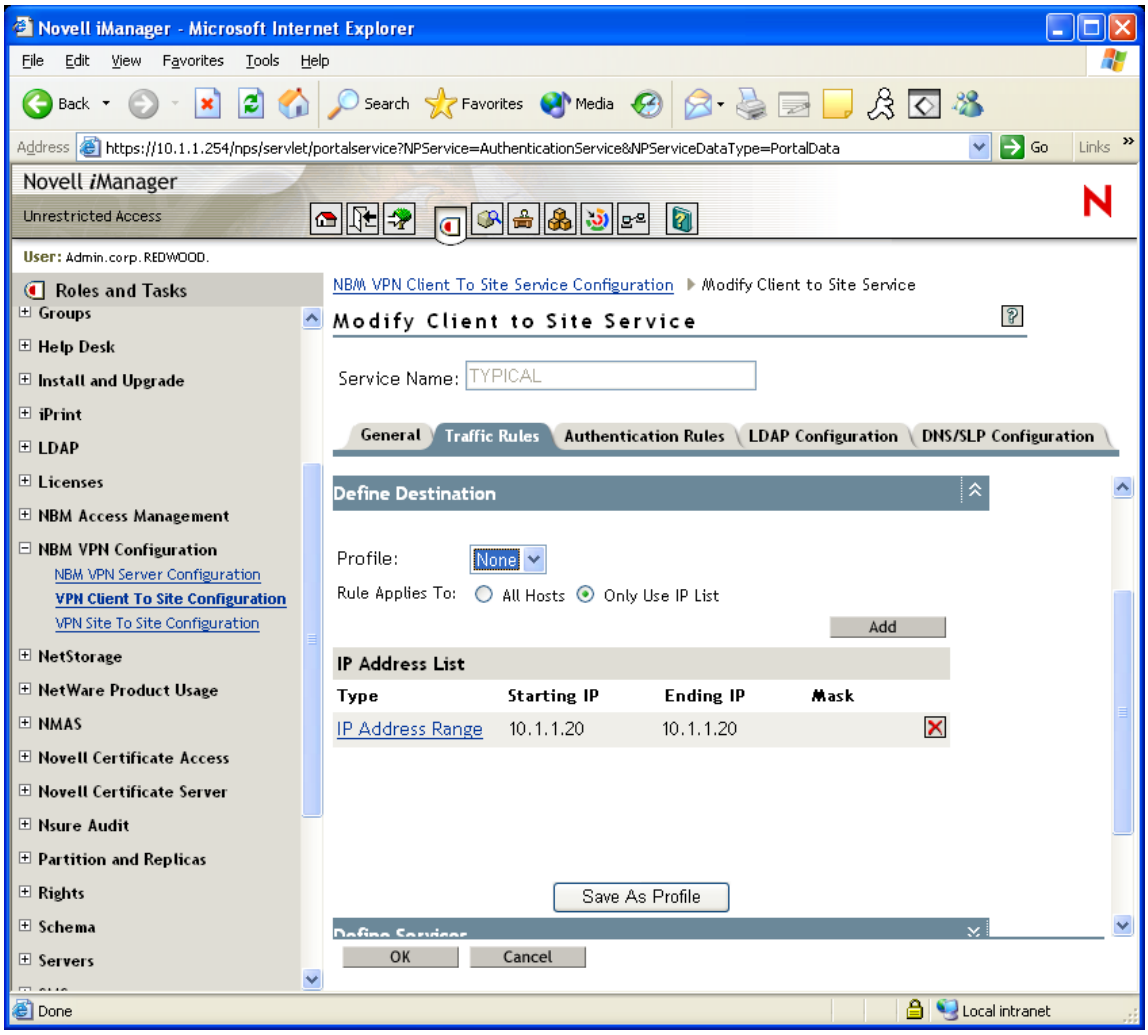
Enter the fully-qualified LDAP name of the **RemoteUsersGroup**, in this case **CN=VPNRemoteUsers,OU=phx,O=dd.** Be sure to use commas, not periods, for LDAP syntax, and watch for case-sensitivity.

Click **OK**.



Your entry is added as a LDAP Remote user or group name.

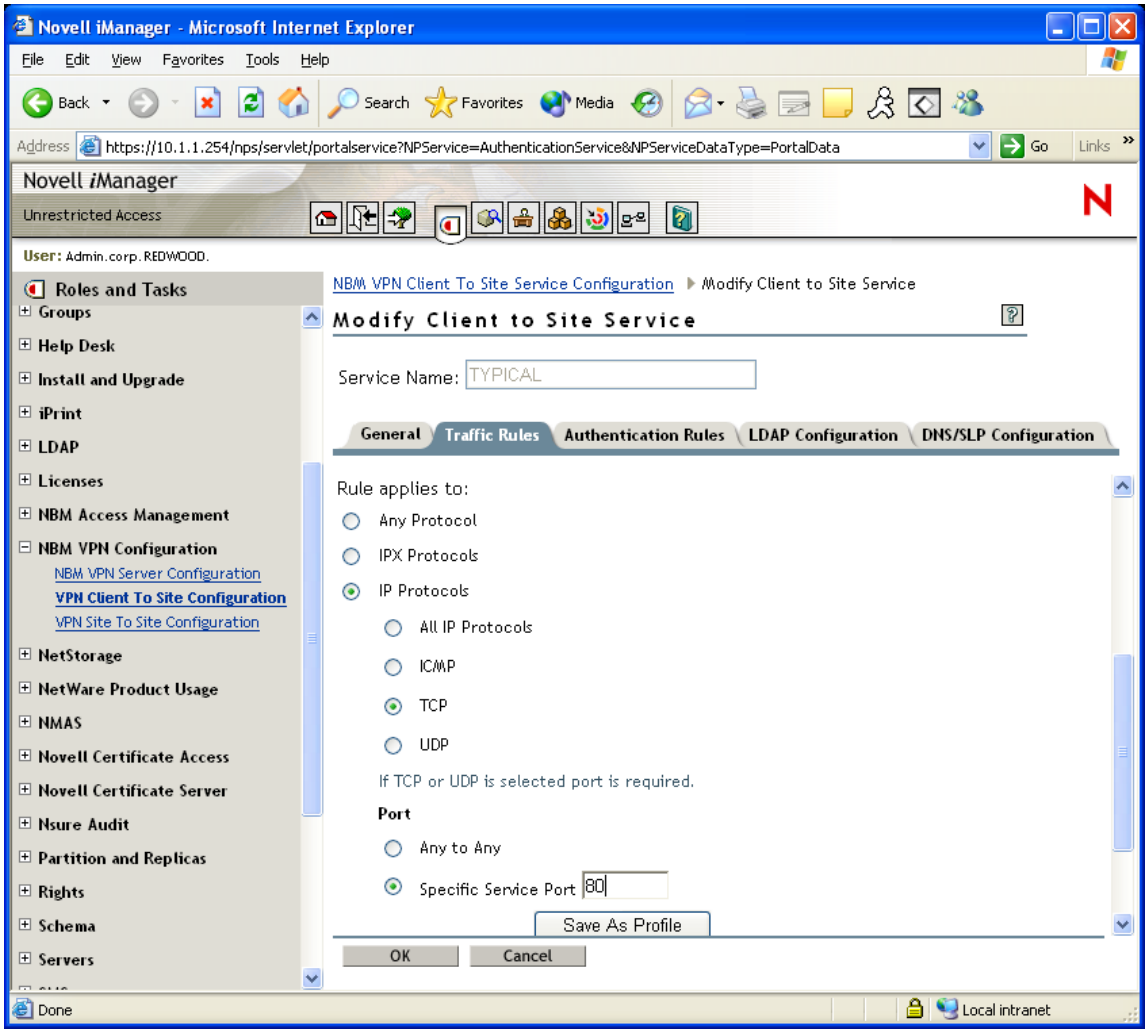
Expand the **Define Destination** section.



Select **Only Use IP List**.

Click **Add**, and add an **IP address range** of **10.1.1.20 to 10.1.1.20**.

Expand the **Define Services** section.



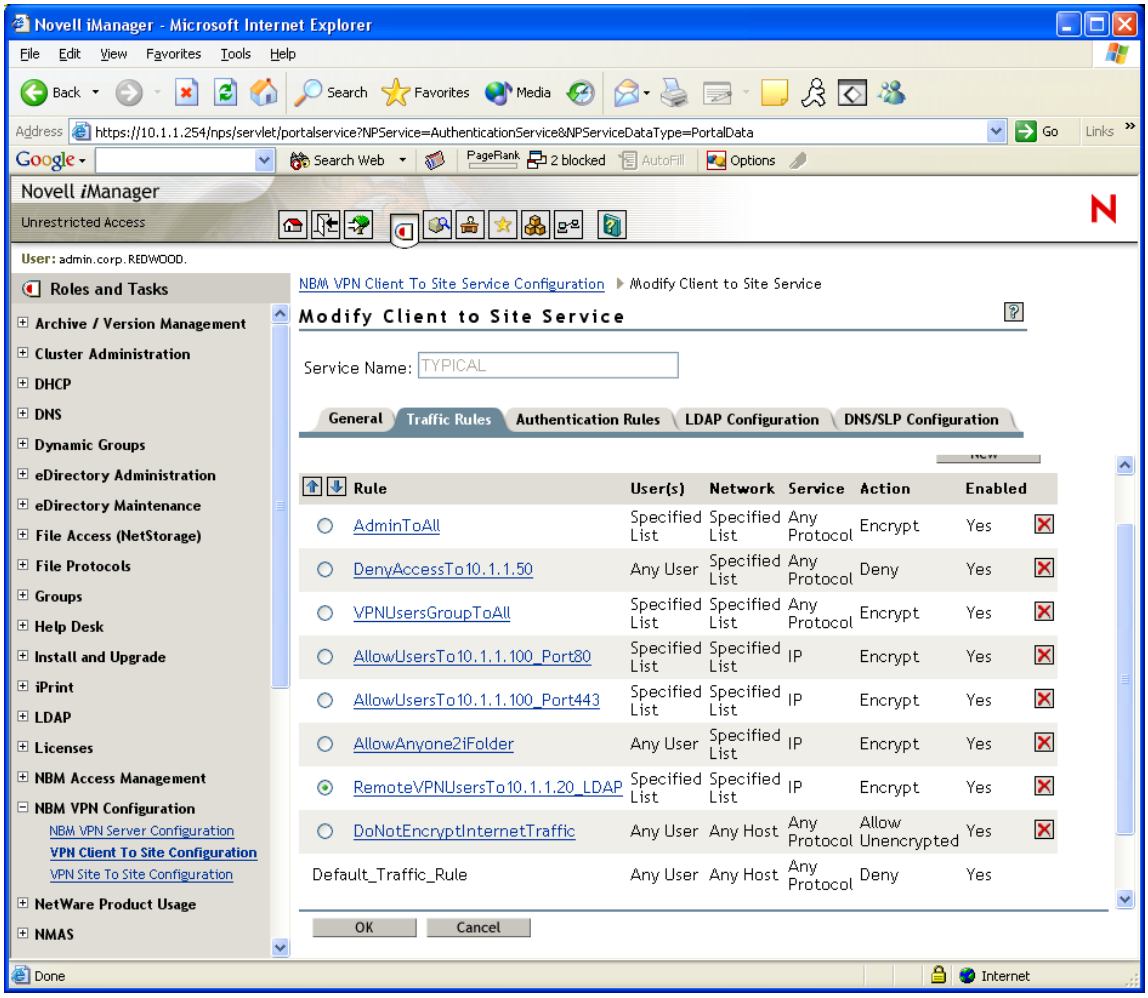
Select Rule Applies to **IP Protocols**.

Select **TCP**.

Select **Specific Service Port**, and enter a port of **80**.

Scroll down and click the **Apply** button.

The new rule applies at the bottom of the Traffic Rules list.



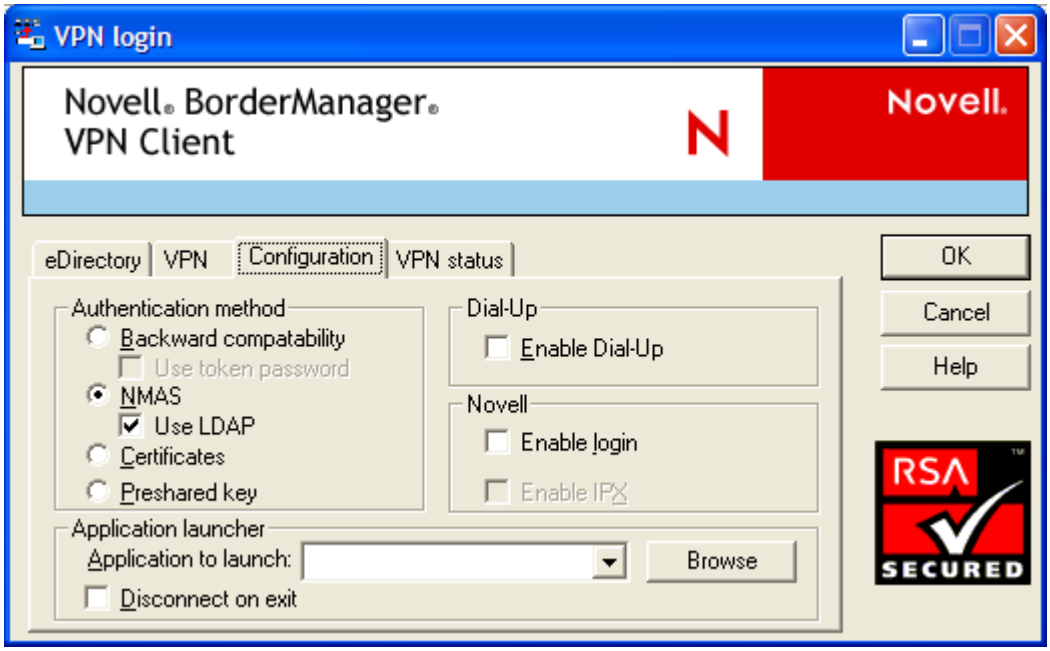
Move the new rule ABOVE the DoNotEncryptInternetTraffic rule! Otherwise the new rule will never be used, because the other rule bypasses VPN for all traffic.

Click **OK** to update the Client-to-Site service with the new changes.

You can now test LDAP authentication through the VPN. (You may have to STOPVPN and STARTVPN to get the new settings to work).

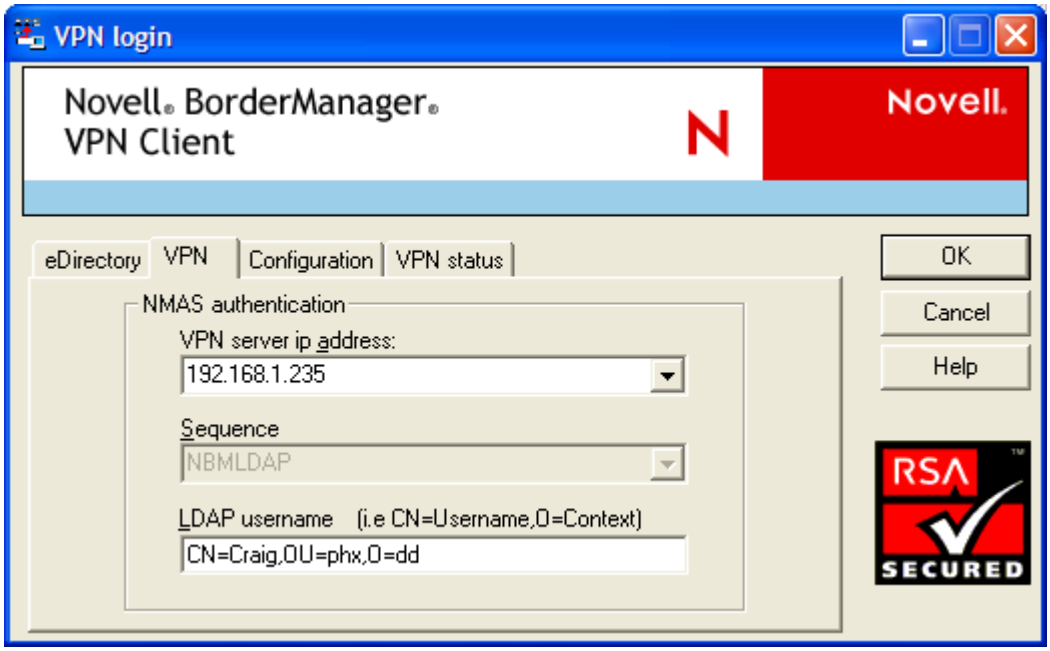
Note LDAP authentication is case-sensitive, to both user ID and password, although that may change with patch level on the servers involved. If you have user accounts in the remote directory such as “Craig”, you may be denied access if you try to authenticate as “craig” or “CRAIG”.

Configure VPN Client for NMAS/LDAP



Launch the VPN client, and select the **Configuration** tab.

Select **NMAS**, and **enable** the **Use LDAP** check box.



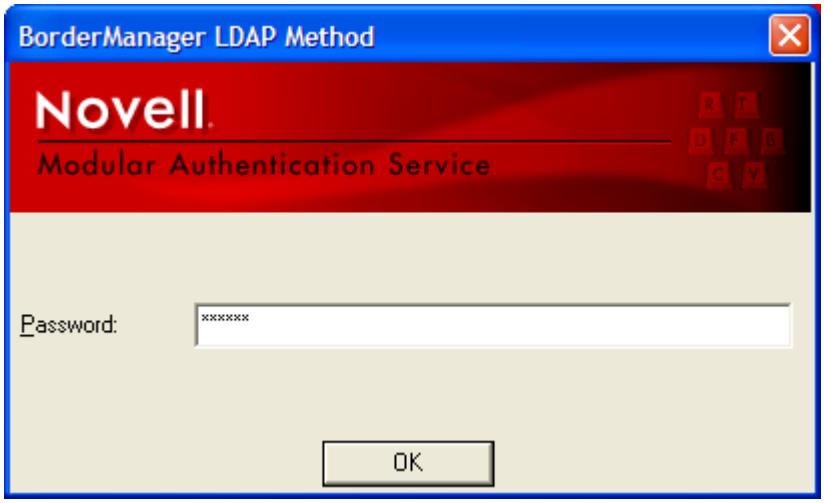
Select the **VPN** tab.

Enter the **public IP address** of the VPN server.

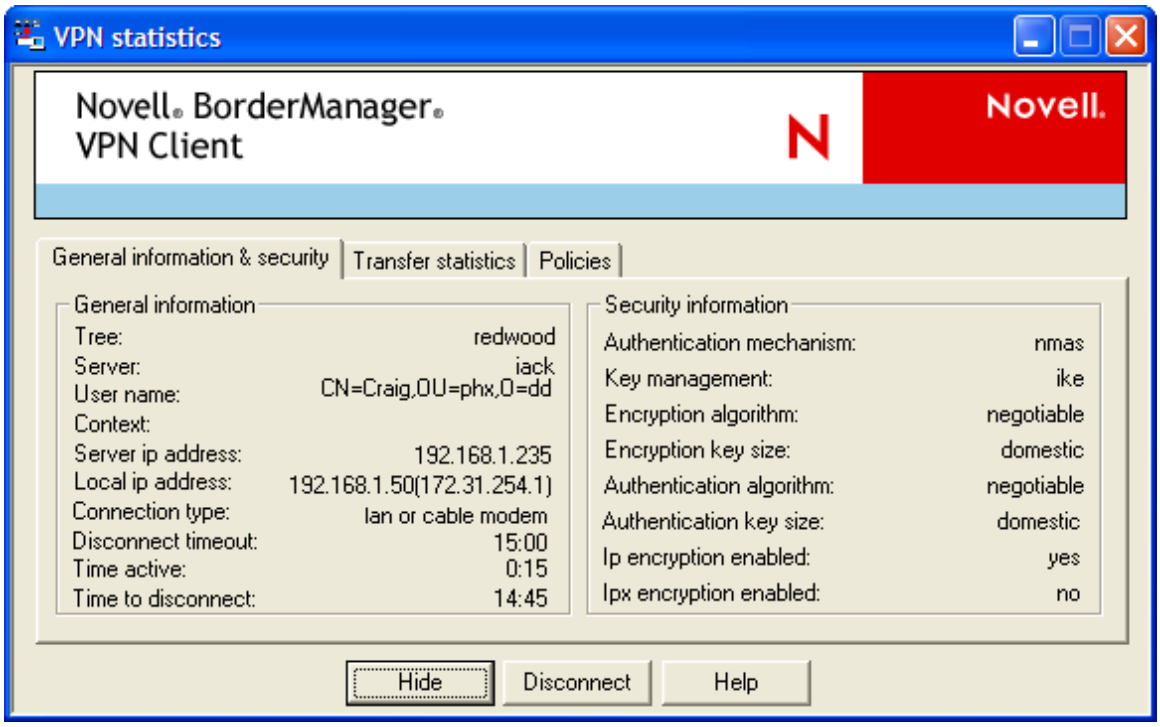
Enter a **fully-qualified LDAP username**.

The LDAP username must be one that exists in the remote LDAP server's directory, and must be allowed by settings in the LDAP Configuration menu in the Client-to-Site service. The name is case-sensitive.

Click **OK** to start the connection.



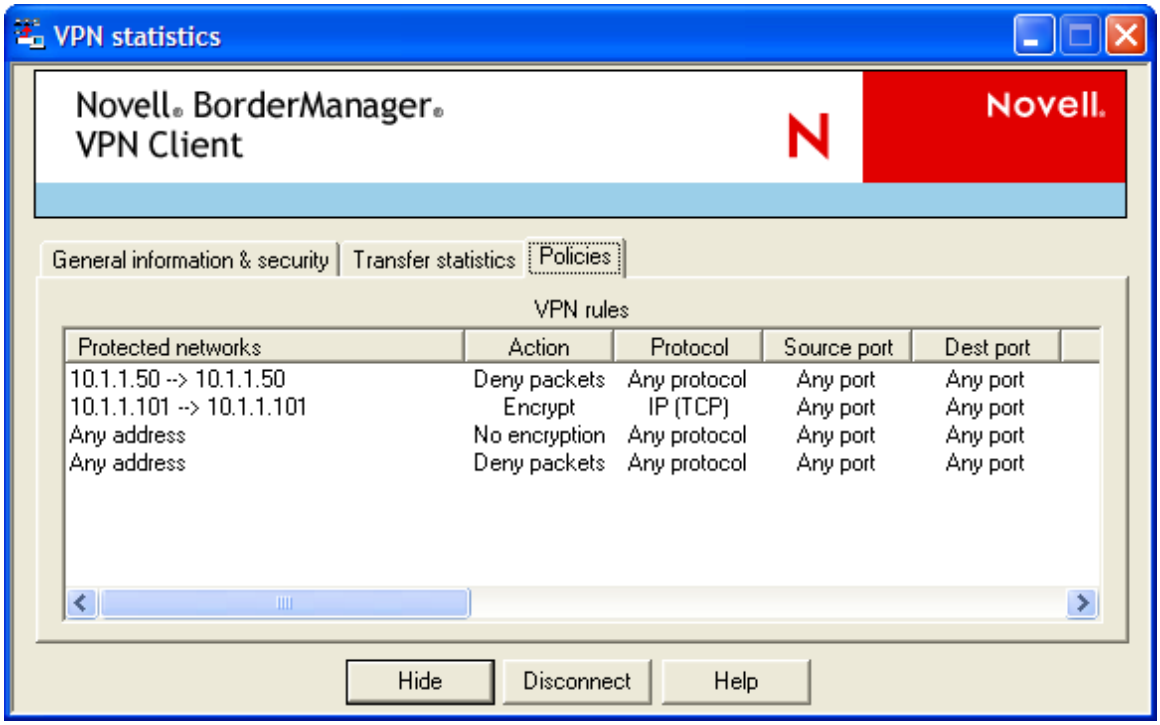
You should get a LDAP Password prompt. Fill in a valid **password**, for the user ID in the remote directory. Click **OK**.



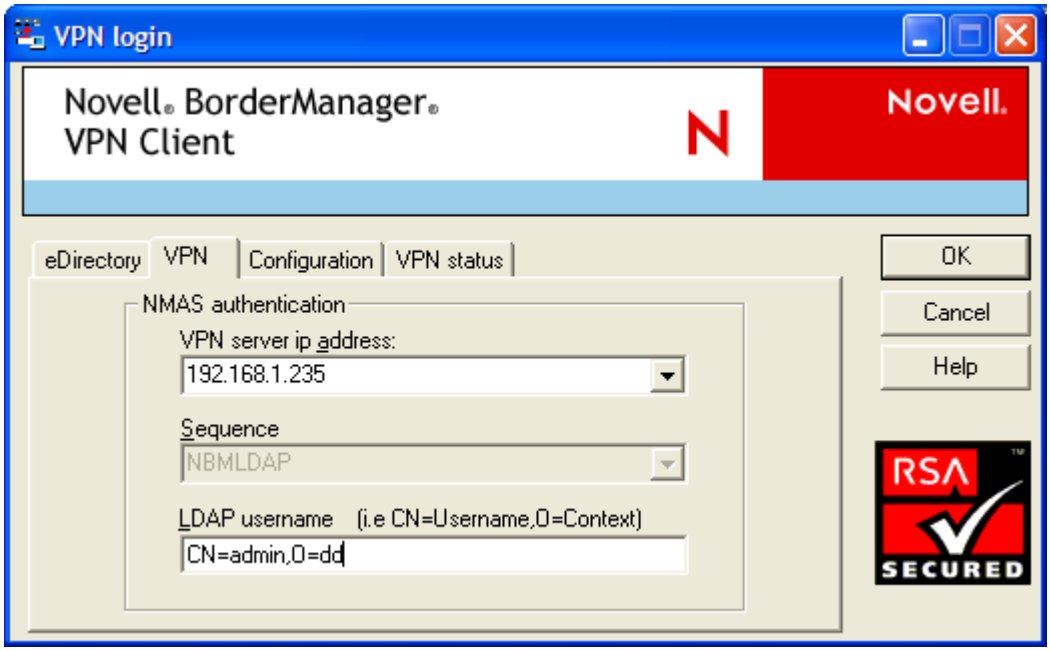
When connected through LDAP, the VPN client **General information & security tab** should show the LDAP user name, but the VPN server's NDS tree and server name.

This screen also shows the assigned VPN tunnel address (172.31.254.1 in the example above).

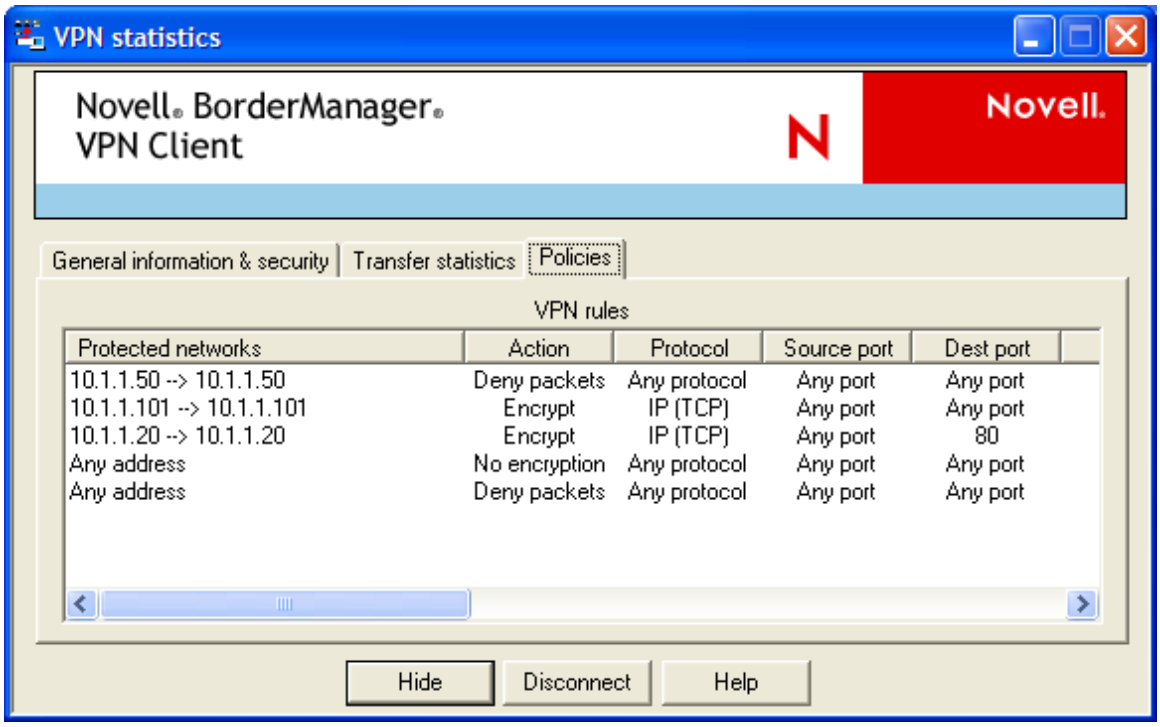
Select the **Policies** tab to see if the Traffic Rules are applying as expected.



Notice that the entry for the LDAP Group access to 10.1.1.20 is missing. This is because the only traffic rules being applied to the LDAP-authenticated client are those that apply to All Users. The traffic rule for RemoteVPNUsers is not applying here because Craig.phx.dd is not in that group.



Disconnect the VPN connection, and log in again as CN=admin,O=dd, a user that IS in the RemoteVPNUsers group.



Looking at the Policies for a member of the RemoteVPNUsers group, we can see a new entry in the middle of the list, encrypting data to 10.1.1.20.

Using BorderManager 3.8 VPN Client – Certificate Authentication Mode

Certificate Authentication mode uses a X.509 user certificate to authenticate the user to the VPN server. This mode would be used when non-Novell VPN client software is used to make a VPN connection. It can also be used with the Novell VPN client, although it is much more effort to configure than the NMAS NDS Password method.

In this mode, a special User Certificate must be created from the user ID in the NDS tree, and exported to a .PFX file. That .PFX file must be installed in a particular directory on the VPN client. Getting the file configured and installed on the client is further complicated by the fact that you can only export a user certificate for the user account in which you are currently logged in. **This means that the users must either export their own certificates, or you have to be able to log in as that user to export the certificate for them.**

There is a special case where this all becomes much easier to configure. That case is where a remote VPN user brings a laptop into the network, logs into the same NDS tree as the VPN server using Client32, and then makes use of a special option in the VPN client called 'Get Certificate'. The Get Certificate option not only gets a user certificate for the user, along with allowing the user to specify the certificate password, it actually produces the certificate in the first place. This procedure also stores the certificate in the proper directory on the client PC automatically.

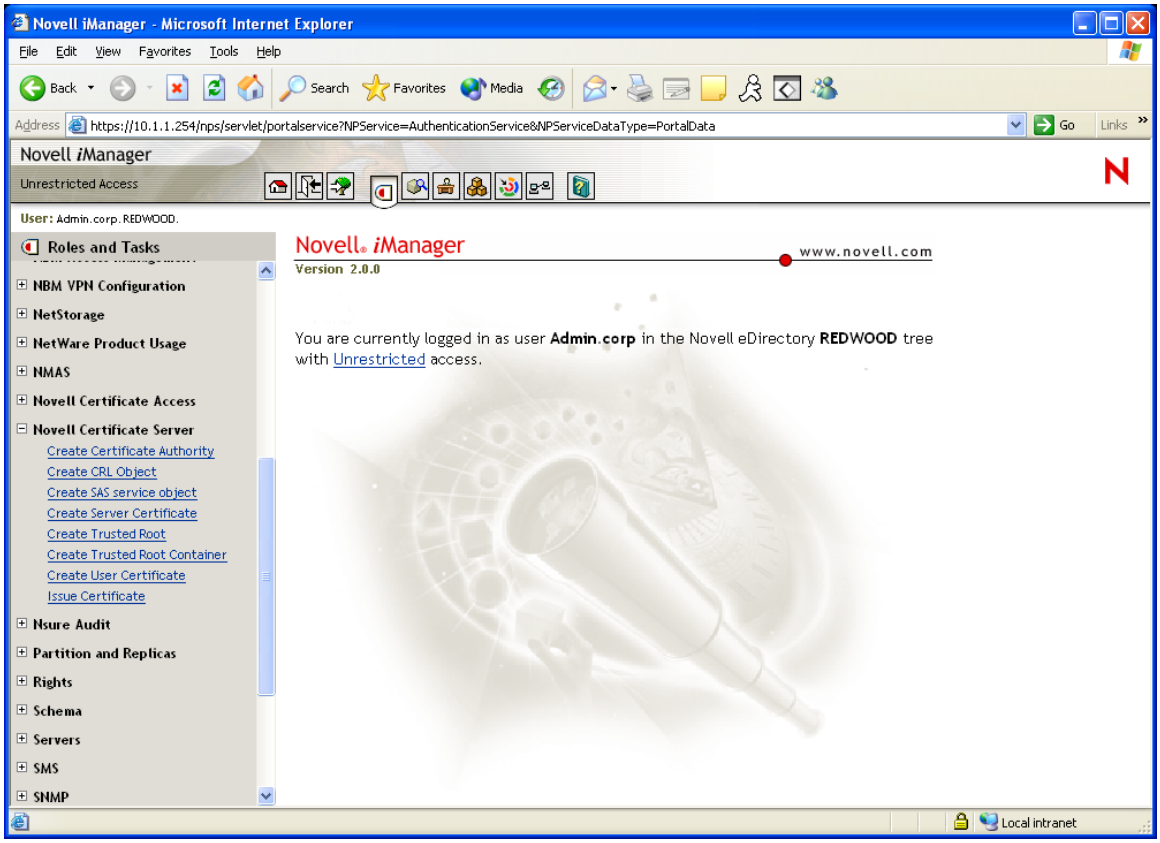
All other options involve more work, in terms of an admin creating user certificates, and having the user export there own user certificates, and finding a way to distribute the resulting PFX file and password to the users.

Create a VPN User Certificate

This example shows how to create a custom user certificate usable for VPN communication, and then export it to a file. An admin can create the User Certificate, but only the user can export it to a file.

The exported file can then be placed in the appropriate directory for the VPN client software to be used in certificate authentication mode. The appropriate directory for the Novell BorderManager 3.8 VPN client is C:\NOVELL\VPNC\CERTIFICATES\USERS.

Only the iManager method for creating a user certificate is shown, but the reader should be able to figure out how to do the same operations in ConsoleOne from the example.



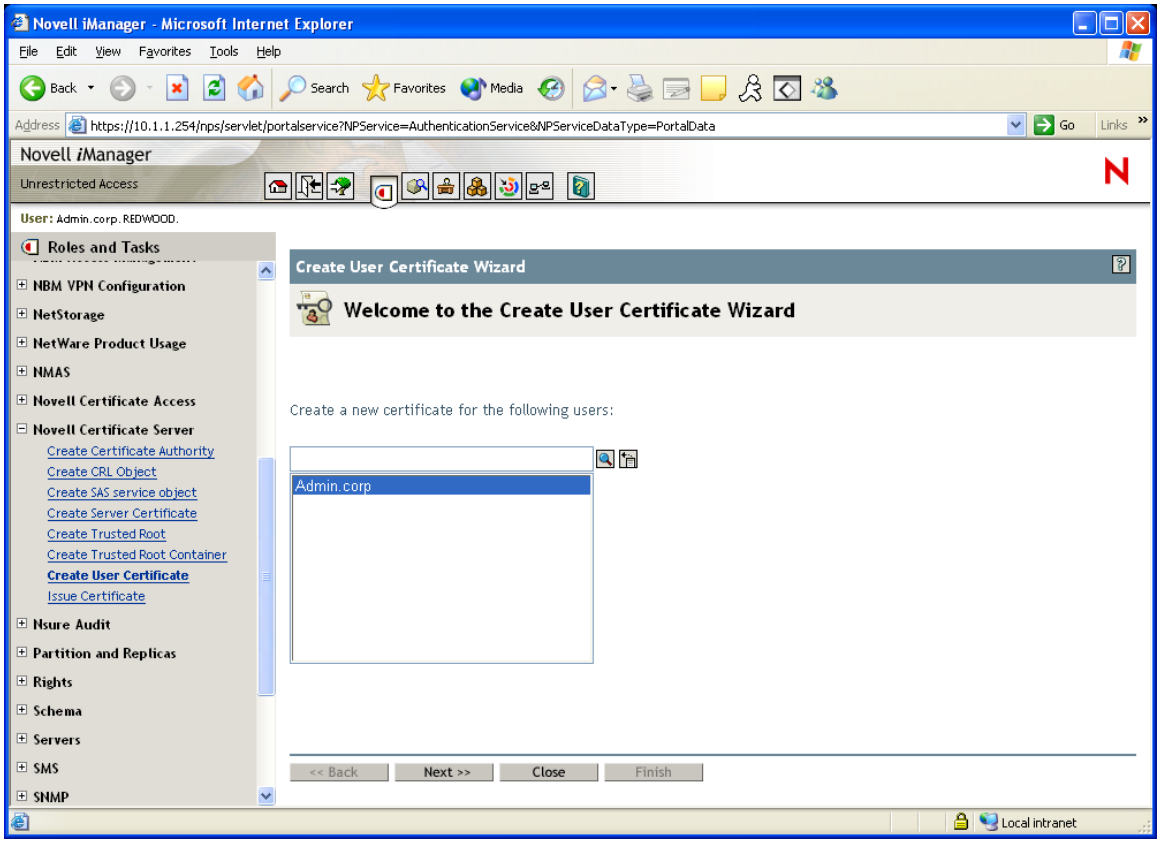
Start by logging into iManager.

Expand the **Novell Certificate Server** link.

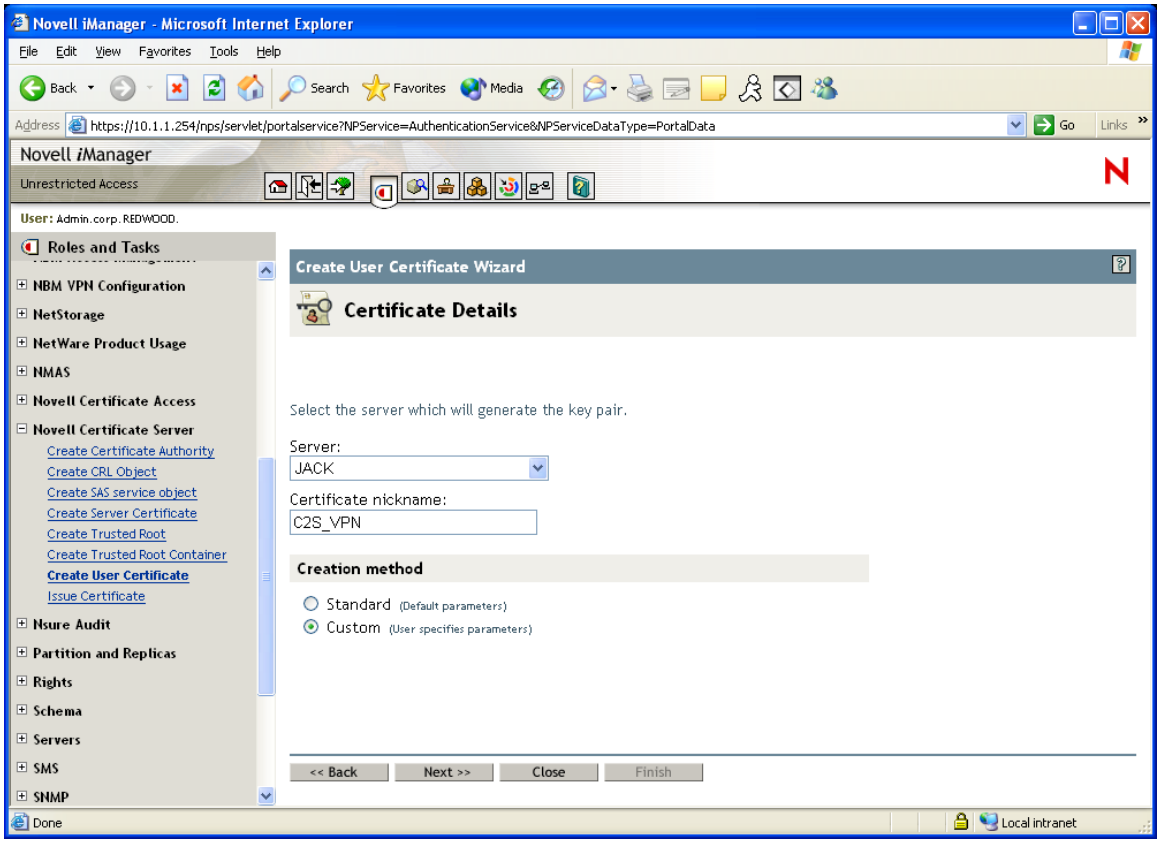
Click on **Create User Certificate**.

You should be prompted to select a user. You can also select multiple users and create user certificates for each.

Browse to the **Admin** account and **select** it.



With the user accounts of interest selected, click on **Next.**

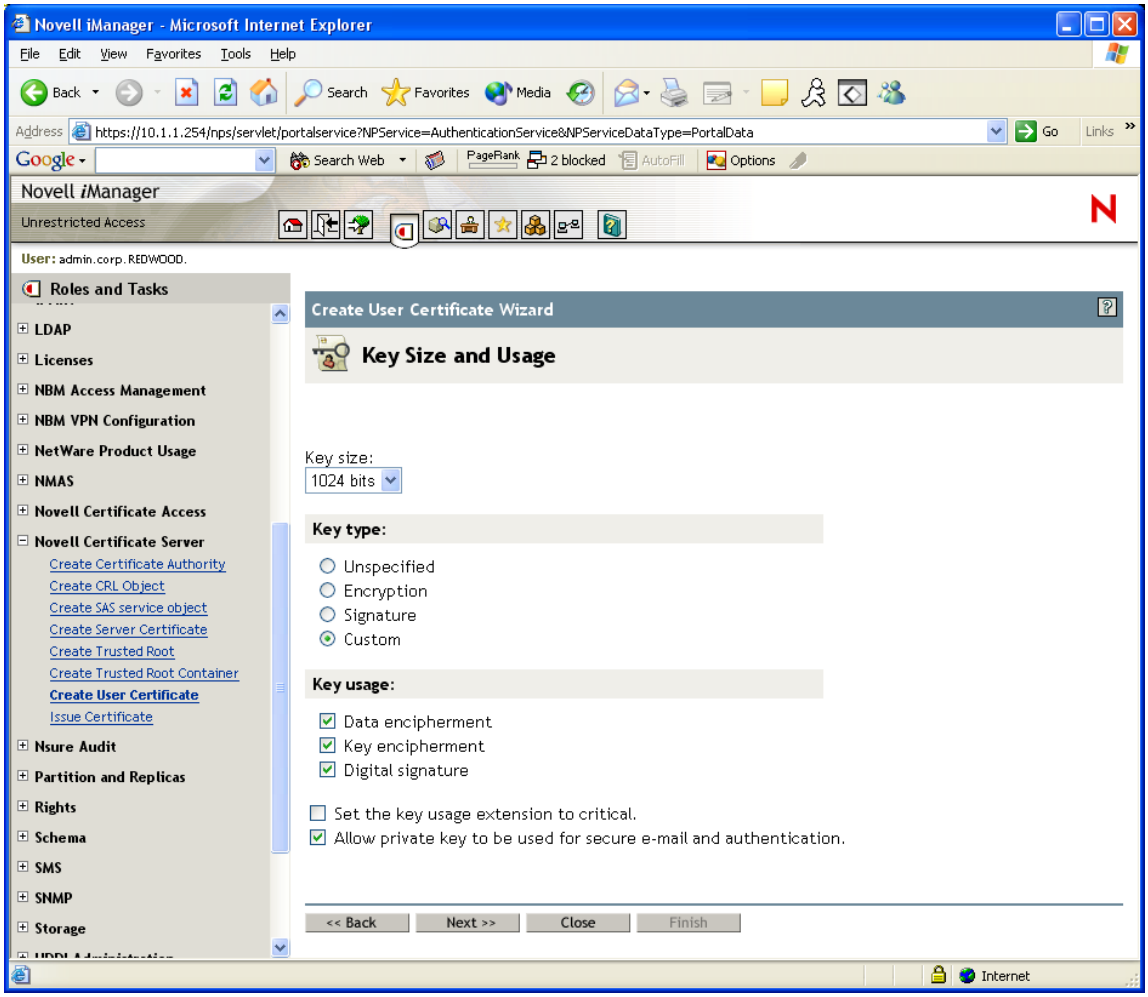


You must select the Server that will issue the certificate. Select the BorderManager 3.8 server.

Give the certificate a descriptive name in the **Certificate Nickname** field. This name will identify the particular user certificate within the NDS user access later. (A user can have multiple user certificates, each created with different settings).

Under **Creation Method**, choose **Custom.**

Click **Next**.



Set the **Key Size and Usage** parameters as follows:

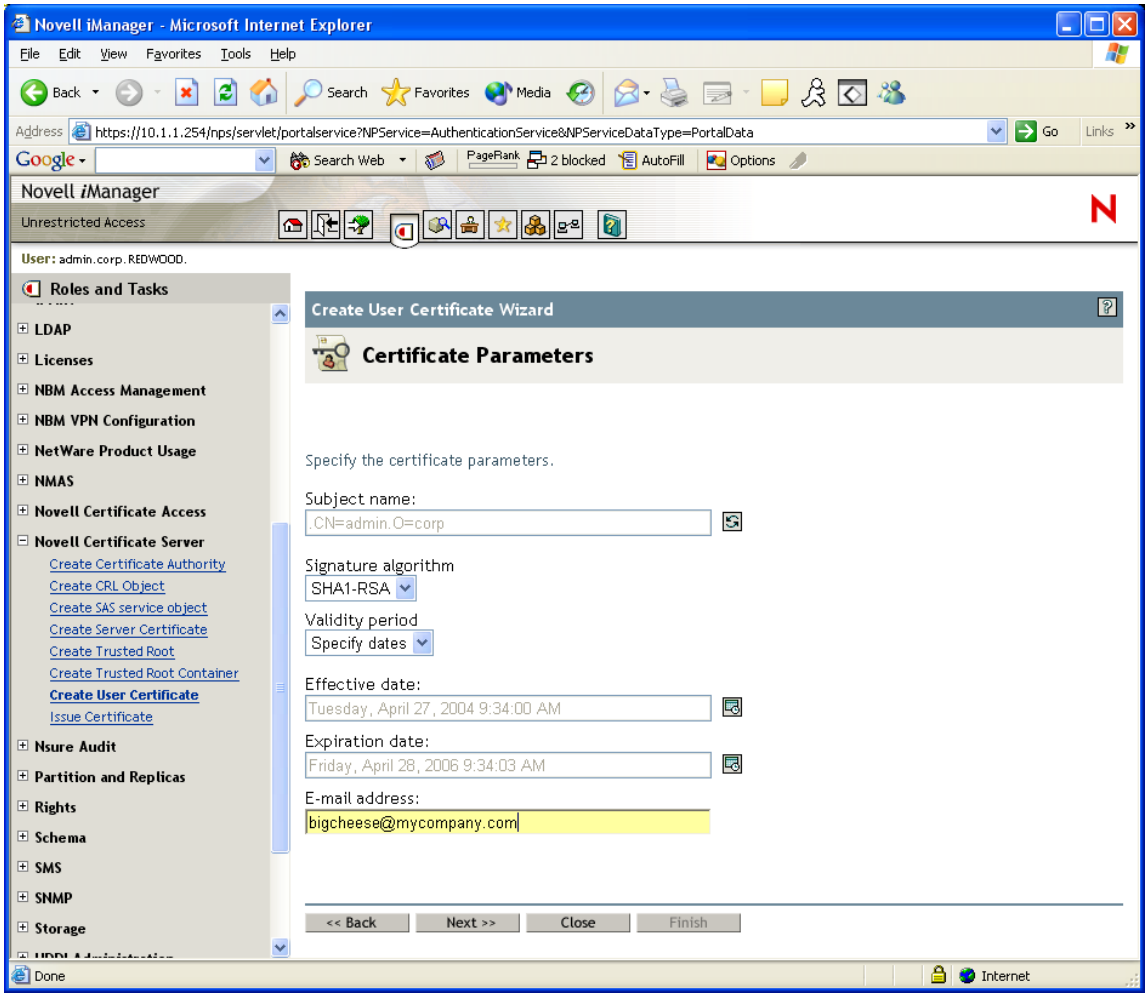
Key Size: 1024 bits

Key type: Custom

Key Usage:

- **Data encipherment enabled**
- **Key encipherment enabled**
- **Digital signature enabled**

Click **Next**.



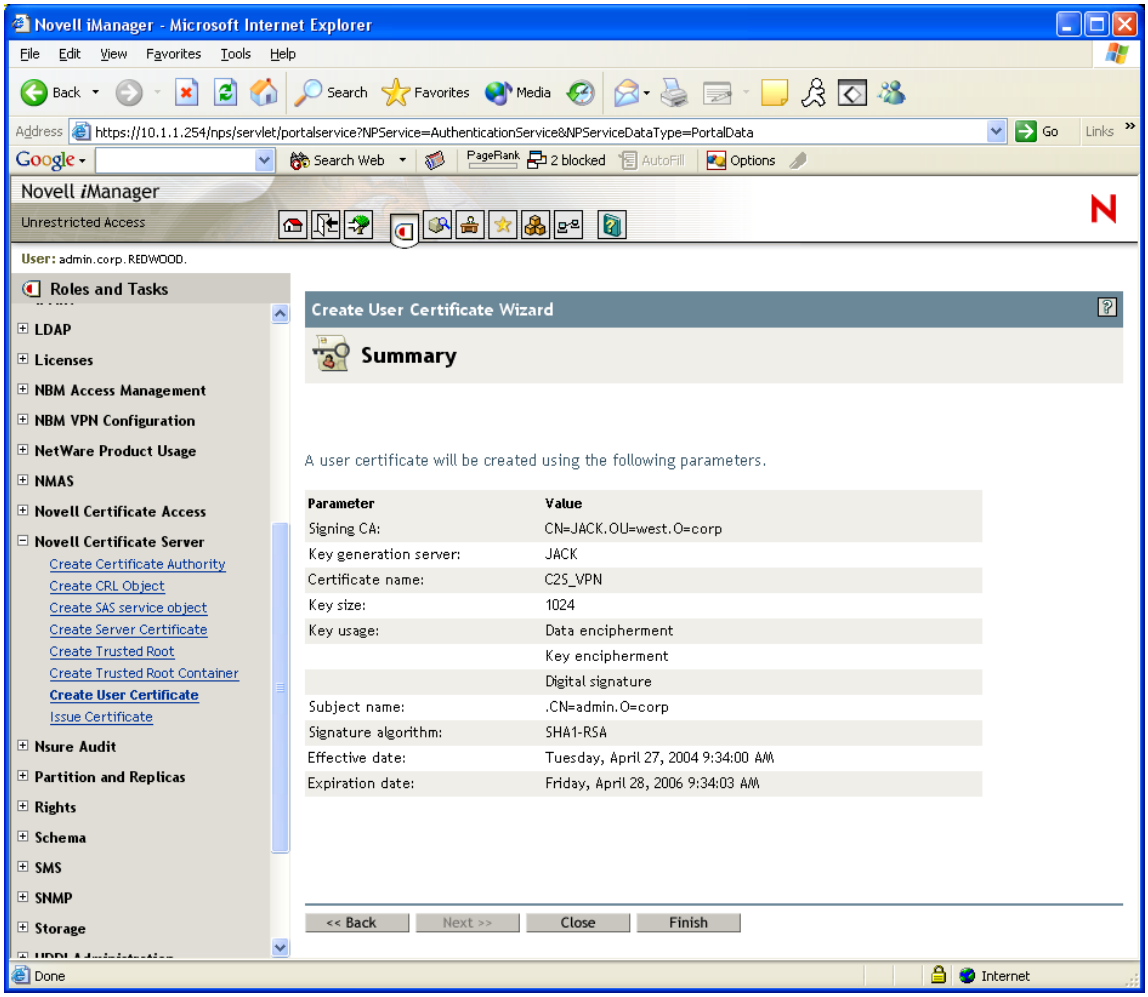
In the **Certificate Parameter** menu, change to the following parameters:

Validity Period: Specify Dates

Effective date: (pick yesterday's date)

E-mail address: fill in the user's email address (optional).

Click **Next.**



You will see a **Summary** screen.

Note the Subject Name. (**CN=admin.O=corp in this example**). This subject name is what you enter in a Client-to-Site Authentication Rule to allow the user with the certificate to authenticate.

Click **Finish**.

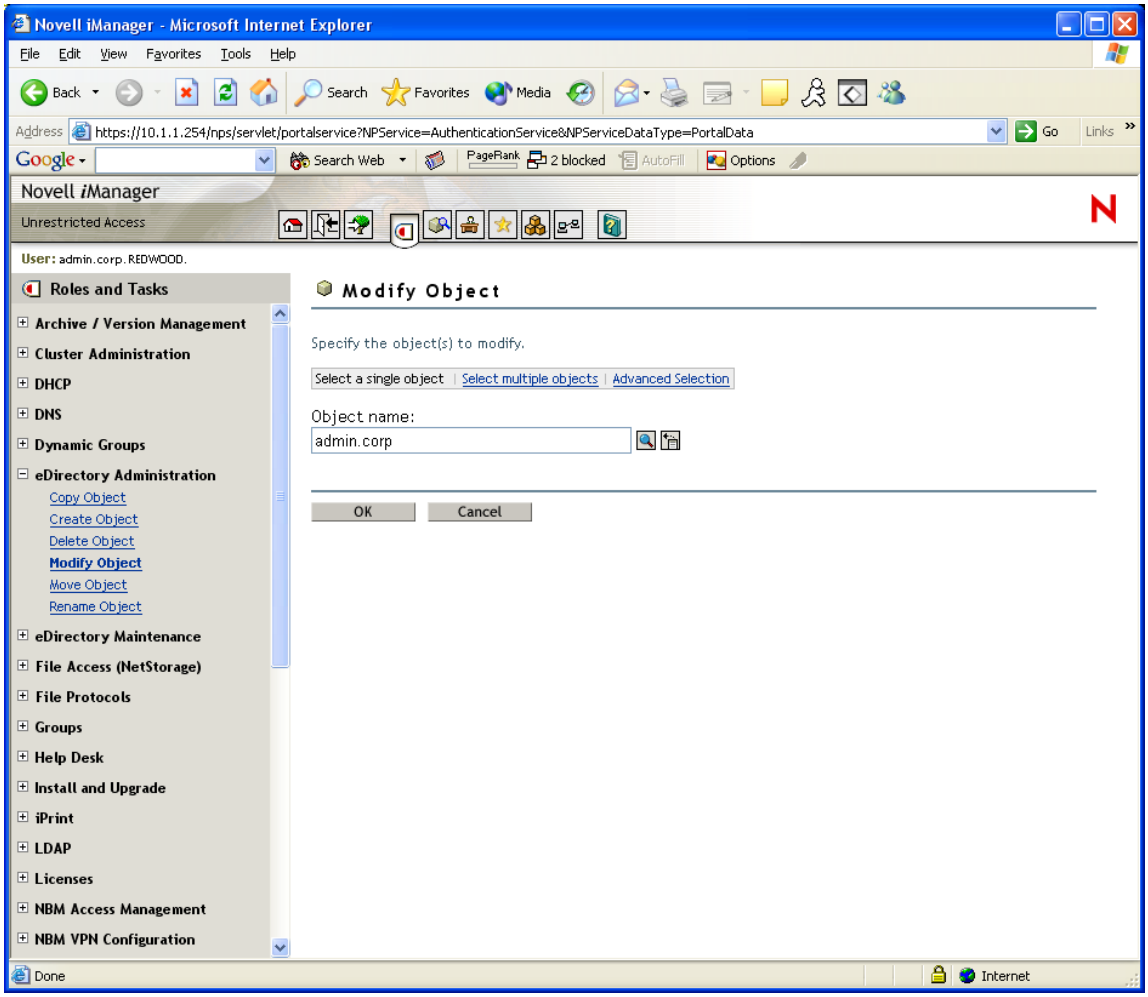
You should see a **Success** screen. Click **Close**.

Export a User Certificate to a File

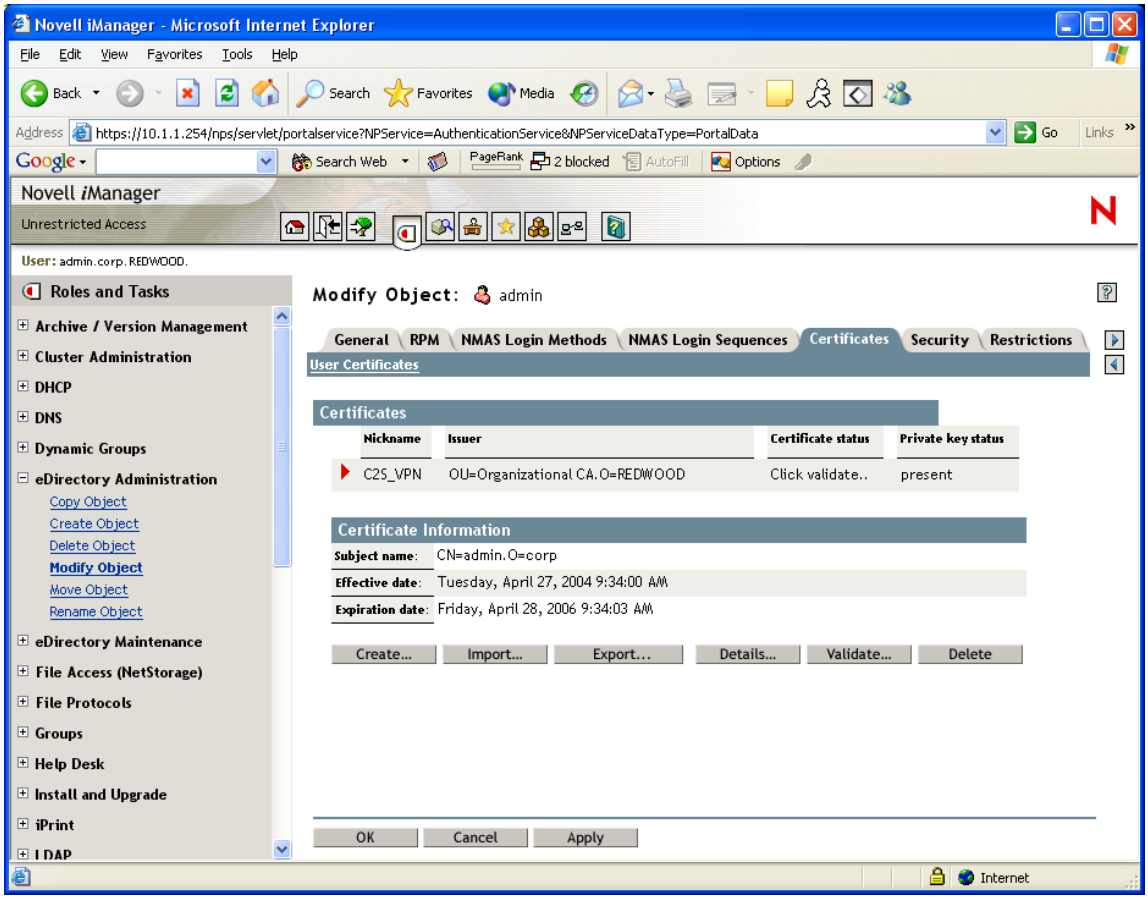
Once the user certificate has been created, it must be exported to a file to be used on a remote VPN client.

The export procedure is simple, but has a huge limitation: **only someone logged in as the user can export that user's certificates**. An Admin user can export the user certificates for the Admin account, but not for other user accounts. Each user is expected to export his/her own certificate, partly because the export process also imbeds a password into the certificate for later use.

Start by logging in to iManager (as the user needing to export the certificate, Admin in this example), and expand the **eDirectory Administration** link. (ConsoleOne can also be used to export user certificates). Select **Modify Object**. You should see a menu to select a user. **Browse** to the **user object** and select it.



Once you have selected the user account, click **OK**.

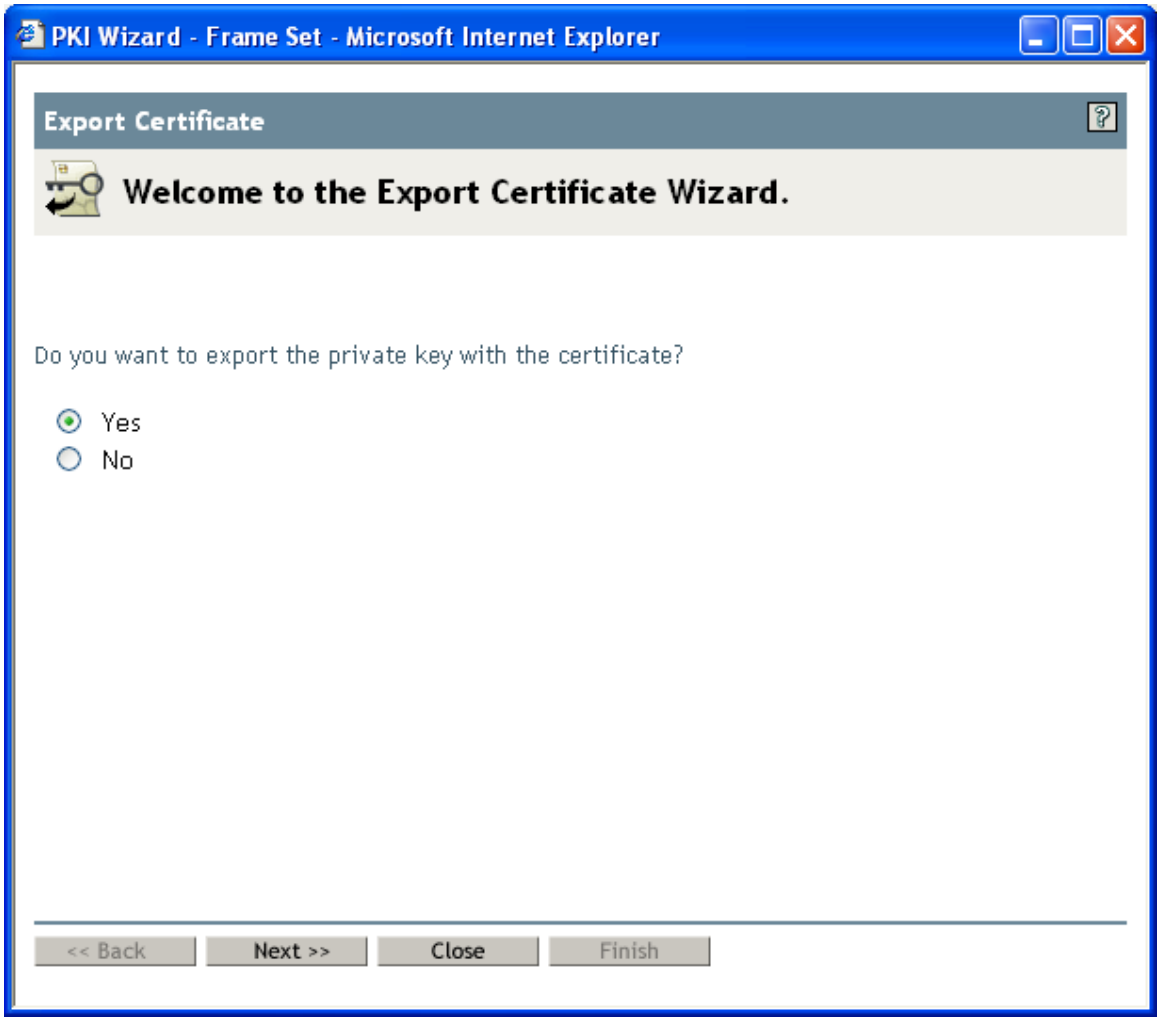


You should see the user account details. Choose the **Certificates** tab.

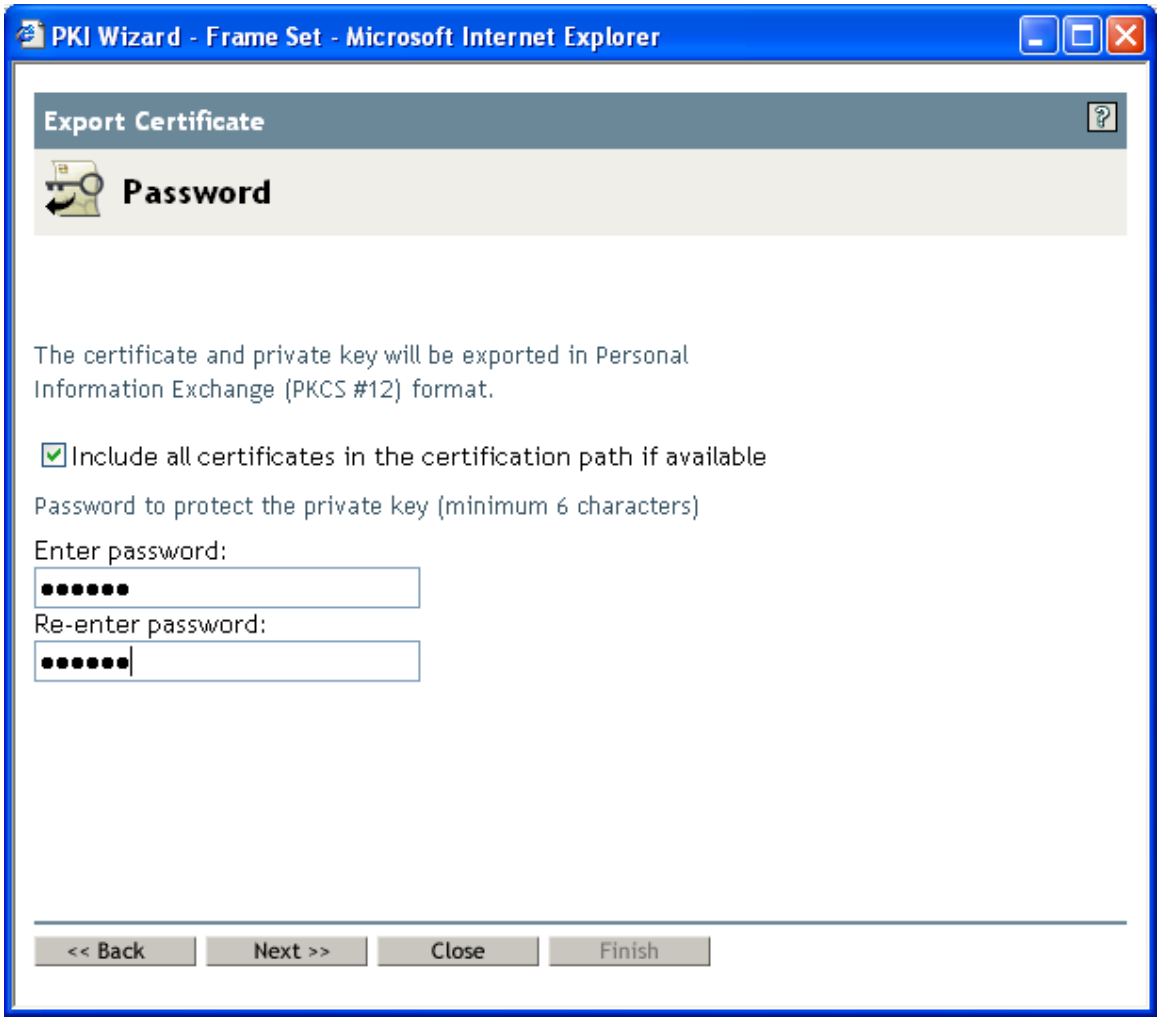
If there is more than one user certificate, select the one created for VPN usage.

Click on **Validate**, and make sure the user certificate is valid before continuing.

Click on **Export.**



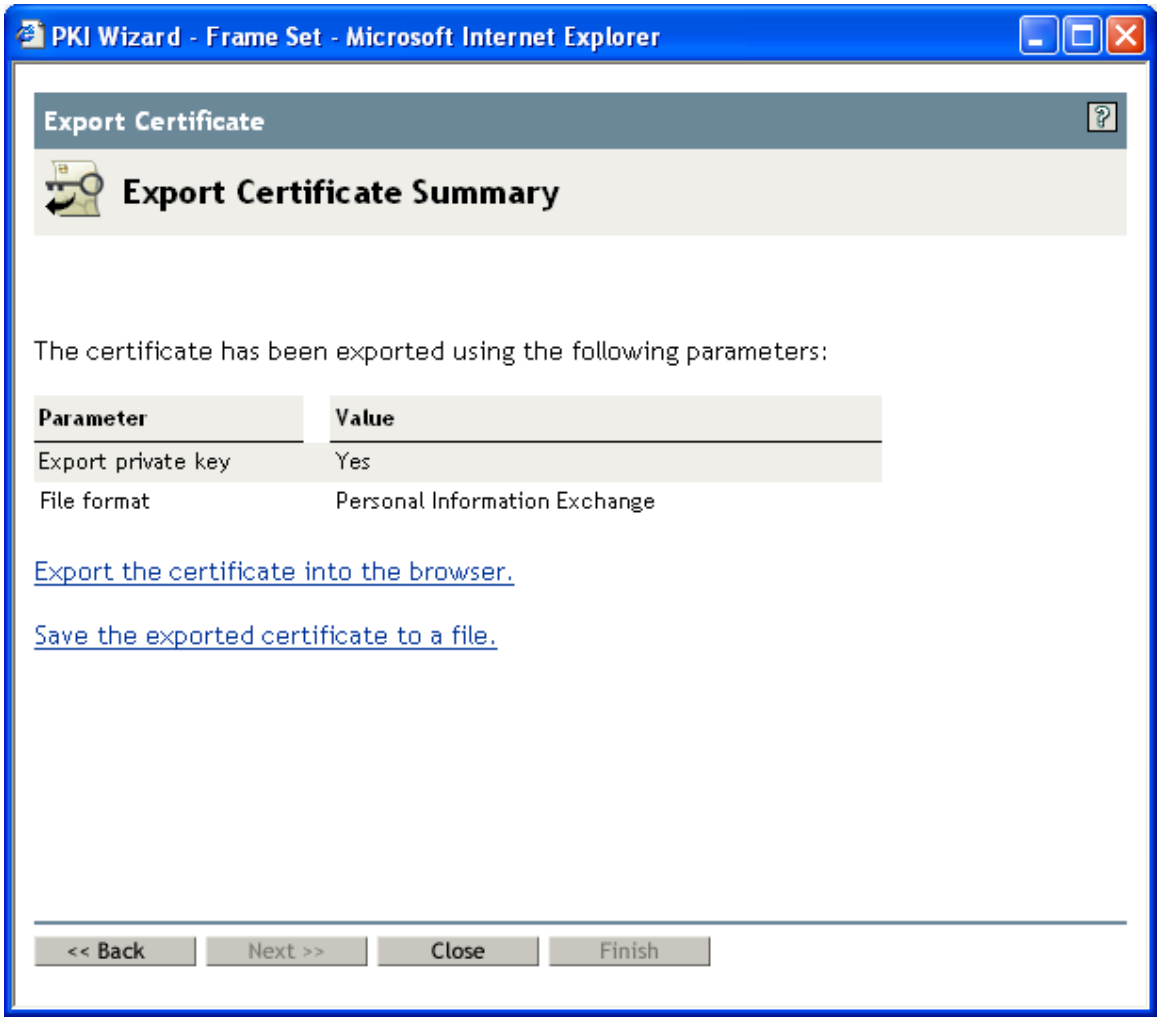
You want to export the private key with the certificate. Select **Yes**. Click **Next**.



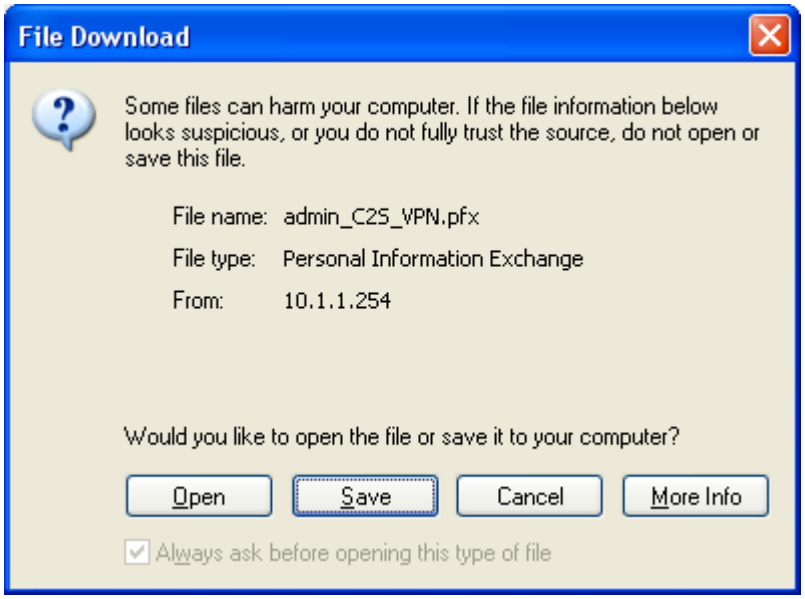
You must enter a **password** to protect the private key. You must use a minimum of six characters in the password.

The user will need to know this password later in order to use the certificate.

Click **Next**.



At the Export Certificate Summary menu, click **Save the exported certificate to a file**.



A file save dialog box should appear. The file name is already chosen for you.

Save the file where you can later (as the user) retrieve the file so that it can be copied to the remote VPN client.

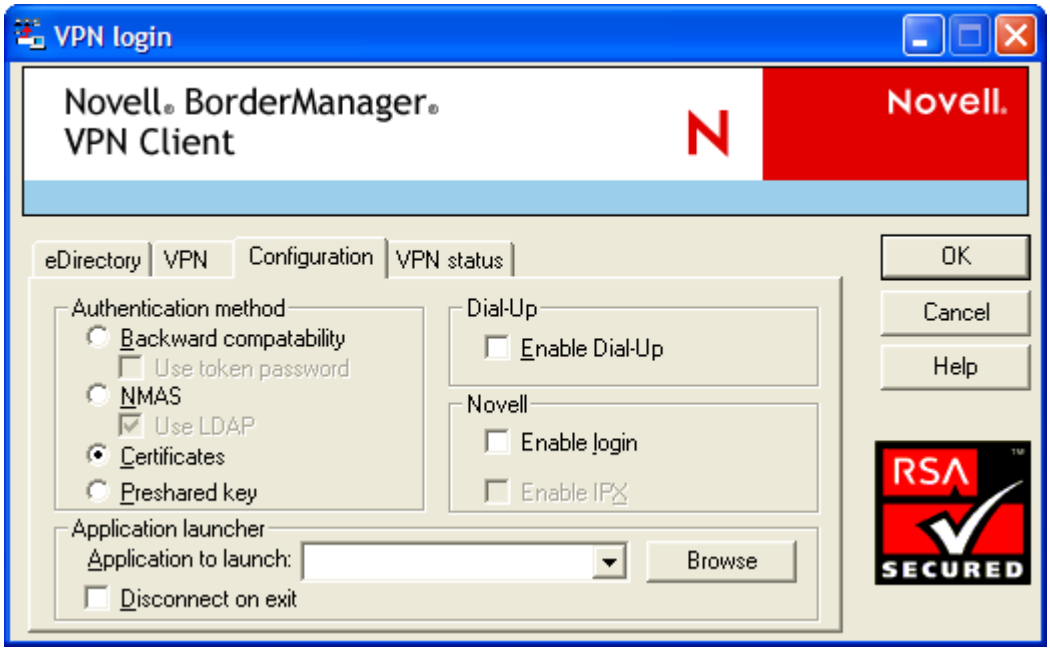
Once the certificate has been saved to a file, it needs to be placed in a particular subdirectory under the Novell VPN client.

Copy the file to the client's **C:\Novell\VPNC\Certificates\Users** directory.

VPN Client Option – Get Certificate

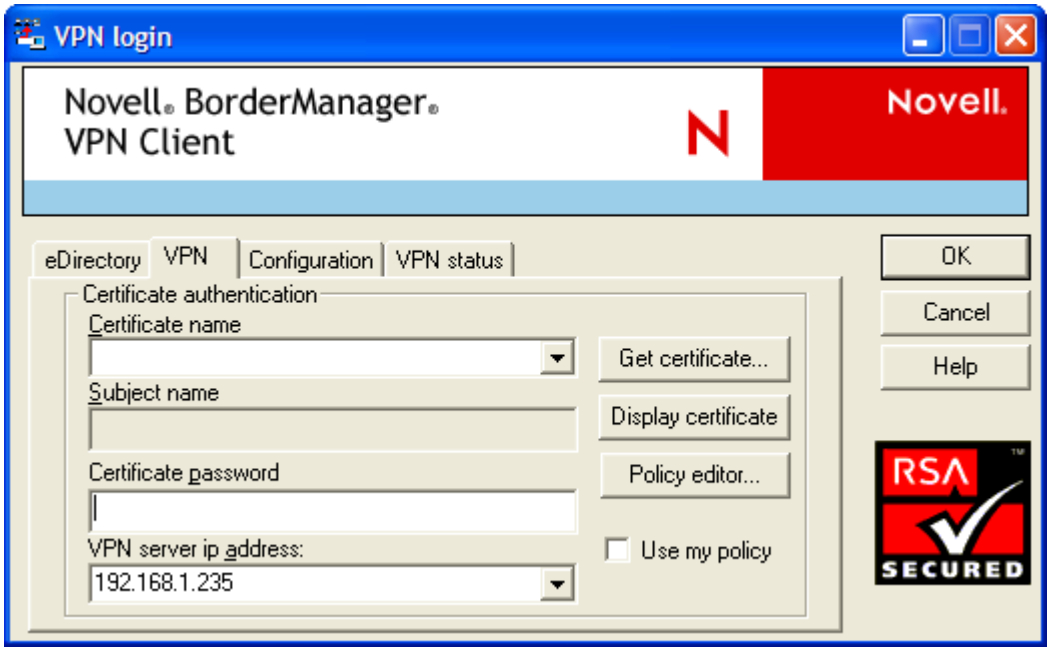
Another way to have a user get a user certificate for use in the Novell VPN client is to make use of the Get Certificate option in the VPN client itself. This option has the advantage that it can not only get the certificate automatically (export the file and put the file into the proper VPN client directory), it will also create the user certificate to start with.

However, this method has the severe limitation that the user must already be logged into the NDS tree, inside the LAN, and not by using the VPN client connection. This effectively means that the method is designed for users who can bring their laptops into the network, and use the Get Certificate method while connected on the inside of the firewall.

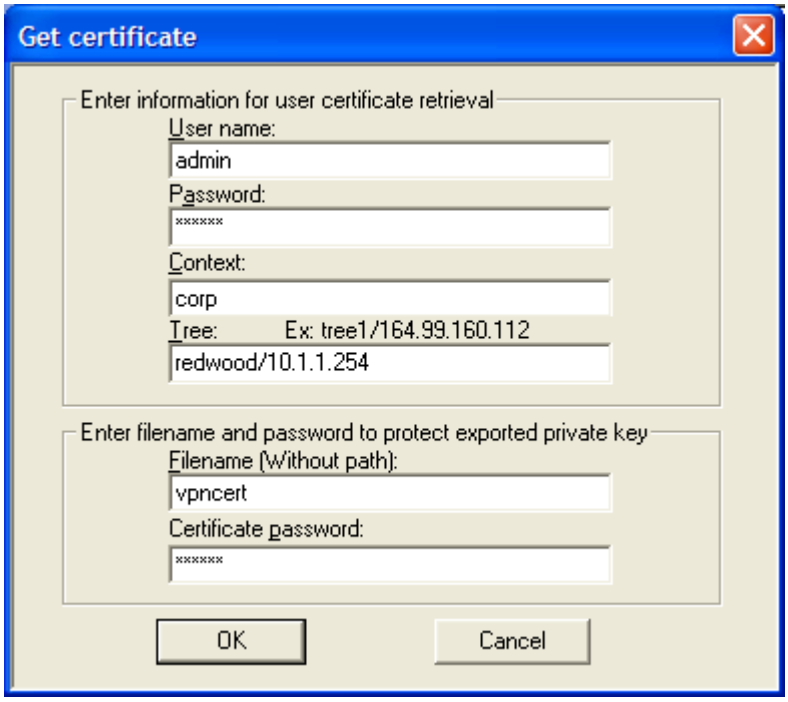


While logged into the network, launch the VPN client, go to the **Configuration** tab, and select **Certificates**.

Change to the **VPN** tab.



Click **Get certificate…**



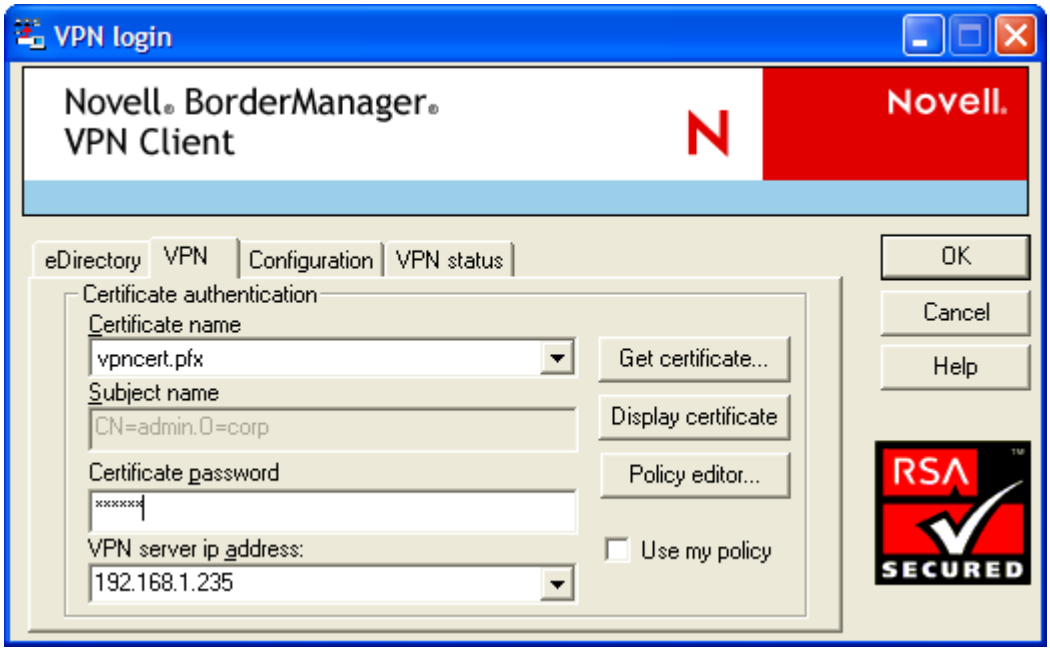
Fill in the **user name**, **password**, **context** and **NDS tree** where the user certificate is to be created.

The user name must already exist in the context.

Note The tree name needs to be entered in the format **<tree>/<ipaddress of VPN server>.** In the example shown, the tree name is redwood, and the IP address used is the private IP address of the BorderManager server, but could be any server in the NDS tree.

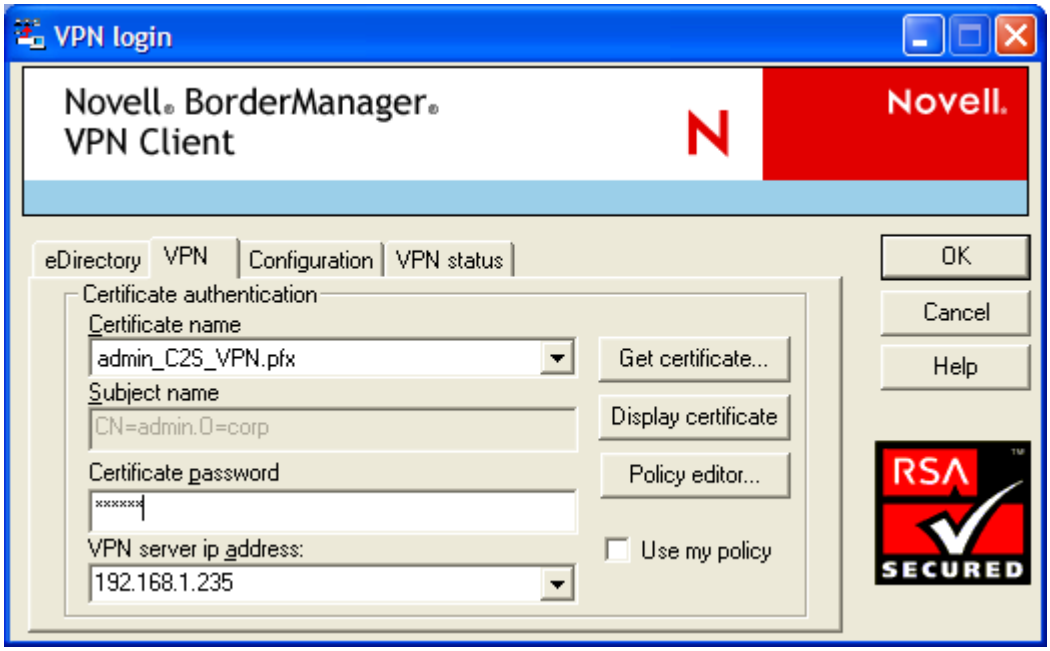
Also type in a **file name** for the certificate and **certificate password**.

Click **OK**. If this method works, you will a) create a new user certificate, and b) have your certificate installed automatically in the VPN client.



Once you have the certificate created, and the pfx file in the proper location in your VPN client directory (C:\NOVELL\VPNC\CERTIFICATES\USERS), you should be able to select the certificate and enter its password.

The **Subject name** of the certificate will not be displayed unless you type in the **password** for the certificate. Shown above is the certificate created through the 'Get Certificate' method, when the PC was connected to the network and logged in.

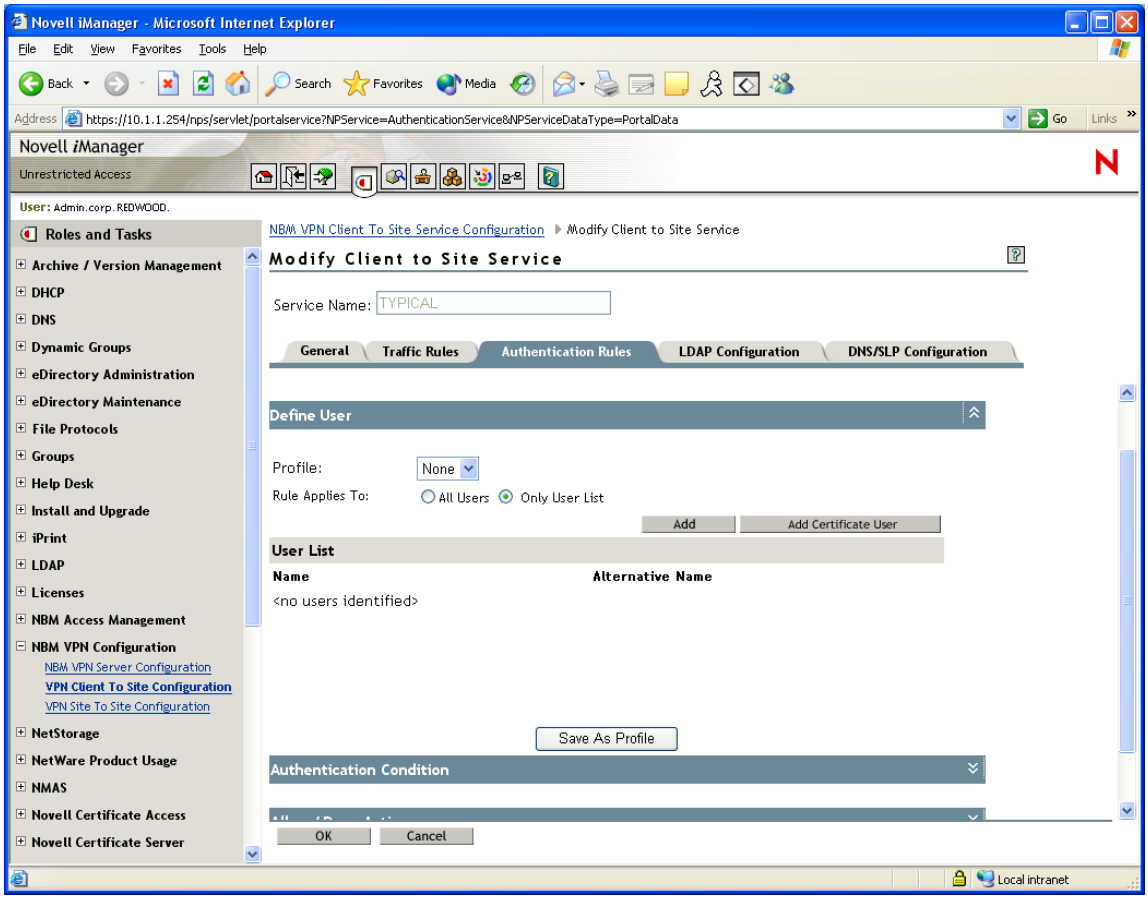


Shown above is the certificate created and exported in iManager. The resulting pfx file was copied to the proper location on the VPN client PC as described earlier.

Either certificate will work.

Configure Certificate Authentication / Traffic Rules

In order to use the Certificate Method of authentication in your Client-to-Site VPN, you should have an access rule in iManager that allows either the particular certificate subject name, or an access rule that allows all users. You will also need a traffic rule that calls out the certificate subject name or all users. This example shows how to add a rule for each, allowing only the admin user in the REDWOOD tree to authenticate in certificate mode.



Go to your Client-to-Site configuration, and choose **Authentication Rules**.

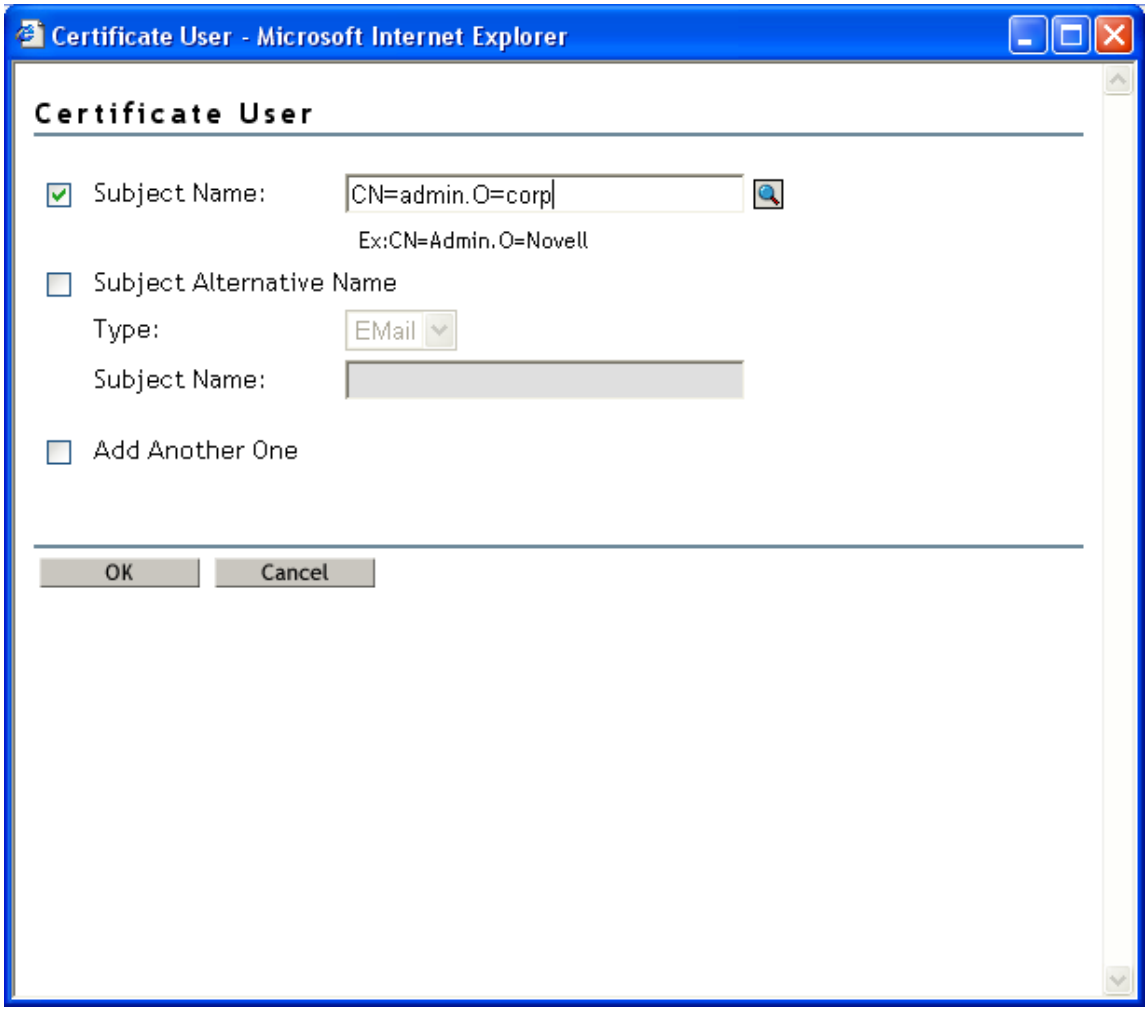
Click on **New** to add a new rule.

Give the new rule the name **AllowCertificates.**

Expand the **Define Users** section.

Select **Only User List**.

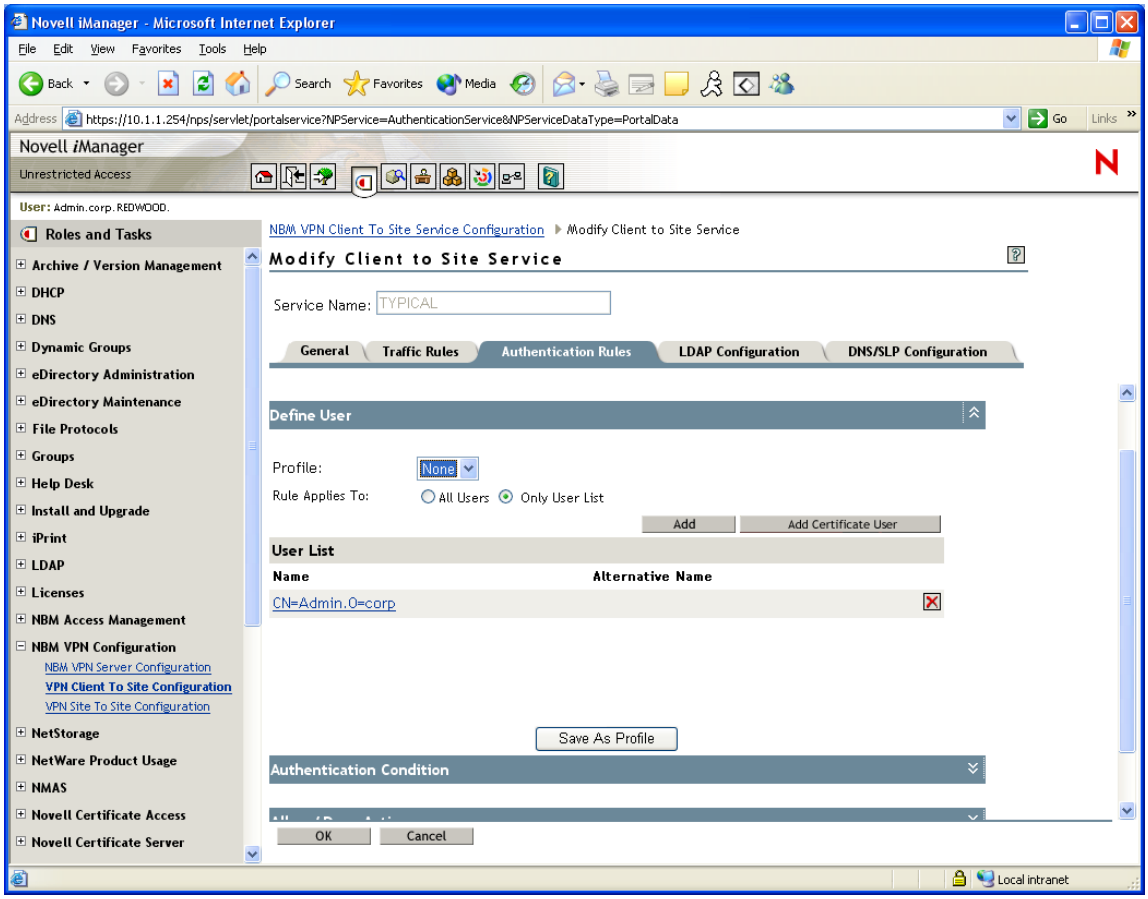
Click on **Add Certificate User**.



A **Certificate User** menu appears.

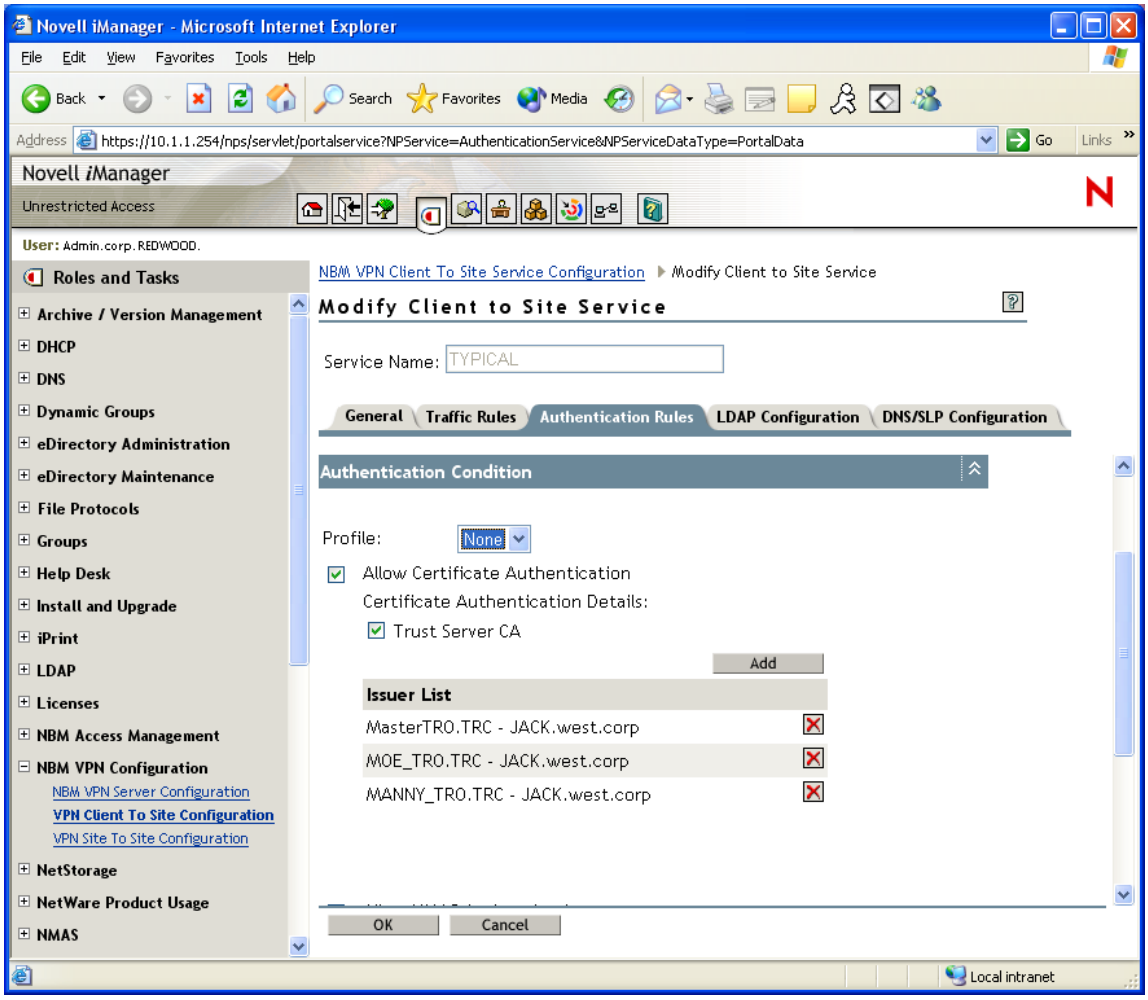
If you are adding a certificate user that is in the same NDS tree as the BorderManager VPN server, you can browse to the user account and select a user certificate to be used. (This assumes you already have configured the user certificate for that user). iManager will automatically fill in the proper subject name from the user certificate in this case. Otherwise, you will have to manually type in the subject name of the user certificate.

Click **OK**.



The subject name for the user certificate appears in the **User List** menu.

Collapse the **Define User** section, and expand the **Authentication Condition** section.



If the Certificate Authentication method is used, we specify that the server's Certificate Authority is to be trusted, meaning that any user authenticating with a valid user certificate issued by the Certificate Authority in JACK's tree will be trusted.

If you want to allow users outside of the NDS tree to be authenticated to the VPN server using the certificate method, you must call out a Trusted Root Object that applies to the user certificates Trusted Root. For instance, the screenshot shows that the MOE_TRO and MANNY_TRO objects were added as Issuers. (Those objects were created for two NDS trees in the Site-to-Site VPN chapter). The certificate authorities for the trees covered by the MOE_TRO and MANNY_TRO objects can issue User Certificates to NDS users in those trees, and this VPN will be able to authenticate those users. (Traffic Rules would have to be present to allow traffic for those users as well).

Enable **Allow Certificate Authentication**.

Enable **Trust Server CA**.

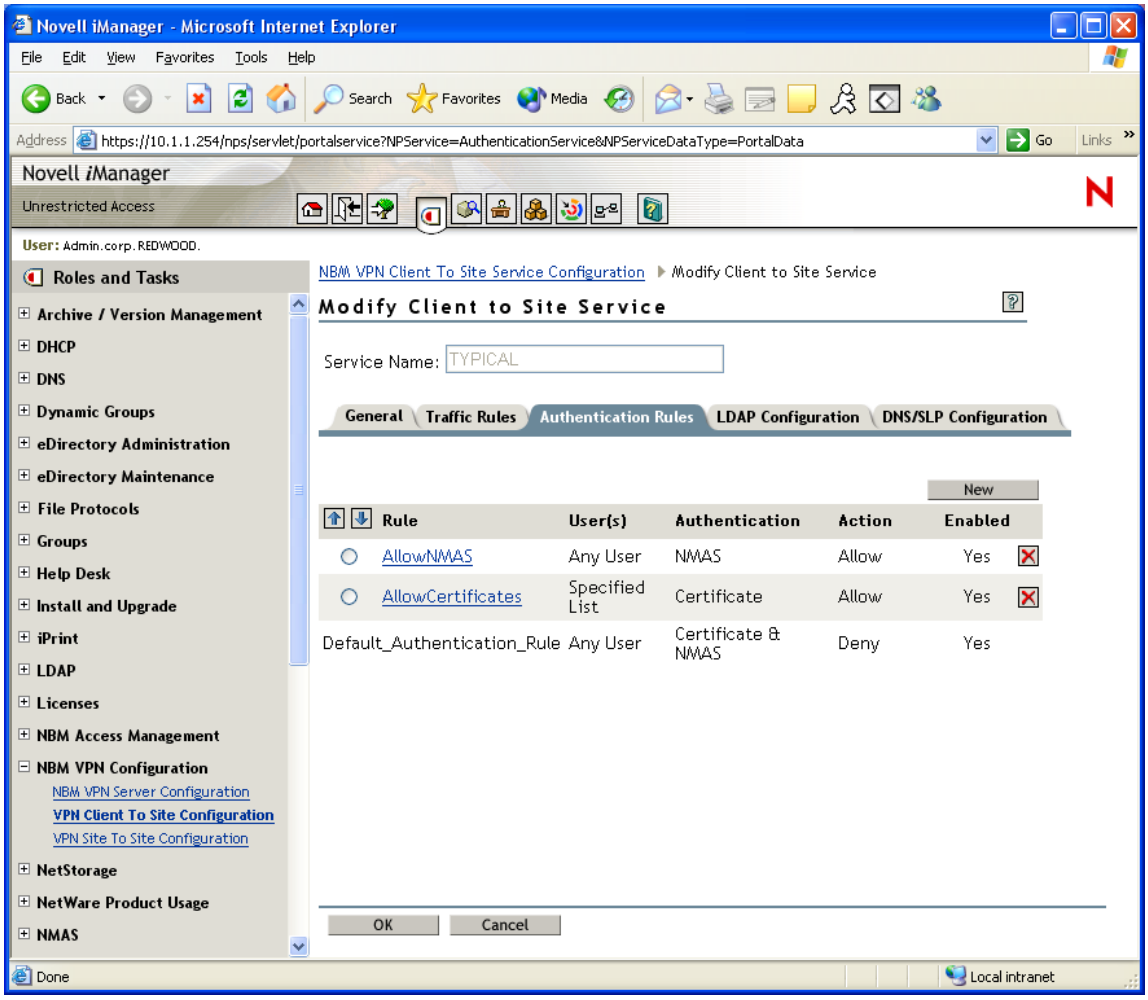
Click on the **Add** button above the **Issuer List**, and browse to the server's **Trusted Root Container**.

Select the server's own **Trusted Root Object**, which is shown as **MasterTRO.TRC – JACK.west.corp** in this example.

If you are authenticating users from outside your own NDS tree, you will have to have created a TRO for whatever trusted root created the certificate.

Browse back to the TRC, and add the TROs for MOE and MANNY as well.

Collapse the **Authentication Condition** section, and click on **Apply** to save the changes.



You should now have an access rule to allow Certificate Authentication for the Admin user.

Click **OK** to update the server.

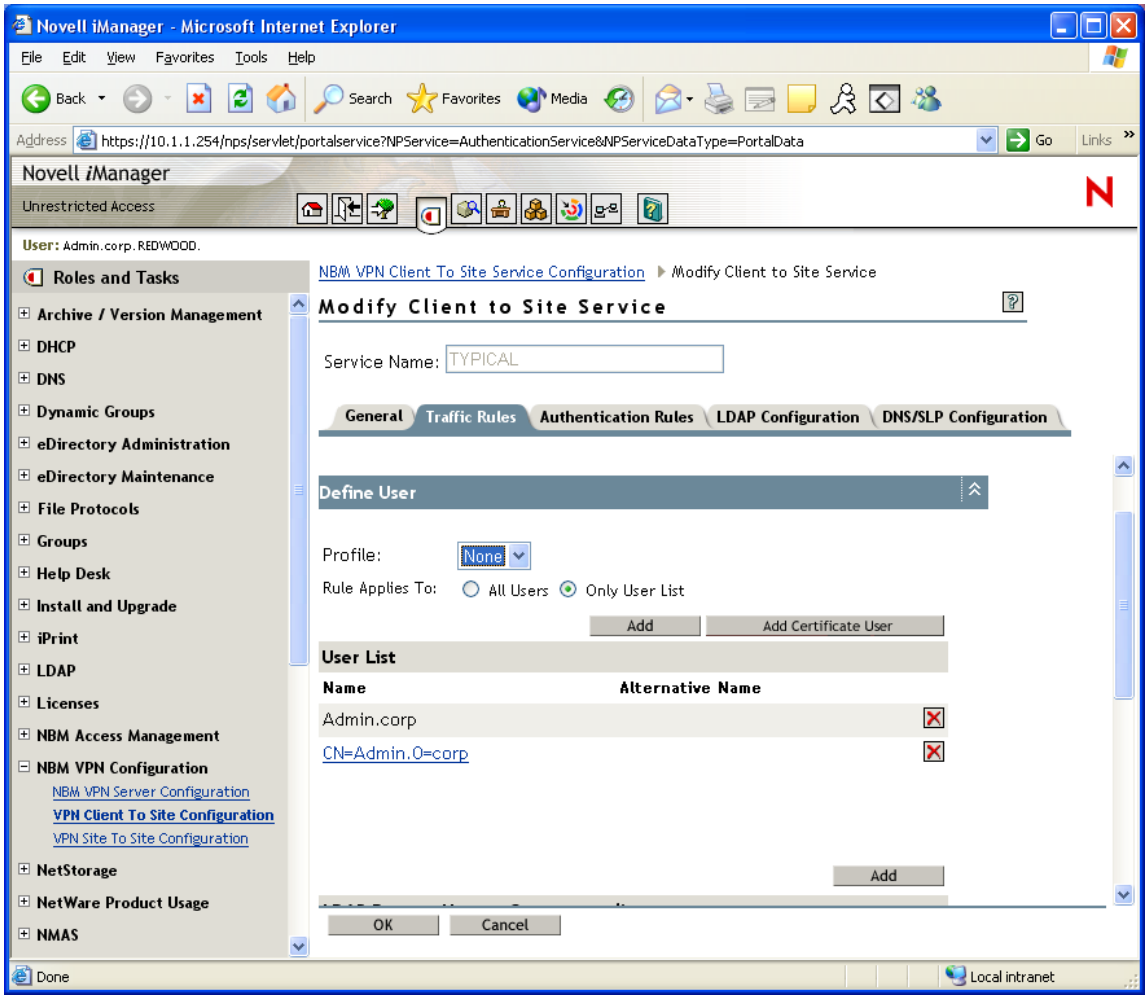
Now go back into the Client-to-Site configuration, and select **Traffic Rules**.

The only traffic rules previously created that will apply to a certificate-authenticated user are the ones that call out All Users. For this example, we would like the Admin.corp user to have the same access rights when authenticated by certificate mode as he/she does when authenticated by NMAS mode. The obvious place to do that is in the existing AdminToAll traffic rule. All we need to do is to add the certificate user as a defined user.

Select the existing **AdminToAll** rule.

Expand the **Define User** section. Click on **Add Certificate User**. Select **Subject Name**.

In the same way as adding a certificate user in the Authenticate Rule, **browse** to the **admin** account, **select it**, and in the drop-down list that appears in the **Subject Name** field, select the VPN **user certificate**. Click **OK**.



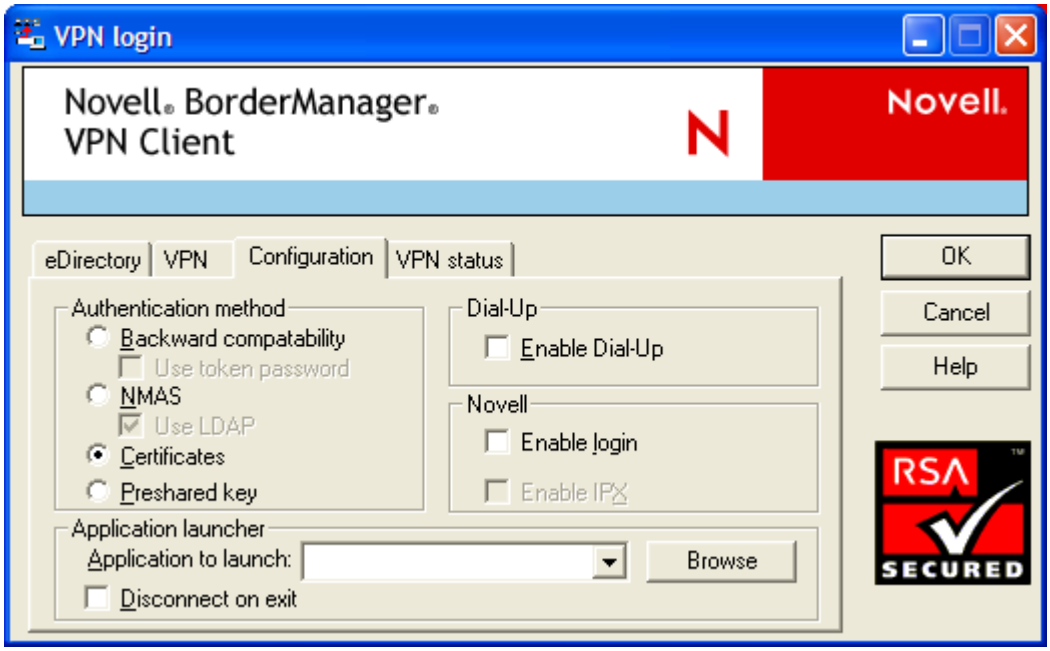
The **User List** now shows an entry for the subject name of the user certificate for the Admin account, in addition to the existing entry for the NDS user ID.

Scroll down, and click **Apply**.

Then click **OK** to save the changes to the VPN server.

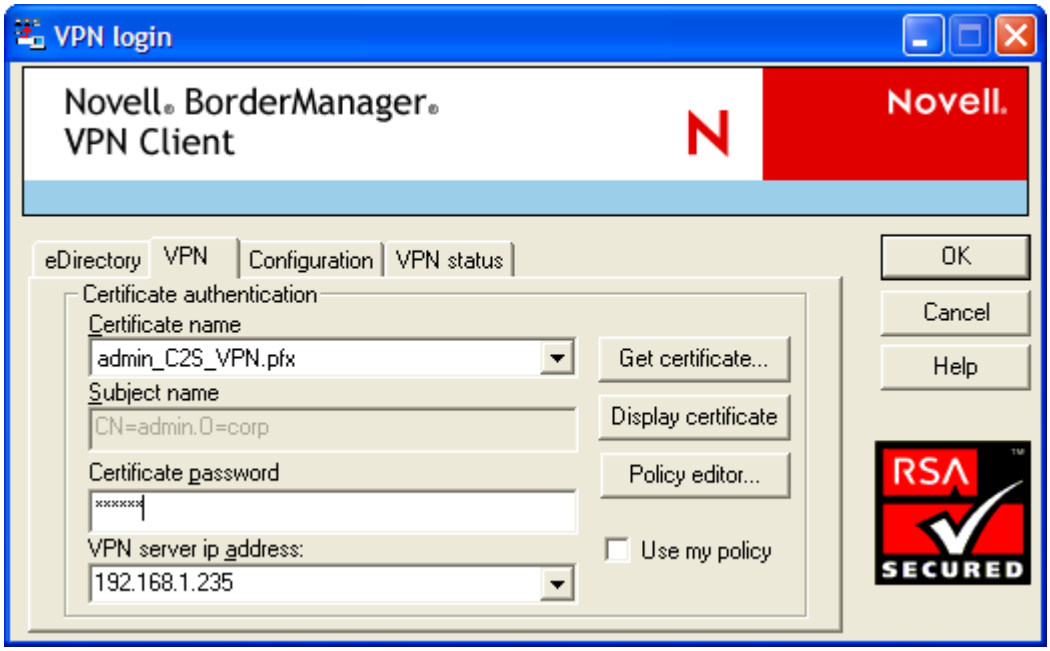
You should now be able to test certificate mode access, and have the same protected network policies as is authenticated with NMAS.

Connecting in Certificate Mode



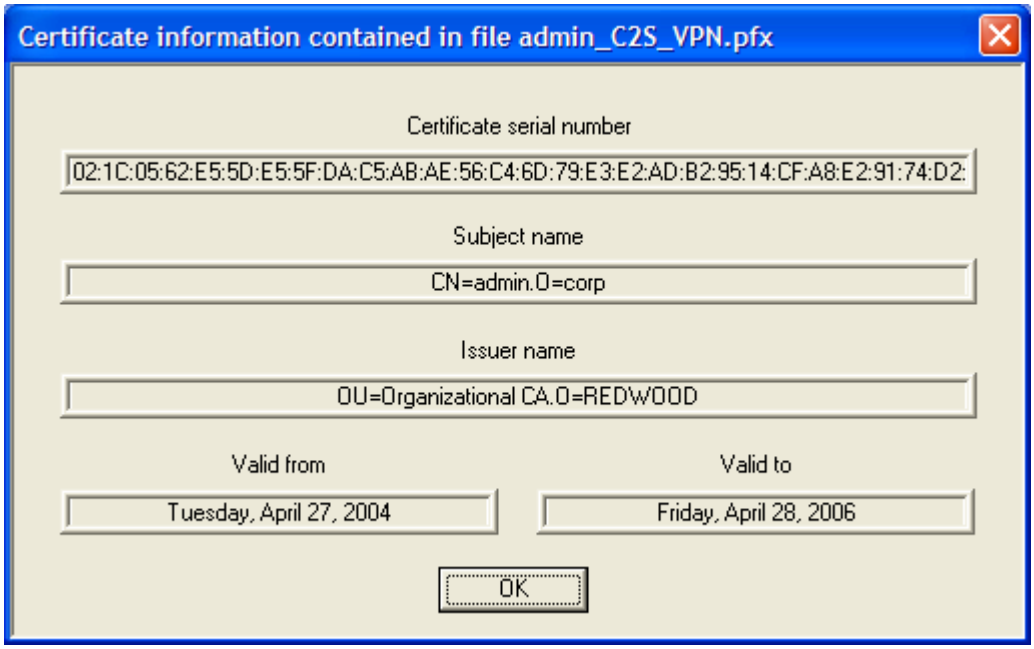
Launch the VPN client, and select the **Configuration** tab.

Under the Authentication method section, select **Certificates**.



Select the **VPN** tab. Select the **Certificate name** (if more than one user certificate file is installed, there will be multiple choices). Enter the **Certificate Password**. Enter the **VPN server IP address**.

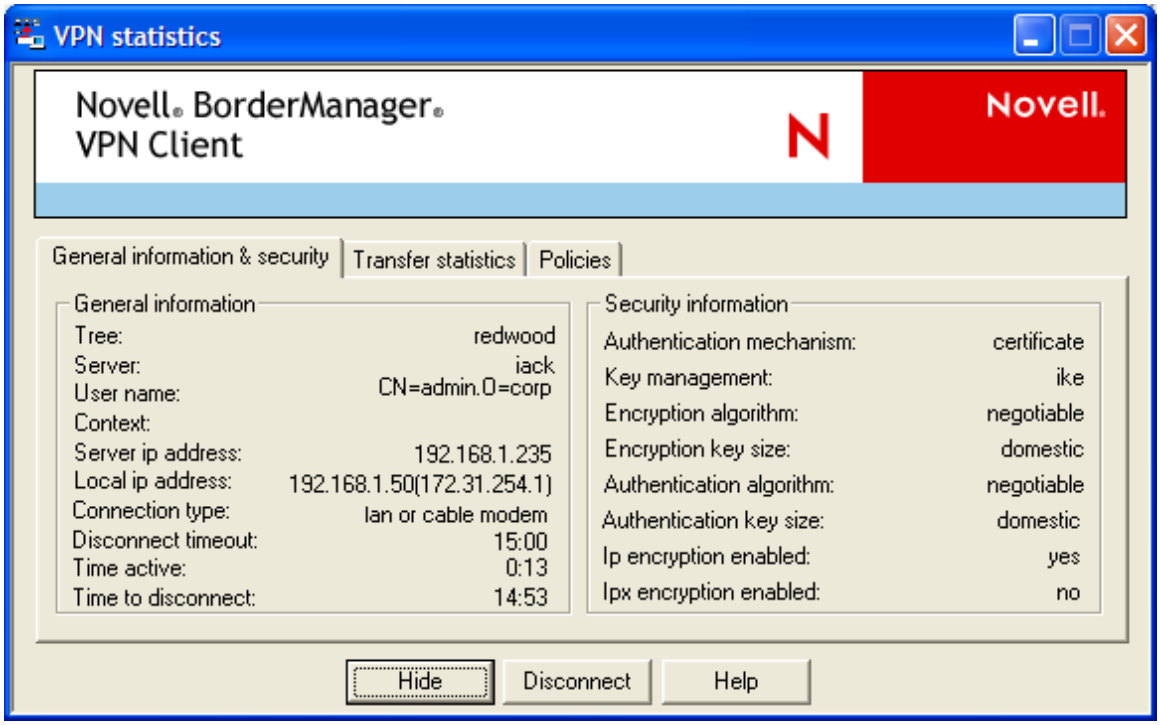
Click **OK** to start a VPN connection.



If you click **Display Certificate** with your user certificate selected, you should see all necessary details about that certificate.

For instance, the **Subject Name** displayed should match any access rule on the Client-to-Site service that calls out a certificate user in the Authentication rule.

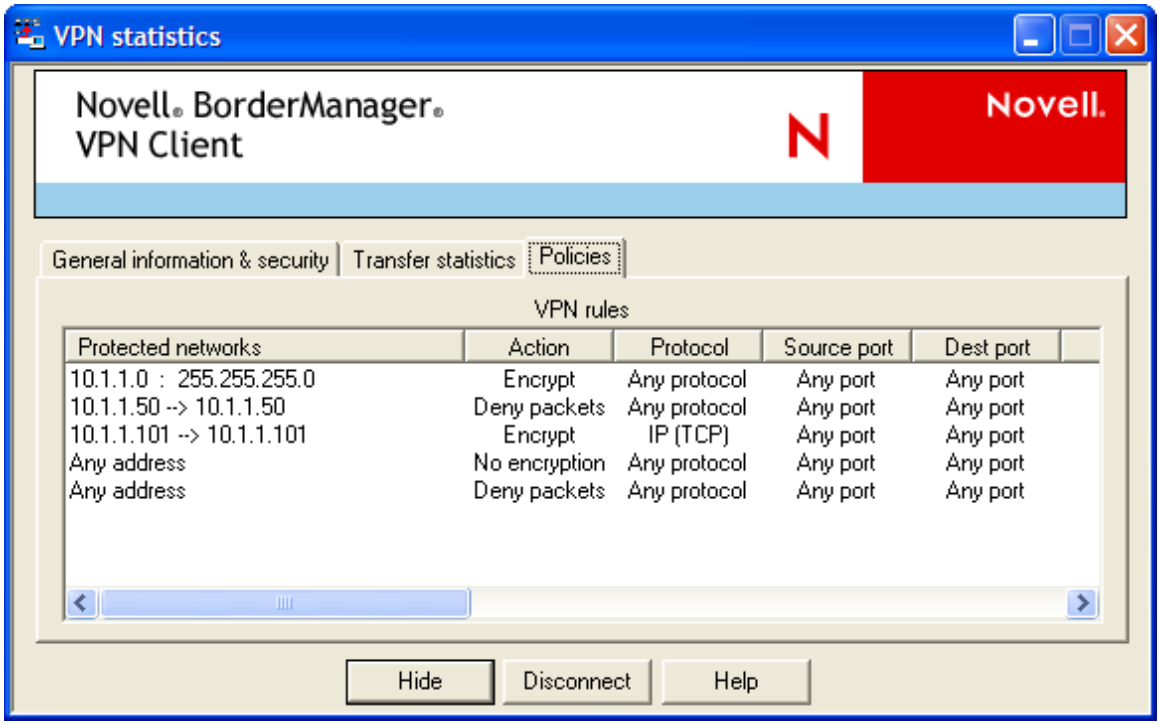
Click **OK** to close this menu.



Once connected, you should see the same basic type of information seen with NMAS-based authentication, as shown in an earlier example in this chapter.

The **General information & security** tab will show the **User name** as the Subject Name of the user certificate.

The local IP address will show the IP address assigned to the remote PC's network card (192.168.1.50), and also the VPN Tunnel IP address (172.16.254.1).



The **Policies** tab will show the protected networks, and each entry should correspond to a traffic rule that applies to the authenticated user.

Using Client-to-Site VPN in Shared Secret Mode

Shared Secret (also known as Preshared Key) is a VPN authentication method that is very simplistic used primarily for troubleshooting VPN connectivity, when used for Client-to-Site VPN. Because all VPN clients using shared secret must have the same key, it is not very secure, and should not be used for production use. (For Site-to-Site VPN, each server can have a different shared secret, and it is not configured at the server console. Shared secret is OK for Site-to-Site VPN.)

Shared secret is one way to connect a non-BorderManager server or non-Novell VPN client to a BorderManager 3.8 server to create a Client-to-Site or Site-to-Site VPN. (Certificate mode is the other way to connect a non-BorderManager server for VPN).

When using Shared Secret for Client-to-Site, authentication and traffic rules are not used. Anyone connecting Client-to-Site via Shared Secret has encrypted access to all internal hosts accessible by the assigned VPN tunnel address.

Configure the Server

The server is configured at the console prompt with some character string (the shared secret) that acts as a password for connecting with VPN clients.

With shared secret, all data is encrypted and all internal routes are available, once the VPN connection is made. Traffic rules and authentication rules do not apply.

On the server console, type in the following command:

SET IKE PRE-SHARED KEY=1234567

If IKE.NLM is loaded (VPN is running), the server should respond with a login prompt:

Enter fully distinguished Admin user name

Type in the Admin user ID, for instance: **Admin.corp**.

Enter password

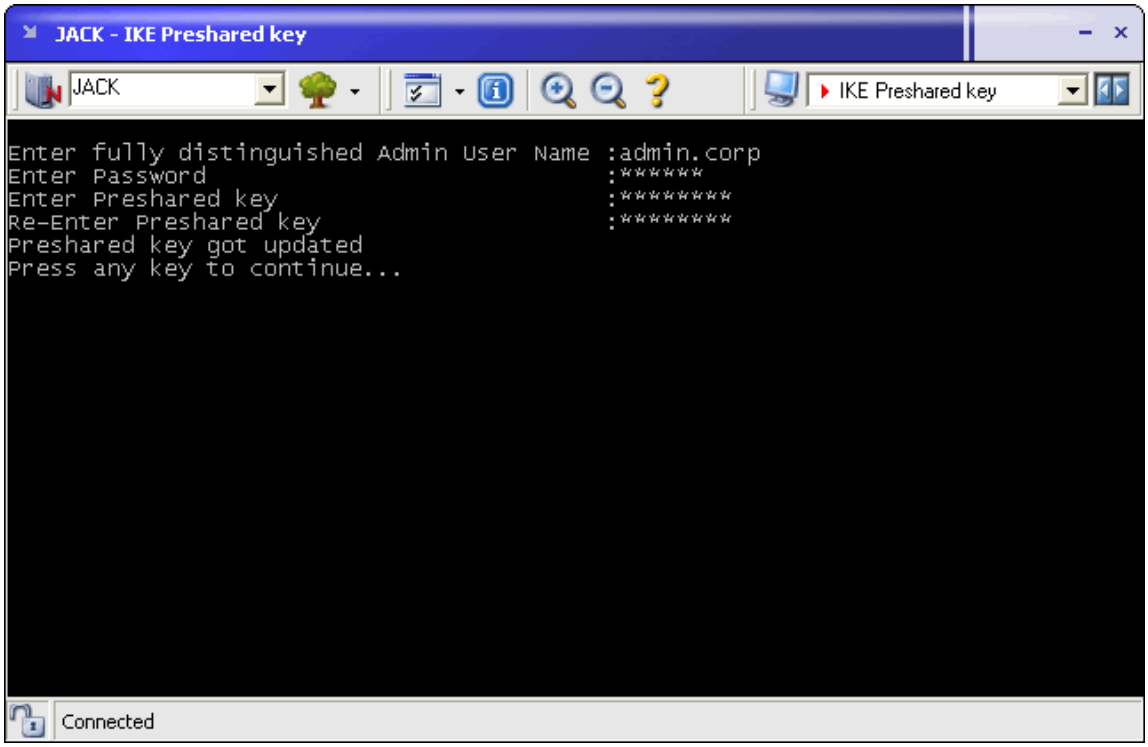
Enter the admin password.

Enter Preshared key

Enter a string of characters to be used as the actual shared secret. This does not need to match the initial value (1234567) in the original SET statement. In this example, **12345678** is used.

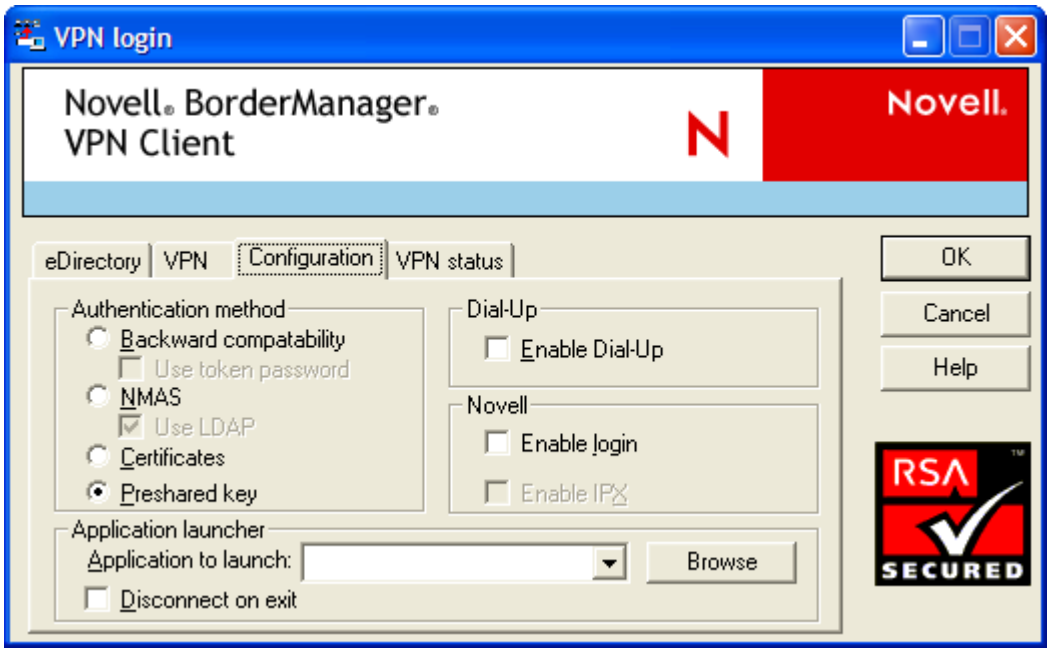
Re-enter Preshared key

Repeat the shared secret (12345678)



The server is now set to allow a VPN connection via shared secret.

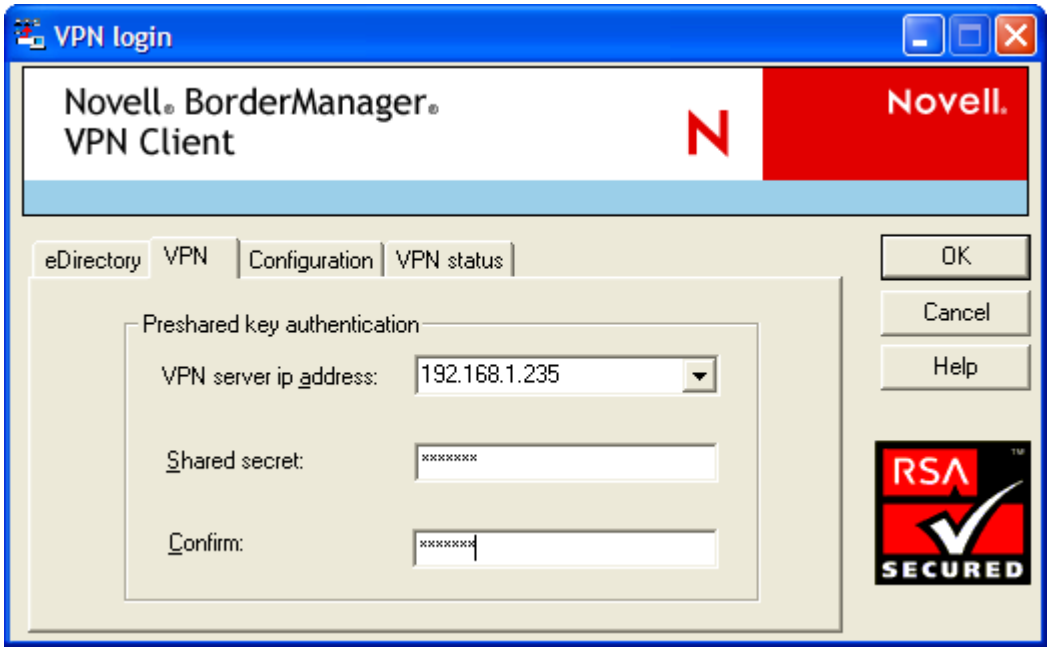
Configure and Use the VPN Client



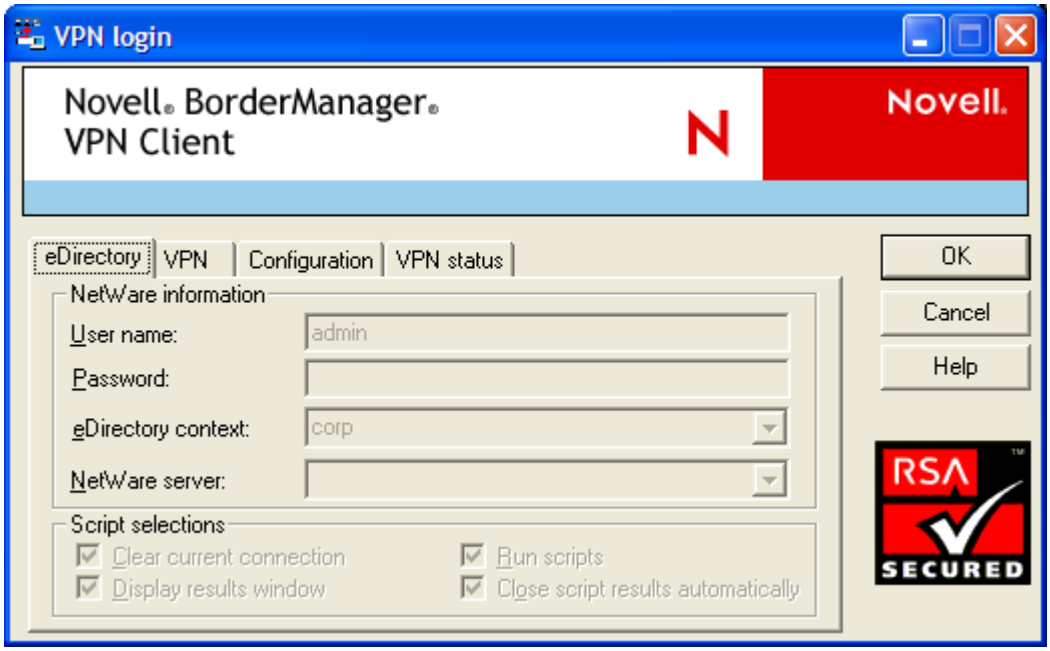
Launch the BorderManager 3.8 VPN client.

Select the **Configuration** tab.

Select **Preshared** key.

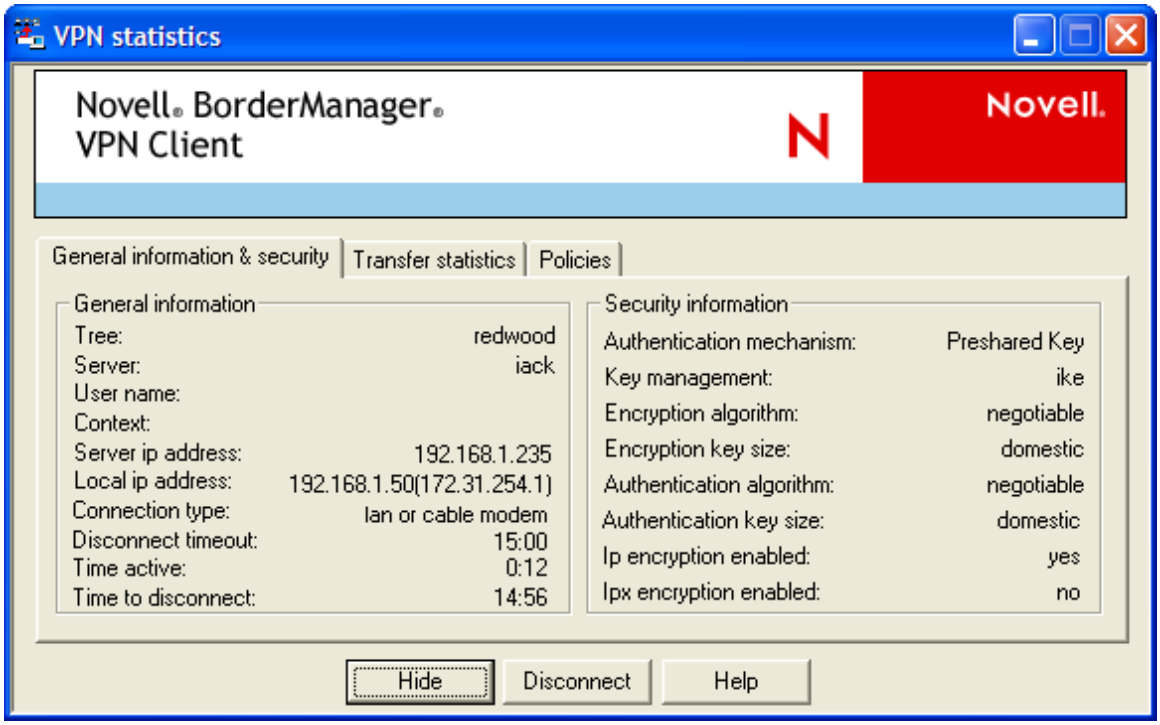


Select the **VPN** tab.

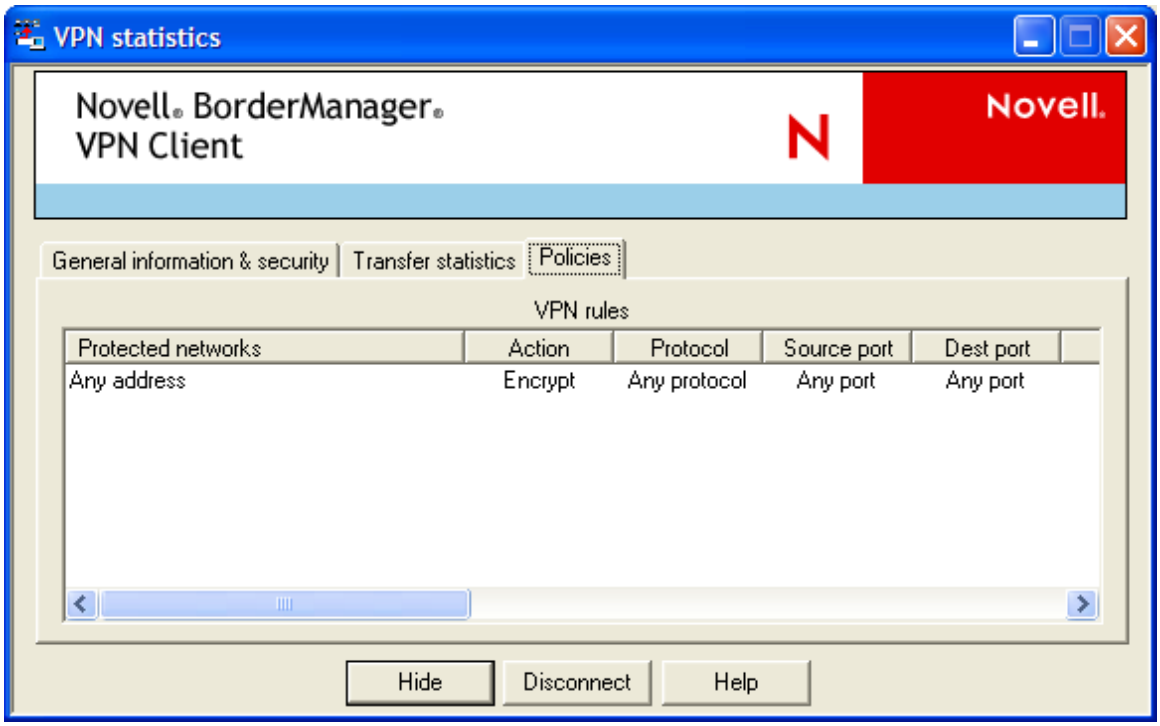


Check the eDirectory tab – all entries are grayed out, since there is no authentication you can enable with shared secret mode.

Enter the **VPN server IP address**, and the **shared secret**, and click **OK** to connect.



You should connect. The **General information & security** menu will show that you are authenticated without a user name.



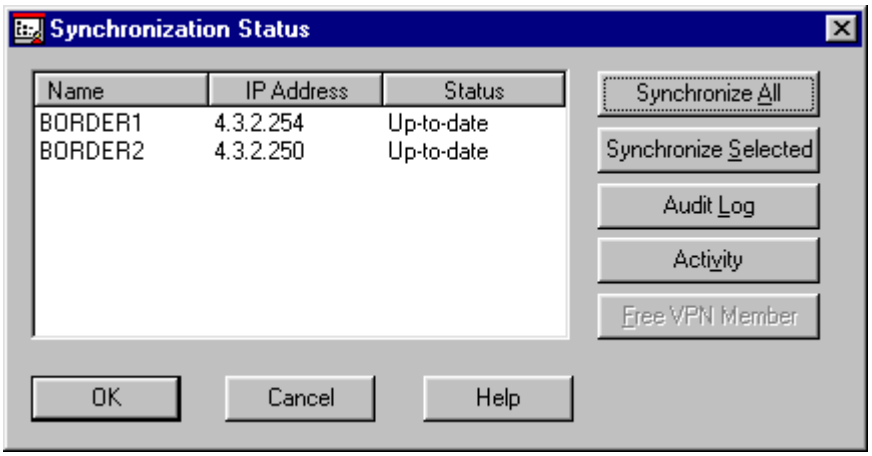
The **Policies** menu will show that any address is available through the VPN, and traffic will be encrypted.

Chapter 21 – Viewing VPN Data

This chapter shows how to view log data for both Client-to-Site and Site-to-Site VPN.

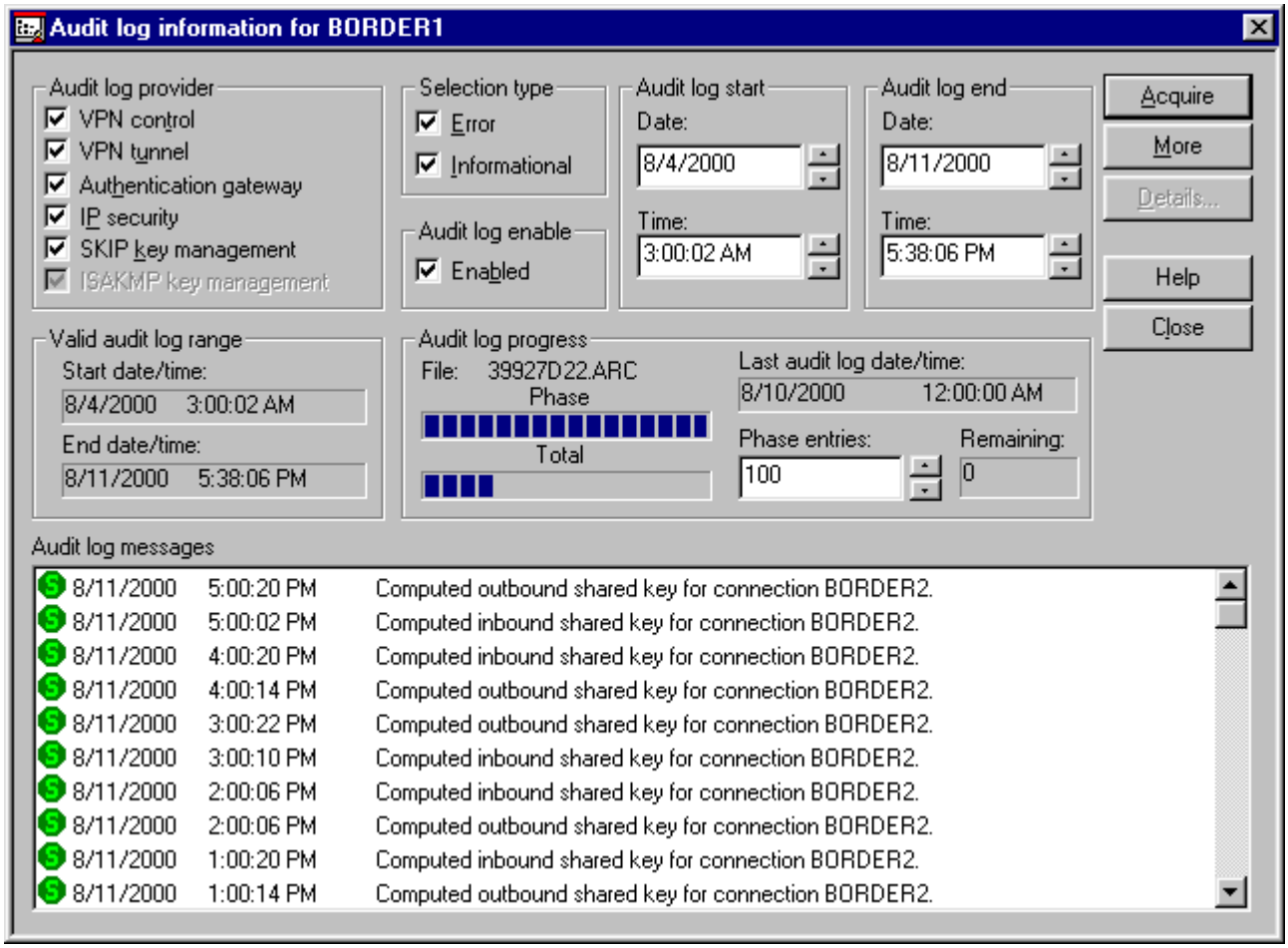
Legacy VPN - Using NWADMN32 To View VPN Log Data and Activity

Legacy VPN refers to BorderManager 3.7 and earlier (SKIP-based) VPN. All monitoring of legacy VPN is done in **NWADMN32, BorderManager Setup main menu, VPN menu, Master Site to Site details, Status**. (Whew! It's really buried in there!)



To see real-time or audit (history) VPN activity, select the VPN server of interest from the Synchronization Status menu, and click on the **Audit Log** or **Activity** buttons.

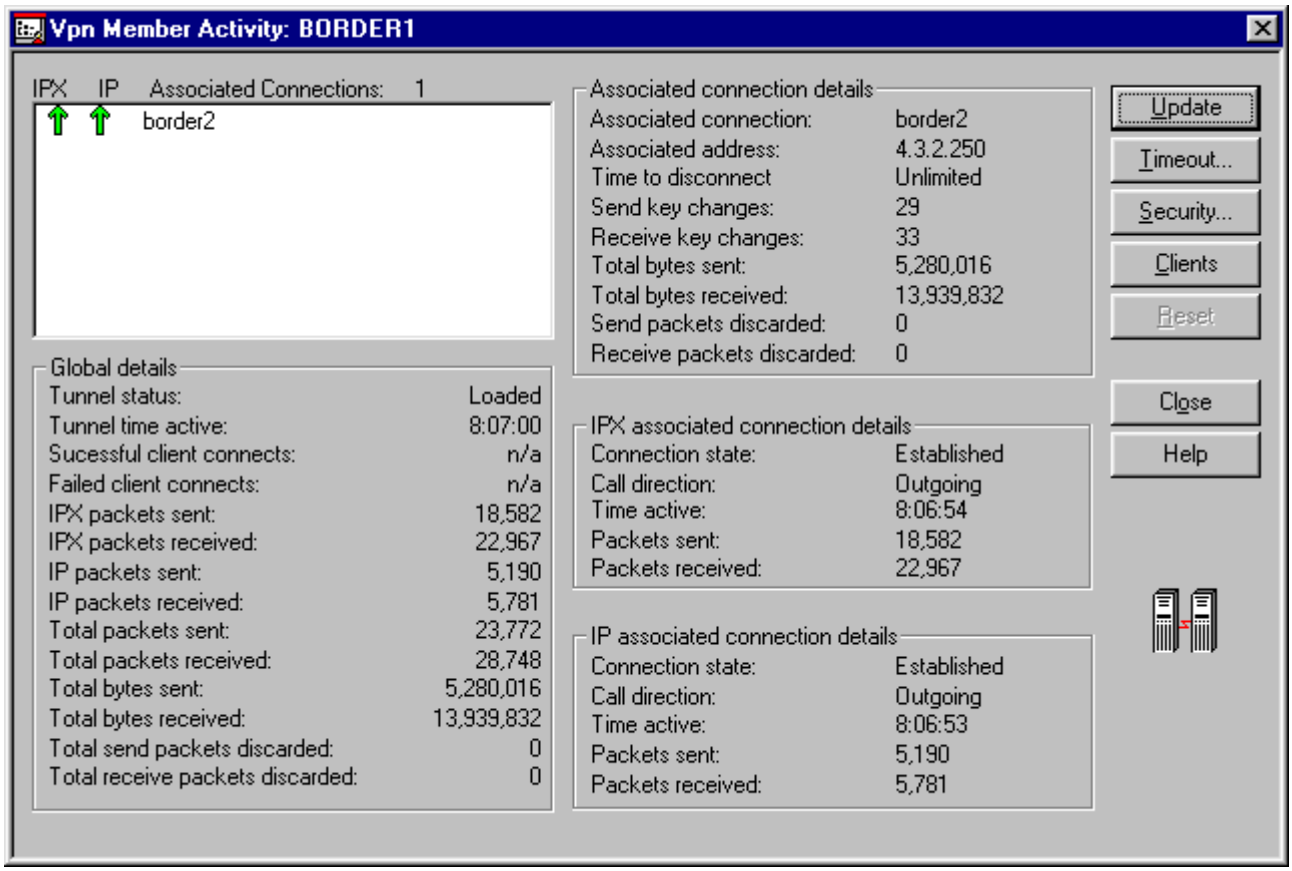
In the examples shown below, the BORDER1 server was selected.



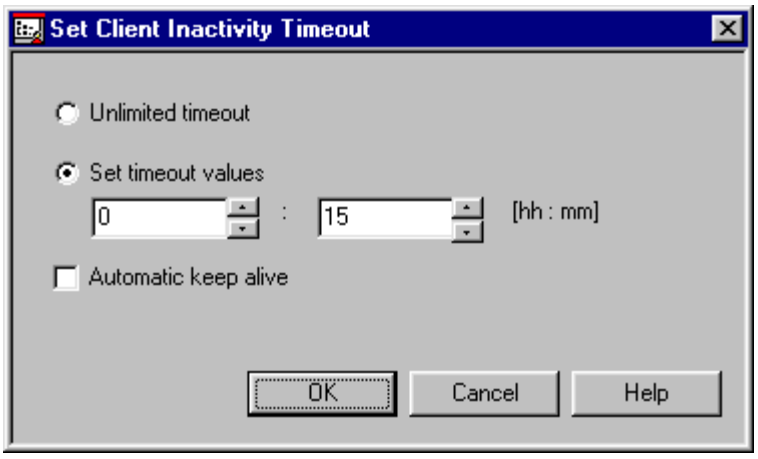
This is an example of audit log (history) data for the time frame of 8 August 2000 though 11 August 2000.

Click on the **More** button to page through the data.

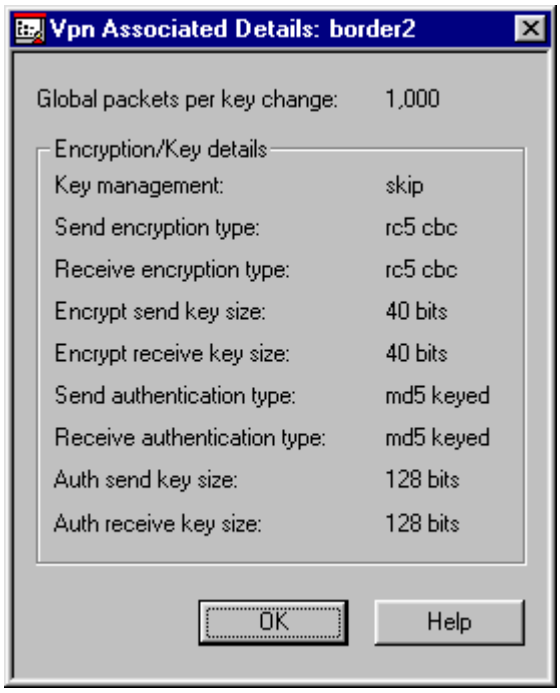
Clicking on the **Activity** button in the Synchronization Status menu shows one of two screens that display current (real-time) VPN activity. Note the "**Clients**" button on the right side of the menu. Clicking on this button will change the display from showing server (server-server) VPN activity to Client (client-server) VPN activity.



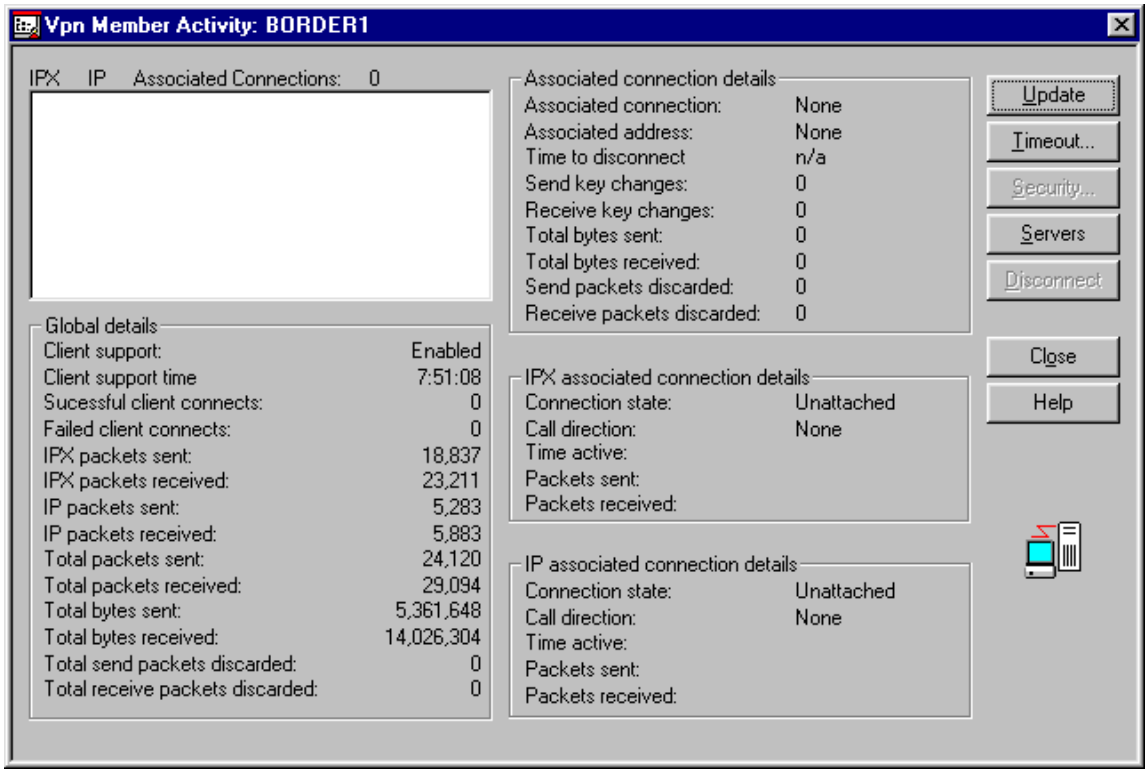
The example shown shows data for site-to-site VPN activity. (Note the button on the right side of the screen that says Clients. Clicking on the Clients button switches the activity screen to show real-time data for VPN client-to-site, if any has been configured.



Clicking on the **Timeout** button allows you to set the timeout value for client-to-site inactivity. If no data has been received from a VPN client after the length of time defined by the timeout value, the VPN server will terminate the VPN connection.



Clicking on the **Security** button at the VPN activity screen shows the VPN encryption options configured.



Clicking on the **Clients** button at the VPN Member Activity screen shows real-time data for any active VPN client-to-site connections. Clicking on the **Servers** button at this screen switches the display back to VPN site-to-site activity.

BorderManager 3.8 VPN – Using Novell Remote Manager to View VPN Data

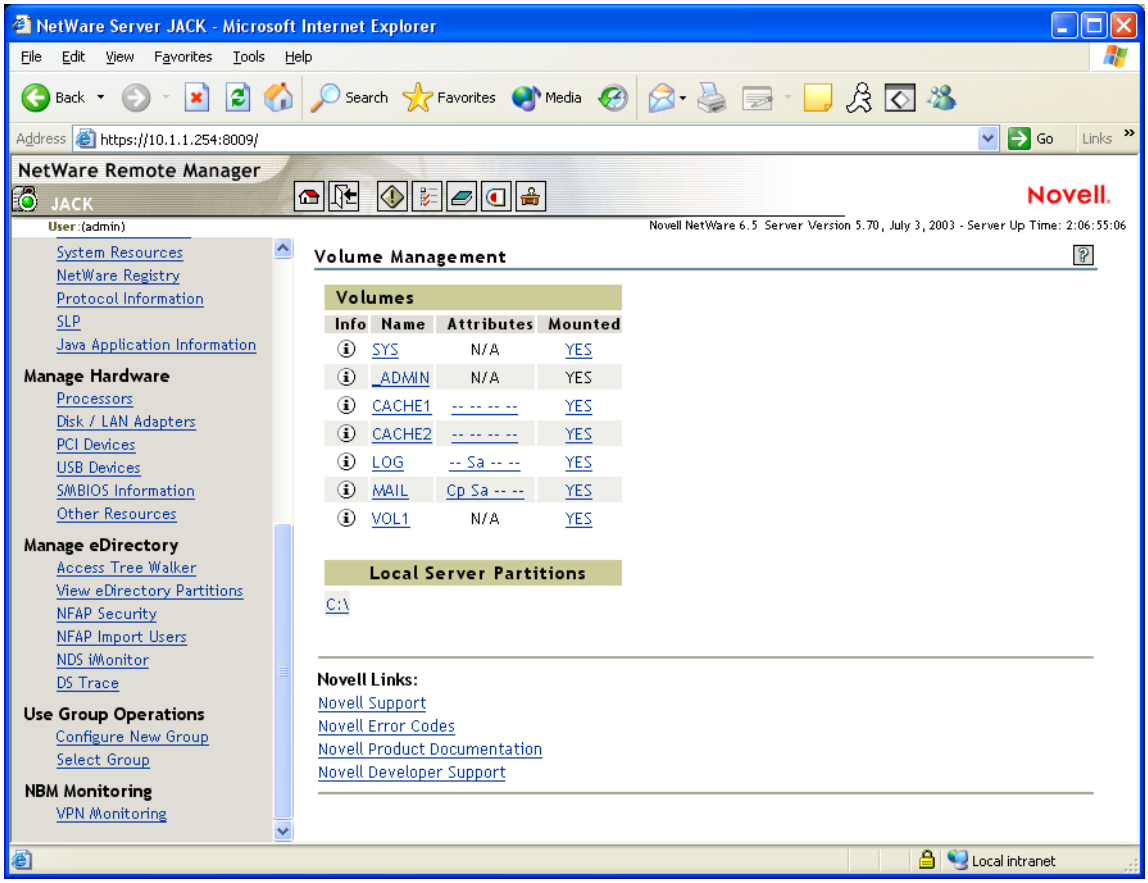
Unlike Legacy VPN in BorderManager 3.7 and earlier, which used NWADMN32 to view Audit Log data, you must use Novell Remote Manager to view BorderManager 3.8 data.

Note You can also view data directly, with the CSAUDIT command at the BorderManager server console. Novell Remote Manager provides a much more formatted view of the data.

Launching Internet Explorer and pointing to Novell Remote Manager on a BorderManager 3.8 VPN server should automatically show an option for VPN Monitoring, as long as VPMON.NLM is running.

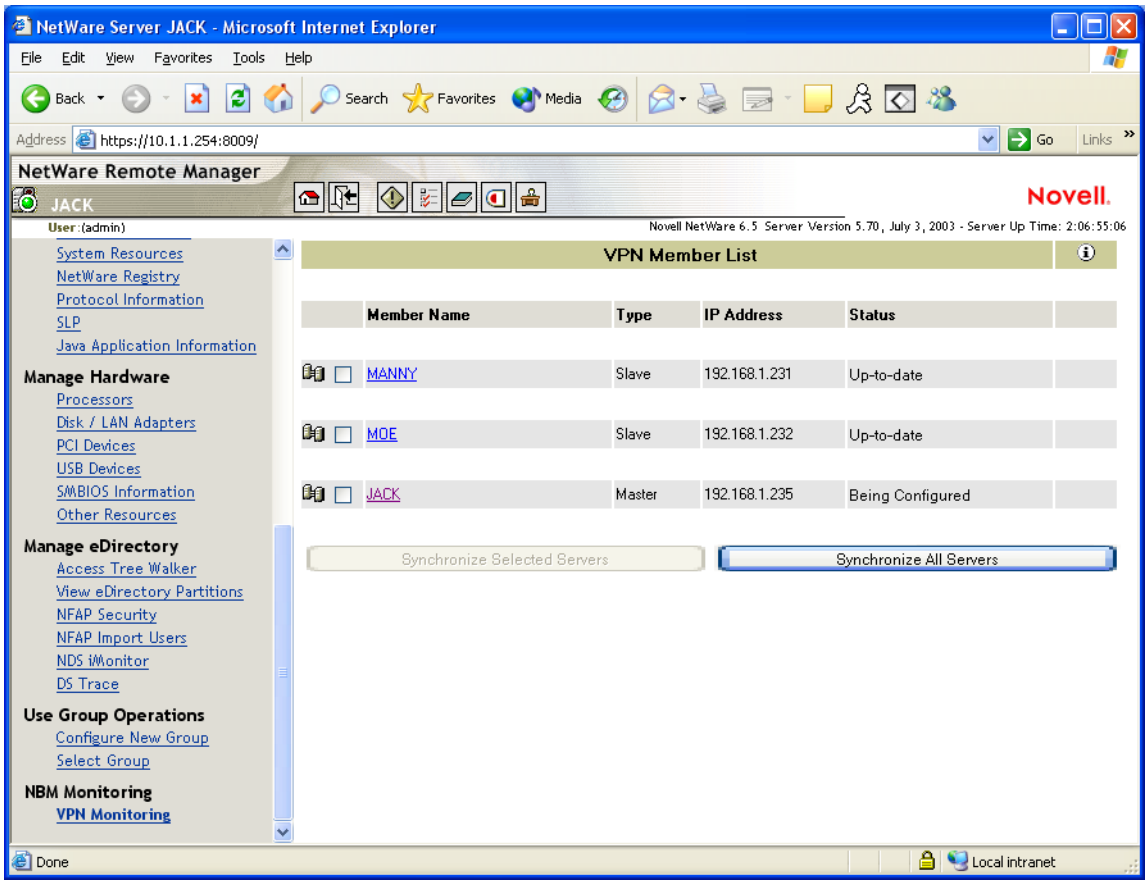
Viewing BorderManager 3.8 Audit Log Data

Enter the private IP address of the BorderManager 3.8 server in the browser, with :8008 appended to begin Novell Remote Manager. You should be presented with an SSL certificate (if SSL is required and working properly), and then a login prompt. Log in as Admin or an admin-equivalent user. You must use NDS distinguished naming convention here (such as admin.dd).



Near the bottom left of the active window, you should have an entry for **NBM Monitoring**, with a link called **VPN Monitoring**. Click on the VPN Monitoring link.

VPN Member List Menu

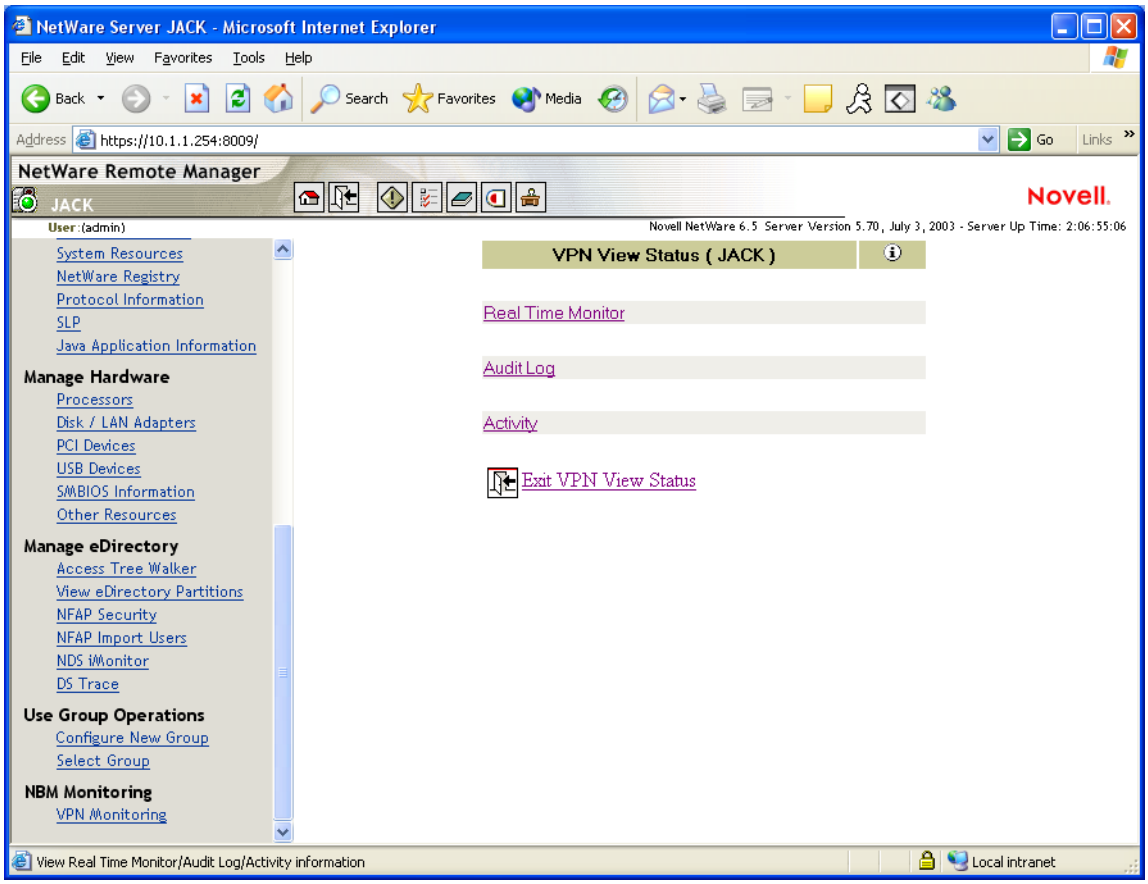


You should now see one or more BorderManager 3.8 VPN servers. In the example above, three BorderManager 3.8 Site-to-Site VPN servers are visible.

The browser is pointed to the BorderManager 3.8 server named JACK in this example. Select the server of interest (here, JACK) by clicking on the server name link.

You may have to use NRM on the VPN server to connect to that server's VPN link. (Use NRM on JACK to view JACK, use NRM on MOE to view MOE, etc.)

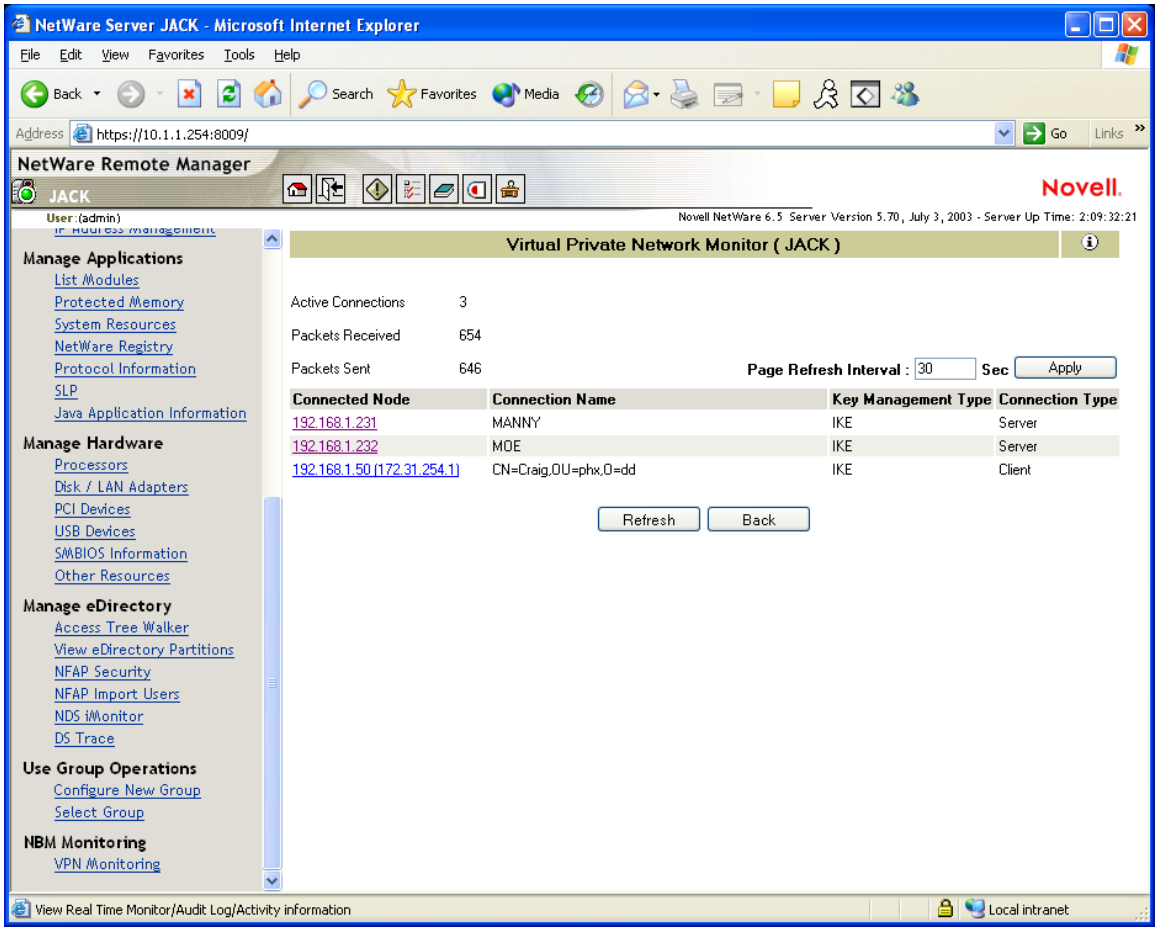
VPN View Status (JACK) menu



At this point, you should have three options to select: **Real Time Monitor**, **Audit Log**, and **Activity**. Each option is shown below.

Real Time Monitor

If you have a BorderManager 3.8 Site-to-Site VPN active, select **Real Time Monitor** to view connection status between VPN servers. There is no real equivalent for this screen in legacy VPN.



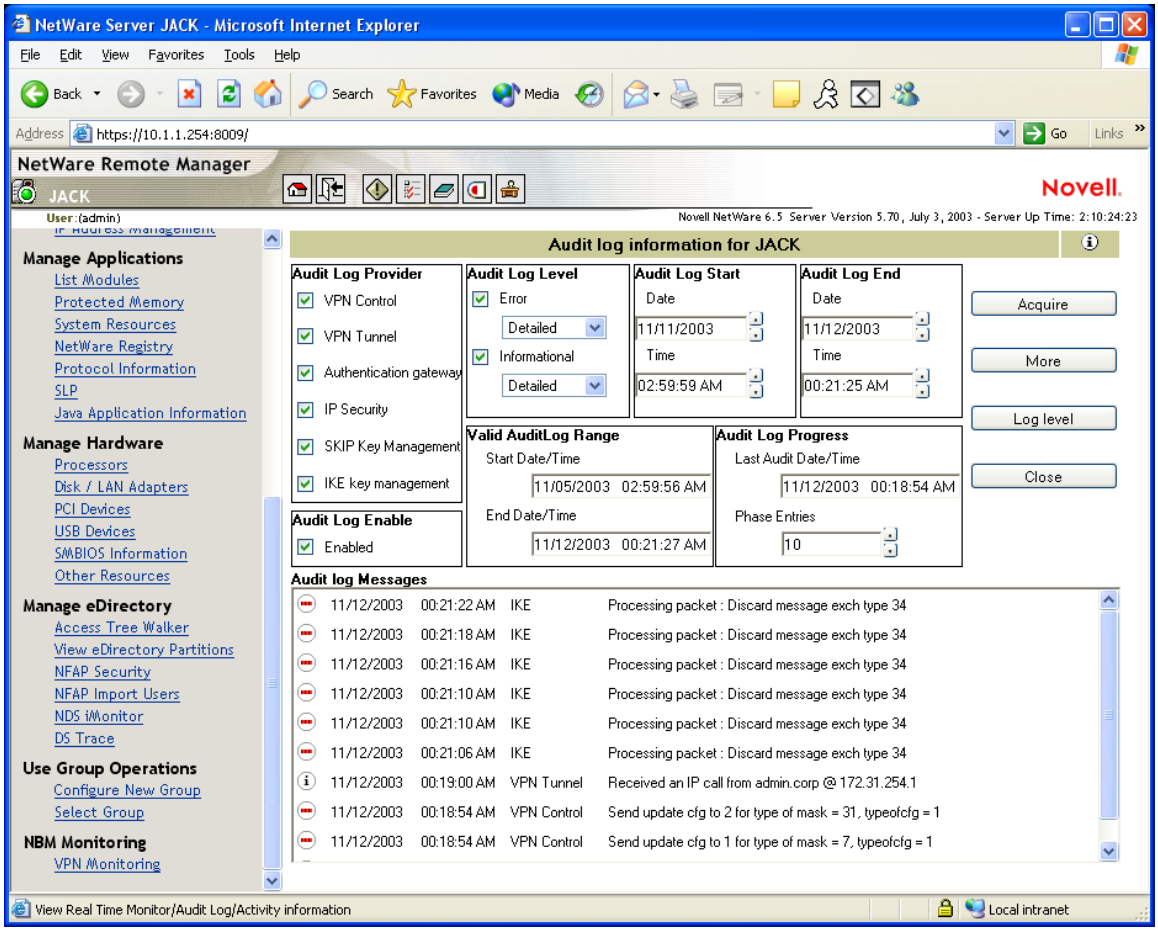
The **Real Time Monitor** shows connection status to VPN servers and any VPN client connections in use at the moment.

Click **Back** to return to the VPN Status menu.

Audit Log

Select **Audit Log** to view audit log records for the VPN server. This selection is equivalent to the NWADMN32 audit log view in legacy VPN.

Once you have brought up the Audit Log menu, you can choose to filter the log data to be retrieved with a series of check boxes and date entries.



Once you have chosen the data to be retrieved, click on the **Acquire** button to have the browser display entries from the audit logs.

By default, all data (information & error, etc.) will be retrieved from the log files. You will see 10 entries at a time.

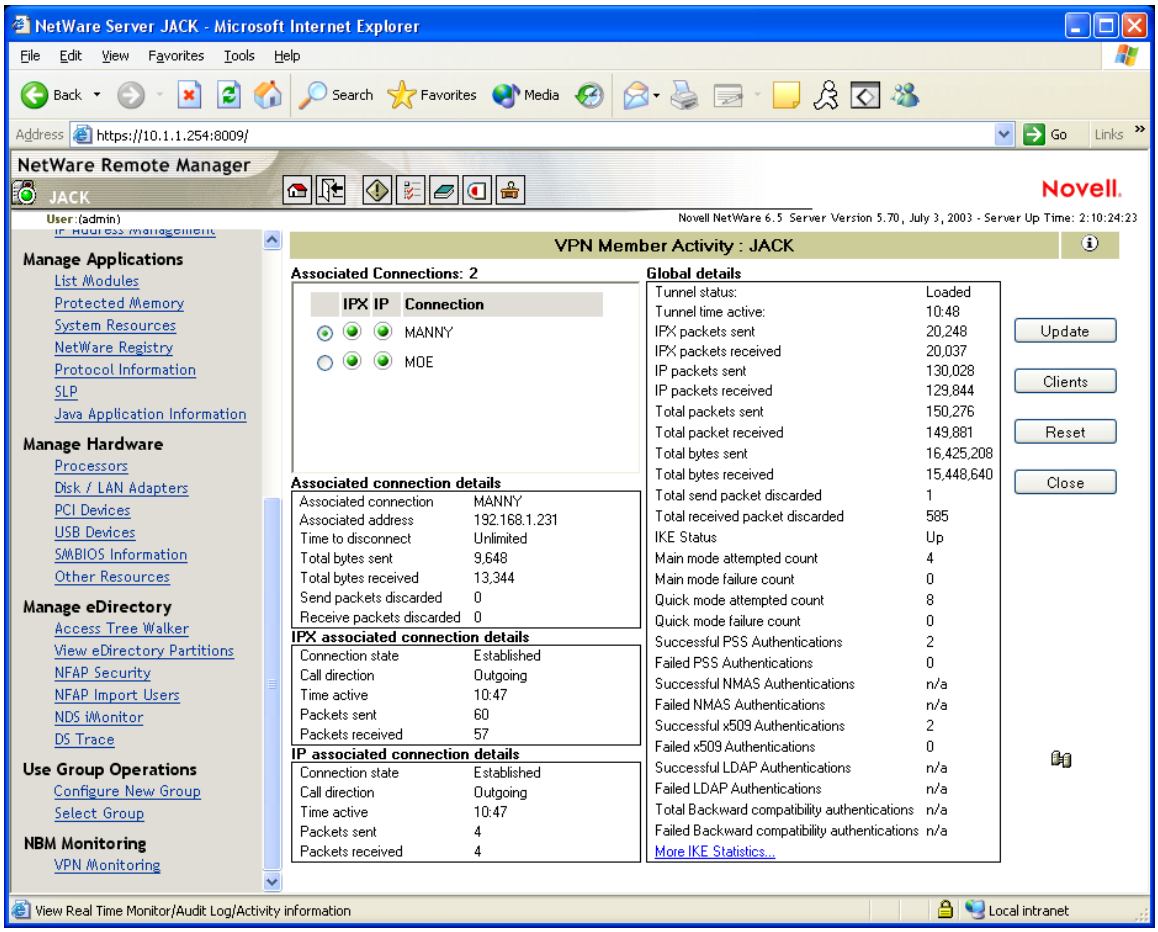
Clicking on **More** will bring in the next (older) set of 10 entries, etc.

In the example shown above, the most recent 10 entries from the audit logs have been retrieved and displayed in the browser.

Clicking on any of the audit log messages at the bottom of the screen will display more detail on that message.

Click on the **Close** button to return to the VPN View Status menu.

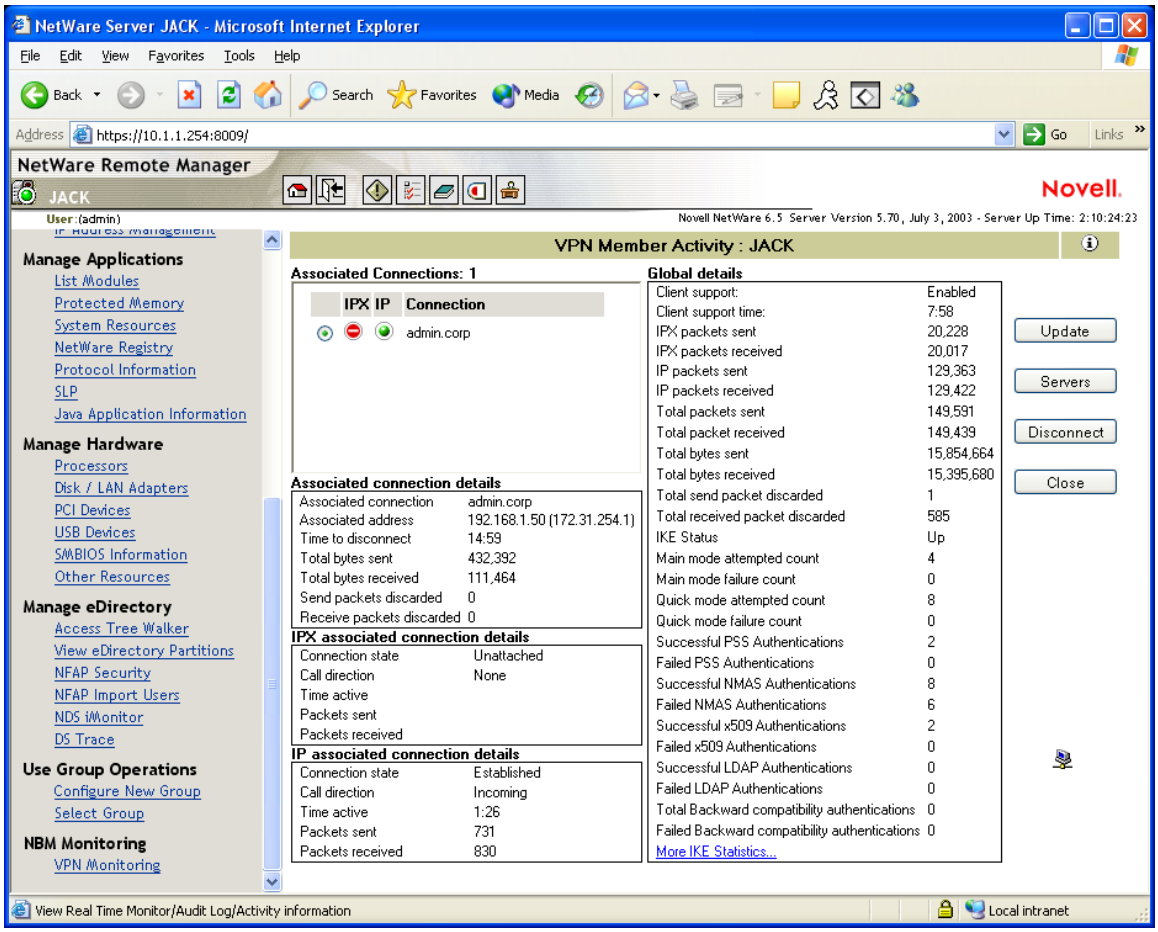
Current Site-to-Site Activity



The screenshot above shows the current Site-to-Site activity as viewed from JACK.

Clicking on the **Clients** button in the right panel switches the display to show Client-to-Site current activity.

Current Client-to-Site Activity



The screenshot above shows the current Client-to-Site activity as viewed from JACK.

One VPN client connection is active, and from the syntax of the user name under the Connection field, it can be seen that the user was authenticated by NMAS, as the name is in standard NDS format.

The Red icon for IPX indicates that the VPN connection has never seen an IPX packet. The green icon under IP indicates that not only has some IP traffic been seen crossing the VPN tunnel, that traffic has been seen relatively recent, or the color would be different. (Yellow means that some traffic was seen at one time, but not for a minute or longer).

Click on the **Close** button to return to the VPN View Status menu.

<This page intentionally left blank. This is to facilitate putting in chapter tabs in a ring binder for double-sided printing. The main chapters should start on an odd-numbered page.>

Chapter 22 - Access Rules

Concept

Note This chapter discusses access rules configured in NWADMN32, mostly for proxies. Access rules for BorderManager 3.8 VPN are configured with iManager, and are shown in the BorderManager 3.8 VPN chapters.

Access rules control the use of the BorderManager application-level services.

If you ever took a Novell certification test, you probably remember being quizzed on some part of the OSI model, with the application layer at the top of the heap. Here is where that knowledge can actually be put to good use!

The Access Rules do NOT control routed traffic, they can only control the proxies, the legacy Client-to-Site VPN and the IP Gateways. If you have enabled dynamic NAT, routing and have packet filter exceptions allowing certain outbound traffic, you will not be able to prevent users from bypassing the proxies, and as such, access control rules.

Access Rules work on a top-to-bottom approach. The first rule check is whatever rules is highest in the list, then the next, and then the next, and so forth until you get to the bottom of the list. Only one rule is ever actually 'hit', no matter how many rules you have in the list.

The FIRST rule that matches your criteria is used, and no other rules are checked. This means that it is critical to structure the rules in such a way as to have the desired effect. Putting a deny rule in below another rule which allows access will not work, and putting an Allow rule in below a Deny rule will not work, all things being equal about the rule source and destination.

Rules applying to NDS objects require Proxy Authentication. That is, if the host trying to browse is not authenticated (for any reason), the rules based on a source equal to an NDS user, group or container are **ignored**.

The Default Deny Rule

The last rule in the rule list is always the default rule. The default rule is not shown, but can be seen by clicking on the Effective Rules button. The default rule is created when you install BorderManager, and is always set to Deny Any source to Any destination. If you don't like it, you can simply add your own Allow All rule to the end of your rules list to effectively override the default rule.

Rule Inheritance

You can apply rules to NDS containers, and the BorderManager server will inherit them as long as those rules are applied to containers between the BorderManager server object and the Root of the NDS tree. The rules applied to the server object will have priority over inherited rules – that is, they will be placed above inherited rules in the rules list. The farther away the container that the rules are assigned to, the lower in the rules list they will appear.

Applying rules to NDS containers is not often done because it takes BorderManager a long time to walk the tree to find and read the rules. Sometimes this can be a very long time indeed, depending on your NDS design, WAN links involved, replica placement, and other factors. During the time that the rules are actually being read, all traffic across the BorderManager server is denied, at least that traffic normally allowed by access rules.

Proxy Authentication and NDS-based Rules

One of the big selling points for BorderManager is the ability to base rules on NDS-objects such as users, groups or containers. Not only can you control the Internet access of the users this way, you can also log the traffic by user name. This is NOT the same thing as assigning a rule to a container so that it is inherited – it is using the user, group or container as a source in the rule definition itself, regardless of where the rule is stored in the NDS tree. In this book, NDS-based rules really mean access rules where an NDS object is used in the source definition part of the rule.

There are some common misunderstandings about NDS-based rules. First of all, NDS-based rules really only apply to the HTTP Proxy and the FTP Proxy. (There are some other proxies that can make use of the NDS-based rule as long as you have already authenticated using the HTTP Proxy.) Secondly, you must enable Proxy Authentication in order to use the NDS-based rules – just logging into the NDS tree is not good enough to provide authentication.

Finally, the users need to be in the same NDS tree as the BorderManager server.

Note NDS-based rules are simply **skipped** if the user is not proxy authenticated! And not all proxies can make use of proxy authentication.

Selective Proxy Authentication & Access Rules

There are times when you do not want all hosts to have to authenticate to use the HTTP Proxy. Here are some examples:

20. You have a server or application that needs some sort of HTTP access, but is not running Client32, and is unattended. This can include other proxy servers in a cache hierarchy, or servers updating antivirus definitions through the HTTP Proxy.
21. You have some hosts that are unable to run Client32 (for CLNTRUST), and you do not wish to force the users of those hosts to go through SSL Proxy Authentication. (Might include Macintosh computers, or selected PC's or Linux/Unix boxes.)
22. You wish to allow browsing to certain URL's without forcing the users to authenticate, especially when using SSL Proxy Authentication. An example might be an internal web site.
23. You wish to allow an entire subnet some access based on the subnet address, without invoking authentication. Perhaps all hosts on that subnet are in a different NDS tree.

On my own test network, I have two PC's used by my family that do not have Client32 loaded, and I do not want my wife and children to have to use SSL Proxy Authentication. At the same time, I have several servers using the HTTP Proxy that would be unable to access the internet without some sort of exception to proxy authentication. This includes a server in a cache hierarchy, and a RedHat Linux server using Up2date through the HTTP Proxy.

The answer is found in the Authentication Context Menu, with the option '**Authenticate Only when user attempts to access a restricted page**'.

With that option enabled, **two passes through the access rules may be made** – once looking for rules which apply to Any or to a selected IP address, and a second pass looking for rules based on NDS user, group or container.

It is critical that the access rules be structured correctly in order to achieve the desired result!

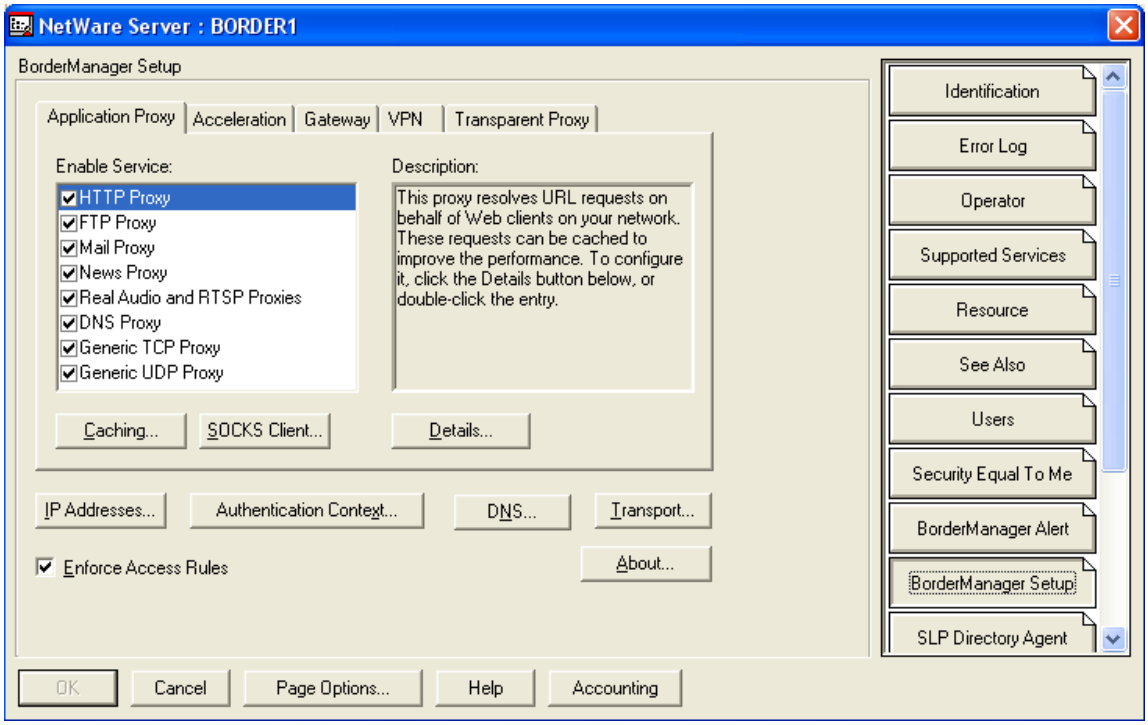
Think of it this way: Look at all the rules based on URL (or port 80 or 443, in general) that do NOT call out user, group or container as a source. Those are the only rules examined in the first pass

through the rules when the 'authenticate only …' option is enabled. If you should have a rule allowing Any to Any destination , or one Denying Any to Any destination, then a second pass through the rules will never be made, because there will always be a match on the first pass. You must be more specific as to what is allowed or denied, or allow the default Deny Any rule to block access after two passes have been made through the rules. By specific, I mean that you should have your Allow or Deny rules always call out a user, group or container, or some selected IP addresses, so that if a match is NOT made, a second pass looking for NDS sources will occur.

Examples of how these rules might look is shown later in this chapter.

Enforce Rules

On the BorderManager Setup main menu screen, you have the option to enforce access rules. Unless this box is checked, none of your access rules will be applied. Unchecking this box is often a good troubleshooting step if you suspect the failure of a proxy to function might be related to an incorrect or missing access rule.



Check the **Enforce Access Rules** box or no access rules set up for BorderManager will be applied.

Unchecking the Enforce Access Rules box is one thing you can try when troubleshooting to eliminate a variable.

Be aware that not enforcing rules can be dangerous – you could be giving free access to your internal network to anyone with a VPN client, if you have (legacy) Client-to-Site VPN configured.

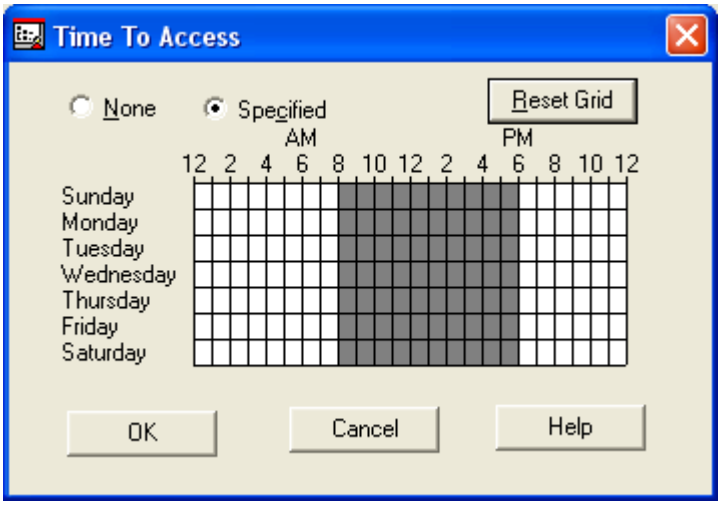
Time Restrictions

You can set time restrictions for an access rule that makes the access rule effective only during certain time frames.

BorderManager can only set time restrictions in one-hour increments, and time settings **do not change with daylight savings time changes.**

Consider this rule example, which denies certain types of URL's for browsing during working hours.

A Deny URL access rule for a particular web site has been created. It is desired that the rule only deny access between the hours of 8:00am and 6:00pm.



The Time Restrictions button was checked, and the time grid was grayed out between the hours of 8:00 am and 6:00 pm.

When this rule is put in place, the web site in the access rule is blocked starting at 8:00 am for the rest of the working day. At 6:01 pm, that site is available, unless blocked by some other access rule.

Setting Up Access Rules

From the NWADMIN screen, select the BorderManager server (here, BORDER1), and then select the **BorderManager Access Rules** tab to bring up the Access Rules main menu.

When BorderManager is first configured, you have the option of allowing or denying traffic. Allowing traffic just results in not enforcing rules. Denying traffic results in enforcing rules and relying on the default deny rule.

BORDER1 will always be configured to Deny All traffic that does not meet the criteria of one of the rules listed in the Access Rules screen. You can check this by clicking on the Effective Rules button, which not only shows the default rule (at the bottom of the list it shows), but also any rules inherited from containers higher in the tree.

Rules are not implemented unless the Enforce Access Rules box is checked on the BorderManager Setup main menu screen.

Caution: It is not recommended to apply rules to containers unless you thoroughly understand the ramifications of the rules inheritance, timing and NDS design issues involved.

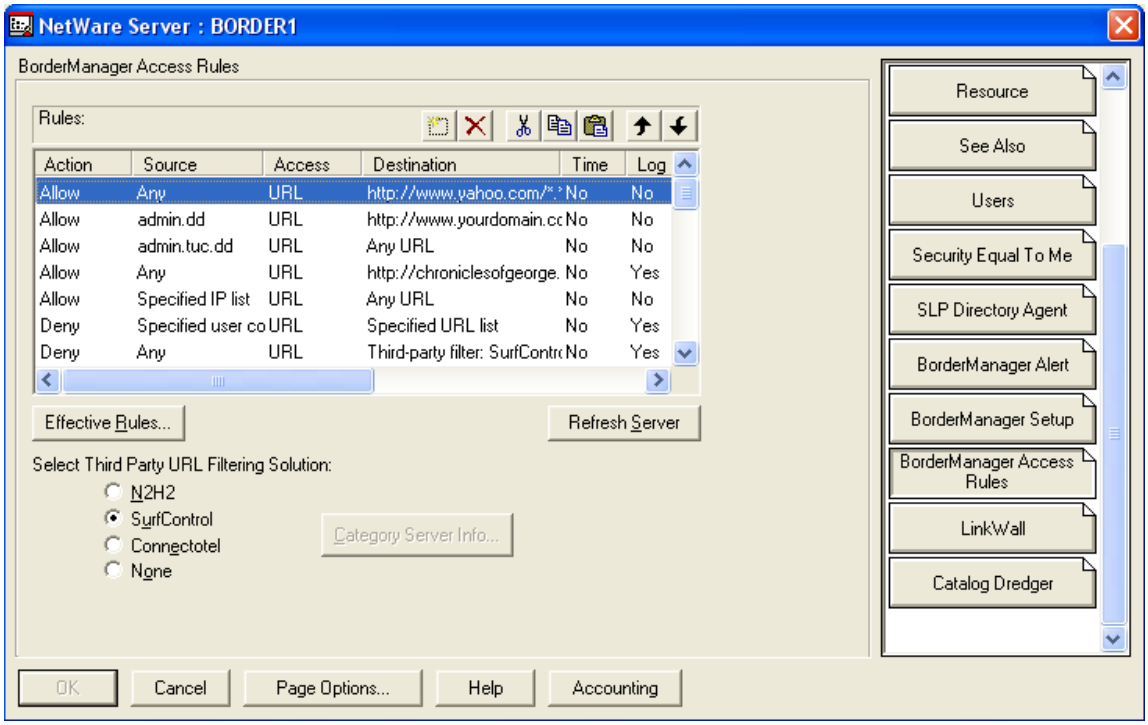
Access rules can be based on NDS object (requires Proxy Authentication to be enabled!), DNS hostname, or IP address or subnet. Rules set with a source of ANY will apply to both NDS and IP sources.

Rules are read from top to bottom. If a rule is matched, no further rules below it are checked. Structuring the order of the rules is critical to success. If a Deny rule based on SurfControl is to be set up, but there is an Allow All rule above it, no one will ever get to the SurfControl rule. Sometimes you need to use the **Refresh Server** button to apply a rule change to the server.

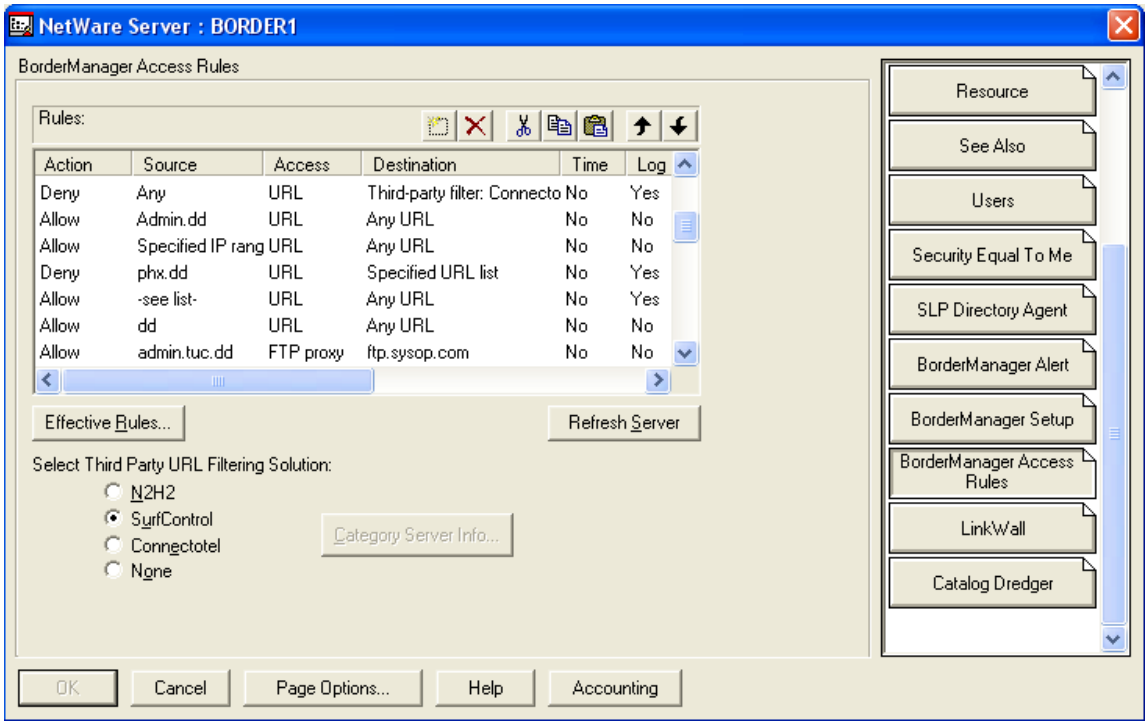
Note Putting the least frequently used rules below more frequently used rules may enhance performance, though you may not notice any real difference.

Explanation of the Effective Rules

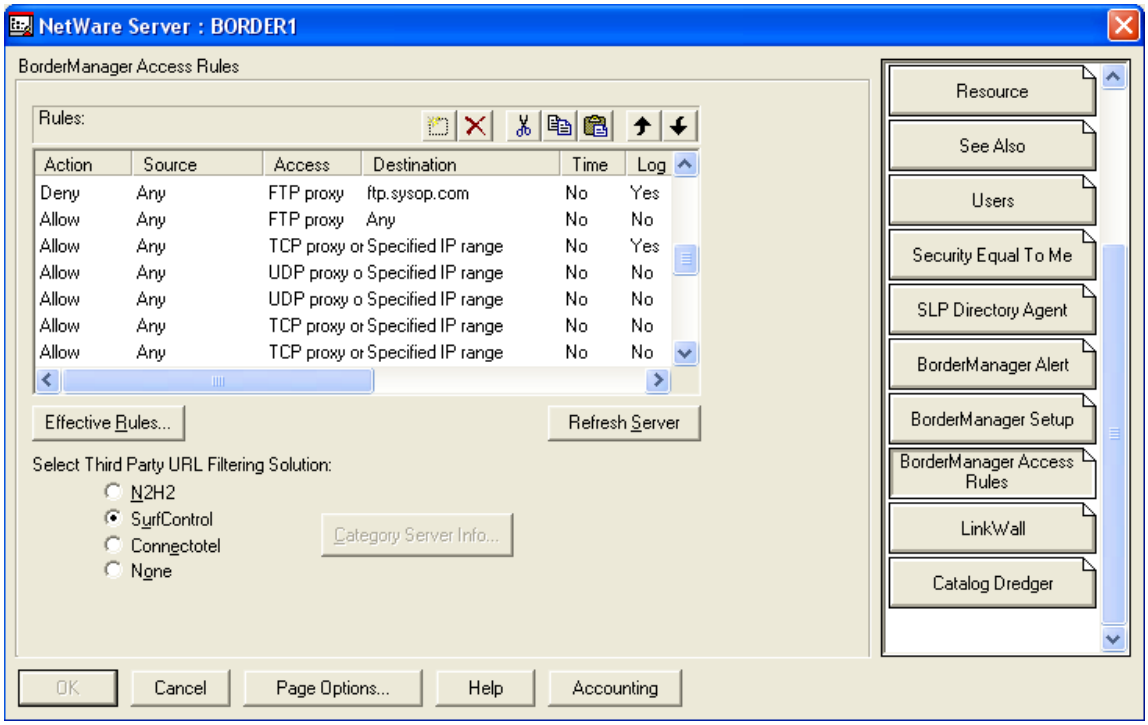
The following access rules are in place on BORDER1. There are additional rules inherited from containers higher in the NDS tree, and they are not shown unless you click the Effective Rules button. The Effective Rules are shown in the next section.



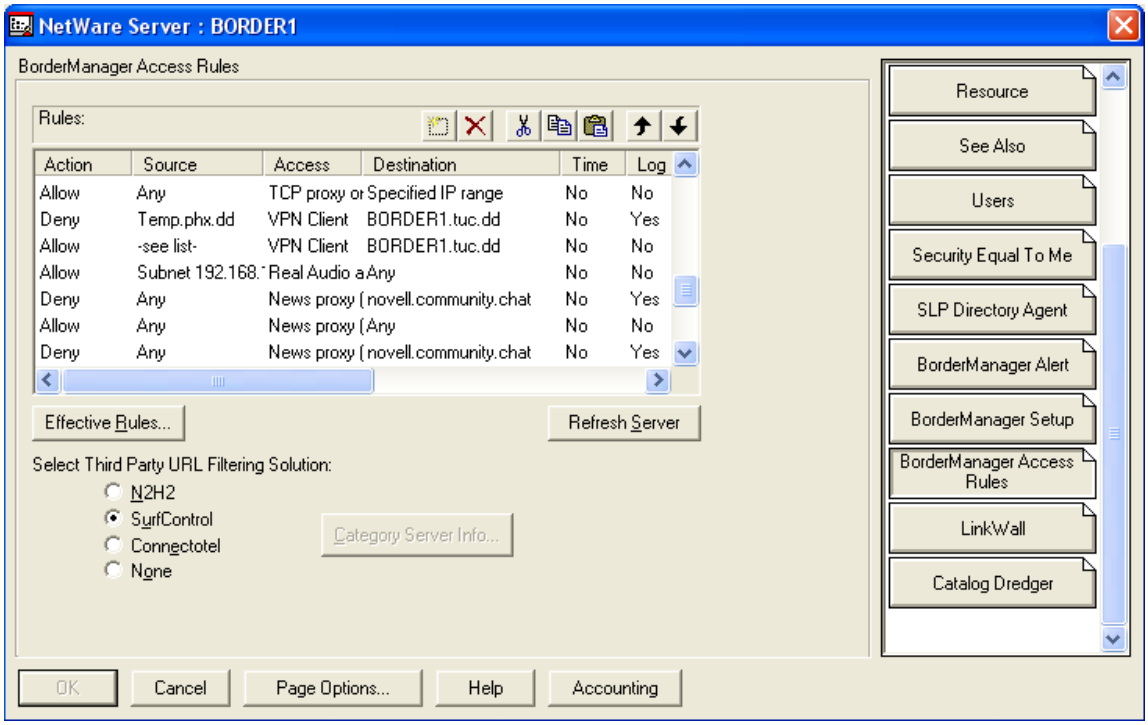
The example above shows the top of the rules list. The following graphic shows the middle of the list after scrolling down.



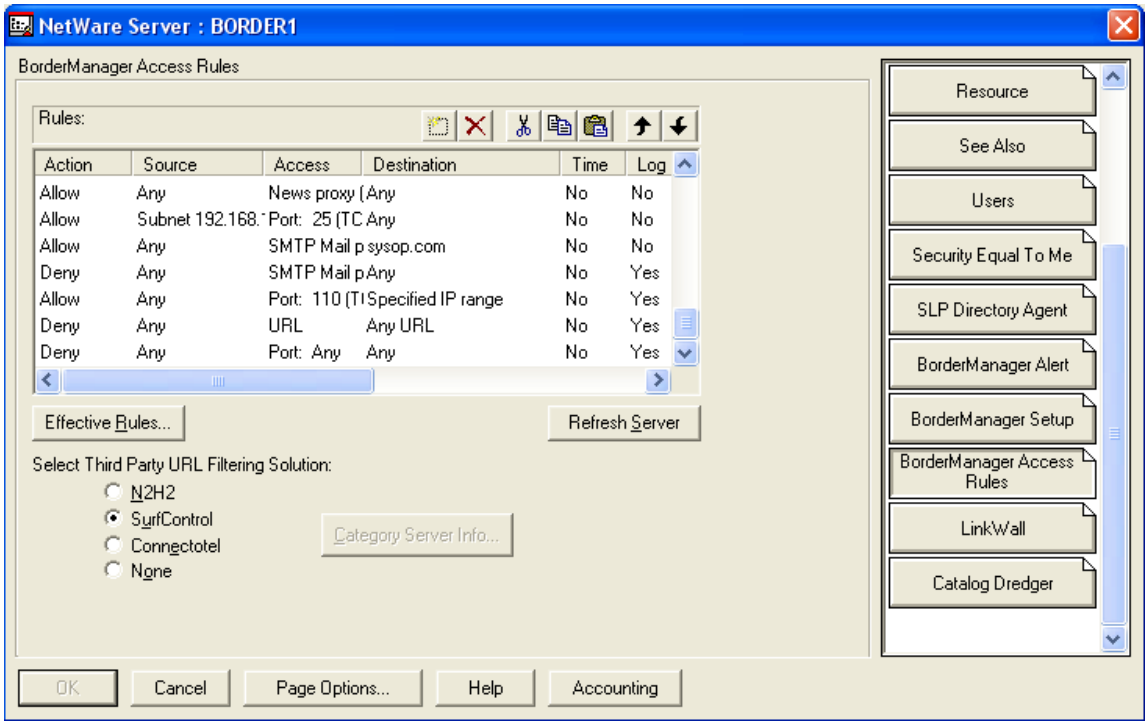
The graphic above shows the rules after scrolling down a bit.



Here are more of the rules after scrolling further down.



More rules…



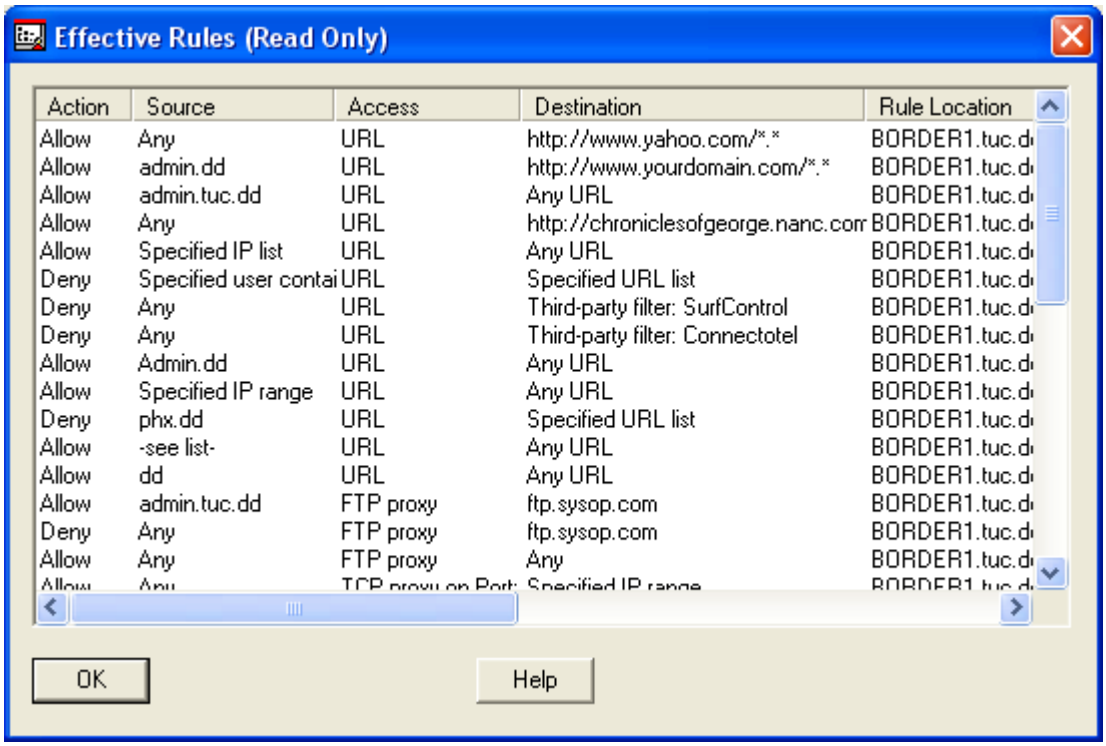
The graphic above shows all the remaining rules at the bottom of the rules list not visible in the previous graphics.

The rules shown are all applied to the BorderManager server object.

Some additional rules, not seen in the graphics above, have been applied to containers higher in the tree than the BorderManager server, and they can be seen by clicking on the **Effective Rules** button.

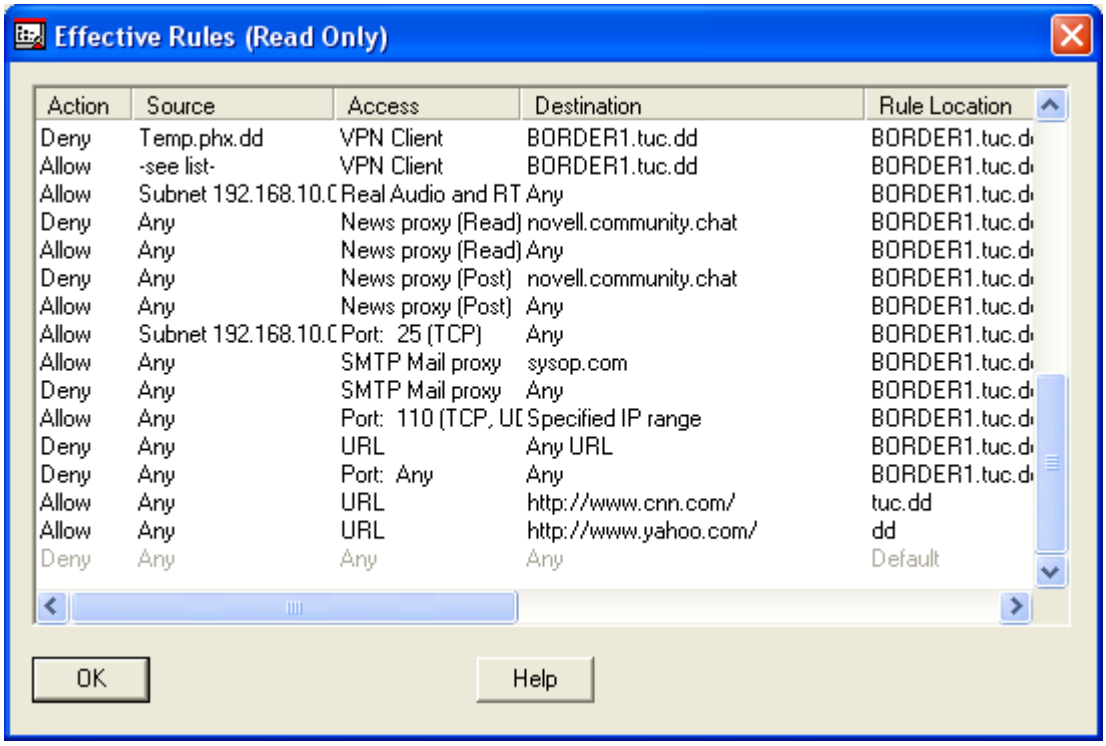
Checking Effective Rules

Clicking on the **Effective Rules** button will show you ALL the rules that the BorderManager server has in effect. You will see both the rules applied to the server object itself, and rules inherited from higher in the NDS tree.



The example above only shows the top part of the **Effective Rules** list. There are so many rules that the list must be scrolled down to see them all.

Note I have adjusted the column borders in the examples shown so that the columns in view can be more easily seen. You can drag the rule divider columns as you like to see the complete column.



The graphic above shows the bottom of the rule list after scrolling all the way down.

Compare the end of the **Effective Rules** list in the examples above against the previous example showing only the rules applied to the BorderManager server object. You will notice **three additional rules** added at the bottom of the screen, one of which is in gray.

The additional rules consist of one rule inherited from the **TUC.DD container**, and one rule inherited from the **DD Organization container** high in the NDS tree, and the **default rule** (Deny Any).

The default rule is the one in gray at the very bottom of the rules list. The default rule is always there. While the default rule cannot be changed, an equivalent rule reversing the installed default rule can easily be added at any time. Just add an Allow Any rule at the bottom of the rules list if needed.

The inherited rules bear some explanation. BorderManager servers can search from their server object to the root of their NDS tree for access rules applied to containers. Only a container on a direct path to the root of the NDS tree will be searched for an access rule. If a 'parallel' container has an access rule, BorderManager will not see it.

In the NDS tree used for these examples, a Deny URL rule was placed in the PHX.DD container, but the BorderManager server (located in TUC.DD) does not see it. Only the access rules placed in the TUC.DD and DD containers were seen. Notice how the

inherited rules are positioned in the rules list. All the rules assigned to the BorderManager server object are placed above the rule assigned to the TUC.DD container. The rule placed on the TUC.DD container is placed above the rule assigned to the DD container. You have no ability to rearrange these rules. Thus, the rules 'more local' to the BorderManager server override the rules assigned 'farther away' to containers. Since the rules are read from top to bottom, it is possible that the Deny URL rule (which is a SurfControl rule) could override the two inherited Allow URL rules (although that is unlikely in this case because the Allow URL's are not supposed to be in the SurfControl denied categories).

Note the nature of the Allow URL rules involved here. The source definition is different, and that aspect will have an effect as follows:

1. Any user can access http://www.yahoo.com because of the position of that Allow URL rule high in the list.
2. The .admin.tuc.dd user is allowed to access any URL. This means that Proxy Authentication would have to be used by the .admin.tuc.dd user or the rule would be skipped over. Because this Allow URL rule is placed higher in the rules list than the Deny URL rules following it, the .admin.tuc.dd user will be allowed to access all URL's, including reverse proxies.
3. All users will be denied access to the specified destination URL's by the Deny URL rules near the middle of the list. One Deny URL rule happens to be a SurfControl list rule (explained later in this book). The SurfControl list rule will not allow anyone (except .admin.tuc.dd) to see what is considered objectionable material.

Note It may be worthwhile to set up a separate SurfControl Deny rule for each SurfControl category in order to be able to tell users which category was denied to them, by tracking an Access Control Log entry to the access rule number.

---

4. Members of the NDS group InternetUsers.Tuc.DD are allowed to access any URL that has not already been blocked by the SurfControl and the rule designed to block certain downloads above it. This means that users must be proxy authenticated AND be members of the InternetUsers group. If the users are not proxy authenticated, this rule will be skipped over.
5. The inherited rules from higher in the tree are both blocked by the Deny Any URL rule applied to the BORDER1 server object. If that Deny rule had NOT been applied to the BORDER1 server object, then all users would be able to access the http://www.cnn.com web site, because of the

Allow URL rule inherited from the TUC.DD container. Note that the source definition for this rule is Any, which means that users do not have to be proxy authenticated in order to match this rule. Thus users that were not in the InternetUsers group or who were not proxy authenticated could still access this web site.

6. Again, The inherited rules from higher in the tree are both blocked by the Deny Any URL rule applied to the BORDER1 server object. If that Deny rule had NOT been applied to the BORDER1 server object, then All users would be able to access the http://www.yahoo.com web site because of the Allow URL rule inherited from the DD container. However, this rule is redundant and would never have been used because it matches the first rule at the top of the list. This is an example of what can happen when you have rules being inherited from containers higher in the tree.
7. All users will be denied all other URL's (or ports) because of the Default Deny Any rule at the very bottom of the list. The Deny Any action is configured when you set up BorderManager, and could also have been set up to Allow Any instead. If you want to change the action of the Default Rule, you would have to add another rule in front of it. You cannot change the Default Rule except by reinstalling BorderManager. However, adding an opposite rule at the bottom of the rules list is easily done.

Note If you are using inherited rules, adding another rule to the very end of the rules list can only be done by adding the rule as high or higher in the NDS tree as the inherited rules.

It can sometimes be useful to add other Deny rules to the end of the access rules list, as has been done on BORDER1. Why? In order to log the sites (or ports) which are being denied. There is no feature in the Default Rule to log access attempts, so you would have to add an access rule above it and enable rule logging. This may be useful for troubleshooting.

Rules Applied On BORDER1

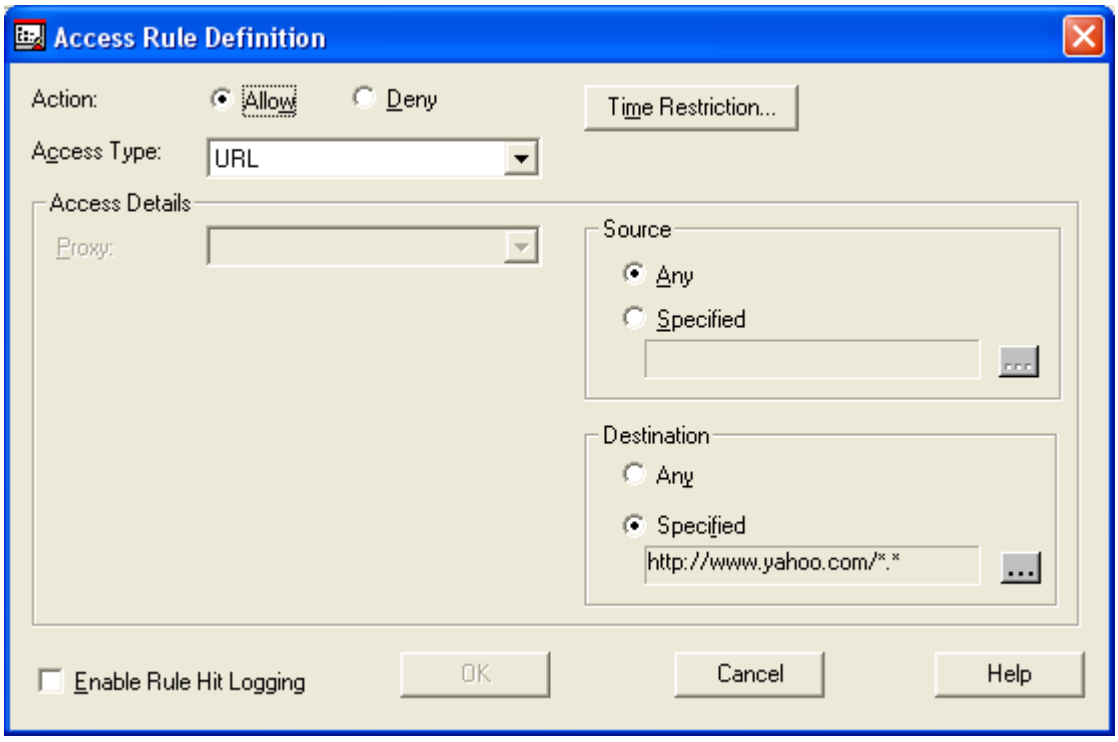
All of the access rules applied on the BORDER1 server are explained below so that you can see how the rules work together.

Allow All users to Access Selected URL's

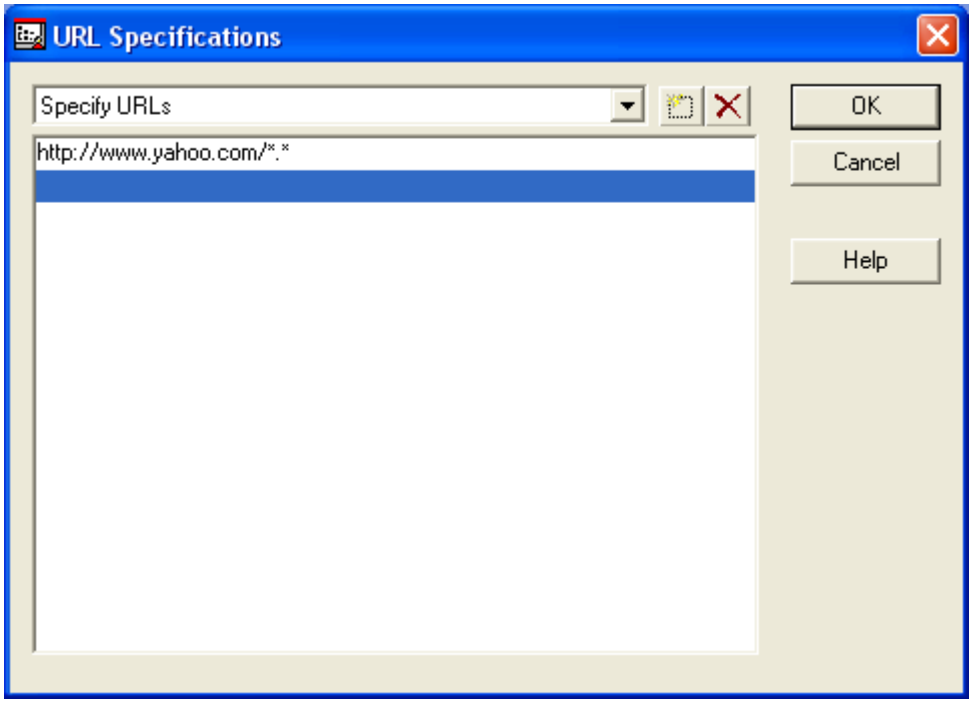
This access rule was originally put into place to allow access to http://www.yahoo.com after Yahoo somehow ended up on the CyberPatrol NOT list and was blocked. However, the same rule can be enhanced as desired by adding additional 'known-good' URL's to the list, which might otherwise be blocked by some later Deny rule.

Note You can go to the http://www.surfcontrol.com web site to see if a particular URL has been placed in a particular category.

Because this web site is used as a home page by many users, the rule check will come up frequently, and it has been placed at the top of the rules list for performance reasons.



These are the access rule settings, and the following screen lists the specified destination URL's.

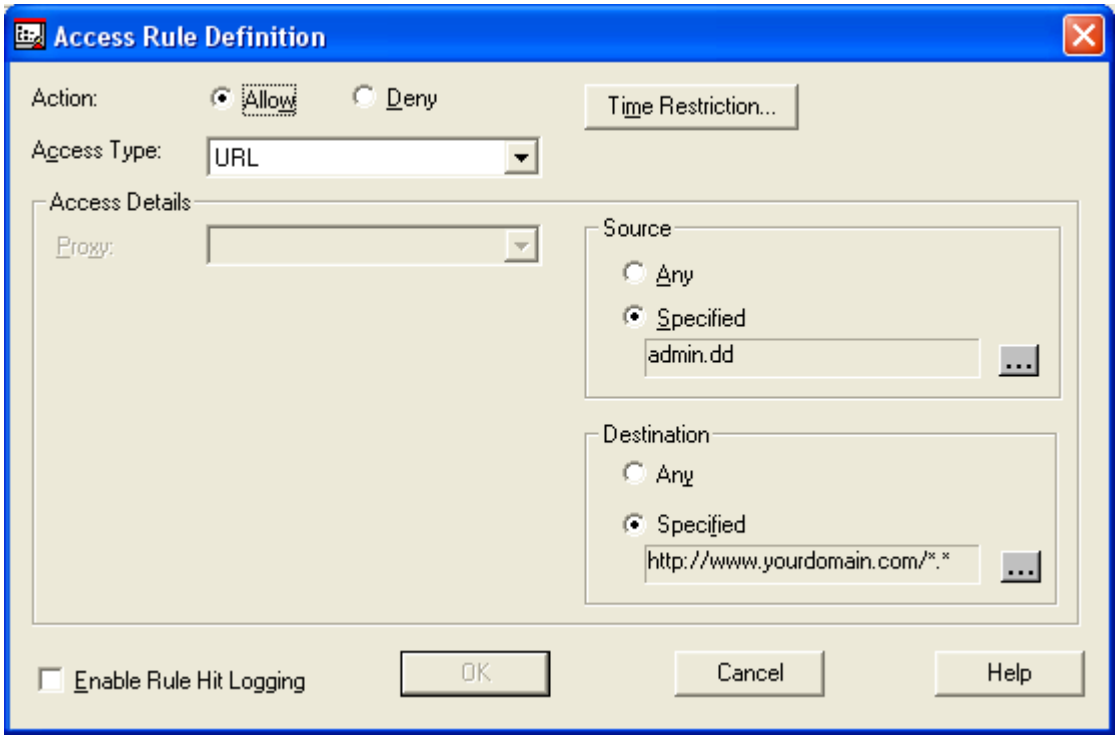


The example shows only one URL placed in the access rule list – **http://www.yahoo.com/*.*** The asterisks are necessary wildcards to also ensure that subpages of the host URL can be accessed.

This example was once used to allow access to the Yahoo web site after that web site was mistakenly put on a CyberPatrol CyberNOT blocking list.

Allow the Admin User to Access a Reverse Proxy

This rule has been configured to allow the Admin.dd user to access the reverse proxy for WWW2.YOURDOMAIN.COM



The Source for this rule has been designated as **Admin.dd**, and the Destination has been specified as **http://www.yourdomain.com*/***. The wildcards (*/*) in the access rule allow subpages of the main URL to also be accessed through the reverse proxy.

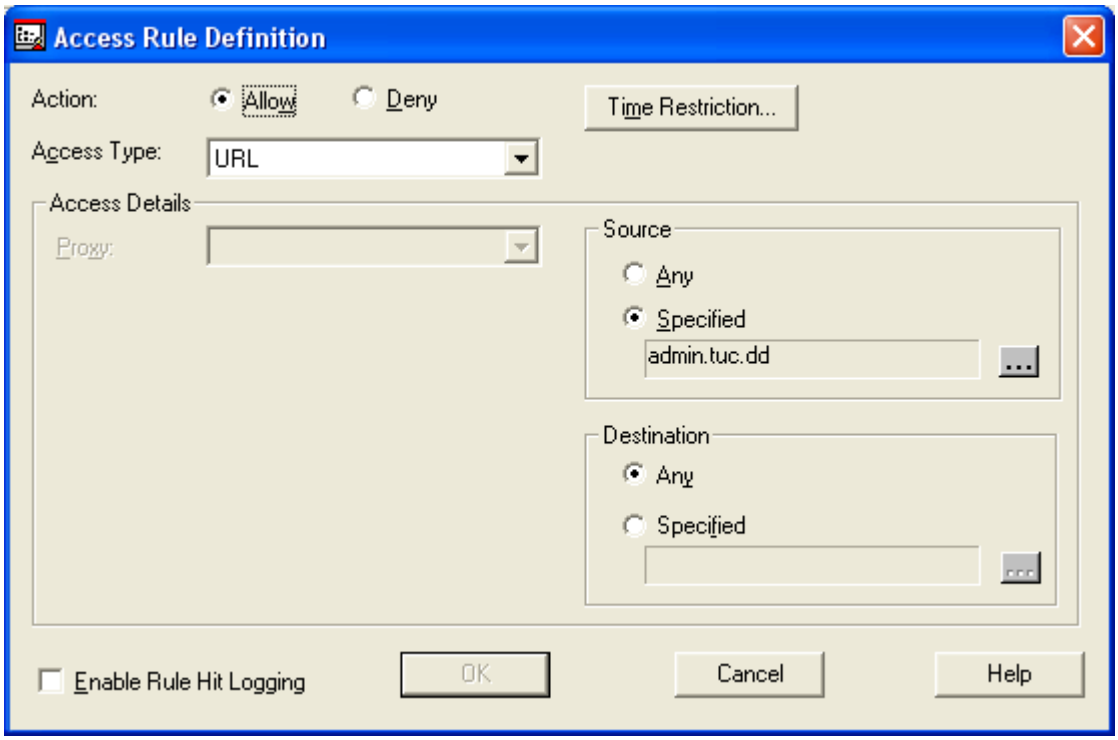
The rule will apply equally to traffic from the internal LAN, as long as the browsers are configured to go through the HTTP Proxy. However, if the browsers of the internal users are configured to bypass the proxy for the URL shown, they may be able to access the web server without going through the HTTP Proxy.

This access rule needs to be above any rule that would Deny access to Any URL, or it would never be applied.

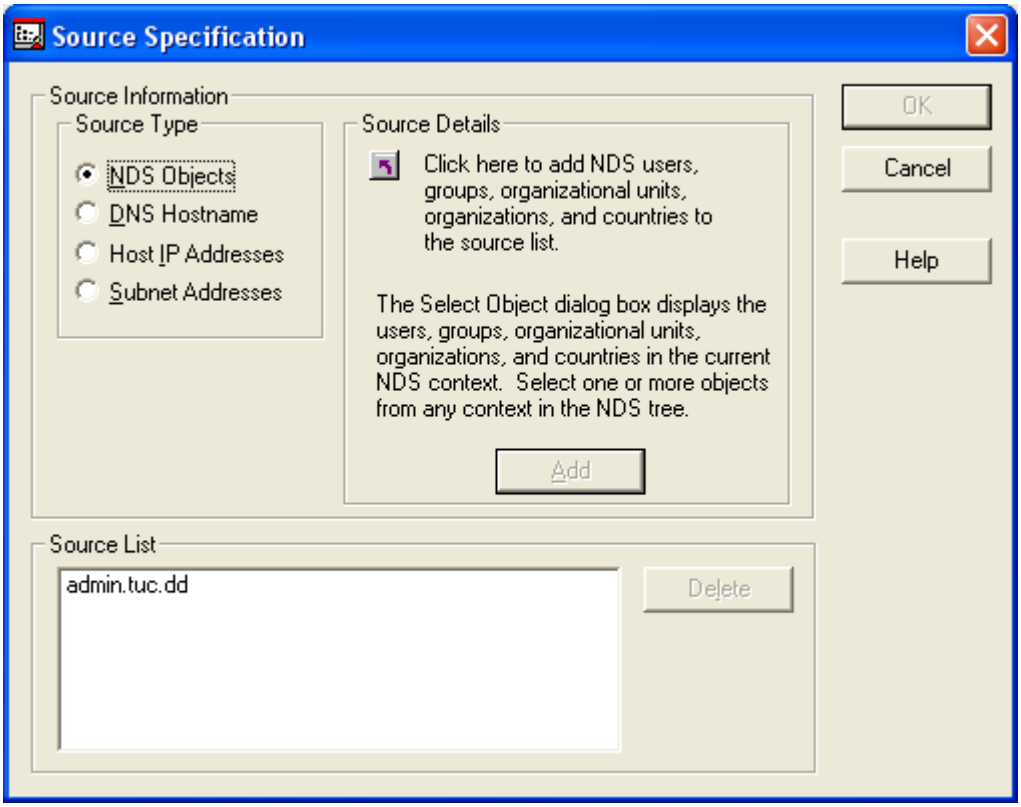
Reverse proxied websites ignore access rules unless the option to 'Enable Authentication for this particular accelerator' is checked in the reverse proxy configuration.

Allow Selected Users Access to Any URL

This rule was added to allow a selected user to be able to browse to any web site and verify if those sites should or should not be blocked by other access rules.



The following screen shows the users ID's authorized to access Any URL.



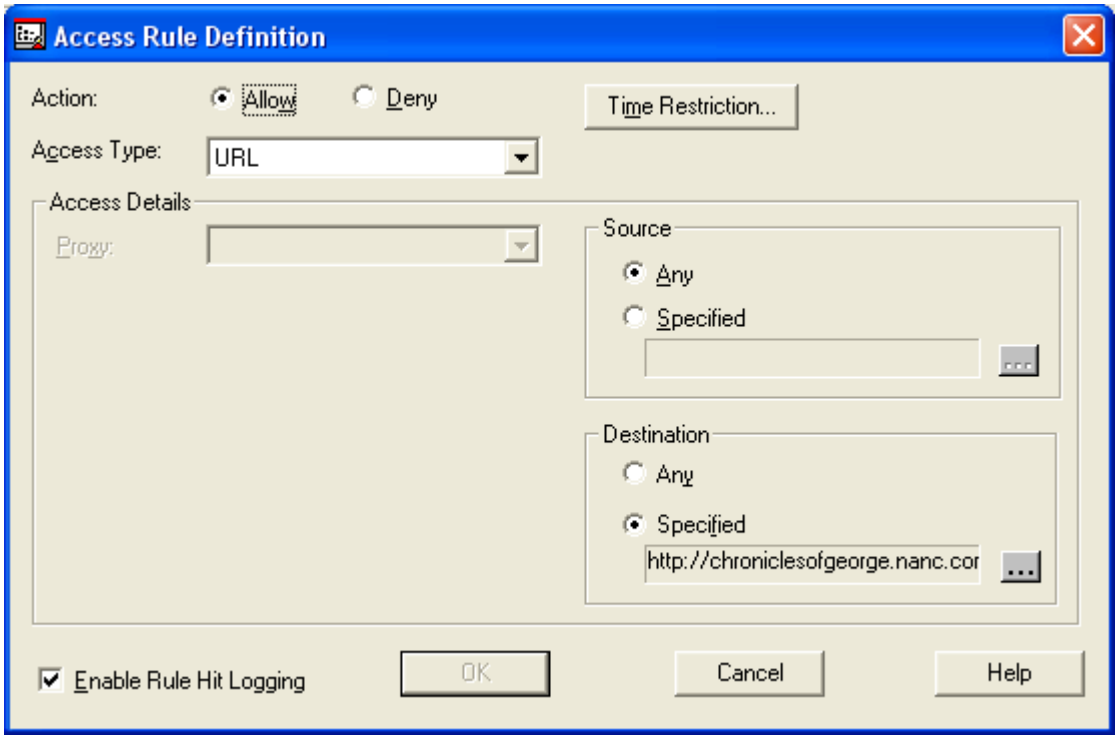
The source list shows the user ID's allowed to browse to any URL. Note that CLNTRUST or an SSL Proxy Authentication login **must** be used in order for this rule to be invoked because the source list specifies NDS objects.

Note If CLNTRUST is not running or SSL login has not been achieved, this rule will be ignored and access to a URL will be granted or denied based on other access rules farther down the rules list.

Track Usage for a Particular Web Site

This kind of rule can be put into place specifically to find out who is accessing a particular URL showing up on the Proxy Console screens with a tremendous amount of data being transmitted.

The desire might be to question the user to find out what is causing the large amounts of data transferred, and to see if the activity was related to a read-ahead bug, or possibly a Web Cam.



The important points about this rule are that a particular URL was specified (**http://chroniclesofgeorge.nanc.com/*.***), and **Rule Hit Logging** was enabled.

Because rule hit logging was enabled, the Access Control logs will show either an IP address or User ID (if Proxy Authentication was used) of person accessing this URL.

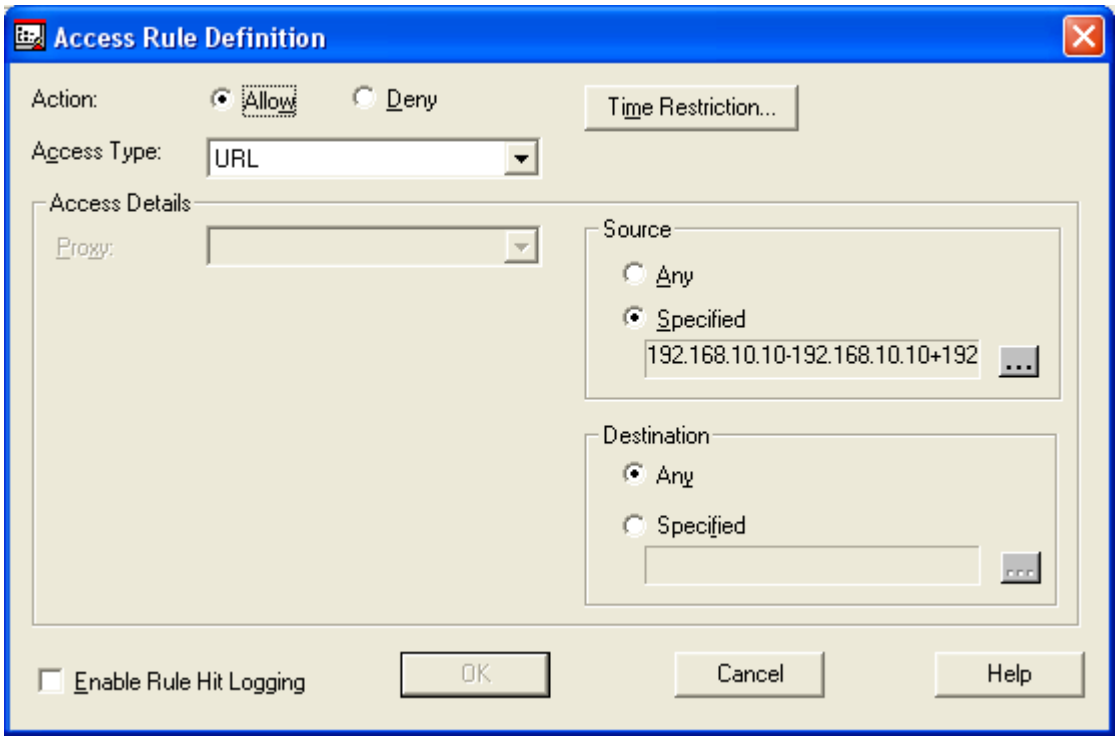
This example shows **one way** of tracking use of a web site to a user.

One of the subtle points about this example is that it would be used when most URL access is NOT logged. If you log ALL browser access through Access Rule Hit Logging, you end up with a very large log that is tedious to search and slow to export. The Common log files are generally used to track all outbound web access – this rule simply allows an easier method of finding a particular user.

Due to logging concerns, this rule must be added above any rule that allows users to browse if those rules do not enable access logging.

Allow All URL's for Specific IP Addresses

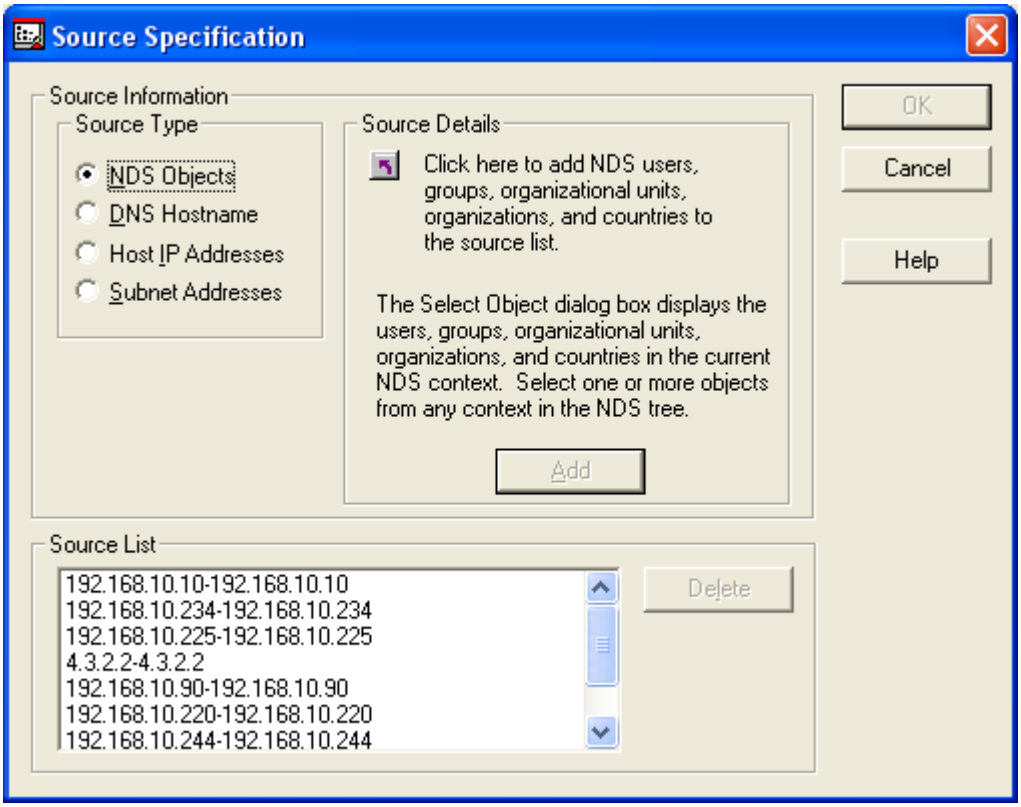
This rule is designed to work in a situation where selective proxy authentication is being used. Refer to a section later in this chapter for a specific explanation, and some other access rule samples.



The purpose of this rule is to allow a number of internal hosts to make use of the proxy for browsing without having to authenticate. This rule makes no sense if the option '*Authenticate only when users attempts to access a restricted page*' is not enabled in the Authentication Context menu.

Within a network, there may be a number of hosts (typically servers) that may need web access through a proxy, but where proxy authentication is not useable. These hosts include test servers, other proxy servers configured in a proxy cache hierarchy, and hosts designed to do some form of automated browsing activity without a user logged in.

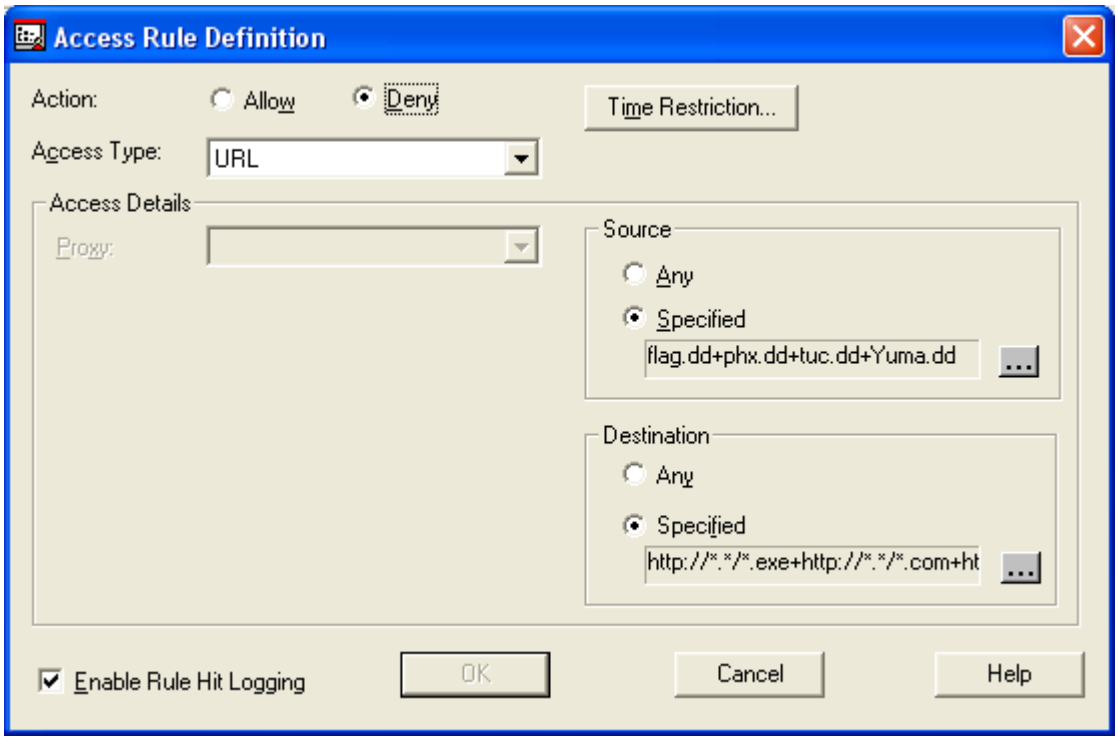
A number of host IP addresses and ranges have been configured in this rule.



Generally speaking, the IP addresses configured here are for test servers.

Block Selected Downloads

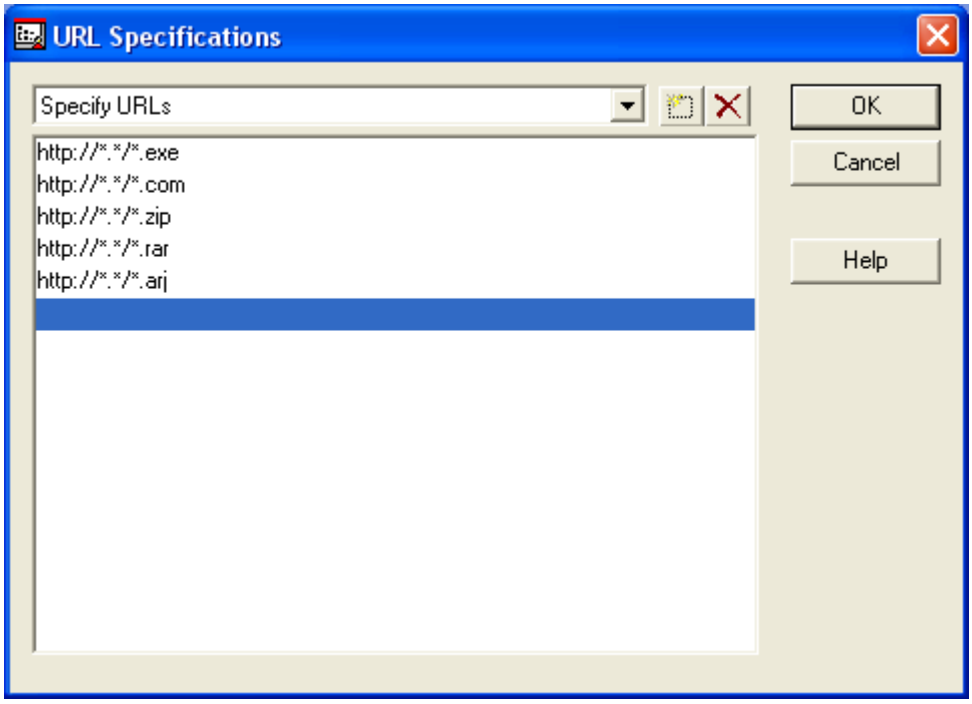
This rule is designed to prevent users from downloading EXE, COM ARJ, RAR and ZIP files from the Internet. It makes use of wildcard characters.



Rule Hit Logging is enabled, as it is desired to know what access has been denied through a study of the Access Control logs.

Due to the location of this Deny rule in the access rules list, the only user that will be able to download the specified files using a browser through the HTTP Proxy will be the Admin.tuc.dd user, which has an allow Any URL rule higher in the list.

The destination URL's specified are shown on the next page.



Note the syntax of this rule. Wildcard characters have been specified that will match any URL that ends in EXE, COM, ZIP, RAR or ARJ.

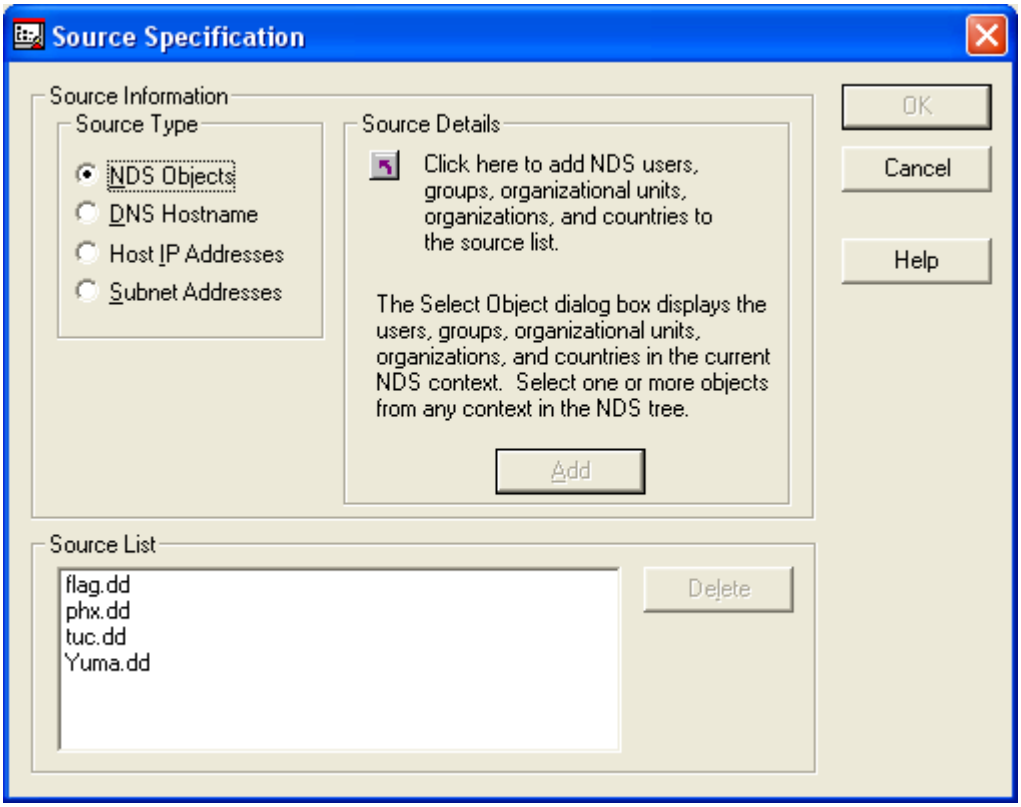
The syntax to use is:

HTTP://*.*/*.<filename extension>

The example shown will block various extensions when downloaded via HTTP, but not when downloaded via FTP. To make the rule more general, use a wildcard in place of the HTTP. For example:

***://*.*/*.<filename extension>**

CAUTION *HTTPS files will NOT be controlled by this technique or by using HTTPS in the access rules, due to the nature of how HTTPS (SSL) traffic is tunneled through the proxy. To control HTTPS sites, you must configure access rules with Port 443 access rule.*

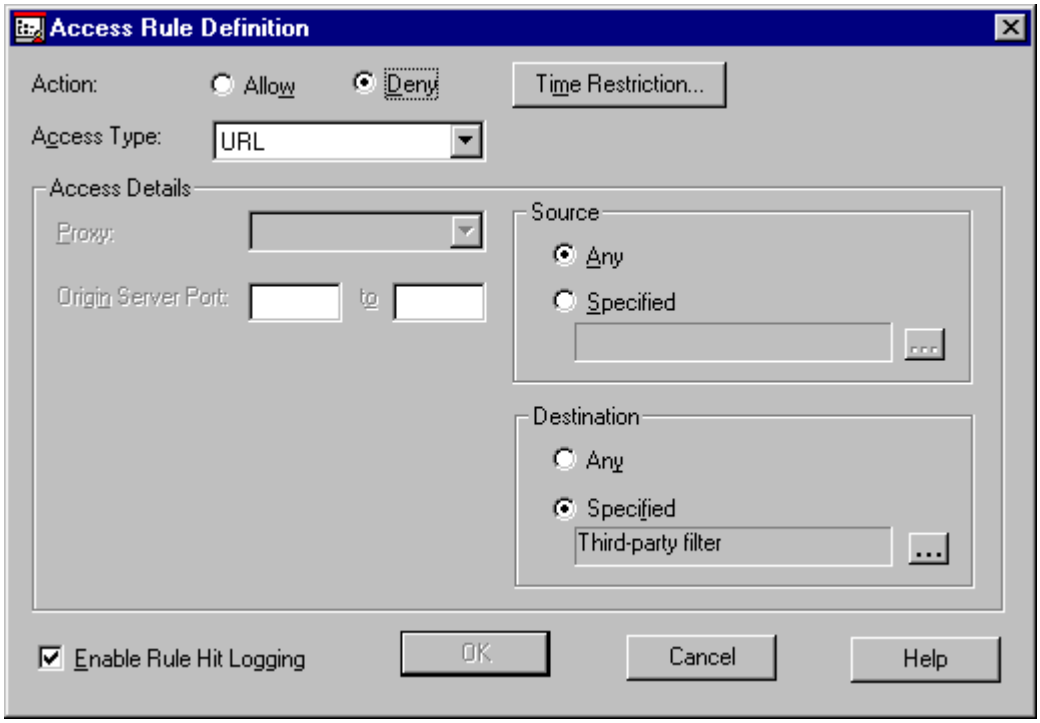


The rule applies to any user in the following NDS containers or below them:

- **Flag.dd**
- **Phx.dd**
- **Tuc.dd**
- **Yuma.dd**

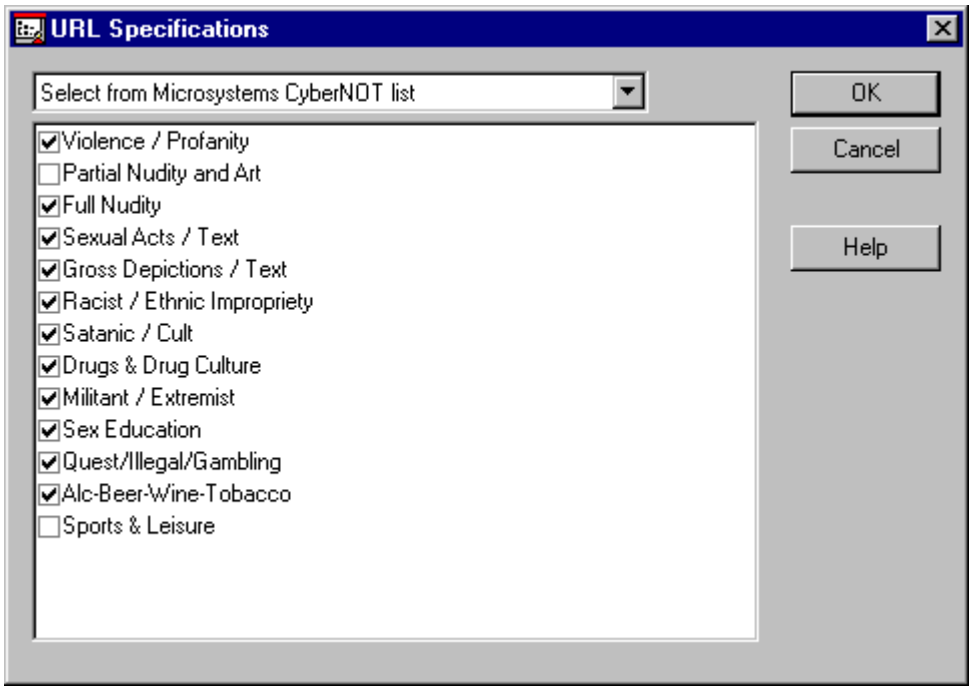
Deny Access to URL's with CyberPatrol

This rule would be used in place of the SurfControl rule shown in the next example, if you are still using the old CyberPatrol software that came with BorderManager 3.0 – 3.6.



This rule denies access to all URL's in the specified third-party filter, in this case most of the categories on the **CyberPatrol CyberNOT list**. The specific categories denied are shown later in this book. This rule also has **Rule Hit Logging** enabled, so all access attempts denied by this rule will show up in the Access Control Logs.

These are the denied categories.

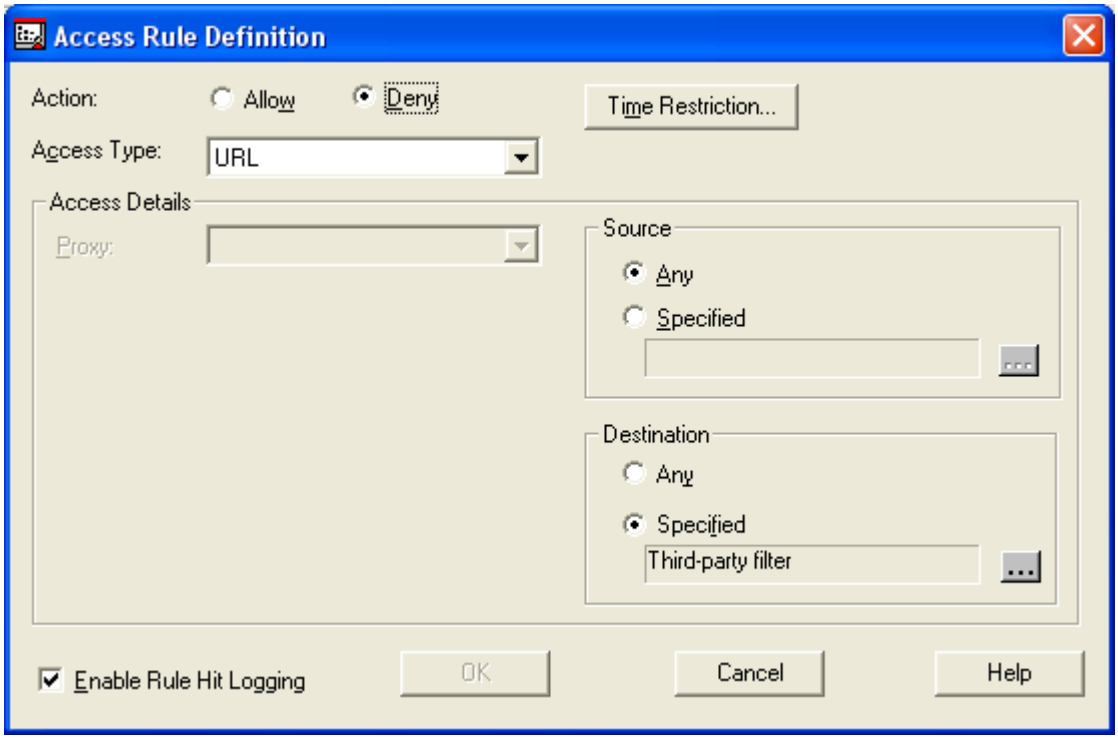


These categories were picked arbitrarily for this book, though I have found them to be typical for the corporations I have worked at.

If you are wondering how to get CyberPatrol installed and working, see the chapter later in this book on that explains CyberPatrol, SurfControl, LinkWall and N2H2.

Deny Access to URL's with SurfControl

This example shows how an Access Rule for SurfControl looks, once it has been registered.

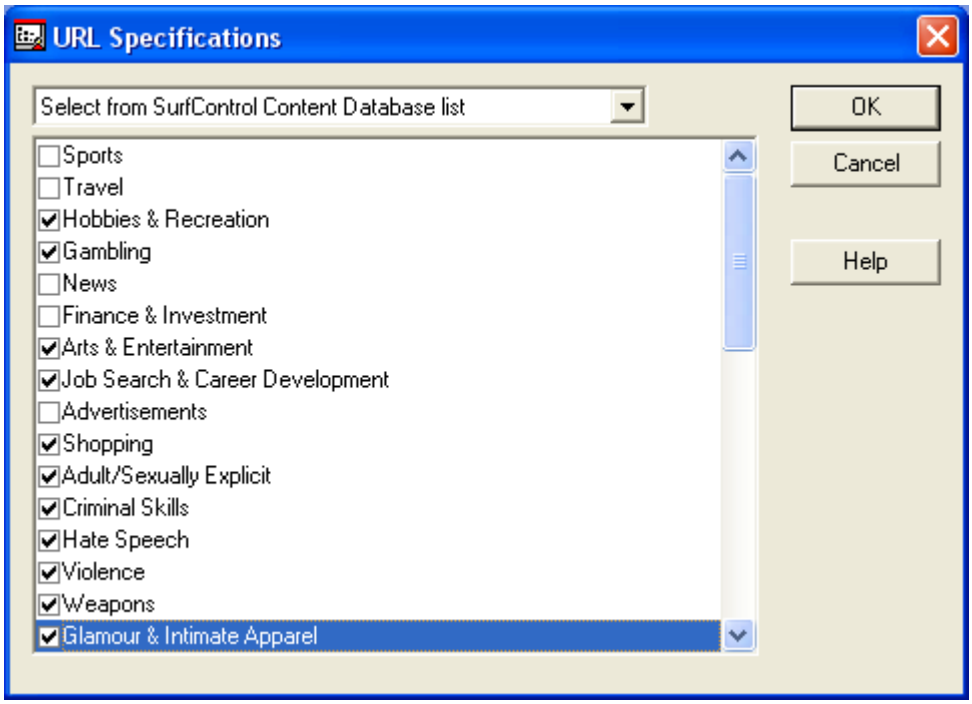


This rule denies access to all URL's in the specified third-party filter, in this case most of the categories on the SurfControl Novell BorderManager list. The specific categories denied are shown later in this book.

This rule also has **Rule Hit Logging** enabled, so all access attempts denied by this rule will show up in the Access Control Logs.

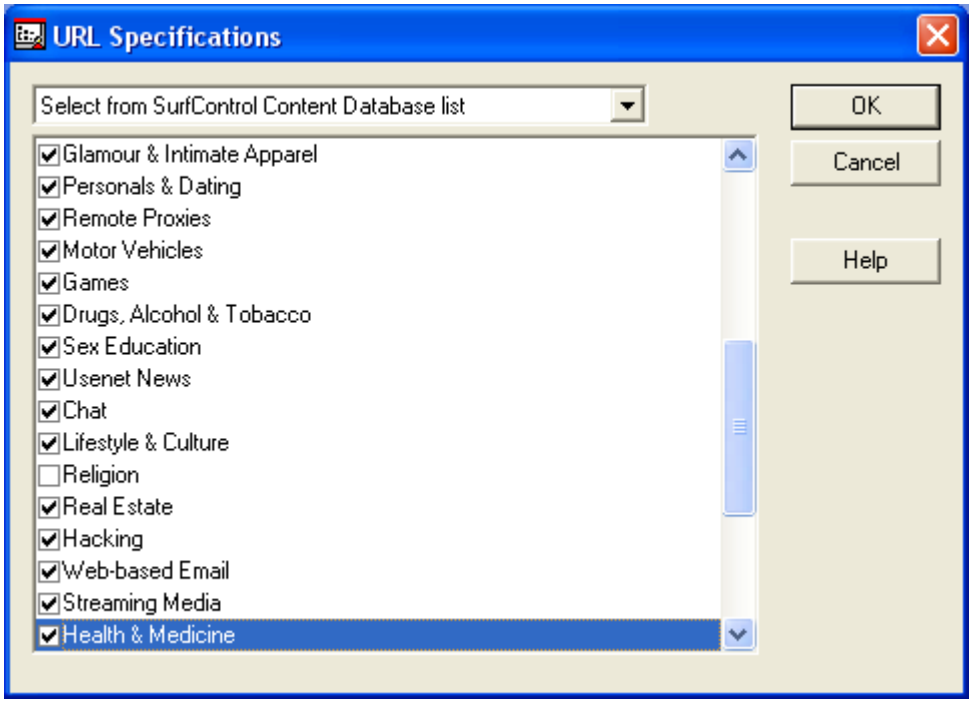
Note The SurfControl option at the bottom of the Access Rules menu (under Select Third Party Filtering Option) must be selected in order to use SurfControl. The menu option itself first shows up with PROXY.NLM from BM37SP2 or later patches.

These are the denied categories.

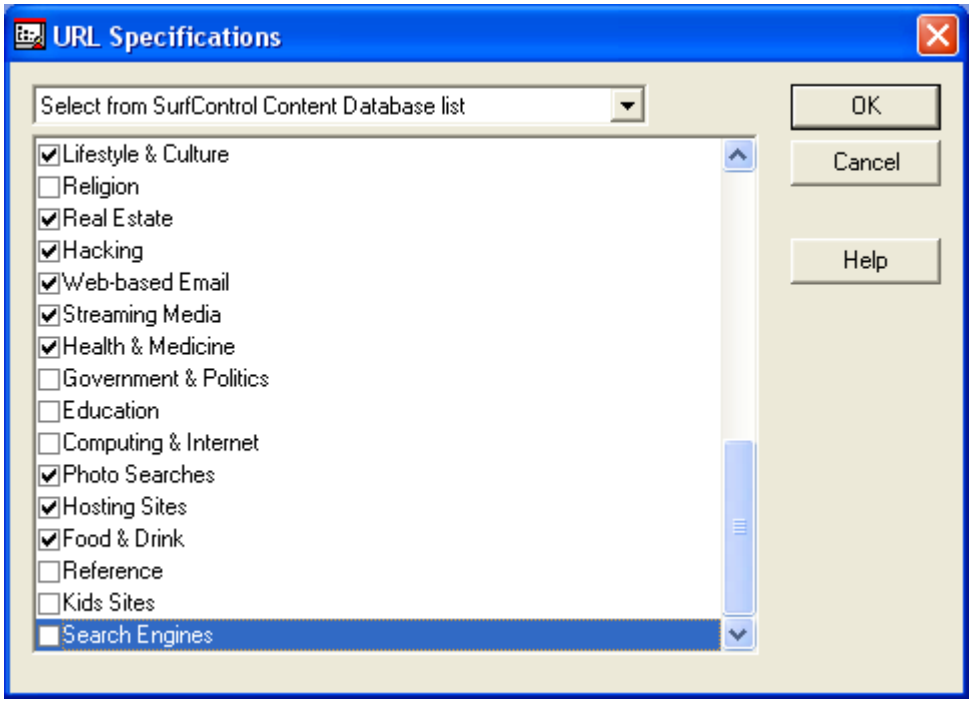


The screenshot above shows some of the categories. The following screenshot shows additional categories visible after scrolling down.

Notice that Advertisements is left unchecked. SurfControl can block many advertisements, but the result is that the users are left with small '403 access forbidden' graphics throughout their web pages as the imbedded online advertisements themselves are denied. And each blocked advertisement ends up in the access logs, adding essentially useless log data.



Here are additional categories shown after scrolling down the SurfControl list. These categories are present in Service Pack 1 and 2 of SurfControl. SurfControl Service Pack 3 adds the last 8 categories shown in the screenshot below.



These categories were picked arbitrarily for this book. Most of these categories only appear if a SurfControl subscription is active.

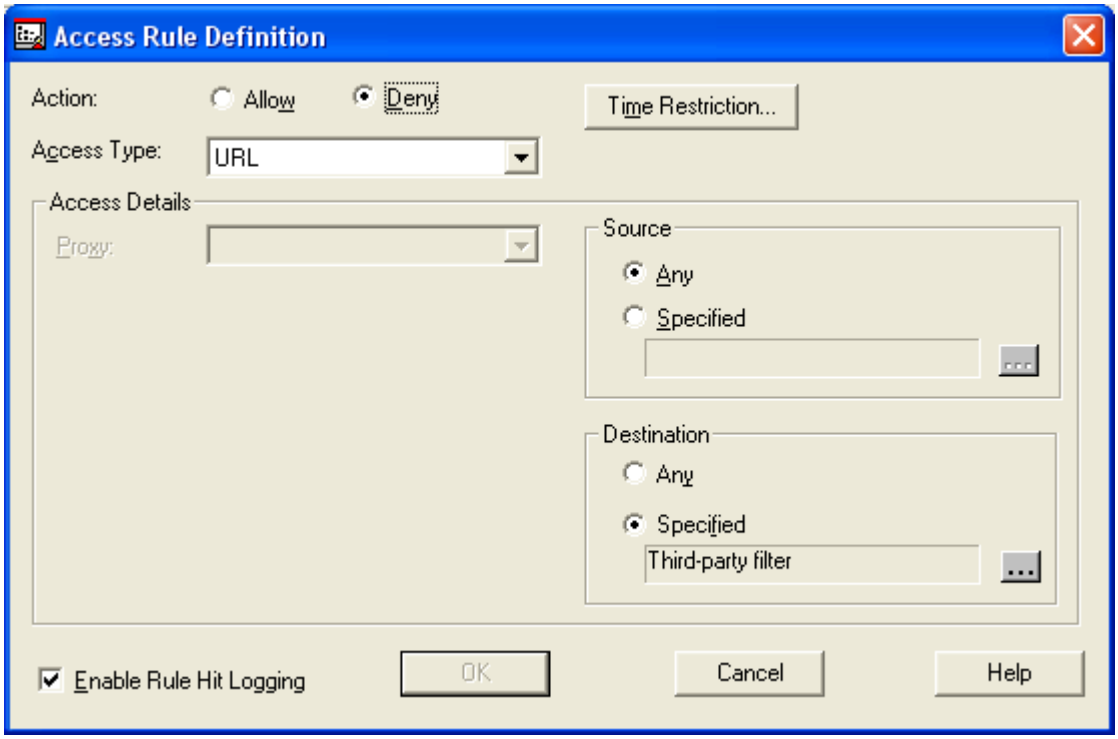
If you are wondering how to get SurfControl installed and working, see the chapter later in this book on that explains CyberPatrol, SurfControl, LinkWall and N2H2.

Deny Access to URL's with LinkWall

LinkWall is a third-party product by Connectotel (http://www.connectotel.com) that is designed to read one or more text files of URL's into an access rule, usually to deny those web sites.

LinkWall also can integrate with the third-party utility called RTMonitor to show where people are browsing in real-time, and almost immediately add sites you don't like to a blocking list.

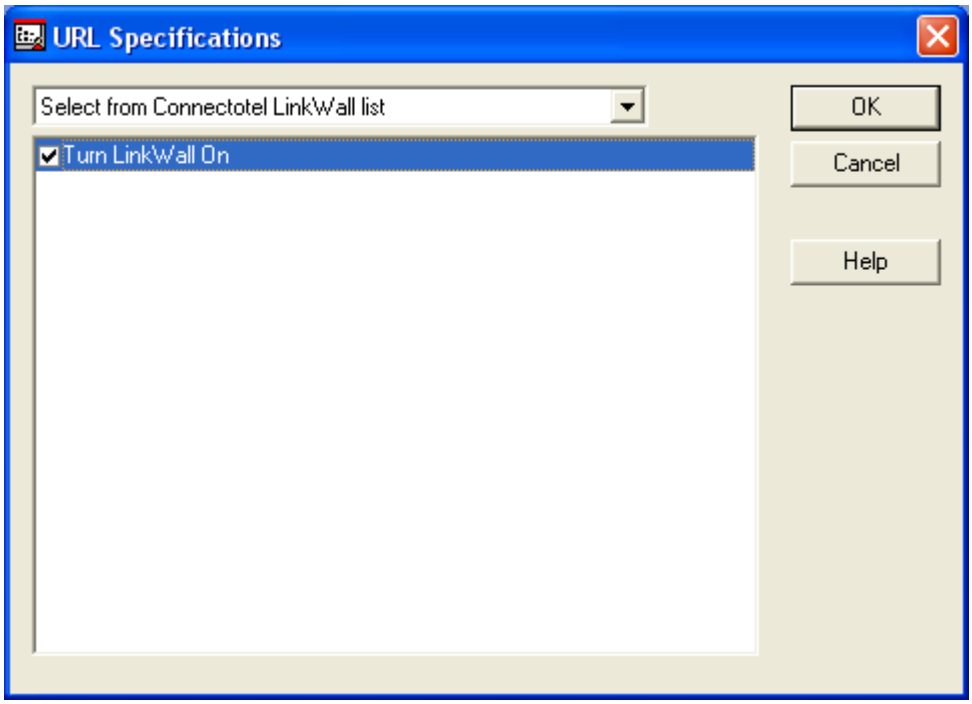
LinkWall installation and configuration is shown in a chapter later in this book.



The access rule for LinkWall looks a lot like the one for SurfControl, until you look at the specified destination.

Contrary to what it may seem like, you do NOT have to choose the Connectotel option at the bottom of the Access Rules menu in order to use LinkWall. LinkWall will work fine running on the server at the same time as SurfControl, or running while BorderManager is using N2H2.

This is the denied category.

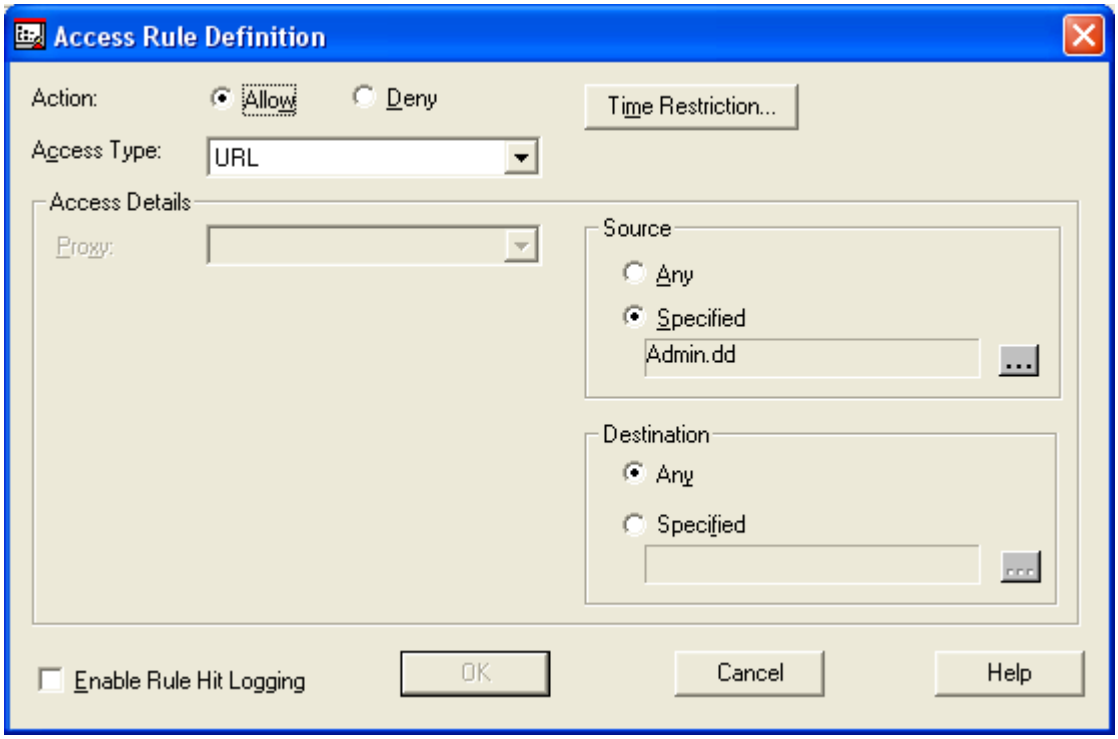


There is only one option – use the LinkWall blocking list.

The choice of what to block is up to you, by maintaining the lists of URL's that LinkWall uses, which can be extensive. See the chapter later in this book about configuring LinkWall.

Allow Admin to Get to Any URL Not Already Blocked

This access rule allows the Admin user to get to any URL that is not already blocked by one of the Deny URL rules higher in the list. Those rules are the SurfControl and LinkWall rules.

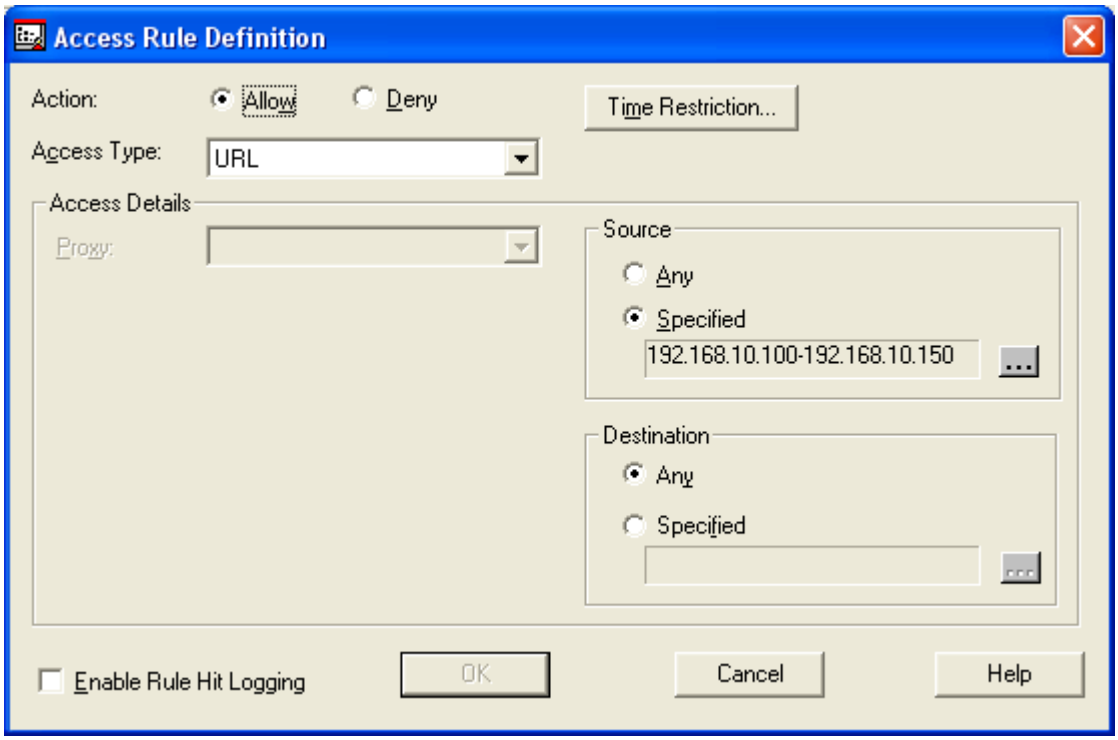


Admin.dd is higher in the NDS tree than the Deny rule for file extensions, so Admin is able to download those files.

This rule allows Admin to get to sites that are blocked by the following rule.

Allow Specific Hosts Access to Any URL Not Already Denied

Like the earlier rule that applied to test servers that needed to browse without proxy authentication, this rule is also designed to work in a situation where selective proxy authentication is being used. Refer to the section later in this chapter that covers this situation in detail, with a simpler set of access rules.

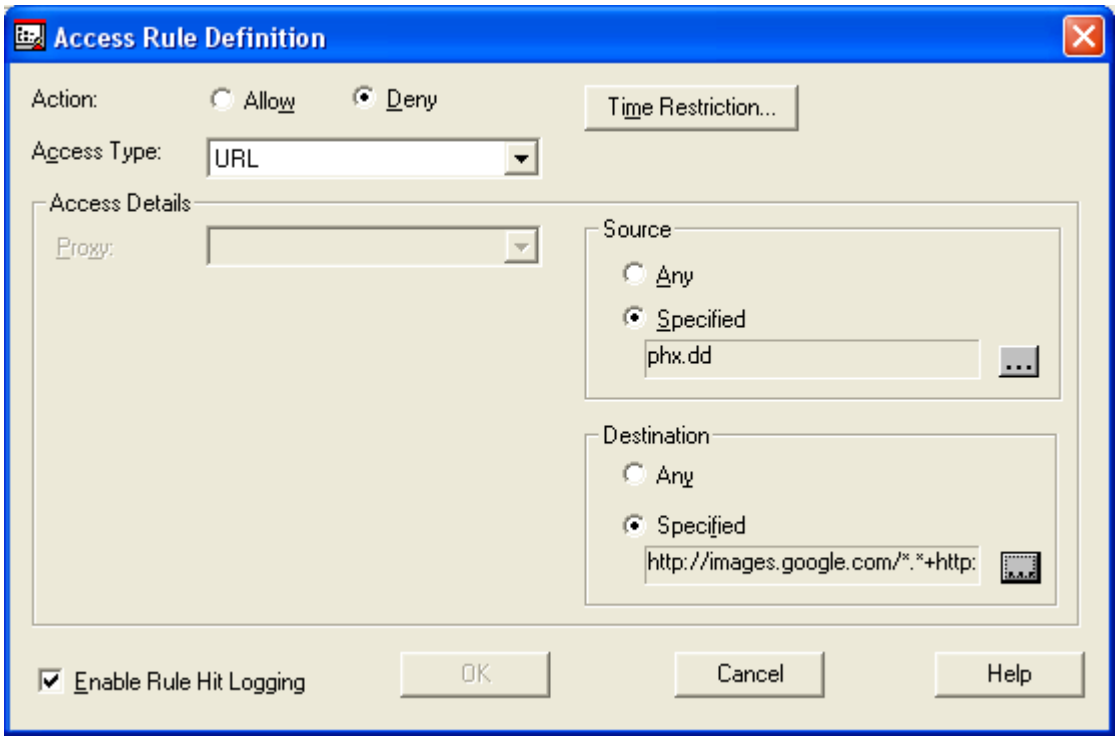


This access rule allows a range of IP addresses to browse, but not until after the SurfControl and LinkWall deny rules have been checked.

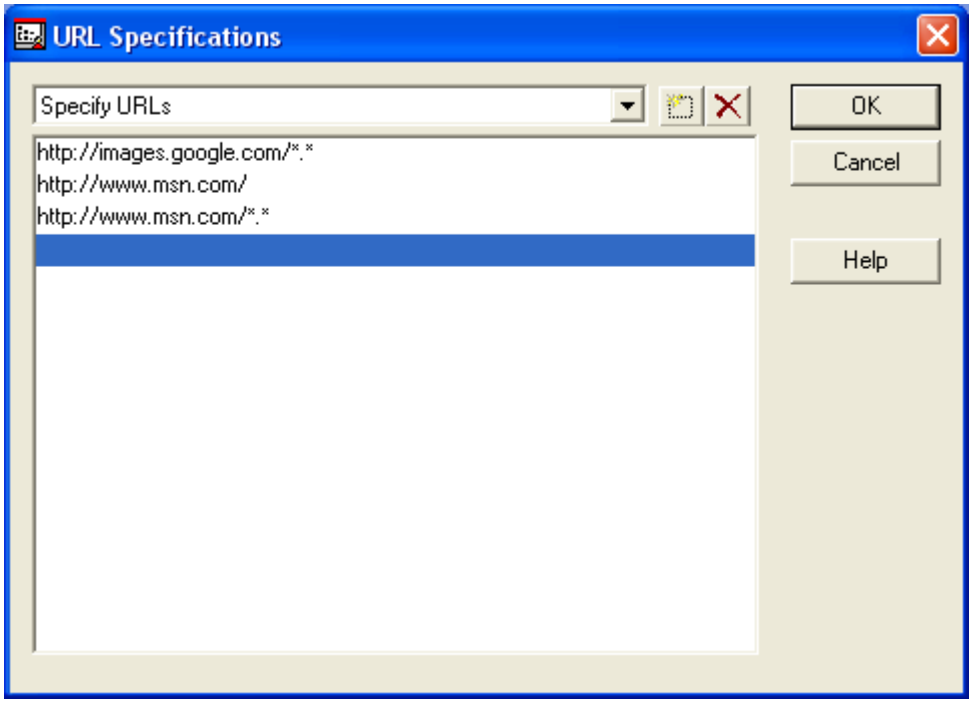
This rule only makes sense in a configuration where you do not want the hosts in the selected IP addresses to have to use proxy authentication. Otherwise, an Allow URL rule specifying the top of the NDS tree as the source would be used.

Selectively Deny Access to Certain Web Sites

This rule denies the users under one NDS container access to a couple of web sites, in this case WWW.MSN.COM and IMAGES.GOOGLE.COM.



The purpose of this example is to show a typical way that you might have to block some web sites, using two entries and wildcards.



Notice that the second line blocks www.msn.com, while the next line blocks www.msn.com/*.*.

(This web site is used as an example only – it might not require this technique to block it).

Some web sites use some form of redirection when you access the site, and you may find that you are not blocking all of the site with a simple www.name.com/*.* rule. You may have to have one entry without wildcards, and one with wildcards for the rule to work.

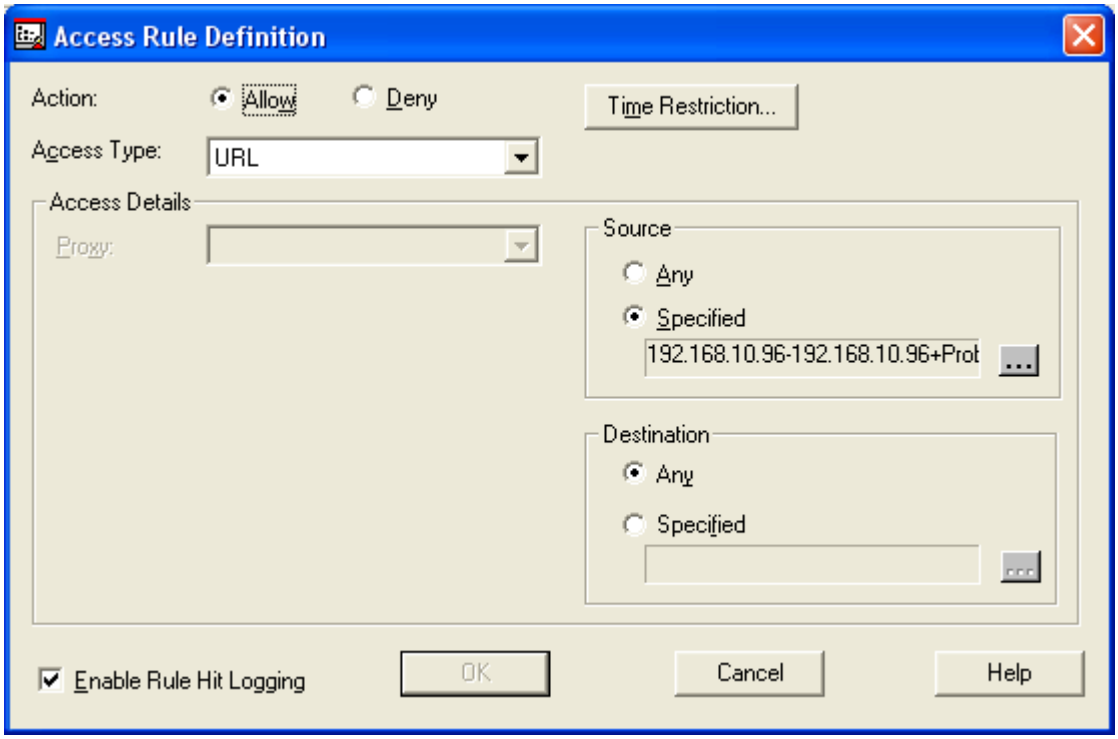
The first line is designed to block a web site that SurfControl typically does not block.

Go to www.google.com. You will see a link to Images. If you put in a search term of Pamela Anderson, and click on Images, you will probably understand why many school sites want to block this URL.

Track Specific Users with an Allow URL Rule

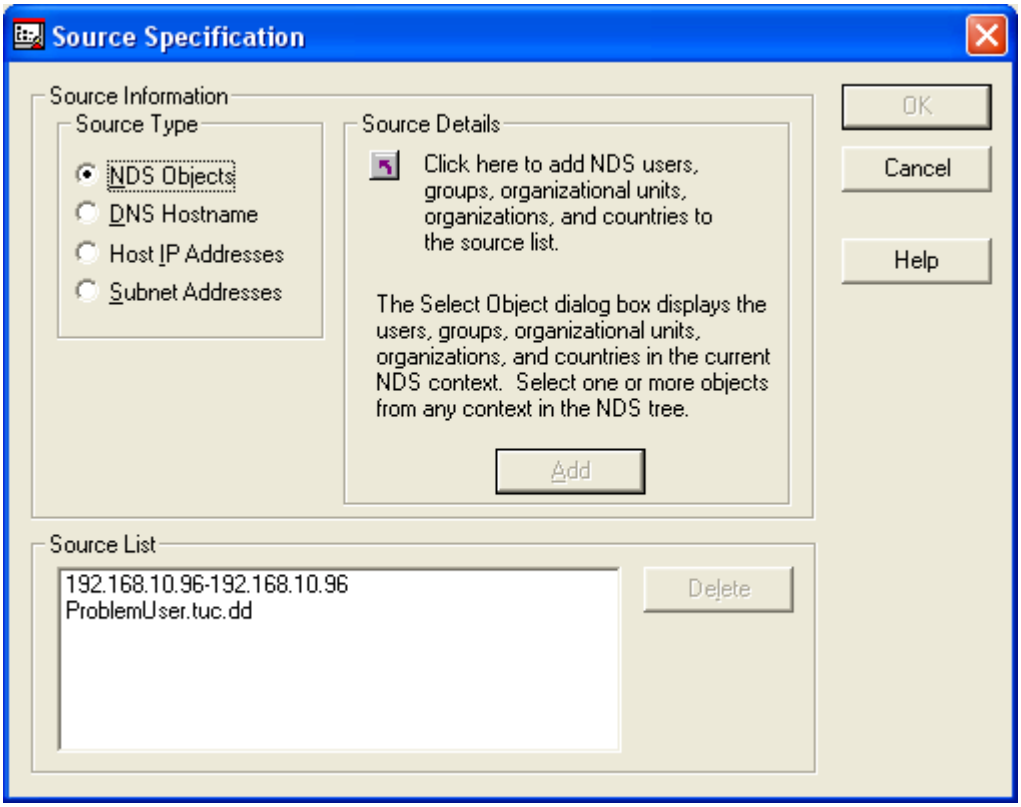
A rule such as this can be put into place strictly to allow Access Control Logging of a specific IP address, and a specific user, in order to easily see what sites are being accessed by that user.

If using proxy authentication, only the user ID is required as a source. If not using Proxy Authentication, the user can only be tracked by setting a source equal to the user PC's usual IP address. Obviously, short DHCP lease times can create a problem with an IP-base rule, but most DHCP assignments tend to remain with the same PC for long periods of time if the PC is not powered down for too long.



The specific NDS object and IP address being tracked is shown below.

Note that **Enable Rule Hit Logging** is checked, which is the only point of having this rule.



More explanation of the functionality of this rule is needed here.

The purpose of the rule is to try to find out what a particular user or PC is doing in terms of browsing the Internet. For this particular rule, logging has been enabled, even though the rule is allowing access. In the other rules shown, logging has not been enabled for Allow URL rules.

Access Control rule logging puts data into a Btrieve file in the SYS:\SYSTEM/CSLIB directory, and is difficult to control in terms of how much data is stored and when the data is rolled over. For these reasons, the author prefers not to log too much data with Access Control logging. For browsing via the HTTP Proxy, the common log files, which can be placed on a volume other than SYS, are generally sufficient to see what sites are being accessed.

Note See Novell TID 2938132, "Managing the proxy cache log files" for a method of controlling the size of the log files. Or see Novell TID 10013835, "How to Manage the BorderManager Proxy Cache", which is basically the same TID.

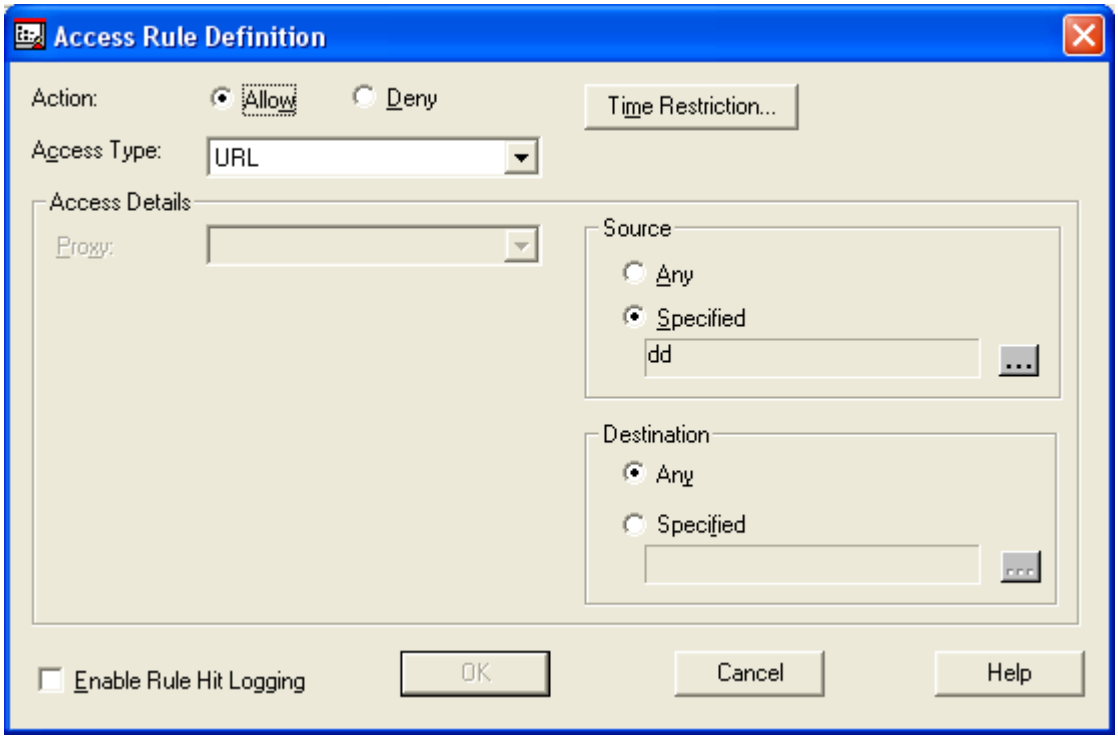
In this case, it is desired to see where a particular user has been browsing, perhaps simply to see what time of day the user is browsing the Internet. The Deny URL rules for SurfControl and

LinkWall are already logging denials for any user, but no rule would track where the ProblemUser ID has been. Therefore, a special access rule allowing this user to browse, placed after any denial rules in the rules list, is needed to keep track of the user's activities. Note also that this rule has to be placed higher in the rules list that any other rule which allows the user to browse, or logging may not be done for the user. (Depends on if logging is already being done on an Allow URL rule that applies to the user).

This sort of rule is typically put into effect temporarily, and removed when no longer needed. It has a high degree of correlation with people getting disciplined or fired. It is not a good idea to do something like this without the express approval of the Human Resources department at large corporations, as it might lead to accusations of discrimination and lawsuits.

Allow Authenticated Users to Any URL

Up until now, the rules have been denying many sites, or selectively allowing a few for all users. This rule allows anyone in the .DD container and below to browse all web sites not blocked by a rule higher in the NDS tree.

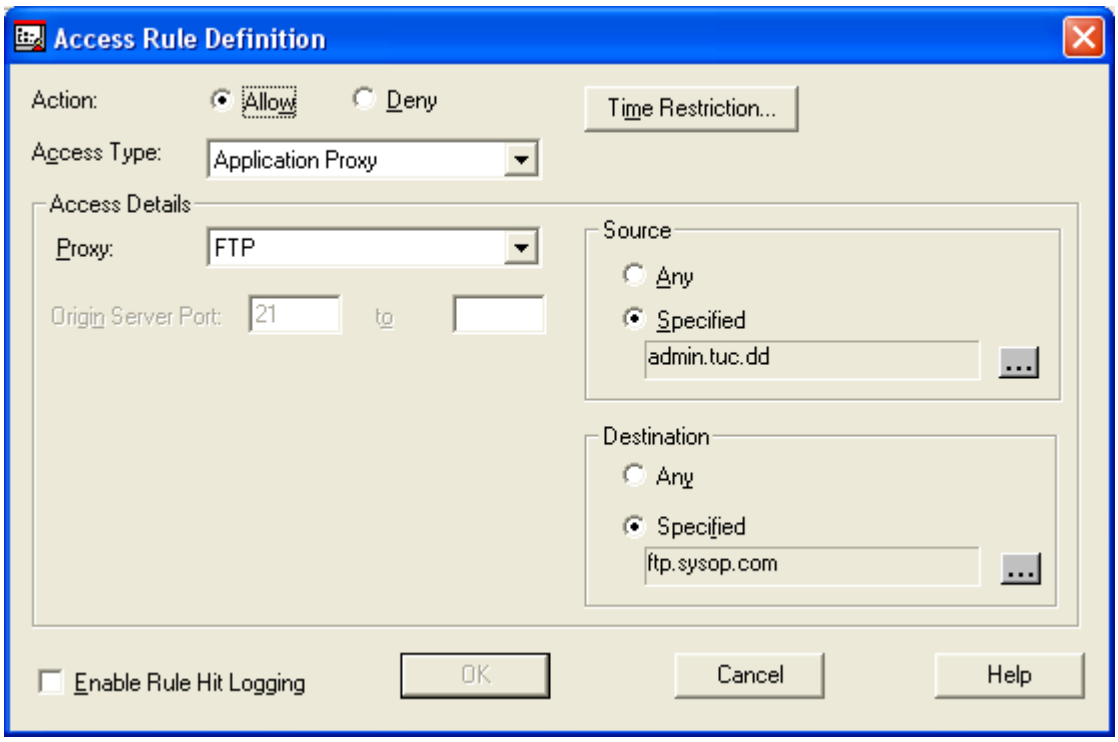


As long as a user is proxy-authenticated, he/she should be able to browse through the HTTP Proxy, unless trying to get to a blocked file extension, denied SurfControl category, or a LinkWall listed site.

Allow Admin User to FTP Accelerator (FTP Reverse Proxy)

This rule has to be placed above the rule shown next, which denies all users to the same site. The Admin.tuc.dd user will be able to access the FTP site, while all others will be blocked. There is another rule following the Deny rule, which then allows all users to access the FTP Proxy for all other sites. The three FTP Proxy rules work together.

This series of three FTP Proxy rules is a good example of how you have to structure and sequence rules to allow selected access to desired sites.

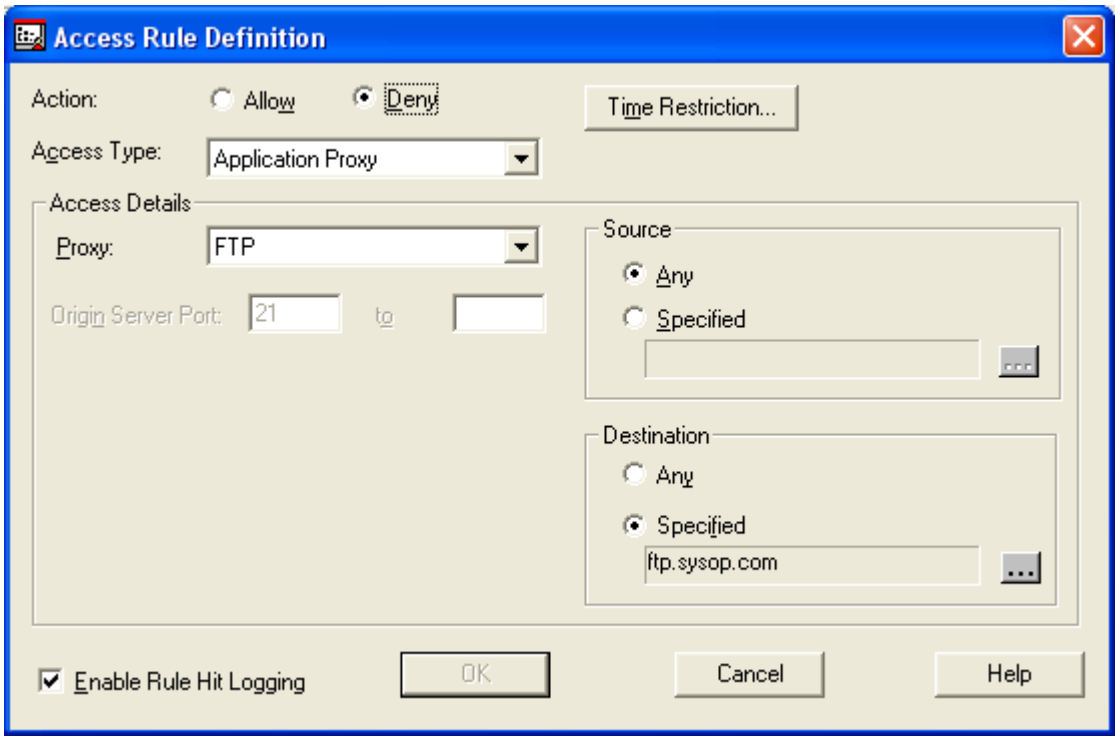


The only user allowed to access the specific site ftp.yourdomain.com is **Admin.tuc.dd**. The point of this rule is to control inbound access through FTP Acceleration.

Review the chapter on Acceleration to see how the FTP accelerator is configured. (??check FTP accelerator example)

Deny All Users Access To FTP Reverse Proxy

This rule works in conjunction with the previous rule. While the previous rule allows Admin.DD to access the FTP site through an FTP accelerator, this rule blocks everyone else.

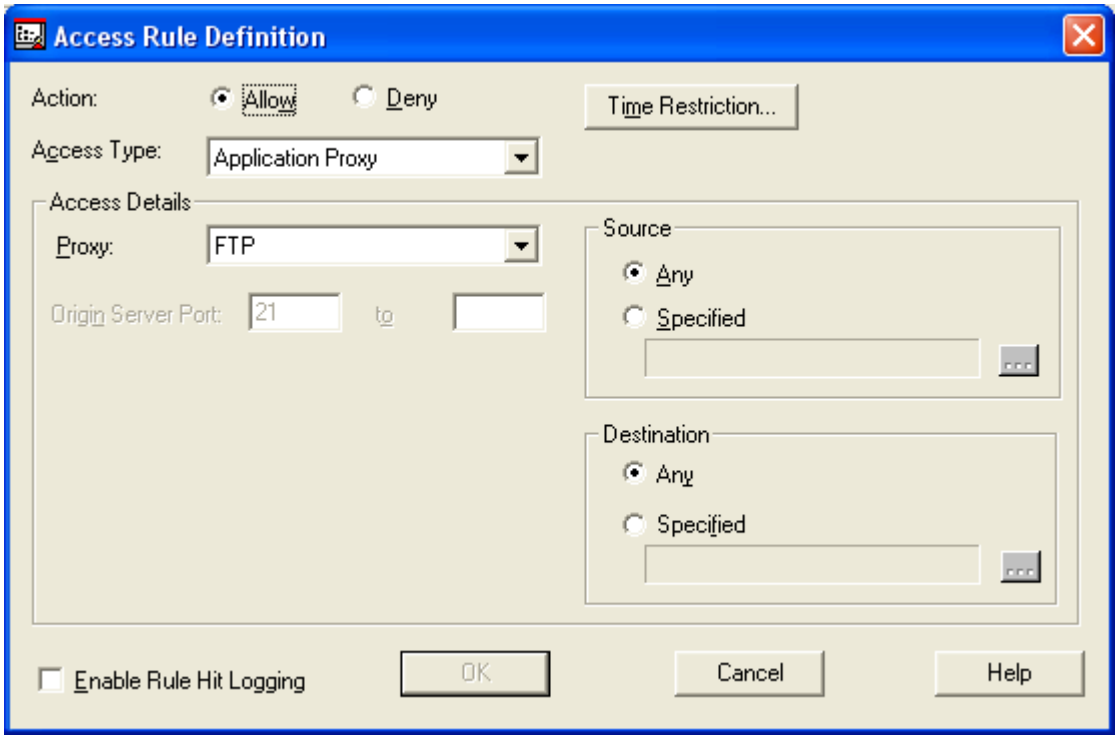


As long as this rule is placed below the rule allowing Admin.tuc.dd to access the same site, it will block everyone except that user.

Allow All Users Use of the FTP Proxy

Note FTP Proxy applies only to FTP clients. Browsing to FTP sites through the HTTP Proxy can be done using a browser if access rules have been set up to allow Any URL. If Access Rules are instead set up to allow ports 80 and 443, then FTP browsing should be blocked, but browsing to non-standard linked references will also be blocked.

The FTP Proxy, along with the HTTP, Transparent HTTP and Transparent TELNET proxies, is designed to be able to make use of NDS-based sources in an access rule. However, if you wish to use the FTP Proxy with a source rule based on a user, group or container, you must also use a particular syntax to pass your NDS user ID and password to the FTP Proxy as part of the FTP login process. The rather complex syntax is explained in the FTP Proxy chapter.



The example shown above allows any internal user to make use of the FTP Proxy.

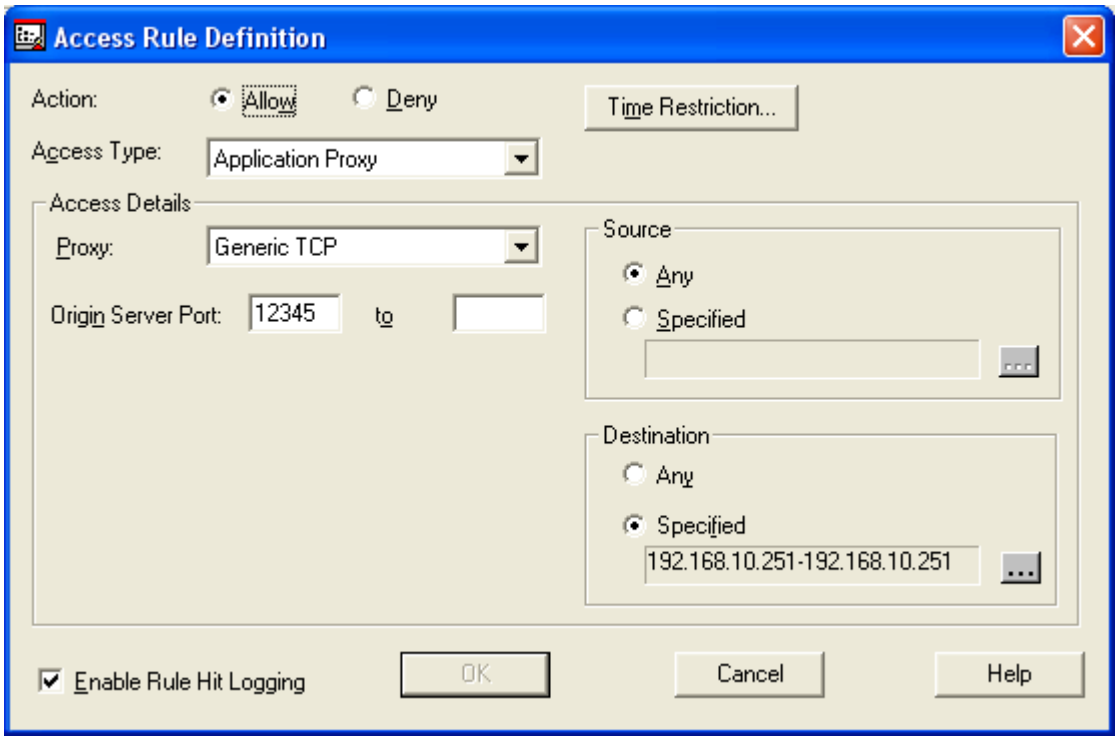
You may need to add an allow rule for ports 20 and 21 to allow **browsers** to access FTP servers through the HTTP Proxy.

This rule is intended to allow outbound access through the FTP Proxy, but needs to be placed underneath the previous rule denying access to FTP.SYSOP.COM, or any user on the Internet would be able to access that web site through the FTP accelerator.

Allow Generic Proxy Access to Web Manager

NetWare 5.x servers running Novonyx web servers use a Web Manager service that allows you configure your web server

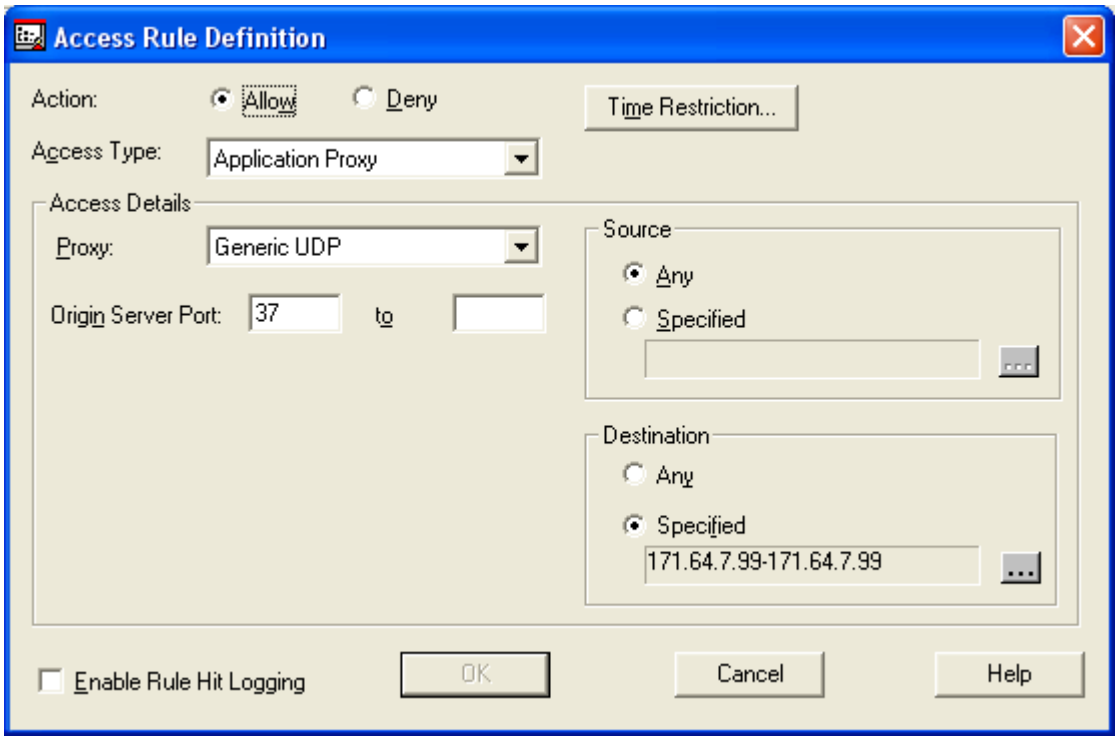
While the Web Manager information is delivered in a browser format, it is NOT using HTTP protocols, per se, and will not work though HTTP acceleration (reverse HTTP proxy). However, it will work fine through a Generic TCP Proxy set to proxy the defined port number for the Web Manager.



A user accessing the public IP address of the Generic TCP Proxy as defined earlier in the book (see the chapter Generic TCP Proxy), will be proxied through to internal IP address 192.168.10.250 on port 12345. Web Manager will then ask for a user ID and password.

Allow Access To Generic UDP Proxy for Port 37 (RDATE)

This rule allows access to the Generic UDP proxy set up for RDATE time services. If you have an internal NetWare time reference server using RDATE.NLM to set the time to an Internet time server, you can use a generic proxy like this to allow outbound access to a time server.



Note RDATE.NLM is available for free from http://www.murkworks.com.

The destination allowed for this generic proxy is set to **171.64.7.77**, a time server in Stanford University, California.

This proxy would be used by setting a server running RDATE on an internal NetWare server to point to the BORDER1 private IP address (192.168.10.252). BORDER1 will see UDP port 37 traffic addressed to its IP address, and it will automatically forward that traffic to the configured destination IP address, as well as return traffic from that destination.

Note One syntax for using RDATE on an internal NetWare server might be: **LOAD RDATE /u /p 60 /v 2 /m 999999999 192.168.10.254**

No time restrictions have been set up for this rule.

Inbound pcANYWHERE Access Rules Using Generic Proxies

It is possible to use generic proxies for traffic coming into the network as well as traffic going out of the network. One example is to use a pair of generic proxies (one UDP and one TCP) to provide access to a pcANYWHERE host on the internal LAN.

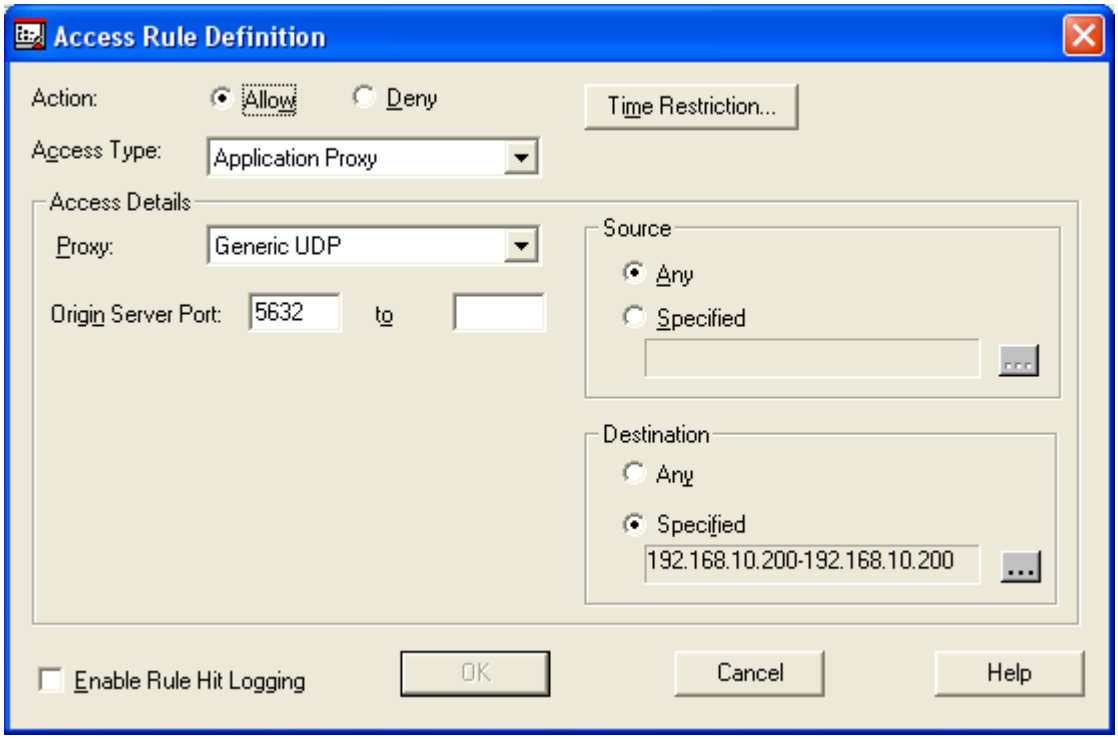
Note This example will only allow a single internal host to be set up for access from the Internet. If additional internal hosts are desired to be accessed from the Internet, static NAT using packet filter exceptions and secondary public IP addresses would be one comparatively easy way to accomplish the task. Using multiple generic proxies with secondary IP addresses can quickly get very complicated because of issue of needing to have a unique IP address/port number combination on the private interface.

The pcANYWHERE program (versions 8 and 9, at least), locates hosts using UDP port 5632. If a host does not respond on port 5632, UDP port 22 is also tried, because early versions of pcANYWHERE used UDP port 22. You normally do not need to worry about supporting port 22, but if you have very old pcANYWHERE versions in use, you may want to add another Generic UDP proxy for port 22.

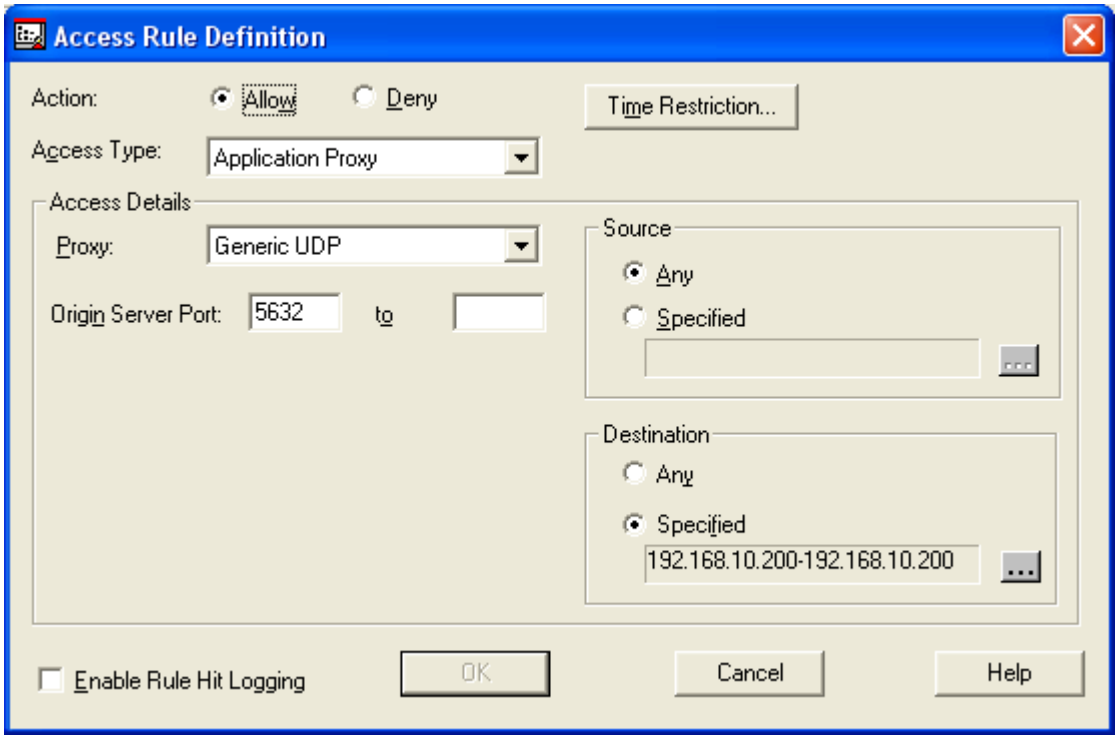
Once pcANYWHERE locates a suitable host using UDP, it switches to TCP port 5631 to transfer data. Therefore, both a Generic UDP and a Generic TCP proxy need to be configured.

If dynamic NAT is in use on the BorderManager server, inbound traffic will not be able to access this proxy (or a reverse proxy) unless NAT Implicit Filtering has been disabled, or if SET NAT DYNAMIC MODE TO PASS THRU=ON has been set (manually, or in AUTOEXEC.NCF).

If generic proxies (or any proxy) are to be used with secondary public IP addresses, you must also configure packet filter exceptions as needed to allow both the source and destination traffic for the secondary IP address. This is explained in more detail in my book "Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions", available at http://www.craigjconsulting.com



This example shows the Generic UDP proxy set up to listen for port 5632 traffic on the main public IP address (4.3.2.254) and pass that traffic to destination IP address 192.168.10.200.

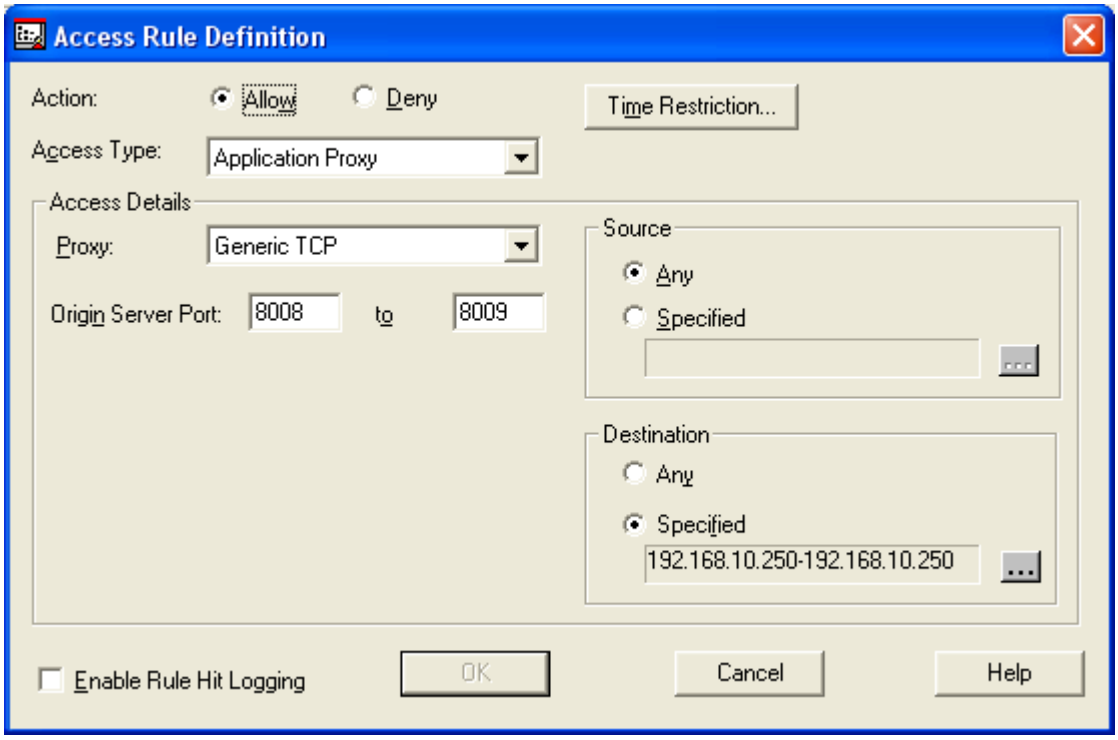


This example shows the Generic TCP proxy set up to listen for port 5631 traffic on the main public IP address (4.3.2.254) and pass that traffic to destination IP address 192.168.10.200.

These two generic proxies work in concert, and allow inbound pcANYWHERE traffic, but not outbound pcANYWHERE traffic. Generally speaking, adding stateful packet filter exceptions for UDP destination port 5632 and TCP destination port 5631 are more flexible for allowing outbound pcANYWHERE access to any pcANYWHERE host listening on the Internet.

Inbound Generic Proxy Access To Novell Remote Manager

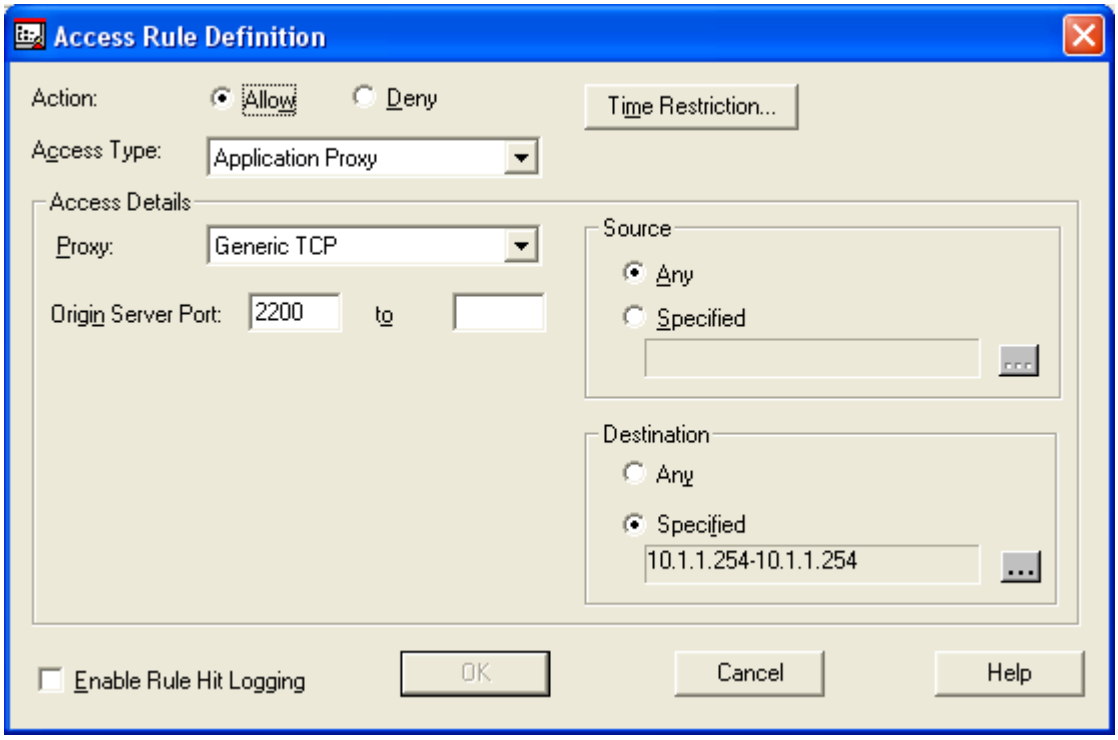
This rule allows access to the Generic TCP proxy configured for Novell Remote Manager ports 8008 and 8009 to function.



The port numbers are restricted to 8008 through 8009, and the destination IP address is the address of the internal server to which the generic TCP proxy maps.

Inbound Generic Proxy Access To iManager

This rule allows access to the Generic TCP proxy configured for iManager port 2200 to function.

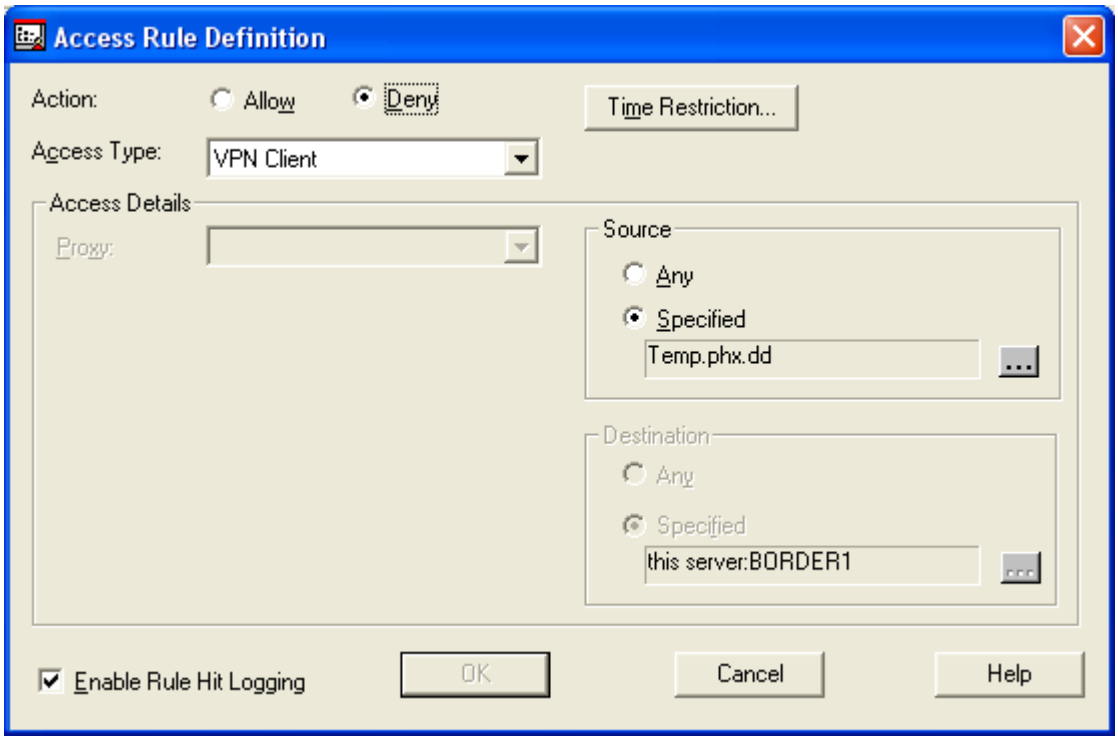


The port number is restricted to 2200, and the destination IP address is the address of the internal server to which the generic TCP proxy maps.

Deny Legacy VPN Client Access to the BORDER1 Server

This rule denies a particular user access to legacy Client-to-Site VPN. Legacy VPN is any VPN prior to BorderManager 3.8.

It is needed if this user is to be denied, because a following rule allows VPN access for all users in this user's NDS container.

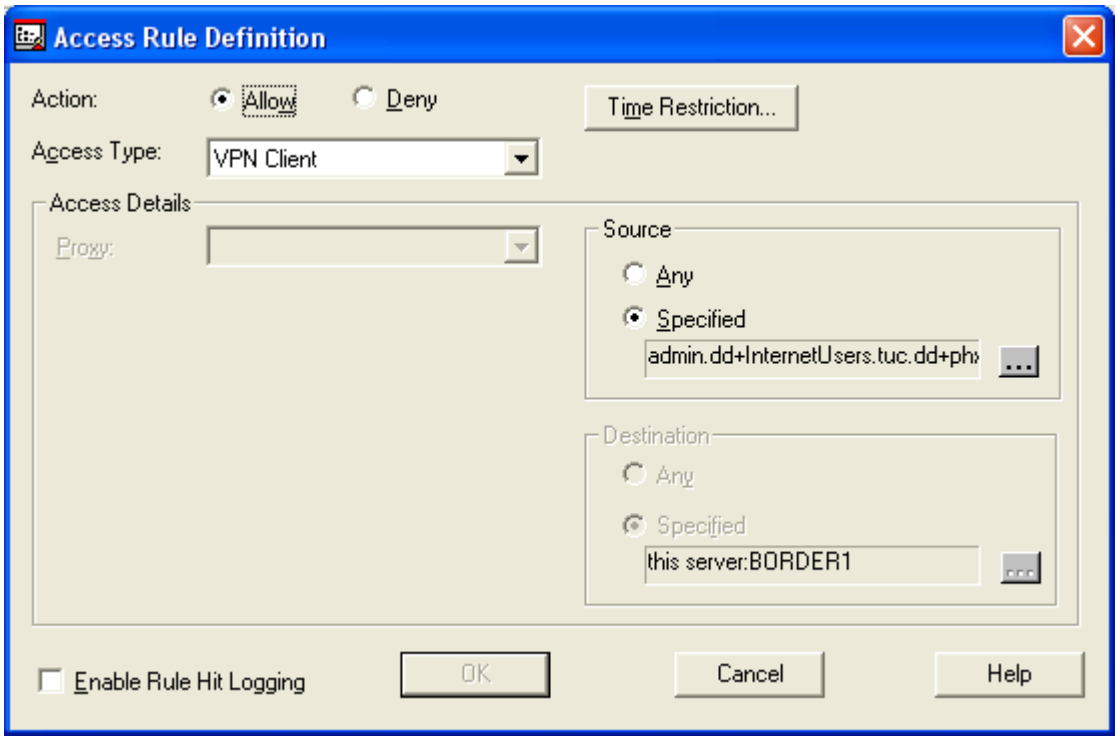


The particular user ID being denied is **TEMP.PHX.DD**.

Allow Legacy VPN Client Access to the BORDER1 Server

Note the previous Deny VPN Client rule, which applies to a user within an NDS container that is allowed by this rule.

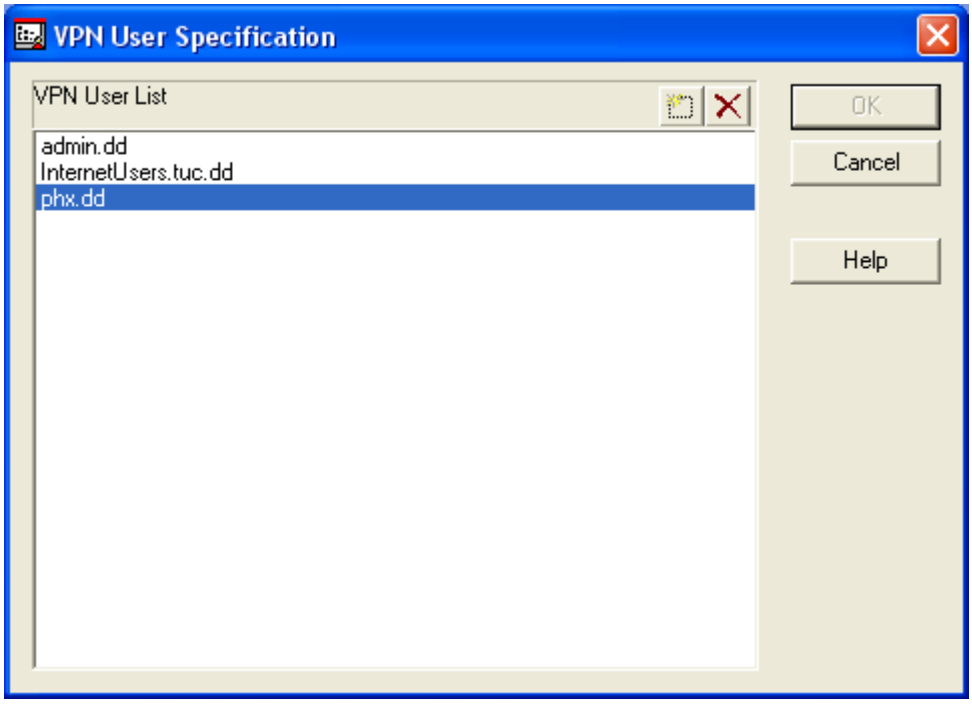
Because that Deny rule is higher in the Access Rules list than this Allow VPN Client rule, this rule is overridden for that one user.



This rule allows VPN Client-to-Site access to the BORDER1 server for the designated users, groups or containers.

Logging has been enabled so that VPN client access connections can be audited.

Note You should realize that this rule only controls access to the VPN connection itself, not to internal resources once the VPN connection is established. You cannot allow a user to connect to the VPN, and then deny that user access to certain servers by using BorderManager Access Rules. Once the user is authenticated to the VPN, his/her PC becomes a remote node on the network, as if it were physically plugged into the local LAN.

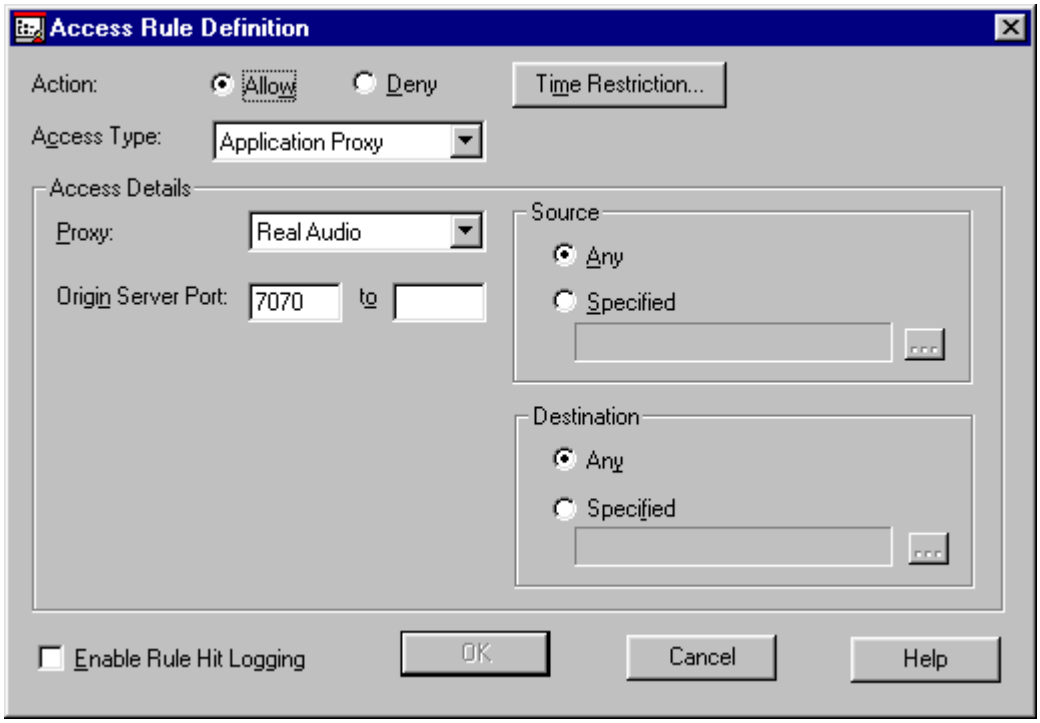


These are the NDS user ID's authorized to access VPN services:

ADMIN.DD, members of the **INTERNETUSERS.TUC.DD** group, and all members of the **PHX.DD container** are authorized to make Client-to-Site VPN connections to the BORDER1 server.

Allow Access to RealAudio Proxy (BorderManager 3.0)

This rule allows any host to use the RealAudio Proxy.

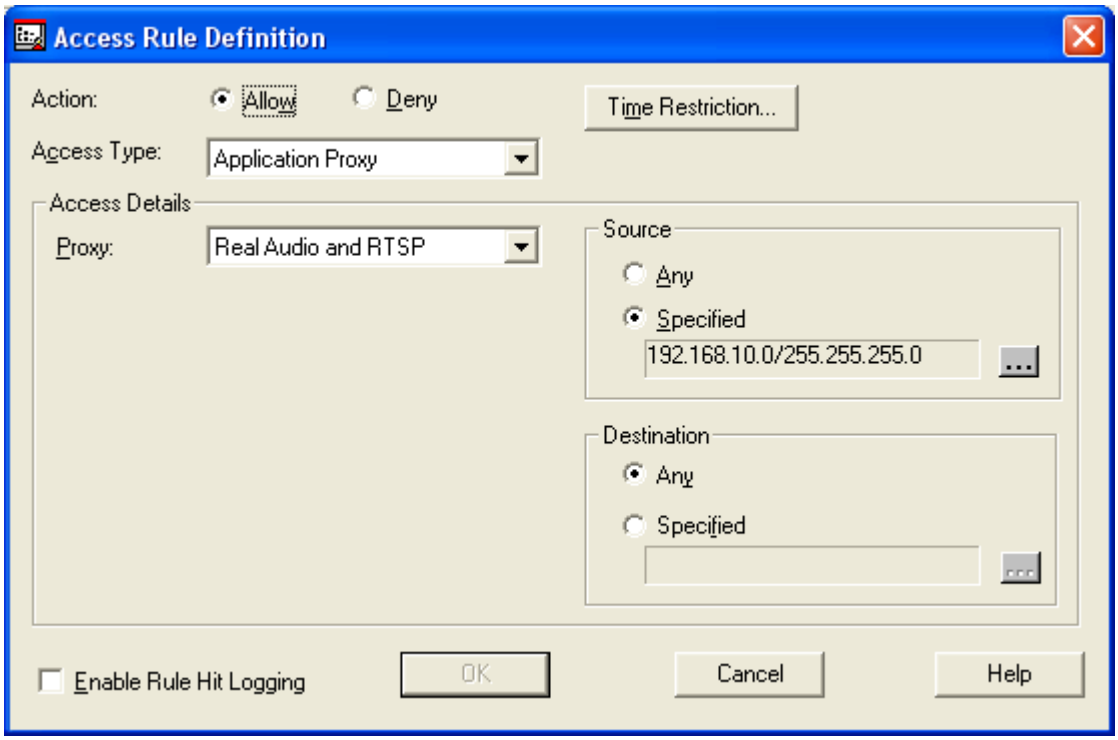


This rule shows what a BorderManager 3.0 server has available.

The RTSP proxy is not available for BorderManager 3.0.

Allow Access to RealAudio Proxy (BorderManager 3.5 and later)

This rule allows any host to use the RealAudio and RTSP Proxy.



This rule shows what a BorderManager 3.5 or later server has available.

The RTSP proxy also shows up with the RealAudio Proxy.

Notice that the 192.168.10.0 subnet has been configured as a **Specified Source**. The idea here is to prevent possible relay from the public side of the proxy, by at least calling out the internal subnet of the LAN, instead of Any.

Spam relay and HTTP relay have been done from BorderManager Transparent and Mail Proxies in the past. It is always a good idea to limit the source of your proxy usage to internal users or addresses.

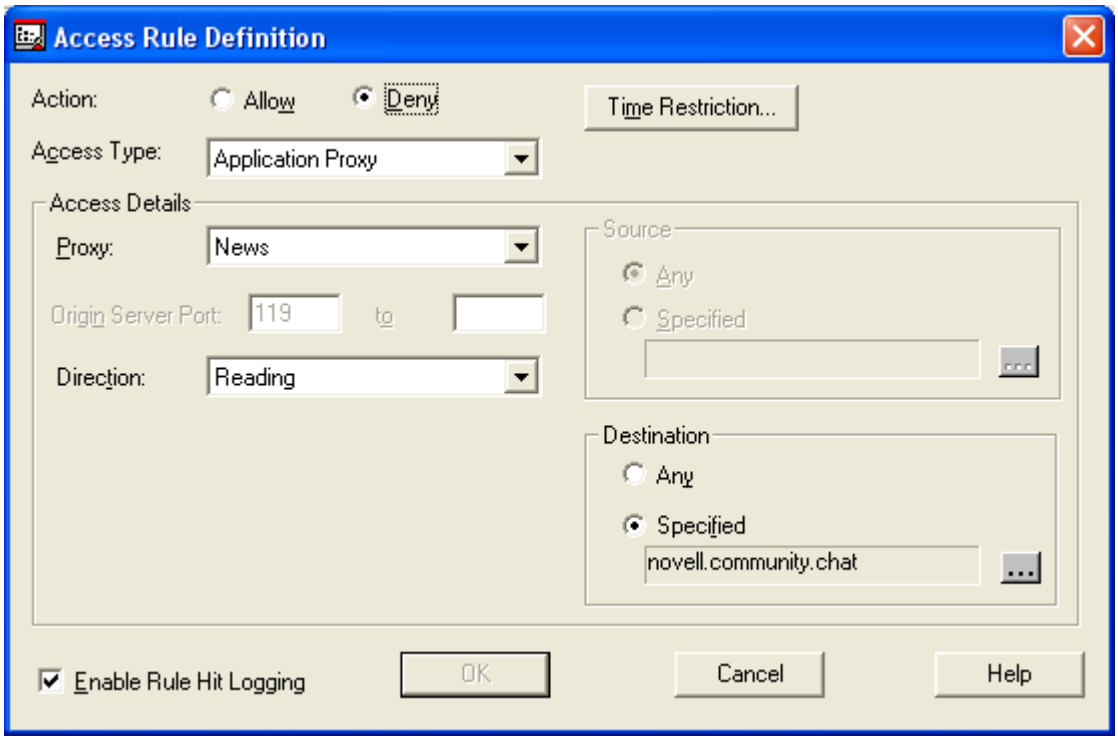
Access Rules Controlling News Proxy

There are two possible types of Access Rules related to the News Proxy. One is used to allow Reading, which is essentially used to allow outbound traffic. The other type of rule is used for inbound traffic, to allow NNTP inbound to an internal NNTP server.

The follow set of four access rules should make it clear how to selectively block certain newsgroups from a Usenet server.

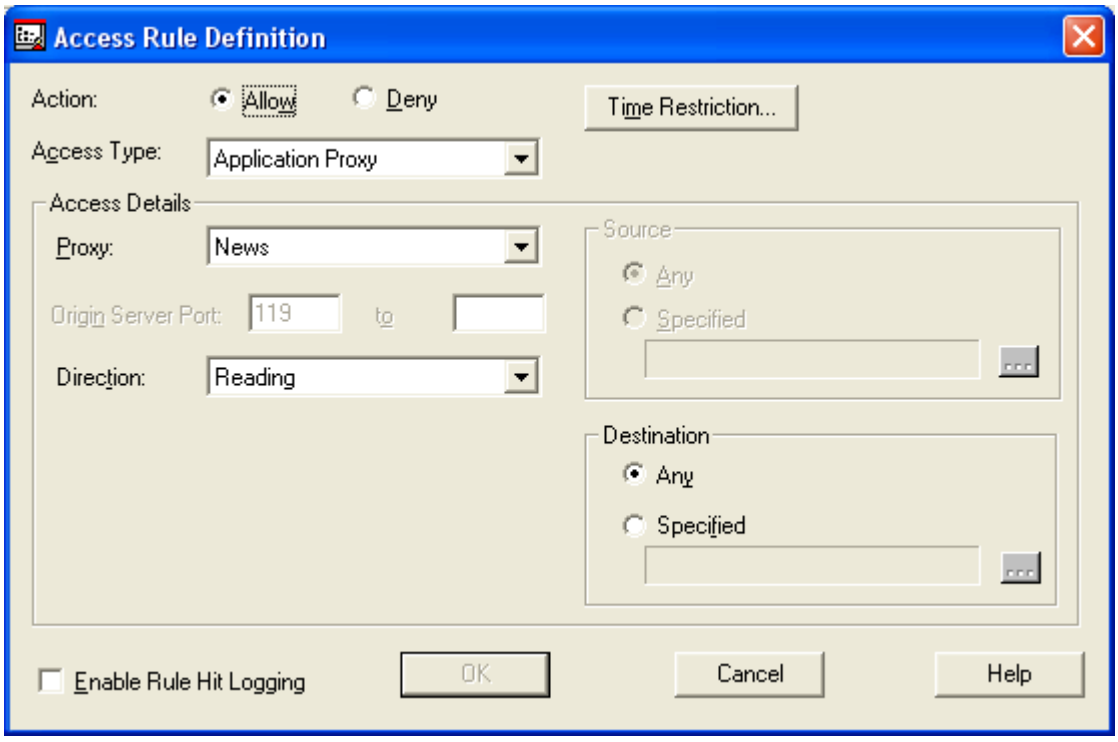
The objective is to allow the users on the LAN to access the Novell public forums through the News Proxy, except for the Novell Community Chat forum.

Deny a Specific Newsgroup for Reading



This rule denies the newsgroup novell.community.chat from being read when using the News Proxy.

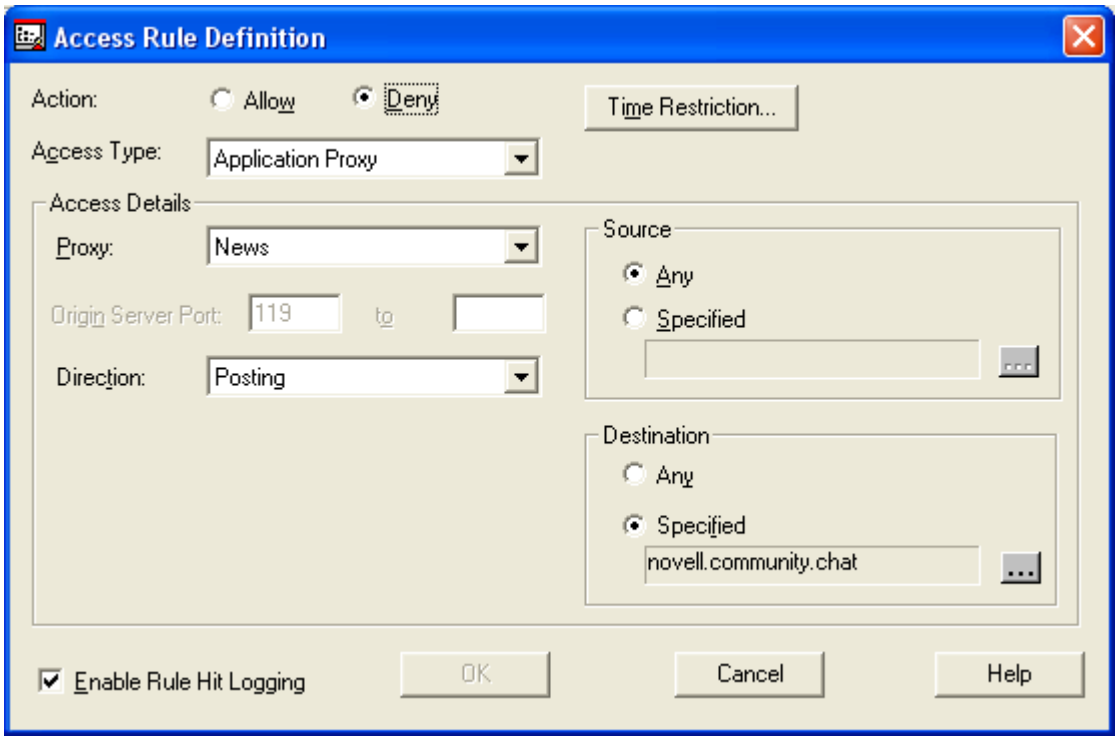
Allow All Newsgroups to be Read



This access rule allows internal users to read any newsgroups not previously denied by another rule, when using the News Proxy. Since the previous rule denied novell.community.chat, this rule allows all other newsgroups hosted at support-forums.novell.com to be read.

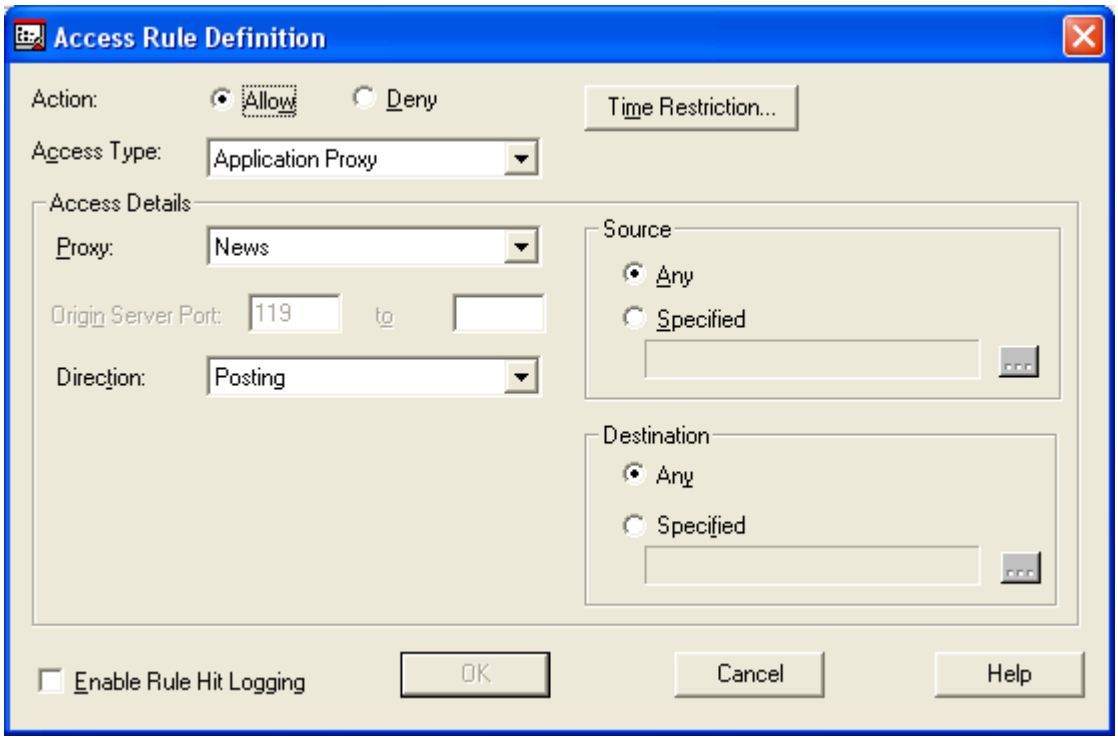
The News Proxy is configured to point to support-forums.novell.com.

Deny Posting to a Specific Newsgroup



This rule denies anyone from posting to the novell.community.chat newsgroup when using News Proxy.

Allowing Posting to All Newsgroups

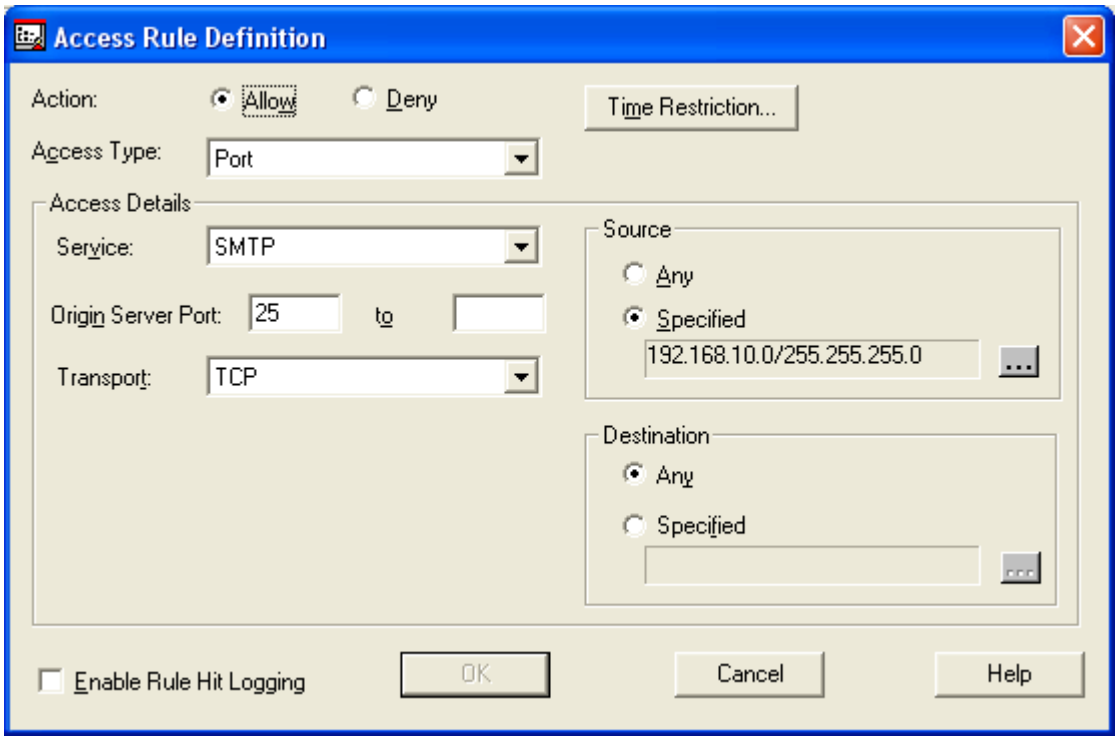


This access rule allows users to post to all newsgroups accessible through the News Proxy. Since the previous rule denied access to the novell.community.chat newsgroup, the effect of this rule is that users can post to all other newsgroups.

This book does not cover a configuration with an internal NNTP server.

Allow Outbound SMTP Through the Mail Proxy

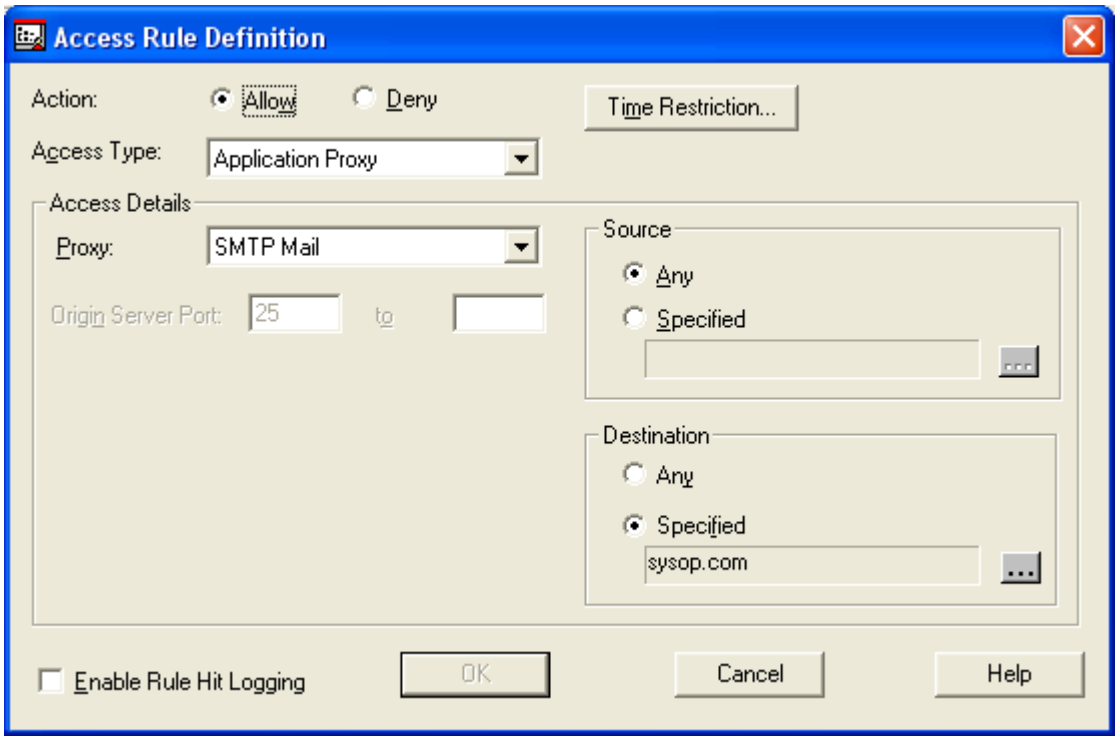
It is important to know that different patch levels of BorderManager 3.x have completely different controls for Mail Proxy. The later patches for BorderManager 3.5 and later use settings in the PROXY.CFG file to control spam relay access. BorderManager 3.8 Mail Proxy may completely ignore the access rules shown here. Still it will not hurt to put in the access rules as shown, in case they are application to your patch level.



The example shown allows any host on the 192.168.10.0 network to access the Mail Proxy to send SMTP email to any external SMTP server.

Review the section on the Mail Proxy to see how this rule and the next two rules act together to allow SMTP through the Mail Proxy while not allowing spam mail to be relayed off the BorderManager server.

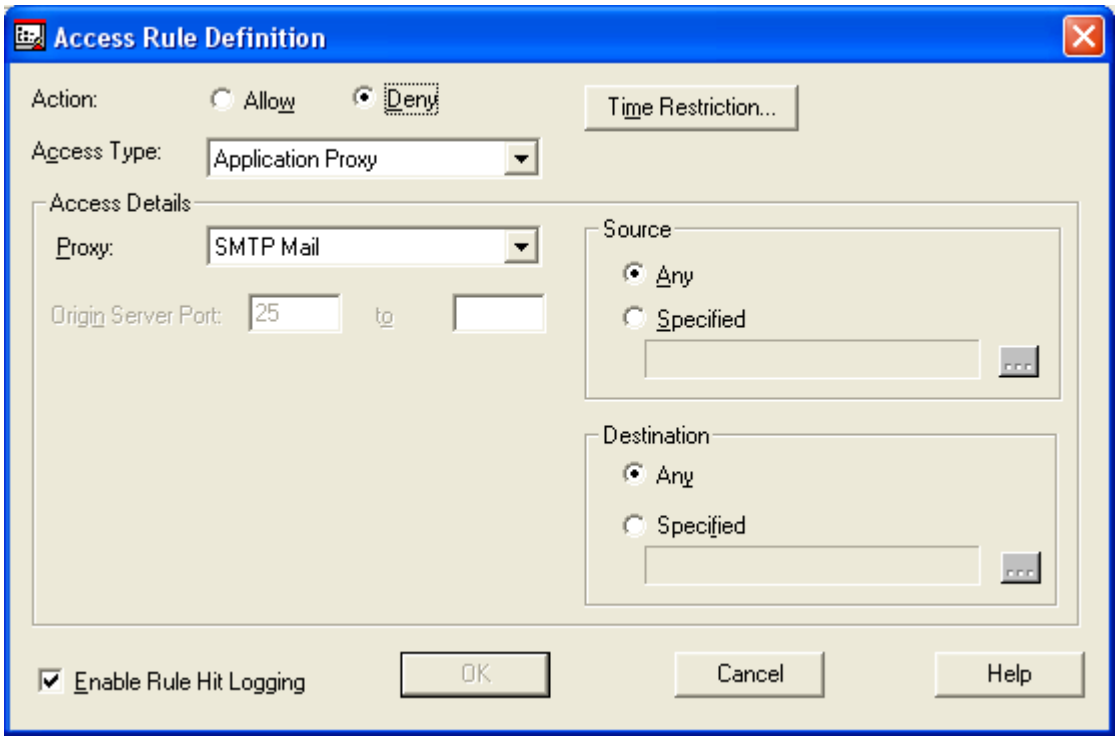
Allow Inbound SMTP Mail Through the Mail Proxy



This access rule allows SMTP mail to be delivered from Any host, but only to the SYSOP.COM domain. The previous rule allowed internal users to send SMTP mail to any domain, which effectively allows outbound SMTP. This rule effectively restricts inbound SMTP mail to only the specified domain so that Internet hosts cannot relay email off the Mail Proxy.

Review the chapter on configuring Mail Proxy for more detail on how these access rules control mail usage.

Deny All SMTP Mail Through the Mail Proxy



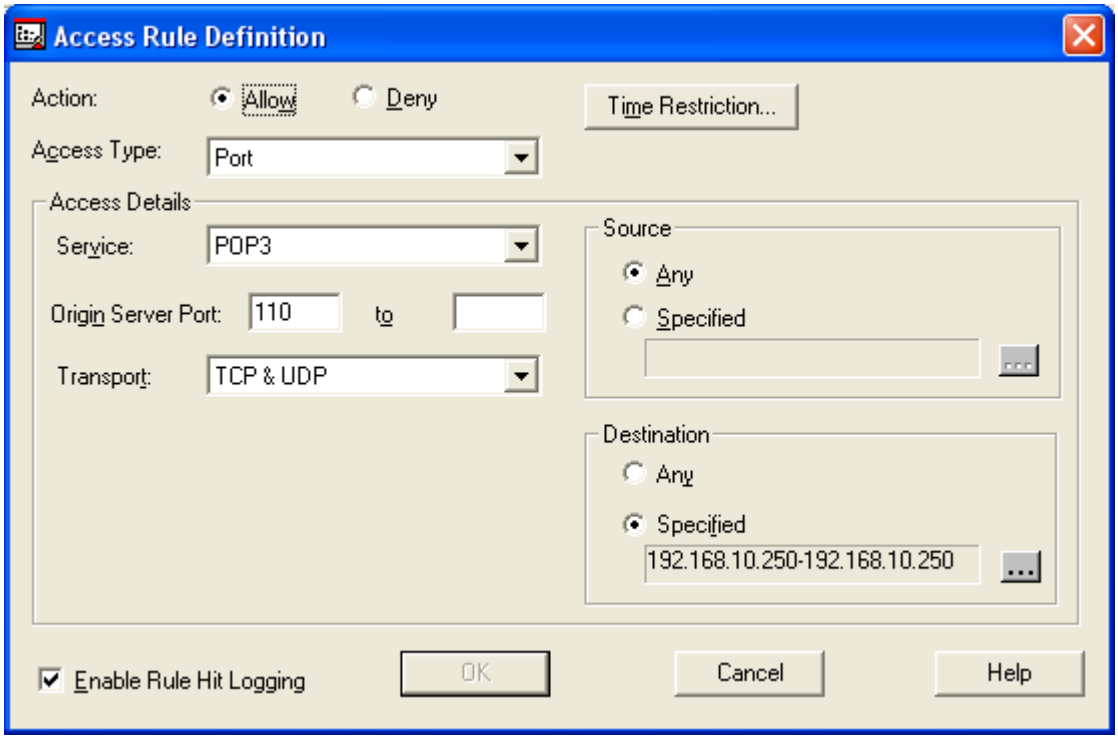
This access rule stops all SMTP mail from being sent through the Mail Proxy. The previous Mail Proxy access rules have allowed only the desired traffic.

Coupled with a rule to allow internal hosts to send SMTP anywhere, and external hosts to send SMTP only to the internal mail domain, this rule should block spam relay attempts. (A spam relay attempt is when an external host uses your Mail Proxy to send SMTP mail from to some other domain than yours. Mail Proxy was very vulnerable to this practice, when unpatched, and when the proper access rules and/or PROXY.CFG settings are not used).

Review the chapter on configuring the Mail Proxy for more explanation on how these rules control Mail Proxy usage.

Allow Inbound POP3 Through the Mail Proxy

The Mail Proxy will listen on all defined IP addresses for both SMTP and POP3 traffic. However, an access rule is required to allow even internal users to check POP3 mail through the Mail Proxy.

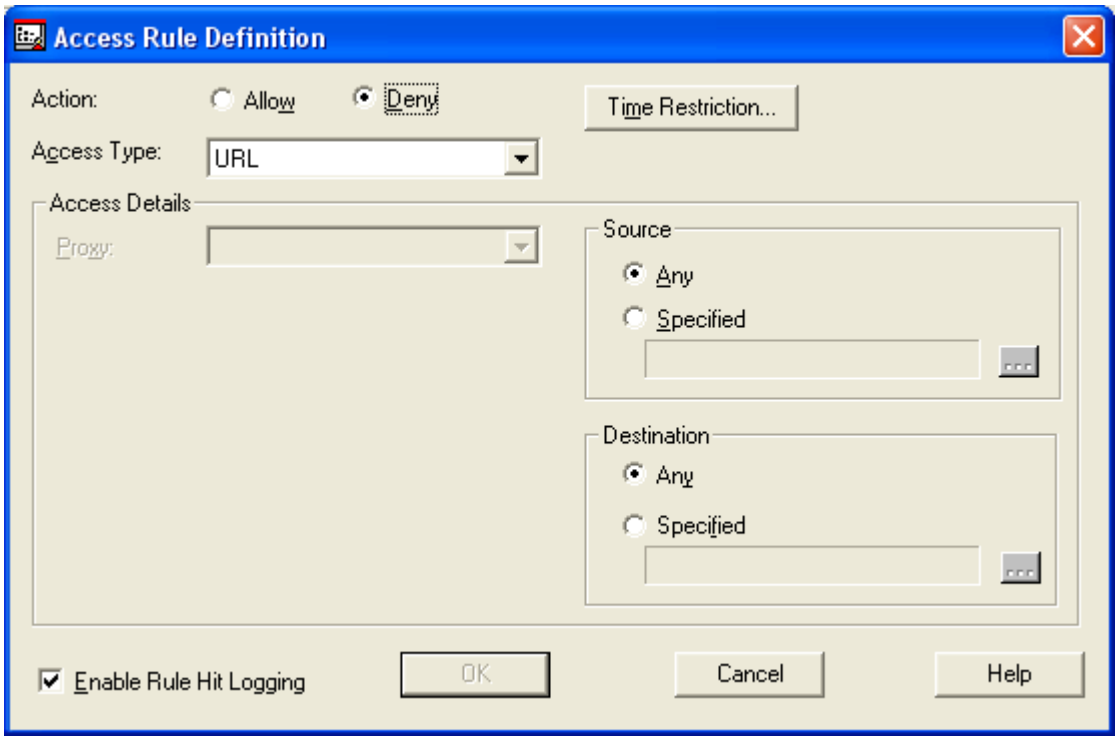


This rule allows POP3 traffic (TCP port 110) to be proxied through the Mail Proxy to an internal POP3 mail server at internal IP address 192.168.10.250.

A similar rule could be set up to allow internal users to access POP3 mail servers on the Internet by adding another rule with a source equal to the internal IP network and a destination of Any.

Deny All URLs For Troubleshooting Purposes

This rule exists only for the logging capability. The default rule (Deny All) will stop any browsing access not specifically allowed to this point, but does not log the denials.

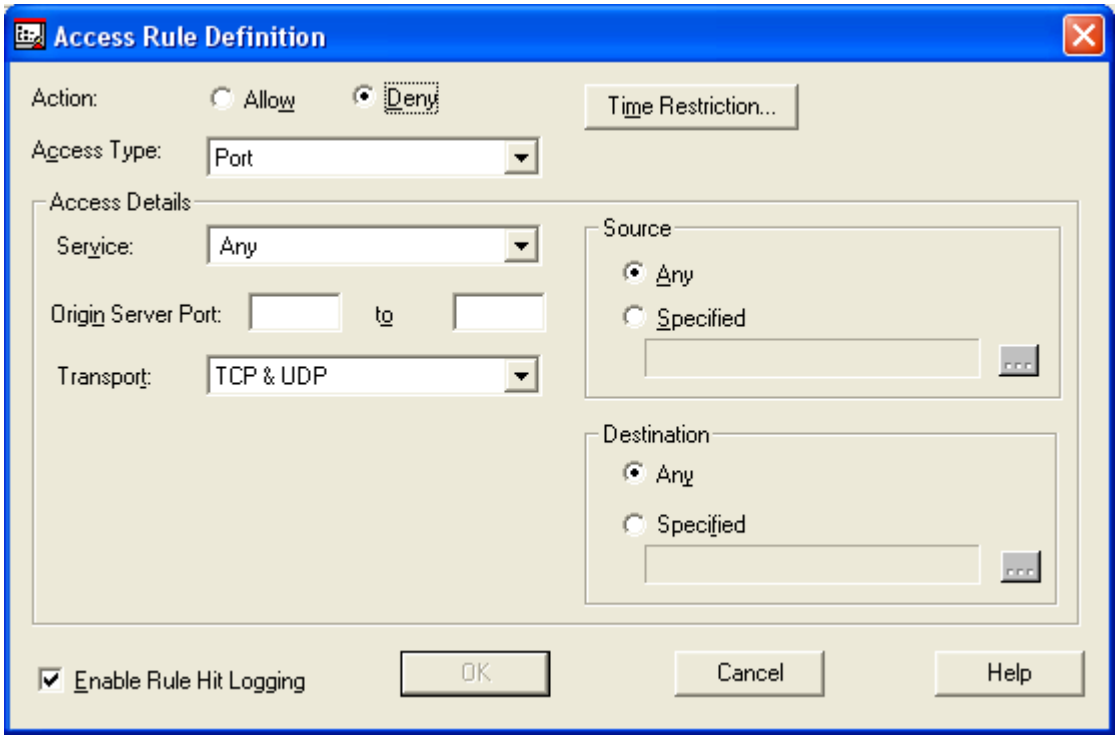


The **Rule Hit Logging** box is checked. Should a URL be denied, and you are not sure why, this rule may provide the information in the Access Control Log that helps to see what was going on.

Deny All Ports for Troubleshooting Purposes

In the same way that the last rule logs URL denials, this rule logs Port denials to the Access Control Log. It can be useful to see why some service will not function as expected.

As one possible example of the usefulness of this rule, it might show you that a Java applet is trying to make a request on a particular port number without going through the HTTP Proxy. The user would think that the browser is failing to work through the HTTP Proxy, but the Access Control log might show that user is making DNS requests or some non-standard port number requests at the same time that the user tries to browse to a particular web site.



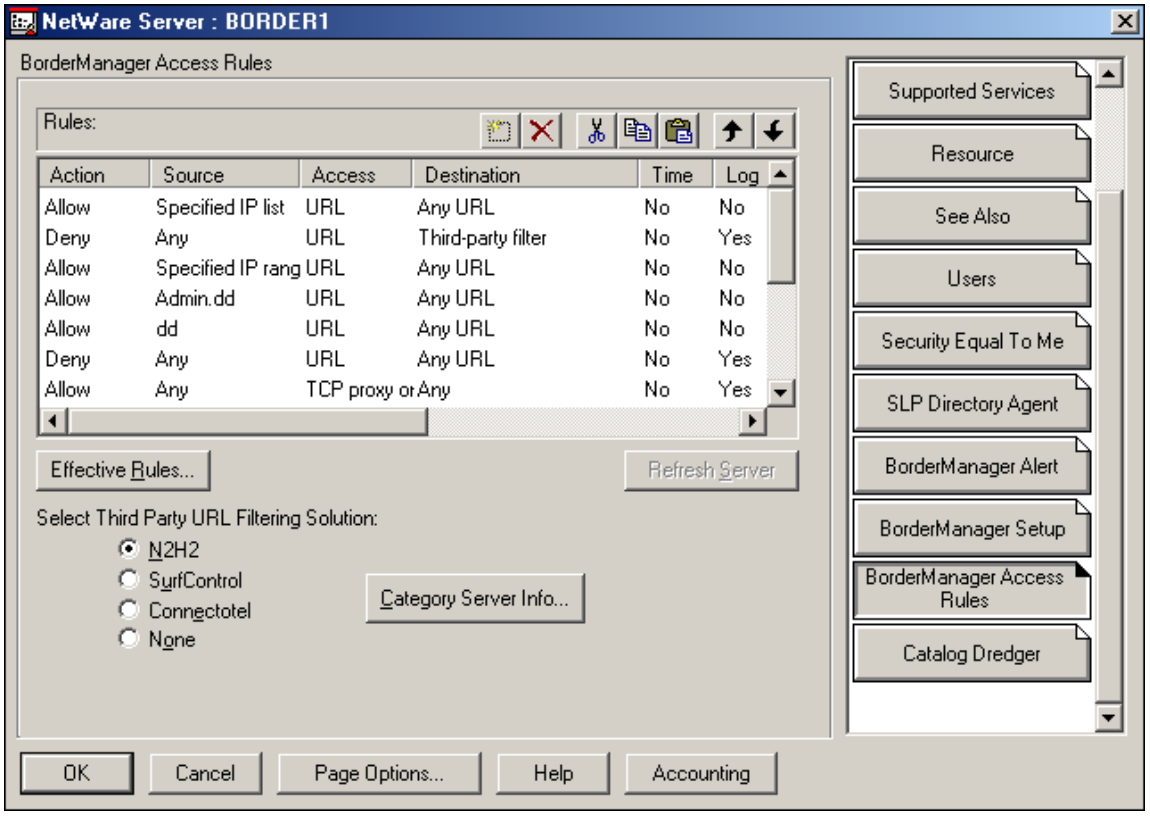
The **Rule Hit Logging** box is checked. Should a port number be denied, and you are not sure why, this rule may provide the information in the Access Control Log that helps to see what was going on.

N2H2 Access Rule Example

Please do not confuse this section with the previous section. It shows a completely different set of access rules than in the previous example. I have shown only a simplified set of rules here to try to avoid confusion. The purpose is to show a new feature available to BorderManager 3.7 after installing the BM37N2H2.EXE patch.

In this example, I simply show a third-party access rule for N2H2 instead of SurfControl. Please refer to the section on N2H2 in the next chapter for details on how to set up N2H2 to work with BorderManager 3.7.

The prerequisites are that you must have a separate server running N2H2, and you must applied the BM37N2H2.EXE patch (or later), to your BorderManager server. Once the proper patch has been applied, the Access Rules menu on your BorderManager 3.7 server will look different, as shown below.



Depending on the patch level you have for BorderManager 3.7, new options for N2H2, SurfControl, Connectotel and None appear underneath the access rules. The screenshot shown above was taken with the BM37SP1.EXE patch installed. You have the choice of using only one third-party filtering solution at a time (N2H2 or SurfControl). Connectotel's products (LinkWall, AdWall and

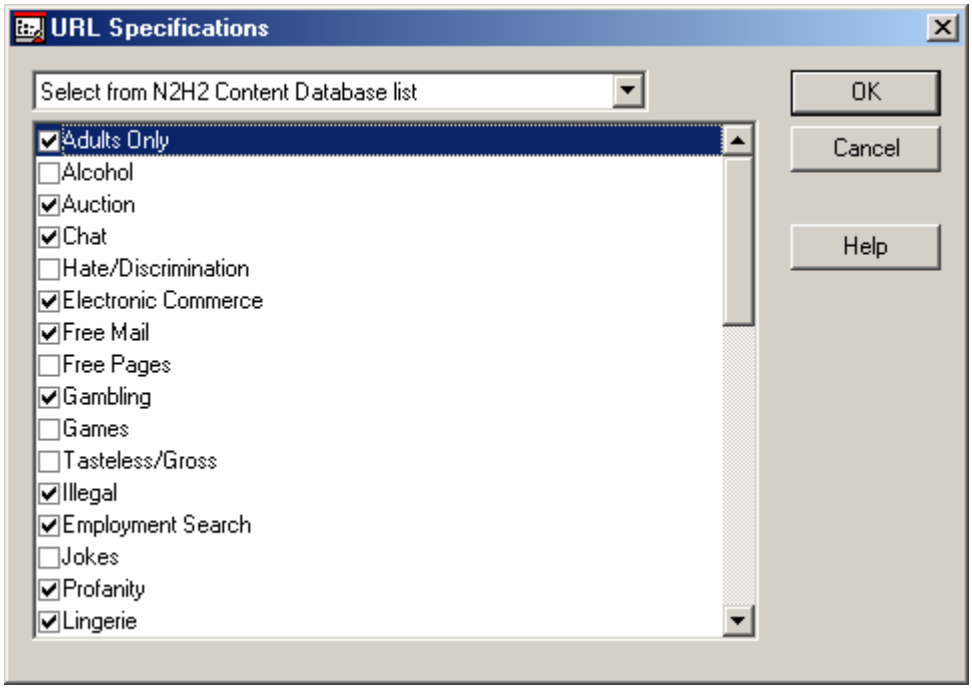
FileWall) can be used at the same time as N2H2 or SurfControl, despite the implication of the access rules menu screen.

See the section on configuring N2H2 later in this book for information on installing the product.

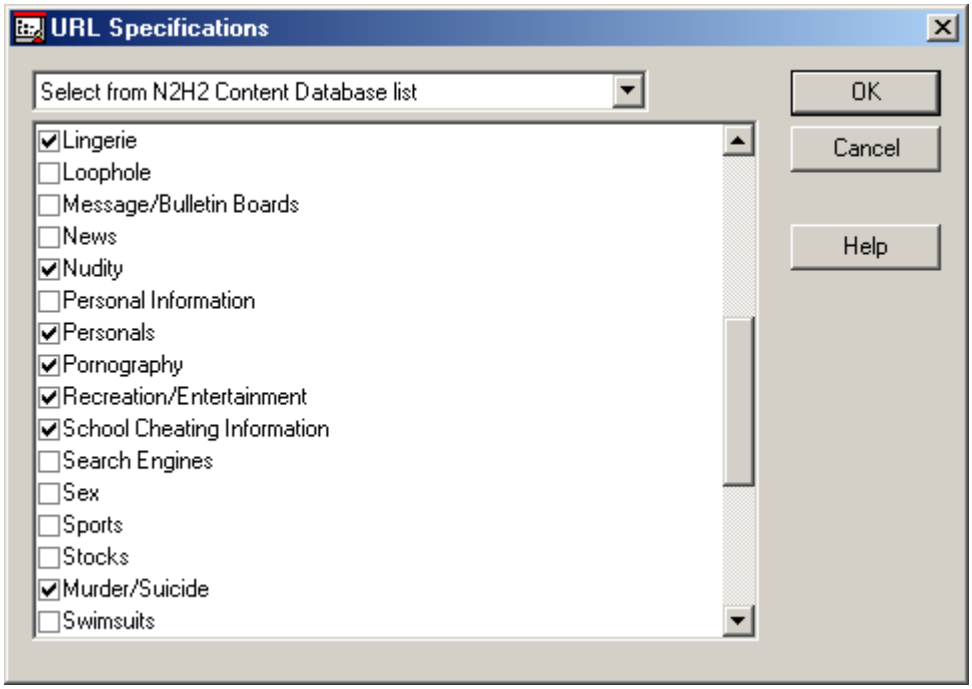
You cannot assign or copy SurfControl, N2H2 or Connectotel access rules to a container, only to a server object running the third-party filtering product.

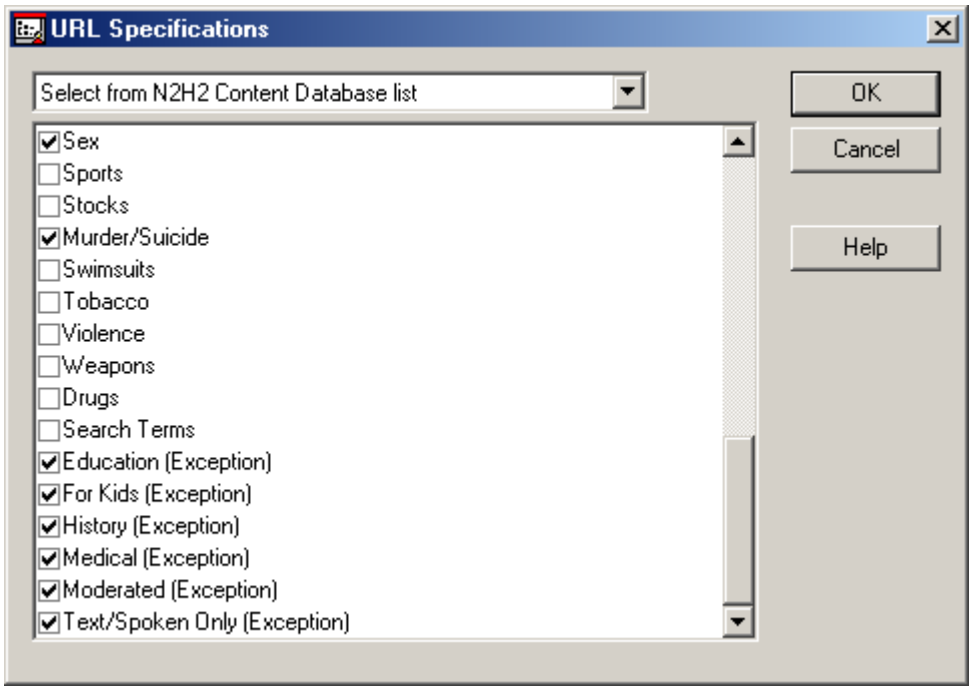
Aside from having to configure the N2H2 Sentian Category Server, on a separate server and configuring BorderManager to point to the N2H2 Sentian server, the access rule works almost the same as any other access rule. However, as of this writing, there is one important difference: if the N2H2 Sentian server is unavailable, BorderManager will eventually skip rule enforcement of the access rule. This generally has the effect of allowing traffic that would have been denied by a Deny URL rule for N2H2. Novell is working on a patch to fix this issue.

The categories denied in the N2H2 rules are shown in the following screenshots. Choosing the categories for N2H2 is very much like selecting CyberPatrol or SurfControl categories. See the next section for an example of setting up a CyberPatrol access rule.



The screenshot above shows the first part of the N2H2 category list. The remaining categories are shown below.





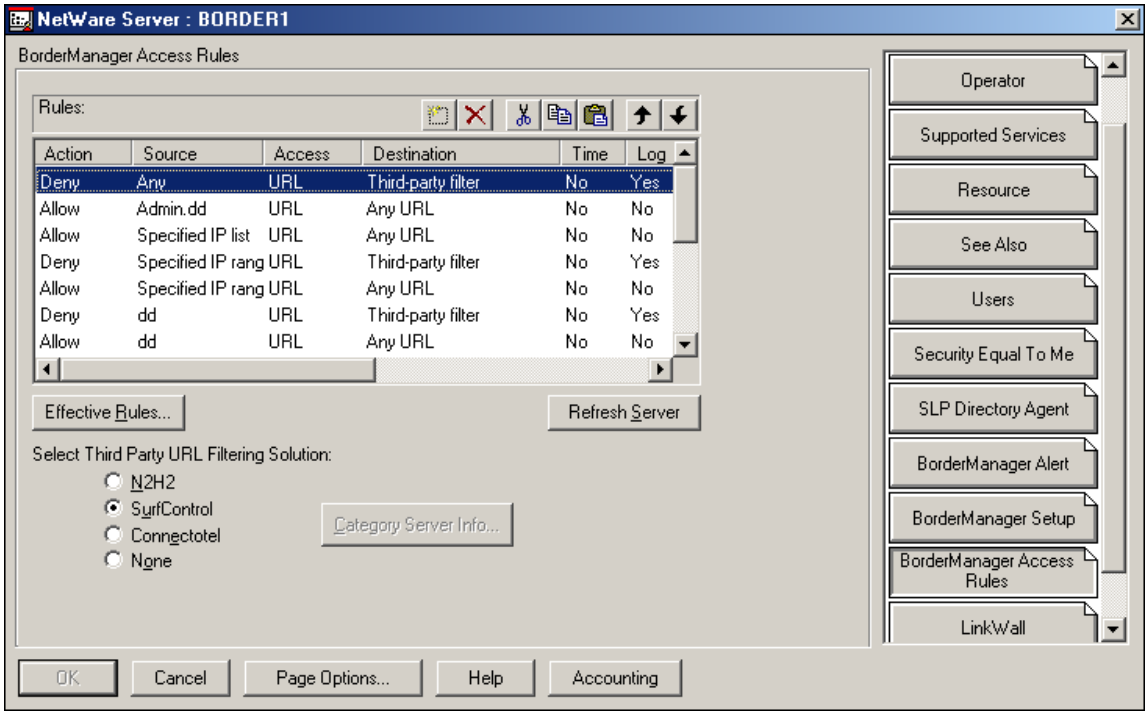
The screenshots above show the remainder the N2H2 categories selected.

Please see the next chapter for information on configuring the N2H2 Sentian Category Server.

LinkWall Access Rule Example

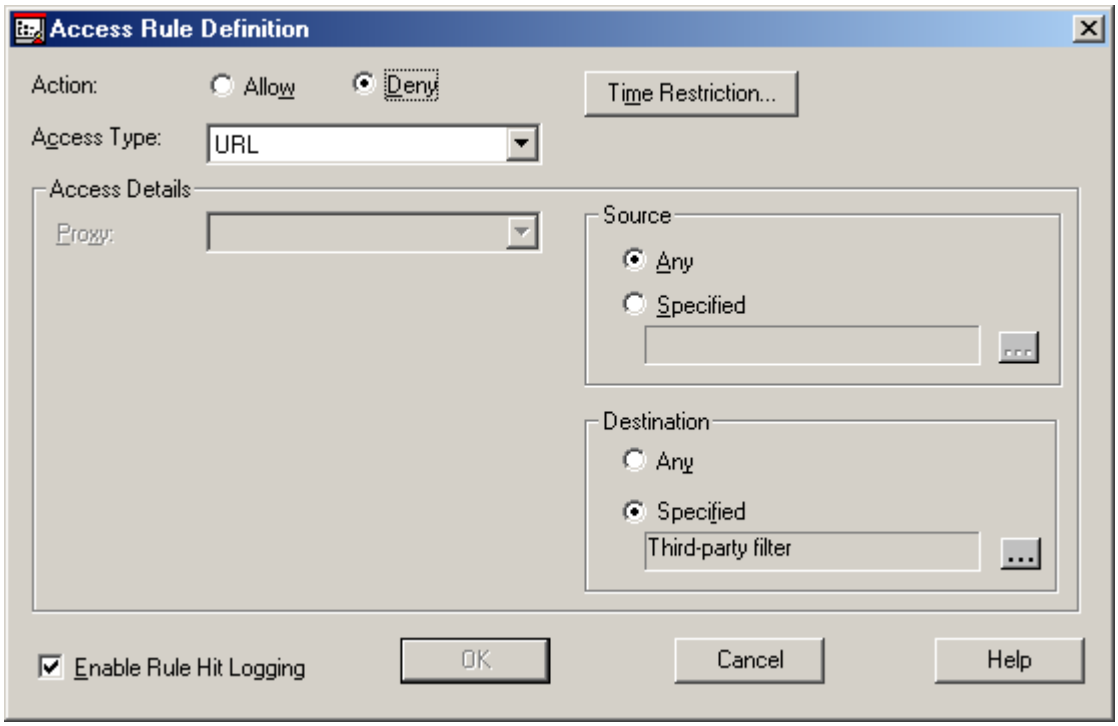
LinkWall is a third-party filtering product from Connectotel. See http://www.connectotel.com, and the following chapter, for more information on installing and configuring LinkWall.

LinkWall access rules are much more basic that N2H2 or SurfControl. Essentially you can only turn on the product or not. LinkWall allows you to selectively filter categories of URL's, but the categories are configured using text files, outside of NWADMN32. You can also click on the LinkWall tab (seen in the extreme lower right on the following screenshot) to edit the LinkWall configuration file in NWADMN32.

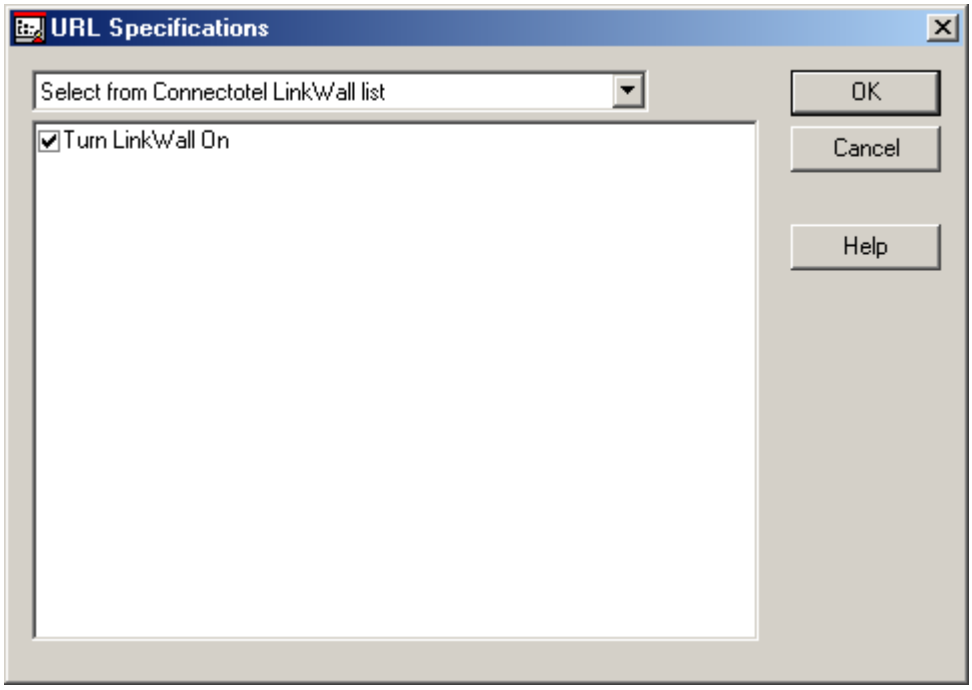


The screenshot above shows a number of third-party filters in place in the access rules menu. In this case, only the first rule is for LinkWall.

Note that LinkWall rules can be added in spite of the fact that the Third Party Filtering Solution in the lower left of the Access Rules Menu is not set to Connectotel.



The access rule for LinkWall has been configured to deny URL's, and Rule Hit Logging is enabled. The destination is set to Third-party filter.



In the Destination settings, there is a drop down list which contains the Connectotel LinkWall list choice, if LinkWall is already installed.

There is only one option to set – either turn LinkWall on, or don't. Configuration of which URL's to block with LinkWall is done in configuration files outside of NWADMN32. (However, you can edit the LINKWALL.LST file itself from within NWADMN32 by selecting the LinkWall tab. There is an example file shown later in this book in the chapter covering LinkWall installation).

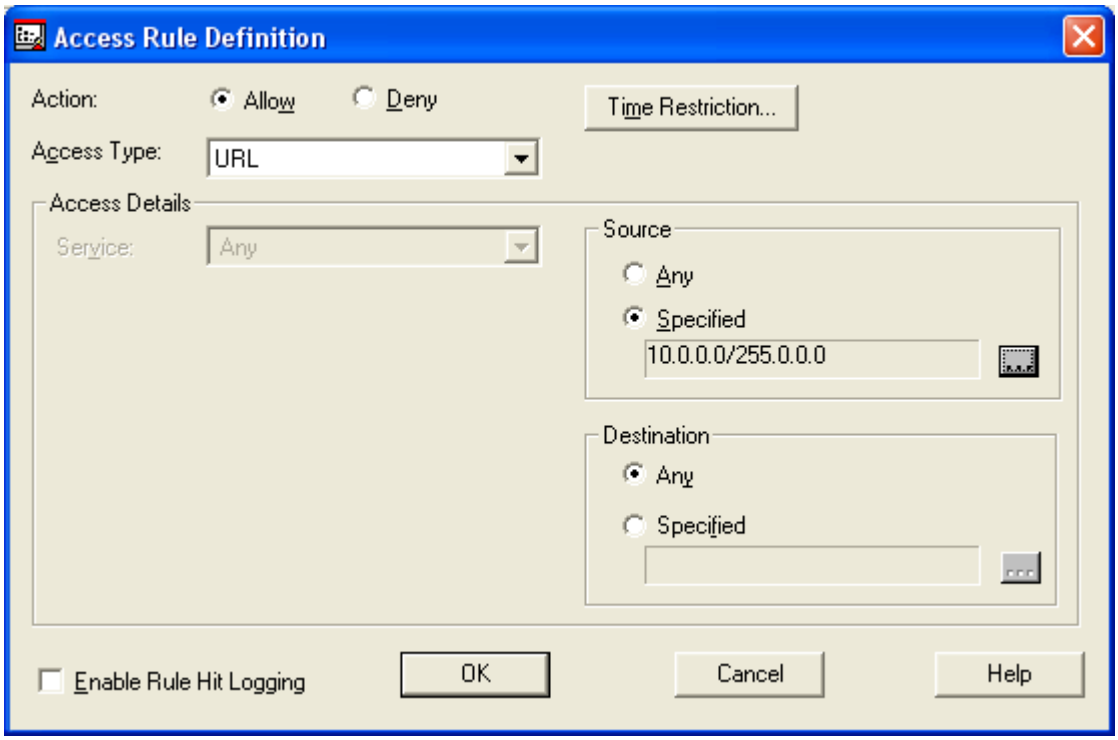
In the example shown in the chapter covering LinkWall installation, LinkWall is used with Squidguard Blacklists for pornography to deny the URL's within the lists to all users.

Example - Setting an Allow All URL Rule

If the Default Rule is to Deny Any, you must add in a rule to allow at least some access, or no one will be able to browse at all through the web proxy server. Often, companies put in a series of specific deny rules to block selected sites, then follow those with an Allow Any rule to allow any traffic that has not matched a previous rule in the rule list. Also, it is common to see a specific allow rule at the top of the rule list to let selected users or departments have more access than other users. For this example, we set up a rule that allows all access. Be careful to position the rule in the rule list properly – after a SurfControl, N2H2 or LinkWall Deny rule for example!

CAUTION *You should not use a source of Any if possible. It is possible under a number of circumstances to relay traffic off a BorderManager proxy from the Internet if access rules do not deny that traffic. Rather than Allow All, at least specify a source equal to your internal IP subnets.*

At the BorderManager Access Rules screen, click the icon to add a rule.

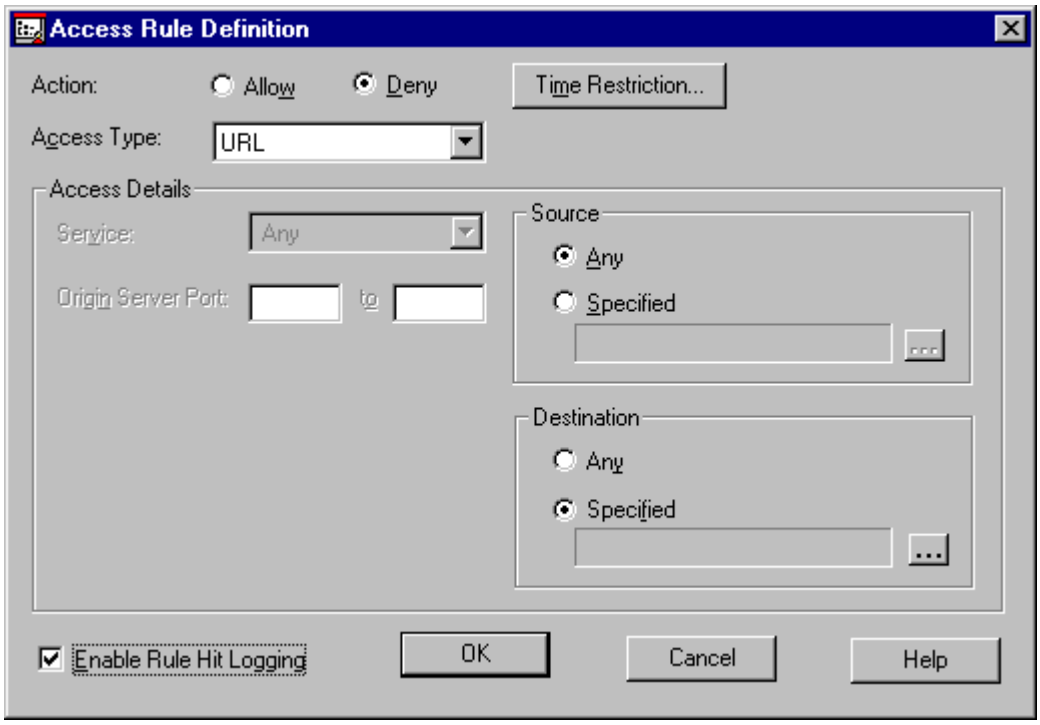


Select URL for Access Type, enter a source of a subnet address that covers your internal network and click OK to save the rule. Be sure to then position the rule in the rule list to be the LAST rule, or else it will override all other rules.

Example - Adding a CyberPatrol CyberNOT List Deny Rule

CyberPatrol rules allow you to allow or deny a set of predefined URL's based on a list of criteria (established by CyberPatrol). To add a common rule to deny URL's in a typical business environment, follow these steps. Be sure to put this rule in AHEAD of any Allow Any URL rule, or it will never be used!

First, click on the add symbol (small box next to the red X)



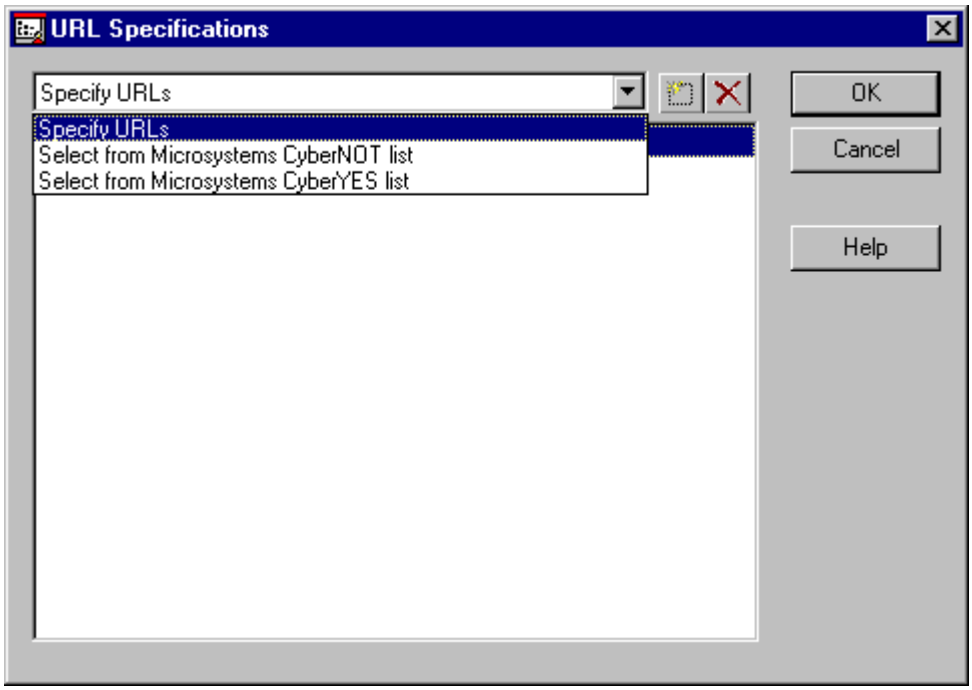
In this case, select an Access Type of URL. Select a Destination of Specified. If you want to log each denial based on this rule, check the Enable Rule Hit Logging.

It is recommended to only enable rule hit logging for deny rules. Generally speaking, if you are allowing access to a resource, you don't need to log it.

Some organizations will want you to log ALL traffic to perform 'Internet Policeman' duties. They will also probably want YOU (system administrator) to periodically collect and review the log data. I sincerely hope your organization is not one of these, as it can be very tedious to gather the log file data, and if you do not gather it periodically, it will roll over and be lost.

Once you have selected the above settings, click on the Specified Destination browse button to set the destination URL's up.

CyberNOT List Selection



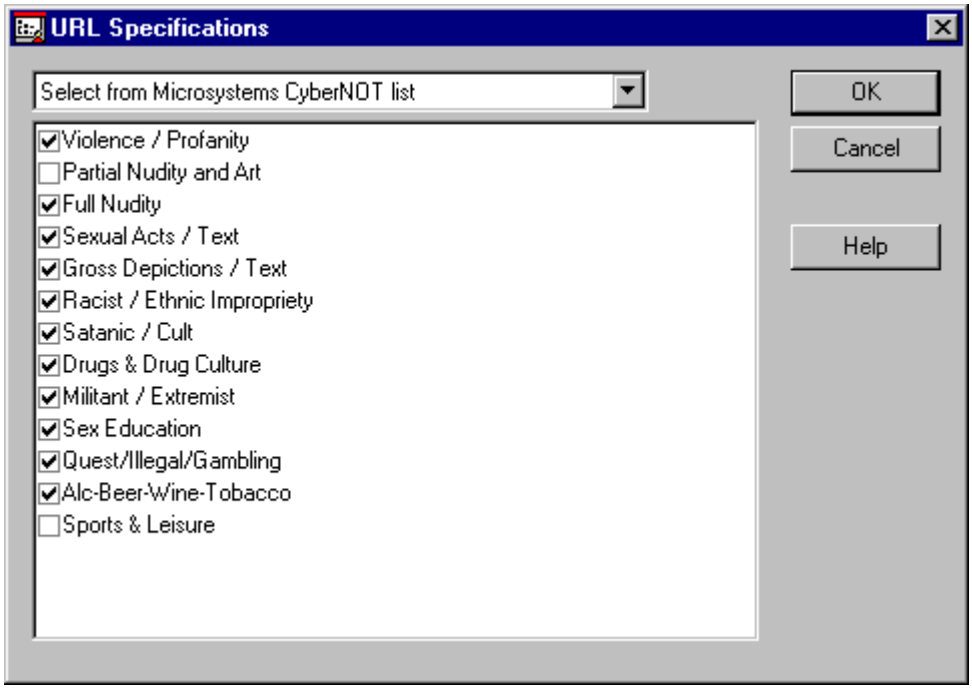
When you browse to a specified URL destination, you can add your own list of URL's to allow or deny, or you can select one of the CyberPatrol predefined lists by scrolling down the Specify URL's menu.

Select the **CyberNOT list**

Note If you have installed SurfControl, you will have an option called Select from SurfControl Novell BorderManager List. If SurfControl is in evaluation mode, you will have only a few categories to select from. If you have a current SurfControl subscription, you will have many categories to pick from. See the chapter on installing SurfControl and CyberPatrol for more information on setting up SurfControl. If you have configured the N2H2 Sentian Category server, you will see N2H2 categories.

CyberNOT List Definitions in Use

From the CyberNOT list, you can select entire classes of URL's from categories predefined by Microsystems CyberPatrol.



The following categories have been denied:

- Violence / Profanity
- Full Nudity
- Sexual Acts / Text
- Gross Depictions / Text
- Racist / Ethnic Impropriety
- Drugs & Drug Culture
- Satanic / Cult
- Militant / Extremist
- Sex Education
- Quest / Illegal / Gambling
- Alc-Beer-Wine-Tobacco

These categories were selected arbitrarily for this book, but are typical of the sites I see denied at large corporations in the United States.

Once you have selected the categories desired, click on **OK** to save them.

Note that CyberPatrol will stop downloading CyberNOT list updates when:

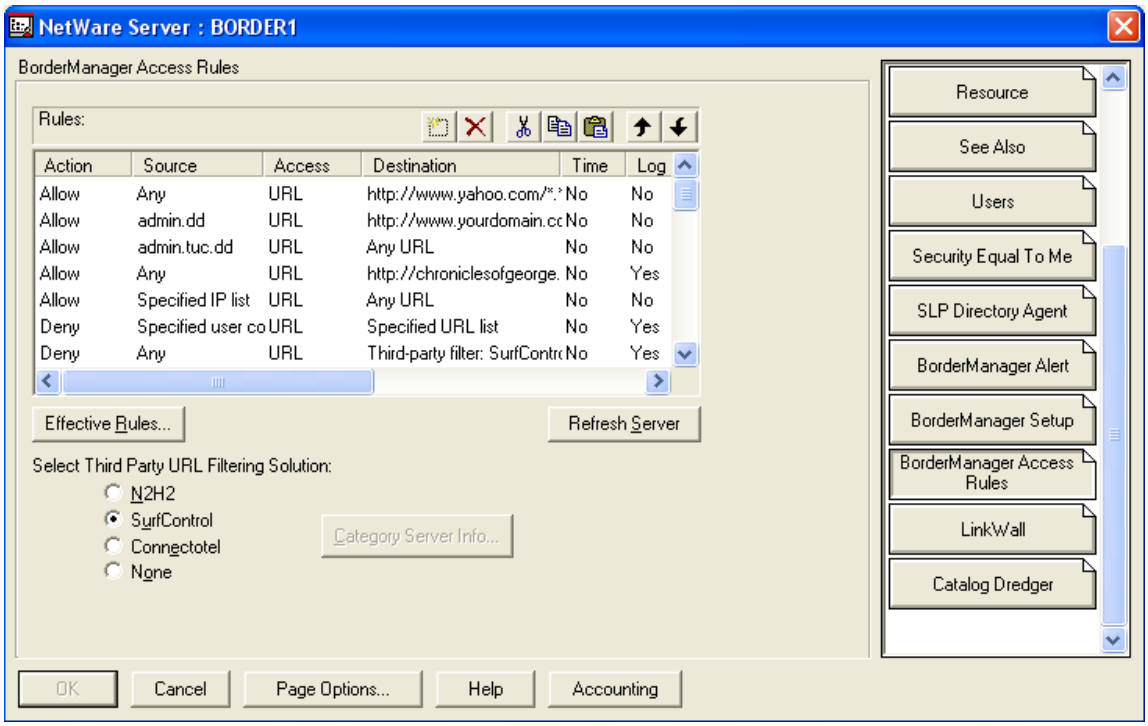
- The 45-day evaluation period has expired, or
- you have exceeded one year from the time you registered the software.

In both cases, you will not be notified of any change; the downloads will simply stop, and your CyberNOT list will quickly become out-of-date. You will need to run the SYS:\ETC\CPFILTER\REGISTER.EXE program again with a new registration code obtained from CyberPatrol to re-enable the CyberPatrol downloads. If you need to evaluate the software for longer than 45 days, deleting and reinstalling the software will start the 45-day evaluation program over again, though this may violate the terms of the evaluation license on most circumstances.

The SurfControl version of CPFILTER is quite different from the CyberPatrol version. It only provides a few categories if it is not registered. If you register the product, many more categories appear for your use. If your subscription expires, those categories disappear, and will not be blocked by a Deny URL rule you had set up earlier. Also, the SurfControl version of CPFILTER requires MUCH more RAM for caching a massively larger amount of URL's. SurfControl recommends an additional 512MB of RAM be added to a BorderManager server when subscribing to SurfControl. The CyberPatrol version of CPFILTER only holds 64,000 entries, while the SurfControl version holds several million, which accounts for a large increase in caching requirements.

The Refresh Server Button

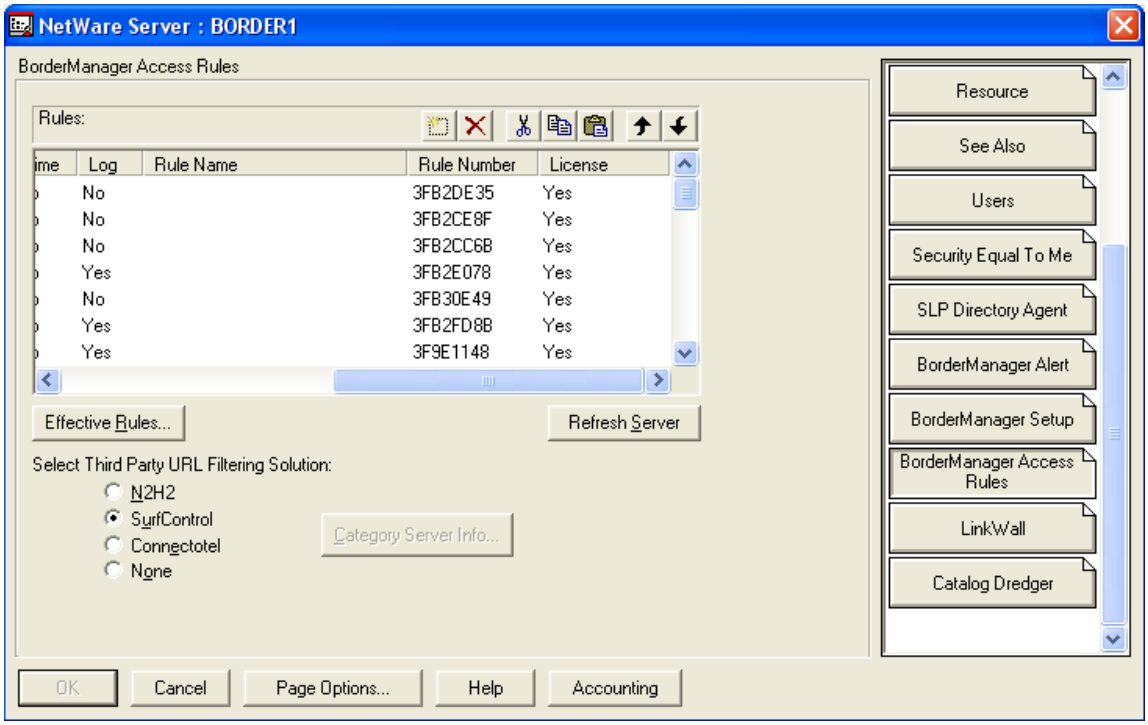
There is an innocuous looking button on the Access Rules screen near the bottom right. This button is used to cause the server to 'refresh' its rules list by forcing it to search through NDS for new or changed rules. It is necessary to use this button if you should base rules on NDS groups and then add or delete a new member of the group. ACLCHECK should periodically check NDS for rule changes every several hours, but rules don't normally pick up new group members immediately. The same may also hold for access rules applied to NDS containers.



Note the **Refresh Server** button in the lower right under the rules.

Those Additional Rules Fields

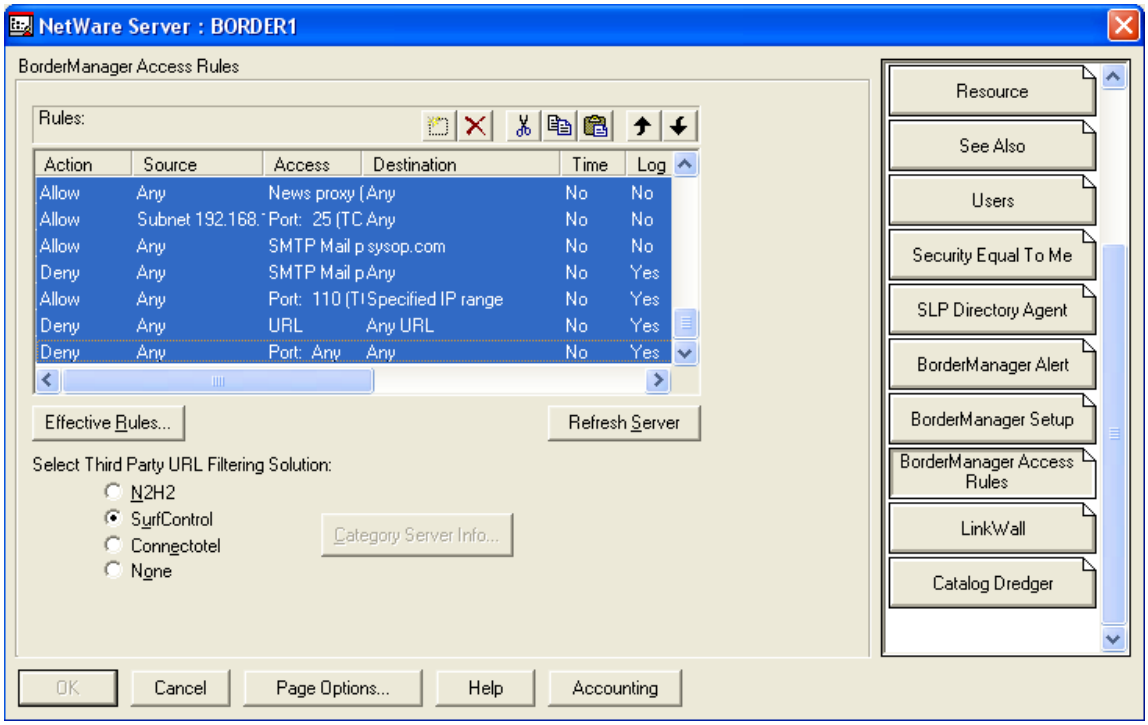
If you look at the Access Rules set up, you will notice that they may be scrolled from side to side. There are additional fields associated with rules that are not usually visible. These extra fields *cannot* be modified or used!



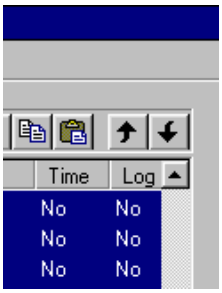
I have scrolled the rules list to the left to see additional (unusable) fields on the right. It is particularly unfortunate that the rule name cannot be filled in.

Backing up Access Rules

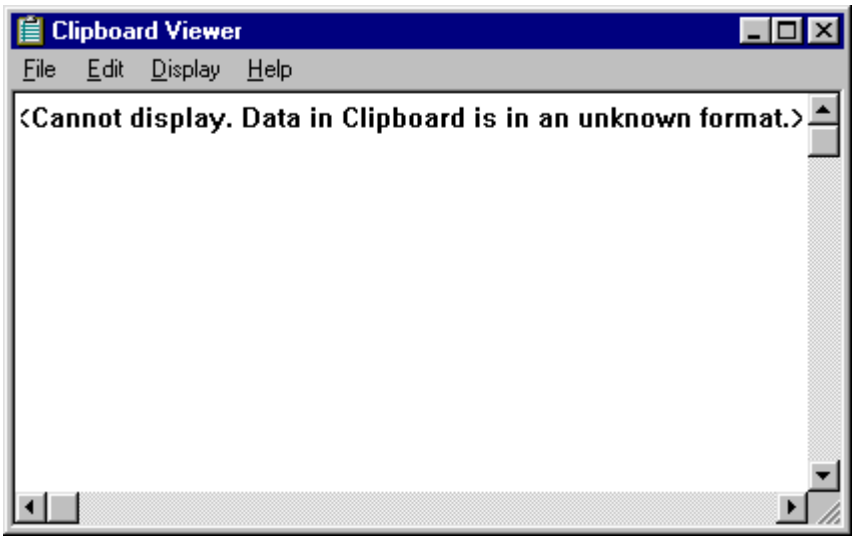
If you want to back up your access rules, there is an easy way to save them to a file.



Select all of the rules in NWADMN32.



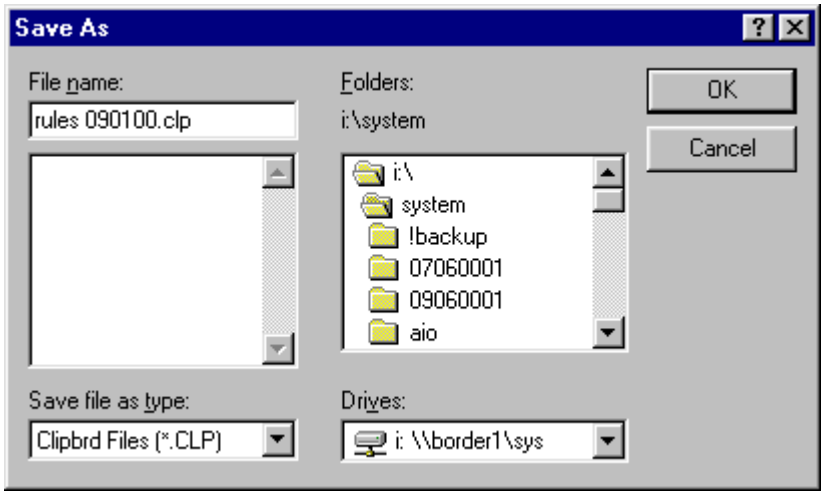
Click on the **copy icon**. (Looks like two pieces of paper, to the left of the clipboard icon).



Load the **clipboard viewer** in Windows 9x. (Programs, Accessories, System Tools, Clipboard Viewer.

If you don't have the Clipboard Viewer, In Windows 9x you will have to add it from Control Panel, Add/Remove Programs, Windows Setup, System Tools, Details, Clipboard Viewer).

For Windows XP, run the CLIPBRD.EXE program, which should be located in the SYSTEM32 directory.



Save the contents of the clipboard as a **.CLP** file

To restore the rules, just reverse the process, by loading the file into the Clipboard Viewer, and using the Clipboard icon in the Rules screen to 'Paste the clipboard rules to the end of the list'.

Selective Proxy Authentication Example Rules

Please do not confuse this section with the previous sections. It shows a completely **different set of access rules** than in the previous examples. I have shown only a simplified set of rules here to try to avoid confusion.

In these examples, I am trying to show how to allow certain hosts on an internal network to browse through the HTTP Proxy without requiring proxy authentication. At the same time, other hosts DO require proxy authentication. This sort of access rule configuration can be of use for any network where there are just some hosts where a) CLNTRUST is not usable, for whatever reason, and b) SSL Proxy Authentication is not useable or is not desired.

A classic example of a case where you might want to do this is when you have an antivirus server that needs to automatically access a web site to download updates, without a user being logged into your NDS tree.

In this example, I am trying to allow and deny the following:

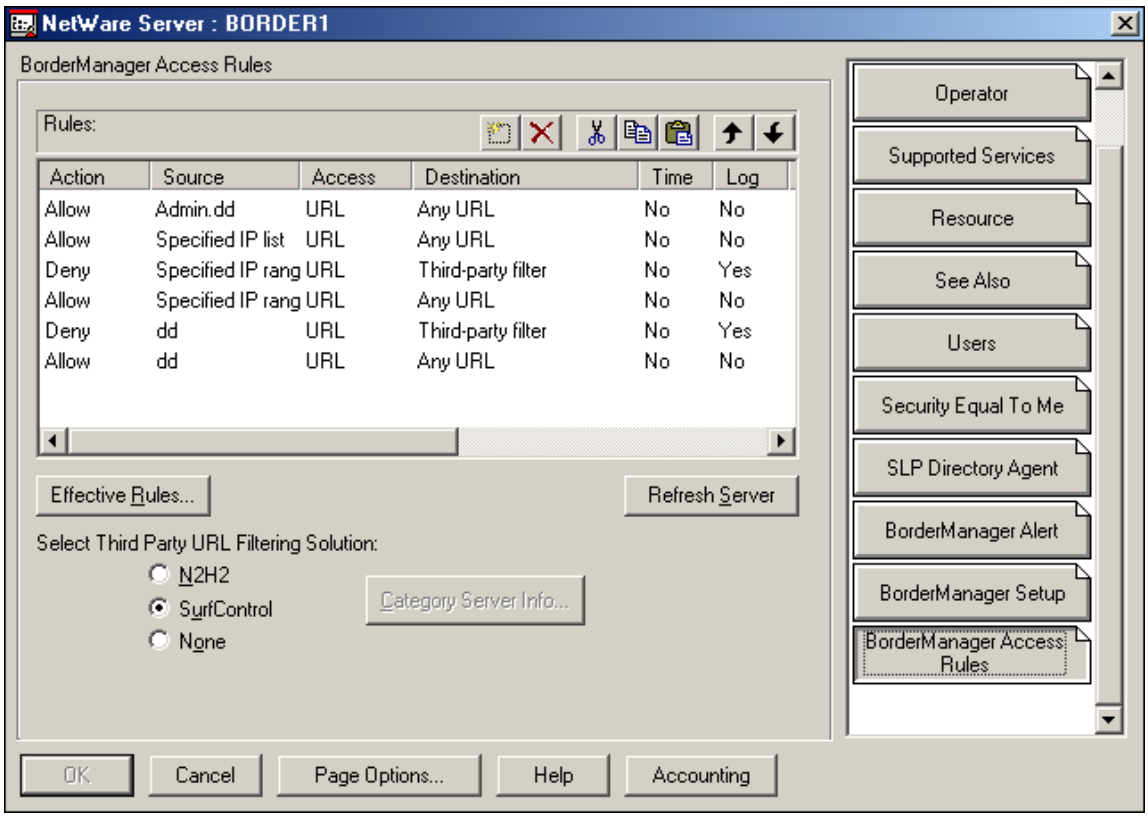
1. The admin user can access any web site. This will require authentication.
2. Hosts on IP addresses 4.3.2.250 and 192.168.10.244 can access any URL without proxy authentication.
3. Hosts on IP addresses 192.168.10.100 through 192.168.10.150 can access any web site not denied by a SurfControl access rule, without proxy authentication.
4. All hosts in or under the DD container in the BorderManager server's NDS tree can access any URL not already denied by a SurfControl access rule. Proxy authentication will be required if the hosts are not using an address specified above.

The host at 4.3.2.250 happens to be (in this example) another proxy server set up in a cache hierarchy. That server has its own set of access rules to control who can browser through it, but it needs to have full access at the parent proxy server.

The host at 192.168.10.244 is a RedHat Linux server, and the intention is that it can use proxy settings for Up2date patch updates from the RedHat network.

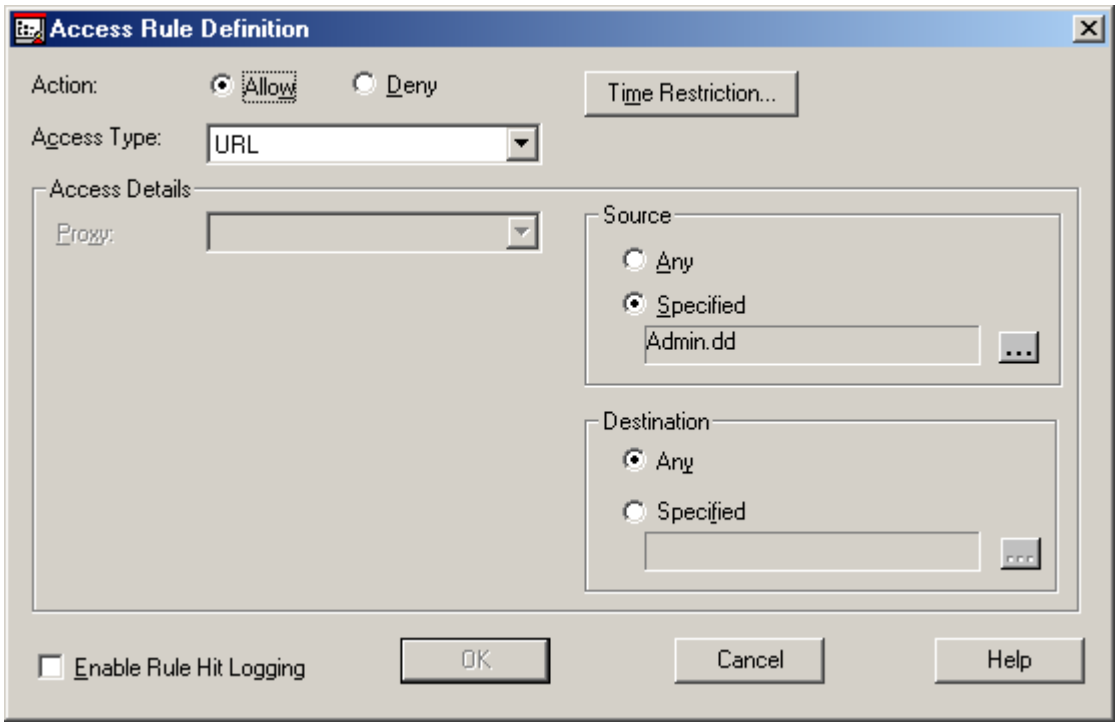
The IP address range 192.168.10.100 through 192.168.10.150 represents an address range configured with DHCP where there are host not running CLNTRUST, and for which I prefer not to invoke SSL proxy authentication.

Access Rules



The rules are structured as shown in the screenshot above. Remember that the rules will be read first for sources without NDS users, groups or containers, and a second pass through the rules will be made if required. Proxy authentication will be invoked from the server only on the second pass through the rules. That means that the first rule and the last two rules show above will be ignored on the first pass through the rules.

Allow Admin to Browse Any URL



This rule allows the Admin.dd user object to browse to any URL. It will not be seen unless a complete pass through the rules was already made looking for matches based on IP address or Any.

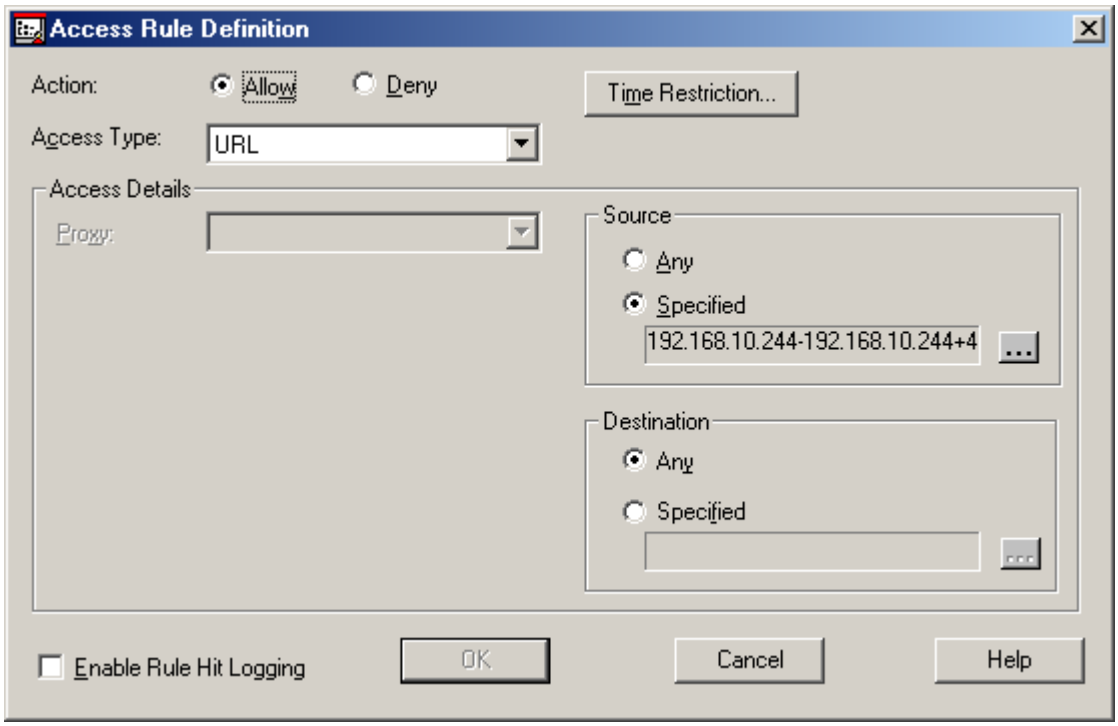
The Admin user might be blocked by the SurfControl IP address-based access rule that follows, if the Admin user happens to be browsing from an IP address denied in that SurfControl rule.

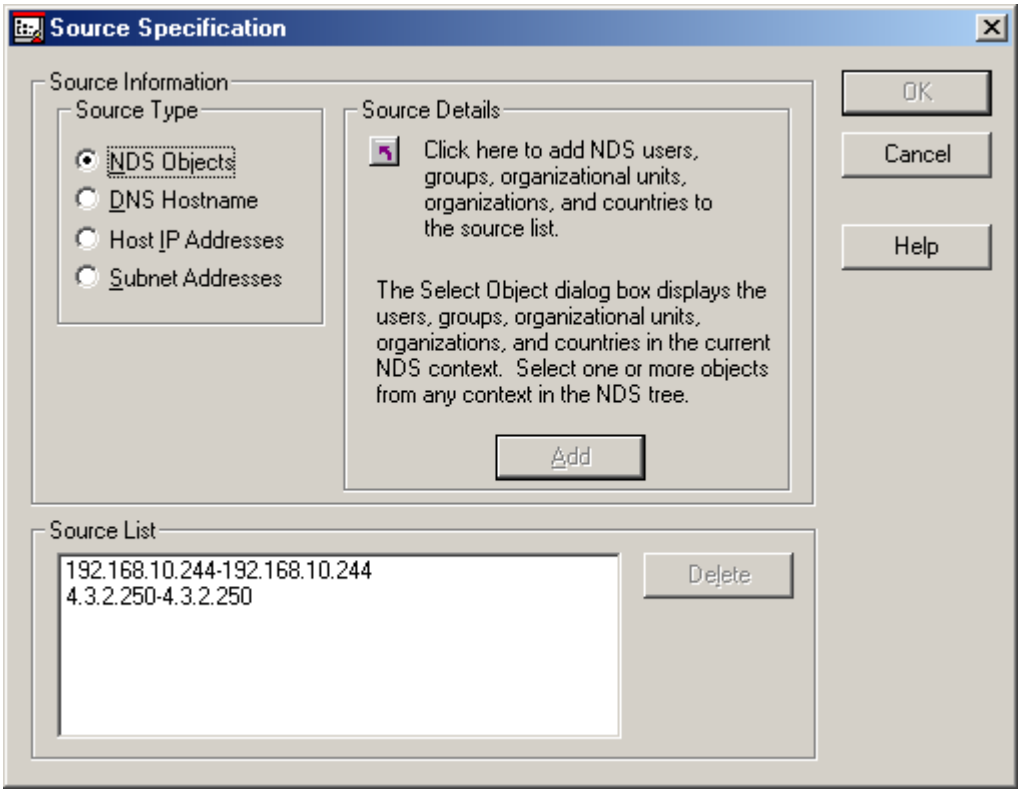
If the SurfControl rule would have been set up to block Any source, the Admin user would be blocked regardless of IP address used.

Note One way to allow the Admin user's PC access to any HTTP URL, regardless of access rules, would be to set up filter exceptions for his/her IP address, and not have the Admin user's browser configured for a proxy.

Allow Selected Hosts to Any URL

This rule allows two hosts to browse to any URL, based on the hosts' IP addresses.

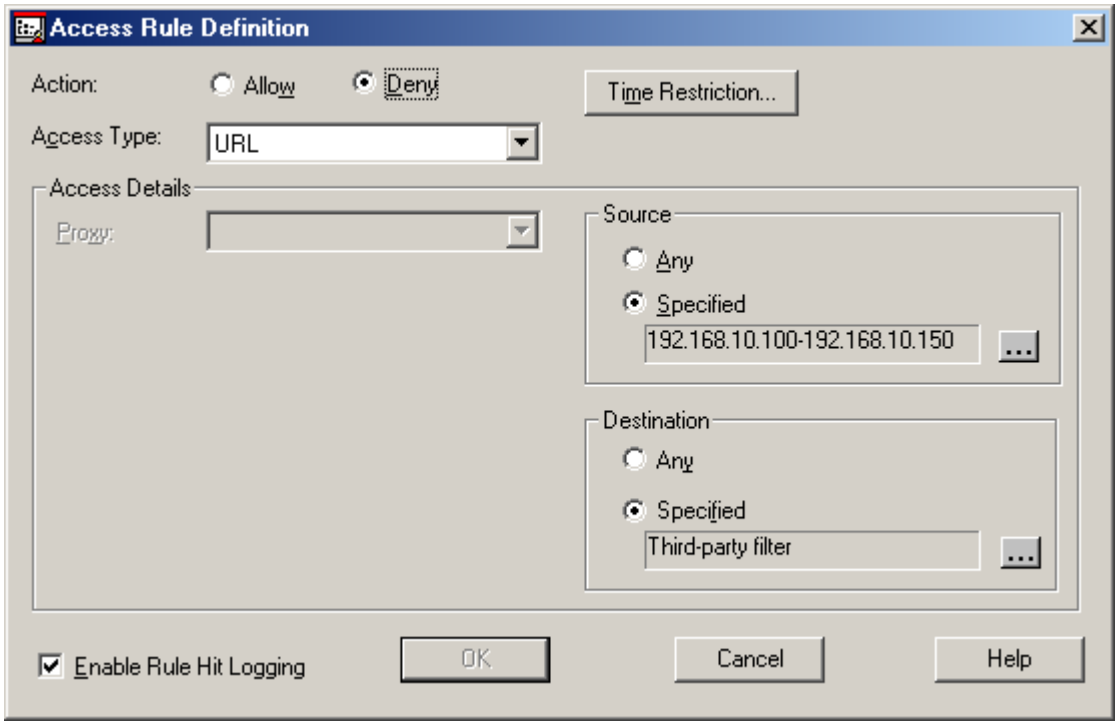




The screenshot above shows the IP addresses configured in the access rule.

In my example, the addresses above apply to two particular hosts that need to be allowed HTTP Proxy access without invoking proxy authentication.

Deny SurfControl URL's to Selected Users



This access rule denies access to a rule list contained in a third-party filter (SurfControl in this example, but could be N2H2 or CyberPatrol).

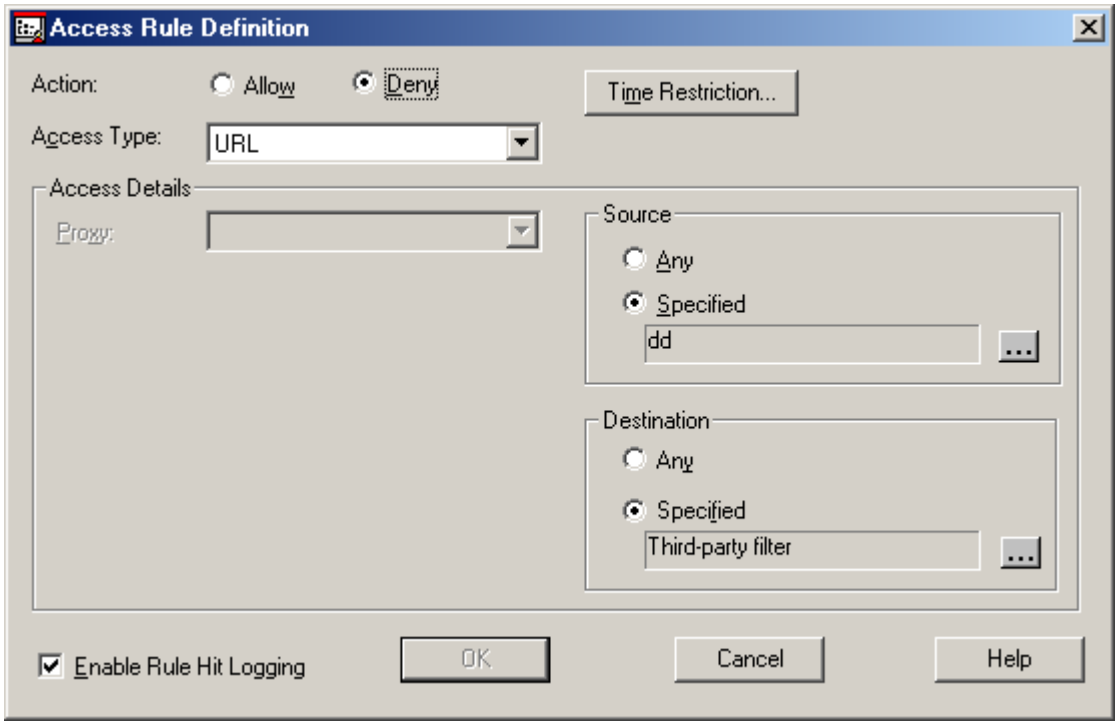
The rule calls out a source equal only to the 192.168.10.100 through 192.168.10.150 IP addresses.

The idea behind specifying these source addresses is to allow the Admin user to NOT be blocked by the SurfControl rule, IF the Admin user is not logged in at one of the denied addresses.

If this access rule applied to Any source, then the Admin user would be affected by it, before proxy authentication was invoked, regardless of the IP address on the Admin user's host system.

If the Admin user happens to be logged in at one of the addresses specified here, there is no way to prevent this rule from coming into play and allow access, since proxy authentication will not have been invoked yet, and there will be no way that the BorderManager server can tell if the user at the source IP address is the Admin user.

Deny SurfControl URL's to NDS Users

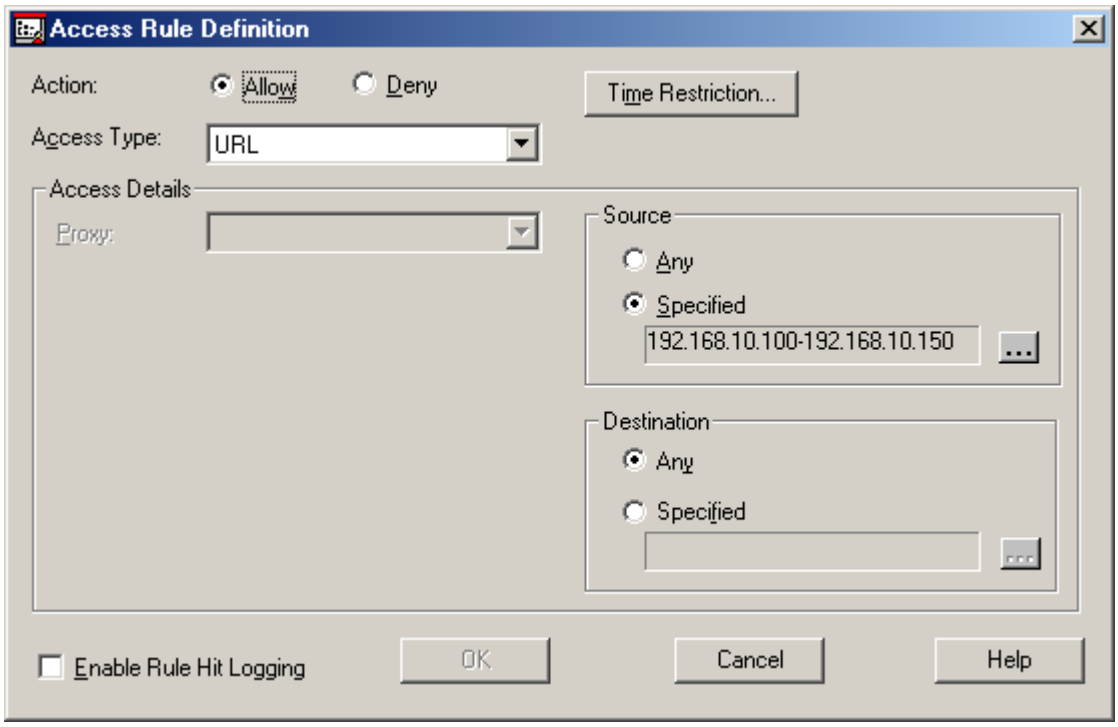


This access rule covers users all non-Admin users, once proxy authentication is invoked.

The first pass through the rules looked for non-NDS sourced rules. That would have allowed access to the Linux and Proxy servers mentioned earlier. Also, users on the 192.168.10.100 through 192.168.10.150 addresses would have been allowed or denied access by IP Address-based rules. On the second pass through the rule, where proxy authentication was invoked, the Admin user would already have been allowed to any URL by the first NDS-sourced rule. This rule therefore catches all other users in the BorderManager NDS tree, on the second pass through the rules.

As you can see, allowing selective proxy authentication can get complicated.

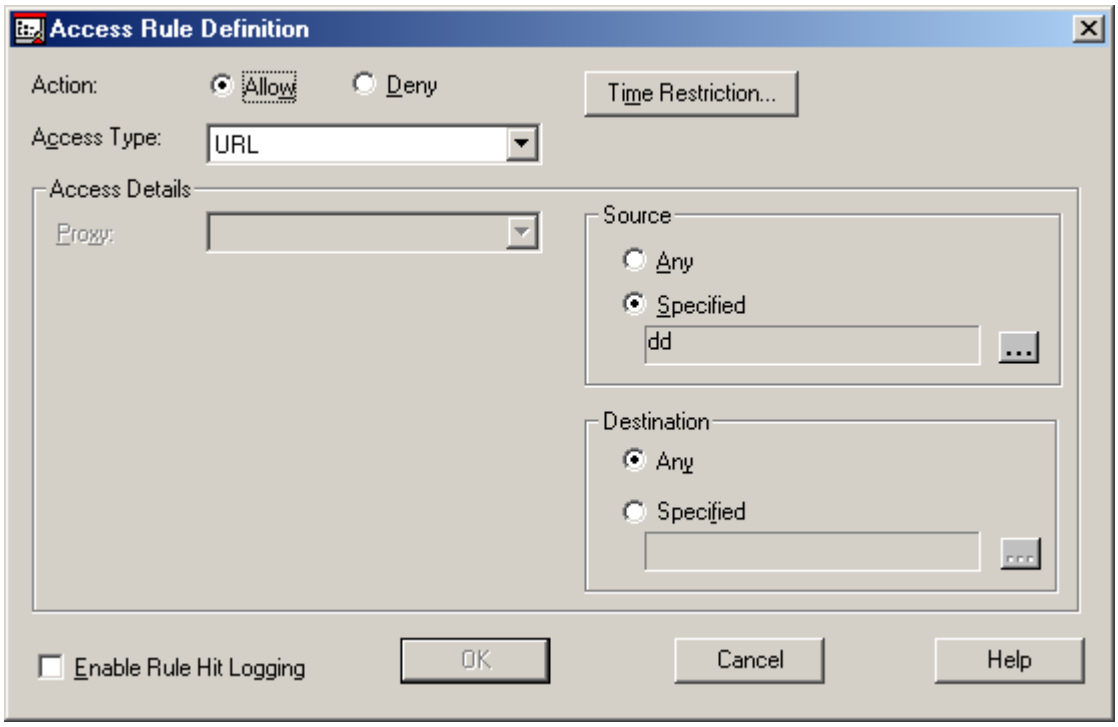
Allow Selected IP Addresses to Any URL Not Already Denied



This rule allows the selected IP addresses to browse to any URL not already denied by a previous rule (SurfControl).

This rule is necessary to allow the source IP addresses (192.168.10.100 through 192.168.10.150) to browse without undergoing proxy authentication.

Allow All NDS Users to Any URL Not Already Denied



This access rule allows any user object in the BorderManager NDS tree in the DD container or below to access any URL. Previous rules might have allowed or denied traffic based on IP address or NDS user name, but this one will catch any users not already allowed. Proxy authentication will be invoked when this rule is hit.

Should the host not proxy authenticate, the default Deny Any rule would be hit, and access would be denied.

Effect on Logging with Selective Proxy Authentication

When you enabled selective proxy authentication, you can get some odd results in the log files. Remember that two passes are made through the access rules, the first for rules without NDS sources, and the second for rules with NDS sources.

Because it is possible, even likely, that you could have rules that take effect without first proxy authenticating the client to the server, your log files will in at least some cases not show the user ID.

User ID's only show up in the log files after someone is proxy authenticated.

As an example, you might have a SurfControl rule to deny pornography sites to Any source. You might also have a rule to allow an NDS container to browse URL's. This leads to a situation where someone could be denied access by the SurfControl before they have been proxy authenticated by hitting another rule. However, once an NDS-sourced rule is used, proxy authentication of the user occurs. What you would see in the log files is first the IP address of the user, and later the NDS user ID of the user. Since authentication times out and has to reoccur over time, you could see log files with first a name, then an IP address, then a name, then an IP address, etc.

This is a consequence of how selective proxy authentication works. If the user is allowed or denied access to a URL before authentication happens, the logs can only show the IP address of the user, not the user ID.

The only way to force the logs to always show the NDS user ID would be to somehow force the user to access a URL that is not covered by an access rule which allows or denies access based on IP address or Any.

Chapter 23 – SurfControl, CyberPatrol, N2H2 and LinkWall

Versions of BorderManager prior to 3.7 included the CyberPatrol program CPFILTER.NLM to do content filtering with Access Rule controls. BorderManager 3.7 includes a new version of CPFILTER.NLM based on SurfControl. The SurfControl program is much more comprehensive than CyberPatrol. BorderManager 3.8 can use SurfControl, but the program is not included on the product CD.

By applying a patch to BorderManager 3.7, access rules can also be configured to use an N2H2 Sentian Category Server.

SurfControl

Note The version of SurfControl that ships on the BorderManager 3.7 Product CD is obsolete. You should download the new version (Service Pack 3 as of this writing) to get new features of SurfControl. The download is approximately 60+MB, and includes a relatively up-to-date version of the SurfControl database. BorderManager 3.8 does not ship with SurfControl on the CD.

The SurfControl version of CPFILTER.NLM only runs on BorderManager 3.7 or 3.8.

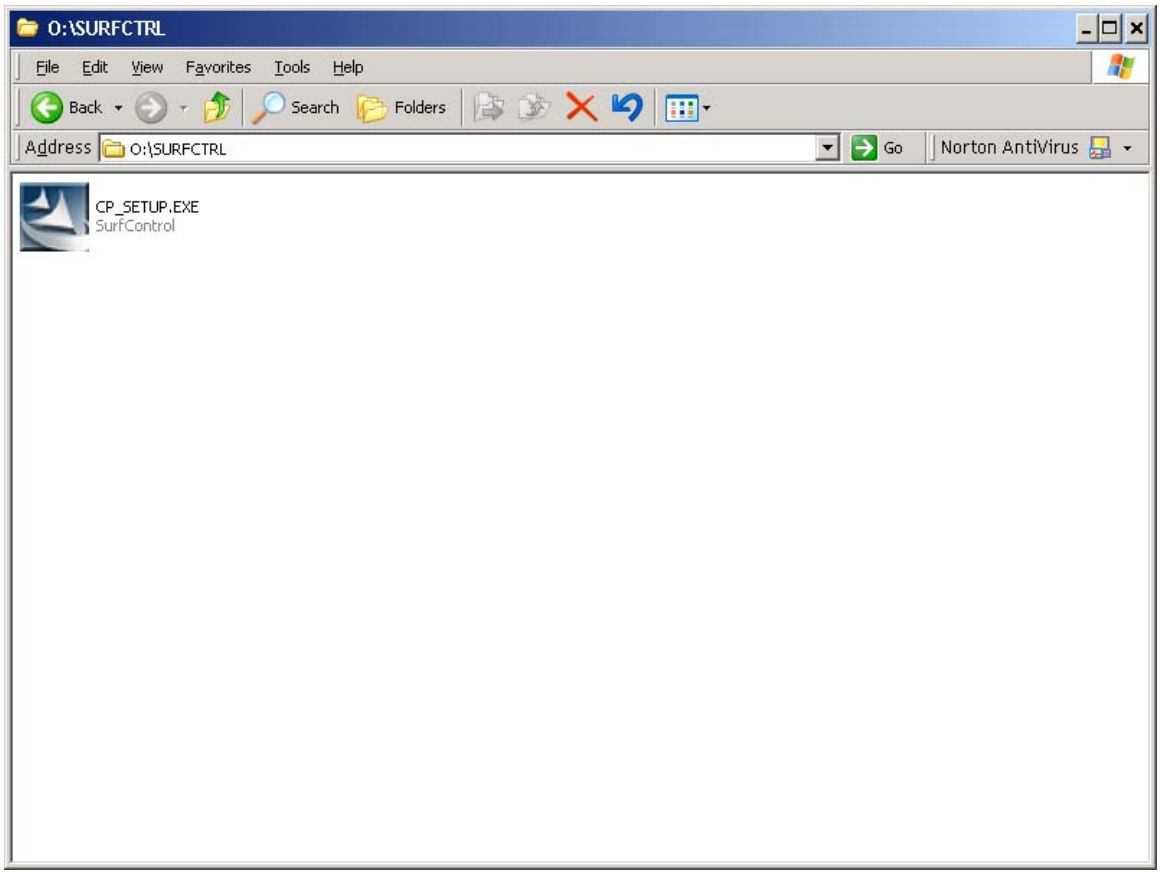
Only the Service Pack 3 version of SurfControl contains all 40 categories – previous versions had only 32 categories.

The SurfControl version of CPFILTER.NLM can be run in evaluation mode, but it will not block some of the most useful categories, such as pornography sites. If you register the program, many more categories show up on the list. Updates to the lists will be downloaded automatically. If the SurfControl subscription expires, the program reverts to an evaluation mode, where only some of the site categories are blocked.

To install SurfControl, locate the SYS:\SURFCTRL directory on your BorderManager server. If using the (old) version of the program, it should be in the root of the SYS: volume. If you downloaded the latest version (highly recommended), it will be located wherever you saved it.

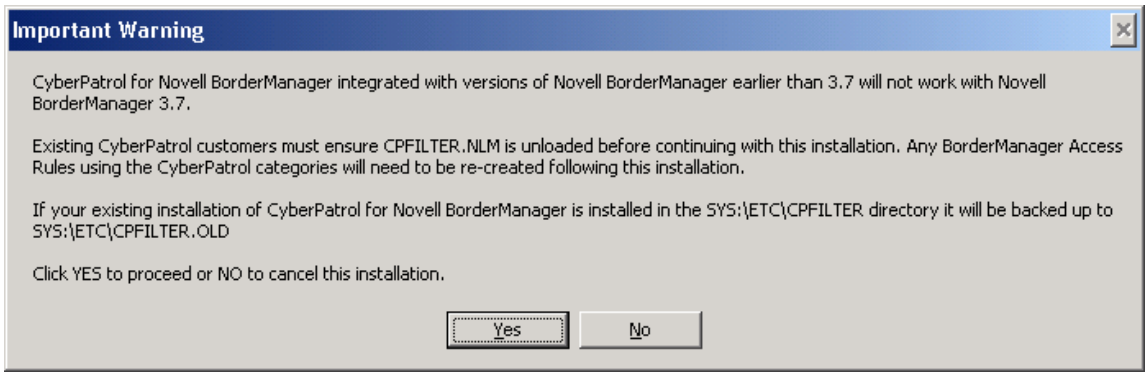
Run the CP_SETUP.EXE program. (This version does not play the Hawaii 5-O theme as the CyberPatrol version did).

SurfControl configuration, like CyberPatrol in pervious versions of BorderManager, requires you to run a CP_SETUP.EXE program to extract the various files required. You will be required to select a drive letter mapped to the SYS volume of a BorderManager 3.7 server.

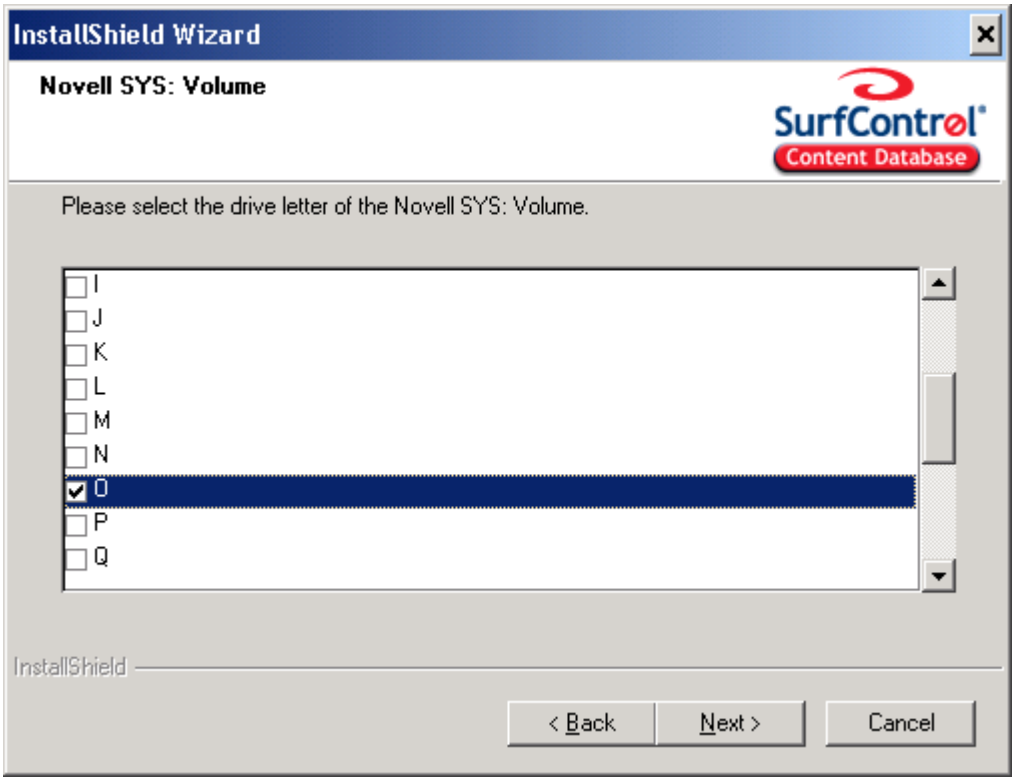


Run the CP_SETUP program, and you should see a screen showing files being extracted, and then a Welcome screen. Click on **Next** at that point.

You should then see a license acceptance screen. Click on **Yes** to accept the licensing requirements.



You may see a warning message about previous versions of CPFILTER.NLM. Be sure to unload CPFILTER.NLM from the server before continuing. Click on **Yes** when ready to continue.



You will be prompted for the drive letter of the BorderManager 3.7 SYS: volume. The choices shown will be those drive letters currently mapped on your server.

Select the BorderManager server's drive letter and click on **Next**.

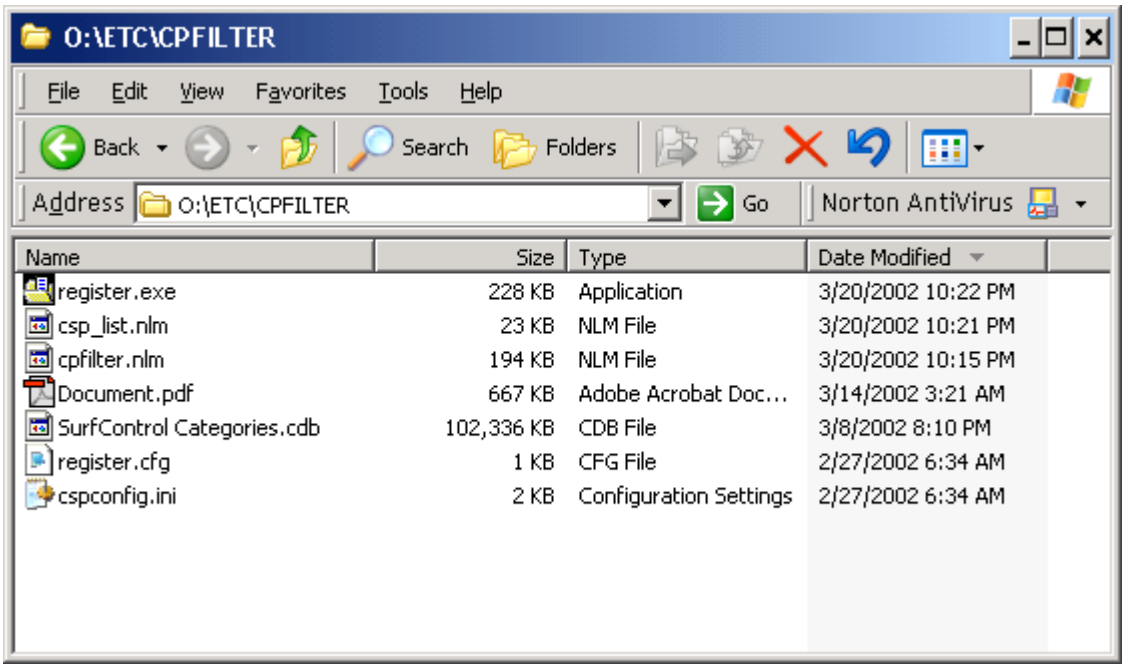
If you had an older version of SurfControl already installed on the server, the new version will rename the old directory to SYS:ETC\SCV5SP2.BAK. You will have to reregister the new version.

You should see a window telling you that files will be copied to <drive letter>/ETC/CPFILTER.

Click on **Next**.

Once the files are copied, you should see an InstallShield Wizard Complete screen. Click on **Finish** to complete the installation.

You can now load CPFILTER.NLM on the server. Add the command LOAD SYS:\ETC|CPFILTER\CPFILTER to the AUTOEXEC.NCF file (or to the STARTBRD.NCF file).



You should see files in the SYS:\ETC\CPFILTER directory similar to the above. That screenshot was taken after installing SurfControl over an existing CyberPatrol installation.

Note the large **SurfControl Categories.cdb** file, which accounts for a large amount of RAM used by the CPFILTER.NLM when it is loaded.

You might wish to LOAD MONITOR, and go to System Resources, Alloc Memory (bytes) and see how much RAM CPFILTER.NLM is using. For a registered version, you will need as much as 512MB of RAM – just for SurfControl – on your server, in addition to the RAM suggested just for BorderManager (another 512MB). Therefore, a minimum amount of RAM in your BorderManager 3.7 server, with SurfControl to be used, is 1GB. (1024MB) Or more.

When the SurfControl update process runs, the CPFILTER.NLM may temporarily double in size, leading to a large RAM requirement. The version of CPFILTER that shipped with BorderManager 3.7 always doubled the RAM usage when it updated itself. SurfControl Service Pack 2 (or later) does not double the

RAM usage by default, but instead swaps in an updated CDB database to RAM from disk. (Previously, a copy of the CDB database was updated in RAM, then swapped in to replace the existing database already held in RAM. This procedure caused the doubling of RAM usage when the update process ran, but it also minimized the period of time during the update swap process where users might be denied access due to the updating going on).

The SurfControl Service Pack 2 (or 3) default settings cause the database to be swapped from disk into RAM as needed. While this behavior greatly reduces the amount of RAM needed during the update cycle, it also increases the (small) window of time during the update process where users could be denied access to the Internet. (A SurfControl access rule denies browsing activity if the database is not loaded into RAM).

Should the older behavior be desired, it can be achieved by adding a new setting in the SYS:ETC\CPFILTER\CSPCONFIG.INI file. (I do not recommend changing the Service Pack 2 default settings). If you want the old method of updates, add the following lines under the [SurfControlGeneralList] section: FileBasedLiveUpdate=0 and SingleMemBlockSwitch=0. See the SurfControl Administrator Guide for more details.

SurfControl Service Pack 2 and later versions support updates through an upstream proxy server (cache hierarchy server). In the CSPCONFIG.INI file, under the [SurfControlGeneralList] section, add the lines UseProxy=1, ProxyServer=<upstream IP address>, and ProxyPort=<port number>. See the SurfControl Administrator Guide for more details.

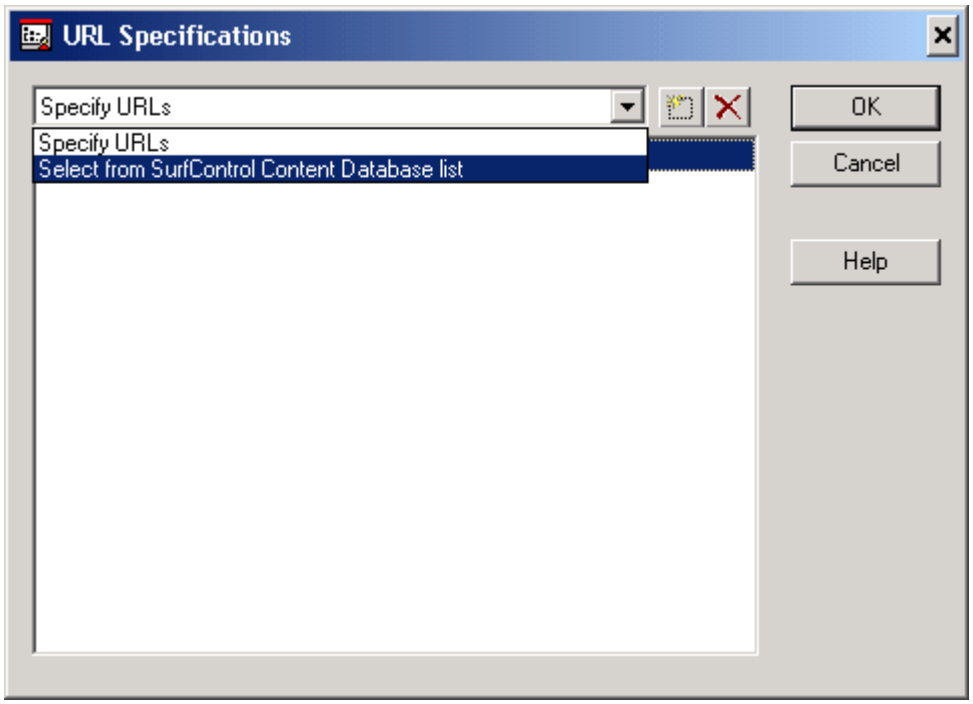
The SurfControl Administrator Guide can be found, in PDF format, at the SurfControl Web Site.

The CSPCONFIG.INI File for Service Pack 2 or 3

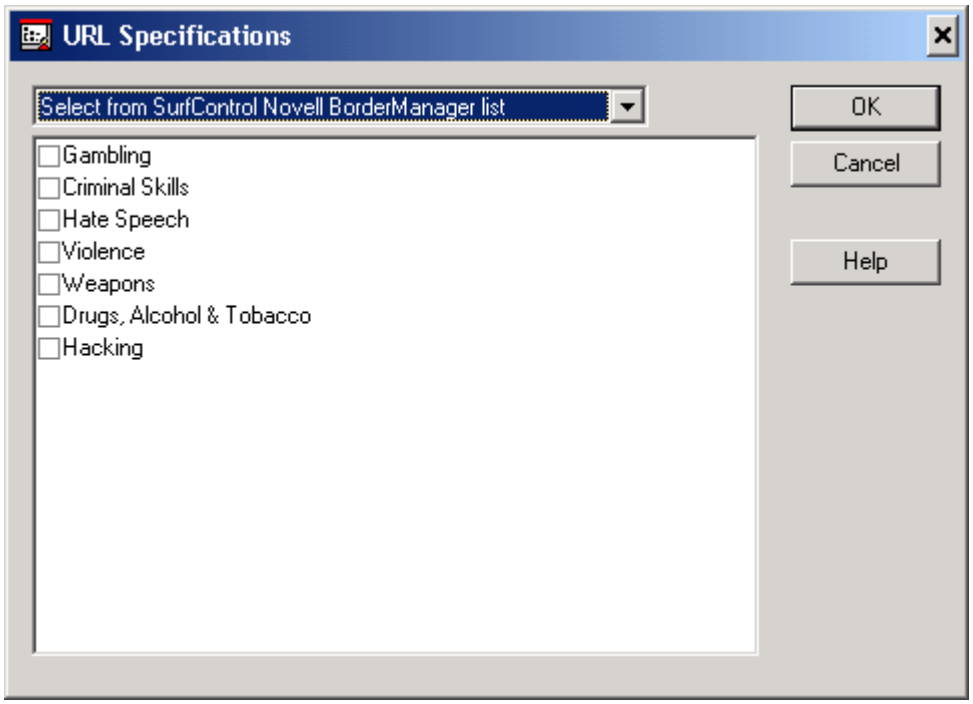
```
################################################################################
#     CSPConfig.ini
################################################################################
#
# DESCRIPTION
# ===========
# [CSPList]                 The Content Service Provider section name
# Providers=CSPName1,CSPName2   The List of CSP's
#
# This section lists all configured Content Service Providers in a
# comma separated list.  Each named CSP MUST have it's own section of
# configuration settings in the ini file.
#
# [CSPName1]                The settings for the named CSP
# Type=CSP                  Always set to CSP
# Service=                  The full path & name of the CSP DLL
# CDB=                      The full path & name of the CDB File
#
[CSPList]
Providers=SurfControlGeneralList

[SurfControlGeneralList]
CDB_PREALLOC_SIZE=350
Data 2=CF9A95E066D11268CEFDCB7B58B67FF0F187EF2E3012F3
Data 1=CF9A95EDCEEC2B226AA486BAC0E011101AD1
WorkingDir=
Licence=
Service=CPFILTER.NLM
CDB=SurfControl Categories.cdb
Categories=
Type=CSP
WebServer=st4update.surfcontrol.com
Port=80
URL=/cgi-bin/GenLiveUpdate.dll
RemoteDirectory=UDBDownload
```

SurfControl Access Rules (Unregistered):

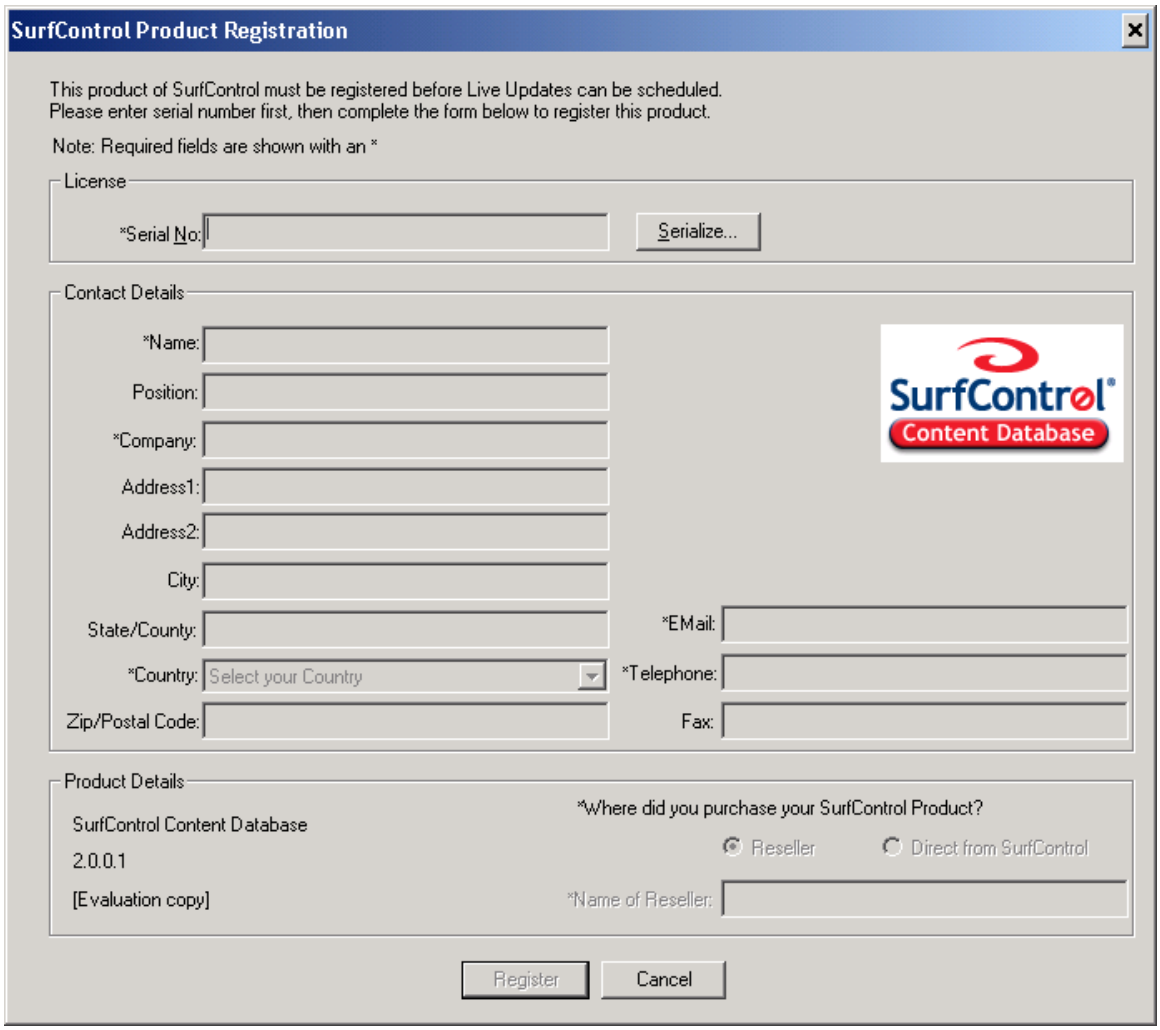


If you have not registered SurfControl, you will not see very many categories to pick from. The list gets larger when you register.

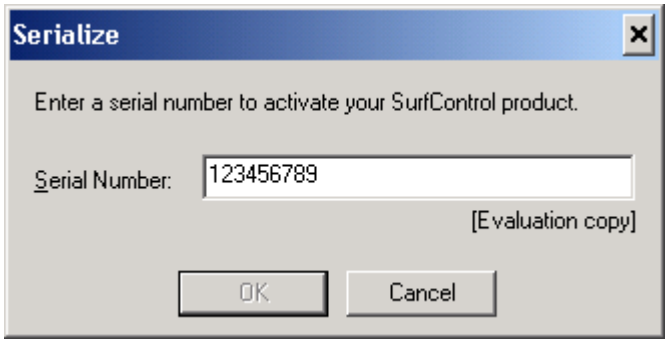


Registering SurfControl

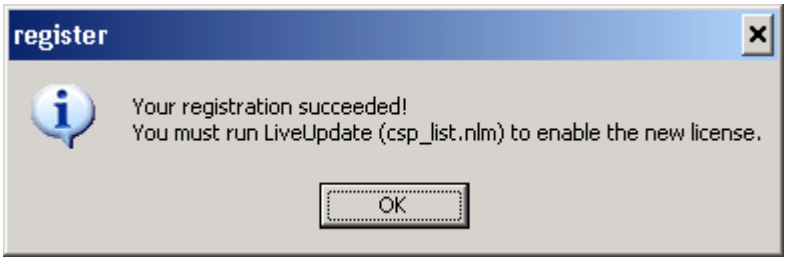
Visit the SurfControl web site, at http://www.surfcontrol.com, to get details on purchasing a SurfControl license, or getting a 45-day evaluation code to try out SurfControl.



Then run the SYS:\ETC\CPFILTER\REGISTER.EXE program



Enter your Serial Number, and fill in the rest of the required information.



If your serial number is correct, you will see a success window. Click OK.

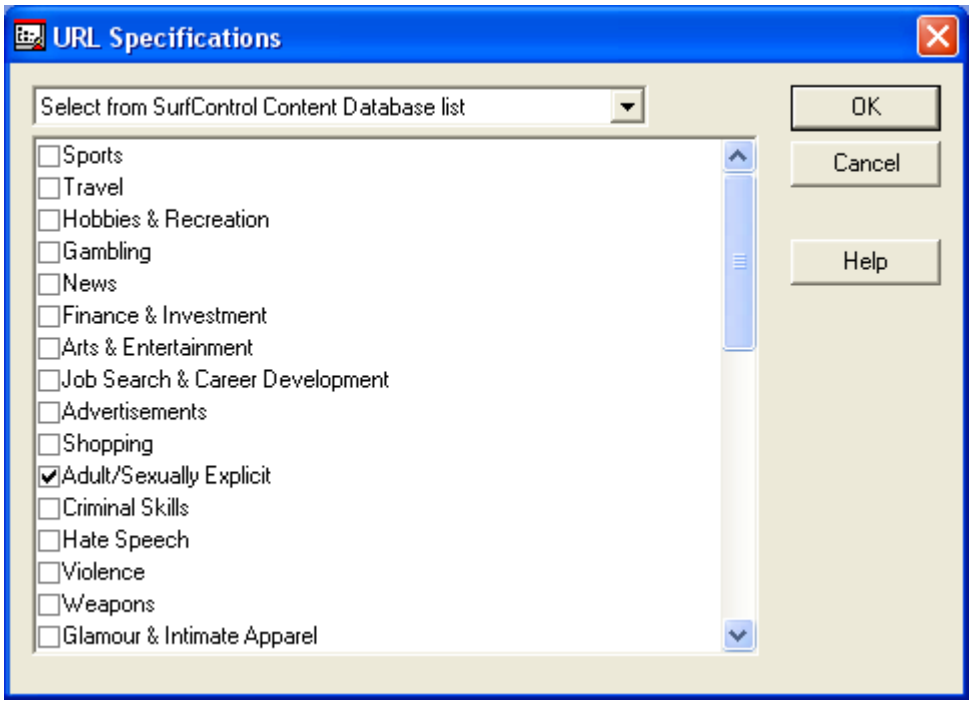
Note I have seen a number of cases where the registration program did not succeed because it needed to contact SurfControl, and filtering on BorderManager blocked the request. I have often resorted to simply unloading IPFLT on the BorderManager server to get the registration program to work, then immediately loading IPFLT again.

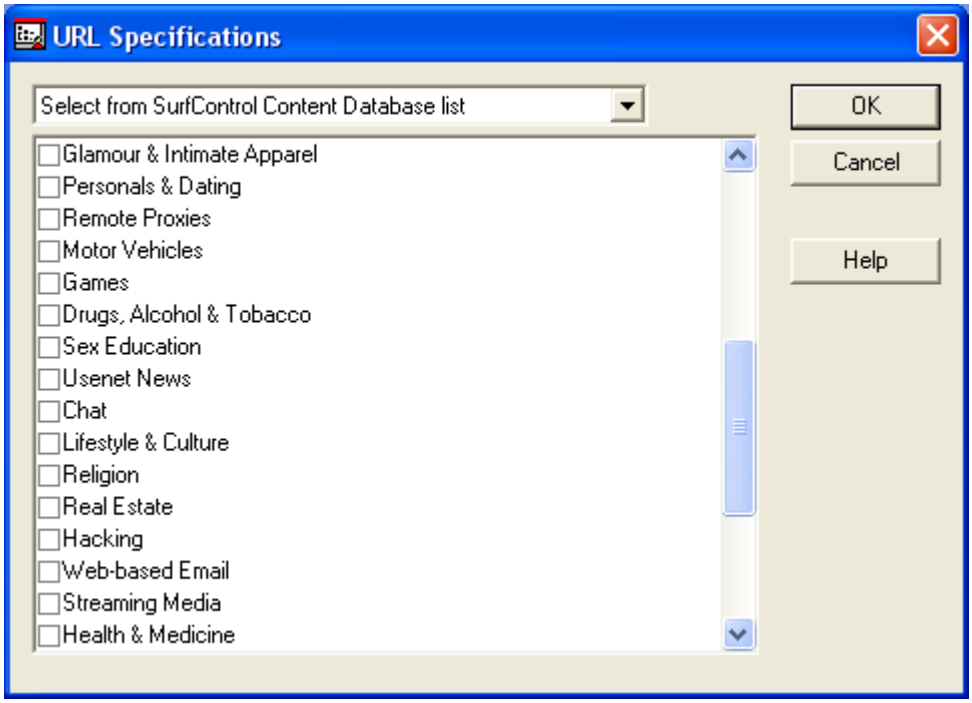
Next UNLOAD CPFILTER.NLM, then LOAD CPFILTER again.

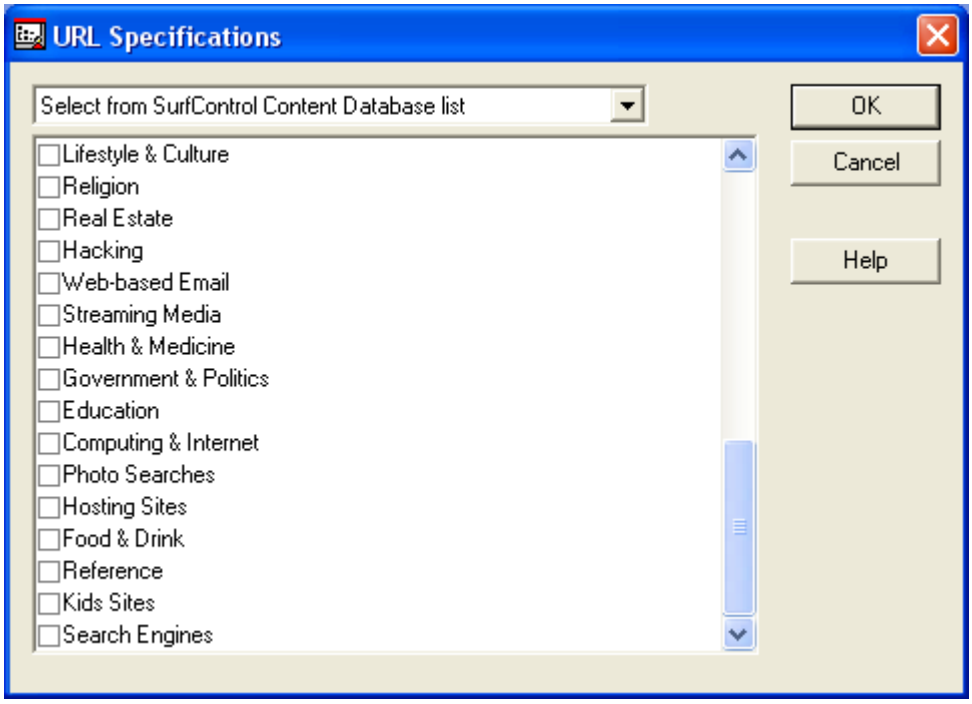
You can use LOAD CSP_LIST.NLM to update the SurfControl database once you have registered SurfControl. CSP_LIST will automatically load CPFILTER if necessary.

CSP_LIST will automatically attempt to update the SurfControl database when you run it, but the process may take several minutes to more than a day, depending on the number of version updates it needs, and your Internet bandwidth.

Now you should be able to see many more categories to choose in a SurfControl Access Rule. (Service Pack 3 categories shown – previous versions do NOT include all 40 categories).







Note the last 8 categories – if you do not see them, you need to download and install Service Pack 3 (or later) of SurfControl.

Updating SurfControl

Unlike CyberPatrol, SurfControl does not automatically update itself. Instead, you must launch the SYS:\ETC\CPFILTER\CSP_LIST.NLM module when you want an update to occur.

The CSP_LIST process can be somewhat lengthy, and it can result in the CPFILTER.NLM doubling its RAM usage at some point during the update, if SurfControl Service Pack 2 or later is not installed. For this reason, it may be useful to have full control over the scheduling of the updates.

CSP_LIST will unload itself when the SurfControl update process is completed.

There are several ways to schedule when CSP_LIST runs. This book covers two of them: CRON, and Scheduled Tasks.

SurfControl Memory Usage During Updates

When the CSP_LIST update program is running, and the update process can take hours, memory usage can be much higher than normal. This is because the CPFILTER.NLM will **double** its memory size during the update process, if not using SurfControl Service Pack 2 or later.

A new, temporary database is created in the CPFILTER directory. Changes to the database are downloaded and merged into the temporary database. Eventually, the temporary database is up-to-date, and it is loaded into memory at the same time as the old database is in memory. (This is when CPFILTER actually needs twice as much RAM as usual). Once the new database is loaded into RAM, the old database can be unloaded, and CPFILTER shrinks back to normal size in RAM. This process allows the update to occur without blocking (or allowing) browsing. It is the swap-from-RAM method. If you install SurfControl Service Pack 2 or 3 version, the default setting is to swap-from-disk. The same temporary files are created, but instead of holding the updated database in RAM, it is held on disk and swapped from disk. This swap process is slightly slower that the swap-from-RAM process, and your browsing could be denied during the swap process. However, the swap-from-disk method has the huge advantage of not doubling the RAM usage (up to 700MB required), and risking RAM fragmentation issues.

Reducing SurfControl RAM Requirements

Because the CPFILTER.NLM can take up quite a bit of RAM (I saw 183MB in normal usage with SurfControl Service Pack 1, on my server, twice that during the update process), you must have much more RAM available on the server than was previously required

with CyberPatrol. As the database was updated day after day, it constantly grew, until I needed to reserve 300MB of RAM for the database to load. With SurfControl Service Pack 2 or 3, the initial RAM reservation is increased to 350MB, but it does not double in use during updates by default.

Setting the swap-from-RAM or swap-from-disk behavior is done with a command in the cspconfig.ini file, after Service Pack 2.

However, there is a way to reduce the memory usage when CSP_LIST runs, even if you are not using Service Pack 2 or later.

This technique involves preventing the doubling of the RAM usage by CPFILTER during the update process. If you unload the BorderManager modules (STOPBRD.NCF), before loading CSP_LIST, then CPFILTER should not use more than its normal amount of RAM. This may be an option for some environments, by scheduling the process to occur at night, or over a shutdown period on a weekend.

SurfControl Disk Space Usage During Updates

The SurfControl content database file (SYS:\ETC\CPFILTER\SurfControl Categories.cdb) starts out quite large, at over 100MB in size. During the update process, at least one temporary copy of that file is created, along with numerous other files. The total disk space used during the update process may triple temporarily, to over 300MB.

Updating Through A Cache Hierarchy / Upstream Proxy

With SurfControl Service Pack 2, you can update the SurfControl database through an upstream proxy server. You must add the following commands to the CSPCONFIG.INI file:

[SurfControlGeneralList]
UseProxy=1
ProxyServer=<Proxy Server IP address>
ProxyPort=<Proxy Server Port Number>
ProxyName=<Proxy User ID> - (Optional, used if you have to authenticate to the upstream proxy server)
ProxyPassword=<Proxy Password> - (Optional, used if you have to authenticate to the upstream)

See the SurfControl Administrator Guide for more details. That guide can be found online at the SurfControl web site.

Scheduling SurfControl Updates

Because CSP_LIST does not run automatically, the system administrator will have to load it manually, or use some scheduling program to load it periodically (usually in the middle of the night). Here are three different methods of scheduling an update.

Using CRON to Schedule SurfControl Updates

CRON.NLM is a scheduling program ported from UNIX. When running, it 'wakes up' every minute, looks for any commands in the SYS:\ETC\CRONTAB file to execute, and then 'goes to sleep'. The key to using CRON is having the correct syntax of commands in the CRONTAB file. See this Novell TID 10024685 for information on using CRON.

The following CRONTAB file should result in the CSP_LIST command being run once per day at midnight.

```
# Syntax is MINUTE - HOUR (0-23) - DAY-OF-MONTH - MONTH - DAY-OF-WEEK
# See Novell TID 10024685
# Use settings in SYS:\ETC\CRONTAB, and LOAD CRON.

# Load CSP_LIST at midnight each day to update SurfControl database
0 0 * * * SYS:\ETC\CPFILTER\CSP_LIST
```

If you plan on using the CRON method, be sure CRON is loaded in AUTOEXEC.NCF

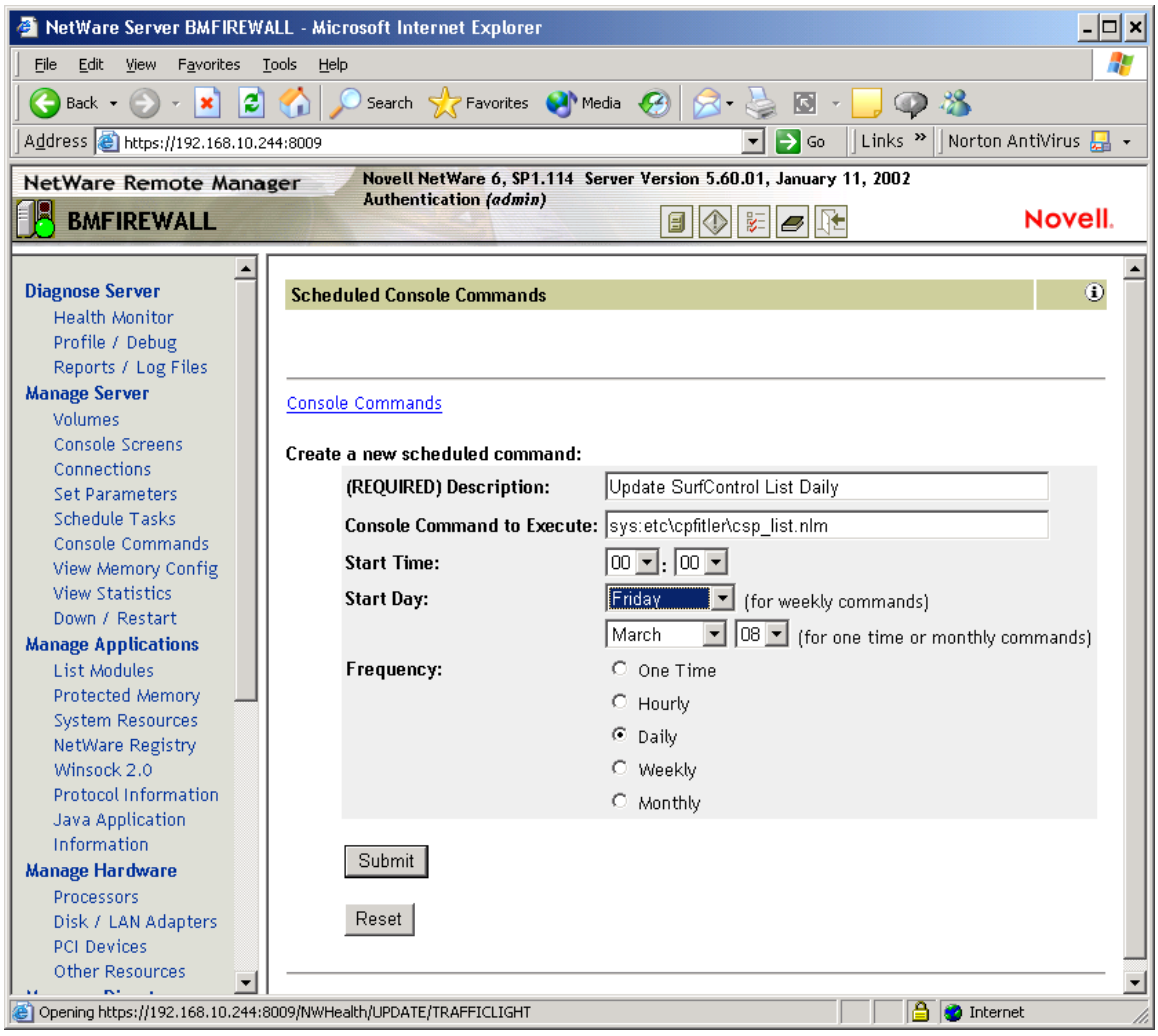
You may have to add CRON.NLM to a NetWare 6.5 server. You should be able to download a copy in the CRON5.EXE patch from http://support.novell.com.

Using Scheduled Tasks to Schedule SurfControl Updates

An alternative method for scheduling commands to run, or files to load, is to use the Scheduled Tasks feature in Remote Manager. In this method, commands are stored in the NetWare Registry files (files kept in the DOS NWSERVER directory, and not directly editable).

Start your browser, and start a HTTPS session on port 8009 to your BorderManager server's private IP address. In this example, the BorderManager 3.7 server is located at IP address 192.168.10.244.

Point your browser to https://192.168.10.252:8009 and log in to NDS. You should then see the Remote Manager options. In the left column, you should see a link called Schedule Tasks. Select it.



Provide a description, such as "Update SurfControl List Daily". The console command you want to execute is "SYS:\ETC\CPFILTER\CSP_LIST.NLM".

Select a schedule frequency and start time that suits you. The example shown above will load CSP_LIST once per day at midnight. (CSP_LIST unloads itself when it completes its work).

Note Remote Manager works best when using Internet Explorer. While Netscape will work to some extent, I found in my testing that my previously scheduled tasks sometimes did not show up near the top of the screen unless I used Internet Explorer.

Using TaskMaster to Schedule SurfControl Updates

To automate this task using the TaskMaster Server Batch Processor, Task Scheduler, Console Shell and Data Replication/Synchronization utility from Avanti Technology, Inc. (http://www.avanti-tech.com)

If not already installed, install TaskMaster or TaskMaster Lite as instructed in the TaskMaster User's Guide or via the TaskMaster Setup utility and load the TaskMaster NLM.

Create an ASCII text file using Notepad or your favorite text editor and write the command to be executed:

LOAD CSP_LIST

Save the text file (usually naming it something associated with the task type and using an extension .TSK to signify it is a TaskMaster Task script). Be sure to save the text file either in the SYS:SYSTEM directory or the directory from which the TaskMaster NLM loads (by default, SYS:\SYSTEM\TASKSMSTR).

Note: The directory restriction is for security purposes to limit the location of tasks which can be scheduled and executed by the TaskMaster batch processor.

Toggle the Server Console screens (using the Alt-ESC key combination) to the TMConsole (Shell) screen. At the prompt TMConsole (Shell) prompt, enter the following command:

```
TMSCHEDULE ADD [dos_name.ext] 00:00 YYYYYYY
```

Replace the [dos_name.ext] with the DOS name of the text file created above (no drive, volume, or path specification needed). The field following the file name is the time the task should execute (in military form: 00:00 - 23:59) and the final field is the days of the week the task should execute (weekdays, Sunday through Saturday with 'Y' or 'N' entries).

Tasks can also be scheduled for execution on specific dates, specific days of the month, at specific minutes after each hour, and at intervals. To verify proper scheduling of the task, enter the following command at the TMConsole (Shell) screen prompt:

```
TMSCHEDULE
```

The TMSCHEDULE command will display a list of all currently scheduled tasks and those tasks that are scheduled to execute today.

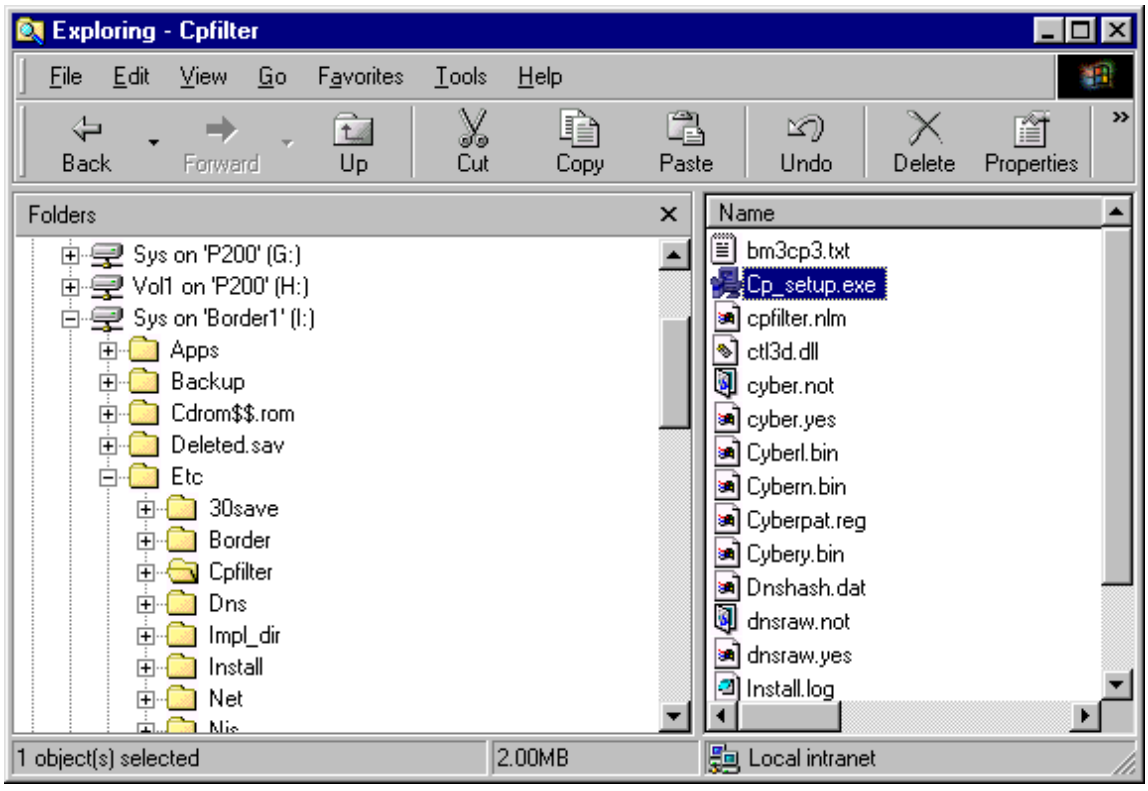
CyberPatrol

CyberPatrol was included with BorderManager 2.1 through 3.6. There have been some updated versions available in certain patches, but the basic functionality and use is identical among all versions.

CAUTION *As of mid-2003, CyberPatrol updates have halted by SurfControl. You must upgrade to SurfControl to get filtering capability from SurfControl now.*

CyberPatrol is fairly old technology, and can hold only about 64,000 sites in its CyberNOT list. (The newer SurfControl version of CPFILTER.NLM holds over 3 million).

CyberPatrol Access Rules (CyberYES list and CyberNOT list) depend on the proper installation and registration of the CyberPatrol version of the CPFILTER.NLM



To initially install the NLM, one must first run the SYS:\ETC\CPFILTER\CP_SETUP.EXE program in Windows. This program will create several other files in the same directory, including the CPFILTER.NLM file.

Now, in the BorderManager AUTOEXEC.NCF file, add the line LOAD SYS:\ETC\CPFILTER\CPFILTER directly after the LOAD BRDSRV line.

Registering CyberPatrol

Once the CP_SETUP.EXE program has been run, you must run the REGISTER.EXE program in the same directory in order to input registration codes to enable the program for more than 45 days.

Unless the registration process is completed, CPFILTER will only work properly for 45 days. At the end of the 45-day evaluation period (or when the registration time frame expires once CPFILTER has been registered), CPFILTER will not download any additional CyberYES or CyberNOT list data. However, It will continue to function with whatever list data has been already been downloaded.

To Register CyberPatrol's CPFILTER, you need to have serial number codes from Microsystems (CyberPatrol). These codes are tied to a 16-digit serial number, which you must call Microsystems to get

BORDER1's serial number is not shown. This serial number must appear in the REGISTER.EXE Serial Number field, along with BORDER1 (uppercase) in the Registered Owner field. The unlock codes given to you by Microsystems are keyed to the combination of the serial number and registered owner.

If a new version of CPFILTER is needed, it can be found in the cp-setup.exe program available at ftp://ftp.microsys.com/cyber/novell. You should first check to see if a newer version is available from the Novell Minimum Patch list (at http://support.novell.com) as a patch coming from Novell should have been more thoroughly tested.

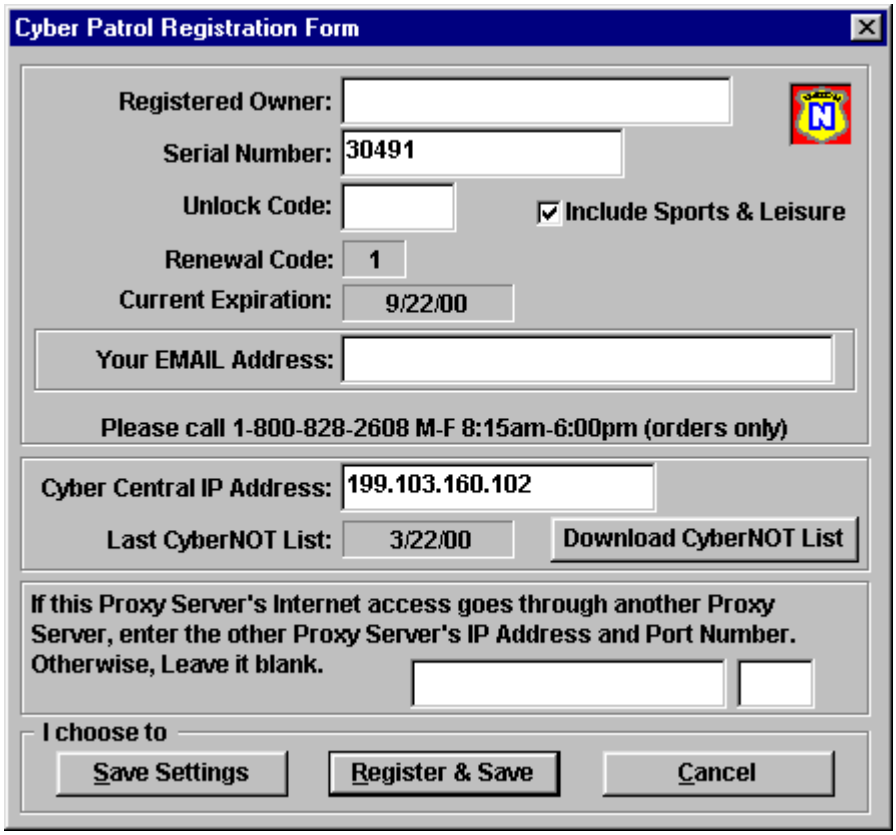
Note For BorderManager 3.0 and 3.5, a newer version of cpfilter.nlm than that included on the installation CD is available from the Minimum Patch List at http://support.novell.com. You should install the newer version before configuring CyberPatrol for the first time to avoid duplication of effort.

If a new version is to be installed, you should first delete all the old files in SYS:\ETC\CPFILTER. Next copy the new CP-SETUP.EXE file to the SYS:\ETC\CPFILTER directory, and run the CP-SETUP.EXE program to extract the new files. When prompted for a drive letter, mapped to BORDER1\SYS:\, use F, but not F: (do not include a colon). The REGISTER.EXE program will then automatically run, and you can type in the required data. To get a new serial number and unlock codes, call CyberPatrol at 1-617-761-1350. Type in the correct data and the unlock code and click on Register & Save.

CyberPatrol updates are downloaded daily, and every 10 days, a completely rebuilt list is downloaded.

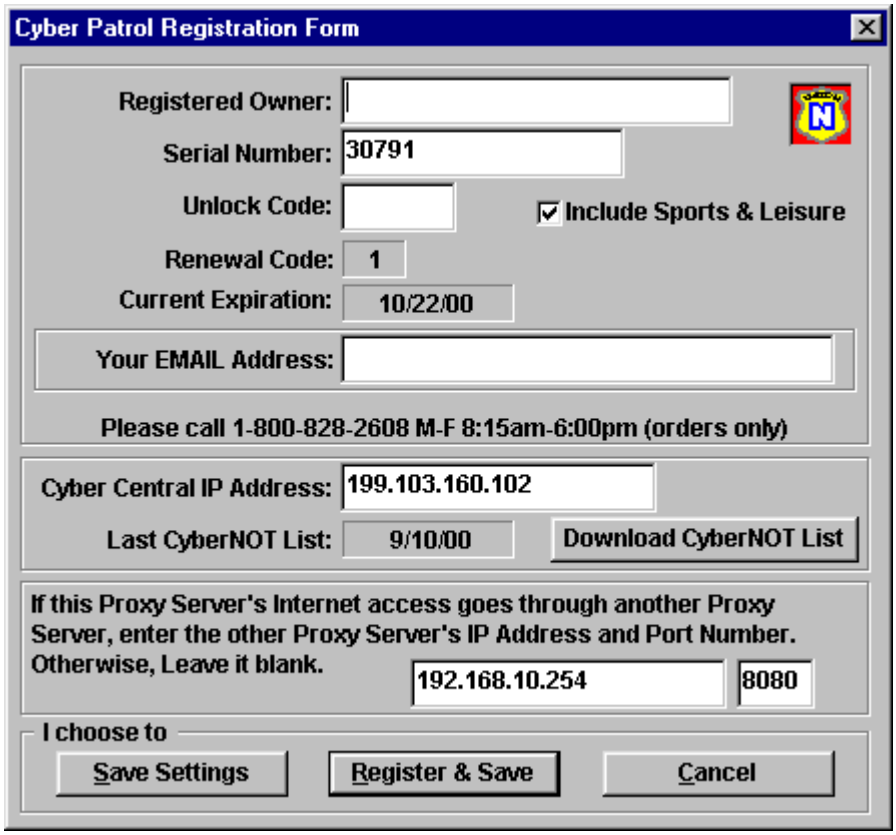
The CyberPatrol REGISTER.EXE Program

Run the REGISTER.EXE program from the SYS:\ETC\CPFILTER directory.



This screen shot shows the unregistered settings. The unlock codes are provided over the phone from CyberPatrol, and they are tied to the server's IP address/port number and server name (Registered Owner). Changing any of these settings requires CyberPatrol to provide new unlock codes.

The Proxy Server field is only used if the path to the Internet from the BorderManager server has to go through an upstream proxy. Consider the following example:



This example shows that in order for the CyberPatrol updates to be downloaded, another CERN proxy server at 192.168.10.254 using port 8080 is to be used. In this case, the CPFILTER.NLM program will send a request to the upstream proxy just like a browser normally accesses the BorderManager HTTP Proxy.

The upstream proxy can be any CERN proxy, not just a BorderManager server.

Downloading a New CyberNOT List On Demand

You can run the SYS:\ETC\CPFILTER\REGISTER.EXE program and click on the Download CyberNOT List button to schedule a new download of the latest CyberNOT list. Once you click on the button, a new CyberNOT list is supposed to be downloaded within an hour.

In order to download a new CyberNOT list more quickly, you must click on the Download CyberNOT List button in the register.exe program, then, at the server console, type UNLOAD CPFILTER, followed immediately by LOAD SYS:\ETC\CPFILTER\CPFILTER. This is supposed to prompt an immediate (within one hour) download of the latest list.

N2H2

How N2H2 Works

Unlike SurfControl, which runs completely on the BorderManager server, as of this writing N2H2 Sentian Category Server runs only on RedHat Linux (version 7.2) and Windows 2000 Advanced Server. By the time you read this, other options may be available.

The N2H2 Sentian Category Server is basically a database or IP addresses, URL's and categories. Sentian can be configured to update its database periodically from N2H2. Proxy hosts, such as BorderManager, send requests to the Sentian server for URL's or IP Addresses, and receive back one or more categories for that URL. BorderManager then examines the category to see if it is to be allowed or denied in the Access Rules, and acts as needed.

Sentian updates itself using HTTP. You will need to set some means of allowing Sentian to gain access to the N2H2 update servers without proxy authentication. (See the following example for a way of doing that through HTTP proxy). Sentian can be configured to use HTTP Proxy, or you could set up filter exceptions to allow the required traffic.

You can contact N2H2 to get a 30-day evaluation of either the Windows or RedHat Linux software. You start by filling out a form on the N2H2 web site. When I got the software in the summer of 2002, I found that you could not directly download the software, not did I get a URL via email. It appears that you must provide a valid telephone number, and allow an N2H2 sales engineer contact you in order to actually get the evaluation software. Hopefully that has changed by the time you read this.

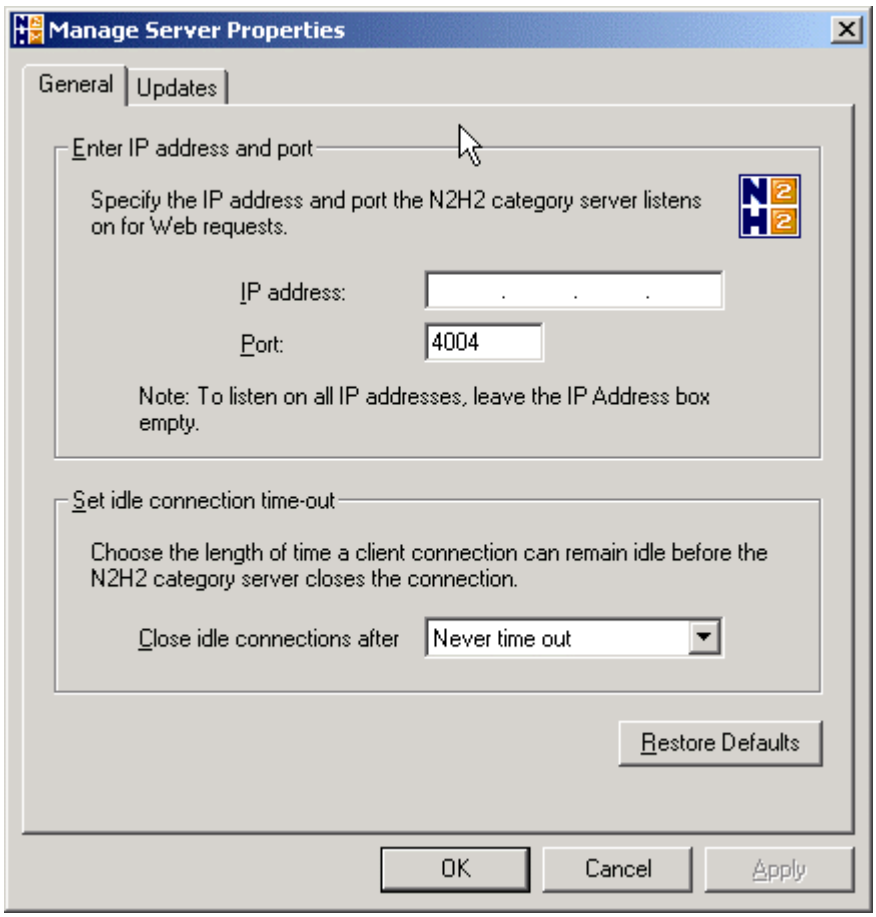
N2H2 Configuration on Windows 2000 Advanced Server

First, install N2H2 Sentian Category Server on either Windows 2000 Advanced Server or RedHat Linux 7.2. This example shows only Windows 2000 Advanced Server. I attempted to installed the Linux version on RedHat 7.3, as that was all that I had at the time, and I could not get the software to run.

The installation program for Sentian on Windows is straightforward. Simply run the setup program and take the defaults. Once you have installed the software, you must configure it.

Select **Start Menu**, **Programs**, **Sentian**, **Sentian.**

General Menu



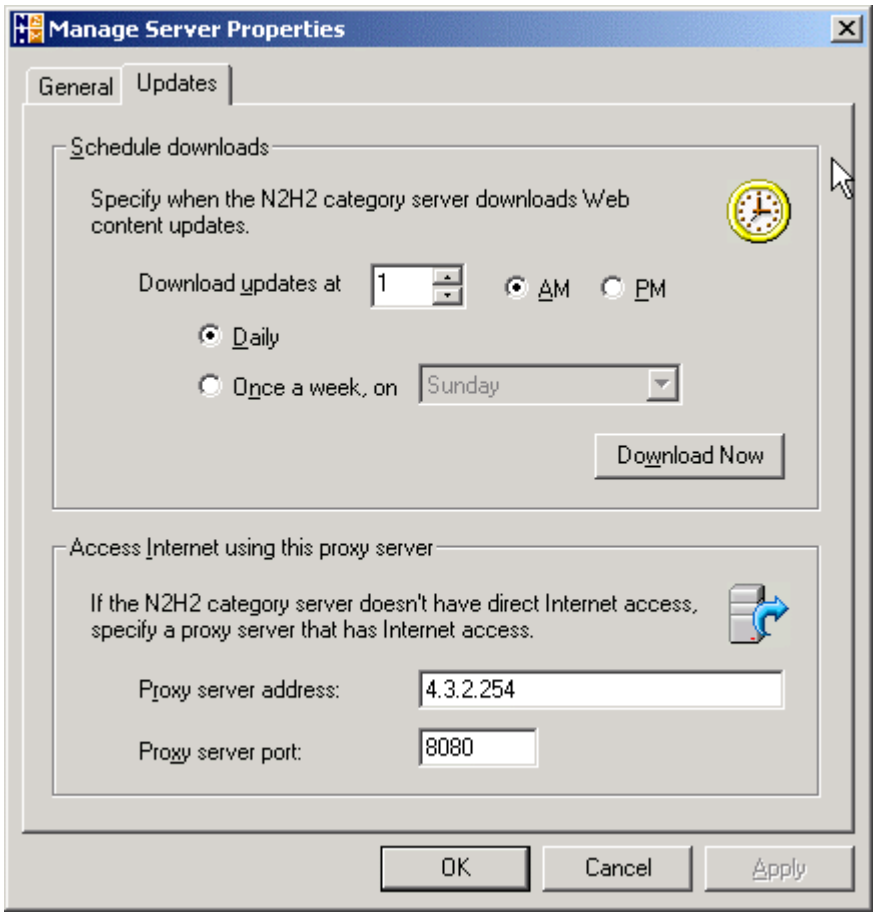
Do NOT fill in the IP address – leave it blank! (When I filled in the IP address with the address of the server, BorderManager timed out requests to the N2H2 server. I have no idea why this peculiar behavior occurred).

The port number used needs to match the port number configured in the BorderManager server Access Rules menu. Oddly enough, the port number default is different between the Sentian Linux and Windows versions, being 4000 for one and 4004 for the other. Just be sure you match both Sentian and BorderManager port selections.

Set **Close idle connections after** to **Never time out**.

Updates Menu

Select the Updates menu to configure how the N2H2 Sentian Category server updates categories automatically.

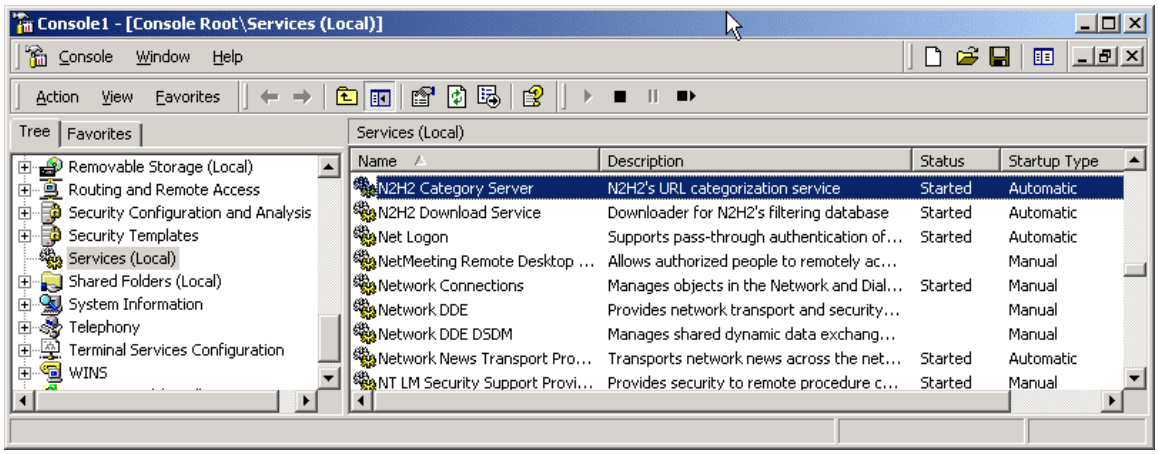


You can configure N2H2 to update itself daily at a particular time, or once per week.

If the N2H2 server is behind the firewall, it can be configured to use the HTTP Proxy in order to update itself with new URL lists. If you do not configure an HTTP Proxy, the N2H2 server needs to be able to access the N2H2 servers using TCP destination port 80. Basically, this means you either set up filter exceptions to allow port 80 out from the N2H2 server's IP address, use Transparent Proxy, or use HTTP Proxy. Should you configure N2H2 to use a proxy, you must also have the appropriate access rules to allow N2H2 Sentian Category server to access the N2H2 servers. (Just set up an access rule allowing the N2H2 server to access any URL. See the following section if you have Proxy Authentication enabled).

Windows 2000 Services Configuration

Using the Microsoft MMC, you can access the Services menu for your Windows server.



The N2H2 Sentian Category Server program installs itself to run as a service. The update process also runs as a service. You may have to configure both services to start automatically.

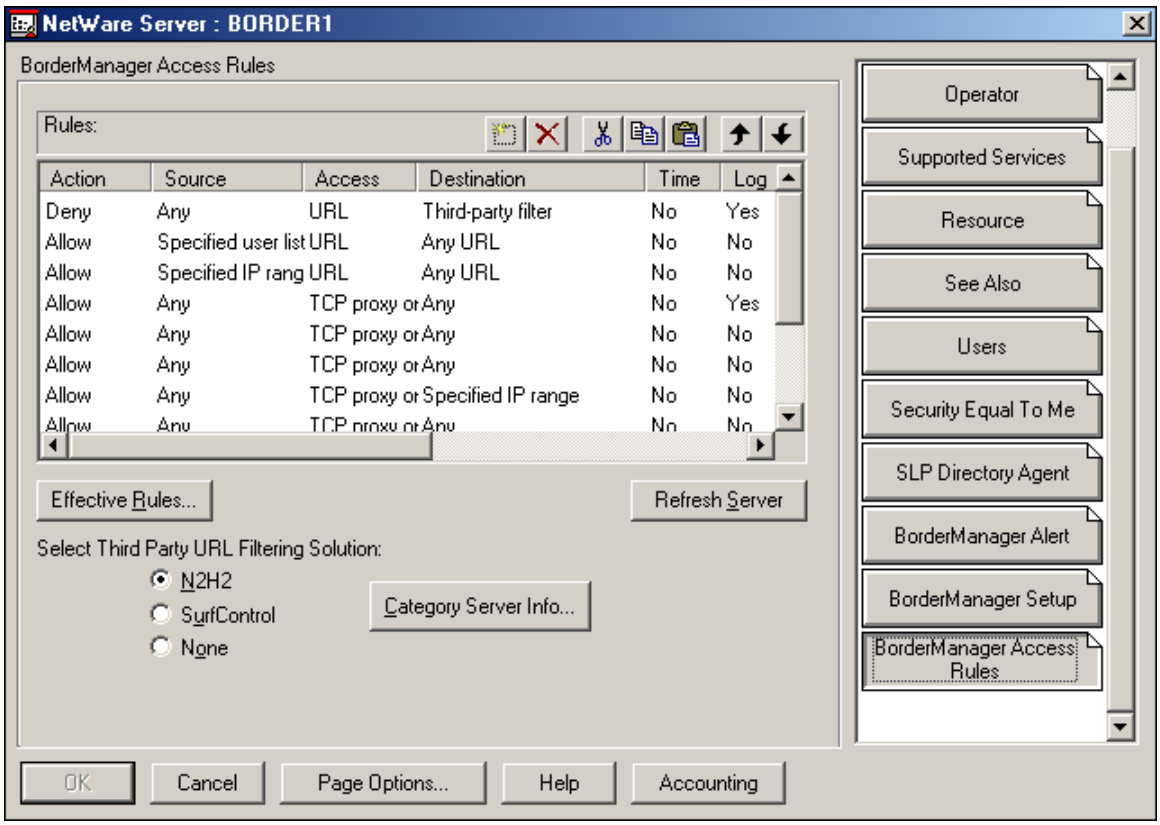
BorderManager Configuration for N2H2

The BorderManager server needs to be able to access the N2H2 Sentian Category Server using TCP on the specified port number. The default port number for Sentian Category Server is 4004 for Linux and 4000 for Windows 2000. (You can change the port number as needed).

If the N2H2 Sentian Category Server is located on the private side of the BorderManager server, you should not need to add any filter exceptions for the BorderManager server to communicate with the N2H2 server. However, the Sentian Category Server needs to contact N2H2 using HTTP in order to update its database of URL's. You can configure the N2H2 server to use port 80, or you can have it use the HTTP Proxy (normally using port 8080). If you use port 80 (no proxy), set up a stateful filter exception on the BorderManager server allowing outbound HTTP.

The BorderManager server needs to be version 3.7 or later, with the BM37N2H2.EXE patch (or later) installed. The BM37N2H2.EXE patch allows you to configure access rules to use either SurfControl or N2H2, but not both at the same time.

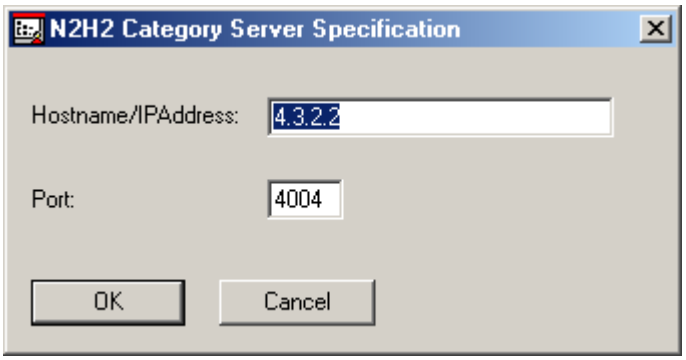
Once the proper patch is installed on BorderManager 3.7, the Access Rules menu will have configuration entries for Third Part URL Filtering Solution as shown below:



To configure SurfControl access rules, select the SurfControl option and enter access rules as desired for SurfControl as shown elsewhere in this book.

Configure Category Server Communications

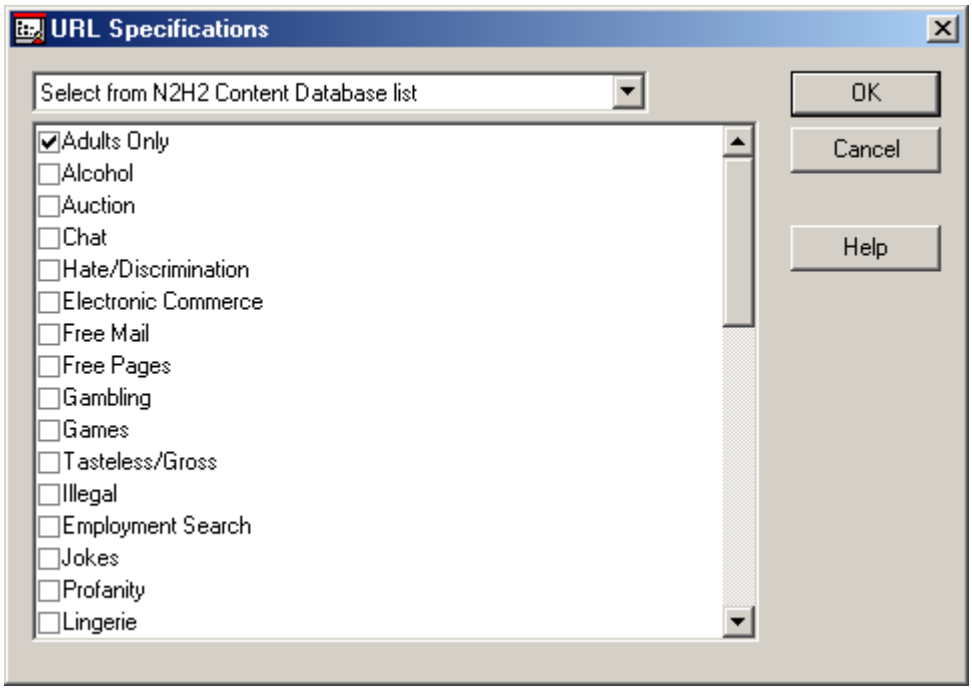
To configure N2H2 access rules, you must select the N2H2 option, and then configure N2H2 parameters by clicking on the Category Server Info menu button in the BorderManager Access Rules menu.

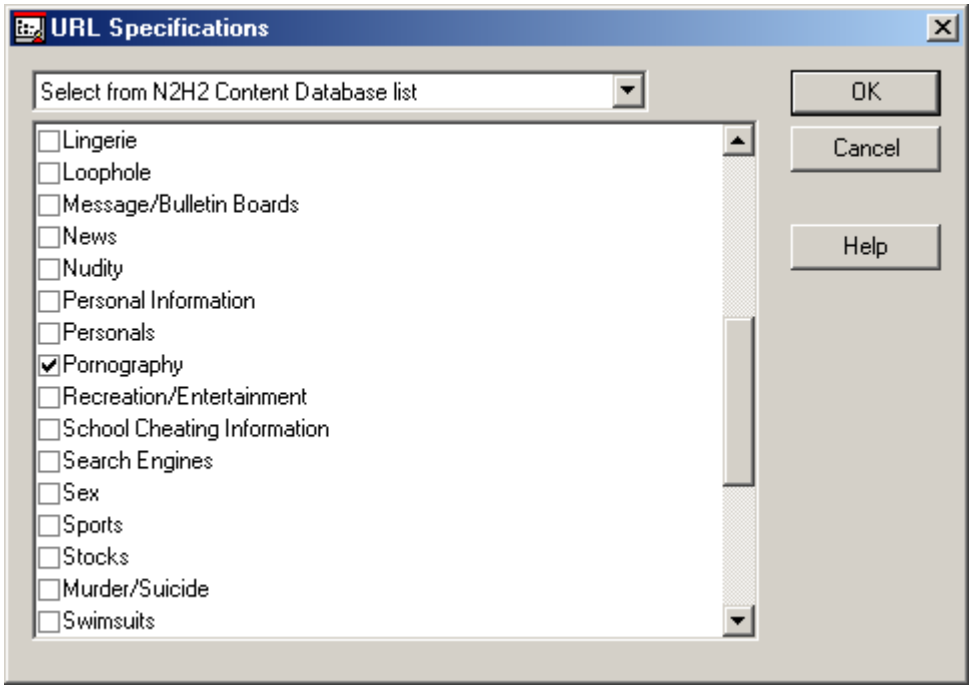


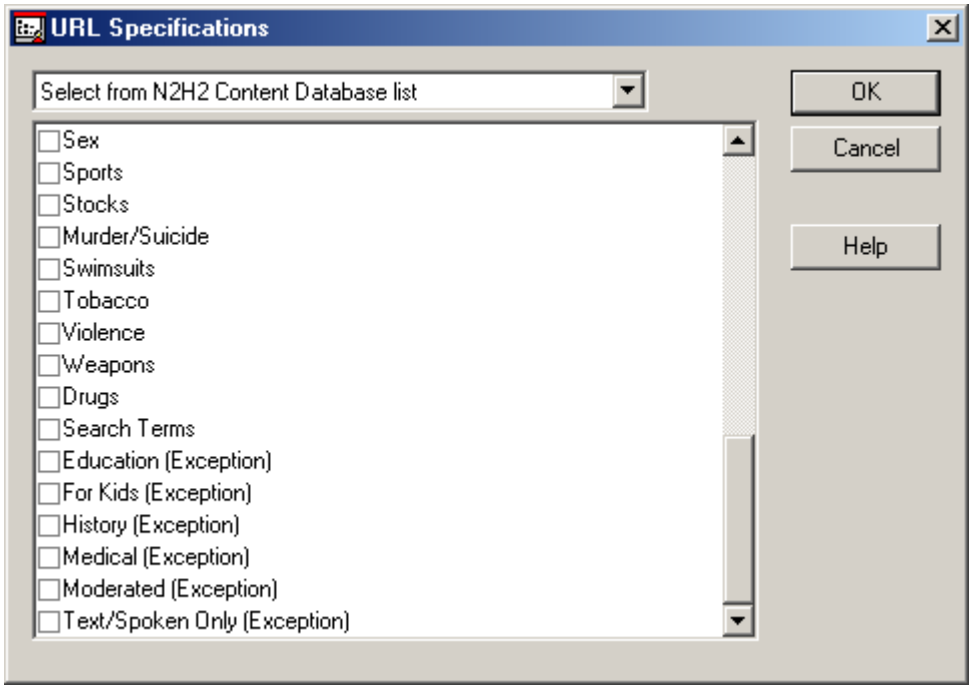
Clicking on the Category Server Info menu button as shown above allows you to configure the IP address of the Sentian Category Server as well as the port number used for communications between the BorderManager server and the N2H2 Sentian Category Server. Be sure the BorderManager port number matches the port number configured on the Sentian server.

BorderManager will then send data to the Sentian Category Server at the at the selected IP address and port number, using TCP protocol.

N2H2 Sentian Category Server selection list







The screenshots above show the options available in a N2H2 content database access rule, with a couple of categories selected.

Note the six exception categories at the end of the N2H2 content database list. Checking these options in a Deny rule allows those categories rather than denies them. These options are most useful in an educational environment.

LinkWall

LinkWall is a content filtering product from Connectotel (http://www.connectotel.com) that is designed to create an access rule from a text file list of URL's. Besides the obvious fact that you could put together your own list of URL's and easily create an access rule from them, you should know that there are free URL blacklists available for download on the Internet. LinkWall can directly import these lists in many cases. Specifically, LinkWall can import the Squidguard Blacklist. Blacklists are categorized lists of URL's and IP addresses that are used with Deny URL rules. (LinkWall can be used with Whitelists as well). The most common use of blacklists in the United States is for blocking pornography sites.

LinkWall also has a bit of integration with the RTMonitor program/ (RTMonitor is described elsewhere in this book). RTMonitor has the option to immediately add some URL you select in the display to a LinkWall-monitored file, and refresh LinkWall. This effectively means you can see where people are browsing, and block the sites almost instantly, with a few mouse clicks.

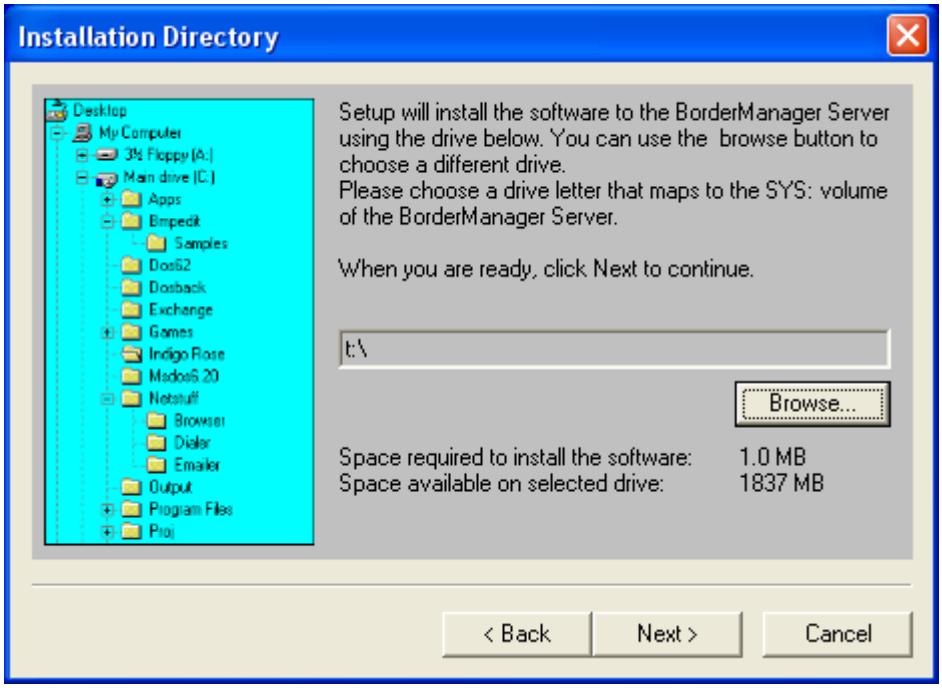
One advantage LinkWall has over SurfControl and N2H2 is that those products charge a yearly licensing fee, while LinkWall can make use of free blacklists. However, the free blacklists may not be as extensive or updated as often as SurfControl or N2H2 data. In addition, you have to manually download updated blacklists, although Connectotel is working on an automated download system as of this writing. Another advantage is that LinkWall will run on a BorderManager 3.5, 3.6, 3.7 and 3.8, whereas SurfControl and N2H2 run only on 3.7 and 3.8.

Note LinkWall has gone through multiple versions since the first mention in this book. When BorderManager 3.7 came out, a new version of LinkWall was required to run properly, and that version contained particular settings in various configuration files that you had to set manually on BorderManager 3.7 servers. The latest version as of this writing (ver. 1.26b), installs correctly on BorderManager 3.8 and earlier, without you having to adjust the LinkWall configuration files.

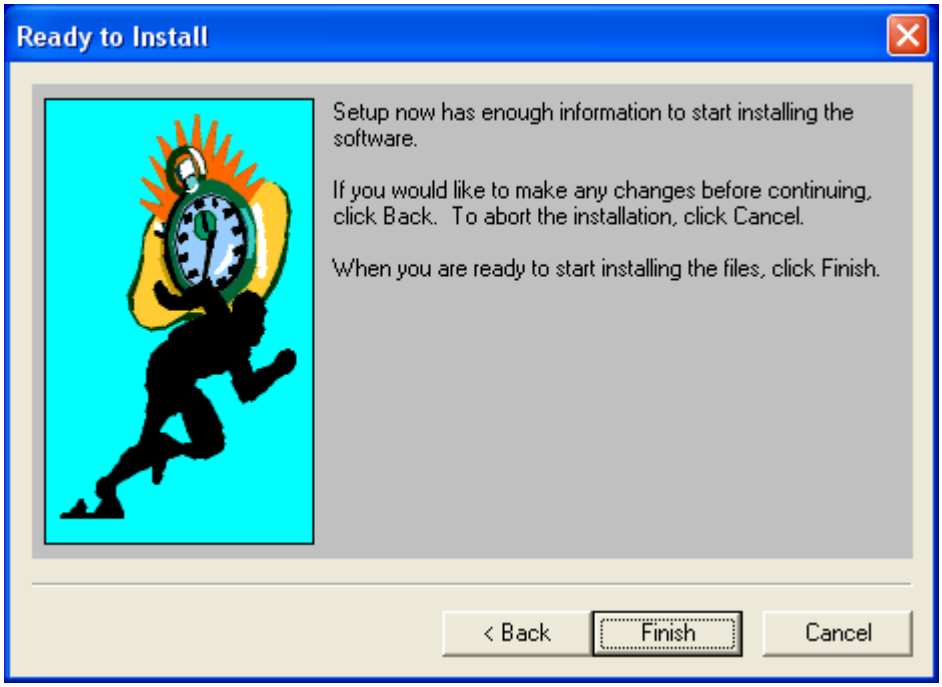
Installing LinkWall

Download the LinkWall installation file from Connectotel's web site. Launch the executable file LINKWALL.EXE from a Windows PC that has a drive letter mapped to the SYS volume of a BorderManager 3.x server. The following example shows LinkWall version 1.23a being installed to a BorderManager 3.8 / NetWare 6.5 server.

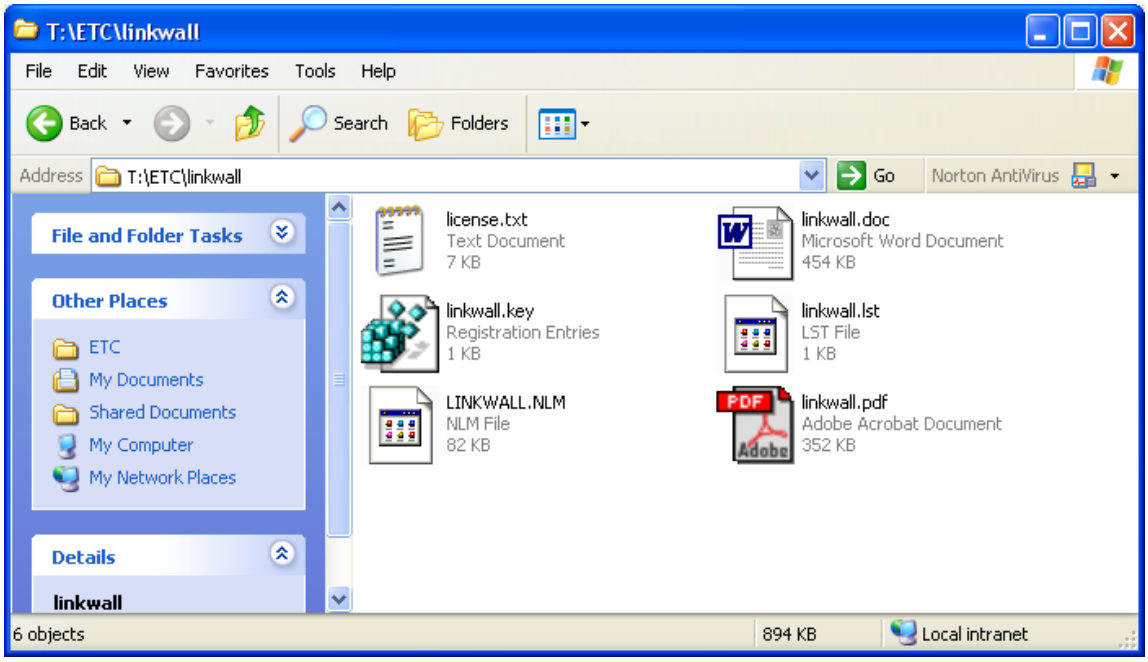
When you launch the LINKWALL.EXE executable, the setup program runs. Have a drive letter mapped to the SYS volume of the BorderManager server, and click **Next** to continue.



Set the drive letter for the BorderManager 3.x SYS volume and click **Next**.



Once you have selected the drive letter of the BorderManager 3.5, 3.6, 3.7 or 3.8 server, click **Finish**.



A number of files should be extracted and copied to the SYS:\ETC\LINKWALL directory…

…and you should get a final setup menu. Click on **Finish** to exit the installation process.

To use LinkWall, you must:

- Edit the LINKWALL.LST file, either in NWADMN32 or a text editor. This file tells LINKWALL what to filter, unlike CyberPatrol, SurfControl or N2H2. You can either add URL's into the LINKWALL.LST file or tell LinkWall to point to other files with lists of URL's.
- Edit the LINKWALL.NCF file with startup options to enable logging to screen or file, if desired.
- Start LinkWall by running the LINKWALL.NCF file. You should add a command to AUTOEXEC.NCF to start LinkWall when BorderManager starts. With BorderManager 3.7 or 3.8, you should add the command to the STARTBRD.NCF file, and add an Unload Linkwall command to the STOPBRD.NCF file.
- Add an Access Rule to make use of LinkWall.

Documentation for the LinkWall program is included in the SYS:ETC\LINKWALL directory.

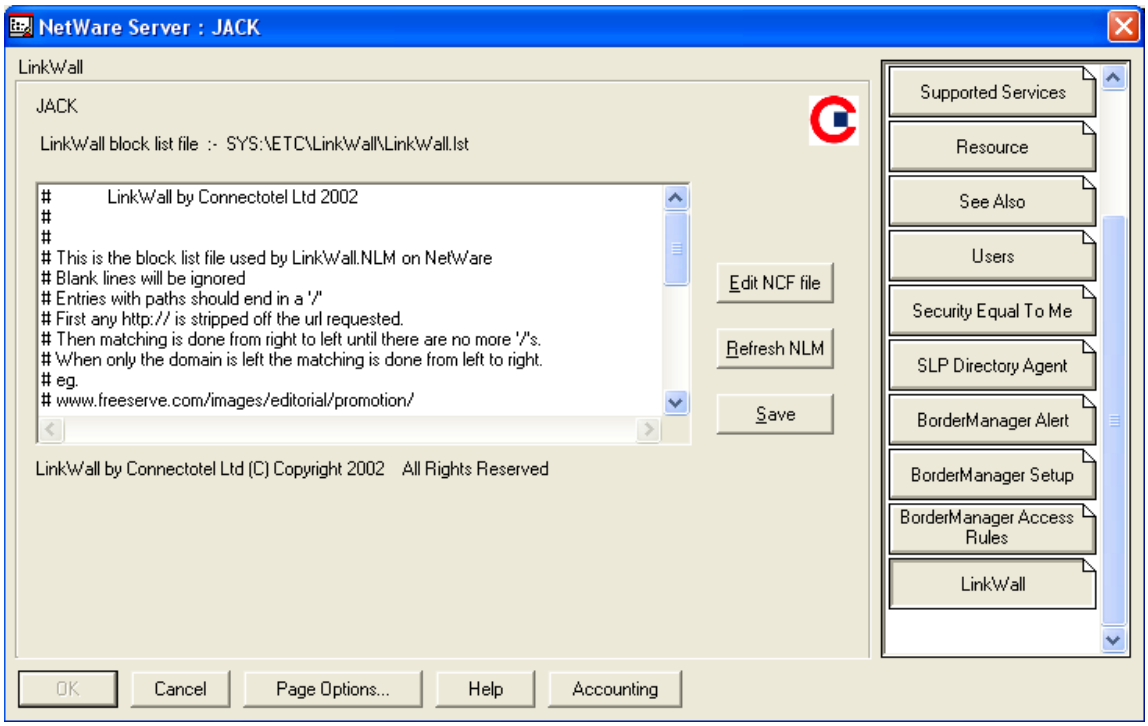
Note Once you are running LINKWALL.NLM, you should always unload it before trying to unload PROXY.NLM.

LinkWall Configuration In NWADMN32

LinkWall URL lists are controlled by entries in the SYS:\ETC\LINKWALL.LST file. You can edit the file with any text editor, or you can use the LinkWall tab in NWADMN32.

Launch NWADMN32, from the BorderManager server with LinkWall installed.

In NWADMN32, Select the BorderManager server object that has LinkWall installed.

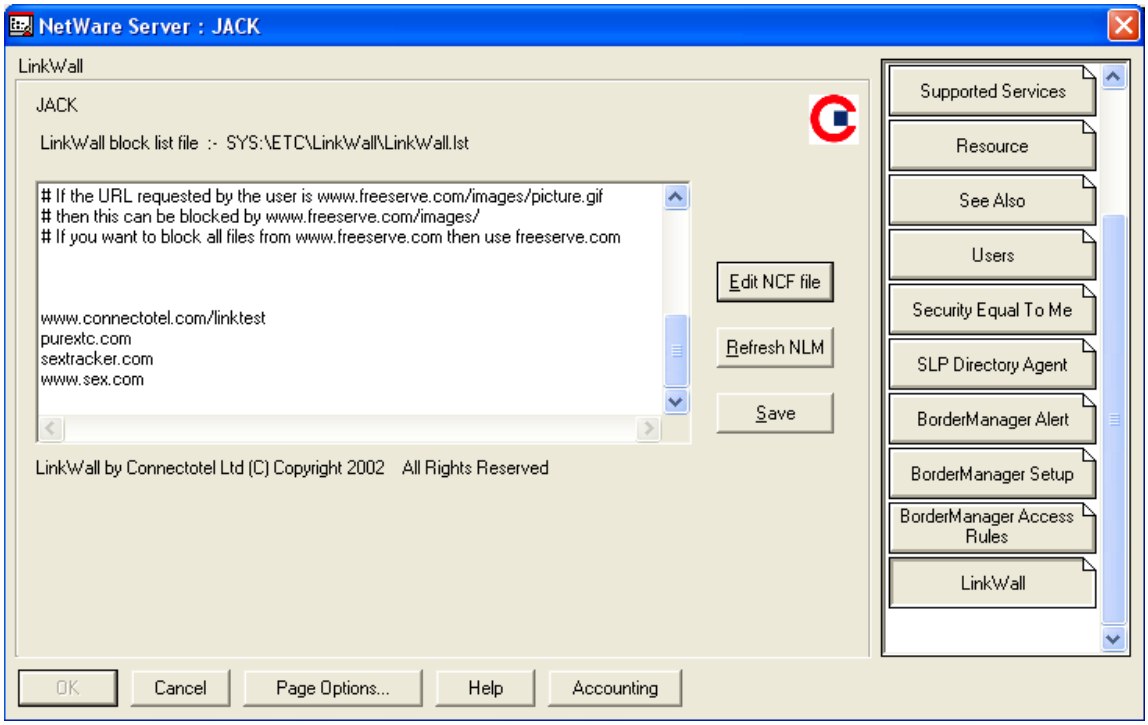


If the LinkWall snapin is installed on the server, you should have a LinkWall tab on the server object.

The button for Edit NCF file will allow you to edit NCF file settings to start LinkWall with optional logging settings.

The button for Refresh NLM will stop and restart LINKWALL.NLM to pick up new configuration settings.

The Save button saves edits to the LINKWALL.LST file, which is shown in the window to the left of the buttons.



The screenshot above shows the LINKWALL.LST file after scrolling down to the end of the menu.

LinkWall normally reads all entries in the SYS:\ETC\LINKWALL\LINKWALL.LST file. These entries are shown in NWADMN32. You can edit them directly by typing into NWADMN32 at this point. You can also edit the LINKWALL.NCF file, which is done by clicking on the Edit NCF file button.

The LINKWALL.LST file can contain URL's to be filtered, and it can also contain links to other files that have URL's to be filtered.

In the example shown above, I have configured LinkWall to include two additional files of URL's to filter, using the $include command.

The $include command tells LinkWall to read another file for additional URL's to filter.

In the example, I have pointed LinkWall to the SYS:\ETC\LINKWALL\BLACKLISTS\PORN\URLS and SYS:\ETC\LINKWALL\BLACKLISTS\PORN\DOMAINS files. The files themselves are part of the Squidguard Blacklist files, downloaded from http://www.squidguard.org.

SquidGuard Blacklist Example for Filtering Porn Sites

Specifically, I downloaded the blacklists in the blacklists.tar.qz file, at: http://ftp.teledanmark.no/pub/www/proxy/squidGuard/contrib/blacklists.tar.gz

I then used WinZip to extract the .TAR file from the downloaded file.

Next, I used WinZip to extract the all the individual files & subdirectories from the .TAR file, into the SYS:\ETC\LINKWALL directory. The extraction process created a SYS:\ETC\LINKWALL\BLACKLISTS directory for me, and within that directory it created directories for the following blacklists:

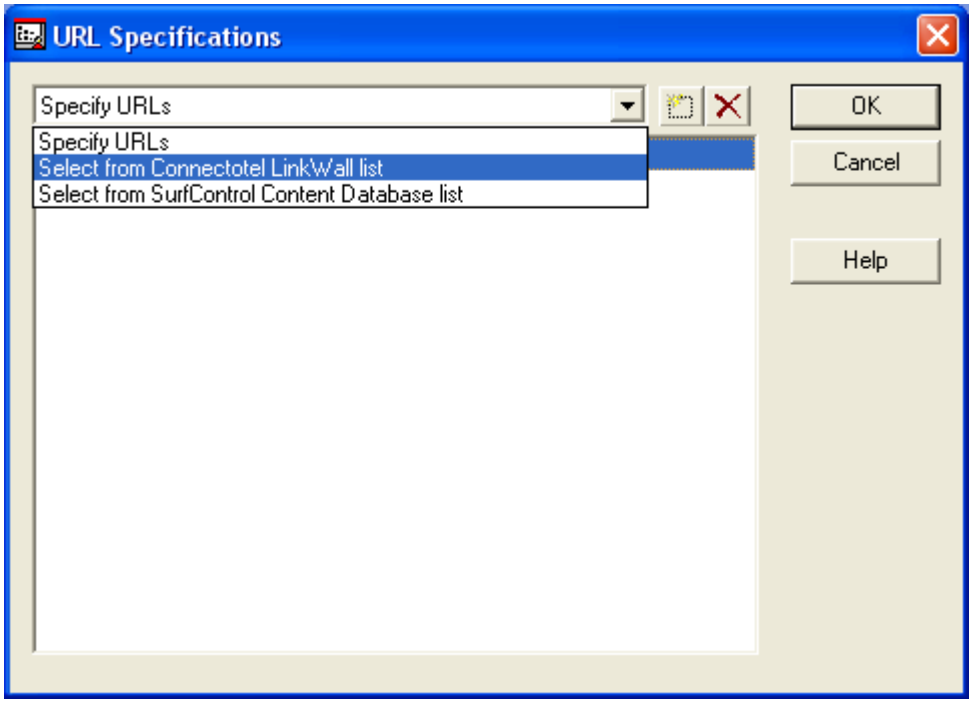
- Ads
- Aggressive
- Audio-video
- Drugs
- Gambling
- Hacking
- Mail
- Porn
- Proxy
- Violence
- Warez

Within each directory, there are several files, including URLS and DOMAINS. There might also be one or more .DIFF files, which give changes from a previous blacklist that you must merge (or $include) manually.

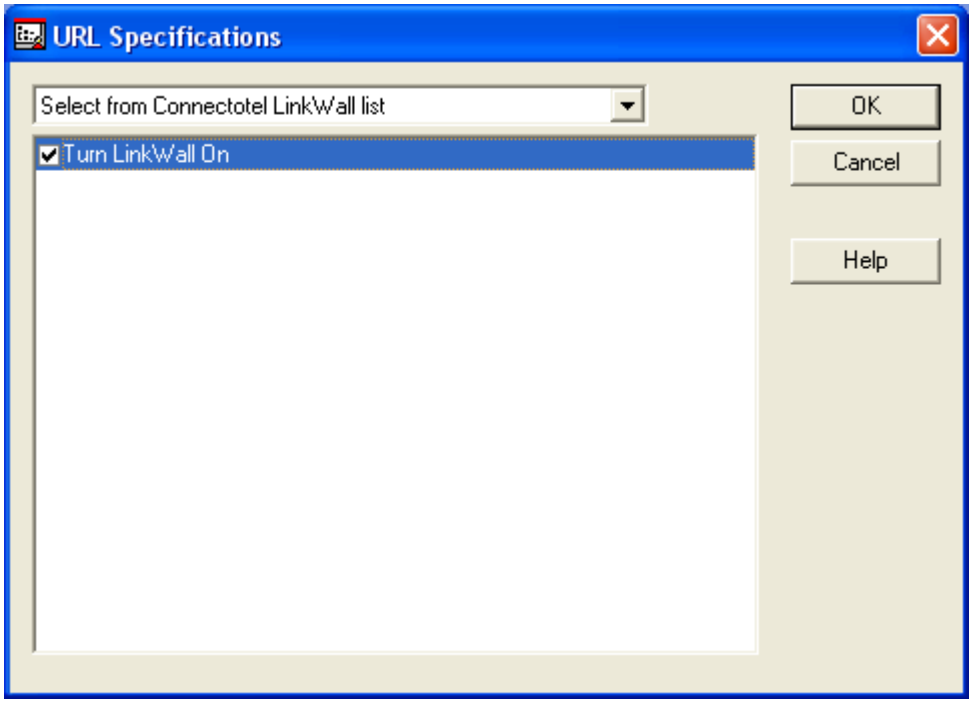
I then pointed LinkWall to use only the Porn blacklist URLS and DOMAINS, by using the following $include commands in LINKWALL.LST:

```
$include sys:etc\linkwall\blacklists\porn\urls
$include sys:etc\linkwall\blacklists\porn\domains
```

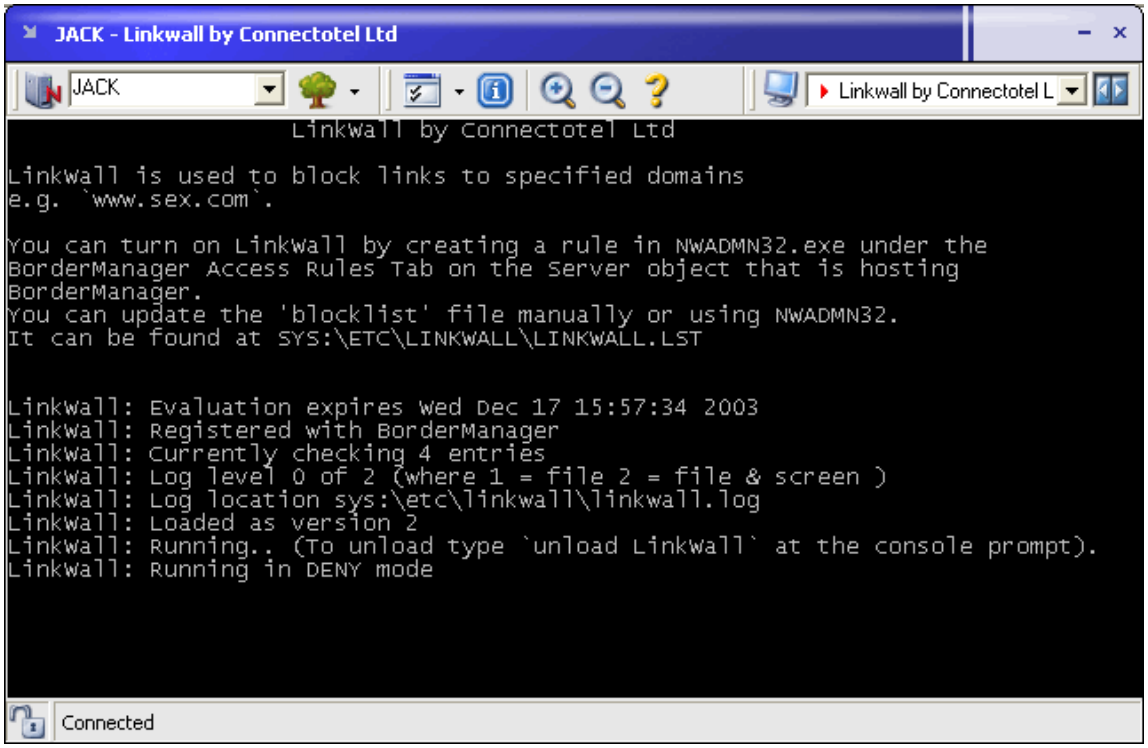
Finally, I added an access rule to Deny URL for the LinkWall option in NWADMN32.



When entering the access rule Destination, I selected LinkWall from a drop-down menu. That menu will only appear if the LinkWall snapin is installed to the server before launching NWADMN32.

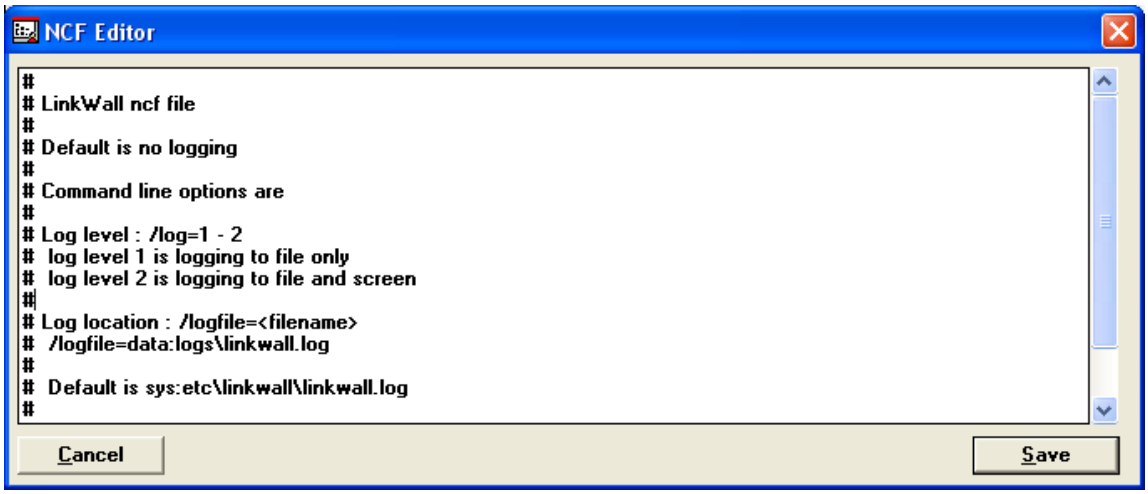


Once you select LinkWall in the access rule destination, you need to select the **Turn LinkWall On** checkbox to enable LinkWall in the access rule.



Next, I launched LinkWall by running the LINKWALL.NCF file on my BorderManager server.

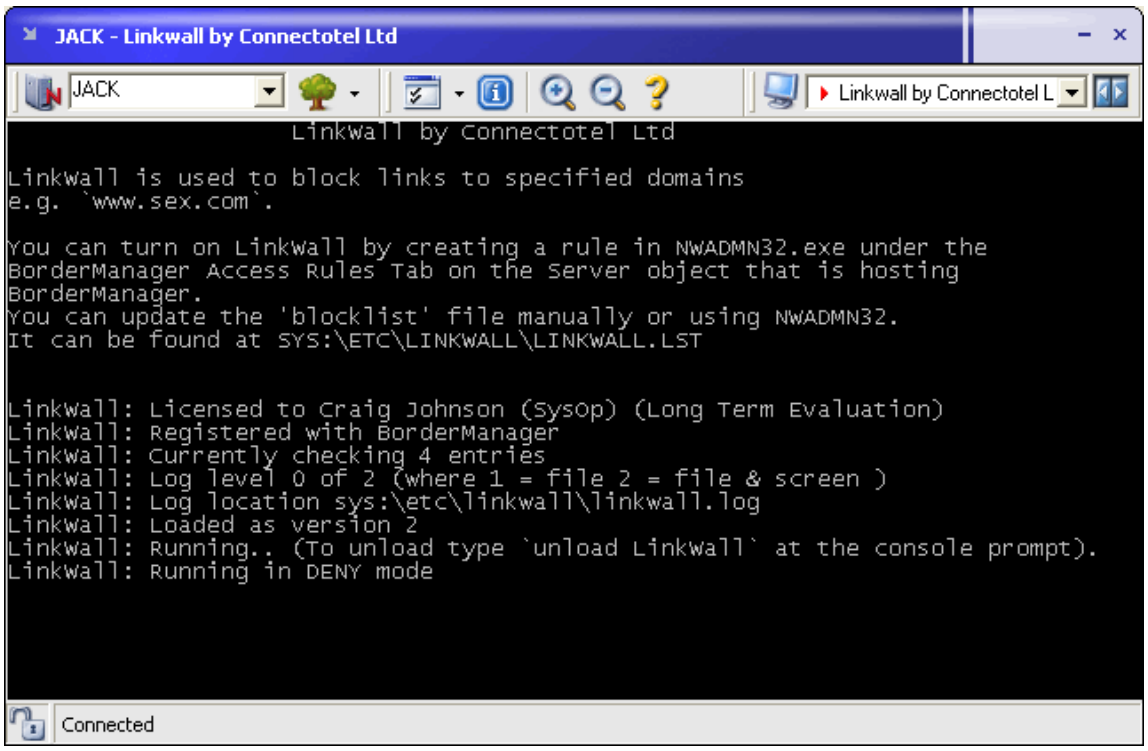
LinkWall Startup Options



From the LinkWall tab, you can edit the LINKWALL.NCF file, which is used to launch the LINKWALL.NLM. In the NCF file, you can enable or disable logging and LinkWall options related to BorderManager versions.

Registering LinkWall

LinkWall allows you a 45-day evaluation period, after which it quits working. If you purchase LinkWall, you will receive a file with a registration key. The file is called LINKWALL.KEY. Copy that file into the SYS:\ETC\LINKWALL directory, and stop and restart LinkWall to change to a registered version.



When LinkWall is registered, you should see registration information on a LinkWall screen on the BorderManager server console.

<This page intentionally left blank. This is to facilitate putting in chapter tabs in a ring binder for double-sided printing. The main chapters should start on an odd-numbered page.>

Chapter 24 - Custom Error Pages

Concept

Novell supplies a pretty error page and some nice graphics that come up when a user is denied access to a web site for whatever reason. A lot of people would prefer to put a stronger warning for access denied warnings, and/or explanations on what various error messages mean. You can create your own custom error page by creating a PXYERR.HTM file and placing it in the SYS:\ETC\PROXY\DATA directory. When PROXY.NLM loads, it will pick up the custom error page and use it until the proxy is reloaded again. There are a number of variables that are used to display the correct error messages.

Example

You can modify the default error page that BorderManager puts up. First of all, go to support.novell.com and get familiar with TIDs **10014022**, **10018668** and **10024011**. Those TIDs explain the syntax for calling out the variable proxy error codes, and it gives some ideas on how to create a customize error page.

I pass on the following method, with credit given to Art Montoya of the City of Chandler for some of the important ideas here. Art thought that simply calling out the error code variable as the name of a GIF file might be handy, and it was a good idea. This technique allows you to easily put in whatever description you want for the error code by making a GIF file with the appropriate name. So, rather than have "403 Forbidden" show up as an error when someone tries to access an X-rated site blocked by CyberPatrol, you can instead show:

"403 Forbidden - You have attempted to access an unauthorized site. All such attempts are logged, and the logs are made available for managerial review. You could be subject to dismissal. Contact the systems administrator at 555-1234 and offer him/her a hefty bribe to tell management that you were testing SurfControl porn site blocking for him."

There is one little problem that Art found in using this method. It worked great for Netscape, but it would not work for Internet Explorer. In Netscape, the GIF file called out for a 403 error worked fine as long as the name of the file was "403 forbidden.gif". IE just choked on it. Art found out that IE didn't like the spaces in the file name and needed to substitute a %20 variable. So, for IE, the name became "403%20forbidden.gif". By duplicating every GIF file with spaces and %20 in the names, both IE and Netscape would pull up the proper graphic.

I show a sample PXYERR.HTM file below.

```
<!doctype html public "-//w3c//dtd html 4.0 transitional//en">
<html>
<head>
   <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
   <meta name="GENERATOR" content="Mozilla/4.72 [en] (Win98; U) [Netscape]">
   <title>BorderManager Information Alert</title>
</head>
<body bgcolor="#FFFFFF">
 
<table BORDER=0 CELLSPACING=4 CELLPADDING=8 frame >
<tr height="30">
<td WIDTH="444" HEIGHT="30"><img SRC="<PROXY_ADDRESS>/data/bmtext.gif" height=40
width=445></td>
</tr>

<tr height="30">
<td WIDTH="444" HEIGHT="30" BGCOLOR="#FFFFFF">
<center><font face="Tahoma"><font color="#000000"><font size=+1>An error
has occurred with your request </font></font></font></center>
</td>
</tr>

<tr>
<td WIDTH="444"><img SRC="<PROXY_ADDRESS>/data/<ERROR_STATUS>.gif" width=444></td>
</tr>

<tr height="30">
<td WIDTH="444" HEIGHT="30" BGCOLOR="#FFFFFF"><font face="Tahoma"><font
color="#000000"><font
size=+1>Description: </font></font></font><ERROR_DESCRIPTION></td>
</tr>

<tr>
<td WIDTH="444">Contact the systems administrator at 555-1234 for additional
explanations for the error message.  The most common errors seen are:
<p><b>403 Forbidden</b> - The user tried to access a site that is blocked
by an access rule. X-rated sites are often blocked.
<br><b>502 Bad Gateway</b> - This is a communications issue and generally
means that an invalid URL was entered in the browser (mistyped the address).
Can also result from DNS problems.
<br><b>504 Gateway Time-out</b> - This is a communications issue and generally
means that a valid URL was entered, but a DNS server is not available or
the web server is down..
<p><img SRC="<PROXY_ADDRESS>/data/alertbar.gif" height=8 width=445></td>
</tr>
</table>

</body>
</html>
```

Reload PROXY.NLM to pull up the new custom error page once you have created or modified the PXYERR.HTM file.

If you are having problems getting the proxy to use a custom error page, have a look in THE SYS:\ETC\PROXY\PROXY.CFG file. It should have the following settings:

```
[MiniWeb Server]
Port-Number=1959
Root-Directory=SYS:\ETC\PROXY\DATA
```

If your root-directory is not the same as above, you will need to change either the root-directory, or the location of the custom error page files.

Note The source address for the GIF files is denoted as <PROXY_ADDRESS>/data/bmtext.gif (or whatever the filename happens to be). Some editors may cut off the directory part of the file name (leaving just bmtext.gif for instance), and that will not work. Also, in my sample PXYERR.HTM, I use a width of 444 pixels for <ERROR STATUS>.gif. Be careful not to make your GIF files too large or too small! (By the way, I used Paint to create the 403 forbidden.GIF file, though I used Viewprint to crop it down as it was too large initially.)

Chapter 25 - Using Dynamic NAT

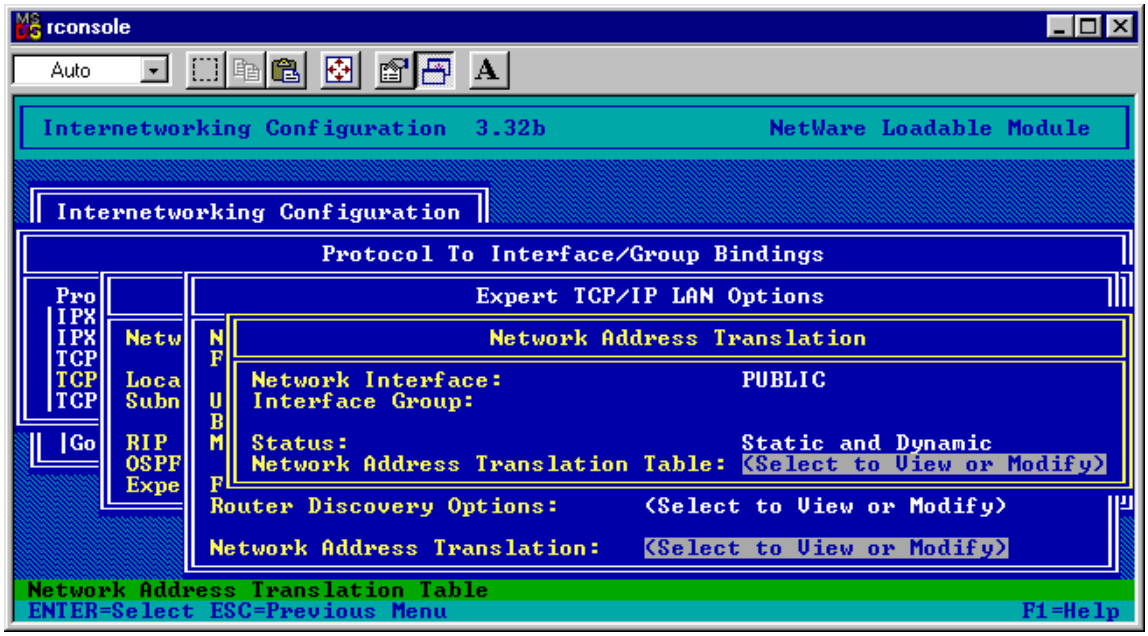
Note Some packet filter exceptions are also shown in the section on configuring reverse proxy acceleration on a secondary IP address.

Concept

Dynamic NAT is used to pass traffic to the Internet when you do not want to or cannot use a proxy. Dynamic NAT, coupled with custom filter exceptions, allows you to selectively bypass the proxy for outbound traffic of your choice.

Note This book has very few examples of using Dynamic NAT, because use of NAT means bypassing proxy, which always involves configuring custom filter exceptions. As such, it is a subject appropriate to my book *Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions*, available via http://www.craigjconsulting.com. That book covers NAT and filter exceptions in great detail.

Dynamic NAT is used to automatically translate (and 'hide') internal IP addresses to a public IP address on the BorderManager server. Dynamic NAT keeps track of the conversations taking place and dynamically couples the return traffic to the original requester. Dynamic NAT is almost always set up on the primary public IP address only (in INETCFG, under Bindings, select the public IP address, then select Expert Options). With dynamic NAT, all the IP packets sent out will have the same source IP address.



The example above shows an entry in INETCFG for both static and dynamic NAT enabled.

Some points in regard to dynamic NAT:

- Dynamic NAT may not be as secure against Internet 'hacks' as using proxies.
- Dynamic NAT still requires packet filter exceptions to allow traffic through.
- Dynamic NAT is used to allow **outbound** traffic – traffic originating from a host on your internal LAN.
- IP Routing must be enabled on the server. (It is otherwise not required for BorderManager services!)
- You MUST have at least two interfaces in the BorderManager server. Trying to use NAT on the same interface with two IP addresses bound will result in communications failures as the ARP table will eventually 'get confused'!

If you have a service running directly on the BorderManager server that you need to access from the Internet, you need to add the following command to AUTOEXEC.NCF so that traffic is allowed to 'get into' the BorderManager server:

```
SET NAT DYNAMIC MODE TO PASS THRU=ON
```

An alternative to the pass thru command is to Disable NAT Implicit filtering in INETCFG, Protocols, TCP/IP, NAT Implicit Filtering.

This INETCFG option is dependent on the NetWare support pack version installed on NetWare 5.1. It does not exist in earlier versions.

In general, if you have dynamic NAT enabled, and something on the server isn't working, try the above SET command or Disable NAT Implicit Filtering in INETCFG.

Some examples of using Dynamic NAT in conjunction with packet filter exceptions to allow traffic to bypass BorderManager proxies follows.

Note This is NOT intended to be a full explanation of working with packet filter exceptions, or to provide numerous examples. To thoroughly understand how packet filter exceptions work, and for many more examples, you should look in the book *Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions*, by Craig Johnson, available at http://www.craigjconsulting.com.

Outbound DNS

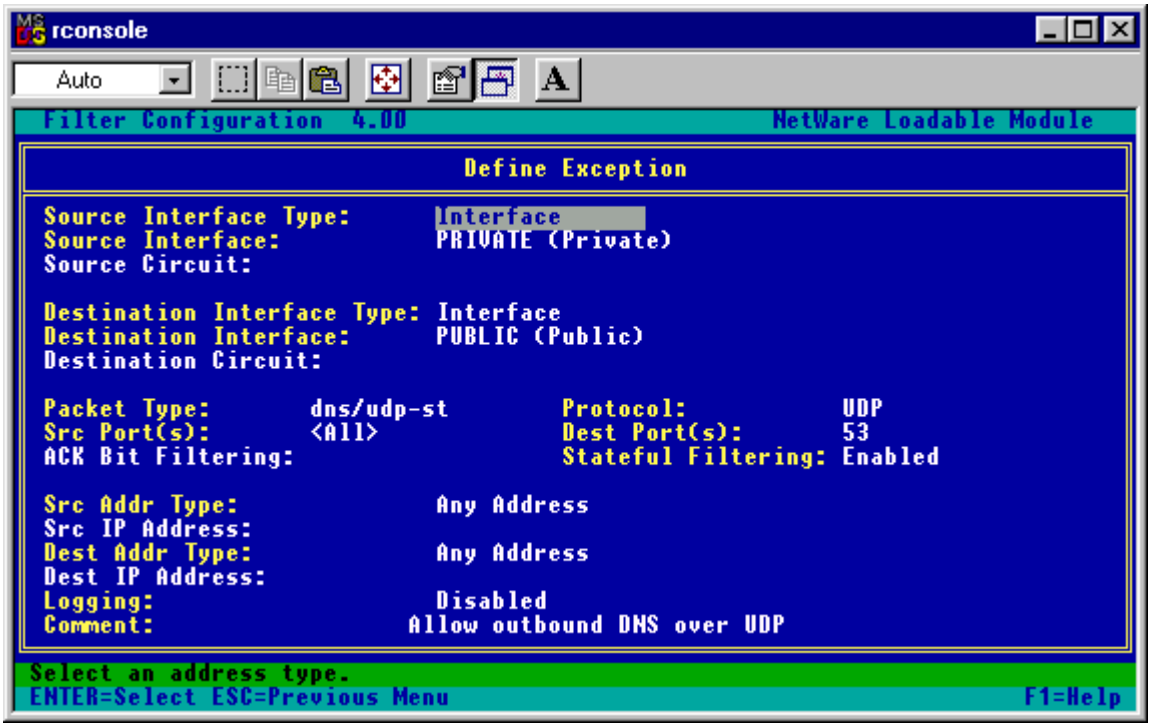
Note This is one example of using packet filter exceptions to allow selected traffic to bypass the BorderManager proxies and route to the Internet. Dynamic NAT is often (usually) required for the example shown to work. The exception (not using dynamic NAT) would be if the internal LAN is using properly registered public IP addresses. This example was taken from *Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions*, by Craig Johnson, available at http://www.craigjconsulting.com. Much more explanation and many more examples are contained in that book.

DNS from Internal PC's to an ISP's DNS Servers

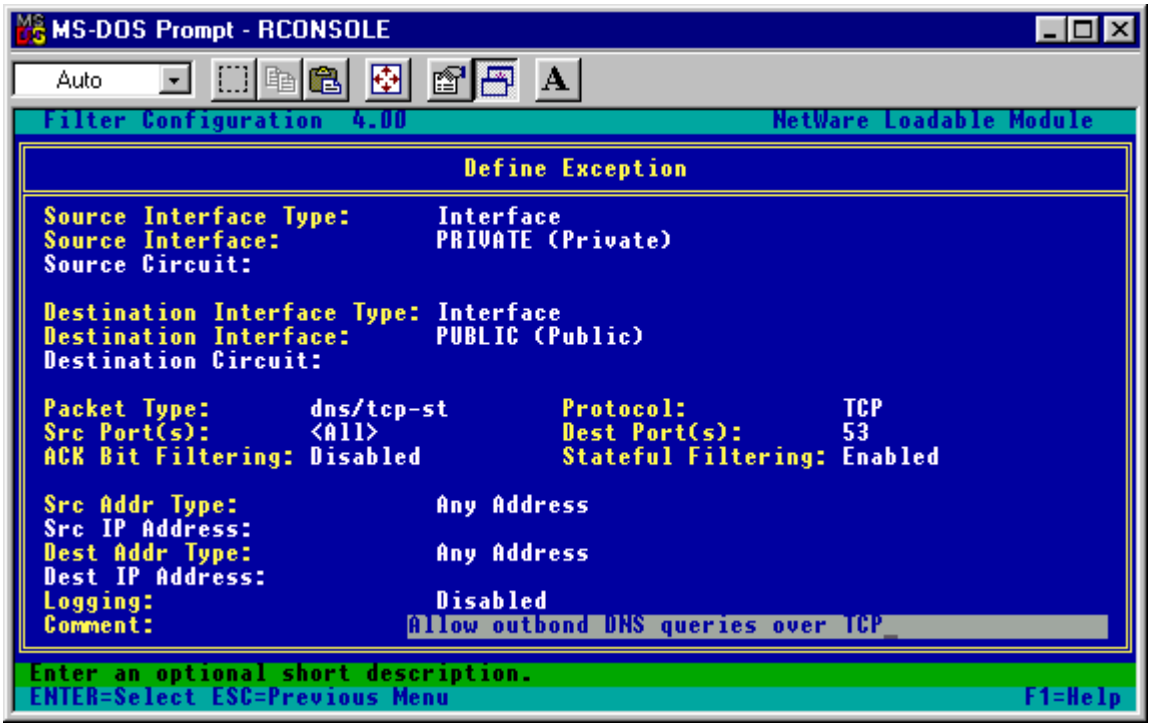
You can also use the DNS proxy in BorderManager 3.x, but if you simply want to pass DNS port 53 requests out through the BorderManager servers so that internal hosts can access external DNS servers, here is how to do it with a stateful packet filter. You may have to create a new packet filter definition, so review the example above for procedures if you are not familiar with the process.

You want to create a packet filter definition called dns/udp-st, and then possibly another one called dns/tcp-st. The first exception will be to allow DNS queries over UDP (commonly used), and the second will be to allow DNS queries over TCP (not so commonly used).

You should be aware that DNS zone transfers are done using TCP, while (most) DNS lookup queries are done using UDP.



This stateful packet filter exception allows outbound **UDP** port 53 (DNS). This stateful packet filter exception allows protocol UDP, source port All, destination port 53 to any IP address. The packet filter exception is applied with a Source Interface of the BorderManager private interface, and a Destination Interface of the BorderManager public interface.

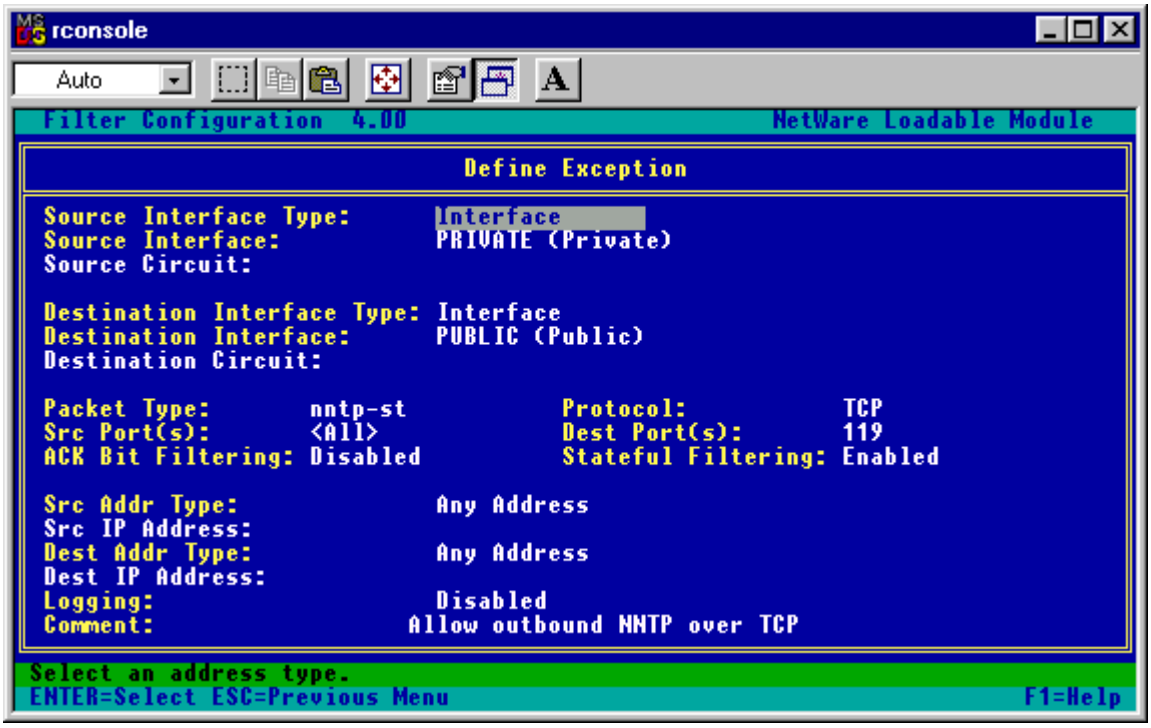


This stateful packet filter exception allows outbound **TCP** port 53 (DNS). This stateful packet filter exception allows protocol TCP, source port All, destination port 53 to any IP address. The packet filter exception is applied with a Source Interface of the BorderManager private interface, and a Destination Interface of the BorderManager public interface.

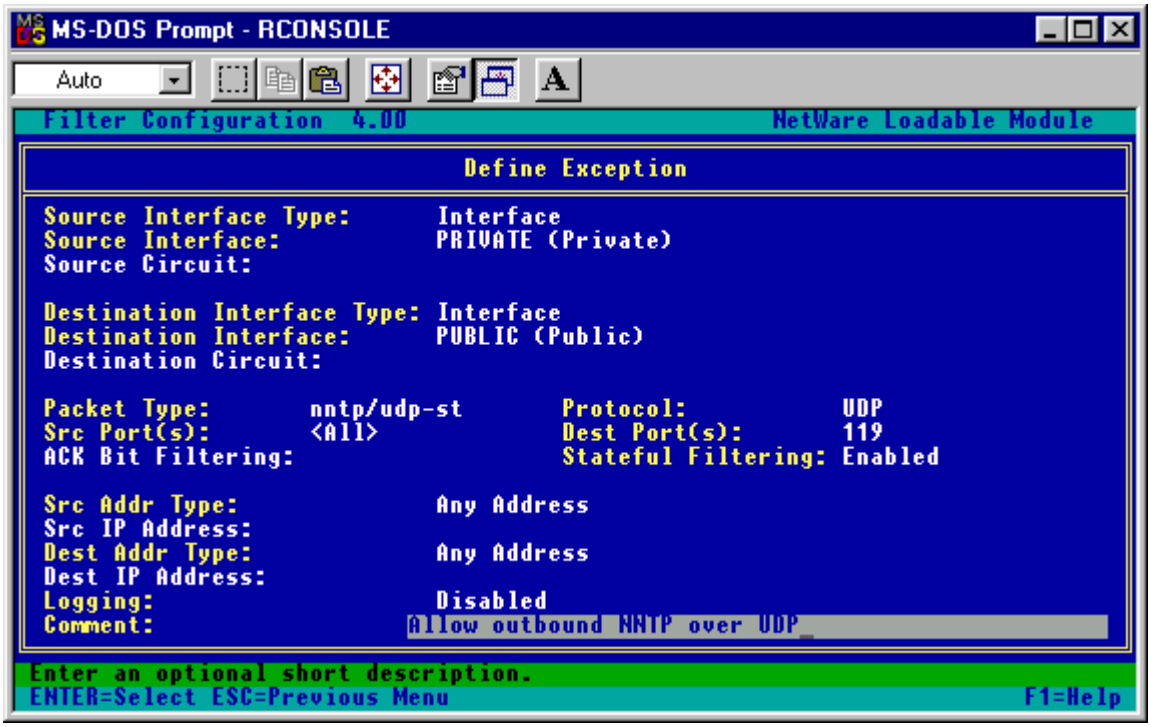
Outbound NNTP

Note This is one example of using packet filter exceptions to allow selected traffic to bypass the BorderManager proxies and route to the Internet. Dynamic NAT is often (usually) required for the example shown to work. The exception (not using dynamic NAT) would be if the internal LAN is using properly registered public IP addresses. This example was taken from my book *Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions*, by Craig Johnson, available at http://www.craigjconsulting.com. Much more explanation and many more examples are contained in that book.

Since the BorderManager 3.x NNTP Proxy service only allows you to proxy one NNTP server for port 119, it is often much easier to just set up a stateful packet filter exception to allow any NNTP server to be accessed across BorderManager from inside the network.



This stateful packet filter exception allows NNTP via protocol TCP, destination port 119 to any IP address. In some cases, it may be necessary to set up an outbound packet filter exception for NNTP via UDP port 119. The packet filter exception is applied with a Source Interface of the BorderManager private interface, and a Destination Interface of the BorderManager public interface.



This stateful packet filter exception allows NNTP via protocol UDP, destination port 119 to any IP address. Most NNTP servers use TCP, not UDP, so it is unlikely this exception will be needed. It is provided as a reference only.

The packet filter exception is applied with a Source Interface of the BorderManager private interface, and a Destination Interface of the BorderManager public interface.

Chapter 26 - Using Static Nat

Concept

Static NAT is used to allow **inbound** traffic through a BorderManager firewall to a specific internal host IP address. If you want to make an internal host available to the Internet with BorderManager, your options are to set up static NAT (and appropriate packet filter exceptions) or Reverse Proxy. Static NAT involves pairing an address on the public side of the BorderManager server with the IP address of any internal host on your network.

Static NAT is almost always done with a secondary IP address assigned to the public interface in a BorderManager server. Using Static NAT with the primary public IP address on the BorderManager server will result in almost all BorderManager services failing.

Static NAT requires packet filter exceptions to work. Generally you set up one packet filter exception to allow desired traffic TO the private internal IP address, and a second packet filter exception to allow traffic FROM the secondary IP address.

Note That's right - I said the packet filter exceptions for static NAT use the internal IP address of the host, not an IP address assigned on the BorderManager server!

Static NAT offers less security than Reverse Proxy.

You can only configure one static NAT address pair for any IP address. If you want more than one internal host to be available to the Internet through static NAT, you will have to have more than one public-side IP address assigned to the server.

For instance, you have two internal FTP servers you wish to get to from the Internet, 192.168.10.100 and 192.168.10.101. You have assigned a secondary IP address of 4.3.2.253 to your BorderManager public IP interface. You set up a static NAT address pair of public=4.3.2.253 and private=192.168.10.100. You cannot now assign the 192.168.10.101 address as a static NAT pair unless you add one more public IP address, such as 4.3.2.252.

Static NAT can be (and usually is) configured in addition to dynamic NAT.

Static NAT To Internal SMTP Mail Server

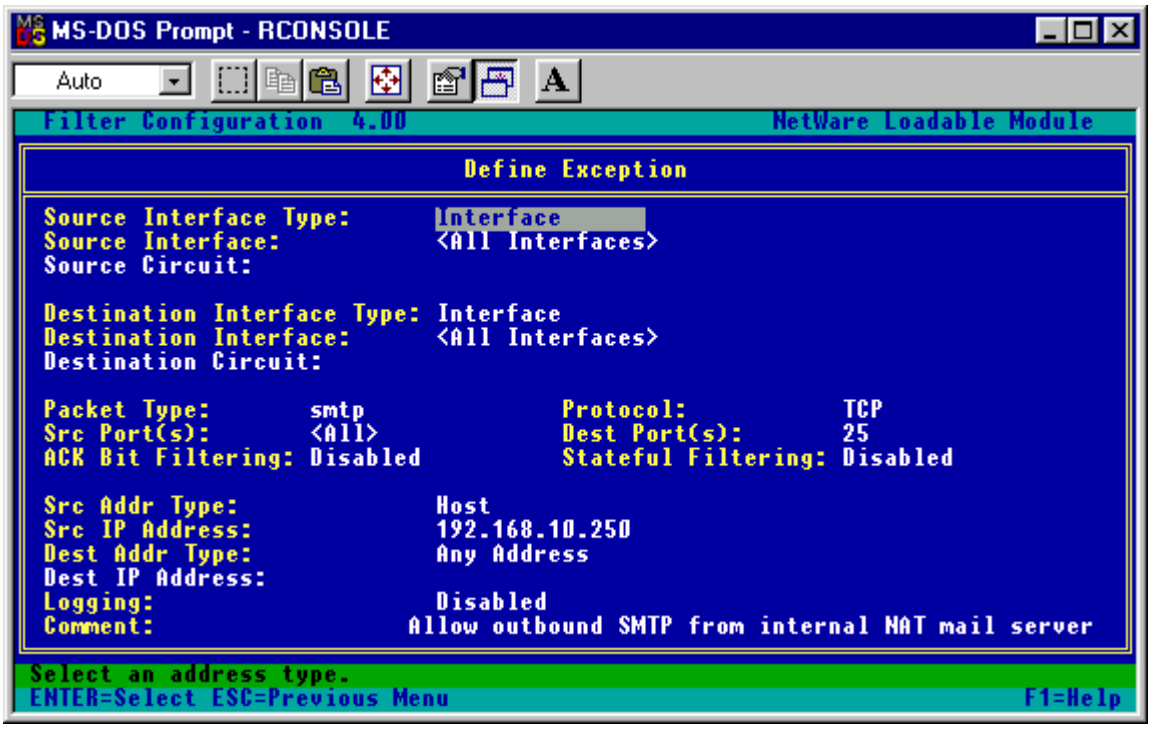
Note This is one example of using packet filter exceptions to allow selected traffic to bypass the BorderManager proxies and route to the Internet. Dynamic NAT is often (usually) required for the example shown to work. The exception (not using dynamic NAT) would be if the internal LAN is using properly registered public IP addresses. This example was taken from my book *Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions*, by Craig Johnson, available at http://www.craigjconsulting.com. Much more explanation and many more examples are contained in that book.

The following examples show how to allow SMTP mail traffic to and from an internal SMTP mail server using static NAT. It is often a good idea to further restrict this static NAT traffic to only allow communications between the internal host and the ISP's mail server. (If the ISP has multiple mail servers, set up packet filter exceptions for each of their mail server IP addresses). Restricting SMTP traffic to only the ISP's mail servers will help prevent someone else from using your mail server as a mail relay host (for spamming purposes).

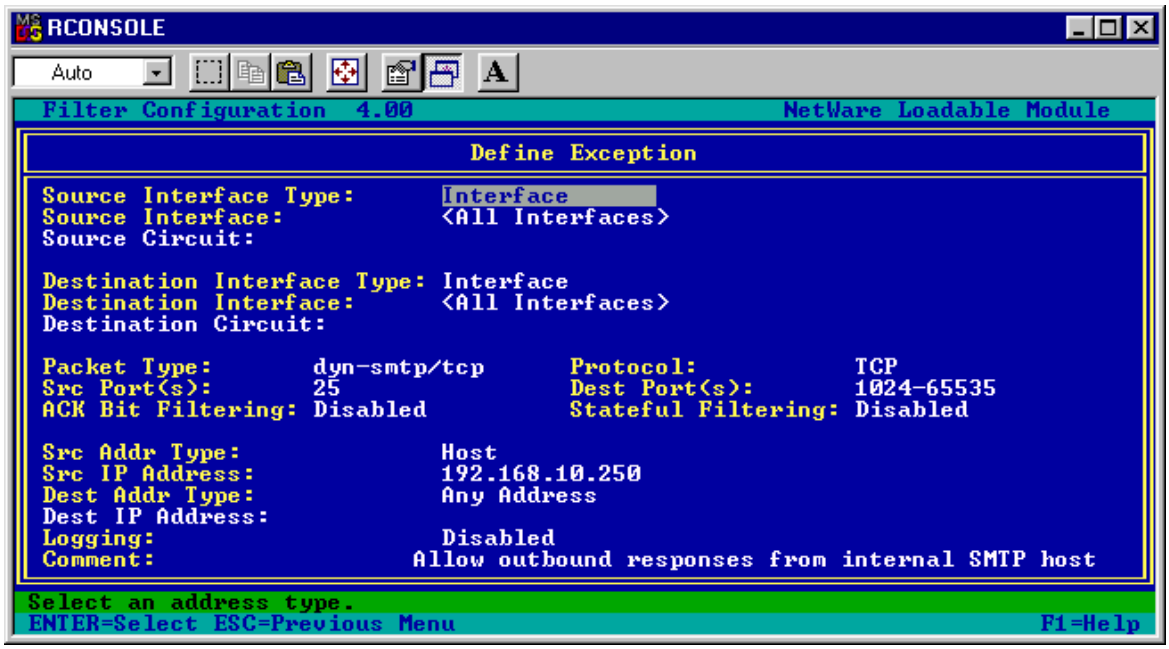
Your SMTP mail server might also need to make DNS queries, and depending on how you have DNS services set up on your network, you may also need to add outbound DNS packet filter exceptions (one outbound, plus one return traffic exception) for the internal SMTP server IP address.

This packet filter allows anyone to send SMTP port 25 mail to the internal SMTP mail server at 192.168.10.250. This packet filter exception allows protocol TCP with any source port and a destination port of 25 to a destination IP address set to the static NAT internal IP address used by an SMTP mail server.

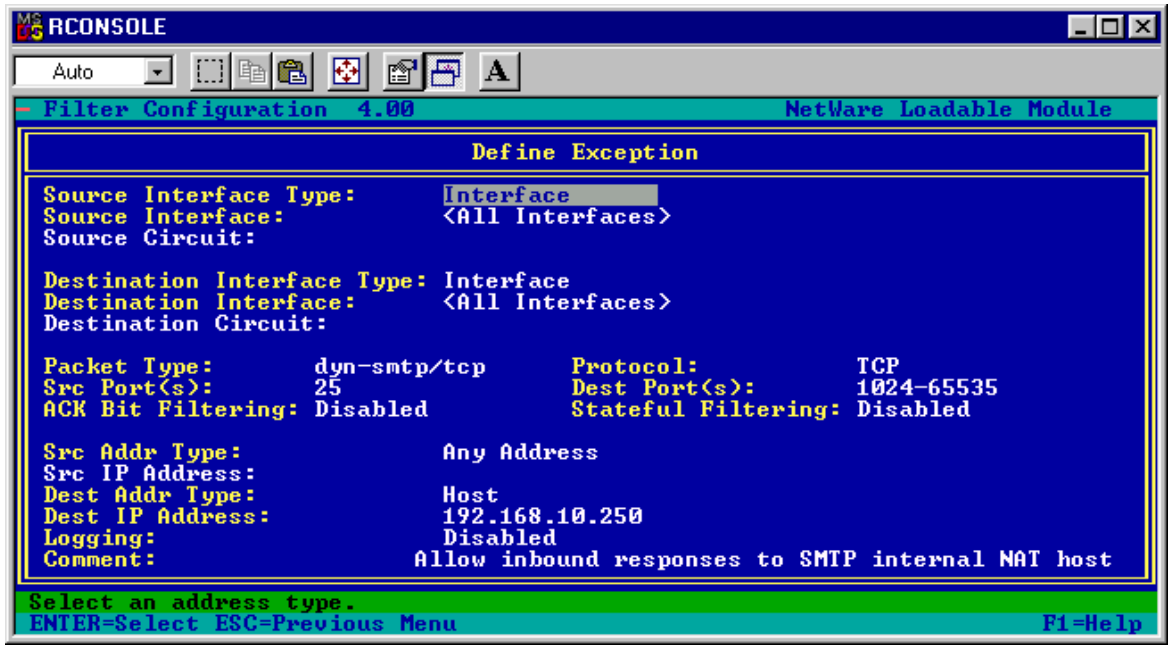
Note Here is where you might want to add your ISP's mail server IP address as a Source IP address.



This packet filter exception allows the internal SMTP mail server to send SMTP mail out. Please observe that the packet filter is also applied to the internal IP address and not the public IP address called out in the static NAT table. The packet filter exception allows protocol TCP with any source port and a destination port of 25 from an IP address set to the static NAT internal IP address of an SMTP server.



This packet filter exception allows the internal SMTP mail host to respond to SMTP requests coming in. This packet filter exception allows protocol TCP with source port 25 and a destination port range of 1024-65535 from a source IP address equal to the static NAT internal IP address of an SMTP mail server. Set the destination IP address equal to the SMTP server of your ISP if you want to allow communications only to your ISP's mail server(s).



This packet filter exception allows the SMTP mail host to receive responses to SMTP requests coming going out. This packet filter exception allows protocol TCP with source port 25 and a destination port range of 1024-65535 from any source IP address, and to a destination source IP address equal to the static NAT internal IP address of an SMTP mail server. Set the source IP address equal to the SMTP server of your ISP if you want to allow communications only to your ISP's mail server(s).

Chapter 27 - BorderManager Alerts

Concept

BorderManager has some alerting capability. It can be configured to send email (SMTP) to selected users on the event of certain NLM's being loaded or unloaded on the server. BorderManager 3.5 and later versions have additional alerting capability controls compared with BorderManager 3.0.

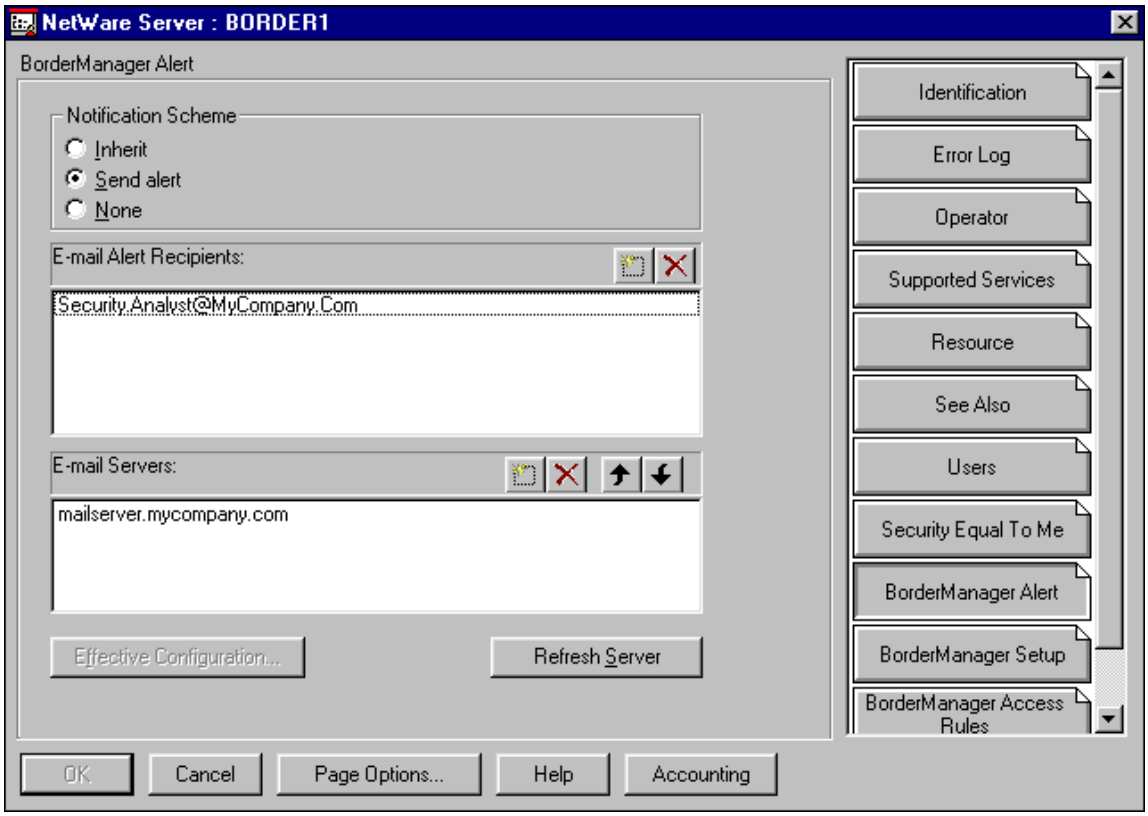
BorderManager alerts (and logging, to some extent) are not a strong point. People frequently ask if BorderManager can detect and log or report hacking attempts. Beyond what the alert feature provides, there is little else that can be done. There are ways to log denied packets from the packet filters, but that feature is intended to be used for debugging purposes and should not be turned on for production use.

Note If you want an decent intrusion detection system (IDS), look into setting up SNORT on a Linux server that sniffs packets going to the BorderManager public interface.

Configuring Alerts

From the NWADMIN screen, select BORDER1 and then select BorderManager Alert to bring up the BorderManager Alert main menu screen.

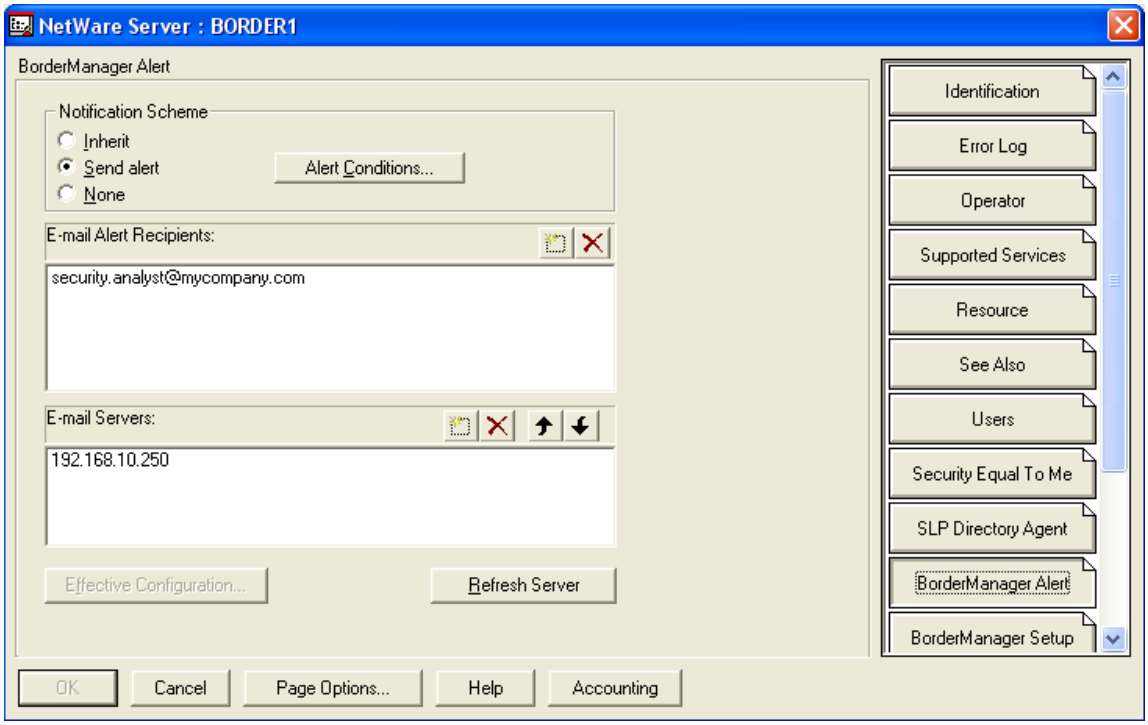
BorderManager 3.0



This example shows the alert configuration menu for a BorderManager 3.0 server.

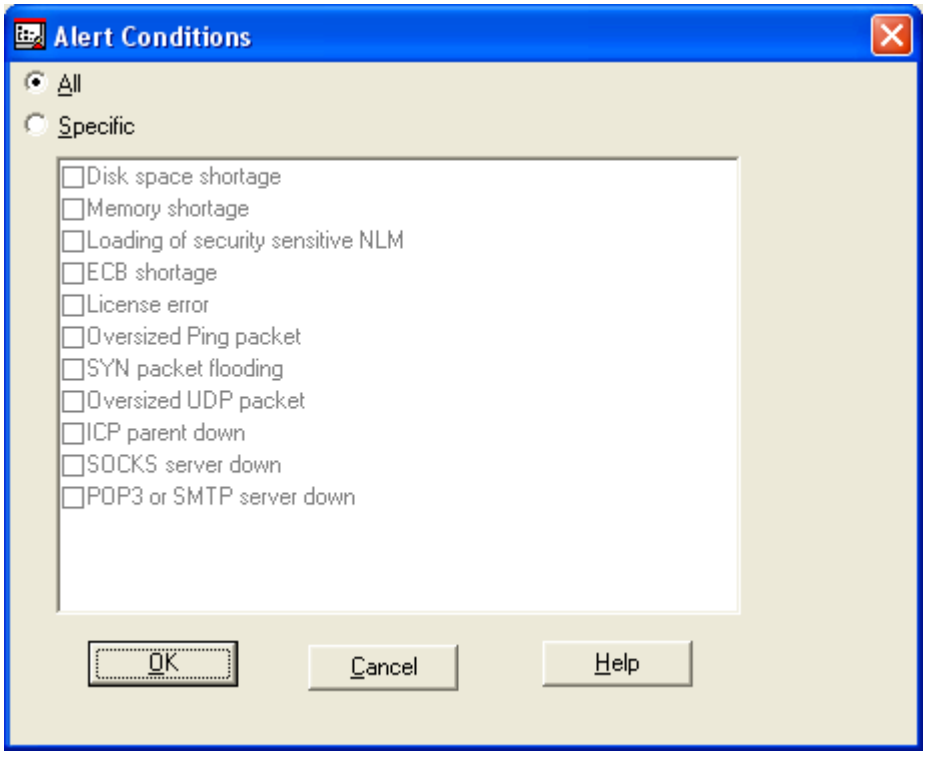
Enter the email addresses of any users to be alerted when BorderManager sees critical NLM's changing. Set up the DNS name or IP addresses of the email servers to forward the mail alerts.

BorderManager 3.5 and Later



This example shows the Alert configuration menu for a BorderManager 3.5 or later server. Note the **Alert Conditions** button, which is not present on a BorderManager 3.0 server.

You can use NWADMN32 from a BorderManager 3.5 or later server to administrate a BorderManager 3.0 server, but if you use the Alert Conditions button, the alert conditions menu will be grayed out, and you will not be able to configure any specific alert conditions.



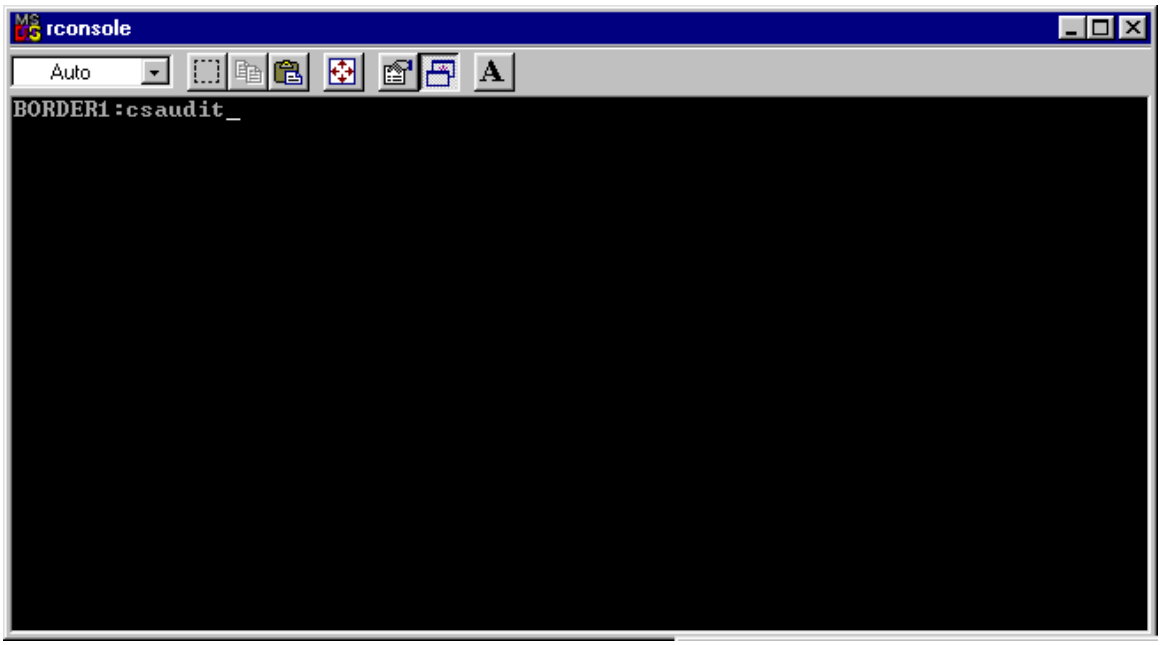
Pressing the **Alert Conditions** button on a BorderManager 3.5 or later server brings up a menu. You can select any or all of the conditions that might cause the BorderManager server to attempt to send an email message as an alert.

Note that the only alert capabilities provided are what you see on the menu! If an SMTP server cannot be reached, the alert function also will not be of much use. The SMTP server must also be allowed to relay SMTP mail to the designated recipient addresses.

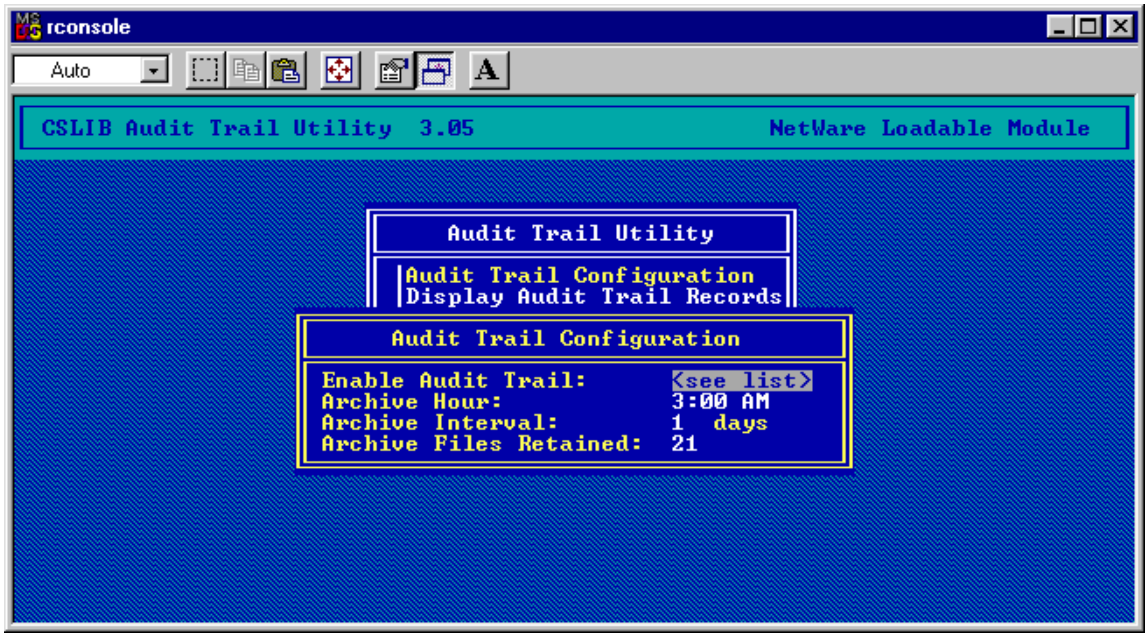
Chapter 28 - Logging

Controlling the Size of the Indexed and Access Control Logs

The Indexed and Access Control Logs (access rule logs) are stored in a Btrieve file under the SYS:\SYSTEM\CSLIB directory. While you cannot (unfortunately) change the location of this file, you can control the size somewhat. Use the CSAUDIT command to bring up a menu entry to set log file parameters.

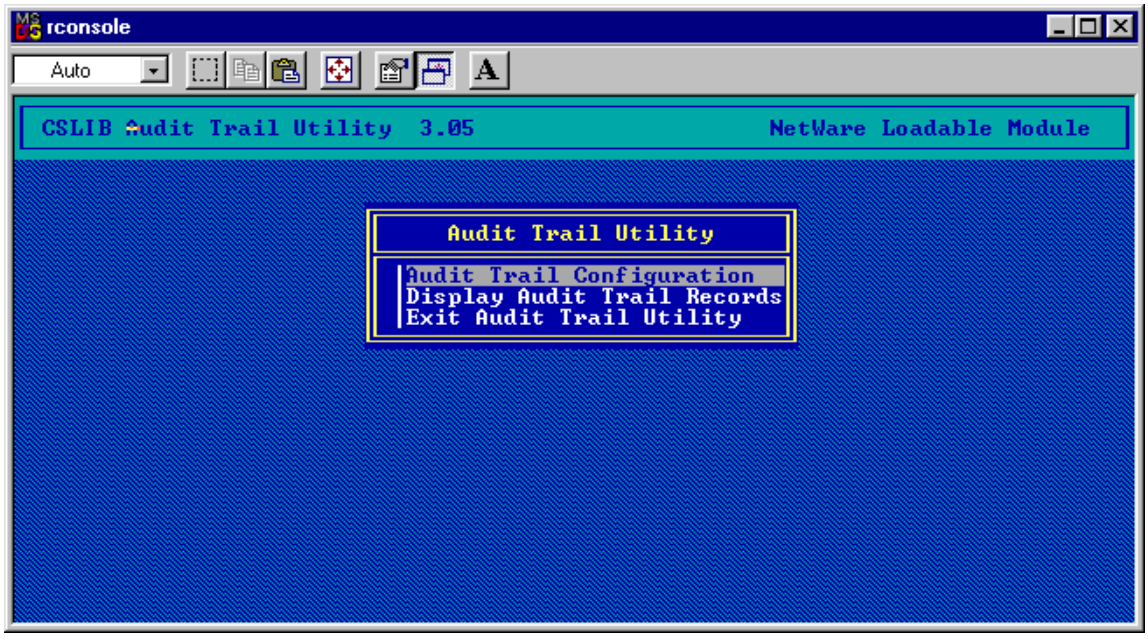


Simply type: **CSAUDIT**. Do not use LOAD CSAUDIT.

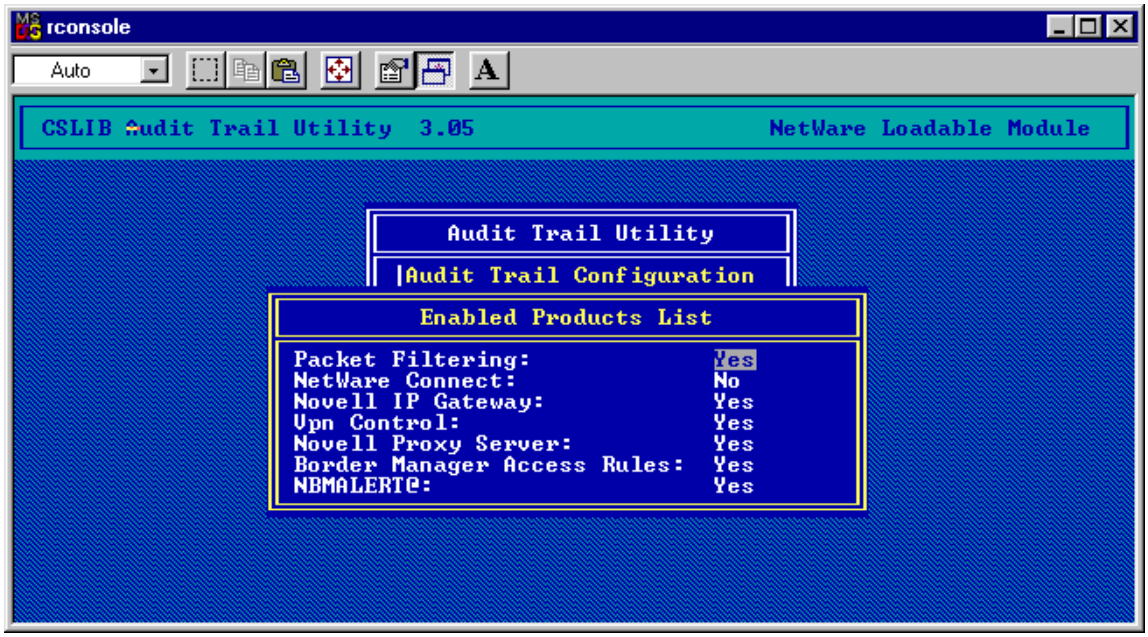


Select **Audit Trail Configuration**

Here you can set the **Archive Interval** and the number of **Archive Files Retained**. This setting saves 21 days worth of data.



Selecting **Enable Audit Trail** will show you what can be audited.



Normally, all the BorderManager installed products should show up here, and you can specify particular services that are supported for Indexed or Access Control Logging.

Viewing Common Log Files

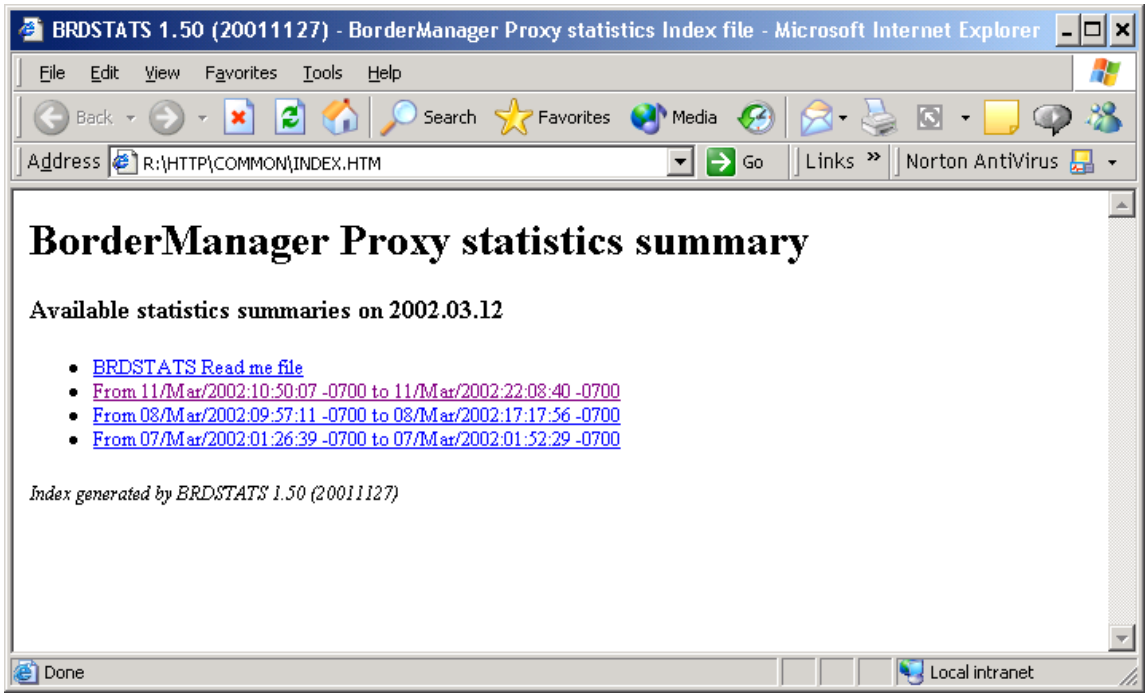
There are several methods used to view log files. The HTTP Common log files are in text format, but are not formatted for convenient reading. The common logs also are not designed to be read or exported from NWADMN32. Instead, the common logs should be read and analyzed by a program such as Webspy, BRDSTATS, or other commercially-available and freeware log analysis programs. See http://www.webspy.com for a downloadable evaluation copy of Webspy – this program does a nice job of analyzing log files for you.

Using BRDSTATS

BRDSTATS is a free program, available from the Novell Cool Solutions web site, or my web site http://www.craigjconsulting.com.

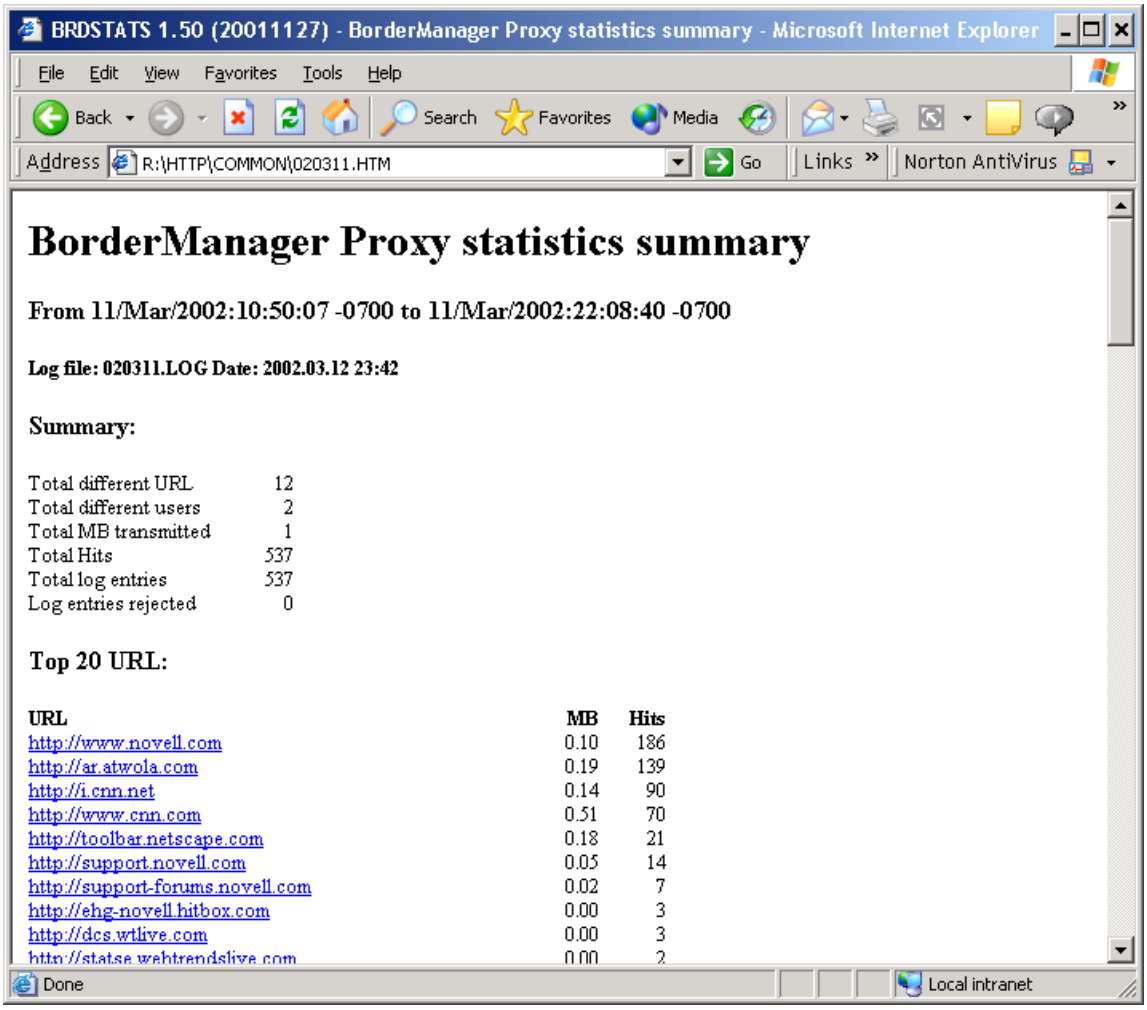
BRDSTATS does not provide the depth of reporting that commercial products can, but it is free, while some other products are fairly expensive.

To use BRDSTATS, copy the BRDSTATS distribution file to the common log directory and extract the files. Run the BRDSTATS.EXE program. The program will parse every log file in the directory and create on HTML file for each log file. BRDSTATS will also create an INDEX.HTML file linking individual log file summaries. Simply launch the INDEX.HTM file in your browser.



The BRDSTATS index.html file should have links to other web pages, each of which summarizes a single log file in the HTTP Common log file directory.

Click on one of the links to view the log summary.



The example above shows just a bit of some of the data generated by BRDSTATS.

Viewing Extended Logs

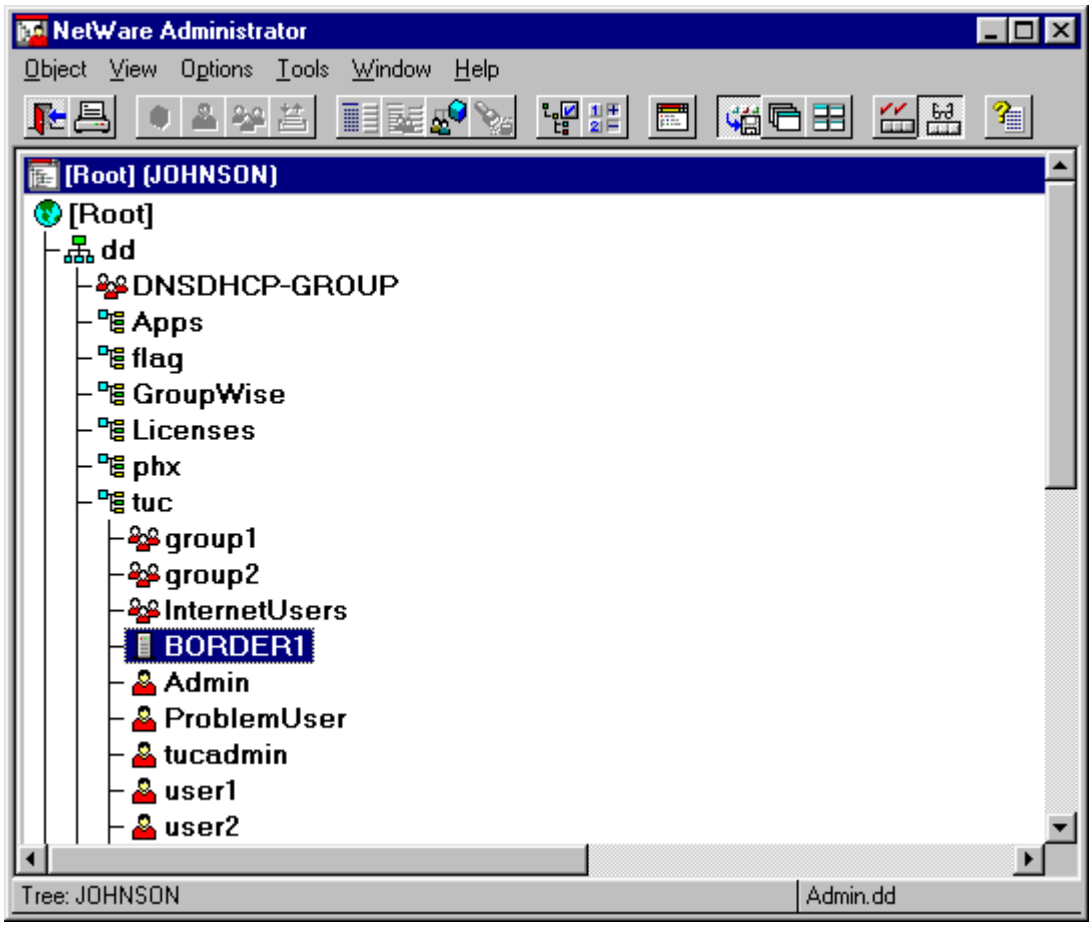
There are relatively few programs that read the BorderManager Extended Log files. Webspy is one such program.

I normally never make use of Extended logging as I don't find the small amount of additional information in those files worth analyzing.

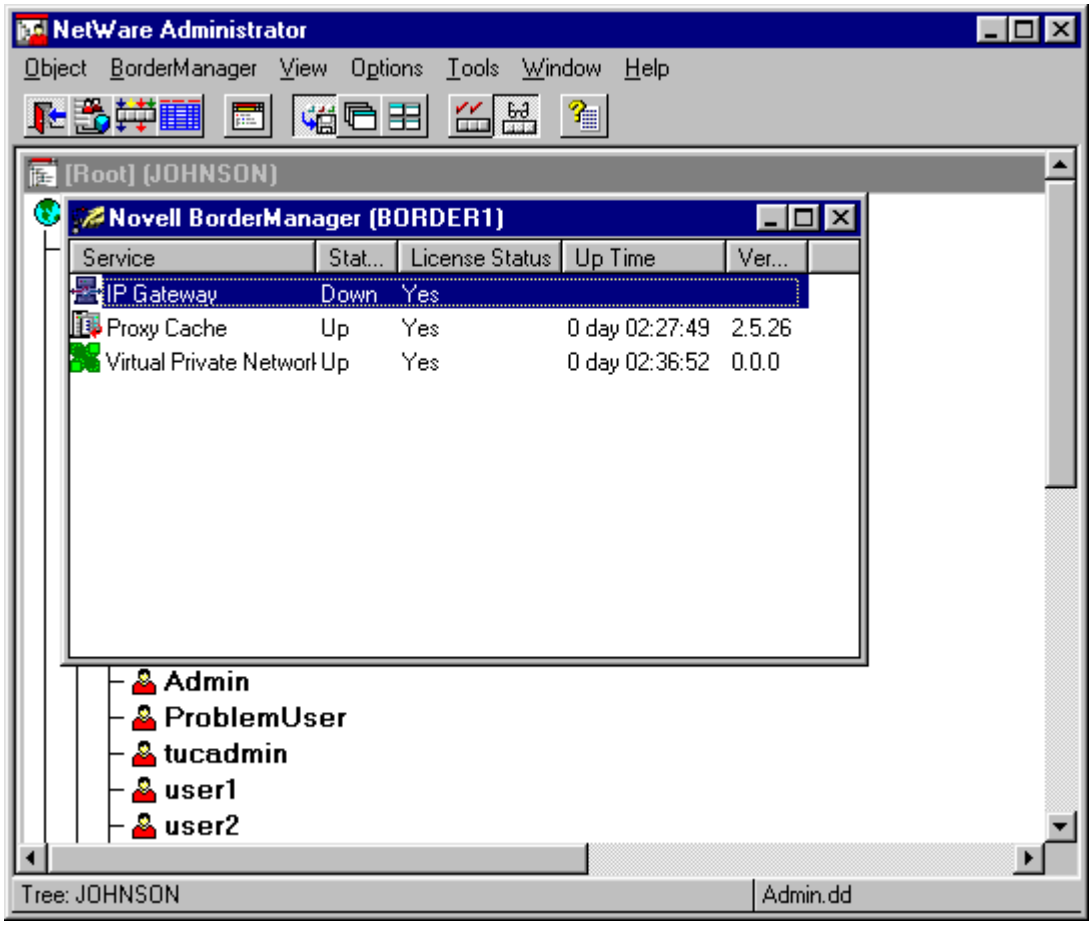
Viewing Indexed Logs

Indexed and **Access Control logs** can only be viewed with NWADMN32, but they can be exported in NWADMN32 to other formats.

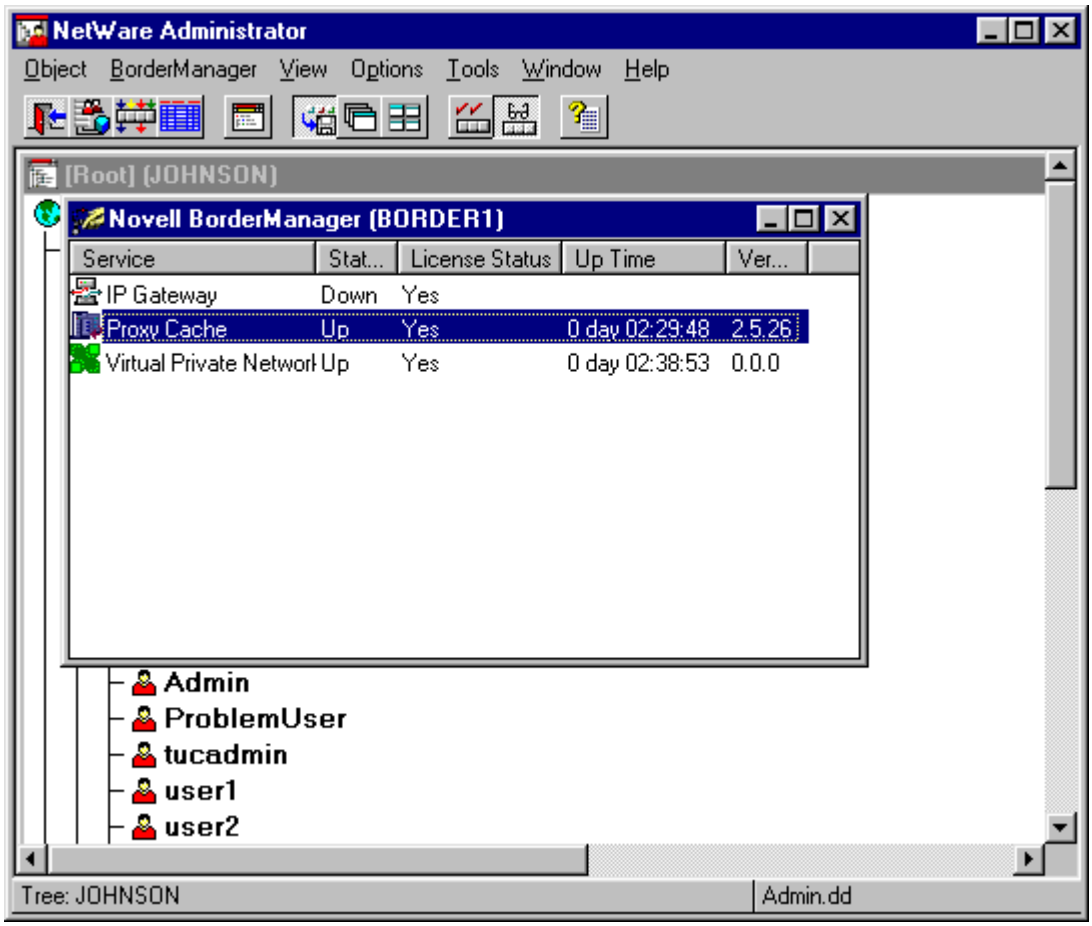
Indexed log files are stored in Btrieve format and can only be viewed by a third-party utility after they have been exported by NWADMN32.



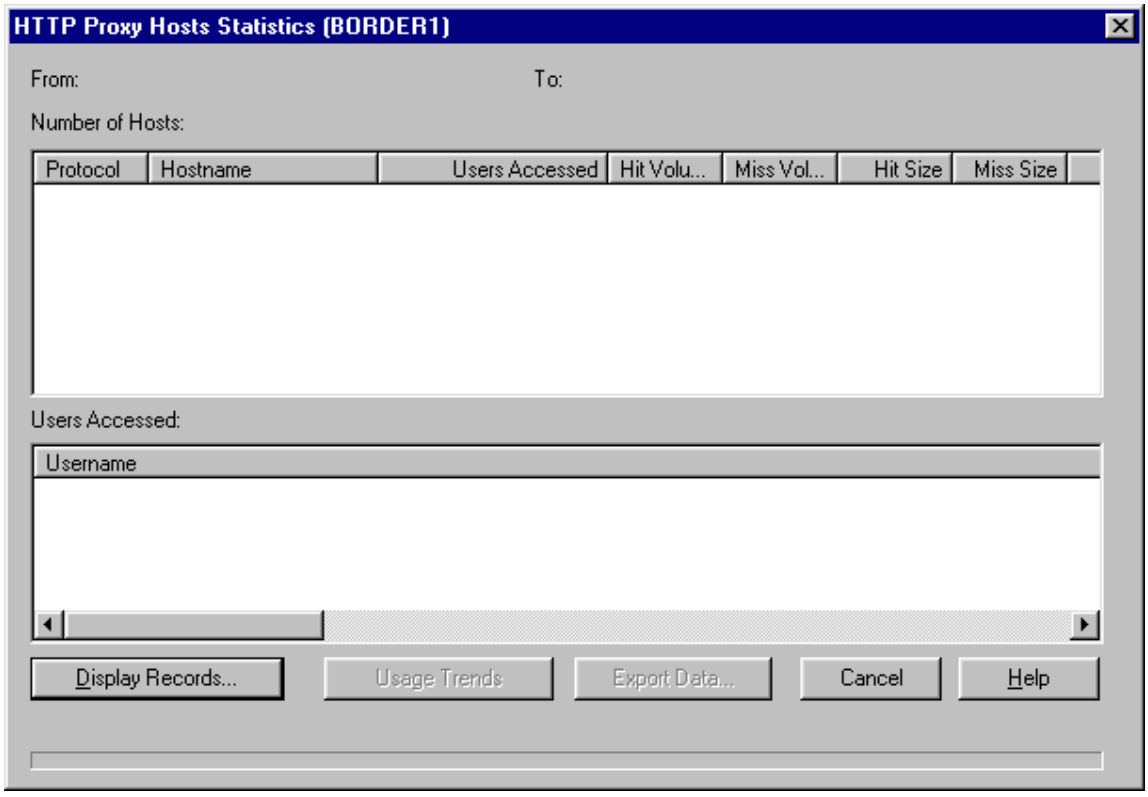
To view Indexed log files, open **NWADMN32**, and single-click on the **BorderManager server icon**.



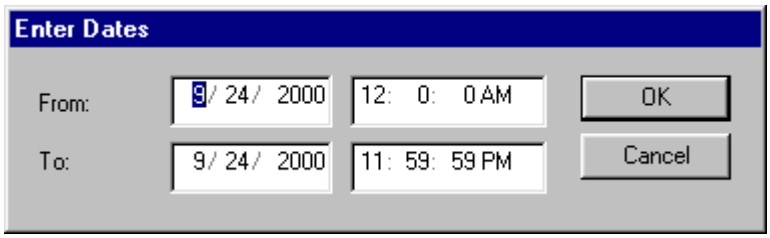
On the top menu, select **Tools**, and then select **Novell BorderManager**



Click the Proxy Cache icon to highlight the Proxy Cache icon if you want to view Proxy Index logs. Click IP Gateway or Virtual Private Network if you want to view those Indexed Logs.

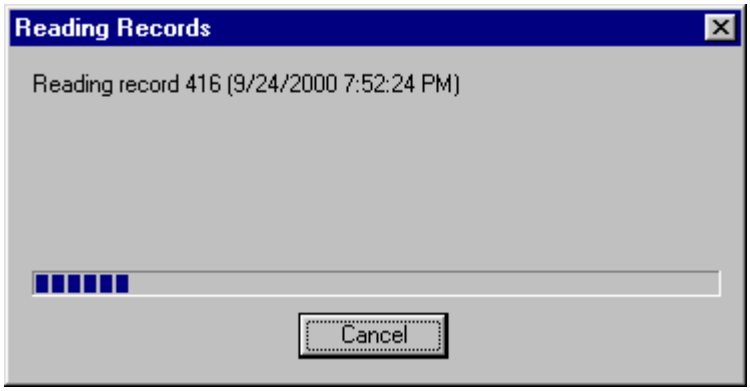


Now, either select **Object**, **View Audit Log** from the drop-down menu, or right-click on **Proxy Cache** in the center window and select **View Audit Log**.



Click on **Display Records** and enter a date range to search.

Click on the **OK** button. You should get data if you have enabled Indexed logging and entered a valid search range covering logged data.

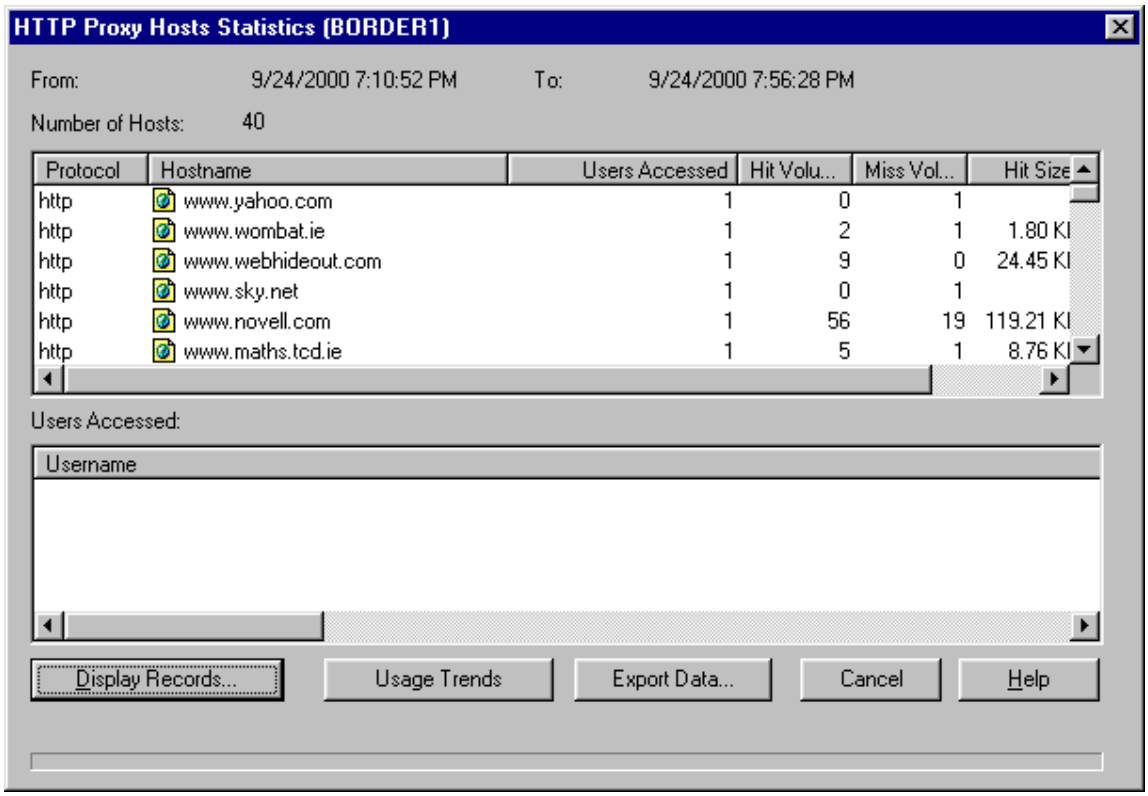


If data is being found, you will see a progress bar. If a lot of data is being processed, this part can be very slow. It is typical for the progress to start out quickly and get slower and slower and slower…

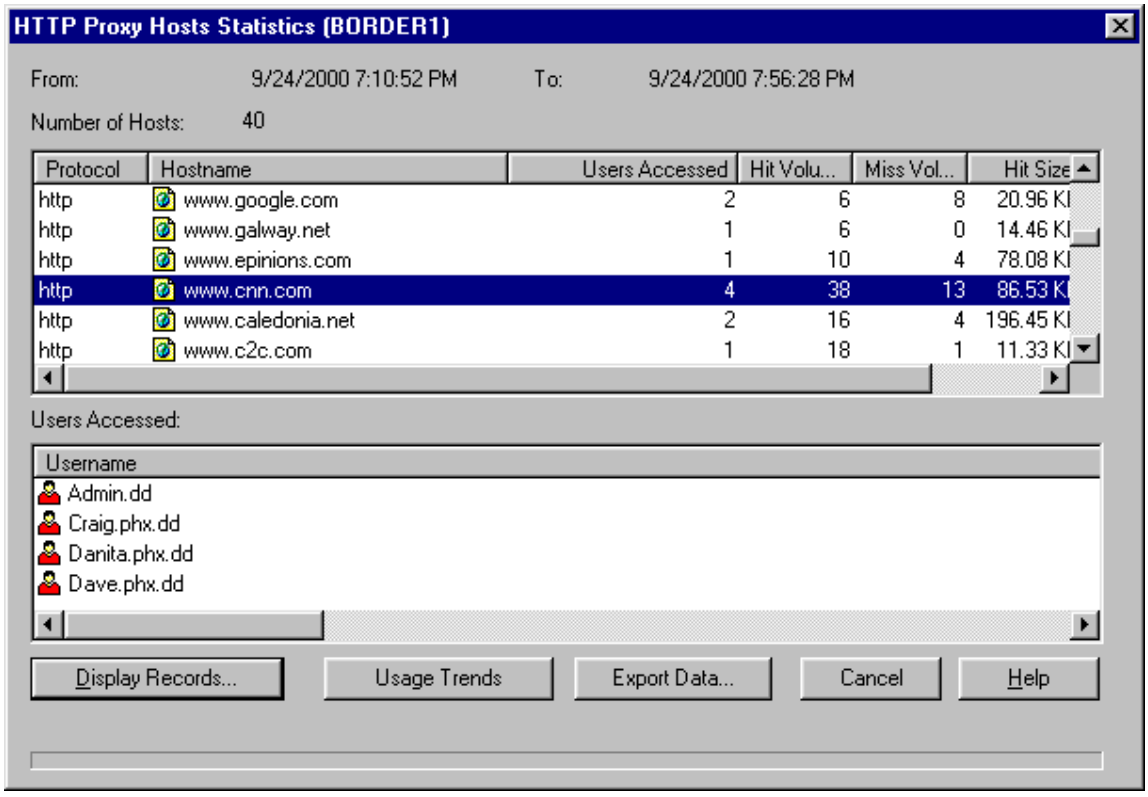
If you get the above, you may have:

- not selected the Proxy Cache icon before viewing the audit log, or
- used an invalid date range, or
- not have configured the proxy cache to use Indexed Logging.

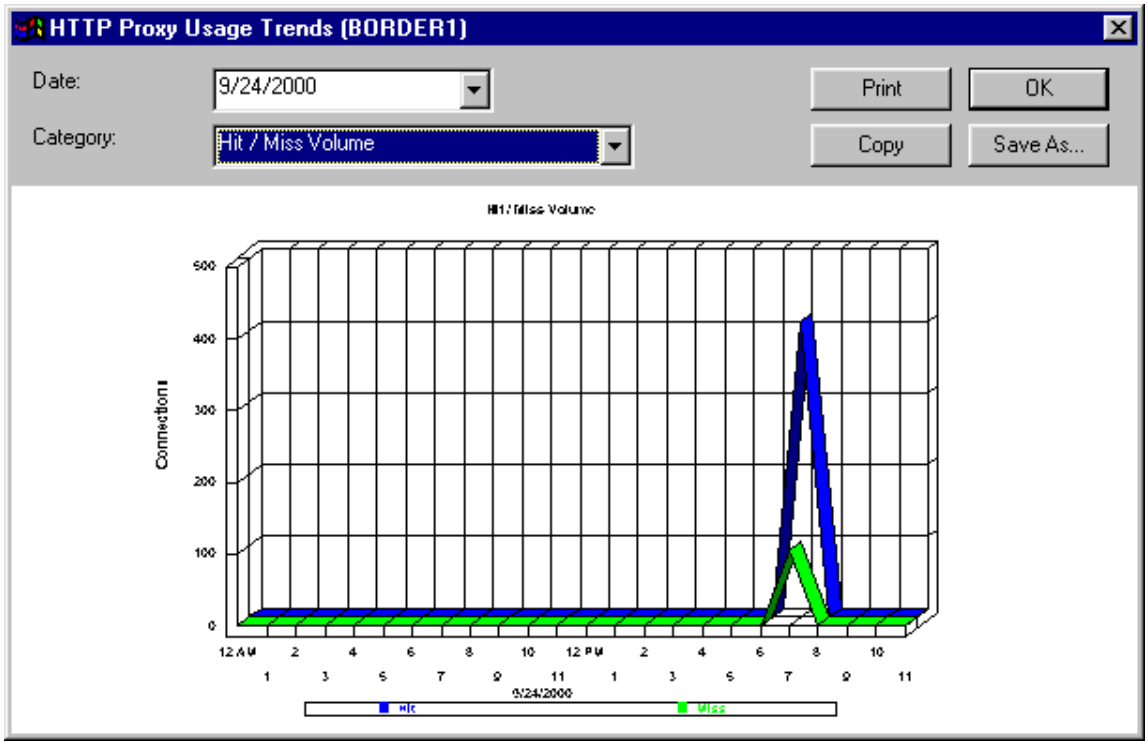
Remember, you only view Indexed or Access Control logs from within NWADMN32 using the method shown here.



You should get some records to view, and clicking on a URL will display those users that accessed that URL in the lower window.



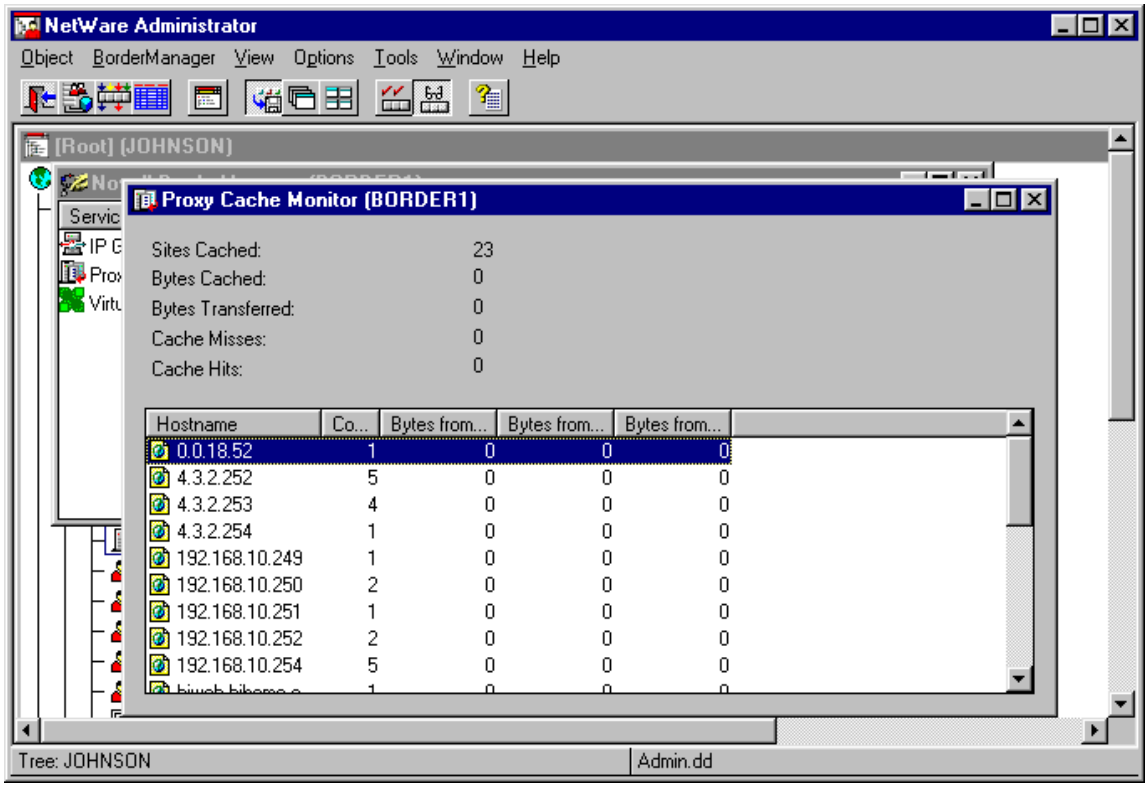
Double-clicking a username will give you a listing by username instead of hostname. You can also click on any of the column headings to sort the data in ascending or descending order.



Clicking on the **Usage Trends** button will graph the selected data over a 24-hour period for you in a number of possible ways. The example above shows the hit and miss volumes graphed.

Viewing Real-Time Proxy Cache Data in NWADMN32

Double-click on **Proxy Cache** to see current statistics

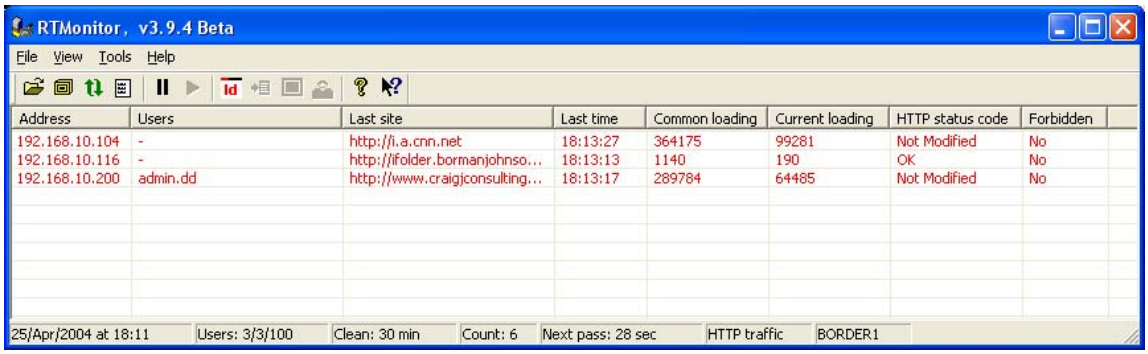


Note BorderManager 3.x only shows you 100 sites on this screen.

Viewing Real-Time Browsing Activity with RTMonitor

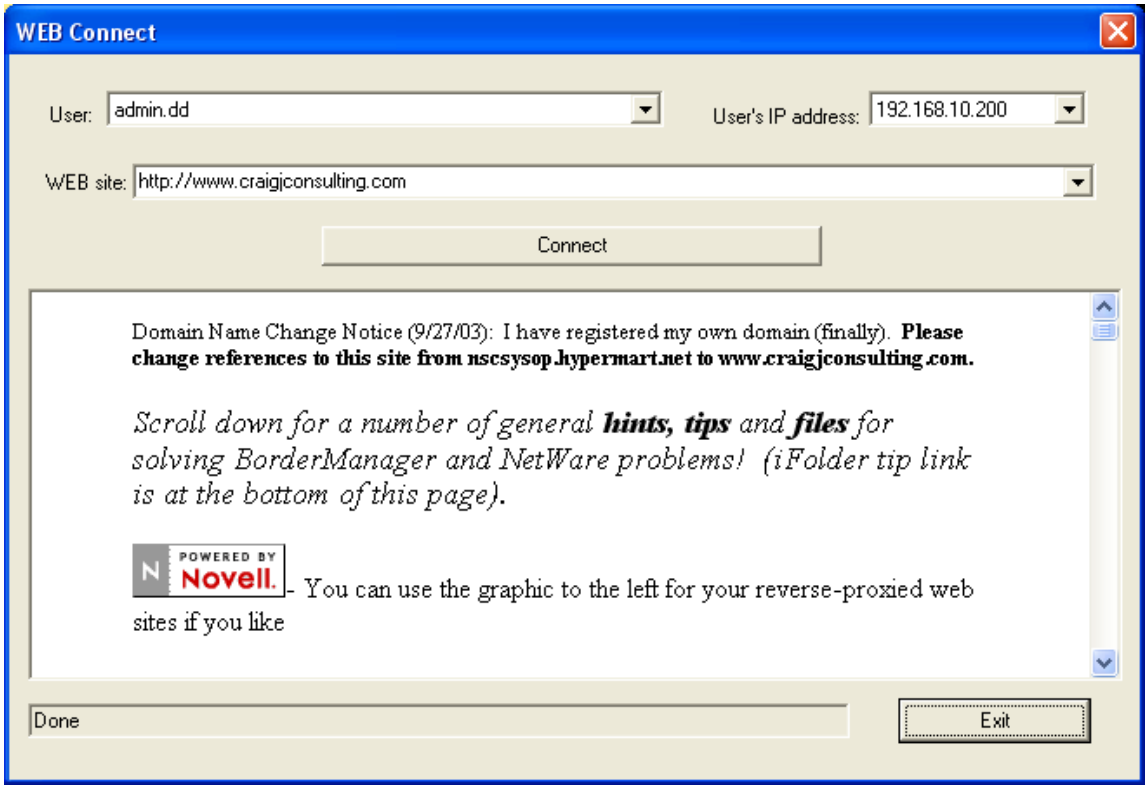
RTMonitor is not included with BorderManager. RTMonitor is an inexpensive (about $41) third-party Windows application that runs on your PC and constantly reads the common log file. The result is a nearly real-time listing of the most current users and the last 20 web sites they have accessed. You can even connect to the URL's to see what the web site looks like.

RTMonitor is available from http://www.caledonia.net. It is described in a tip at my web site, (http://www.craigjconsulting.com and the author, Victor Kulichkin's web site at http://www.kvy.com.ua/rtmon.htm. I have a 3-user demo version at my web site.



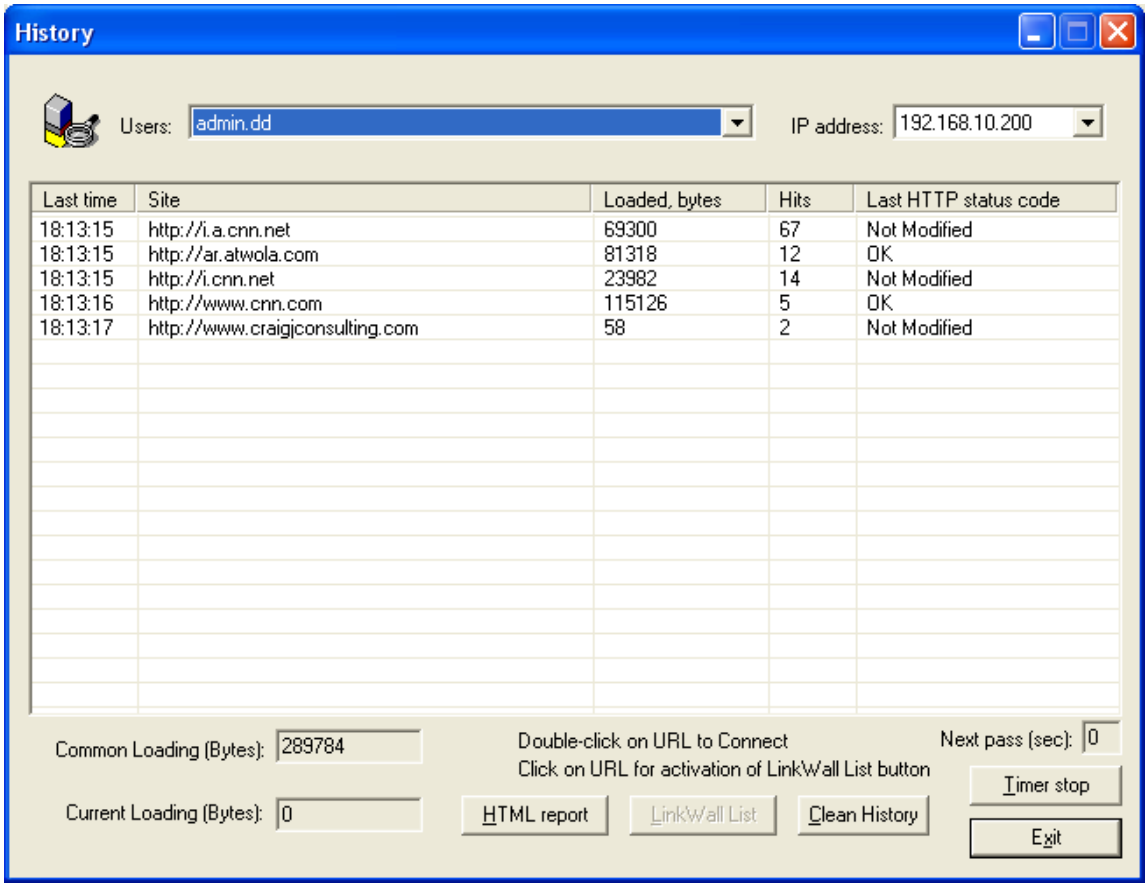
The screenshot above shows RTMonitor version 3.9.4 (beta) running, and showing that there are three connections in process on the server being monitored.

One connection is to www.cnn.com site, from a host at IP address 192.168.10.104. Another is for a local iFolder connection from a PC at 192.168.10.116. The other is for a connection from proxy-authenticated user Admin.dd, at IP address 192.168.10.200, accessing web site www.craigjconsulting.com.



Double-clicking on the www.craigjconsulting.com entry brings up the URL in a window. (This 'postview' function is dependent on Internet Explorer).

If you connect to a URL shown in RTMonitor, the next pass through the Common Log file by RTMonitor will show you as browsing to the site.



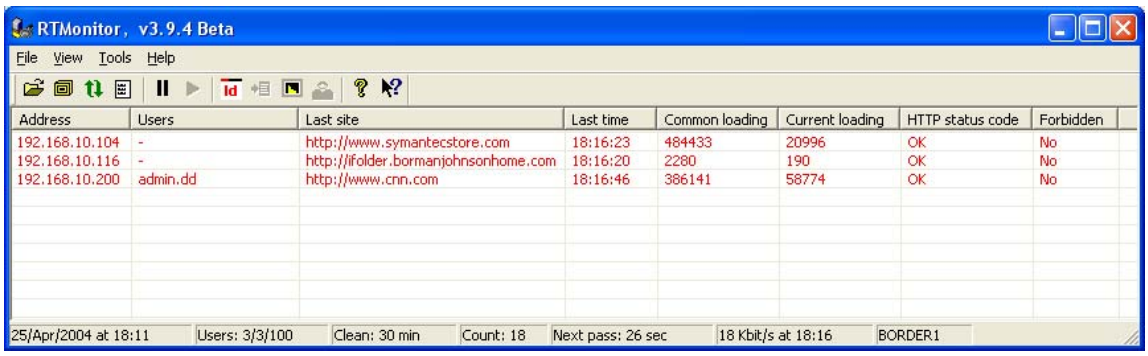
Right-clicking on an entry in the RTMonitor windows gives you the option to look at History. RTMonitor caches the last 20 URL's access by a host.

This is especially useful when URL's contain advertising links, such as www.cnn.com. Without the History option, you might see only the advertisement link, such as ar.atwola.com, without knowing that the host was actually just browsing the www.cnn.com web site.

This feature is also useful in seeing redirects that take place when visiting web sites, which is quite important when debugging access rules.

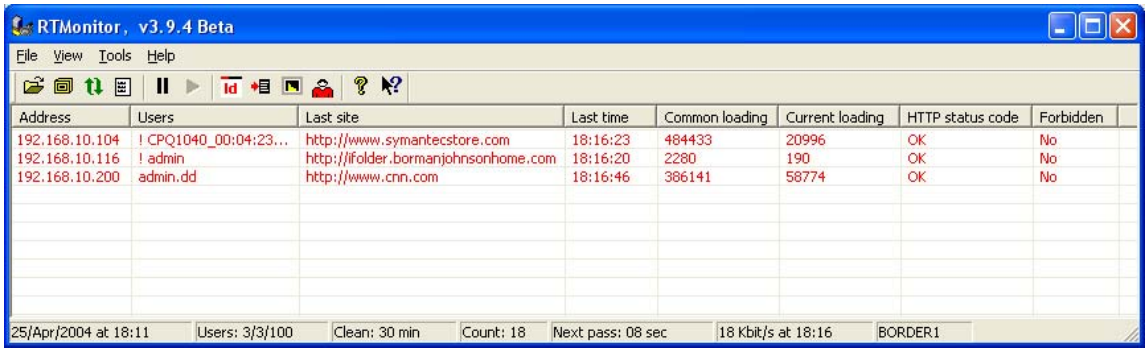
Discovering Who is Browsing Without Proxy Authentication

RTMonitor has an interesting feature that can allow you to see the logged-in name of users that are not proxy-authenticated.



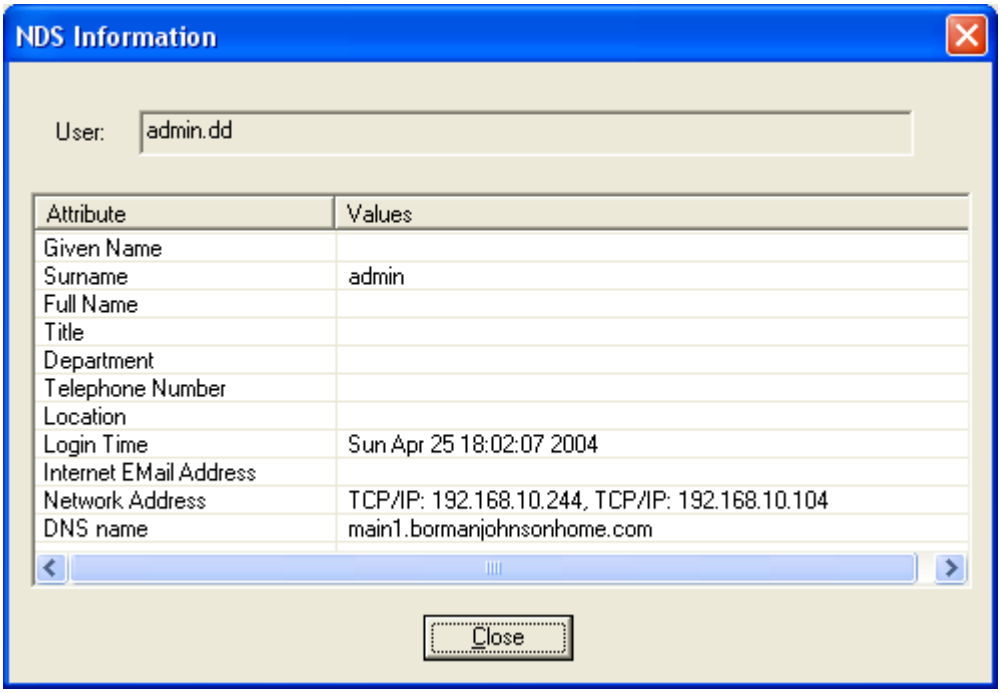
In the example above, someone at IP address 192.168.10.116 is browsing, but there is no user name shown.

Depending on your environment, you may be able to discover the identity of the user at IP address 192.168.10.116, by clicking on the id icon.



Now we can see that Admin is logged in at the IP address 192.168.10.116. RTMonitor has gone to the NetWare server and queried for a login name associated with the IP address 192.168.10.116.

All entries discovered in this manner are shown preceded by the ! character, so that you can tell if the user name was actually logged, or determined by IP lookup. Note that the user who browsed to the URL in the RTMonitor display might not be the user logged in when RTMonitor checks the name against the IP address.



Clicking on the admin.dd entry in the list, then clicking on the red user icon in RTMonitor causes RTMonitor to go to a NetWare server and try to find out details on the logged-in user. In the example above, some information on the user and the workstation is shown, pulled from NDS.

The newest versions of RTMonitor have several other interesting features:

- A graph of average HTTP proxy kbits/second through the HTTP Proxy, for the time that RTMonitor was active.
- A beep function to get your attention if a user has accessed a restricted page in the last analysis pass (403 permission denied).
- Highlighting of user data in bright colors (configurable) when they have attempted to access a restricted page.
- The ability to add selected URL's to a LinkWall blocking list, and tell LinkWall to refresh itself.
- A simple HTML-formatted summary of data held in RTMonitor memory.

Using RTMonitor

I find RTMonitor to be extremely useful for debugging access rules, since it shows me the actual URL that was requested almost immediately after my browsing tests. When a web site redirects me to another URL, or links to some unsuspected URL, RTMonitor shows me exactly what is happening so that I can adjust my access rules accordingly.

Some hints on how to make best use of this program:

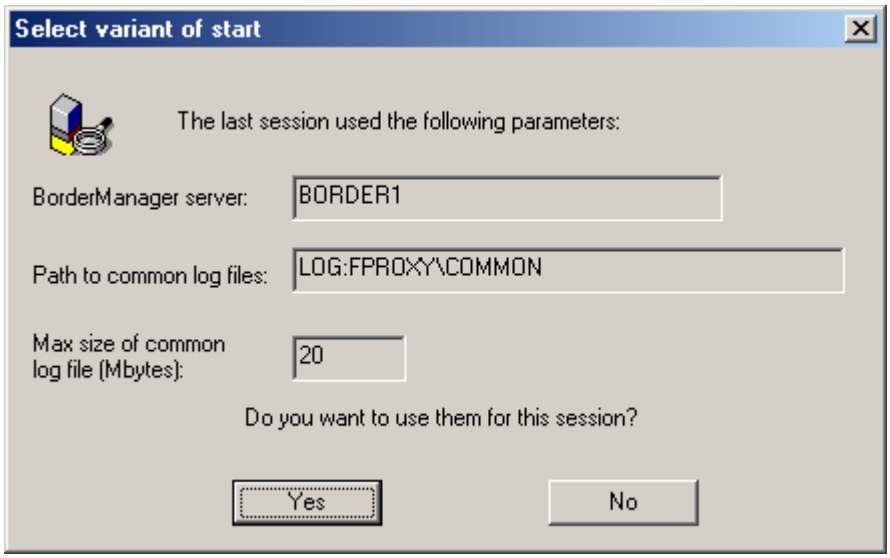
- Using this program requires you to have common logging enabled, so be sure to enable common logging. RTMonitor does not make use of extended or indexed log files.
- Because RTMonitor must parse through the most current common log file, it works best (fastest) if you have multiple small common log files, instead of very large ones. I recommend that you try to roll over your log files frequently, and at least try get them down to no more than 40MB each.
- Because RTMonitor caches the current log file on your workstation while working on it, you must reserve a certain amount of RAM in the program setup to hold the current log file. The default value is 10MB. If you roll your log files frequently, you can reduce the RAM limit for RTMonitor. If you have lots of RAM on your PC and like to have 50-60MB log files, you can increase the cache size limit in RTMonitor. (But RTMonitor will still take longer to parse a 60MB log file than a 10MB log file).
- You will only see a user name if Proxy Authentication is active and the user is authenticated. However, depending on a number of 'IF's', you may be able to have RTMonitor look up the IP address in a log file and associate it with the login name of a user that is at that same IP address. You do this by clicking on the icon that says ID in the latest versions of RTMonitor. All such entries will be preceded by a ! symbol.
- By default, RTMonitor makes another pass through the latest common log file 60 seconds after it completes a pass. However, it may take several seconds to parse the log file itself, so the actual (default) time between log file passes is 60 seconds + whatever time it takes for your PC to access and analyze your log file. Smaller log files are faster. You can change the idle time parameter if you don't like a 60 second delay between passes.
- Active connections are shown in red, while older connections are shown in black. After 30 minutes (default value) with no further activity, the user information is dropped from the RTMonitor display. Regardless of the time entered in the

'Clean Passive Users' parameter, only a certain number of users will be displayed. The default is 100 users, but in RTMonitor version 3.30 or later, you can change that value to quite a large number.

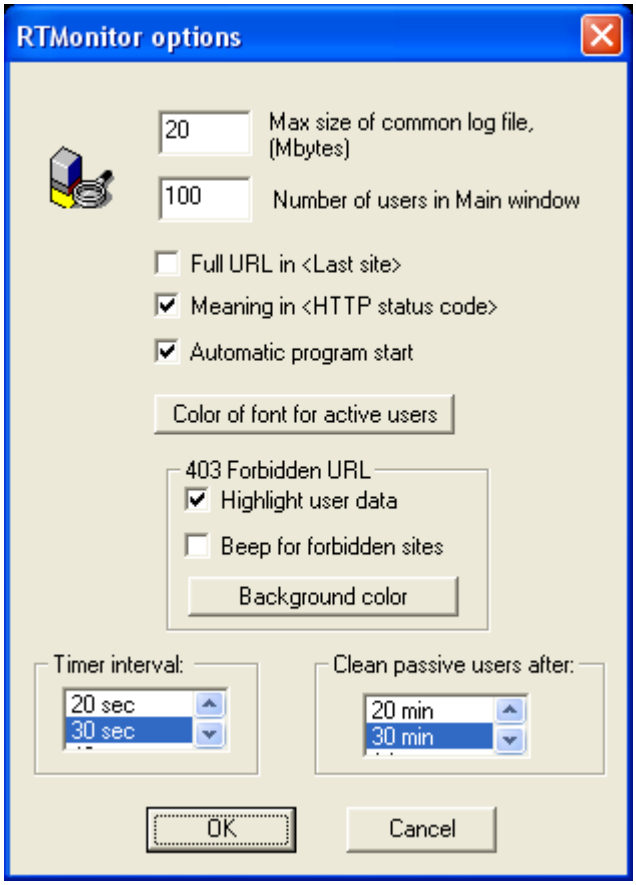
- You can have RTMonitor hold passive users for up to 24 hours in later versions.
- More enhancements are in work – RTMonitor is being constantly improved.

RTMonitor Configuration

Read the RTMonitor help file for additional information on how RTMonitor works. New versions of RTMonitor are adding new features and changing some of the limitations of earlier versions.



You must configure RTMonitor to point to the location of your proxy Common Log files. If you previously used RTMonitor, it should remember the last setting and be able to go directly to that log location.



RTMonitor should also be configured to reserve as much memory on the PC as it may need to cache all the data being read. In the screenshot above, RTMonitor reserves 20 MB of RAM for exclusive use. For very large log files and busy servers, you may need to reserve much more RAM – such as 60-80 MB.

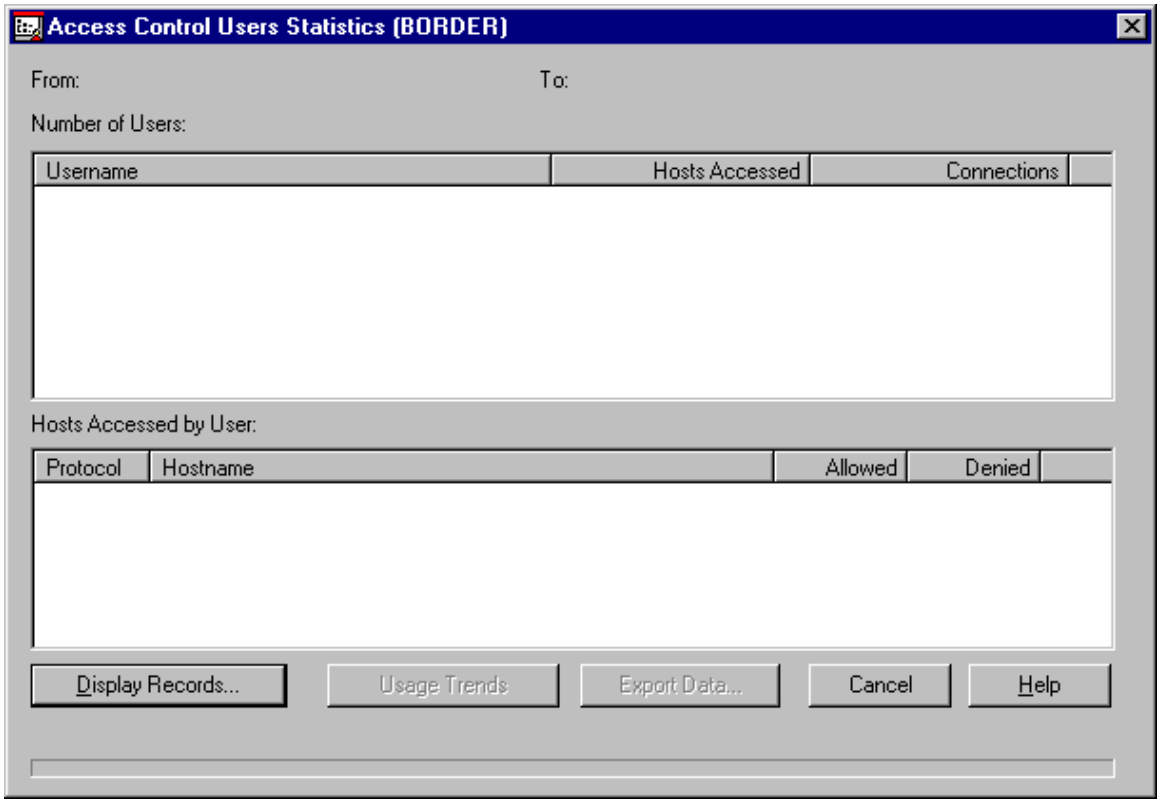
You can have RTMonitor display URL's that were forbidden in a bright color to immediately see if someone has been trying to browse to a URL forbidden by an access rule. You can also have the PC beep once if a forbidden code is seen in the current pass, to get your attention.

RTMonitor normally looks at your current Common Log file once every 60 seconds. You can change this, and the change will affect the amount of traffic you generate on the network accessing the log file. The example shows a Timer Interval of 30 seconds.

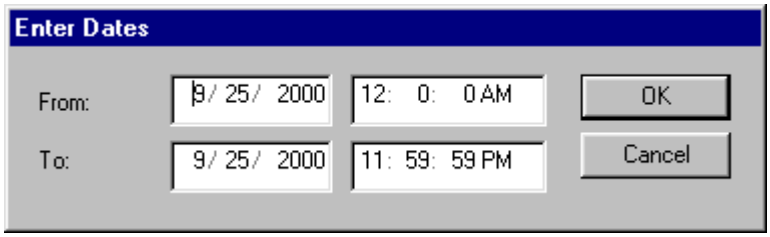
RTMonitor normally discards the current data (passive users) after 30 minutes. You can change the setting, but in any case RTMonitor can only hold up to 32767 records. If more than the maximum number of configured users access the proxy, RTMonitor will discard the oldest data.

Viewing Access Control Logs

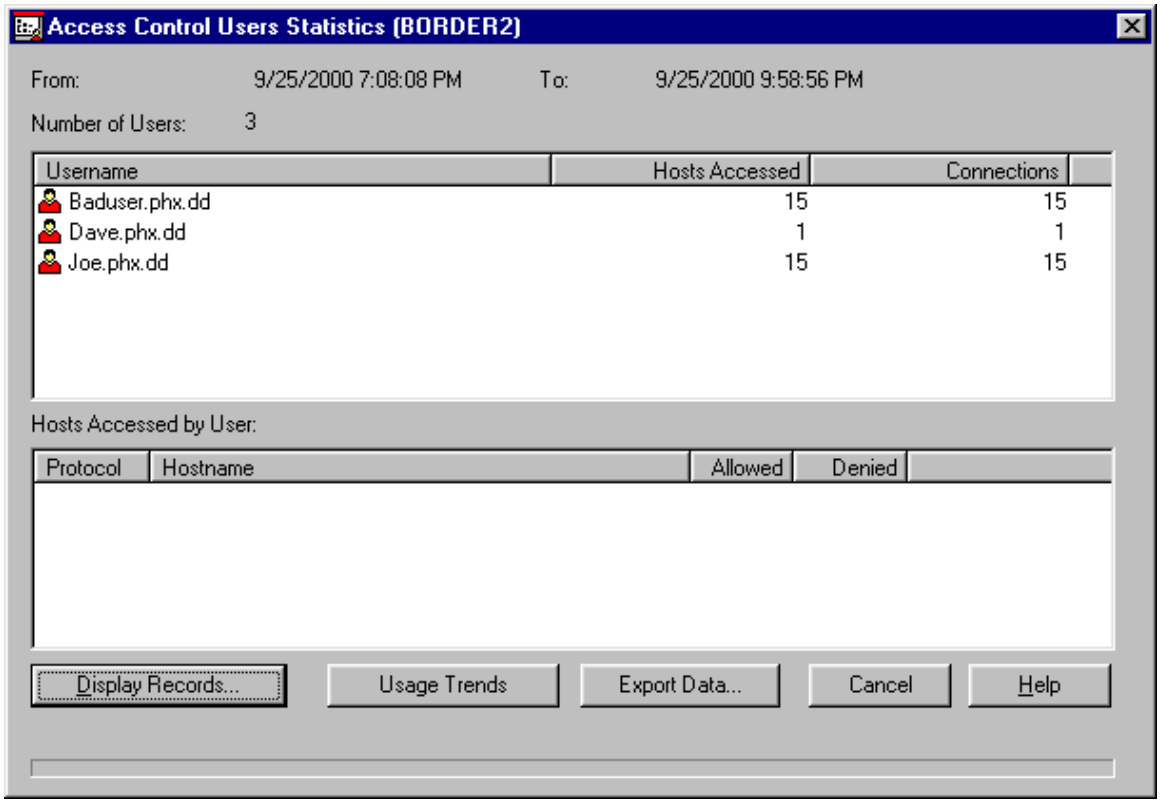
From the BorderManager control screen in NWADMN32, select **BorderManager**, then **View Access Control Logs.**



Now, click the **Display Record** button.



Enter a date range to search and press **OK**.



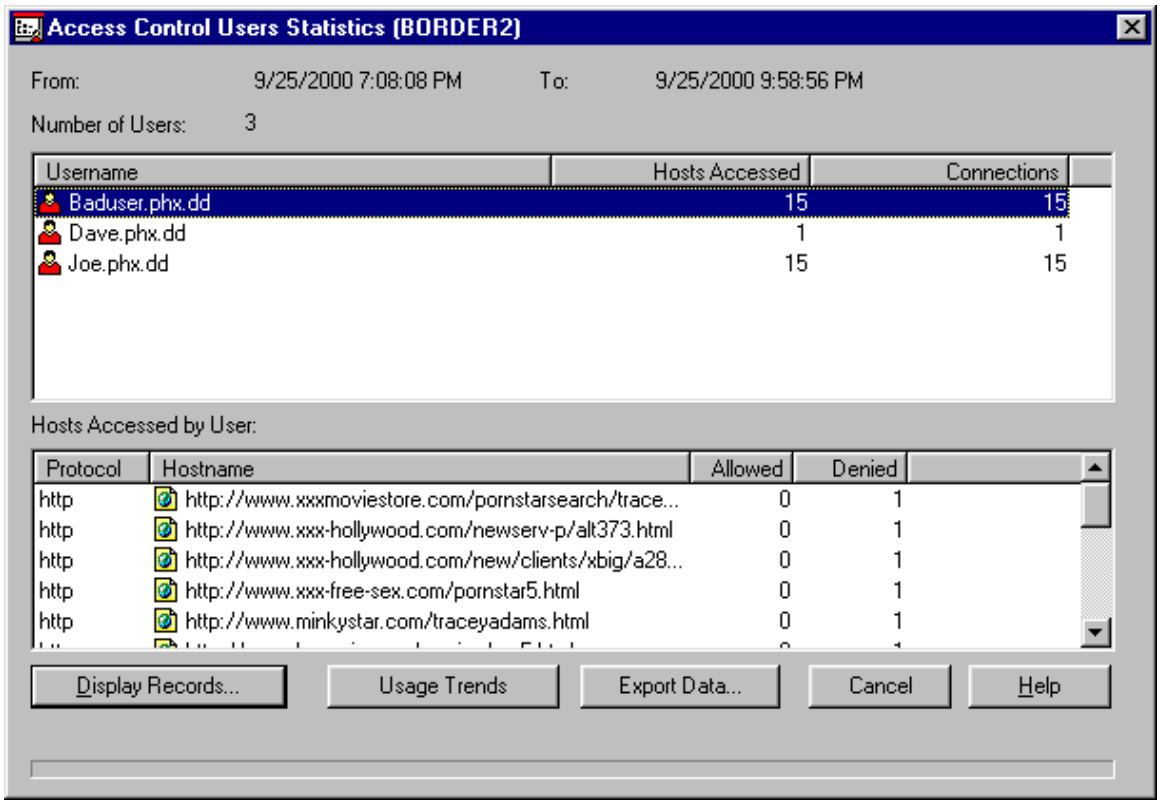
If you enabled **Rule Hit Logging** (on ANY Access Control Rule), you may have data for the date range selected. In the example shown, rule hit logging was enabled primarily for the CyberPatrol CyberNOT list denials, and for one IP address in particular. Clicking on a user ID/host IP address in the list shows the sites that that user attempted to access.

In the example shown, there are only a few users showing up. This is because only a limited range of records searched, and also because Access Control rule logging was only enabled on the CyberPatrol Deny rule for the time period searched.

Note If you are NOT using Proxy Authentication, you will NOT see the user ID's as shown in the example. You will instead see the IP addresses of the host PC's used when browsing. If browsing was done via a Citrix server, the same IP address (or user ID) would probably be shown in the log files as all Citrix users will have the same IP address.

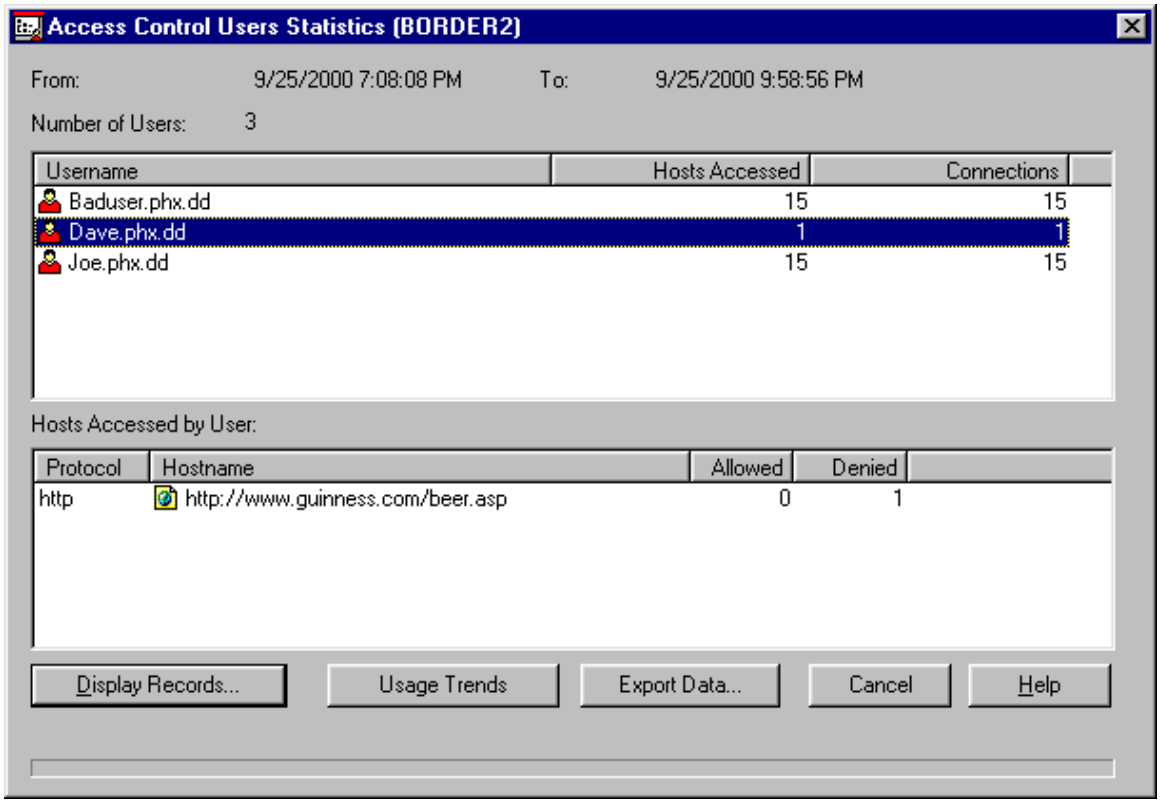
Remember – the ONLY data in the Access Control Logs will come from an Access Rule where Logging was enabled. In general, only enable logging for those rules in which you are really interested because the log files are limited in size. A good candidate for logging is any rule that does a denial of some service. You don't usually care if someone is browsing to acceptable sites. However,

should you be interested in seeing where a particular user is browsing (or you wish to see how much a particular subnet is browsing), you can set up a special rule (after the CyberPatrol deny rule probably) to allow certain IP addresses Any URL, and enable logging on that rule.

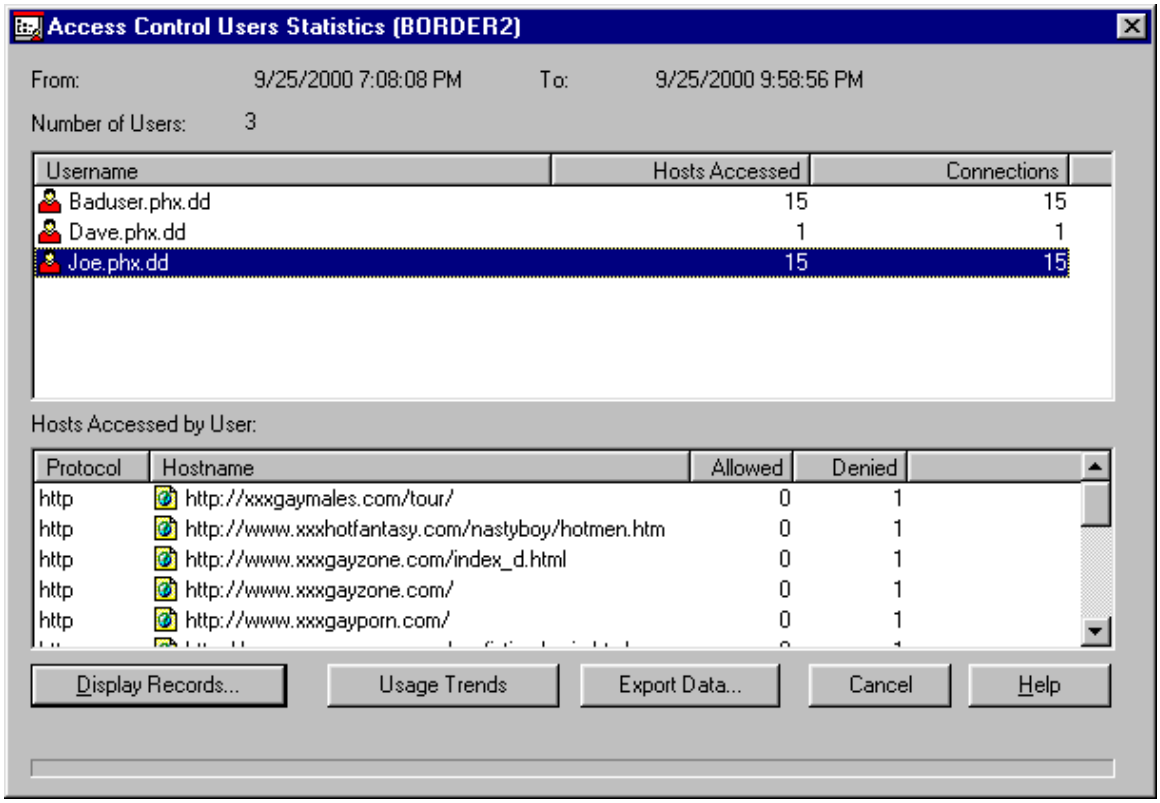


The example above shows sites accessed from a particular user ID.

Note You will only see the URL's accessed when using HTTP Proxy. If you are using Transparent Proxy, only the IP addresses of the hosts will be shown.



The example above shows another user that attempted to access a denied site, in this case an Alcohol-related site on the CyberNOT list.

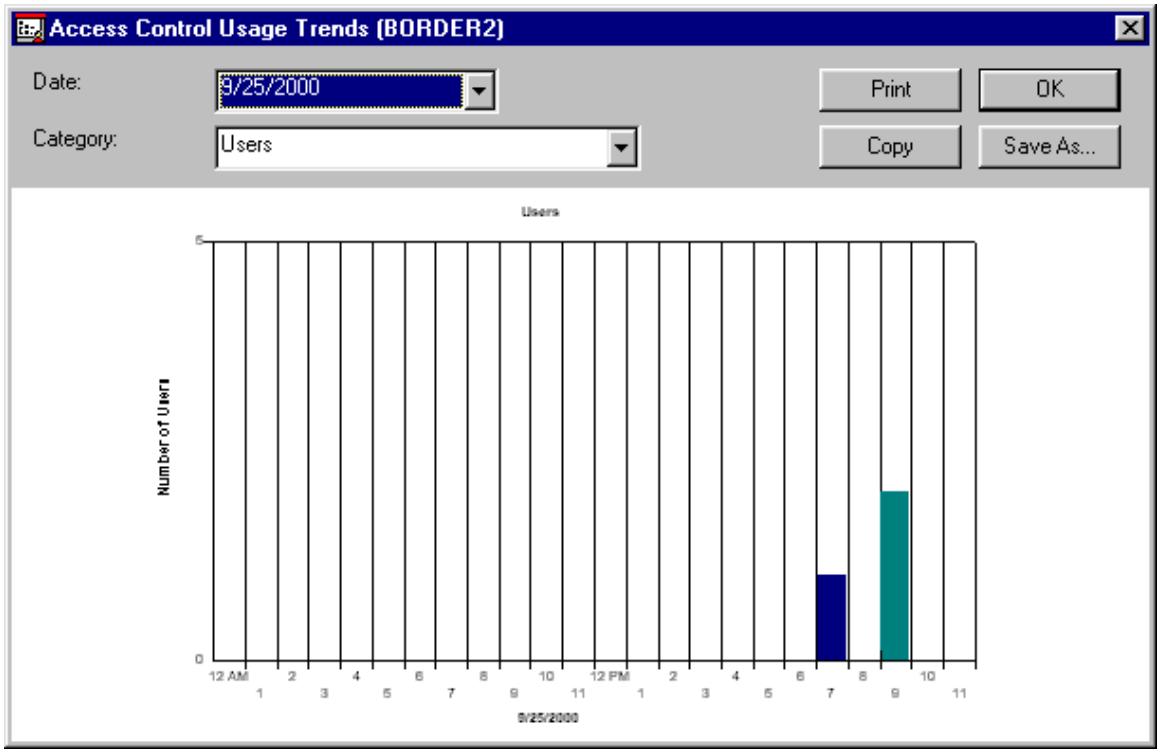


Here is the other user ID showing up in the Access Control Logs.

CAUTION *It is worth noting that the type of information that these log files turn up might be quite embarrassing or harmful if publicly revealed. There should be a policy in place from the Human Relations department or similar organization for handling access logging before you ever enable the logging process.*

Usage Trends

Once you have retrieved log file data (Access Control Log or Indexed Log data), you can make a simple graph of the data by selecting the **Usage Trends** button.



The chart graph above shows the number of users showing up in the Access Control Log data that was selected.

You cannot adjust the time scale for the Usage Trends graph. The data will be displayed on a 24-hour scale, which is primarily useful for seeing daily patterns.

Use the drop-down list in the Category selection at the top of the screen to show usage trends for:

- Users
- Hosts Accessed
- Access Volume
- Access Allowed
- Access Denied
- Users, Hosts, and Access Volumes

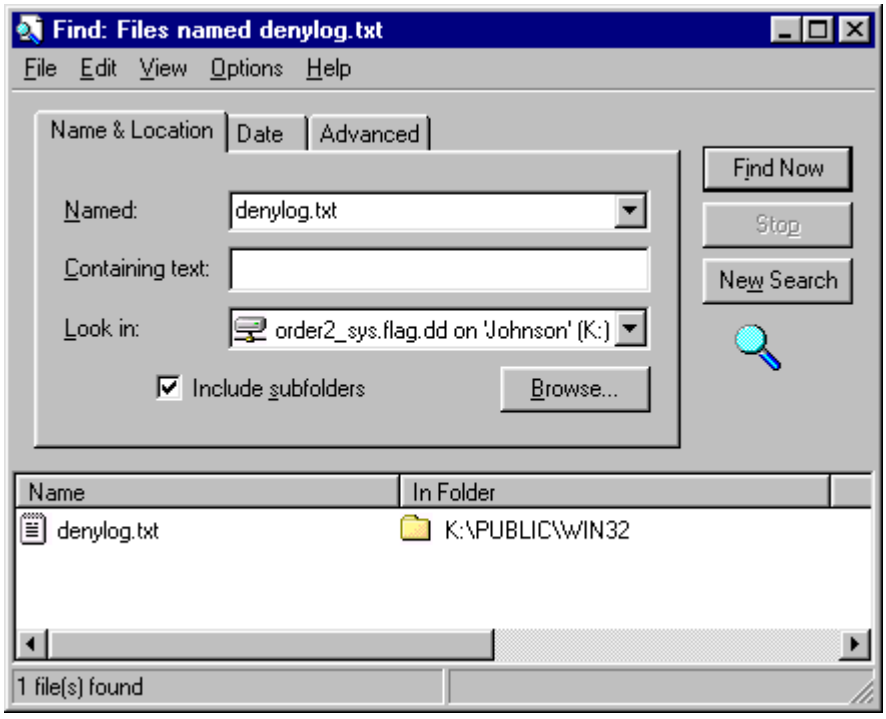
Exporting the Access Control Log to Excel

You may wish to export the Access Control Logs to a program such as Excel in order to manipulate the data in some way.

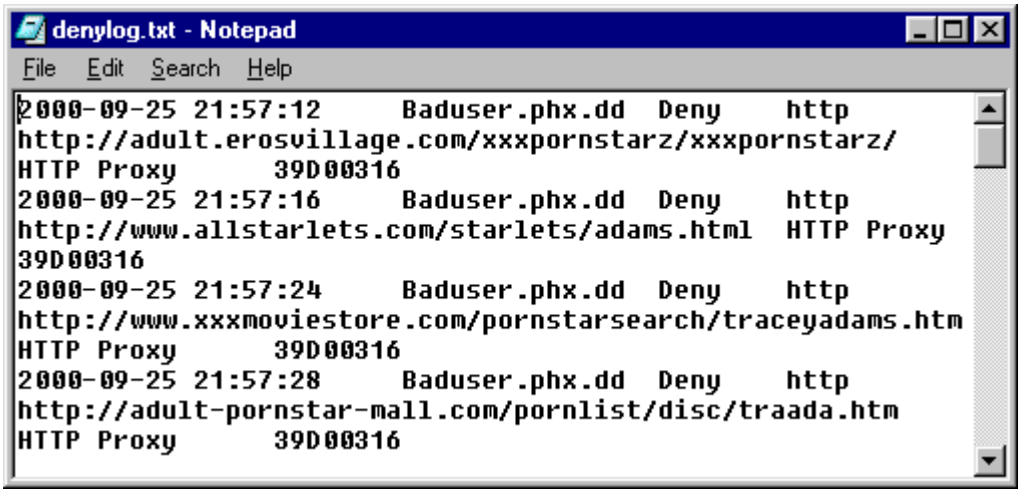
When viewing a date range containing Access Control log data, click on the Export Data button.

Enter a file name to store the exported data, and select a sort category. (You can sort the data later in Excel). Click on the OK button. In the example above, a file name of denylog.txt was entered, and because no drive letter or directory was specified, the file gets stored into the same directory that NWADMN32.EXE is in. This file will be saved in the SYS:\PUBLIC\WIN32 directory.

You should see data being written to the specified file.

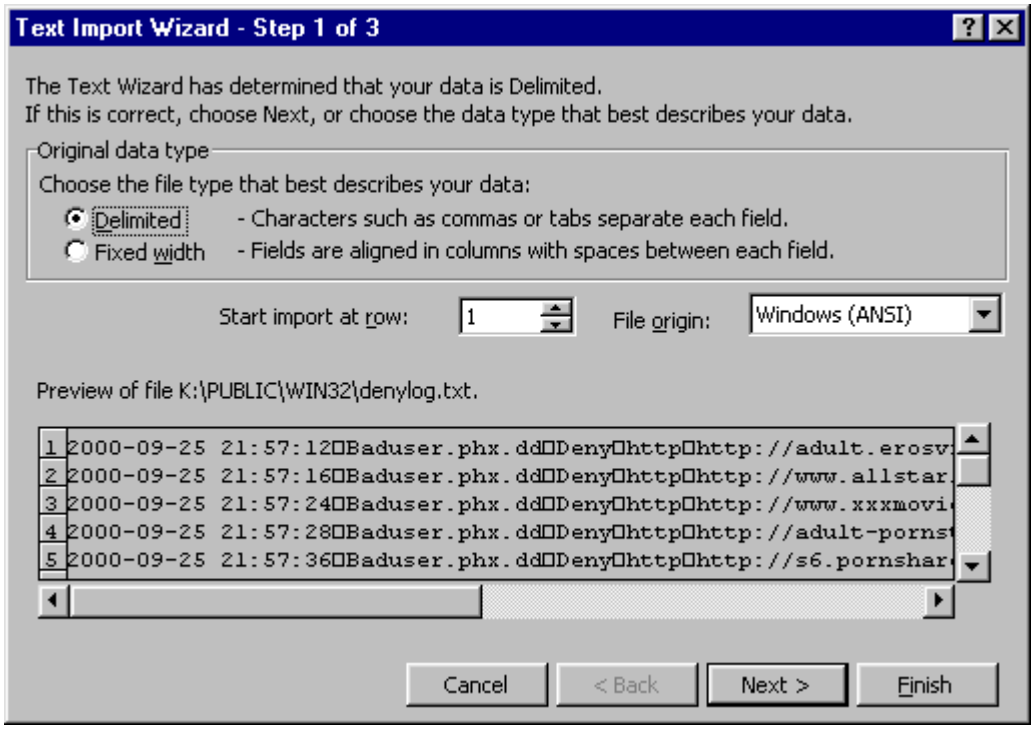


The example above shows where the file was saved.

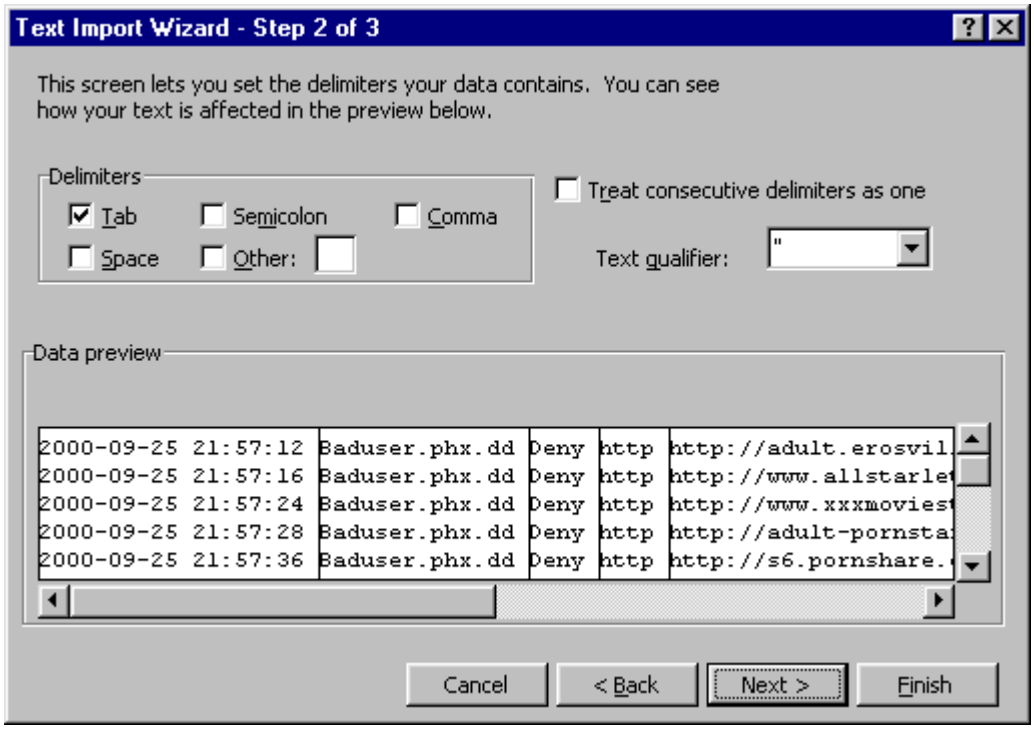


Here is the data as shown in NOTEPAD.EXE.

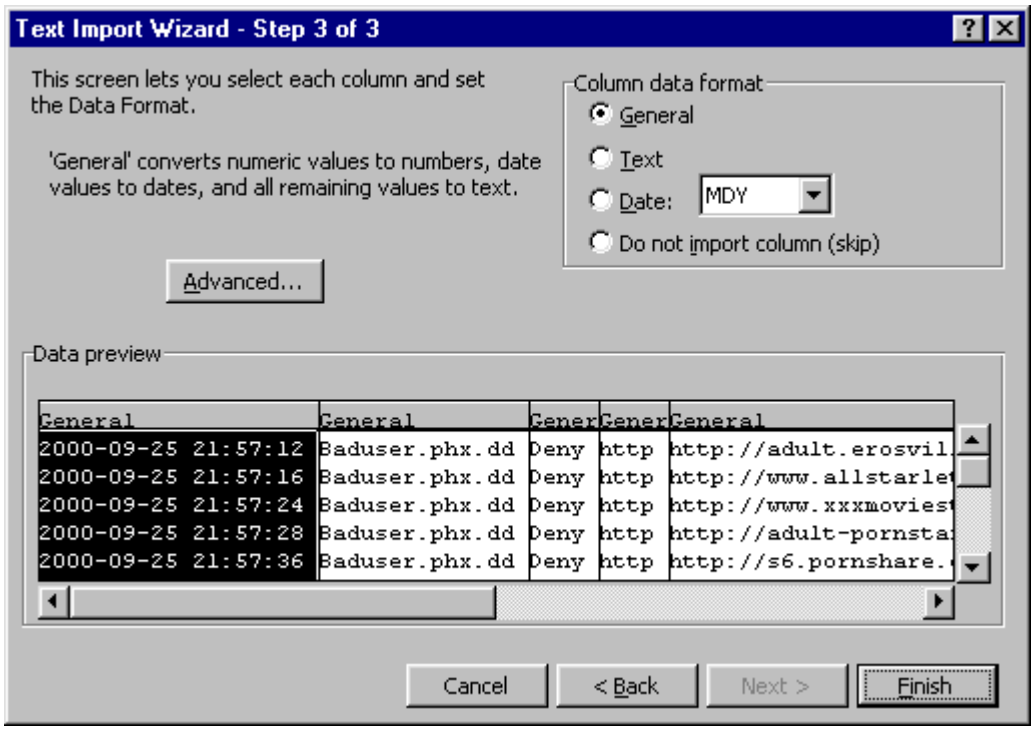
Once you have exported the data to a file, open Excel and import the text file using File, Open (show all files, not just XLS files).



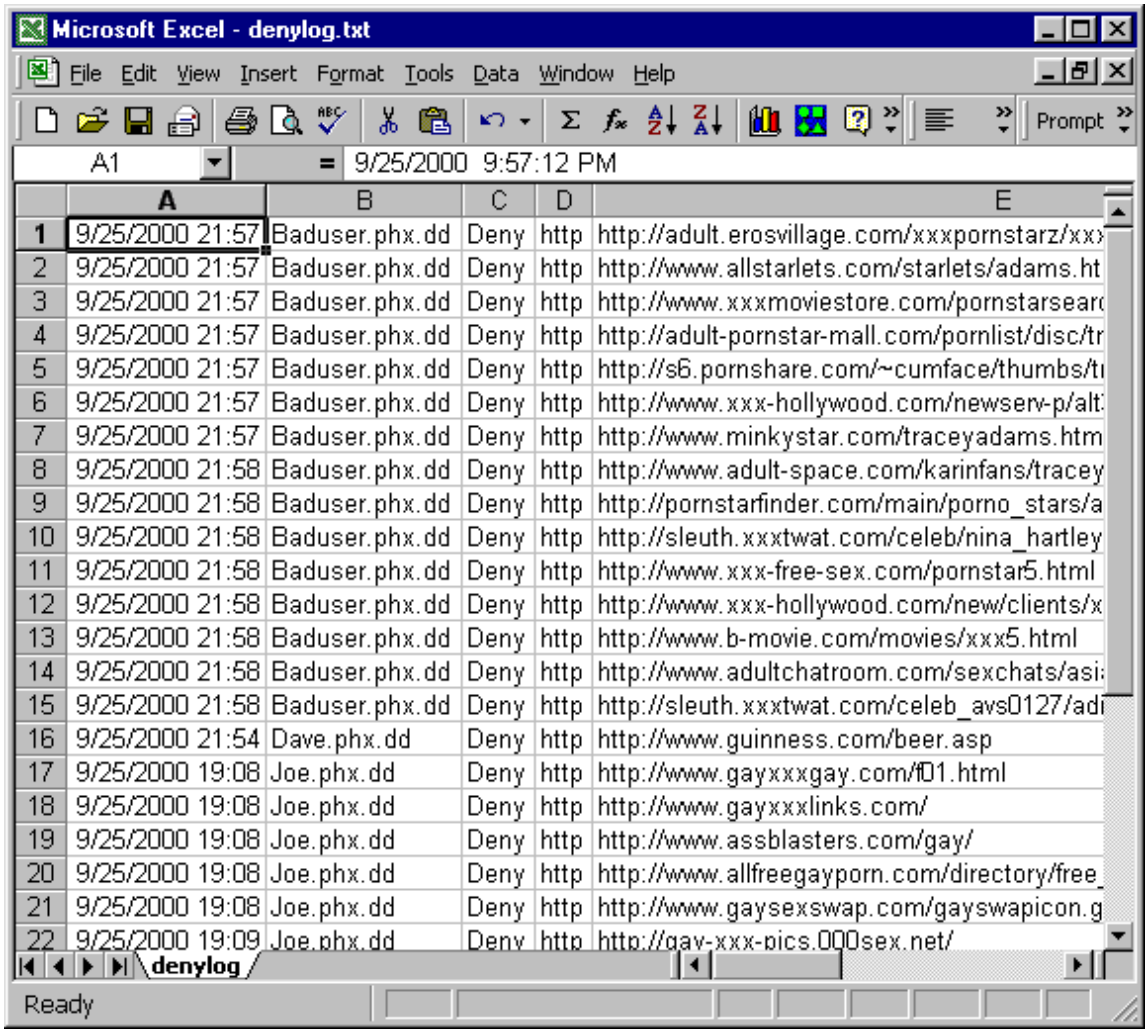
Excel will give you an option on how to interpret the data being imported, and the Delimited option seems to work well. Click **Next** to continue with the import.



Step 2 of the import wizard will suggest use of the Tab character as a delimiter, and it seems to work. Click **Next** to continue.



Step 3 allows you to set the data format for each column. You may want to experiment with these settings, and possibly skip some of the columns. Click **Finish** to bring in the data.



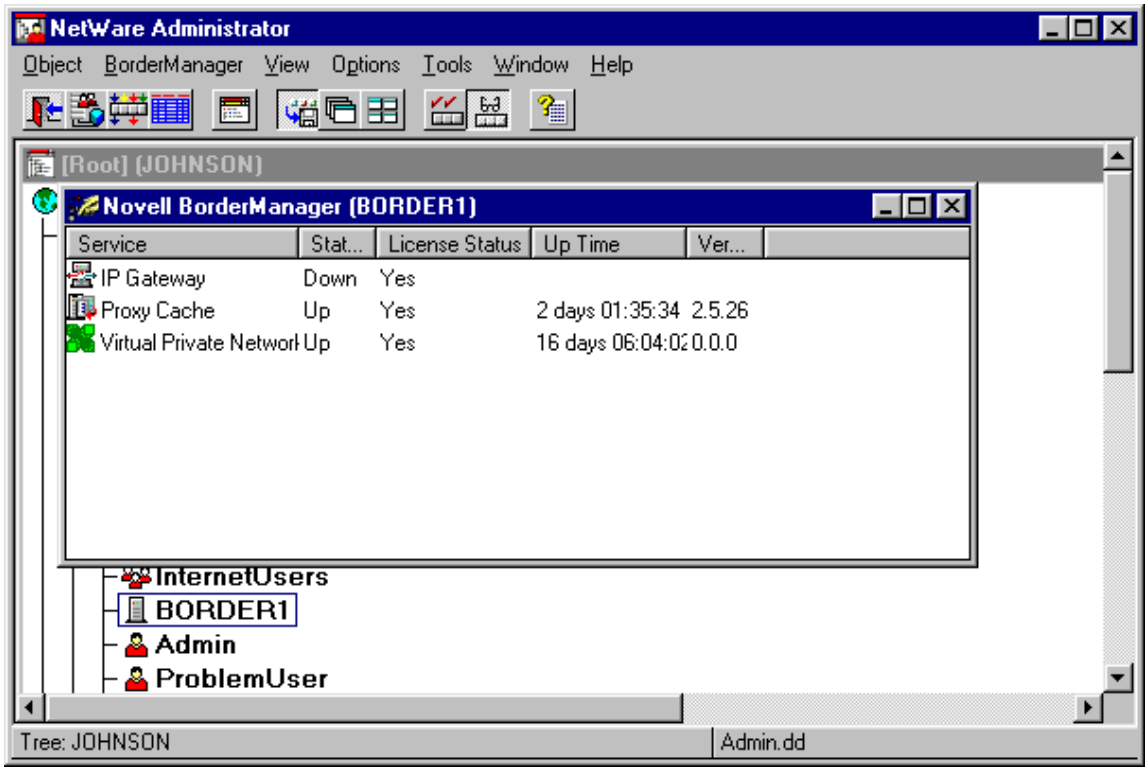
	A	B	C	D	E
1	9/25/2000 21:57	Baduser.phx.dd	Deny	http	http://adult.erosvillage.com/xxxpornstarz/xx
2	9/25/2000 21:57	Baduser.phx.dd	Deny	http	http://www.allstarlets.com/starlets/adams.ht
3	9/25/2000 21:57	Baduser.phx.dd	Deny	http	http://www.xxxmoviestore.com/pornstarsear
4	9/25/2000 21:57	Baduser.phx.dd	Deny	http	http://adult-pornstar-mall.com/pornlist/disc/tr
5	9/25/2000 21:57	Baduser.phx.dd	Deny	http	http://s6.pornshare.com/~cumface/thumbs/t
6	9/25/2000 21:57	Baduser.phx.dd	Deny	http	http://www.xxx-hollywood.com/newserv-p/alt
7	9/25/2000 21:57	Baduser.phx.dd	Deny	http	http://www.minkystar.com/traceyadams.htm
8	9/25/2000 21:58	Baduser.phx.dd	Deny	http	http://www.adult-space.com/karinfans/tracey
9	9/25/2000 21:58	Baduser.phx.dd	Deny	http	http://pornstarfinder.com/main/porno_stars/a
10	9/25/2000 21:58	Baduser.phx.dd	Deny	http	http://sleuth.xxxtwat.com/celeb/nina_hartley
11	9/25/2000 21:58	Baduser.phx.dd	Deny	http	http://www.xxx-free-sex.com/pornstar5.html
12	9/25/2000 21:58	Baduser.phx.dd	Deny	http	http://www.xxx-hollywood.com/new/clients/x
13	9/25/2000 21:58	Baduser.phx.dd	Deny	http	http://www.b-movie.com/movies/xxx5.html
14	9/25/2000 21:58	Baduser.phx.dd	Deny	http	http://www.adultchatroom.com/sexchats/asi
15	9/25/2000 21:58	Baduser.phx.dd	Deny	http	http://sleuth.xxxtwat.com/celeb_avs0127/adi
16	9/25/2000 21:54	Dave.phx.dd	Deny	http	http://www.guinness.com/beer.asp
17	9/25/2000 19:08	Joe.phx.dd	Deny	http	http://www.gayxxxgay.com/f01.html
18	9/25/2000 19:08	Joe.phx.dd	Deny	http	http://www.gayxxxlinks.com/
19	9/25/2000 19:08	Joe.phx.dd	Deny	http	http://www.assblasters.com/gay/
20	9/25/2000 19:08	Joe.phx.dd	Deny	http	http://www.allfreegayporn.com/directory/free_
21	9/25/2000 19:08	Joe.phx.dd	Deny	http	http://www.gaysexswap.com/gayswapicon.g
22	9/25/2000 19:09	Joe.phx.dd	Deny	http	http://gay-xxx-pics.000sex.net/

You should end up with data in a spreadsheet where you can sort by columns, cut data down to users or time periods of interest, etc. Set the column width using Format, Column, Auto-Fit Selection if necessary to display the data on the screen.

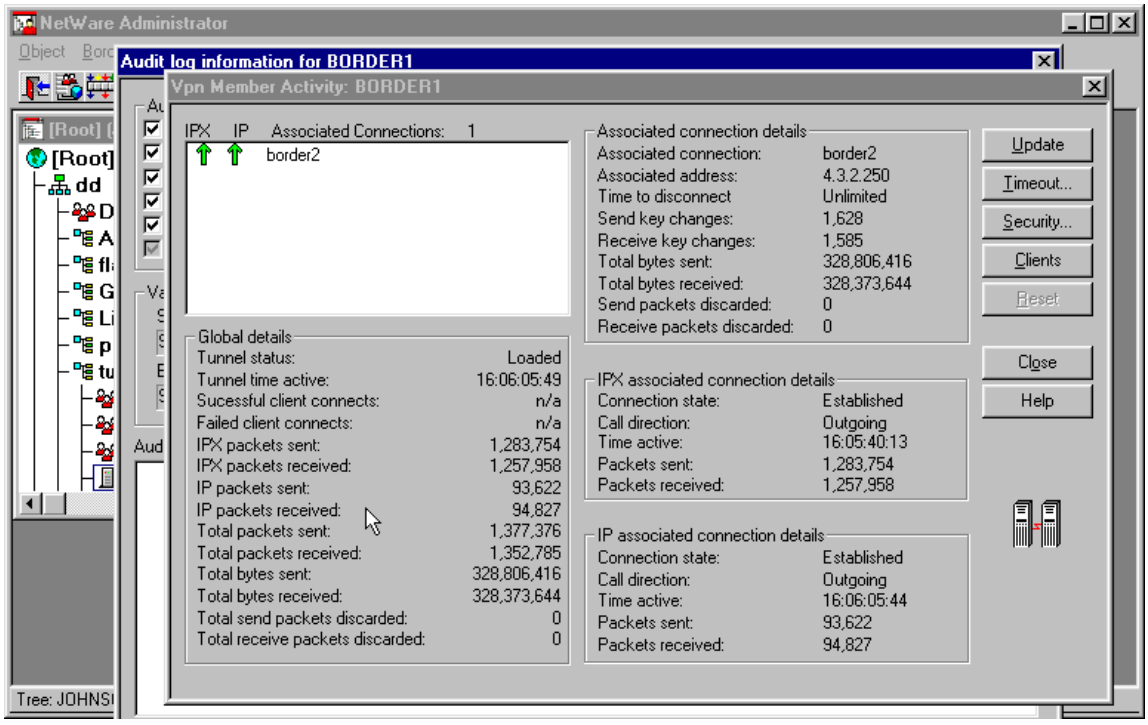
Viewing Legacy VPN Activity

From the BorderManager monitoring screen (highlight BorderManager server, and select Tools, BorderManager), you can view certain activity for legacy VPN. (The same capability for BorderManager 3.8 IKE-based VPN is done using Novell Remote Manager).

Double-clicking on **Virtual Private Network** will show you current VPN activity in real time.

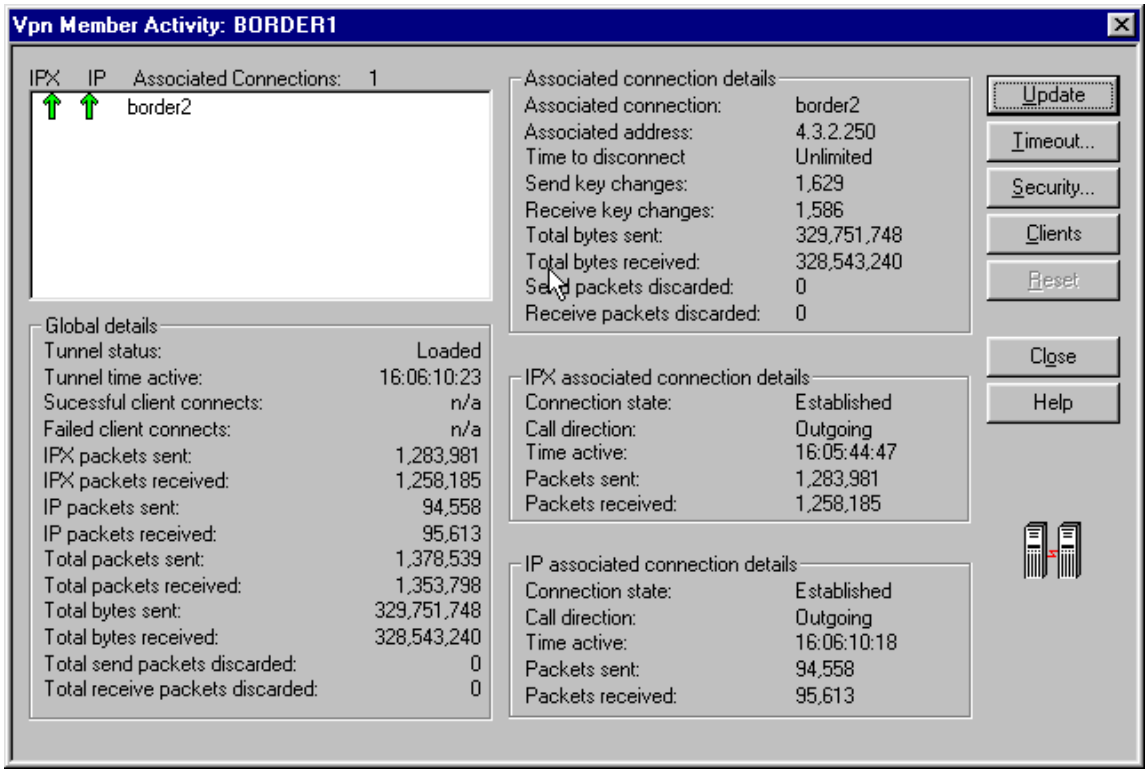


Clicking on the upper menu option **Object**, **View Member Activity/Log** menu option will allow you to see history and logged activity:



Click on **Virtual Private Network** and select **Object, View Member Activity / Log**.

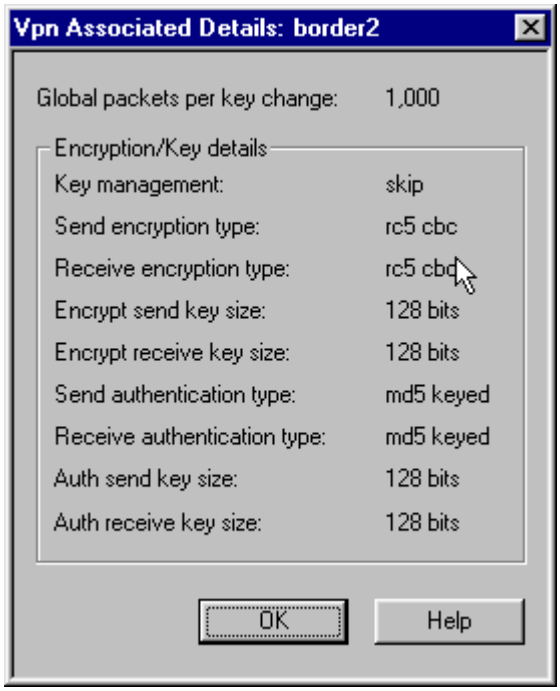
Note that two screens are opened, but one is partially hidden behind the other.



The first screen that comes up will show real-time Server-Server VPN activity.

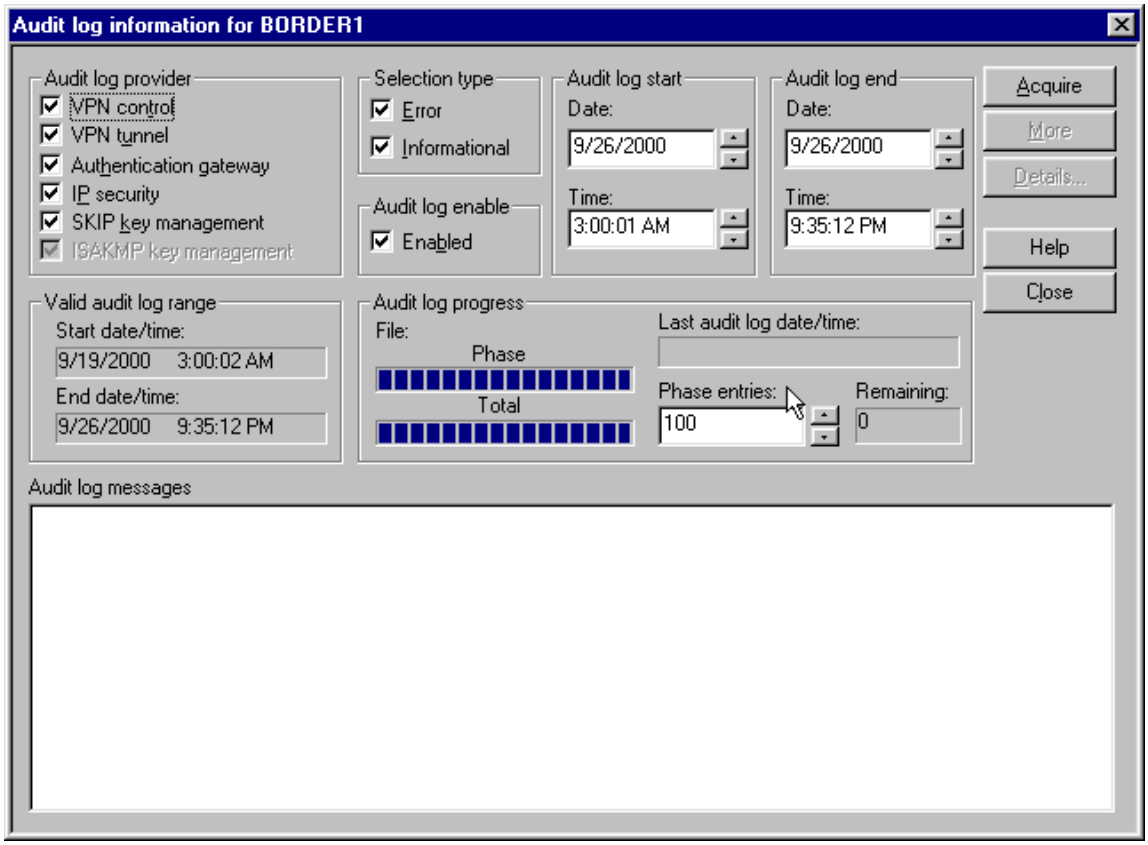
Click on the **Clients** button to see real-time VPN client-server activity. (Not shown here).

Click on the **Security** button to see details on encryption settings.

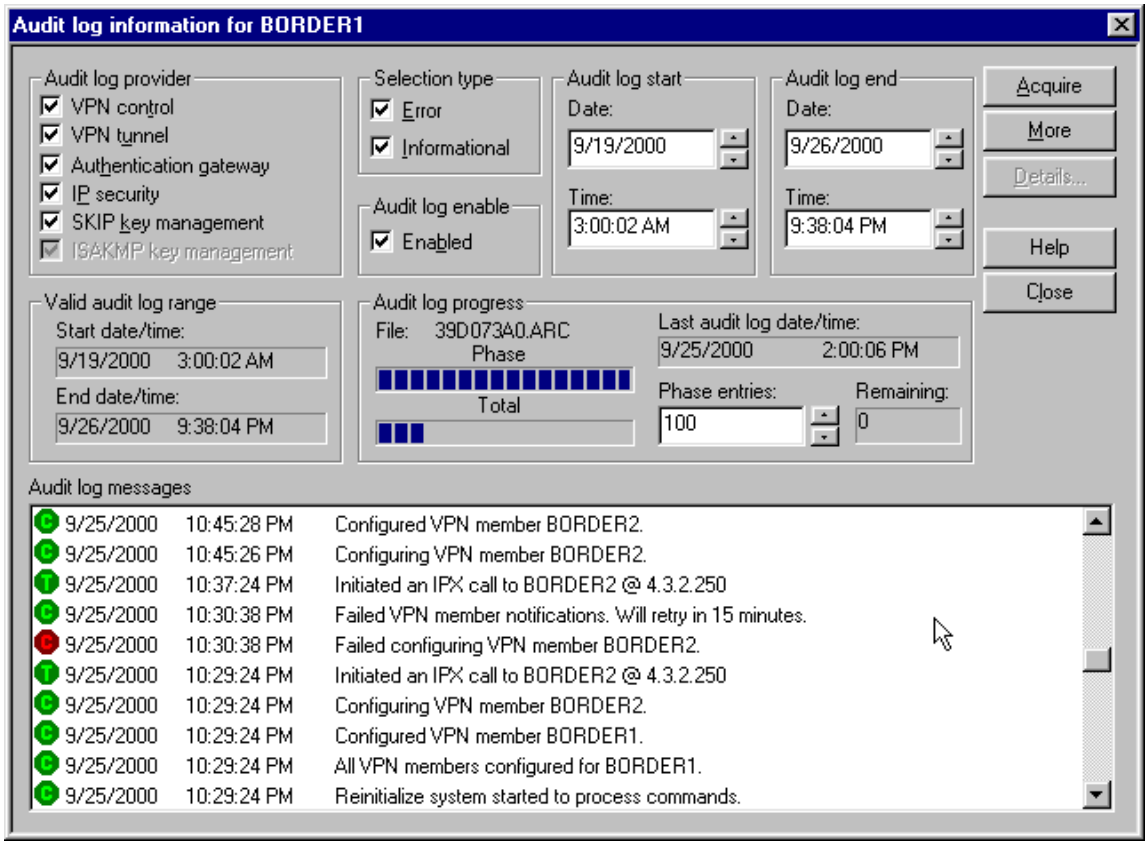


Click **OK** to clear this screen and return to the activity monitor screen.

Click on **Close** to close the Real-time activity screen and see the Audit Log information screen for VPN that is hidden underneath.



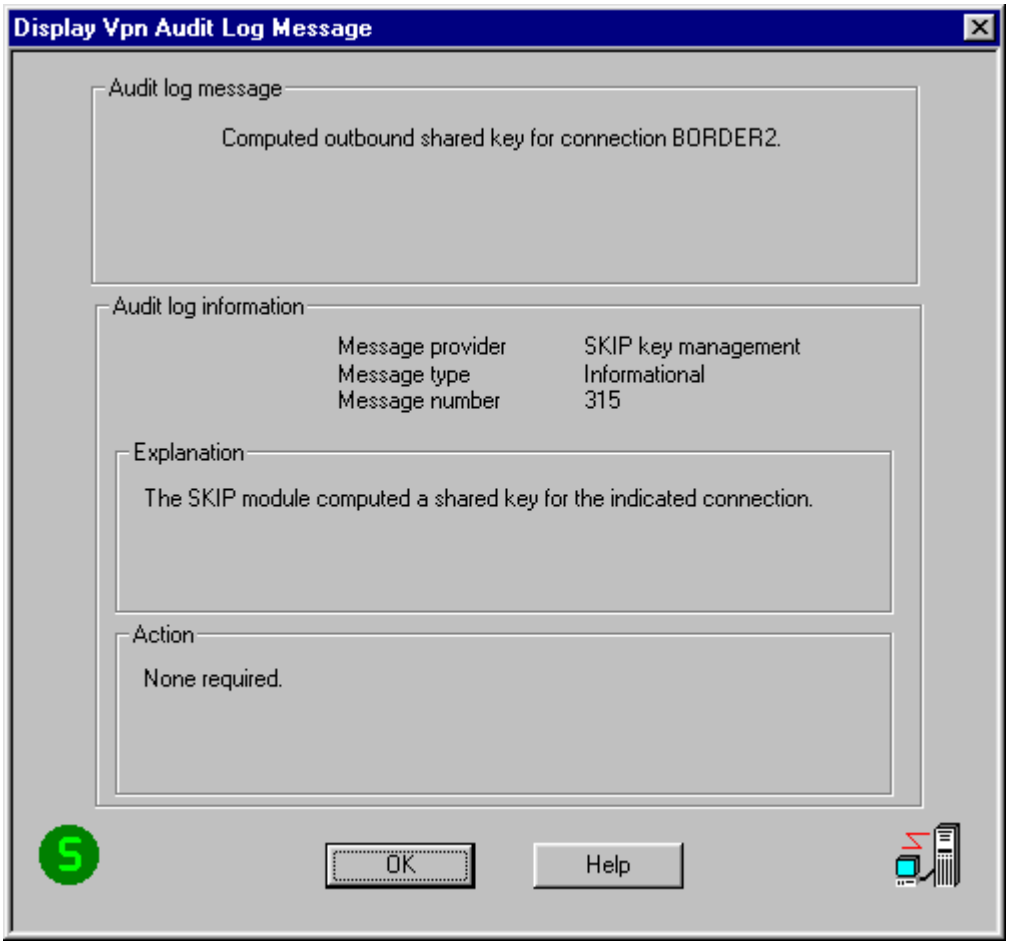
Enter a date range of interest and click the **Acquire** button to see VPN history.



The bottom window should show past VPN activity, and you can scroll through it. You can see both site-to-site and client-to-site VPN events in the bottom window, assuming both types of VPN are configured and there has been activity on both within the specified audit dates.

Click on the **More** button to see additional records.

Clicking on a particular record brings up a detail screen.



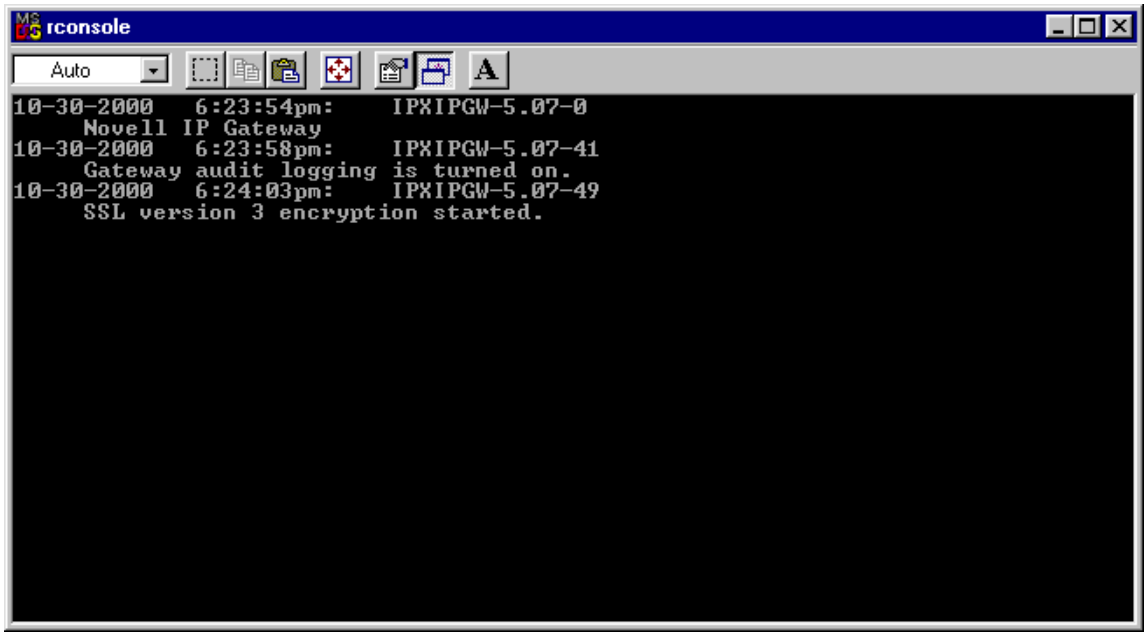
Viewing BorderManager 3.8 VPN Activity

VPN Monitoring for BorderManager 3.8 IKE-based VPN is done using Novell Remote Manager). Examples of this are shown in the chapter on viewing VPN activity.

Chapter 29 - BorderManager Console Screens

There are two BorderManager server console screens available that provide much useful information not available from NWADMN32. Each screen has multiple submenu screens. These screens are called PROXYCFG and the PROXY CONSOLE. The PROXYCFG screen shows how the BorderManager server proxies are configured, and the PROXY CONSOLE screen shows current activity for all of the BorderManager proxy services.

IP Gateway / SOCKS

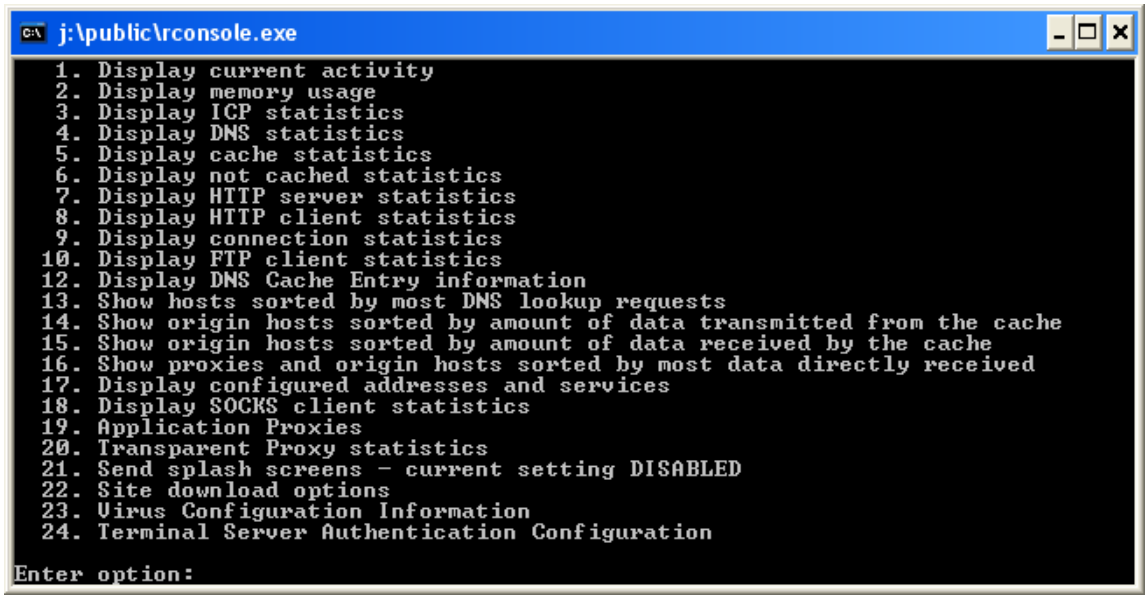


If you have enabled any of the Gateways (IPX/IP, IP/IP or SOCKS), you will have a BorderManager console screen called Novell IP Gateway Access Status.

On this screen, you should see various status messages for the Gateways themselves, and some error messages which might result from SOCKS client authentication.

Proxy Console

This screen is useful for day-to-day analysis and troubleshooting of the BorderManager proxy services.



BorderManager 3.7 with Service Pack 3 Proxy Console Screen

This screen might need to be 'uncovered' by pressing the space bar if one of its submenu screens is being displayed (particularly the site download results screen, or FastCache Current Activity screen).

Note The example shown was taken from a BorderManager 3.7 server patched to BM37SP3. Depending on your server's version and patch level, you may not have an Option 23 or 24.

Some of the most useful submenus from the Proxy Console screen are:

1. Display Current Activity – show the current FastCache activity.

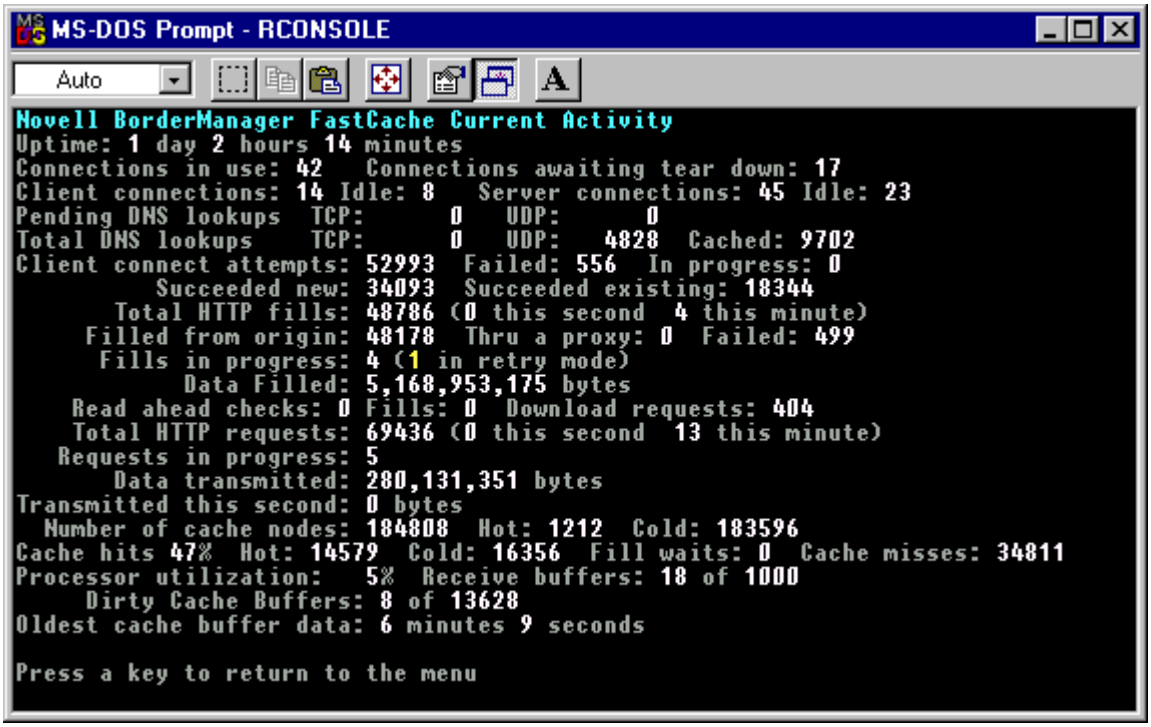
14. Show which hosts have transmitted the most data FROM the cache.

15. Show which hosts have transmitted the most data TO the cache.

19. Application Proxies, which helps to determine if traffic is being passed through one of the proxies, or denied by an access rule.

Option 1 - FastCache Current Activity screen

This screen shows the current HTTP / Transparent Proxy cache activity.



This screenshot is notable for the possible existence of a read-ahead bug, common in BorderManager 3.0 servers. Note the huge difference in amount of data received by the cache as compared to data transmitted from the cache. While a large difference might result from a read-ahead bug (which has been fixed in later BorderManager patches) a bit of investigation revealed that a user browsing to a webcam-enabled site caused the statistics shown above.

This screen is one of the most useful statistics screens for seeing how BorderManager is working. Note the following:

1. **Client Connections**: This value indicates the number of current connections the proxy has to web servers. It does not indicate the number of user connections to the proxy. The proxy may have multiple simultaneous connections to a web server.

2. **Server Connections**: This value indicates the number of current browser connections to the server. When a browser is actually retrieving data from a web site, it could have up to four simultaneous connections working at the same time.

3. **Cached DNS Lookups**: Note that all of the lookups are UDP, which is typical. The cached figure of 9702 indicates the number of URL's held in cache (both in memory and written to disk in the SYS:\ETC\PROXY\PXYHOSTS file). The default upper limit for maximum sites cached is 2500, so you can see that this server has had the limit increased. I recommend increasing the limit to 10,000.
4. **Client connections failed**: It is normal to have a small percentage of failures. You should keep an eye on this value to get a feel for what is a normal ratio in your environment. Failures include access rule denials as well as incorrect URL's typed into a browser.
5. **Fills in progress**: Shows the immediate demand in the server. The number in parentheses (1 in retry mode) indicates that one fill timed-out and is being retried.
6. **Data filled**: This number indicates the amount of data brought into the proxy cache.
7. **Data transmitted**: This number indicates the amount of data sent from the proxy to a browser. In this example, notice that the data filled is much higher than the data transmitted, indicating something to look into. When the data filled is much higher than that transmitted, it might indicate that there is a read-ahead bug at work, with a page being continually requested into the cache. If the server is patched, you should not have that problem. If read-ahead is disabled, you should not have that problem. In this case, the statistics screens 14 and 15 showed a large number of traffic coming from one site, but that same site did not show up as having a lot of traffic being transmitted from cache. Browsing to the site indicated that a web cam was active, resulting in the odd statistics. An access rule was set up to log the users accessing the site, and from the log file it was determined that a single user had been going to the site. Considering the bandwidth spent on that site, a gentle suggestion was made to try not to visit that site during working hours.
8. **Number of cache nodes**: These numbers indicated the individual blocks of data kept in cache. Hot nodes are those that are in memory and have the cached files on disk held open. Cold nodes are those that were cached earlier, but are not actually held as open files.
9. **Hot cache nodes**: The number of cached nodes held in RAM and not written to disk yet. When the maximum hot nodes value is reached, the server's browsing performance may slow down dramatically as the server waits for data to be written to disk and free RAM for new cache data. The default maximum hot nodes value is 7,000, and I routinely boost that to 50,000, via a NWADMN32 setting. The maximum hot node value that can be

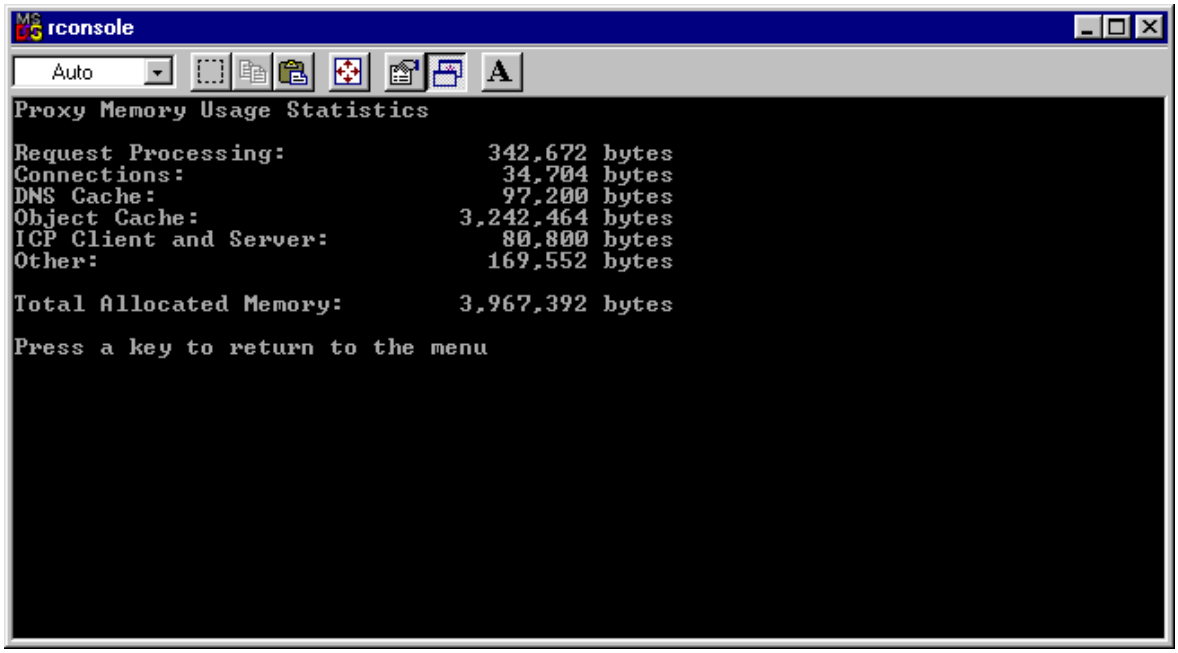
set is approximately 2/3rds of the maximum file locks, which is changed via a SET command.

10. **Cold cache nodes**: The number of cached nodes written to disk cache.
11. **Cache hits**: Hot cache hits are requests for data that were filled by data actually held in memory at the time of the request. For maximum performance, you would want this number to be large, and that takes RAM. Cold cache hits are 'second best'. Those are requests that were filled by finding the data written to disk in the cache volume(s). Cache misses indicate that a request was made and nothing was cached – the data had to come from outside BorderManager.
12. **Cache hits %**: The higher the number, the better. This is the percentage of requests that came out of the BorderManager server's RAM or cache volume. I have found that a 20-50% hit ratio is fairly typical, which means the cache has effectively doubled the bandwidth of the WAN link, as about half the data never had to be pulled in over the WAN link. The percentage varies widely depending on patch level of the server, entries in the PROXY.CFG file, entries in the Cachable Object Control menu in NWADMN32, and the sites being browsed.
13. **Oldest cache buffer data**: This value is a good indication of the need for more RAM. If the value is low (and the value shown, about 6 minutes, is quite low), you need to add more RAM. You should look at this figure when the server has been running for a few days, at the busiest time of day. This figure indicates that all the cache RAM was used up holding only about 6 minutes worth of traffic. A nice value is about 30-60 minutes or more, during a busy time.

In general, you should visit this statistics screen often enough to recognize what is normal, and what is not. It is a good idea to make some screenshots of this console screen and label it with the date, time and any relevant notes regarding the type of browsing activity that was going on at the time.

Option 2 – Display Memory Usage

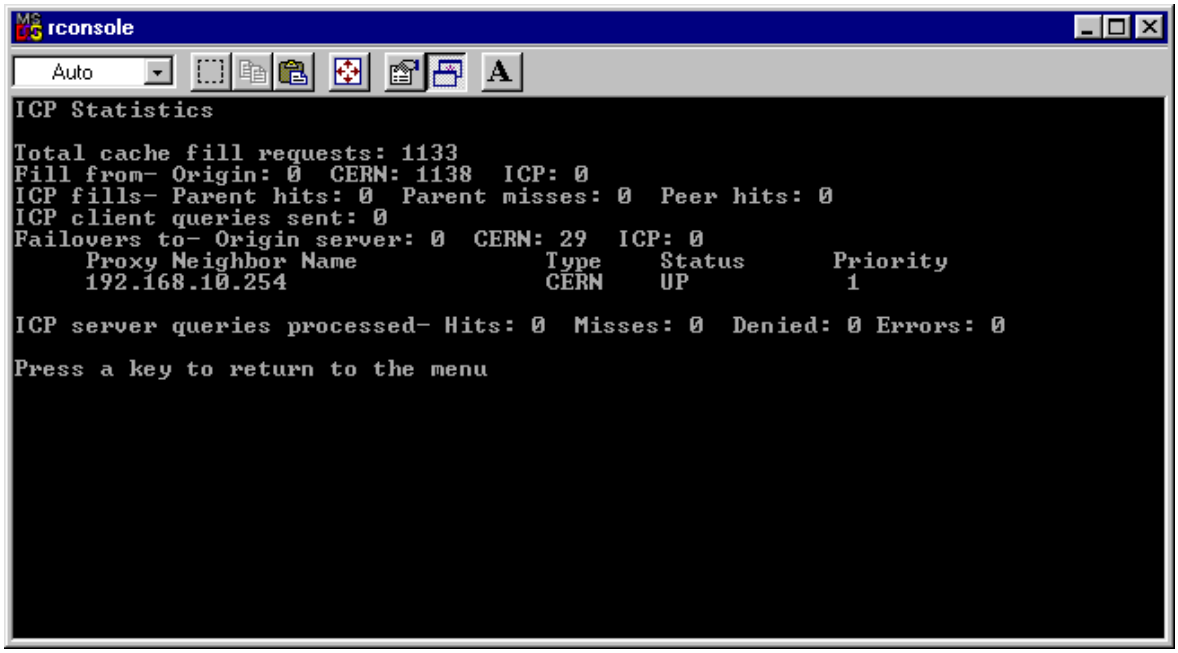
This Proxy Console option shows how much RAM is being used by the proxy components. This memory figure does not include RAM used for caching the HTTP nodes.



The memory usage screen is notable for two things: It generally shows that the proxy activity does not take much RAM. But don't think that this is all the RAM that is being used! This screen does not indicate how much RAM is being used for file caching, which is usually the bulk of the memory usage for BorderManager. Still, this screen might be useful in spotting unusual conditions, perhaps such as a memory leak problem in some BorderManager module.

Option 3 – Display ICP Statistics

This Proxy Console option shows statistics related to use of the Internet Caching Protocol (ICP) proxy cache hierarchy. Most of the statistics will be zero if a caching hierarchy has not been configured.

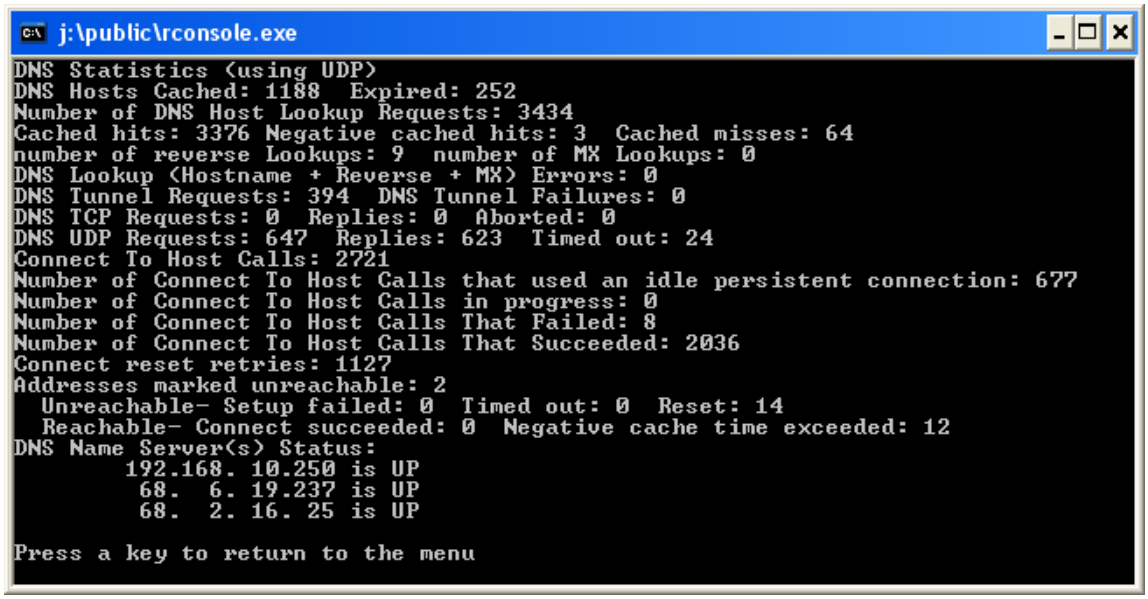


This screen will be useful in tracking activities for a cache hierarchy. The example shown indicates that all fill requests came from a CERN proxy neighbor.

Note The screen shown here, and the ones that follow were not all taken from the same server or at the same time. Some screen examples will clearly contradict others.

Option 4 – Display DNS Statistics

This Proxy Console option displays DNS query statistics performed by the HTTP Proxy.



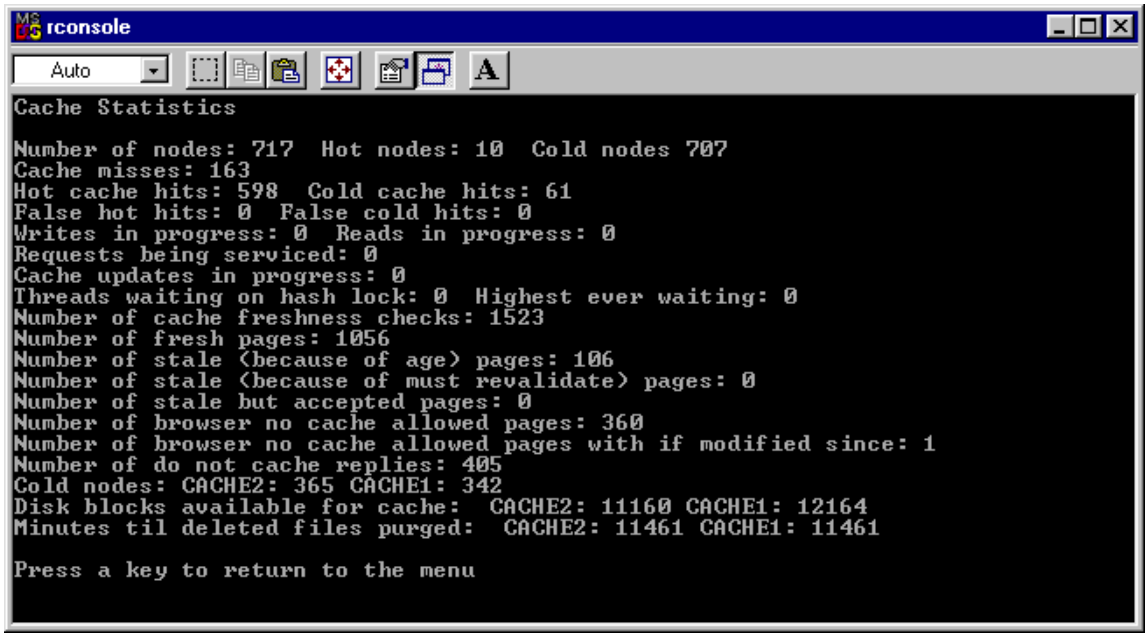
The DNS Statistics screen can be useful in spotting DNS problems. It is best to watch your server statistics to see what the normal patterns are from day to day.

A true warning sign is seeing the DNS server status going UP and DOWN a lot through the day. Those servers should almost never show a DOWN status.

BorderManager determines if a DNS server is up or down by periodically querying for the URL www.novell.com.

Option 5 – Display Cache Statistics

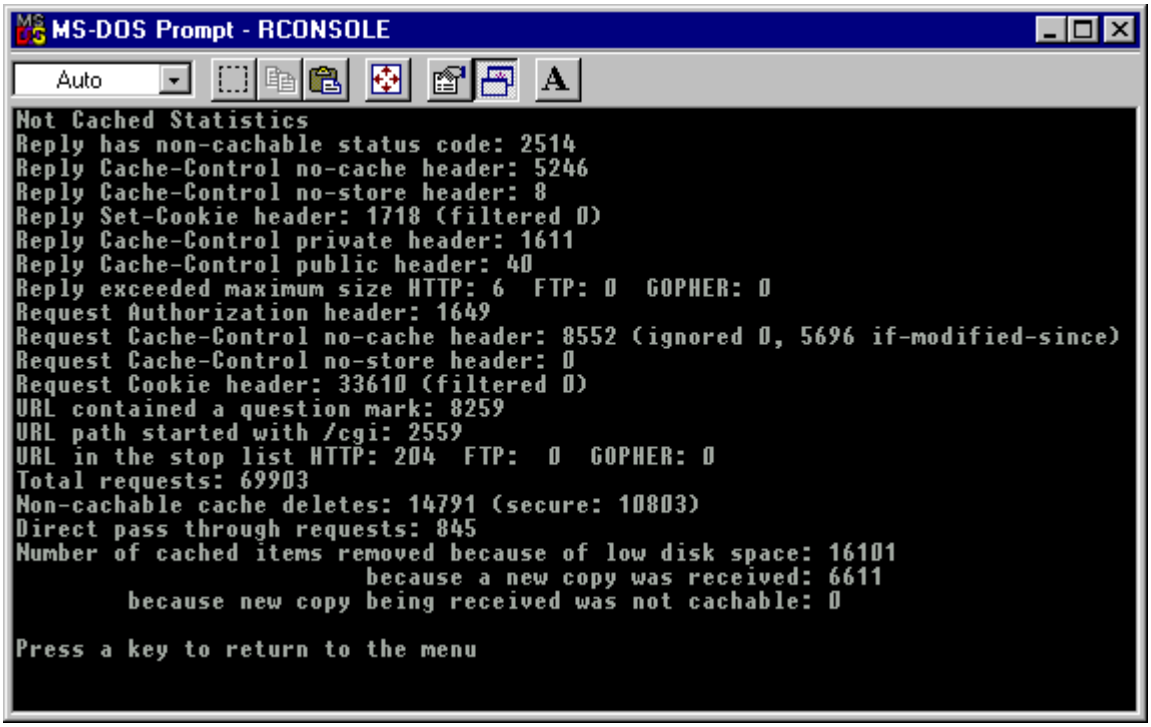
This Proxy Console option displays cache statistics for the HTTP Proxy.



If you want specific data on the HTTP Proxy itself, here is one place to find some. Note that toward the bottom of the screen you can see that multiple cache volumes are in use (CACHE1 and CACHE2) with approximately equal amounts of cached nodes.

Option 6 – Display Not Cached Statistics

This Proxy Console option displays not-cached statistics for the HTTP Proxy.

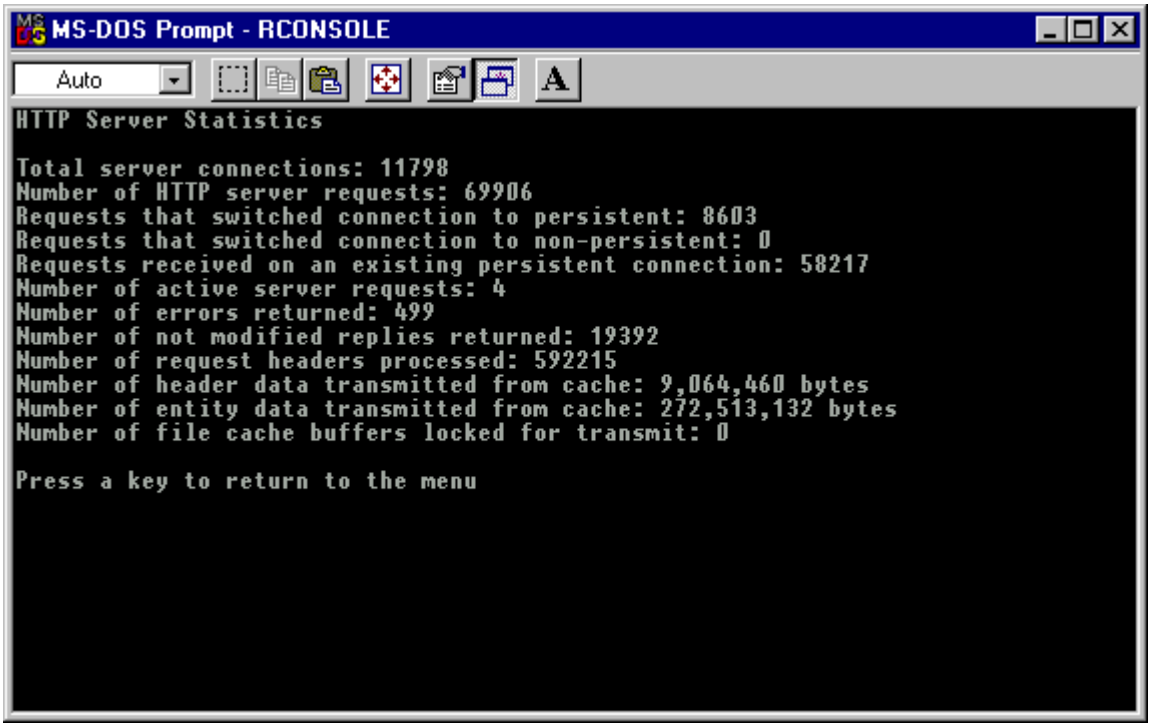


The Not Cached statistics give you some idea on what sort of traffic is passing through the HTTP Proxy without being saved to disk, and why. The example shown indicates that quite a few cache replies came through with HTML coding to bypass the proxy.

Note the URL in the stop list value. This number indicates the number of requests to URL's that were marked in NWADMN32, Cachable Object Control to not be cached. If you are debugging a non-cachable URL and need to see if it is not being cached, this screen should give you a good indication.

Option 7 – Display HTTP Server Statistics

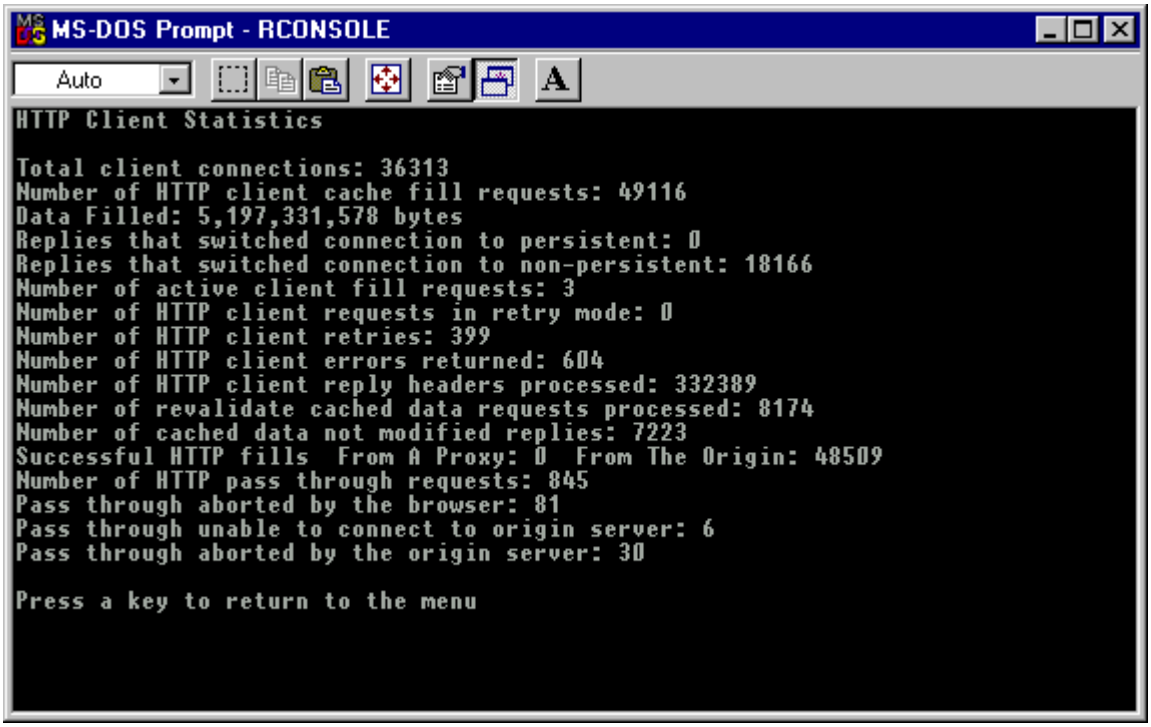
This Proxy Console option displays HTTP server statistics for the HTTP Proxy.



The data in this screen indicate traffic between the Proxy server and the origin server, and not the traffic between the Proxy server and a browser.

Option 8 – Display HTTP Client Statistics

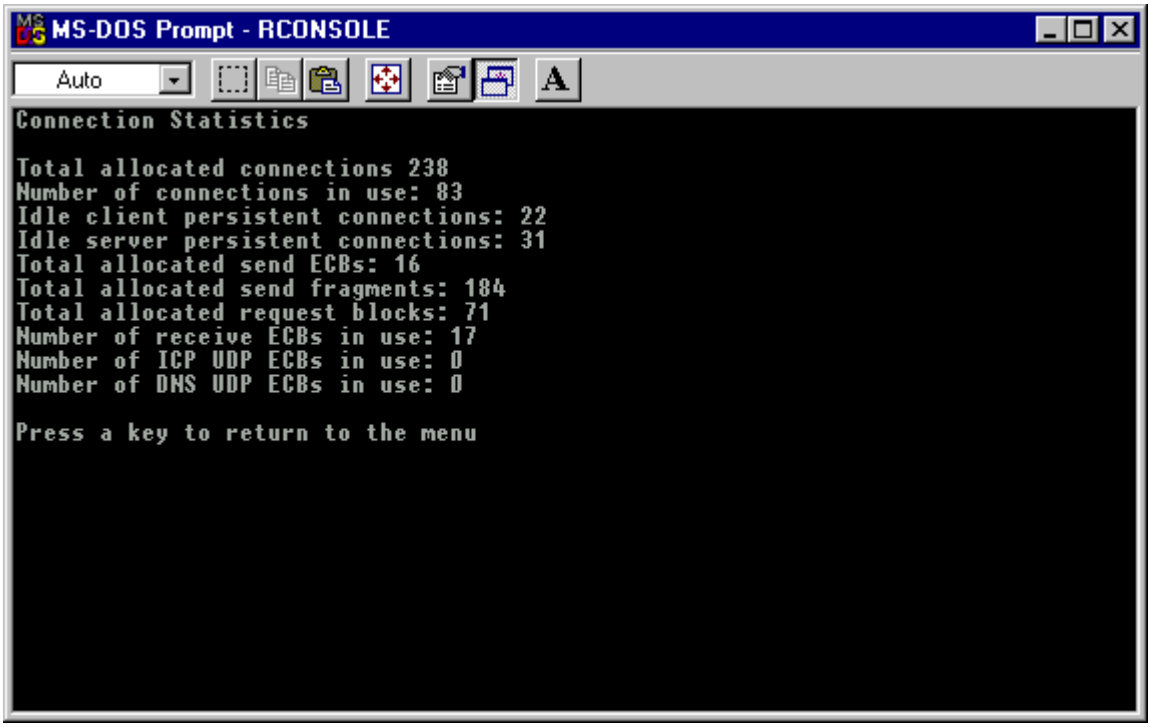
This Proxy Console option displays HTTP client statistics for the HTTP Proxy.



Unlike the previous Proxy screen, this screen shows statistics for the traffic between the Proxy server and browsers.

Option 9 – Display Connection Statistics

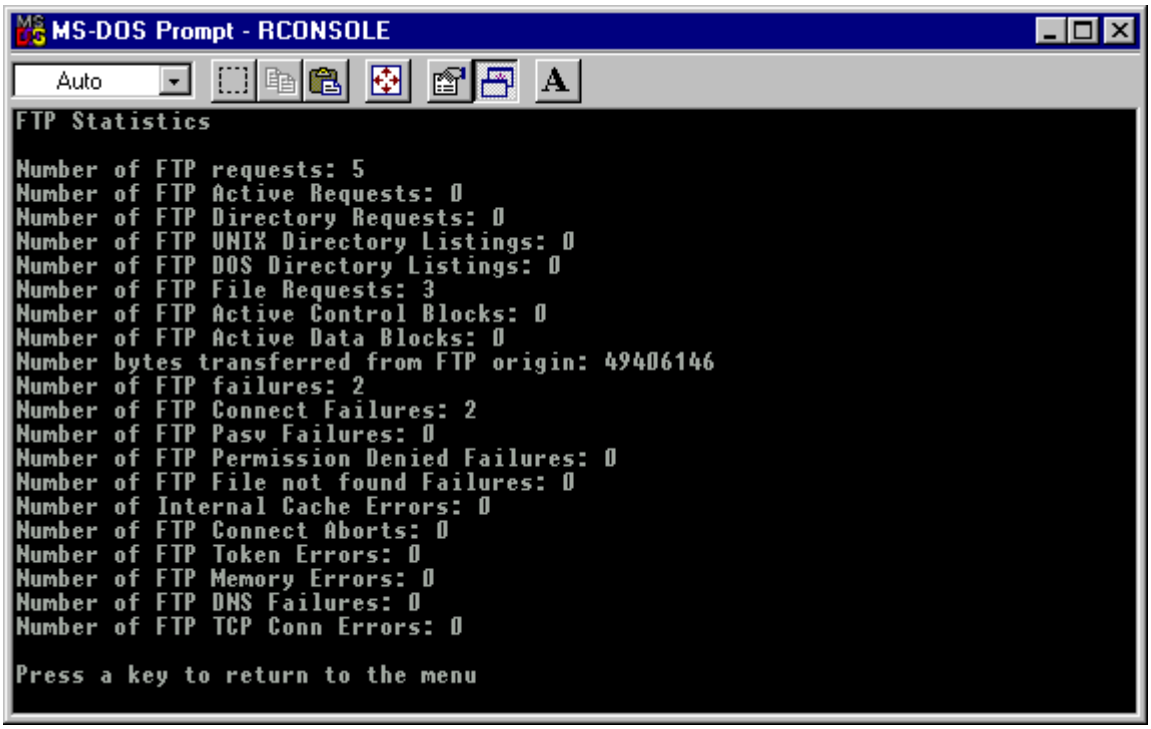
This Proxy Console option displays connection statistics for the HTTP Proxy.



Like all of the Proxy Console screens, the values here are particular to your server, and you should study (and record via screenshot) your statistics to form a baseline. Once you know what your server's typical values are, you will be in a position to use the data for troubleshooting purposes.

Option 10 – Display FTP Client Statistics

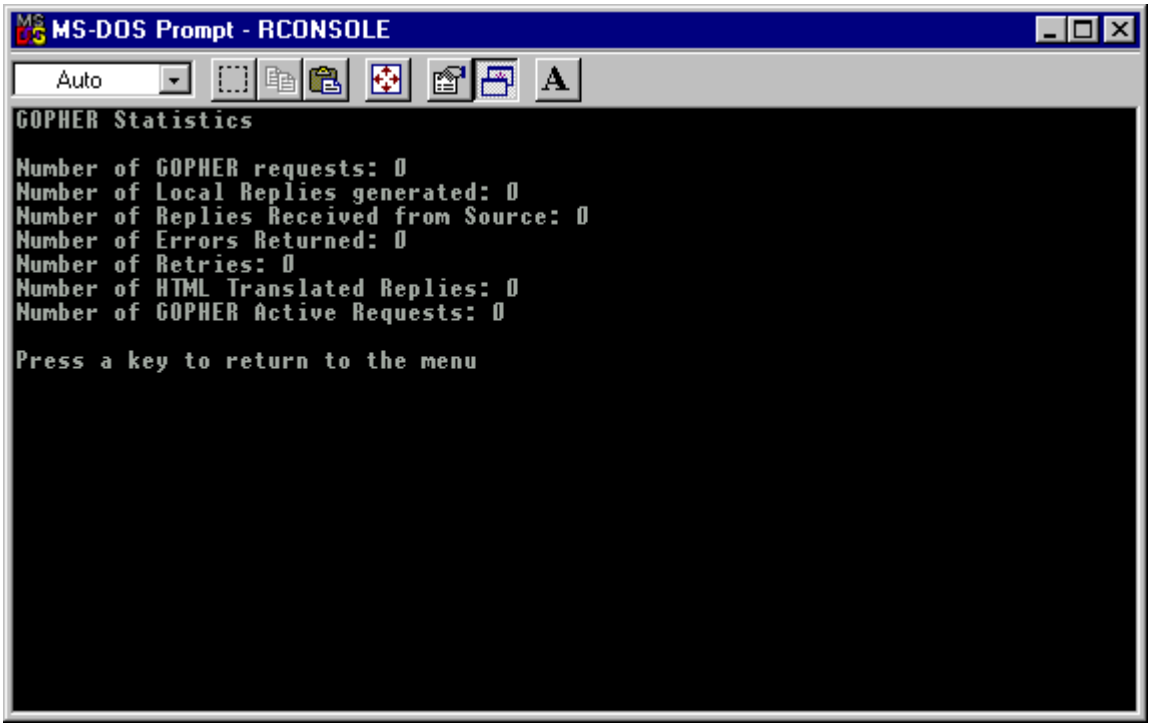
This Proxy Console option displays FTP Client statistics for the FTP & HTTP Proxy.



This screen shows traffic statistics for FTP data transfers.

Option 11 – Display GOPHER Statistics

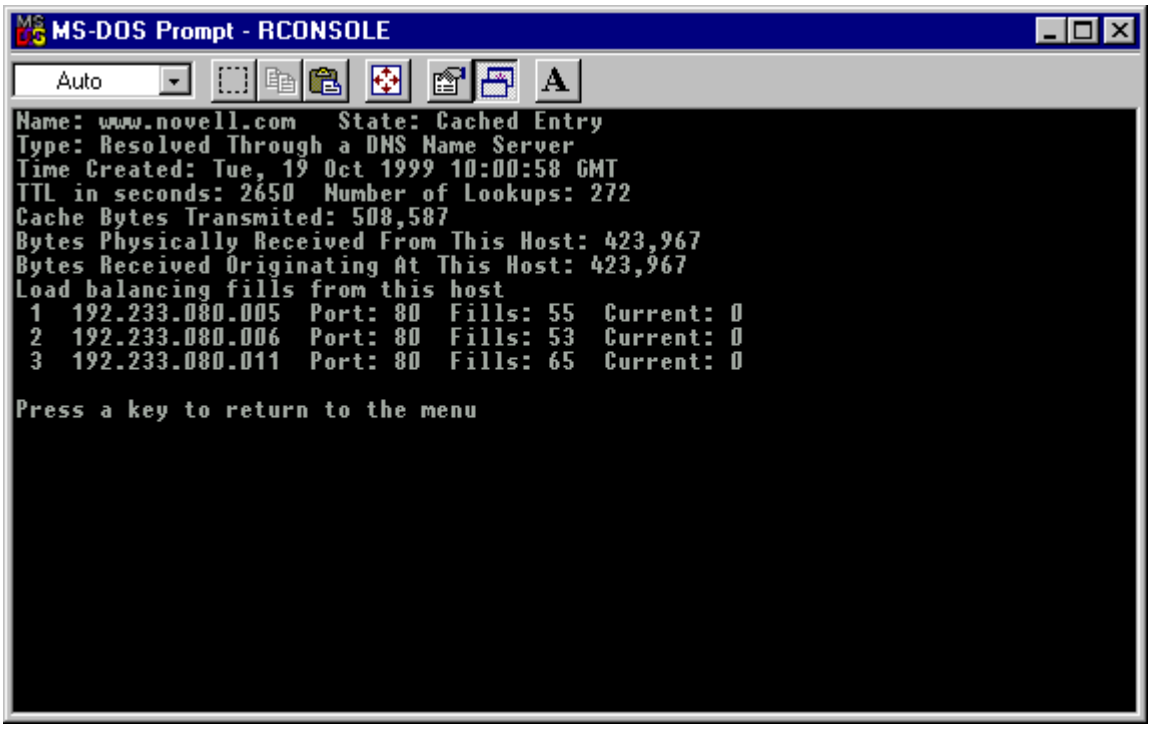
This Proxy Console option displays GOPHER statistics for the HTTP Proxy.



If you have had any type of GOPHER traffic coming through the HTTP proxy, you should see that reflected in this screen.

Option 12 – Display DNS Cache Entry Information

This Proxy Console option displays the cached DNS entries for a particular hostname. You must enter the hostname. This option is useful to determine if obsolete IP addresses are being used by the HTTP Proxy.



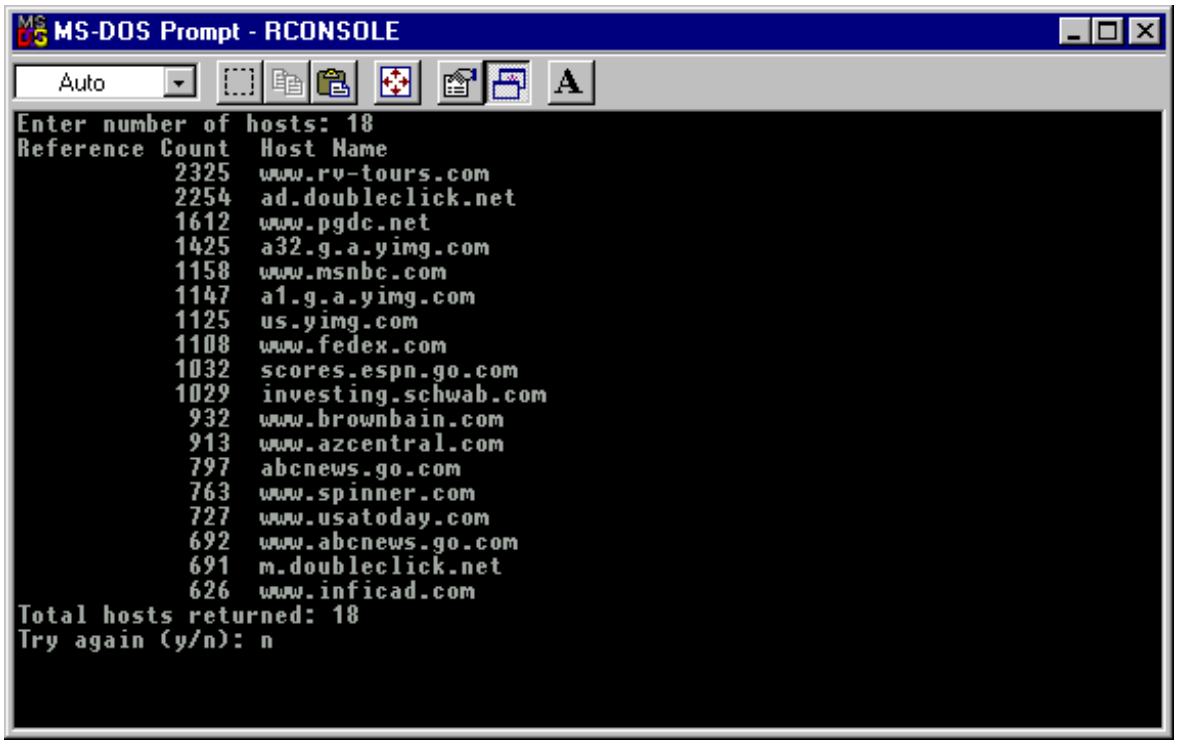
This is one of the more useful statistics screens for debugging purposes. You must type in a URL to check. In this case, www.novell.com was checked. You can see that the URL resolved to three different IP addresses, and the load was balanced pretty evenly across all of them. (Check some busy sites and see just how many servers they use to load-balance! Look at www.cnn.com, www.netscape.com, etc.)

The single most useful aspect of this screen is finding out what IP addresses are being cached for a site. You may find that an incorrect DNS entry is in cache, preventing users from connecting to a particular web site. (In that case, you need to unload PROXY, and delete the SYS:\ETC\PROXY\PXYHOSTS file).

Note the second line from the top of the screen. In this example, you can see that the URL was resolved from a name server. You might also see if the value was resolved from the server's HOSTS file.

Option 13 – Show hosts sorted by most DNS lookup requests

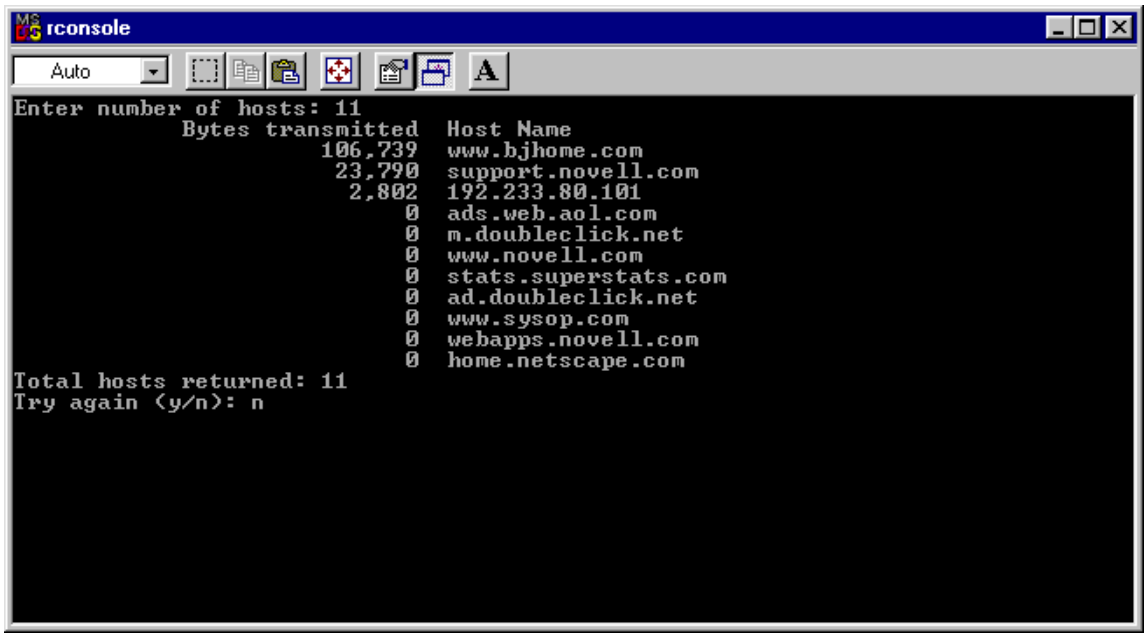
This Proxy Console option displays a sorted list of the sites that have been the target of the most DNS queries. This is one measure of the most active hosts.



Type in the number of hosts for which you want to see data. The results will be sorted by the most accesses, not by the largest amount of data transferred.

Option 14 – Show Origin Hosts Sorted by Amount of Data Transmitted by the Cache

Selecting Proxy Console option 14 will show which hosts have had the most data sent from the cache to a workstation on the LAN. You must enter the number of hosts for which you want data displayed.

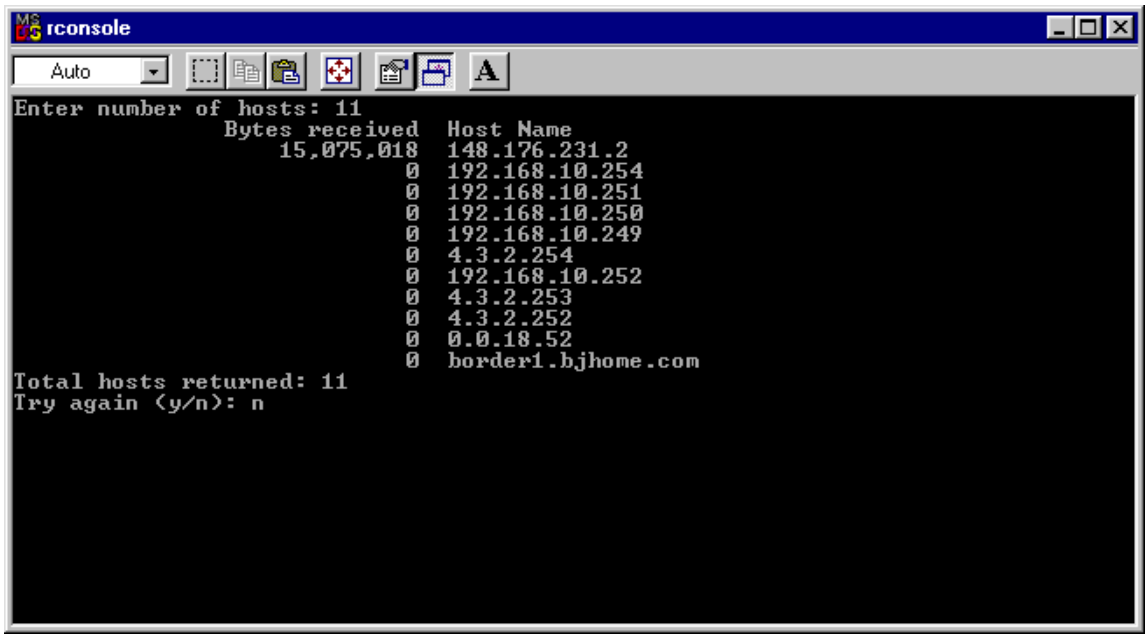


This screenshot shows that the site that sent all the data into the cache in screen #15 isn't even among the top 18 entries for data transmitted out of the cache.

The example shown is rather odd in terms of showing no data for all the sites. This is because the screenshot was taken from a server set up to pull all of the data from a CERN proxy. Without using a CERN caching hierarchy, you should see a number of sites sorted in decreasing order by the amount of data transmitted from the cache to the browser.

Option 15 – Show Origin Hosts Sorted by the Amount of Data sent TO the Cache

Selecting Proxy Console option 15 will show which hosts have had the most data sent into the cache. You must enter the number of hosts for which you want data displayed.



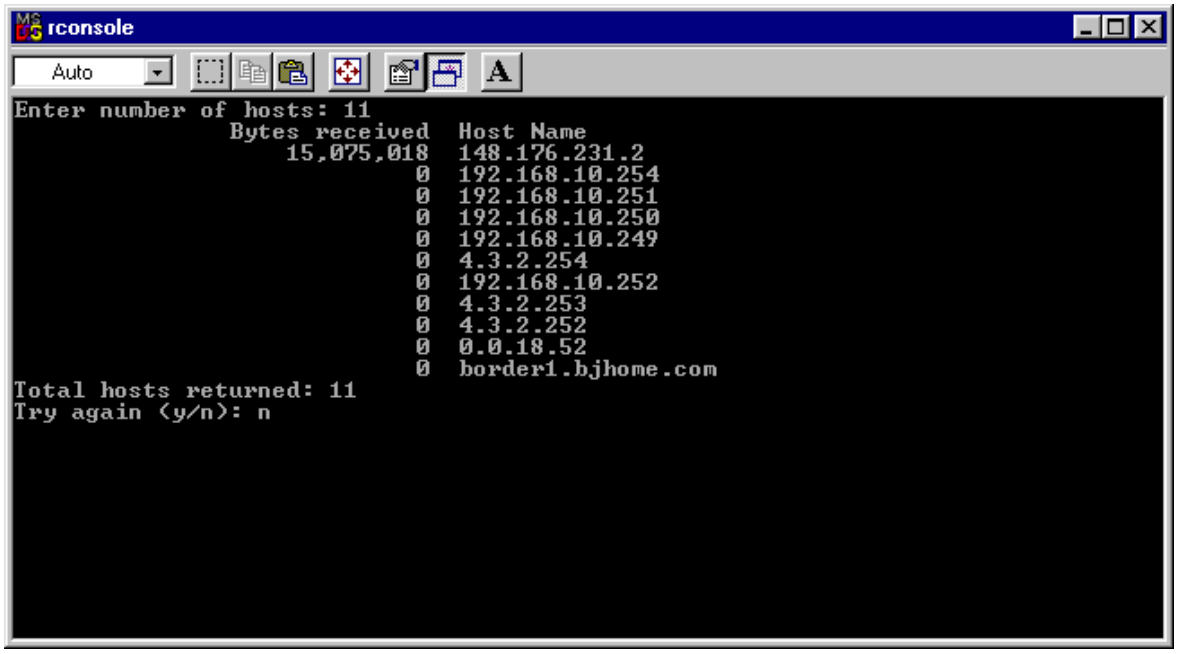
This screenshot shows one host with a very large amount of data sent into the cache. This screenshot was taken at the same time as the previous example for option #14.

The data returned here is somewhat odd-looking because the server was set up to pull all data from an upstream CERN proxy, and for the statistics only show very current data. A few minutes after taking this screenshot, all the sites returned a value of zero.

The statistic above was generated by browsing to a web site with a constantly updating web camera graphic. (In fact, the site has several cameras trained on Loch Ness, updating images every 30 seconds, so that you might be able to spot the Loch Ness monster. Be advised that checking the site in the United States during the afternoon or evening will show you a black image, because it is dark at Loch Ness at that time of the day…)

Option 16 – Show Proxies and Origin Hosts Sorted By Most Data Directly Received

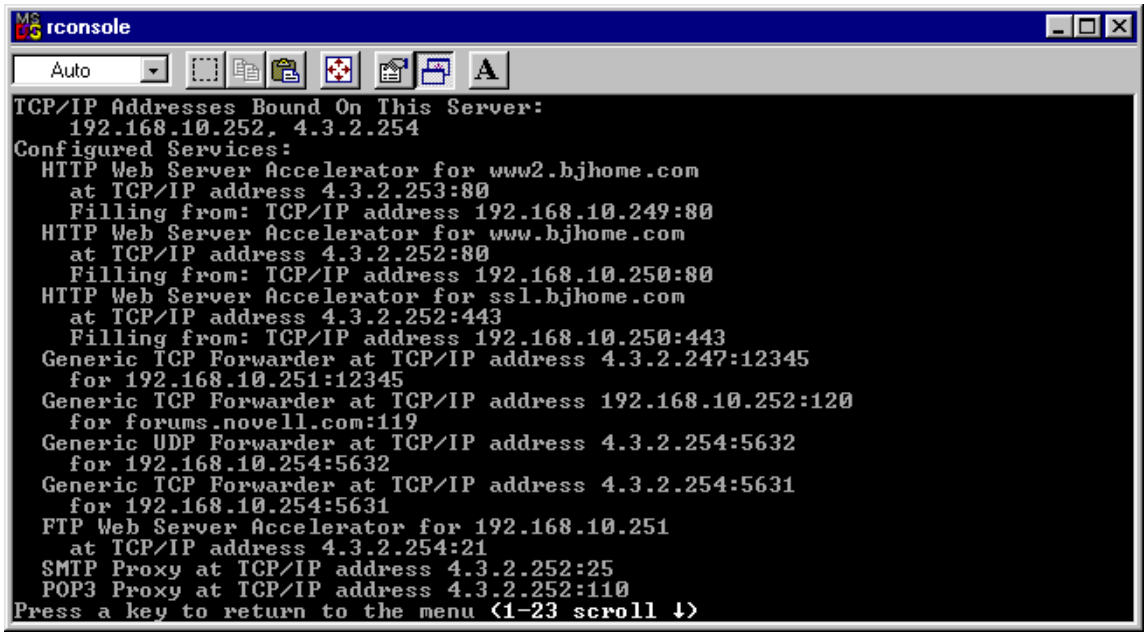
This Proxy Console option displays statistics for the amount of bytes received from both origin hosts and proxies (which would include data received from a hierarchical caching proxy server). If ICP is not configured on the BorderManager server, these statistics should be the same as the statistics for data received from origin servers. You must enter the number of hosts to display.



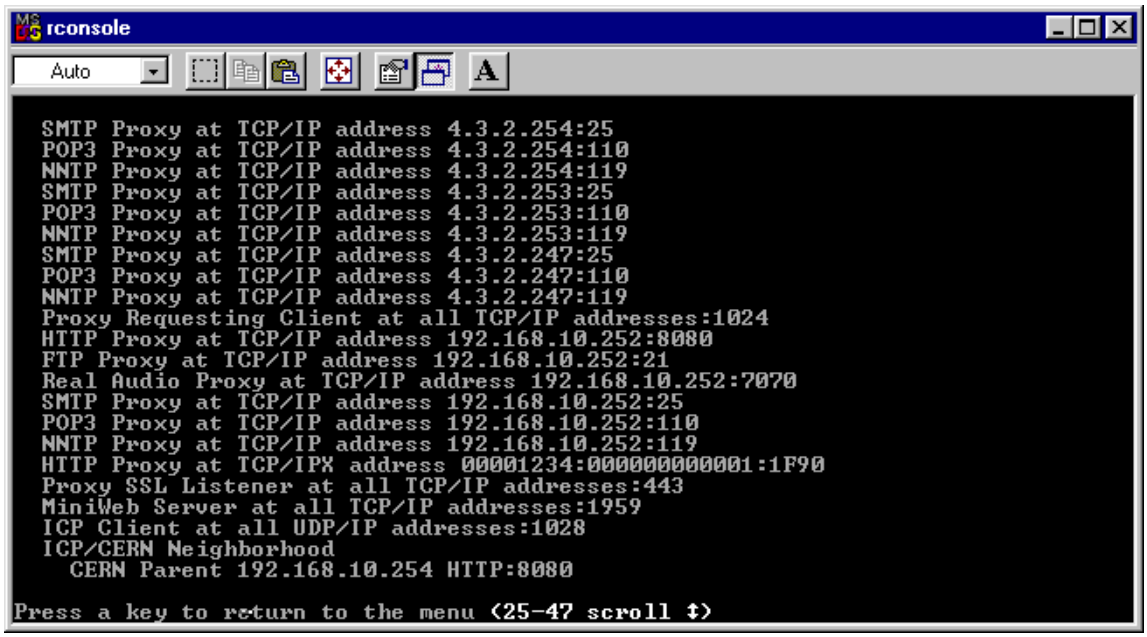
Similar to the previous screen, this example is showing rather odd statistics as a result of the BorderManager server being in a CERN cache hierarchy.

Option 17 – Display Configured Addresses and Services

This Proxy Console option displays all the proxy services and IP addresses configured on the BorderManager server.



Part 1 of 2



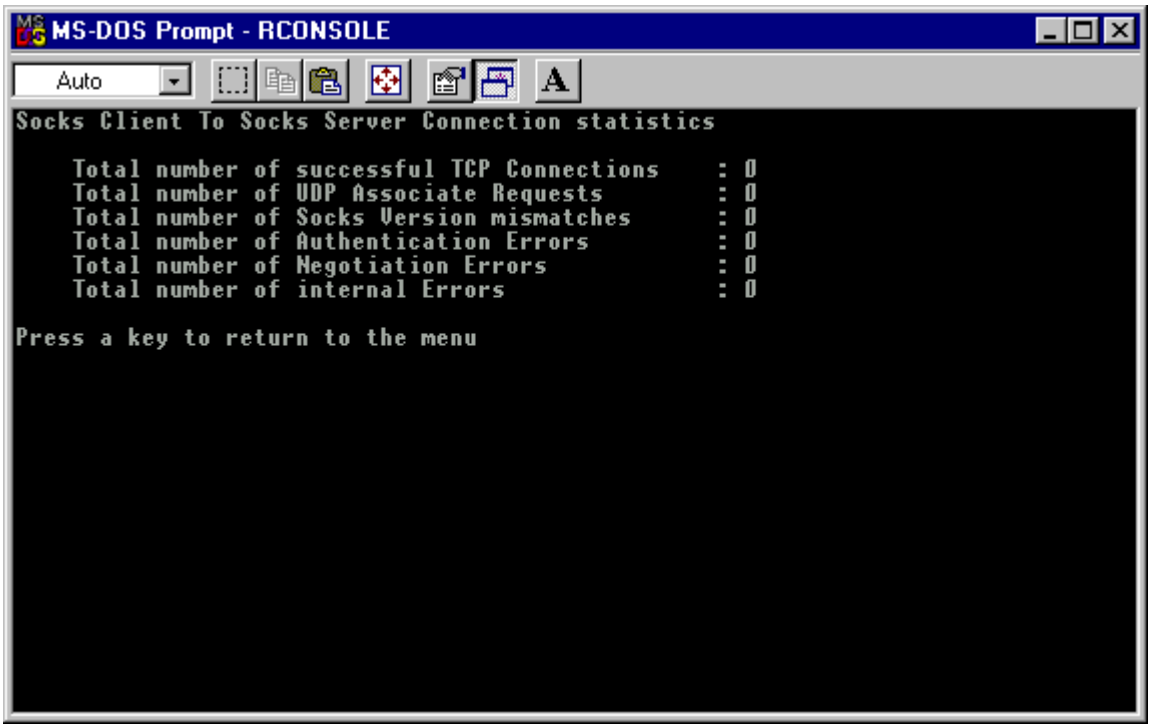
Part 2 of 2

This is one of the most useful Proxy console screens. It shows you all of the configured proxy services. You can see the IP addresses assigned to particular listening port numbers.

You will notice from this screen, that certain proxies will listen on all IP addresses that are defined in NWADMN32 as public. The Mail Proxy is one of them. You cannot tell the Mail Proxy to not listen on a defined secondary IP address, which can be unfortunate. (You can, however, simply not put in packet filter exceptions so that no traffic can get to that secondary IP address).

Option 18 – Display SOCKS Client Statistics

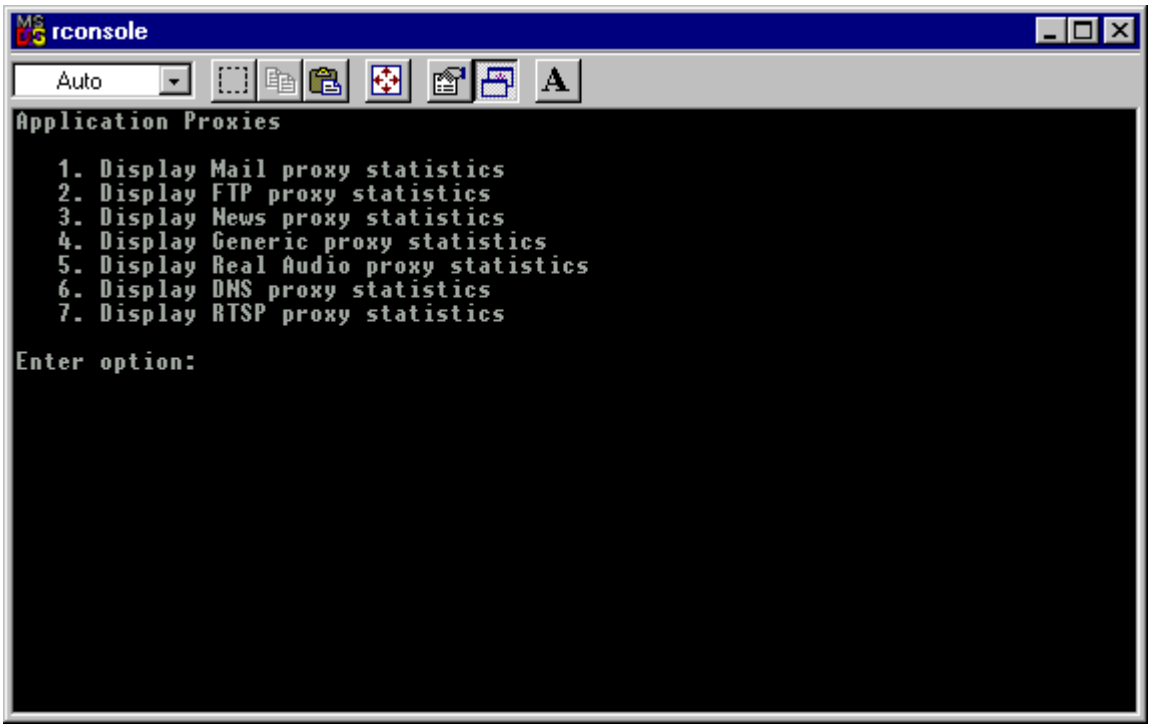
This Proxy Console option displays SOCKS Client statistics for the BorderManager server.



This console screen shows statistics for the SOCKS client, not the SOCKS gateway. The SOCKS client is used when you need to have the BorderManager HTTP Proxy access the Internet through a SOCKS server.

Option 19 – Application Proxies

This Proxy Console option displays a menu of the non-HTTP application proxies.

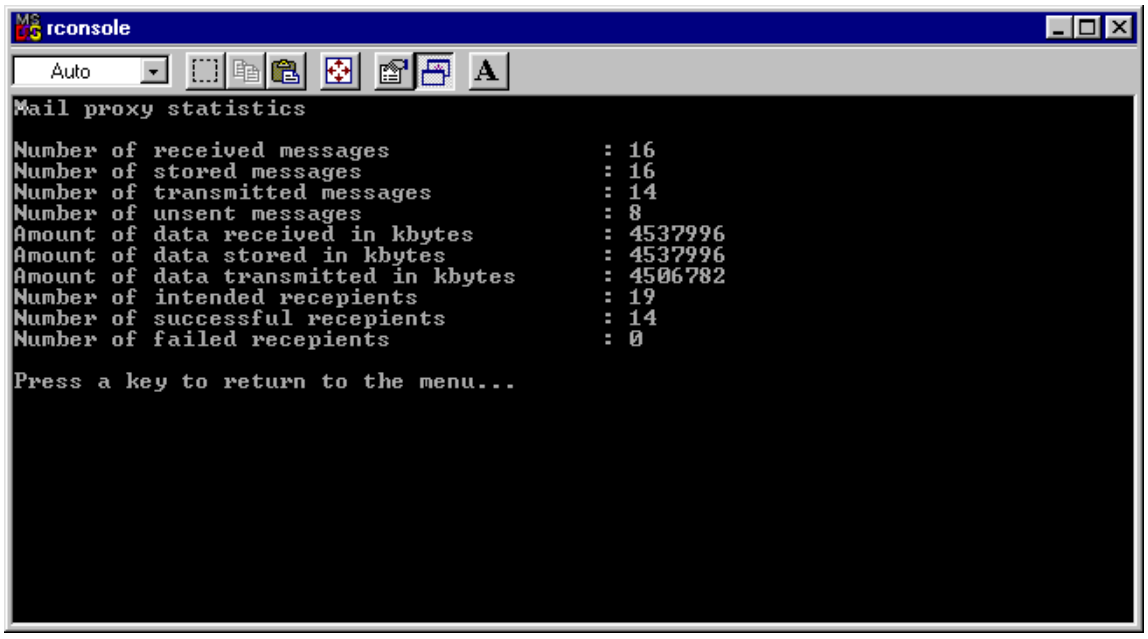


The example above shows a BorderManager 3.5 or later console screen. BorderManager 3.0 will not have option 7, Display RTSP proxy statistics.

Select one of the menu entries to get additional information on the desired proxy application.

The application proxy statistics screens are very useful for tracking usage through the particular proxy, but even more so for troubleshooting purposes. If you should see the number of ACL Denials rise while testing a proxy, you can be assured that the traffic is being seen by the application proxy, but is being denied by an access rule. Frequently, the reason the traffic is denied is because an Allow rule was not correctly configured, or because no Allow rule at all was created for that proxy.

Mail Proxy Statistics



The example above shows the results of a quick test of the Mail Proxy.

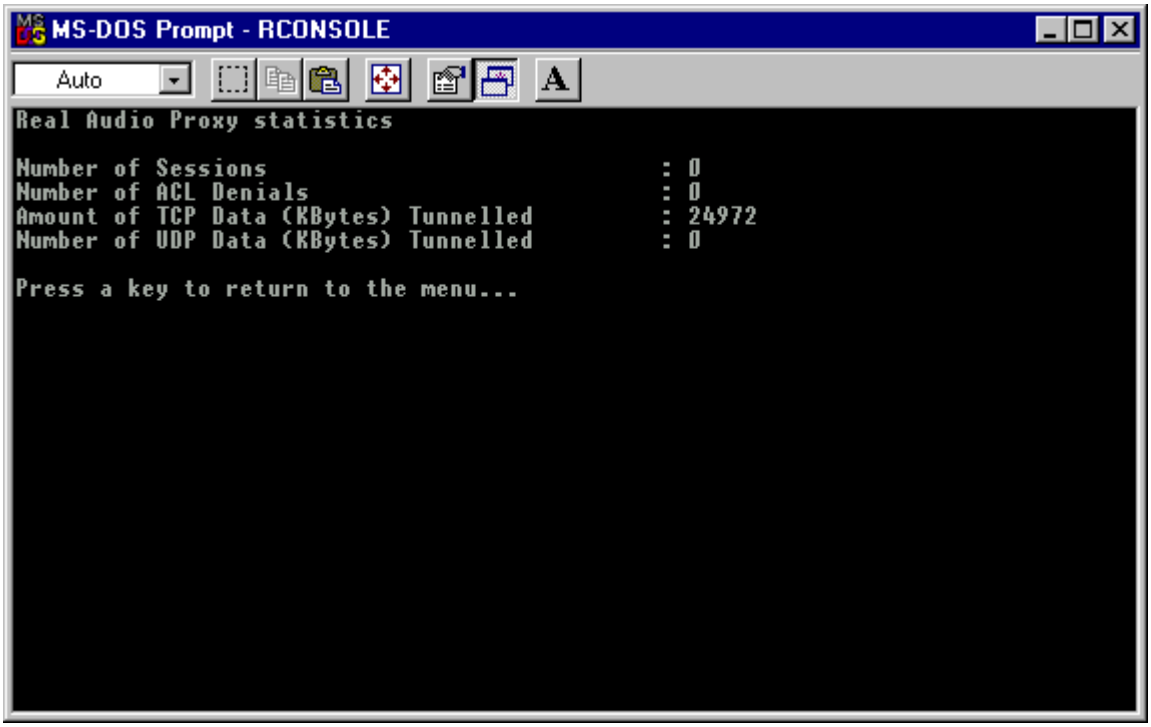
The number of unsent messages, and the difference between intended and successful recipients has to do with a number of messages that were rejected as a result of rules set up to deny spam relay. Messages being relayed through the Mail Proxy actually were accepted into the Incoming spool directory, but not relayed back out again. Eventually the messages were returned to the sender with the text added:

"Undelivered mail: Access Denied for craig@sysop.com"

The test involved trying to relay mail from a test mail domain called sysop.com.

Real Audio Proxy Statistics

This application proxy screen shows the traffic statistics for the Real Audio proxy.



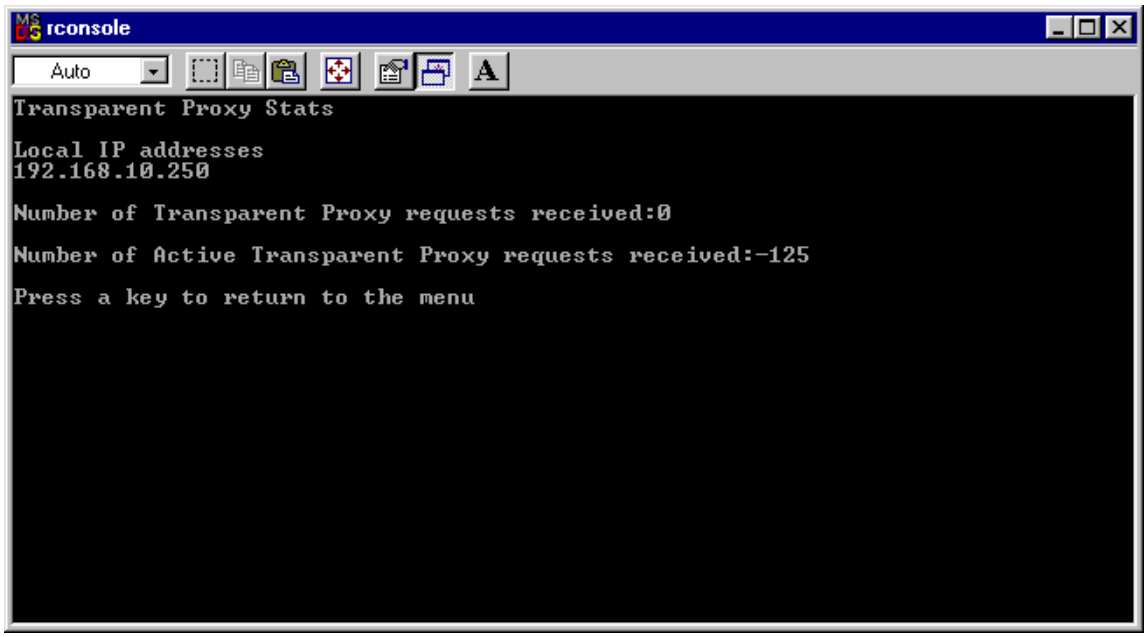
The example shown shows that some data was actually being tunneled by the Real Audio proxy. (Some people find that proxy hard to configure, so it can seem like a big deal when you see some traffic coming through it!)

Note the Number of ACL Denials. If you are lacking an appropriate access rule, this value will increase each time you attempt to use the Real Audio proxy and an access rule (or lack of one) denies the traffic.

Option 20 – Transparent Proxy Statistics

This Proxy Console option displays statistics for the Transparent Proxy.

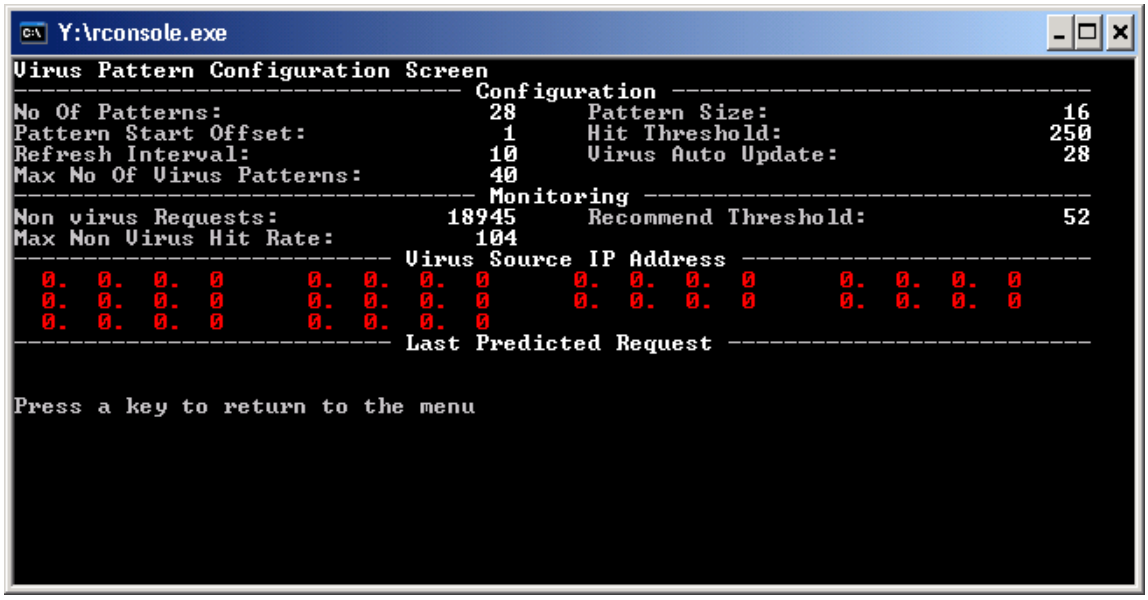
Note This option has always had a bug in that incorrect statistics were shown for Transparent Proxy, including negative values for some parameters.



This statistics screen has historically been inaccurate. The example above was taken from a BorderManager 3.0 server with patches up through BM3SP2 and BM3PC17.

I have never seen a BorderManager server with credible Transparent Proxy statistics.

Option 23 – Virus Pattern Configuration Screen



This option only shows up with later BorderManager proxy patches (starting at version 3.61d for BorderManager 3.6, from the BM36C01.EXE patch).

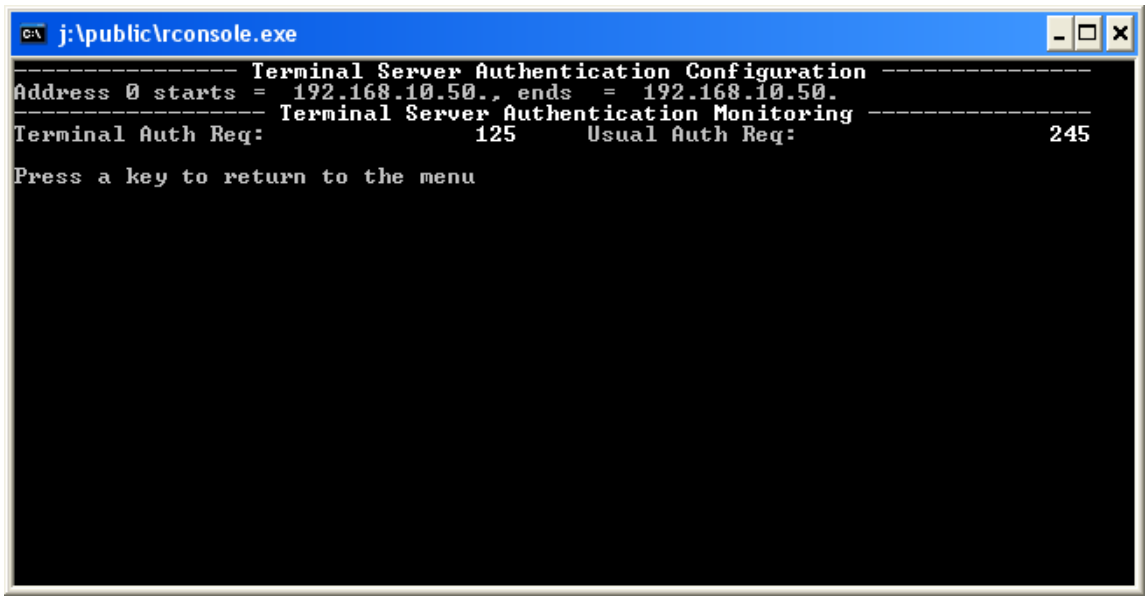
This option shows the number of virus patterns configured in the PROXY.CFG file – 28 in the example shown – and virus activity matching those patterns.

The antivirus pattern matching is used in conjunction with Reverse Proxy Acceleration. If you have an internal web server made available to the internet through HTTP Acceleration, the antivirus pattern matching could be protecting your web server from malicious code. If matching HTML code is sent through the reverse proxy to your web server, BorderManager will drop that data, and record the information on this screen.

Novell has an AppNote (February, 2002) covering antivirus pattern matching in BorderManager at the following URL:

http://developer.novell.com/research/appnotes/2002/february/02/a0202023.htm

Option 24 – Terminal Server Authentication Configuration



Option 24 appears as a Proxy Console menu option only if you have installed the PROXY.NLM version that support Terminal Server authentication. Essentially, this means BorderManager 3.7 or later, or BorderManager 3.5 and 3.6 servers that have had the latest BorderManager 3.7 PROXY.NLM copied to them.

Option 24 will either show that terminal server authentication is disabled, or it will show details on how the authentication is configured, and how many authentication attempts have been seen by the proxy.

Terminal Server authentication and the IP addressing to which authentication applies, is configured in the SYS:ETC\PROXY.CFG file.

In the example shown above, terminal server authentication has been configured only for a single IP address: 192.168.10.50.

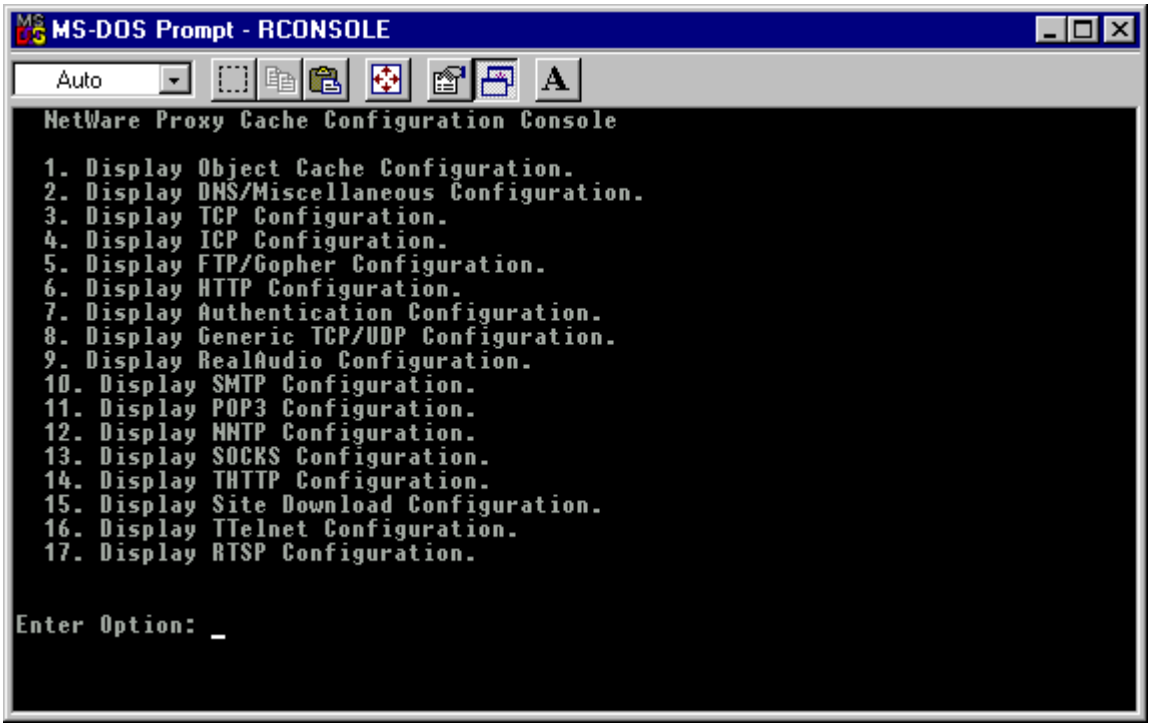
Since PROXY.NLM was loaded on the server, 125 authentication requests were seen by the terminal server method, and 245 requests were seen by the usual methods (CLNTRUST or SSL Proxy Authentication).

<This page intentionally left blank. This is to facilitate putting in chapter tabs in a ring binder for double-sided printing. The main chapters should start on an odd-numbered page.>

Chapter 30 - Proxy Cache Configuration Console

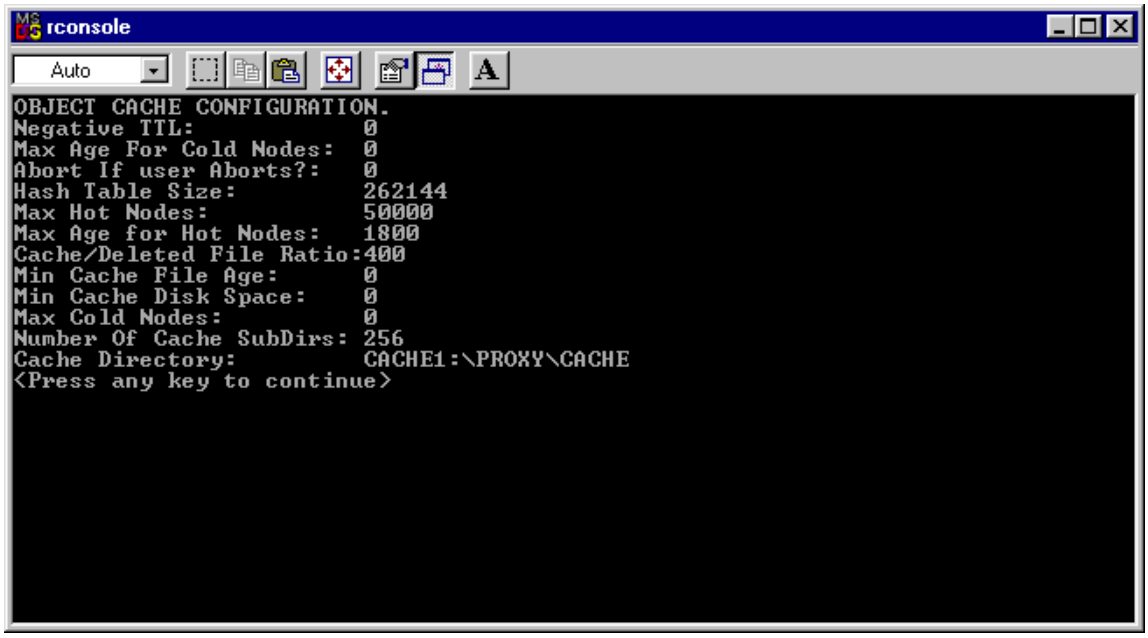
Note Download the file BM3PCFG.EXE file from http://support.novell.com to see Novell's explanation of many of the proxycfg screens. The explanations are quite good.

The Proxy Cache Configuration console screen shows configuration data



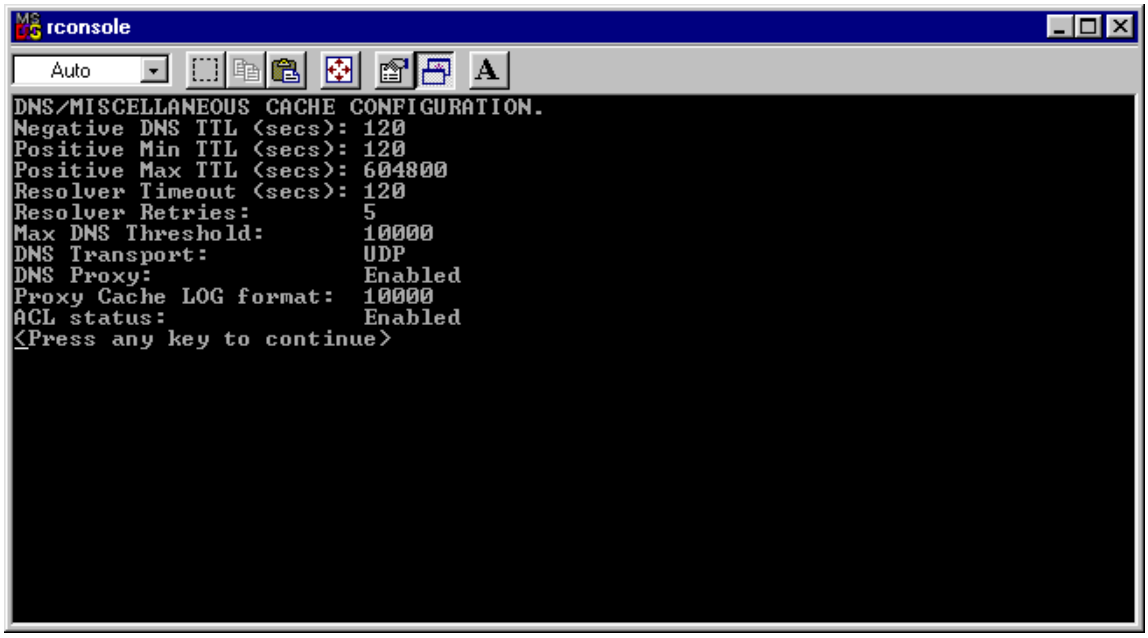
Option 1 – Display Object Cache Configuration

This Proxycfg menu option displays (some of) the HTTP Proxy cache configuration information. Note that only the first configured cache volume is shown on this screen, even if more than one cache volume was configured.



Option 2 – Display DNS/Miscellaneous Configuration

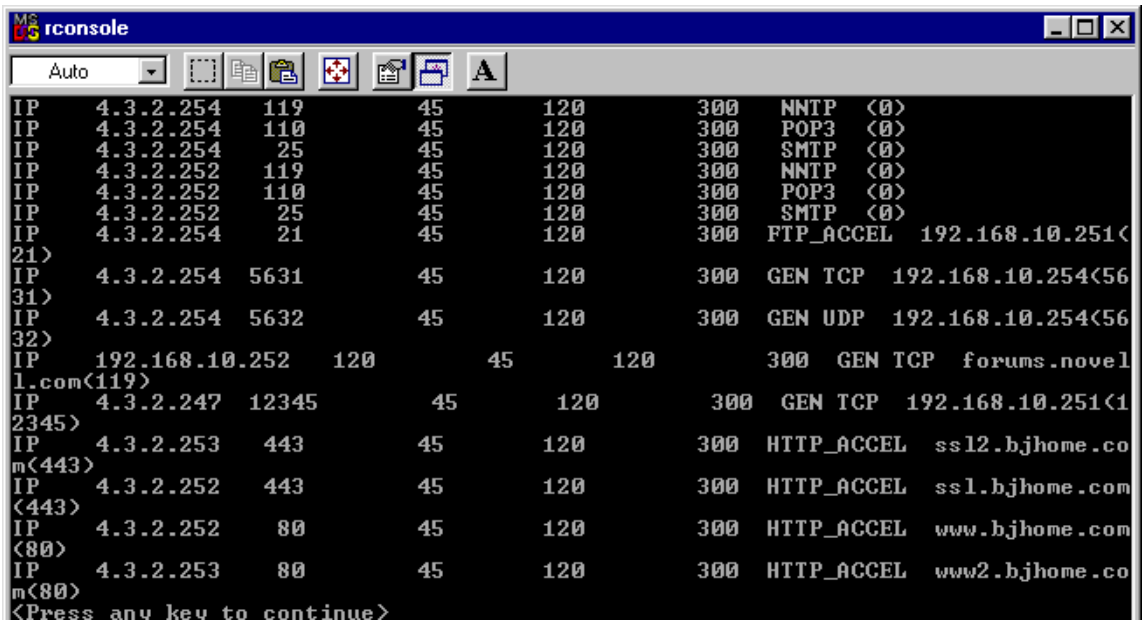
This Proxycfg menu option displays DNS and transport configuration information.



Note that the DNS proxy is disabled in this example. However, the HTTP Proxy will still make use of DNS caching.

Option 3 – Display TCP Configuration

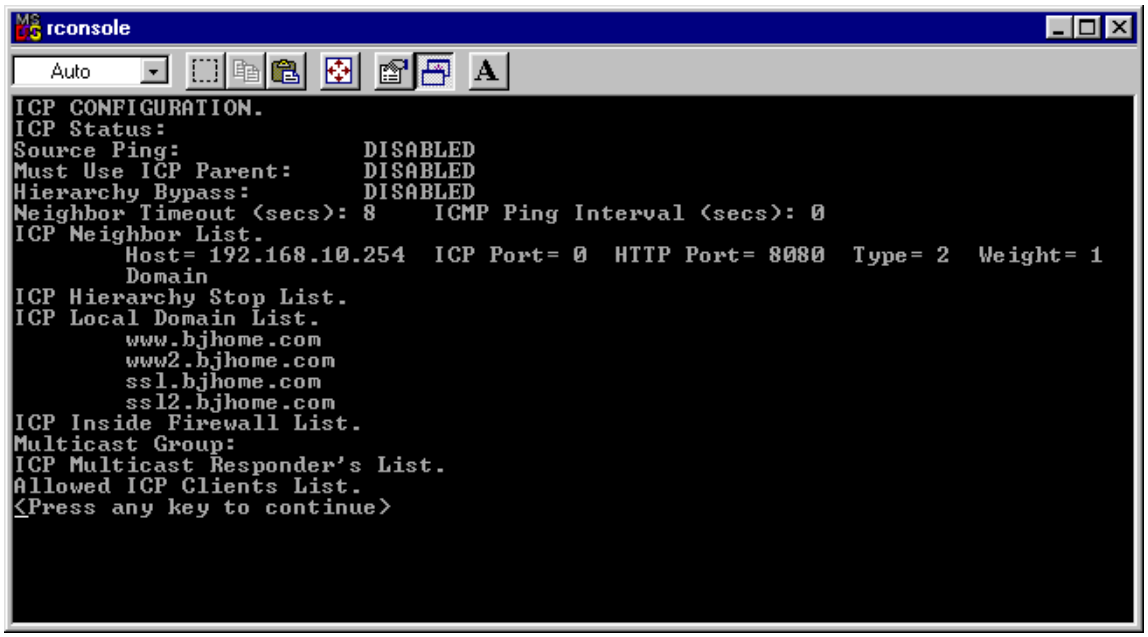
This Proxycfg menu option displays both IP and IPX configured addresses and listening ports.



This example shows the TCP ports being listened on by various proxies.

Option 4 – Display ICP Configuration

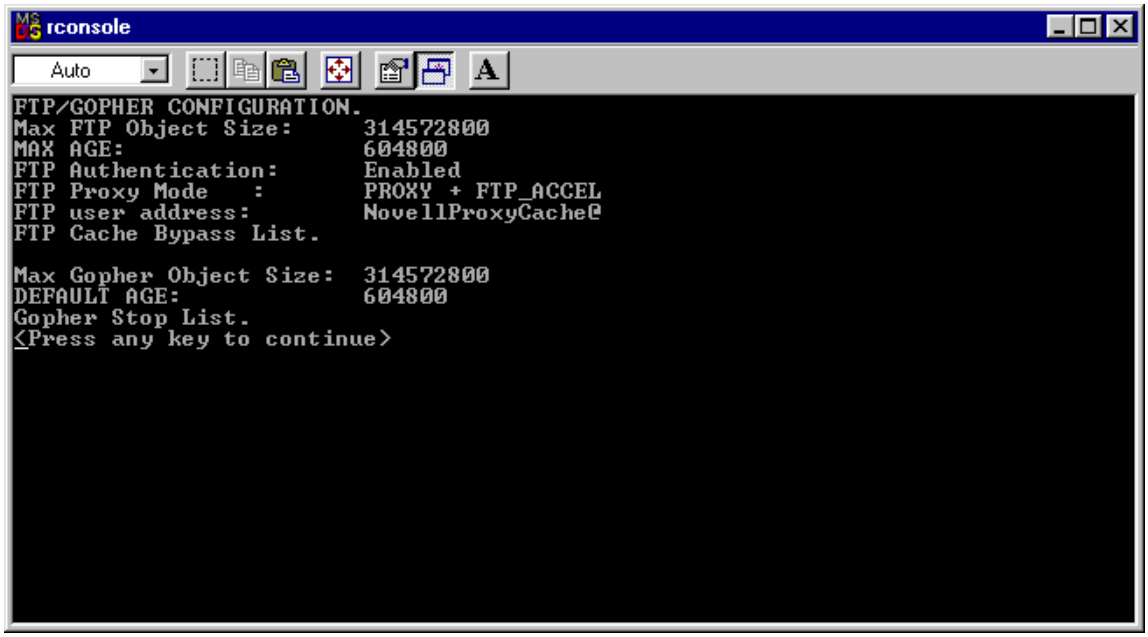
This Proxycfg menu option displays ICP configuration information for a hierarchical caching system.



Although the console screen shows ICP configuration details, most apply also to a CERN hierarchy.

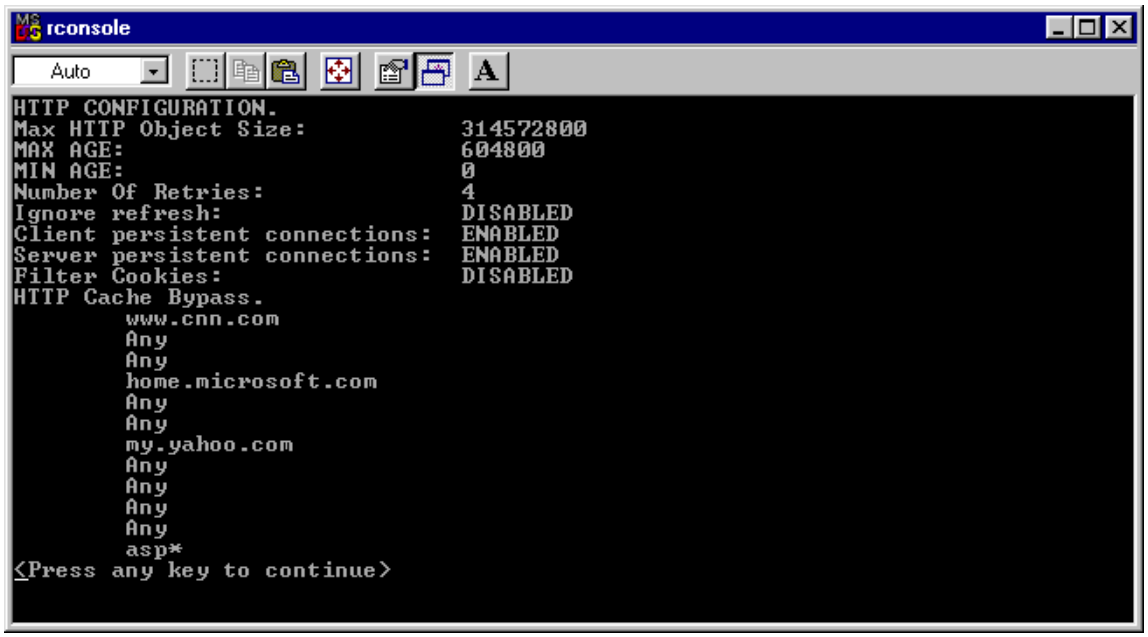
Option 5 – Display FTP/GOPHER Configuration

This Proxycfg menu option displays FTP/GOPHER configuration information.



Option 6 – Display HTTP Configuration

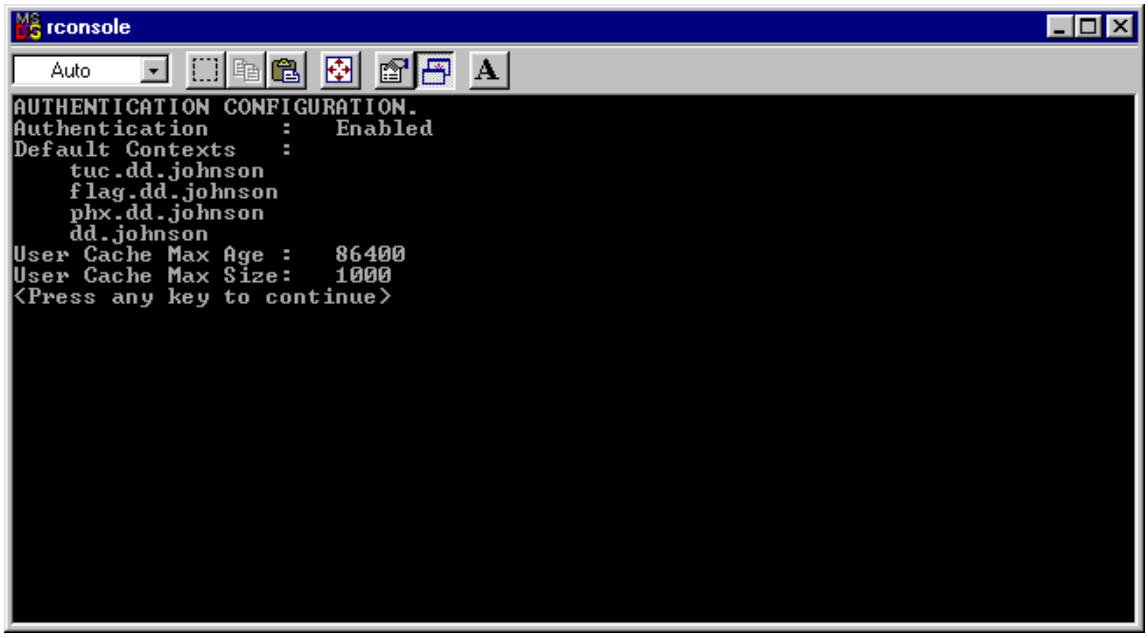
This Proxycfg menu option displays HTTP Proxy configuration information.



This screen will show the currently configured cacheable object control cache bypass entries.

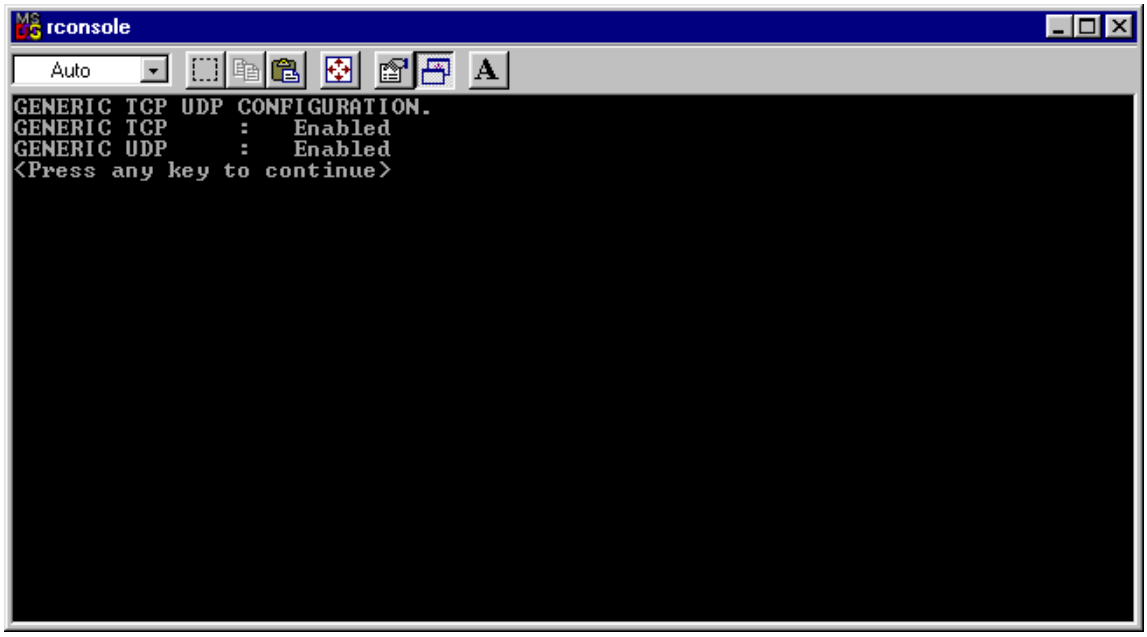
Option 7 – Display Authentication Configuration

This Proxycfg menu option displays proxy authentication configuration information.



Option 8 – Display Generic TCP/UDP Configuration

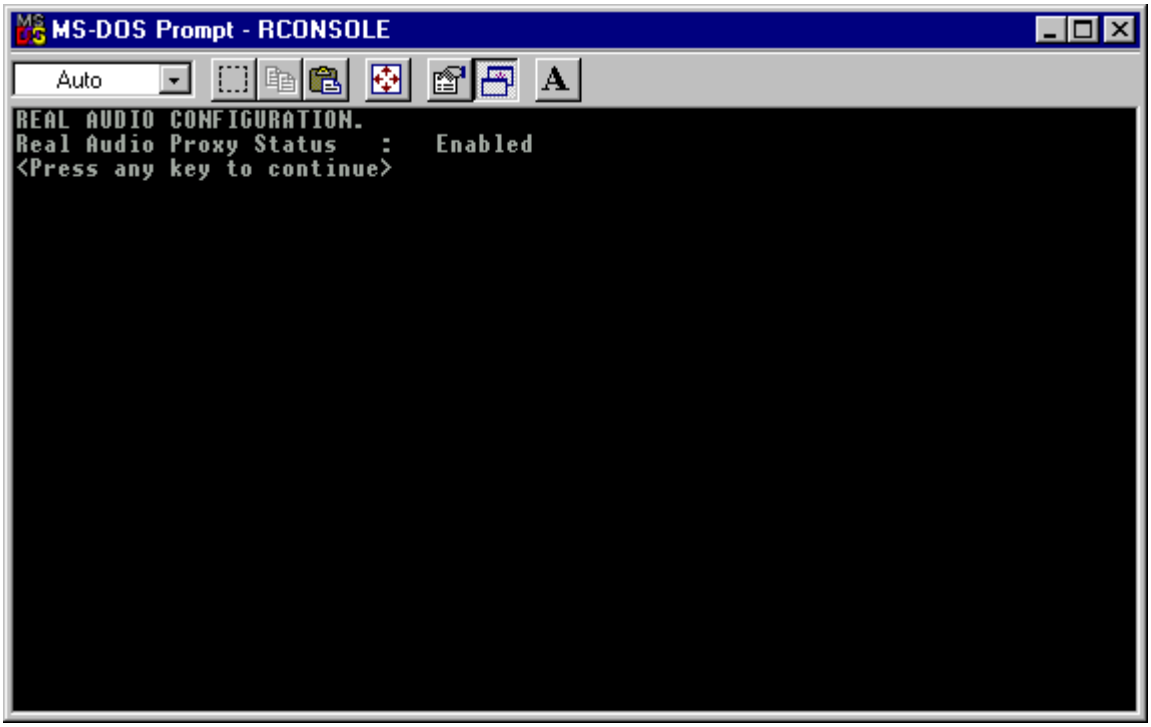
This Proxycfg menu option displays Generic TCP and UDP proxy configuration information.



This console screen will only show if you have configured a TCP or UDP Generic Proxy.

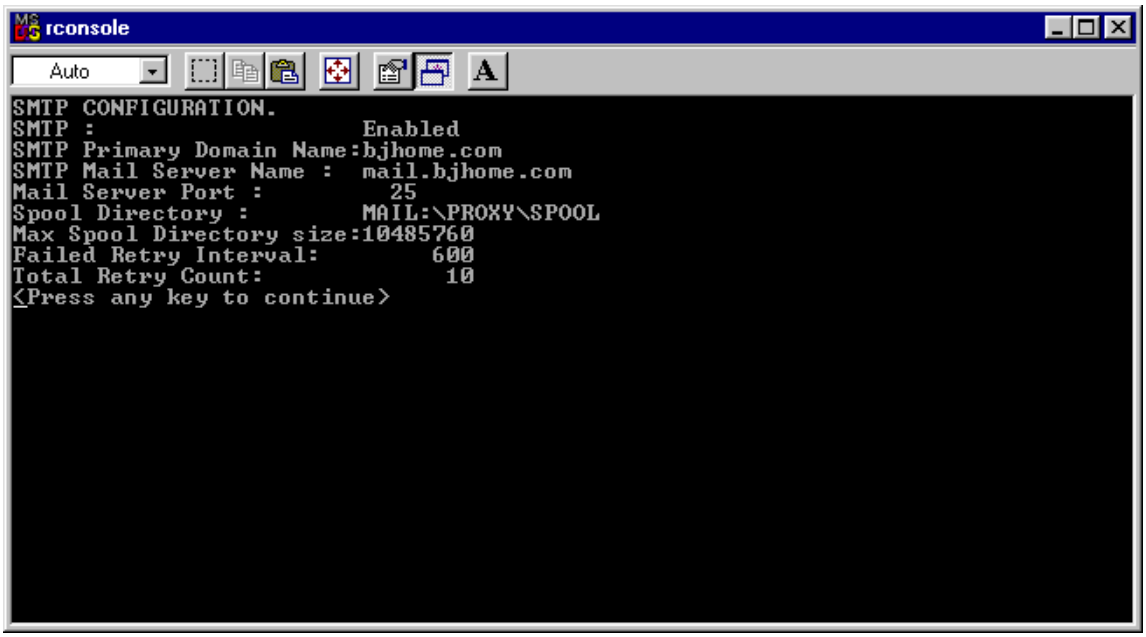
Option 9 – Display RealAudio Configuration

This Proxycfg menu option displays RealAudio configuration information.



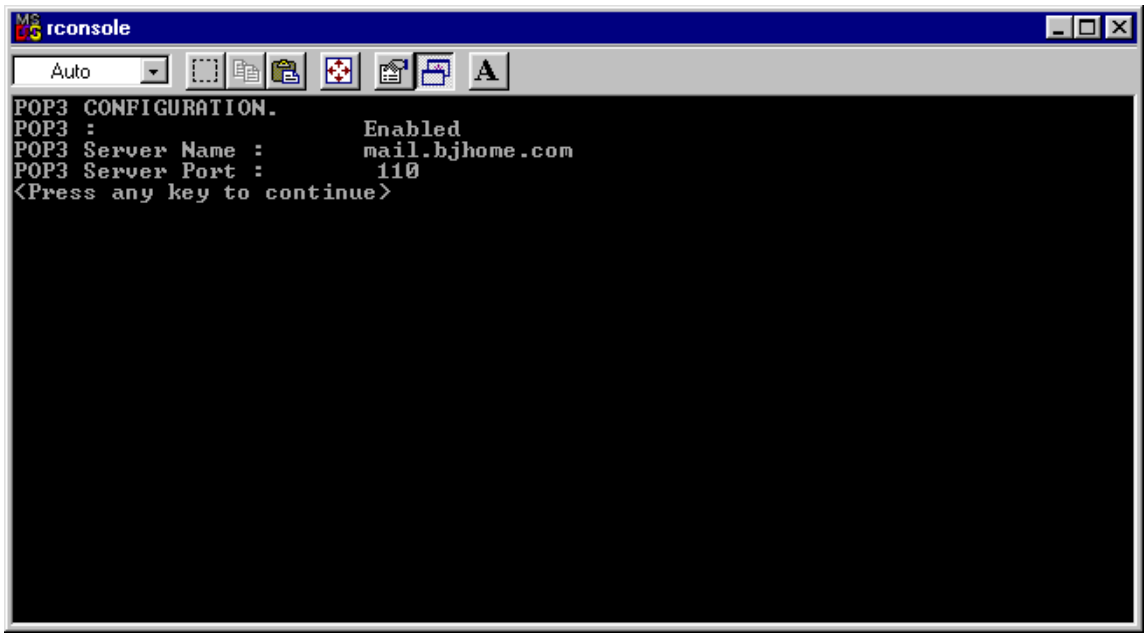
Option 10 – Display SMTP Configuration

This Proxycfg menu option displays Mail proxy configuration information.



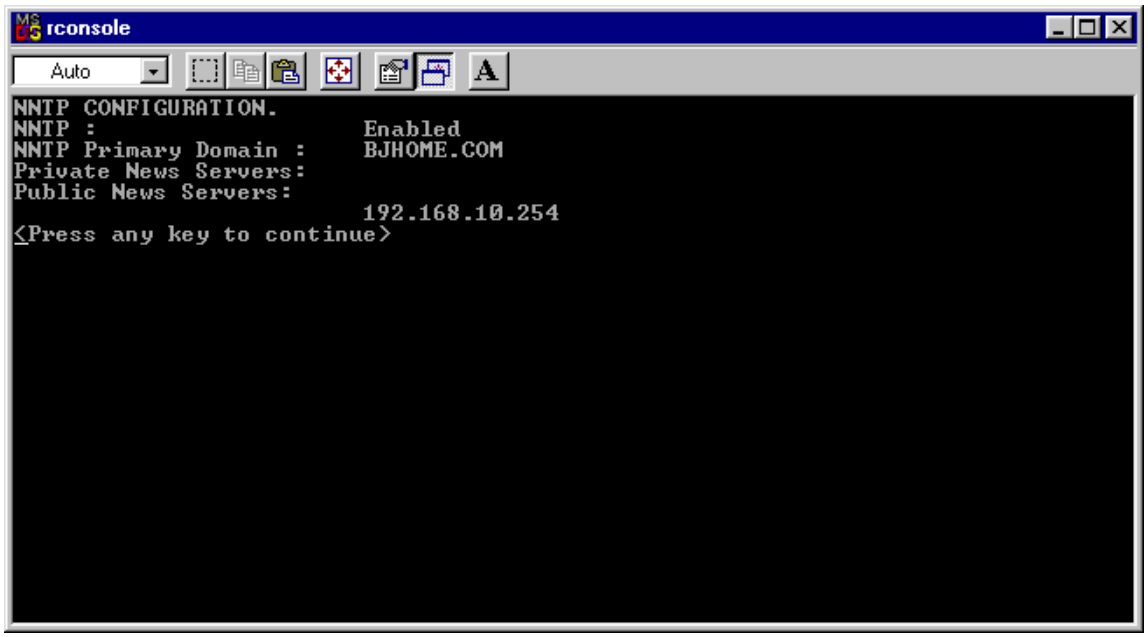
Option 11 – Display POP3 Configuration

This Proxycfg menu option displays POP3 (Mail) proxy configuration information.



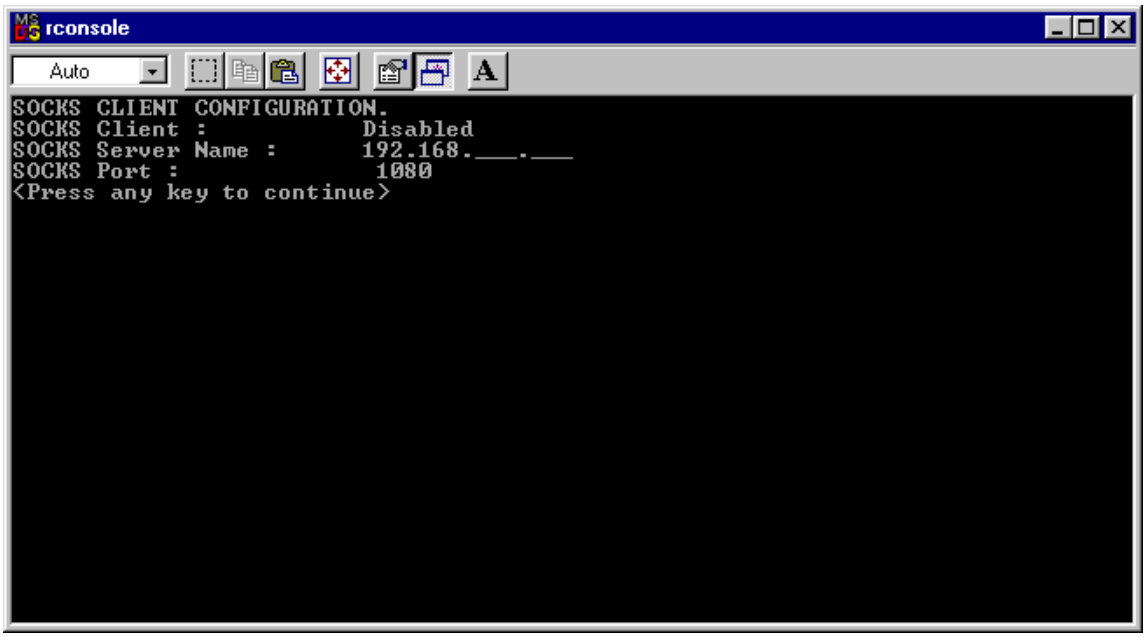
Option 12 – Display NNTP Configuration

This Proxycfg menu option displays NNTP proxy configuration information.



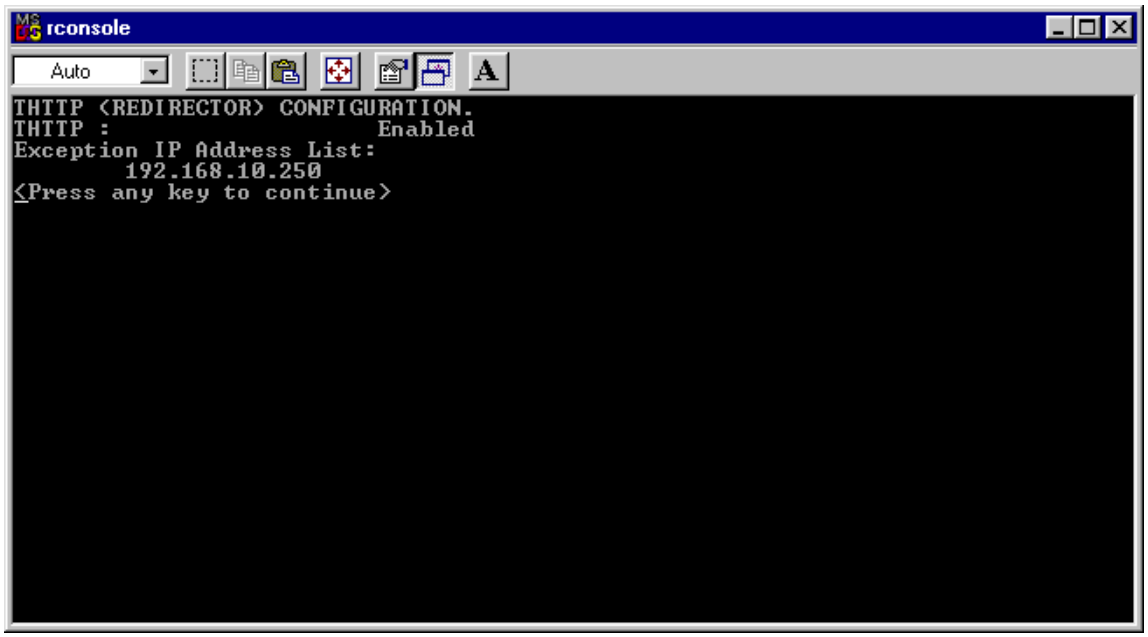
Option 13 – Display SOCKS Configuration

This Proxycfg menu option displays SOCKS Client (not SOCKS Gateway) configuration information.



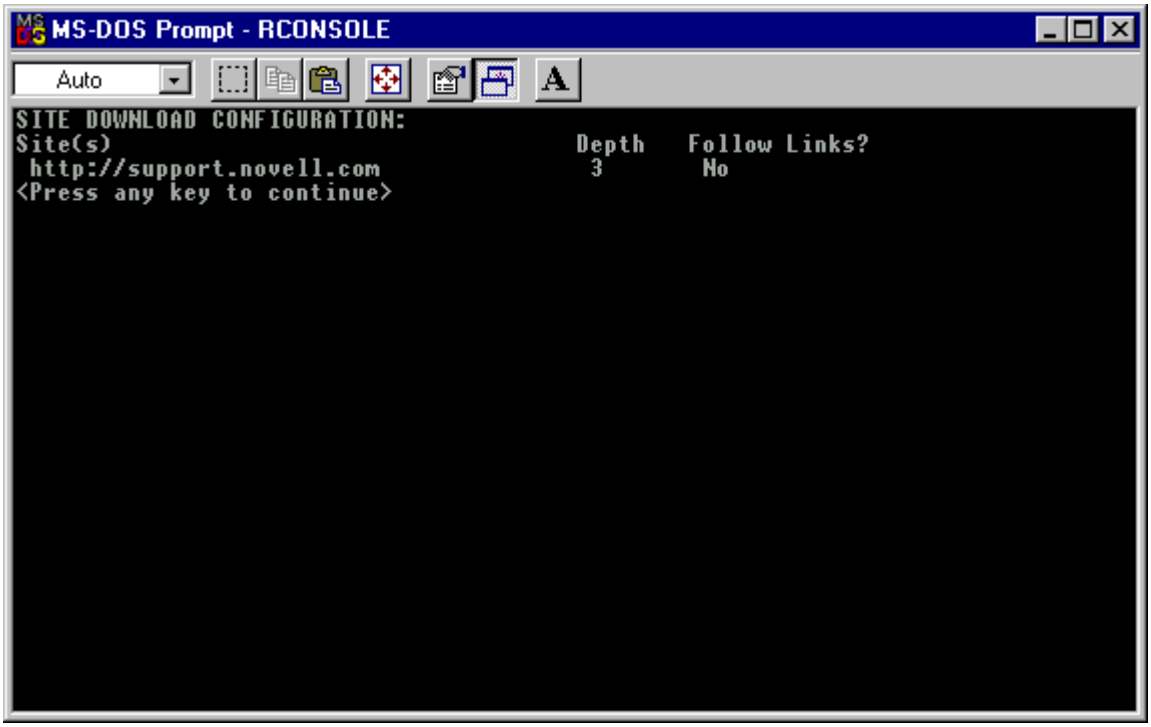
Option 14 – Display THTTP Configuration

This Proxycfg menu option displays THTTP (Transparent) proxy configuration information.



Option 15 – Display Site Download Configuration

This Proxycfg menu option displays site download configuration information.

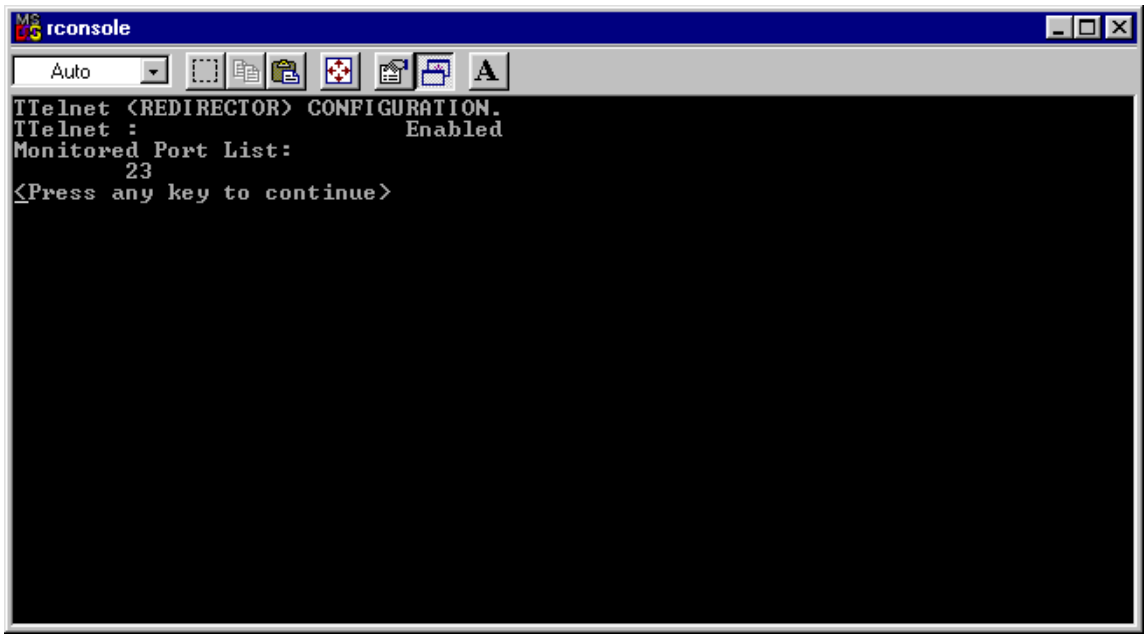


All of the sites you have configured for scheduled download will show up on this console screen.

Option 16 – Display TTELNET Configuration

Note This console screen is seen only on BorderManager 3.5, 3.6 or 3.7 servers.

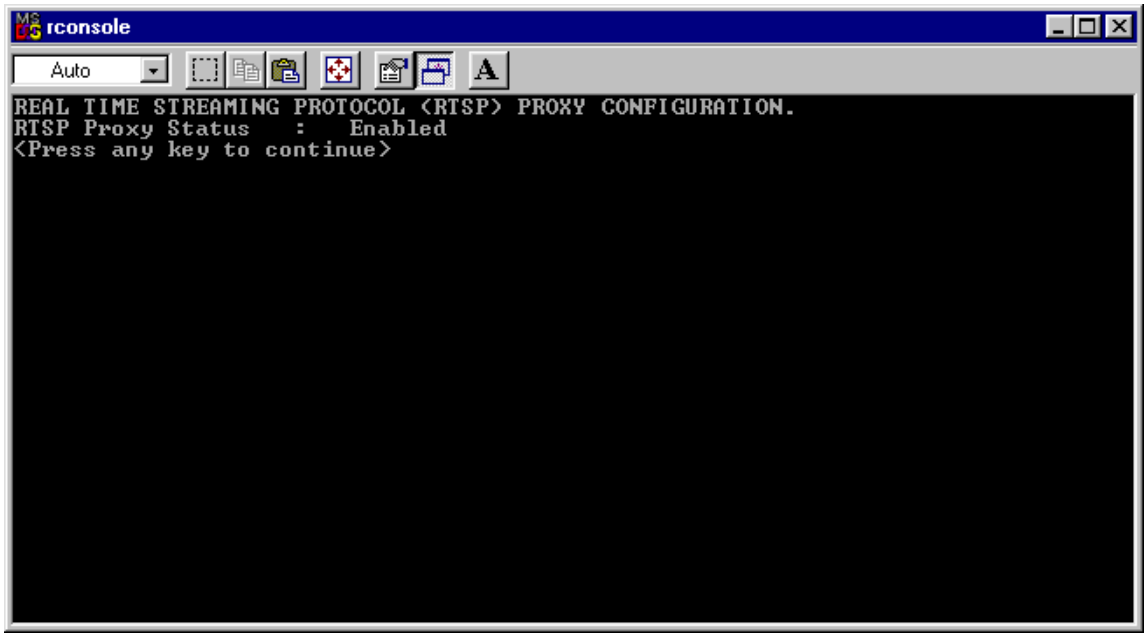
This Proxycfg menu option displays TTELNET (Transparent TELNET) proxy configuration information.



Option 17 – Display RTSP Configuration

Note This console screen is seen only on BorderManager 3.5 or 3.6 servers.

This Proxycfg menu option displays RTSP proxy configuration information. RTSP is Real Time Streaming Protocol, and the RTSP proxy is a subset of the RealAudio proxy.



Chapter 31 – Troubleshooting BorderManager

Sooner or later, everyone has some question about their BorderManager server, and needs to know why something has stopped working. There are two things to keep in mind – Simplify and Isolate.

Simplify the Configuration

There are two things you can do to simplify the situation and help isolate the problem – disable packet filtering and stop enforcing access rules. In a situation where some function of BorderManager has simply stopped functioning, you need to determine if the problem is even related to the BorderManager server, as opposed to some issue with the WAN link, the ISP, or some hardware. Since both packet filtering and access rules are designed to halt communications, it can be useful to disable them and see if communications resume.

Start at the Server

Do not bother trying to troubleshoot a communications problem at the BorderManager server until you have first made sure that the BorderManager server itself can communicate. This is primarily an issue when first setting up the BorderManager server. In particular, the BorderManager server needs to be able to ping Internet addresses by both IP address and DNS name. (Use LOAD PING x.x.x.x to ping an IP address, and LOAD PING WWW.NOVELL.COM for instance to add in a DNS resolution step). If you cannot ping an Internet address from the BorderManager server, your workstations will not be able to either. Another useful communications troubleshooting tools available at the server includes LOAD IPTRACE x.x.x.x (a trace route utility for NetWare).

Isolate the Problem

Look at the IP Packets at the Server

Use SET TCP IP DEBUG=1 at the server console to see the IP packets. (Use SET TCP IP DEBUG=0 to turn off the display.) This option can show you if packets are actually getting sent to the server, getting back to the server from the Internet, or being discarded by packet filters. Especially useful for debugging packet filter exceptions (and explained and shown in much more detail in the book "Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions", by Craig Johnson, available at http://www.craigjconsulting.com).

This option is most useful when there is little to no other traffic on the server as it can produce a tremendous amount of data. You will generally find it useful to use CONLOG.NLM to capture the data to the SYS:\ETC\CONSOLE.LOG file.

When there is a lot of traffic on the server, it may be useful to use the SET FILTER DEBUG=ON command, followed by one of the menu commands that then appears on the server console, to display only particular types of packets, such as TCP discards.

The TCP IP DEBUG command is a feature of TCPIP.NLM. The SET FILTER DEBUG command is a feature of IPFLT31.NLM, and only works on BorderManager 3.x servers.

Is it a Filtering Problem?

People will frequently assume that some communications problem is due to a packet filtering issue, especially if recent changes were made to the packet filter exceptions. There is an easy way to at least tell if packet filtering alone is causing a problem. UNLOAD IPFLT at the BorderManager server console. This command will unload the IPFLT31.NLM (the actual packet filtering module) and disable IP packet filtering. If the communications problem stops, you probably need to consider setting up another packet filter exception or adjusting one that you have. Reload IPFLT, and you can then use SET TCP IP DEBUG=1 to help determine what exactly is being filtered.

If the communications problem persists after disabling IP filtering, you may have another problem, or another problem PLUS a packet filtering issue, but you have to solve the other problem first.

Is it a NAT or a Routing Problem?

If you have disabled packet filtering, and are not enforcing any rules, you might be having a problem routing the packets. The best way I

know of to see if there is a routing problem is to look at the IP packets at the BorderManager server using SET TCP IP DEBUG=1. Using the TRACERT x.x.x.x command (from a Win95 PC) to see where the packets die can also be useful.

Here are some typical symptoms:

- No packets seen coming from an internal PC to the BorderManager server. Cause: no default gateway on the PC pointing back to the BorderManager server. (Or an intervening routing hop does not have default route pointing back to the server.
- No packets received back from the Internet, when not using IP Gateway or a Proxy. Cause: using unregistered (private) IP addresses on the internal LAN, and dynamic NAT not enabled at the server. Enable dynamic NAT on the public IP binding in INETCFG.
- Packets received from the Internet, but seemed to be ignored by the BorderManager server. (As seen using TCP IP DEBUG). Cause: NAT implicit filtering is enabled, and NAT is dropping packets *intended to go to a public IP address on the server*, such as for a Proxy, or VPN. Either disable dynamic NAT implicit filtering in INETCFG, or SET NAT DYNAMIC MODE TO PASS THRU=ON , and add that line in AUTOEXEC.NCF.
- BorderManager server doesn't send packets to the Internet. (As seen using TCP IP DEBUG). This typically means that no default route or an incorrect default route is set up. Be sure to add the correct default route in INETCFG. Do not set up default routes using TCPCON, as those routes do not get permanently saved into the SYS:\ETC\GATEWAYS file.
- If everything seems correctly set up, and static NAT is simply not working, your SYS:\ETC\NETINFO.CFG file may be corrupted. Try renaming that file, and REINITIALIZE SYSTEM at the server console. Then LOAD INETCFG and re-configure all of your LAN settings. Be careful to use the same interface names or your packet filters, which are tied to the interface names, will fail.

Is it an Access Rule Problem?

Access rules can frequently be confusing as both the rule and the position in the rules list relative to other rules has an effect on traffic through Proxies, IP Gateway and VPN. The simplest way to see if you are blocking some communication through an access rule issue is to uncheck the Enforce Rules box in NWADMN32, BorderManager Setup. If communications start working, you need

to go through the access rules list to see if you do not have the correct Allow rule, or if a Deny rule is higher in the list.

How To Search the Novell KnowledgeBase

Surprisingly few people know that you can do a Boolean search of the Novell Knowledgebase

(http://support.novell.com/search/kb_index.htm)

by making use of the word AND in capital letters. This feature goes a long way toward making a search more efficient when trying to track down an problem solution. As an example, typing in search terms

Proxy Tuning

gives you many irrelevant documents, but typing in

Proxy AND Tuning

narrows the results considerably. The AND must be typed using all capital letters.

NWADMN32 Issues

Please refer to Chapter 3, to the section called **Tips for Getting NWADMN32 to Work with BorderManager Servers**.

BorderManager 3.7 / 3.8 Issues

There are two areas that are very different in BorderManager 3.7 from other versions: Packet Filtering and SurfControl. VPN is completely different in BorderManager 3.8 from previous versions.

Packet Filtering Issues

- Filters Not Showing Up in FILTCFG
- NBMRuleContainer Object does not exist
- No Option for NBM Access Management in iManager

Generally, speaking, all of the issues above could be due to the schema not having been extended during the BorderManager 3.7 installation. I have personally seen this several times. The answer is to manually extend the schema from the BorderManager 3.7 server with the following command:

```
LOAD SCHEXT <.admin.ou.o>  <admin password>
```

Once the schema has been extended, perform the FILTSRV MIGRATE process again, and then Reinitialize System.

Another issue is that the default filter exceptions in BorderManager 3.7 are so much more narrow in scope than prior versions, that you may find a number of things which worked in 3.6 require custom exceptions in 3.7. This includes VPN!

I strongly urge the reader to get a copy of my book on BorderManager filtering. That book goes into quite a bit of detail on filtering in general, and certainly covers BorderManager 3.7 issues. See http://www.craigjconsulting.com for "*Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions, Third Edition*".

SurfControl Issues

SurfControl used to have a problem with the database update process running the server out of RAM on NetWare 6.0, if using the version that shipped on the BorderManager 3.7 CD. (There is no version on the BorderManager 3.8 CD. You must download it from SurfControl). This should not be an issue if you immediately update the SurfControl software before running the CSP_LIST process. Download SurfControl's Service Pack 2 (or later) version, and you will have a new version of SurfControl

Another issue – doubling of RAM usage during the SurfControl update process- is also fixed with Service Pack 2. See the SurfControl chapter earlier in this book.

Printing Problems Due to eDirectory 8.7.1

In order to install BorderManager 3.8, you must install eDirectory 8.7.1 or later. Certain patch levels of eDirectory have a bug that can cause older HP JetDirect print servers to fail to work. The problem is fixed with later eDirectory patches. See Novell TID's 1007805 and 2966970.

BorderManager 3.8 Won't Install Over Older Versions

The installation program for BorderManager 3.8 wants to do a clean in-place upgrade for you, if installing on a server where a previous version of BorderManager is already installed. However, Novell could only thoroughly test an upgrade from a few versions with late patches installed. So as not to take the risk of corrupting other, previous versions of BorderManager, the installation routine will refuse to install BorderManager until you uninstall the older version first. For instance, the installation program won't install over the top of BorderManager 3.0 or 3.5.

Luckily there is an easy way around this problem, without actually uninstalling the older version. You will effectively be putting yourself in a potentially unsupported condition, but I have not seen any problems with this technique for at least BorderManager 3.5 servers. The technique is to use the UINSTALL command to remove the offending BorderManager entry from the list of installed products in NWCONFIG. See Novell TID 10022635 for an explanation. This is really quite simple and only takes a minute.

BorderManager 3.8 Installation Fails with Java Error

If the BorderManager 3.8 installation fails with a java error

```
Warning: java.lang.NoClassDefFoundError:
Lcom/novell/application/classes/vpnUpgrade
```

Try renaming the SYS:\NI\UPDATE\DATA\SP.DB file and replace with the SP.DB file from the BorderManager 3.8 installation CD. Path: INSTALL/JAR/PRODUCT.JAR/NISHIP.JAR.\ni\update\data \sp.db.

HTTP Proxy Issues

The HTTP Proxy is generally pretty good, especially when you have the latest patches. Early (unpatched) versions had a nasty bug if read-ahead was enabled (enhances performance) and a broken link was encountered. The proxy would get into an endless loop, requesting the page with the broken link over and over and over, looking like some sort of denial of service attack to the ISP involved. The latest patches seem to have fixed this problem.

HTTP Proxy also has problems with certain HTML chat web sites, and the following addition in the SYS:\ETC\PROXY\PROXY.CFG file may help. (See TID 2942563)

Another issue is a possible problem with certain web site if you have ‘maintain persistent connections to origin servers’ enabled, which normally enhances performance.

If you have cached a web site, and for some reason the DNS information on that site is incorrect (perhaps the site address has changed), you may need to clear the cached DNS entries for the proxy. To do this, you need to first UNLOAD PROXY, then delete the SYS:\ETC\PROXY\PXYHOSTS file, and then reload PROXY.NLM. If the cached data itself is corrupted, or you have to wrong page in cache, you may also need to LOAD PROXY –CC to clear (all) the cached data. If you are up to date on patches for BorderManager 3.5 or later, you do not need to delete the PXYHOSTS file anymore, as the LOAD PROXY –CC will do that for you.

A number of issues are fixed with various patches and relevant settings in the SYS:\ETC\PROXY.CFG file. Symptoms would be inability to access some particular web site, and installing the latest proxy patches with appropriate PROXY.CFG file settings often helps.

There has been a bug related to streaming video through the HTTP Proxy. If the streaming never stops (HTTP Proxy continues to download the stream even after the browser is closed), you need to get the latest proxy patches and PROXY.CFG settings.

There has been a bug with the Read-Ahead function causing all sites to be cached, including sites marked as non-cacheable. As of this writing, I can only advise not enabling Read-Ahead.

BorderManager 3.7 has default filter exceptions that are completely different from previous versions. The intention was to tailor specific exceptions to specific proxies. For instance, the HTTP Proxy is given two default exceptions, one for HTTP and one for SSL. However, there are many web sites on the Internet that use non-standard port numbers. For each of these, you can set up a new, custom stateful filter exception. Or you can consider customizing the server with new default exceptions that are less specific, and more like prior versions of BorderManager.

Transparent Proxy Issues

Transparent proxy has the following issues, as a consequence of its design.

- Open relay from the Internet – Until the BM36C01 patch (or later), the Transparent HTTP Proxy listened on the public IP address and could be used as a proxy (relay) from the Internet. If you see strange IP addresses from Internet hosts accessing web sites on the Internet, someone is probably using your public IP address as a proxy server. Put the latest patches on for BorderManager 3.5 or 3.6.
- Logging – The log files will only show the IP address of the web sites requested.
- HTTPS – Until later BorderManager patches, the Transparent Proxy did not support HTTPS (SSL), and sites that require a user to log in may not work. To get SSL capability in HTTP Transparent Proxy for BorderManager 3.5 and 3.6, use the PROXY.NLM module from the latest BorderManager 3.7 patch, and add the following lines in SYS:ETC\PROXY.CFG (and restart proxy).

[TransparentHTTPS]
HTTPSPort1=443

- Software Virtual Servers – The Transparent Proxy does not work with Software Virtual Servers. (Only one web site at the same IP address will be seen). However, this capability was added in later patches for BorderManager 3.5 and 3.6, as long as the command

TransparentProxySupportsVirtualServers=1

exists in the proxy.cfg file in the [Extra Configuration] section.

- Speed – The Transparent Proxy is slower than HTTP Proxy, partly because the DNS lookups are not cached.
- DNS – The Transparent Proxy does not perform a DNS lookup like the HTTP Proxy. Therefore the workstations have to be configured and able to perform their own DNS lookups.
- Access Rules – Access Rules seem to work somewhat inconsistently.

Mail Proxy Issues

Mail Proxy has had a number of issues throughout its history, particularly if you are not current on the patches. Even with patches, you are limited to proxying only a single internal domain until BorderManager 3.8.

It is essential to check the installation file and readme files for each BorderManager patch to see what issues have been fixed in regard to the Mail Proxy. As of this writing, some of the Mail Proxy issues can only be address with a) a recent BorderManager 3.5, 3.6 or 3.7 patch, b) a command line option (LOAD PROXY –M), and c) certain entries made in the PROXY.CFG file. The settings are detailed in the patch instructions.

BorderManager 3.8 has a new feature called multi-domain support, that allows Mail Proxy to support multiple internal mail domains. This feature is configured in proxy.cfg and is described in the Mail Proxy chapter.

One issue I have seen reported appears to be an anti-spam-relay feature. You may not be able to send inbound email to your domain from a mail client with a user name also from that same domain.

A recent patch available for BorderManager 3.7 and 3.8 allows you to configure the Generic TCP Proxy to use port 25. This option allows you to accept inbound SMTP on the BorderManager public IP address and proxy it to an internal SMTP mail server without using Mail Proxy.

Best to ask in the Novell Support Connection public forums for specific issues regarding this proxy, but I have seen mail messages get stuck in the outgoing spool directory for even the version in BorderManager 3.8SP1A.

DNS Proxy Issues

The DNS Proxy is not bad, but some feel that it is less reliable than simply passing DNS requests through to the ISP's DNS servers with a stateful packet filter exception. If your BorderManager server suffers from ABENDS, try turning off DNS Proxy. I have not seen problems with DNS Proxy in versions 3.6 or later with current patches.

If the DNS servers listed in Proxy Console option 4 vary a lot between UP and DOWN, try setting the DNS transport in NWADMN32, BorderManager Setup from UDP to TCP. This option has been removed in later BorderManager proxy patches, so it is best to ask in the Novell public forums for a fix or workaround to this issue.

IP Gateway Issues

IP Gateway has a long history of issues, most of which result from a misunderstanding of what this feature is all about. First, be sure to understand what it does and how it works!

The issues mostly involve a mismatch of Client32 versions and IP Gateway versions. (IP Gateway includes IPX/IP and IP/IP Gateway in this discussion). There have been several versions of IP Gateway, starting before BorderManager with NetWare 4.11. Basically, you need to have Client32 version 2.2 to 2.5 and possibly 3.0 to work with IP Gateway on BorderManager 3.x. Another problem aspect is that not all versions of programs will work with the IPX/IP gateway, and those problems are often Winsock version issues.

As of this writing, it has been reported in the forums that the IPX/IP Gateway does not work with Novell Client 32 versions 3.3 and 4.8.

Legacy Site-to-Site VPN Issues

Legacy VPN refers to the version of VPN used in BorderManager 3.7 and earlier versions.

Should you find that one of the VPN links has gone down and does not want to come back up, try the following:

1. Be sure the time on the slave VPN server is within a few minutes of the time on the master VPN server.
2. In NWADMN32, BorderManager Setup, VPN, Site-to-Site Details, Status, try Synchronize All (or Synchronize Selected on the Master VPN server and the Slave VPN server giving a problem).
3. Type Reinitialize System at the Master VPN Server.
4. Type Reinitialize System at the Slave VPN Server
5. A new problem has popped up with the IPXRTR.NLM in the NW6SP1.EXE and NW51SP4.EXE patches. IPX support disappears from the Site-to-Site VPN. See my web site http://www.craigjconsulting.com for additional information on this problem, and a workaround, should you be affected. Later patches do not have the problem, which involved loss of IPX communications over the VPN link.
6. The default exceptions in BorderManager 3.7 do not include all of the exceptions required by VPN. As of this writing, you will need to manually add exceptions as indicated elsewhere in this book, or as shown in the Third Edition of "*Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions*", available at http://www.craigjconsulting.com. Alternatively, you can use BRDCFG.NLM from BorderManager 3.7SP2 (or later patches) to rewrite the default filters and exceptions. However, the default exceptions for this version of BRDCFG are considerably different from previous versions, and I do not recommend you change them without a thorough knowledge of filtering.

Legacy Client-to-Site VPN Issues

Legacy VPN refers to the version of VPN used in BorderManager 3.7 and earlier versions.

There is a problem with SLP on Pure IP VPN logins. IPX generally does not have a problem, but if you are logging into the VPN with a pure IP Client32 on the remote host, you may find that you cannot resolve NetWare server names for several minutes, even with a statically configured Directory Agent. As a work-around, you can log into the NetWare 5.x/6.x servers using the server's IP address instead of the server name, or add the server names to the local HOSTS file on the PC. This problem is addressed in the latest VPN client for BorderManager 3.7 and 3.8, which is available for download and is backward-compatible to previous versions of BorderManager.

WindowsME does not support the VPN client prior to the BorderManager 3.7 version of the VPN client.

Windows 2000 and Windows XP do not support IPX over VPN.

Windows XP may well work with VPN clients prior to the BorderManager 3.7 version, but they are not supported by Novell.

VPN over a NAT connection can only be done using BorderManager 3.6 or later, and the NAT connection can only be on the remote client side.

If you have four instances of IPX protocol installed (for multiple adapters like dial-up, Microsoft VPN client, and two network cards), you will not be able to add IPX support to the VPN client when it is installed. You will have to delete one of the adapters, and delete and reinstall the VPN client software.

BorderManager 3.5, 3.6 and 3.7 may not let you connect to the private IP address of the VPN server when dynamic NAT is enabled on the public IP address. To get around this issue, enabled a static NAT mapping of the private IP address to itself. Afterwards, you should be able to ping the private IP address from a remote VPN client. This is essentially a NAT issue, which is supposed to be fixed in NAT 6.00d or later versions.

The default exceptions in BorderManager 3.7 do not include all of the exceptions required by VPN. As of this writing, you will need to manually add exceptions as indicated elsewhere in this book, or as shown in the Third Edition of "*Novell BorderManager: A Beginner's Guide to Configuring Filter Exceptions*", available at http://www.craigjconsulting.com.

BorderManager 3.8 VPN Issues

Note BorderManager 3.8 VPN is complex, and can be hard to troubleshoot. I may have additional suggestions at my web site (http://www.craigjconsulting.com/), but you may also want to open an incident or hire a consultant (like me) to help troubleshoot VPN issues.

Understanding How VPN Gets Configured

A short description of how the VPN configuration process works may prove useful to those who have to debug it when it breaks. BorderManager 3.8 VPN begins by an administrator submitting changes to NDS, and ends by modules that do the actual work being autoloaded on the server. There is a lot that can go wrong.

You submit changes to NDS in iManager, which is itself a combination of java servlets (TOMCAT4) and web page elements (Apache), communicating to NDS via LDAP. If secure LDAP is used (and it is), then SSL certificates and the entire encryption infrastructure of the server and tree get involved. Once the server's VPN configuration is submitted to NDS, java servlets running on the BorderManager server should see the change to the configuration, read the new information, and automatically update files in various locations on the BorderManager 3.8 server. (Such as SYS:ETC and SYS:SYSTEM\VPN). Once the files have been updated, you should see various settings appear in INETCFG, such as the following:

Boards – Should show a VPTUNNEL interface

Network Interfaces - Should show a VPTUNNEL interface

WAN Call Directory – should show entries for other servers in a Site-to-Site VPN.

Protocols, TCP/IP, LAN Static Routing Table – should show a route to the server's VPN tunnel IP address, and (in most cases) a route to other Site-to-Site VPN servers.

Bindings – Should show entries (IP and possibly IPX) for the VPTUNNEL interface

If such items are not seen in INETCFG, then the server has not been configured yet (which is supposed to be done by java servlets from NDS data – you do not edit the files yourself). It may be that there is a java issue and the data has not been read from NDS, or there might be an NDS synchronization problem, or it might be that you have INETCFG running and holding files open so they cannot be edited.

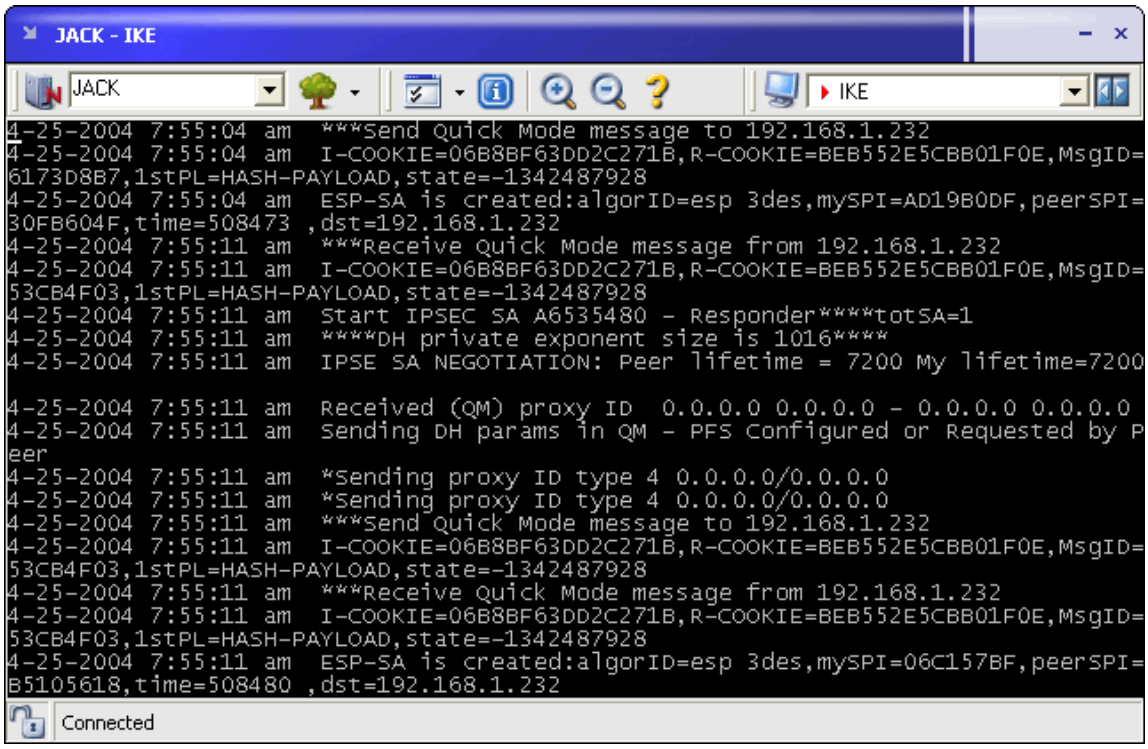
Once INETCFG shows VPN-related entries, a STARTVPN command (which should be seen in STARTBRD.NCF) should cause

modules to load which then bring up VPN components like IKE and make calls to other VPN servers.

Troubleshooting Tools

When things simply don't work, you need to start getting more information. The most obvious place is the IKE console screen, but that is only going to give limited information, and then only for the very initial connection stages of a VPN connection. Here are some things to look at:

- **IKE console screen** – useful for seeing if an IKE connection is failing, working, or even being attempted.
    - Here is an example of the IKE console screen in a working Site-to-Site VPN connection (at the Master).



- **IKE screen present** – If you see the IKE console screen, then at least server has read its VPN configuration from NDS and thinks it should launch VPN services
- **Main Mode and Quick Mode** – If you see the words Quick Mode show up on the IKE console screen, Congratulations! IKE is probably just fine, as Quick Mode only occurs after the initial Main Mode is successful, and Main Mode connections are where you see failures.

- **Unacknowledged message** – This is always bad, as it means that the server has rejected a connection from another server and is sending that server a message (which does not have to be acknowledged) that it is not making a connection.
- **No traffic seen from another VPN server** – Not a good sign, unless the other server just hasn't been configured yet. If routing, filtering and configuration is in place, you should be seeing traffic coming in from another Site-to-Site VPN server.
- **Retransmit Timer Expired :Peer lost our reply** - If you see a message that a peer lost a respond, it means that one server sent a connection request to the other and never got a response.
  - The other server could be down
  - VPN services may not be started on the other server yet
  - Filtering between the two servers could be blocking packets
  - You could be having routing (the servers should be able to ping each other's public IP addresses without filters up, before the PVN is started
  - The IP addressing could be incorrect (wrong server address configured).

- **Novell Remote Manager (NRM)** – NRM should be available if HTTPSTK and PORTAL are loaded when the server starts (this is the default). When VPN is started (STARTVPN or STARTBRD), a module called VPMON.NLM should be loaded. With VPMON loaded, you should have a VPN Monitoring option available on the lower left pane. See examples in the chapters on Viewing VPN data. Within the VPN Monitoring option, you can choose the local VPN server, and have a number of options, but the most useful troubleshooting tool is the Audit Log option.
- **CSAUDIT** – Typing CSAUDIT at the server console brings up a menu with the choice Display Audit Trail Records. That choice should show you any VPN activity taking place, and has a useful Display Option (press Insert) to Display Entries in Descending Order (to see most recent activity at the top of the list). You can also export the log data to a text file.

- **_VPN Command** – Typing _VPN at the server console, once the IKE console screen is present will result in a menu that allows you to display troubleshooting information for both Client-to-Site and Site-to-Site VPN. Typing _VPN again turns off the debug screen.
- **RUNVPN –l3** – If VPN does not load automatically, it generally has something to do with a NDS issue on the server, or possibly a java issue. However, you can get some more detail on what is going on if you STOPVPN, and then RUNVPN –l3 to create debug output for the VPN startup process. RUNVPN –l3 will start VPN services with a debug screen, and also capture output to SYS:\SCMLOG.TXT.
- **PKTSCAN.NLM** – PKTSCAN is a packet capturing sniffer program available on the BorderManager 3.8 Companion CD as well as via download from Novell's web site. Loading this module at the server prompt allows you to capture packets at one or more interfaces on the server, as well as display them there or (best) output the captured data to a trace file. You can use a program like Ethereal (www.ethereal.com) to open the file and look at the data. PKTSCAN can be useful in seeing what kind of traffic is getting to the server. When PKTSCAN is loaded, you should also have a convenient browser-based menu option in Novell Remote Manager, but only if you download a newer version than the one supplied with BorderManager 3.8. As of this writing, PKTSCAN102.EXE is the latest version available from Novell, and it automatically registers itself with Novell Remote Manager when loaded.
- **CALLMGR.NLM** – The CALLMGR utility is provided on the BorderManager 3.8 Companion CD in the CALLMGR directory. This simple NLM dates back to the NetWare connect and NIAS days, and was originally used to force a modem connection. Since the same logic has been recycled in part for VPN connections, you can use CALLMGR to initiate a VPN connection from the server console screen.
- **VPN Schema Extension Utility** – There is a utility program on the BorderManager 3.8 product CD, Unsupported directory, to allow you to manually extend the schema for VPN if that failed during installation.
- **VPN Schema Removal Utility** - There is a utility program on the BorderManager 3.8 product CD, Unsupported directory, to allow you to manually remove VPN schema extensions, in case you feel the need to do that.
- **VPN Migration Utility** - There is a utility program on the BorderManager 3.8 product CD, Unsupported directory, to allow you to manually migrate a VPN configuration from a

previous version of BorderManager in case an in-place migration failed to do that automatically.

- **CFGDUMP.NLM** – There is a handy utility program called CFGDUMP.NLM in the BorderManager 3.8 product CD, Unsupported directory, that will save pertinent BorderManager settings to a text file in the SYS:ETC\PROXY directory. This file can be used for documentation, or to send to Novell or to a consultant for troubleshooting.

BorderManager 3.8 Site-to-Site Issues

Some issues I have seen so far include:

- **VPN will not start on the server**, and you see **public symbol errors about IPSec** in the logger screen (or server console on NetWare 5.1). This generally means that you have the wrong version of TCPIP installed. For BorderManager 3.8 VPN, you MUST have the "(Domestic) NICI" version of TCPIP installed for the VPN to work. This version is available on the BorderManager 3.8 product cd, and is in NW6SP4 as well as NW65SP1. The latest TCPIP patches also include (Domestic) NICI versions.
- Some **changes to Site-to-Site VPN not taking effect** without stopping and restarting the VPN with the STOPVPN and STARTVPN commands. (Most changes should take place within 15 minutes as the default setting for VPN is to retry VPN connections every 15 minutes).
- **Servers stuck in being configured mode**. This one is fairly common, and I know that I do not know all the possible reasons for it yet. Check the following:
    - This may be caused in same cases by filtering issues, especially if IKE connections are OK.
    - If IKE connections are not established, you will never get the VPN server to be configured (except for legacy VPN).
    - One time I saw that the slave server would never get the configuration information pushed from the master. The reason in that case was that there was a file called VPN in the SYS:SYSTEM directory, and that file was preventing BorderManager from creating a SYS:SYSTEM\VPN directory. The directory is required, and it holds VPN information pushed from the master to the slave servers. Deleting that VPN file allowed the slave server to finish being configured.

- **Server-server VPN communications being blocked by filtering**, with stateful filtering failing to allow VPN communications needed to configure the VPN. A symptom is a slave server never getting all the VPN configuration pushed to it from the master. I have seen TCP port 213 traffic being filtered when it should not have. Dropping the filters and restarting VPN services on the master generally gets you past this problem, as does redoing the filter exceptions to use non-stateful exceptions for VPN traffic. Note that reinitializing system, or starting VPN will also reload filter exceptions, so you must either immediately UNLOAD IPFLT or add a filter exception to allow all IP in order to really drop the filters.
- **ACL Check errors** in the IKE console screen, VPN Monitoring Audit Log (in Novell Remote Manager), or CSAUDIT log display. This is caused by one server rejecting the certificate from another server. There are essentially only three things I know of that can cause the certificate to be rejected:
    - Incorrect subject name typed into the configuration on the server. The slave server configuration needs to know the Subject Name of the Master VPN server's VPN certificate. Look at the certificate subject name carefully and type it exactly. Do not mistake it for the Trusted Root certificate name. Perhaps the best way to know what subject name is actually being sent is to look in the Audit Log messages in Novell Remote Manager – there should be an entry in there telling you that there was an ACL error for a subject name. Just use that subject name in the VPN configuration, and it should be accepted if the TRO is OK.
    - Incorrect Trusted Root Object (TRO) created for the trusted root of the other VPN server. The TRO is created inside the Trusted Root Container for each VPN server, from a .DER file exported from another VPN server. The most common errors here are forgetting to create a TRO, or using the wrong .DER file. The .DER file is exported from the other server's Trusted Root certificate when you look at the VPN certificate – don't mistakenly export the server certificate. A VPN slave server only needs a TRO from the master VPN server. A Master VPN server needs a TRO for each slave.
    - VPN certificate created with the wrong values. The VPN certificates need to be created with certain non-default settings, as shown in the 3.8 Site-to-Site VPN chapter earlier in this book. You cannot use the standard SSL CertificateIP or SSL CertificateDNS certificates for Site-to-Site VPN.

- **Server not launching VPN service** – no IKE screen ever shows. I have only seen this in the case of NDS problems. A java application is supposed to read VPN configuration details from NDS and will then launch IKE and other modules as needed. If NDS has problems, it is possible that the java application never sees the server as being configured as a VPN server. In some cases a simple DSREPAIR helps, but usually there is some underlying NDS synchronization issue between servers in the tree.
- **VPN established, but no communications occur across the VPN**. I have seen this happen if the wrong IP address on the server is configured in the VPN configuration. (The private IP address of the server was configured instead of the public IP address).
- **STOPBRD or STOPVPN causes <2> abends** to appear on NetWare 5.1 servers – this is a java-related issue, and I have been able to cure it by upgrading the JVM component to at least 1.31 version 7. You can download a JVM patch from support.novell.com, and (in general) you can get the latest version of JVM patches from developer.novell.com.

BorderManager 3.8 Client-to-Site Issues

Some issues I have seen so far include:

- **VPN Client will not install**. If you have previously had an older Novell VPN client installed on the PC, you must first uninstall it to install the newer VPN client (version 3.8.4 as of this writing). However, you may still get error messages saying that the previous VPN client must be uninstalled before the new client will be installed. In this case, be sure to try to delete the NICI 1.5.7 components with Add/Remove Programs in Control Panel. If that does not work, there is an unsupported utility in the later BorderManager 3.7 and 3.8 patches called VPNRegClean.exe which can be used to clean up leftover registry settings from the old VPN client.
- **VPN will not start on the server**, and you see **public symbol errors** about IPSec in the logger screen (or server console on NetWare 5.1). This generally means that you have the wrong version of TCPIP installed. For BorderManager 3.8 VPN, you MUST have the "(Domestic) NICI" version of TCPIP installed for the VPN to work. This version is available on the BorderManager 3.8 product cd, and is in NW6SP4 as well as NW65SP1. The latest TCPIP patches also include (Domestic) NICI versions.
- **Failed Receiving Server DH Public Value error** when connecting from the VPN client. This is due to a misconfiguration (and possibly an NMAS error) in the Client-to-

Site VPN authentication rule for NMAS. If you have this error, and you changed the NMAS Authentication level from 'Logged' (the default) to 'Password', change back to 'Logged' and the error should go away.

- **LDAP Configuration changes may require a STOPVPN, then STARTVPN** command to take effect.
- **Authentication and Traffic rules not applying to NDS or LDAP containers** – could be a case-sensitivity error for both the user names and the passwords.
- **Disabling a user account not preventing that user** from authenticating in certificate mode. Novell is working on this one as of this writing.
- **LDAP Authentication not working** over a port-forwarding configuration (server behind a NAT hop). Novell assures me that this should work, so it may be a limitation of the router I tested.
- **VPN client installed, but simply not working**. Check the properties of the local area connection, TCPIP, and be sure there is a check in the check box for Novell Virtual Private Network.
- **Cannot browse the Internet while connected to the VPN**. This is a consequence of having a Default Traffic Rule that denies all traffic. The solution is to have a traffic rule just above the Default traffic rule to not encrypt and network address. There is an example of this in the BorderManager 3.8 Client-to-Site VPN chapter.
- VPN client connects, and works, but the **VPN client system tray icon disappears**. An annoying little bug, but relaunching the VPN client (while the VPN is still connected), then canceling it should bring back the icon in the system tree. You need that icon to disconnect cleanly.
- **VPN DNS information not cleared** from the client if the VPN client does not cleanly disconnect. This is a nasty one, because if you configure the VPN to push your internal DNS servers to the workstations, and the remote PC crashes or otherwise does not cleanly disconnect, the internal DNS servers are left on the remote PC. This causes the remote PC to be unable to browse the Internet until those DNS servers are removed.
- **DNS Server information not pushed** to the VPN client. In order to push the DNS server information to Windows 2000 or XP PC's, the user logged into Windows must be at least a Power User.
- **SLP DA information not pushed** to the VPN client. This option requires Client32 4.9 or later on the VPN client. Also,

the user logged into Windows 2000 or XP must be at least a Power User.

- **SLP DA information not removed** from the remote PC after unclean VPN disconnect. A bug similar to the DNS issue described above – if you do not disconnect cleanly from the VPN, SLP DA settings may be left behind and require manual removal.
- **Cannot Get Certificate** in the VPN client. Probably Working As Designed (WAD). This feature requires the client to be already logged into the NDS tree before trying to get a certificate.
- **VPN client crashes Windows 2000 PC**. A bug with a couple of versions of the VPN client (the latest version, BM3XVPN3.EXE as of this writing, has this bug) will crash Centrino-based laptop PC's.
- **Memory leak** with each VPN connection. Check Monitor, System Resources, Alloc Memory and look at the XMGR module. This module SHOULD take only a few K bytes. However, up to at least BM38SP1A, some bug causes it to leak memory, about 2-6K with each VPN connection made to the server. Keep an eye on this one as it can eventually run the server out of RAM. The only workaround until a patch comes out for this problem is to reboot the server.
- **Cannot ping internal IP address of BorderManager server** over VPN connection. In most cases, it is a NAT issue that is supposed to be fixed with BM38SP1A. If you can add a secondary private IP address and ping that, but not the primary private IP address, you probably are seeing a NAT issue. (Test with NAT disabled in INETCFG to confirm). One workaround may be to add a traffic rule at the bottom of the rules list to not encrypt traffic to the BorderManager private IP address.
- **Cannot ping internal hosts** over VPN connection. Check all of the following:
    - VPN tunnel address is not in the same network as the client address. (Remote network should not have the same network address as the VPN tunnel network).
    - Internal host addresses are not in the same network as the client address. (Remote network should not have the same network address as any of your internal LAN segments).
    - VPN server configured with correct Server IP Address (meaning the public address, and not the private address of the server).

  - No traffic rules set up to allow the traffic to internal segments.
  - VPN server not the default path to the Internet for internal hosts. In this case, routers that ARE on the default route to the Internet need to have a static route configured to redirect the VPN client IP addresses (configured by you in the VPN Client-to-Site configuration) to point to the BorderManager VPN server.

- **Preventing Compatibility Mode (Legacy) VPN client connections** – If you have upgraded your old BorderManager server to 3.8, and IKE-based Client-to-Site VPN is working, you may wish to prevent legacy VPN connections from being made to the server. Load VPNCFG.NLM on the server, and remove the VPN configuration. This will not hurt IKE-based VPN, but it will prevent both Site-Site and Client-Site SKIP (Legacy) VPN connections. The problem here is that if you need to maintain legacy Site-to-Site VPN connections, you cannot use this technique since it will destroy those VPN connections. The only control you have is to be careful with NMAS Traffic Rules, as those rules affect the legacy VPN client policies (protected networks).

iManager 2.0 Issues

General Issues

iManager 2.0 is a very complex system that can seem impossible to troubleshoot if something goes wrong. Novell has a TID that tells you to check to see if an incomplete installation occurred, and that you should have 14,000-19,000 files under the Tomcat /4 directory. I can only offer a little advice on troubleshooting it:

- Don't go through a proxy when using iManager (or Novell Remote Manager). Configure your browser to bypass proxy to the iManager IP address (or URL, if you use one to access it). This is especially true when using iManager on your PC and accessing it with localhost.
- If iManager on NetWare does not work, **check to see if it is starting up correctly**. iManager consists partly of a web server (Apache) and partly of java servlets (Tomcat). Look in the NetWare 6.x logger screen when Apache and Tomcat start up. Any errors you see there will be a clue to something going wrong. Also load TCPCON, and look at TCP Listeners. If port 2200 is not showing up, iManager did not load at all. You can also load TCPCON early in AUTOEXEC.NCF, and put Pause statements in various places. That way you can see if something unexpectedly is listening on port 2200 before iManager gets a chance to load.
- If you have a local installation of iManager on Windows, you may find that **you cannot log in to iManager if you have changed the IP address of the server** used when iManager was originally installed. You may have to change the portal.properties file to point to another IP address, or reconfigure iManager itself for a new NDS tree. These steps are actually easy – if you know what to do. See the chapter on iManager 2.0 at the end of this book for the location of the properties file you have to edit. Commenting out the server IP address in there, and the PCO line, allows you to reconfigure iManager by going to http://localhost/nps/servlet/configure. If you do not edit the properties file, you will not be able to configure the settings.
- **iManager sometimes quits working** for me when a browse window opens. Invariably I have to close the browser, and log back into iManager again. In the

meantime, any changes you made that were not saved are lost.

- iManager, even locally installed, **needs to make an LDAP login** to a server for you to log in. Be aware that iManager is configured to point to one server, and that server must be up and running, with LDAP access, for you to use it. If you have iManager configured for LDAP port 389, you must allow clear text passwords on the server. (LDAP Group general properties).

Problems with Unknown System Error in iManager 2.0.1 on Windows

- There is a version of iManager 2.0.1 on the BorderManager 3.8 Companion CD which can be installed on a Windows PC. If iManager does not run properly, you could be missing a java file called njclv2.jar, which should be in the tomcat lib directory on your PC. See Novell TID 10090674. You can find the file on the BorderManager 3.8 product CD. It can also be downloaded from Novell.

Problems with iManager 2.0.1 on NetWare 6.0

There is a version of iManager 2.0.1 on the BorderManager 3.8 Companion CD which can be installed on a NetWare 6.0 server. However, there are a number of configuration file changes that may be required after the installation to get iManager 2.0 to work. Here is a quick list of things to look at.

Installing iManager 2.0.1 on NetWare 6.0

- First, you must have eDirectory 8.7.1 or later installed on the server. You can install 8.7.1 from the BorderManager 3.8 Companion CD. Install 8.7.1 (or later) to the server, reboot, and run a DSREPAIR (unattended full) for good measure.
- Next, you must install JVM 1.4.1 to the server. JVM141SP1.EXE is provided on the BorderManager 3.8 Companion CD in the JVM directory. Install that version of JVM and reboot.
- Next, install iManager 2.0.1 from the BorderManager 3.8 Companion CD to your NetWare 6.0 server. This will install Tomcat version 4 to your server, and it should put lines in AUTOEXEC.NCF to start it automatically. You can run both TOMCAT3 and TOMCAT4 at the same time, but you then have even more possible problems to debug. *The following*

instructions assume that you will run only TOMCAT4, and prevent TOMCAT3 from starting. (Not running TOMCAT3 will break iManager 1.5 and things like the Novonyx web management utility running under Apache.)

Getting iManager 2.0.1 Running on NetWare 6.0

- You can run both TOMCAT3 and TOMCAT4 at the same time, but you then have even more possible problems to debug. *The following instructions assume that you will run only TOMCAT4, and prevent TOMCAT3 from starting*. (Not running TOMCAT3 will break iManager 1.5 and things like the Novonyx web management utility running under Apache.)
- When the iManager installation is completed, you should check that AUTOEXEC.NCF is not loading TOMCAT33 anymore, but is loading TOMCAT4. **Comment out any TOMCAT33 load lines**, and either kill the java process for the old Tomcat33 process (or kill all Java processes and restart TOMCAT4), or reboot. Tomcat33 java process (JAVA -SHOW command) will say "org.apache.tomcat.startup.main". Tomcat4 java process will say "org.apache.catalina.startup.Bootstrap".
- Try starting iManager 2.0.1 using **https://x.x.x.x/nps/iManager**, where x.x.x.x is the internal address of the NW 6.0 server. You should get a certificate (accept it), and if very lucky, you will get a login screen. If so, you are probably done. Otherwise, keep reading.
- Go to **SYS:\APACHE\CONF** and edit the **ADMINSERV.CONF** file. Remark out three lines:
  # Redirect /iManage/ https://172.16.1.254:2200/eMFrame/iManage.html
  # Redirect /iManage https://172.16.1.254:2200/eMFrame/iManage.html
  # Include "SYS:/webapps/eMFrame/WEB-INF/eMFrame-apache.conf"
- Also in the **ADMINSERV.CONF** file, find two lines that have "tomcat/33" in them (JK properties lines), and **change "tomcat/33" to "tomcat/4"**.
  JkWorkersFile "SYS:/tomcat/4/conf/jk/nwworkers.properties"
  JkLogFile "SYS:/tomcat/4/logs/mod_jk.log"

- Also in the **ADMINSERV.CONF** file, go to the end of the file and make sure there is an "**include sys:tomcat/4/conf/nps-Apache.con**f" statement.
- Go to **SYS:\TOMCAT/4\CONF** and see if you have a directory called **JK** with about 8 files in it. If not, copy the JK directory over from the SYS:\TOMCAT\33\CONF directory to the SYS:\TOMCAT\4\CONF.
- While we are at it, let's fix a potential problem with the Coyote /HTTP webserver built into Tomcat4. Tomcat4 includes a miniwebserver that defaults to listening on port 8080, which can conflict with the BorderManager HTTP Proxy. Go to the **SYS:\TOMCAT\4\CONF** directory and edit **SERVER.XML** with Notepad. Search and **replace "8080" with "8081"**. Stop Tomcat4 (TC4STOP command) and restart (TOMCAT4 command). Look in the logger screen, and wait... (and wait a bit more, until you finally see a line that includes ajp12 and 0.0.0.0/9010). You should see a line "INFO: Initializing Coyote HTTP /1.1 on port 8081" if SERVER.XML was correctly edited.
- Stop Apache (NVXADMDN), and restart it (NVXADMUP).
- **Stop Tomcat** (Kill the java processes as noted in step 3, or kill all java processes with a java -killall command, or use TC4STOP if only Tomcat4 is running). **Restart Tomcat4** (TOMCAT4 command). Look at the logger screen and **wait** until you see "INFO: JK2: ajp13 listening on /0.0.0.0:9010:
- **Try https://x.x.x.x/nps/iManager.html**, where x.x.x.x is the private IP address of the server. Hopefully after a short delay you will get a login screen where you can log in as admin. If so, you are probably done. If not, keep reading.
- **You may have to configure iManager** and NDS using the exteNd director in a browser. This step involves an LDAP login to NDS, and a java process that creates an OU in your tree called Extend (or Extend-xxx if there is already an Extend directory in there), and a bunch of objects that control how iManager works. I show the process in Chapter 34 of this book. You start the process by pointing your browser to **https://x.x.x.x/nps/servlet/configure**. Should you want to reuse/reconfigure an existing pco object (already have a Extend OU in the tree), you may need a password that is contained in a file mentioned in Q1 or Q2 above,

assuming you can find the file on a NetWare or Windows server. I do not find it particularly a problem to just create a new pco object and another Extend directory if you can't get into the old one. At the end of this procedure, you need to stop and restart Tomcat4 (tc4stop, and then tomcat4, and then wait a bit).

Miscellaneous Issues

BorderManager Does Not Start After NW51SP7, NW6SP4 or NW65SP1

The latest NetWare patches changed the behavior of the ? command when used in an NCF file to create a delay. The default behavior when using a ? at the start of a command is to wait 10 seconds for a Yes or No (y/n) reply, and then assume the answer is Yes and execute the command. This is very convenient for adding 10-second delays in AUTOEXEC.NCF. However, the latest service packs will no longer allow you to have a space between the ? and the command. If you have a space in there, the command will not be executed. So:

? Startbrd

will not launch BorderManager, while

?Startbrd

will work just fine. If you have any spaces after a ? in your AUTOEXEC.NCF file, remove them and try rebooting for a test.

Dial-Up Connection Keeps Coming Up

NetWare 5.x/6.x servers will multicast there presence on all interfaces by default. Due to the design of the IP stack, this behavior can cause a dial-up interface to be brought up BEFORE any traffic is actually sent. Thus, filtering is unable to prevent the link from coming up, though it can prevent traffic from being sent out. There are two ways to get around this problem - unload NCPIP.NLM or use a newer version of NCPIP.NLM with a new SET parameter. If you unload NCPIP.NLM, you cannot log into the server using pure IP, and all server NCP communications will require IPX. A better way would be to use the newer NCPIP.NLM contained in the latest NetWare 5.x/6.x service packs.

The newer NCPIP.NLM allows a SET parameter to be used to exclude or include advertisements on certain IP addresses. You may need to include all public secondary IP addresses defined, though a dial-up link usually doesn't have multiple addresses assigned.

SET NCP EXCLUDE IP ADDRESSES x.x.x.x (for the version in the service packs, use SET NCP EXCLUDE IP ADDRESSES = x.x.x.x - that is, add the = sign.)

or

SET NCP INCLUDE IP ADDRESSES x.x.x.x (which may be better as you should be able to list only the internal, fixed, IP

addresses). For the version in the service packs, use SET NCP INCLUDE IP ADDRESSES = x.x.x.x – (add the = sign.)

Also, you can easily set the INCLUDE NCP ADDRESS in MONITOR, Server Parameters, NCP. With NetWare 6.x, you have a similar issue (and solution) with SLP communications. MONITOR has a similar setting in the Service Location Protocol menu.

Chapter 32 - Performance Tuning

Novell's TID 10018669 is an excellent source of information for maximizing the caching performance of a Novell BorderManager 3.x server. I do not reproduce it here due to copyright issues, but I show the recommended settings. I also provide a TUNEUP.NCF file with the recommended settings at my web site in tip #23. See http://www.craigjconsulting.com/.

Be careful of the settings if you do not have a dedicated BorderManager server. Some of the settings bias performance very much toward caching, and others trade large amounts of RAM for caching performance. Non-BorderManager services can either slow down or even crash the server if you are not careful in tuning aggressively or do not have enough RAM in the server. Basically, a dedicated production BorderManager server prior to version 3.7 should have at least 256MB of RAM as a starting point.

BorderManager 3.7 or 3.8 servers should have at least 512MB of RAM, and BorderManager 3.7 or 3.8 servers running SurfControl should have at least 1GB of RAM.

I have added some notes in the text below where I have some disagreement with Novell's recommendations. Please see TID 10018669 at http://support.novell.com for explanation of the various parameters.

General Recommendations

- Get the latest patches and drivers.
- Get the latest DISK and LAN drivers from your hardware vendor.
- ALWAYS read the readme file for new patches before applying them.
- Keep Cache Volumes Separate
- Have Multiple Cache Volumes (best to have them on separate physical drives).
- Turn Compression Off
- Turn Block Suballocation Off
- 8k Block Size
- Use DOS Name Space only on cache volumes
- Never use NSS cache volumes!
- Load NETDB.NLM /N directly after INITSYS.NCF

Note I do not recommend loading NETBD.NLM manually at all. Changes to the TCP/IP modules have caused big problems in the past when trying to use NETDB /N.

- Clean out unnecessary entries from the SYS:\ETC\HOSTS file
- Clean out unnecessary entries in the SYS:\ETC\RESOLV.CFG file
- Delete the SYS:\ETC\PROXY\PXYHOSTS file if you suspect DNS cache problems.

Note I also recommend you flag the PROXY directory for immediate purge of deleted files so that you do not build up endless copy of deleted PXYHOSTS files. A new PXYHOST file is saved every 10 minutes.

Use the Following Server Set Parameters

It is IMPORTANT to read the TID (10018669) on these parameters to understand the suggestions and when you might want to use something different.

- Maximum Physical Receive Packet Size = 4224

WARNING! *With many modern LAN drivers, particularly with NetWare 5.x, you should use a Maximum Physical Receive Packet Size of* ***no less than 2048*** *because the LAN drivers require additional overhead! Going too small on this parameter can cause tremendous communications problems.* ***I prefer to waste some memory and leave the value at the default of 4224.***

- Maximum Packet Receive Buffers = 10000
- Minimum Packet Receive Buffers = 5000
- New Packet Receive Buffer Wait Time = 0.1 sec
- Maximum Interrupt Events = 50
- Garbage Collection Interval = 5
- Read Ahead Enabled = on
- Maximum Concurrent Disk Cache Writes = 750
- Dirty Disk Cache Delay Time = 0.1 sec
- Dirty Directory Cache Delay Time = 0.1 sec
- Maximum Concurrent Directory Cache Writes = 125
- Directory Cache Allocation Wait Time = 0.1 sec
- Directory Cache Buffer NonReferenced delay = 30 min
- Minimum Directory Cache Buffers = 1000
- Maximum Directory Cache Buffers = 4000
- Maximum Number of Internal Directory Handles = 500
- Immediate Purge of Deleted Files = on
- Enable File Compression = off

- Maximum File Locks = 100000

> **Note** The Maximum File Locks parameter must be set higher than the maximum hot nodes setting in the BorderManager setup in NWADMN32 or the hot nodes setting will not take effect. The maximum hot nodes usable will be about 2/3rds of this value.

- Enable Hardware Write Back = on
- Enable Disk Read After Write Verify = off
- Worker Thread Execute In A Row Count = 15
- Pseudo Preemption Count = 200
- Minimum Service Processes = 500
- Maximum Service Processes = 1000
- New Service Process Wait Time = 0.3 sec

> **Note** NEW SERVICE PROCESS WAIT TIME in Novell NetWare 6.0 SP 3 and beyond is no longer an adjustable SET parameter. The setting is now dynamic and should not cause any issues.

Use The Following NetWare Administrator (NWADMN32) Settings

> **Note** Your server may require customization from these parameters for bets results, but these are good settings to start with.

- Maximum Hot Unreferenced Time = 30
- Cache Hash Table Size = 256
- Maximum Number of Hot Nodes = 50000

> **Note** Remember that this parameter requires you to set the Maximum File Locks setting higher (suggested value is 100,000 locks).

- Number of Directories = 128

> **Note** You should enter a value or 128 times the number of cache volumes configured as the value entered will be divided across all the cache volumes.

Watch Your Memory - Memory Considerations

- Eliminate any NLM's that you don't need.
- Watch the LRU Sitting Time in Monitor – keep it above 15 minutes.
- Use efficient buffer sizes
- Use DOS name space only on the cache volume(s)

Note You cannot remove name spaces from an NSS volume, so don't waste time trying. NetWare 5 automatically creates legacy volumes with LONG name space added, and you have to use VREPAIR to then remove the LONG name space.

The PROXY.CFG File

The PROXY.CFG file, contained in the SYS:\ETC\PROXY directory, is critical to the operation of BorderManager PROXY.NLM. There are a number of basic, required settings read from PROXY.CFG each time PROXY.NLM is loaded into memory.

See Novell TID 10059667.

In addition to the basic, required settings, there have been many optional settings added with various BorderManager patches that modify how the proxies operate. In most cases, the settings allow the HTTP Proxy to work more reliably, increase performance, or connect to a web server that is not RFC-compliant. In addition, the anti-virus patterns used with later versions of PROXY.NLM to protect reverse-proxied web servers are contained within PROXY.CFG.

An example of the PROXY.CFG file I use on my BorderManager servers is shown below. There are many settings in this file that improve the ability of the proxy to work with problem web sites, or improve performance of the HTTP Proxy. This version of PROXY.CFG is for any version of BorderManager 3.x., but the settings a patch-level dependent. Settings that are dependent on patches which you do not have installed on your server should simply be ignored by PROXY.NLM; they should not cause you any problems.

Tip number 63 at my web site http://www.craigjconsulting.com links to a copy of the most current PROXY.CFG file that I use, and discusses some relevant issues with settings.

If you are using Mail Proxy, see the latest patch documentation or the Novell TID referenced above for examples on Mail Proxy settings. It is very important that you configure certain settings for Mail Proxy that match how you want it to work. Your Mail Proxy settings much match your server addresses and domain name.

Craig's PROXY.CFG File, Revision 12

```
; revision 12, Craig Johnson, June 7, 2004
; http://www.craigjconsulting.com
; settings for patched BM 3.7 and 3.8 servers  (Should be fine with earlier
; versions, though some settings will do nothing if the version of proxy
; doesn't support them).
; You can patch BorderManager 3.5 and 3.6 with certain portions
; of BorderManage 3.7 patches - see tip #1 at www.craigjconsulting.com

; See Novell TID 10059667 for documentation on many of these options.

; Depending on your BorderManager version and patch level, many of
; these settings may be at the default values.

[BM Cookie]
BM_Forward_Cookie=0

[HTTP Streaming]
;The line below fixes the HTTP streaming bug,
;but breaks WindowsUpdate, unless using proxy dated 2003 or later.
; You should have persistent connections enabled in NWADMN32, BorderManager
; Setup, HTTP Proxy Details.
ResetOriginServerConnAfterClientReset=1

[TransparentHTTPS]
;Next entry allows later versions of Transparent Proxy to listen on HTTPS/SSL
HTTPSPort1=443

[Object Cache]
cut thru no CLH length=0

[Extra Configuration]
; This entry works only for BorderManager 3.8, enabling Nsure Audit logging for
proxies
; When Nsure audit logging is enabled, you should disable common, extended and
indexed logging
;EnableNsureAuditLogging=1
;
; Next entry (for proxycfg.dll version from Jan 7, 2004 or later) allows
generic
; proxy to use port 25, to replace Mail Proxy
;AllowGTCPProxyToUsePort25=1
;
; Next entry (for proxy version SMTP1, Jan 7, 2004 or later) allows
; a custom banner to be displayed in a SMTP HELO (mail proxy)
;BM_SMTP_Banner="This is a test BM SMTP Banner.Any unauthorized use of this
software would lead to legal action against the user."
;
; This entry (requires BM37FP3D or later to work) is supposed to help proxy
unload cleanly and quickly
ResBadAddressLoopBreak=1
;
; Next entry (from BM37FP3 patch) fixes caching issue with multiple browsers on
one PC
DonotCache4ContEncoding=1
;
; Next entry (from BM37Sp2) attempts to fix problems with proxy not unloading
SCacheDestroyYieldInterval=200
;
; Next entry (from BM37Sp2) fixes problem browsing certain web sites
DoNotSendExtraCRLF = 1
```

```
;
; Next entry (from BM37Sp2) fixes problem browsing certain web sites
EnableIncomplete302ResponseFix = 0
;
; Next entry fixes a potential ABEND in BM37SP1
EnableHTTPSLogging=0
;
; Next entry prevents Macintosh tunneling to bypass rules
AllowHTTPTunneling=0
;
; Next entry fixes Macintosh SSL Proxy authentication problem
new302Redirect=1
;
; Next two entries are for BM37SP1 servers and deal
; with terminal services cookie-based authentication
; Uncomment to use that feature (see patch readme)
;EnableTerminalServerAuthentication=1
;RedirectHTTPSRequest=1
;
DoNotCacheWhenCookieFound=1
;
; If you have a Netmail Server and it has problems with pages not
; loading completely, try commenting out the following line.
PassContentLength=0
;
IgnoreContentLength=1
;
IgnoreContentLengthCheck=1
;
OC_IgnoreContentLengthFlag=1
;
AckWithNoDataOnSYN=1
;
; The following option prevents many abends
IgnoreDuplicateChill=1
;
RestartTimeoutAfterEverySend=1
;
EnableICSPassThruFix=1
;
TurnOffPersistantPassThru=1
;
EnableNoCachePassThru=1
;
TransparentProxySupportsVirtualServers=1
;
DiscardAcceptRanges=1
;
AllowSecond220Respond=1
;
CodeRedWorkAround=1
;
UseSimplifiedErrorPage=0
;
ResolveProxyIPAddress=0
;
ScanVirusPatterns=1
;
; If this is =0, requests without a domain name
; will have the server's domain name appended
DoNotCreateFullyQualifiedHostNames=1
;
HTTPSAuthenticationSwitch=0
```

```
;
; following line should cause proxy to unload
; without saving cache memory to disk
DoNotSaveMemoryCacheDuringUnload=1
;
Line_Terminator=CR
;

; Next sections about 'authentication' are for BM37SP1 or
; later servers and deal with terminal services
; cookie-based authentication
;[Authentication Subnets]
;PrivateSubnet1=10.0.0.0/255.0.0.0
;PrivateSubnet2=10.4.5.100/255.255.252.0
;PrivateSubnet3=164.99.145.98/255.255.252.0

;[Authentication Ranges]
;PrivateRange1=100.25.4.5-100.25.4.60
;PrivateRange2=20.1.1.1-20.4.5.25

;[Authentication Addresses]
;PrivateAddr1=24.0.4.5
;PrivateAddr2=45.3.45.6
;PrivateAddr3=44.5.6.8


; Next sections are for Mail Proxy.
; If you have Mail Proxy in BorderManager 3.8, you
; can use multiple (internal) mail domain support.
; If you have earlier versions, you can only have
; a single mail domain.

; Next Section is for Mail Proxy on BorderManager 3.7 or earlier
;[BM Mail Proxy]
;BM_Domain=yourdomain.com
;BM_Incoming_Relay=0
;BM_Proxy_Domain=servername.yourdomain.com


; Next section is for Mail Proxy on BorderManager 3.8 with
; and multiple domain support. Use your smtp server IP address(es)
; and domain names.
;[Multiple Domain Support]
;MultiDomain1=192.168.10.250/yourdomain.com
;MultiDomain2=192.168.10.250/yourdomain2.com


; The remaining sections are essentially default settings to allow
; BorderManager and its miniwebserver to function correctly.

[Buffer Tracking]
Enable=0

[MiniWeb Server]
Port-Number=1959
Root-Directory=SYS:\ETC\PROXY\DATA

[MiniWeb Server: Mime Types]
Content-Type: text/html=htm,html
Content-Type: text/plain=txt,text,cla,class
Content-Type: image/gif=gif
Content-Type: image/jpeg=jpg,jpeg,jpe,jfif,pjpeg,pjp
Content-Type: image/tiff=tiff,tif
```

```
Content-Type: image/x-xbitmap=xbm
Content-Type: video/x-msvideo=avi
Content-Type: video/quicktime=qt,mov,moov
Content-Type: video/x-mpeg2=mpv2,mp2v
Content-Type: video/mpeg=mpeg,mpg,mpe,mpv,vbs,mpegv
Content-Type: audio/x-pn-realaudio=ra,ram
Content-Type: audio/x-mpeg=mpega,mp2,mpa,abs
Content-Type: audio/x-wav=wav
Content-Type: audio/x-aiff=aif,aiff,aifc
Content-Type: application/x-ns-proxy-autoconfig=pac

[Log Format]
Delimiter-Character=space

; The virus pattern configuration section allows you to have
; the Reverse Proxy block requests with certain patterns
; in the HTML code.  Most of these patterns listed below
; are for Code Red and NIMDA viruses.  The proxy
; can also 'autodetect' viruses and add them to a list.
; See Novell's AppNote on this from Sept. 2002.
;

[Virus Pattern Configuration]
EnablePatternAutoUpdate=1
MaxNoOfVirusPatterns=128
NoOfVirusPatterns=28
PatternSize=16
PatternStartOffset=1
VirusPattern0=scripts/..%252f.
VirusPatternoffset10=0
VirusPatternvalue10=0
VirusPatternoffset20=0
VirusPatternvalue20=0
VirusPatternorigLength0=57
VirusPattern1=scripts/..%c1%1c
VirusPatternoffset11=0
VirusPatternvalue11=0
VirusPatternoffset21=0
VirusPatternvalue21=0
VirusPatternorigLength1=58
VirusPattern2=scripts/..%c0%2f
VirusPatternoffset12=0
VirusPatternvalue12=0
VirusPatternoffset22=0
VirusPatternvalue22=0
VirusPatternorigLength2=58
VirusPattern3=scripts/..%c0%af
VirusPatternoffset13=0
VirusPatternvalue13=0
VirusPatternoffset23=0
VirusPatternvalue23=0
VirusPatternorigLength3=58
VirusPattern4=scripts/..%%35c.
VirusPatternoffset14=0
VirusPatternvalue14=0
VirusPatternoffset24=0
VirusPatternvalue24=0
VirusPatternorigLength4=57
VirusPattern5=scripts/root.exe
VirusPatternoffset15=0
VirusPatternvalue15=0
VirusPatternoffset25=0
VirusPatternvalue25=0
```

```
VirusPatternorigLength5=33
VirusPattern6=MSADC/root.exe?/
VirusPatternoffset16=0
VirusPatternvalue16=0
VirusPatternoffset26=0
VirusPatternvalue26=0
VirusPatternorigLength6=31
VirusPattern7=d/winnt/system32
VirusPatternoffset17=0
VirusPatternvalue17=0
VirusPatternoffset27=0
VirusPatternvalue27=0
VirusPatternorigLength7=41
VirusPattern8=c/winnt/system32
VirusPatternoffset18=0
VirusPatternvalue18=0
VirusPatternoffset28=0
VirusPatternvalue28=0
VirusPatternorigLength8=41
VirusPattern9=_mem_bin/..%255c
VirusPatternoffset19=0
VirusPatternvalue19=0
VirusPatternoffset29=0
VirusPatternvalue29=0
VirusPatternorigLength9=78
VirusPattern10=_vti_bin/..%255c
VirusPatternoffset110=0
VirusPatternvalue110=0
VirusPatternoffset210=0
VirusPatternvalue210=0
VirusPatternorigLength10=78
VirusPattern11=msadc/..%255c../
VirusPatternoffset111=0
VirusPatternvalue111=0
VirusPatternoffset211=0
VirusPatternvalue211=0
VirusPatternorigLength11=106
VirusPattern12=scripts/..%%35%6
VirusPatternoffset112=0
VirusPatternvalue112=0
VirusPatternoffset212=0
VirusPatternvalue212=0
VirusPatternorigLength12=59
VirusPattern13=scripts/..%25%35%
VirusPatternoffset113=0
VirusPatternvalue113=0
VirusPatternoffset213=0
VirusPatternvalue213=0
VirusPatternorigLength13=61
VirusPattern14=scripts/..%255c..
VirusPatternoffset114=0
VirusPatternvalue114=0
VirusPatternoffset214=0
VirusPatternvalue214=0
VirusPatternorigLength14=57
VirusPattern15=scripts/..%c1%9c.
VirusPatternoffset115=0
VirusPatternvalue115=0
VirusPatternoffset215=0
VirusPatternvalue215=0
VirusPatternorigLength15=58
VirusPattern16=scripts/root.exe
VirusPatternoffset116=0
```

```
VirusPatternvalue116=0
VirusPatternoffset216=0
VirusPatternvalue216=0
VirusPatternorigLength16=81
VirusPattern17=scripts/httpodbc
VirusPatternoffset117=0
VirusPatternvalue117=0
VirusPatternoffset217=0
VirusPatternvalue217=0
VirusPatternorigLength17=30
VirusPattern18=MSADC/root.exe?/
VirusPatternoffset118=0
VirusPatternvalue118=0
VirusPatternoffset218=0
VirusPatternvalue218=0
VirusPatternorigLength18=79
VirusPattern19=MSADC/httpodbc.d
VirusPatternoffset119=0
VirusPatternvalue119=0
VirusPatternoffset219=0
VirusPatternvalue219=0
VirusPatternorigLength19=28
VirusPattern20="c/httpodbc.dll H"
VirusPatternoffset120=0
VirusPatternvalue120=0
VirusPatternoffset220=0
VirusPatternvalue220=0
VirusPatternorigLength20=24
VirusPattern21=d/winnt/system32
VirusPatternoffset121=0
VirusPatternvalue121=0
VirusPatternoffset221=0
VirusPatternvalue221=0
VirusPatternorigLength21=92
VirusPattern22="d/httpodbc.dll H"
VirusPatternoffset122=0
VirusPatternvalue122=0
VirusPatternoffset222=0
VirusPatternvalue222=0
VirusPatternorigLength22=24
VirusPattern23=scripts/..%255c.
VirusPatternoffset123=0
VirusPatternvalue123=0
VirusPatternoffset223=0
VirusPatternvalue223=0
VirusPatternorigLength23=108
VirusPattern24=scripts/.%255c..
VirusPatternoffset124=0
VirusPatternvalue124=0
VirusPatternoffset224=0
VirusPatternvalue224=0
VirusPatternorigLength24=39
VirusPattern25=scripts/..%252f.
VirusPatternoffset125=0
VirusPatternvalue125=0
VirusPatternoffset225=0
VirusPatternvalue225=0
VirusPatternorigLength25=116
VirusPattern26=scripts/..%252f.
VirusPatternoffset126=0
VirusPatternvalue126=0
VirusPatternoffset226=0
VirusPatternvalue226=0
```

```
VirusPatternorigLength26=39
VirusPattern27=default.ida?XXXX
VirusPatternoffset127=0
VirusPatternvalue127=0
VirusPatternoffset227=0
VirusPatternvalue227=0
VirusPatternorigLength27=385
```

Chapter 33 - Odds & Ends

Documenting Your Server

It is very important to document a server in any case, and BorderManager servers are no exception. Unfortunately, with BorderManager there are some features that do not lend themselves to documentation as well as they should. In particular, that means packet filter exceptions and access rules.

My suggestions for thoroughly documenting a BorderManager server include:

Run TECHWALK.NLM

This software produces a text file that is quite comprehensive in documenting many settings. The output of this file can be found in SYS:\ETC\TECHWALK.OUT.

Run CONFIG.NLM

This program is essential to use on any Novell server, and is a good starting point. CONFIG.NLM will produce a text file containing a wealth of information on the server hardware and software in use, as well as listing all the NCF files (including AUTOEXEC.NCF and STARTUP.NCF from the DOS partition), and error logs.

Download the latest version of CONFIG.NLM from the Minimum Patch List at http://support.novell.com.

Use the following command syntax to launch CONFIG.NLM.

LOAD CONFIG /S

Note You must use the LOAD command syntax on NetWare 5.x servers because you will otherwise run the internal CONFIG command and not the NLM. Alternative: Type CONFIG.NLM instead of CONFIG.

This command will produce a file called CONFIG.TXT in the SYS:\SYSTEM directory. The /S option will include SET parameters in the output.

There are other command line options available. LOAD CONFIG /? Will run CONFIG, and also show the options. Currently, those options are
/S – include the SET parameters

/A – append the current information to any existing SYS:\SYSTEM\CONFIG.TXT file.

/D – include a file listing of SYS:\SYSTEM and the local drive

Once you have run CONFIG.NLM, I strongly recommend you copy the resulting config.txt file to another computer, and store it in a directory created from the current date. That way you will be able to access the configuration data if the server is down, and you will be able to easily keep a series of config.txt files stored by date.

Run CONFIG.NLM before and after every change you make to the system files or set parameters, such as installing new software and service packs. The config.txt file can be invaluable in troubleshooting problems, or restoring a server to a previous working state.

There is also a program called Config Reader, available from the minimum patch list at http://support.novell.com which will do some analysis of the config.txt files. Config Reader also has a useful feature of being able to compare two config.txt files and show you the differences. Config Reader runs on a Windows PC, and not on the server.

CONFIG.NLM should run on NetWare 3.11 (at least) and later. I have used it for years and never had a problem, but be aware that there is always some small risk to loading a new NLM on a server.

Caution! *The output from CONFIG.NLM includes the serial number of the server, and can show the RCONSOLE password in the NETINFO.CFG data. If you plan on posting the config.txt file (in the Novell Support Connection public forums for troubleshooting perhaps), be sure to edit out this information first!*

Save Basic BorderManager Settings to a File with CFGDUMP

BorderManager 3.8 ships with a handy little utility file called CFGDUMP.NLM. This file is also available in an Unsupported directory on some BorderManager 3.7 patches. Look in the Unsupported directory on the BorderManager 3.8 product CD. You can use this utility for at least BorderManager 3.6 or later, and probably 3.5. (I did not test it with a version earlier than 3.6). Copy the file to SYS:SYSTEM, unload proxy, and then LOAD

CFGDUMP. You will get a CFGDUMP.TXT file in the SYS:ETC\PROXY directory with many pertinent BorderManager settings recorded there.

Comment Your Filter Exceptions

When you create your own packet filter exceptions, you have the option of inserting a short one-line comment. ALWAYS comment your packet filter exceptions, with at least some explanation of what the exception is intended for. If you are concise, this documentation is almost adequate. FILTCFG.NLM has an option to save the packet filters to a text file, and that option is definitely inadequate as it does not save ALL the information about the packet filter exceptions. I recommend the following two steps:

1. Copy the SYS:\ETC\FILTERS.CFG file to another computer. This file contains all the packet filters and packet filter exceptions, and is a good backup. In case you need to recreate all the packet filter exceptions, it is as simple as unloading IPFLT.NLM, copying this file back, and loading IPFLT again. (Frankly, it is a good idea to copy ALL the files in SYS:\ETC to another computer for backup).

2. Create a spreadsheet (or table in a word processor) that lists the following information, and fill it in for every packet filter exception, including the default exceptions. You can be more descriptive about the exceptions here since you are not limited to a single line of text.

   Source & destination interfaces, source & destination IP addresses, source & destination port numbers, protocol, stateful or non-stateful, and comments.

Screenshot your VPNCFG Screens

Using RCONSOLE, you can LOAD VPNCFG and at least take a screen shot of the Display VPN Server Configuration Information screen, if you have set up any kind of VPN on the BorderManager server.

Screenshot your INETCFG Settings

Using RCONSOLE, consider taking screenshots of the pertinent INETCFG settings. If you have run CONFIG.NLM, this step is optional as the config.txt file will have all the INETCFG information as well.

Screenshot your NWADMN32 Screens

CONFIG.NLM will not record NDS properties, and virtually all of the BorderManager settings are stored as NDS attributes of the server object. The best way I know of to document these settings is to create a document that includes screen shots of every BorderManager configuration menu, including at least a small explanation of the options chosen. (Much like this book). It is adequate to include only the options that have been changed from the default settings.

Once you get through the NWADMN32 menus, import the packet filtering documentation, screenshots of the VPNCFG and INETCFG information, and config.txt files as well.

Although documentation like this will generally amount to some 200 pages or so, it really doesn't take all that long to do, if you do not include much explanation on the menu options.

Back Up Your Access Rules

Select Access Rules, copy them to the clipboard, and use Clipboard Viewer to save the rules to a .CLP file. In Win9x, you may have to install Clipboard Viewer as an optional Windows program – it will show up in the Accessories menu. In Windows 2000 and XP, it should be present in the SYSTEM32 directory as clipbrd.exe. See the example in the Access Rules chapter.

In some of the later BorderManager patches, there is an unsupported tool called ACLDUMP.NLM. Copy this module to SYS:SYSTEM, and load it on the server. It will create a text file call ACL_RULE.TXT in the SYS:\ETC\PROXY directory which contains access rule entries, though in a format that is not very readable.

Miscellaneous Hints

This section contains several hints taken from the BorderManager public forums.

Note I have not personally verified the accuracy of all of this information

PPTP to BorderManager 3.5

Question: I need to tunnel IPX over IP using the PPTP protocol in BM. I'm new to MB and wonder what elements to set up from BM to do this. What is the easiest way? I don't need any other things like proxy or so, just PPTP.

Answer: See Novell TID 2932055 for step-by-step instructions.

Converting Browser Proxy Settings Automatically

Because of the various issues and deficiencies of the Transparent Proxy, it is often used only as an interim step to maintain Internet web browsing access while the workstations are converted to use the HTTP Proxy. Some companies prefer to publish a set of instructions and have the users reconfigure their browsers for the HTTP proxy. Others send help desk personnel around to configure the browsers for the users. Still others automate the process using login script commands or ZENworks applications. The following section shows some possible ways to configure the browser without human intervention.

Internet Explorer

If you want to set Internet Explorer proxy settings without having to go visit every workstation, there are various methods that will work. I describe a number of methods at my web site tip #71 (http://www.craigjconsulting.com), and I have some sample files there.

Push Registry Change In Login Script

The option I use most often is to force a registry command in the login script, using a .REG file and the REGEDIT /S command. The syntax for this is shown below.

These settings have worked for me on Windows XP, but I do not guarantee they will work on all versions of Windows.

LOGIN SCRIPT – In the login script, you need to call out the REGEDIT command and point to the location of the .REG file. That file should be in the Public directory of a mapped drive letter. The example here assumes you have mapped the H: drive to the SYS: volume of a server holding the file.

```
REGEDIT /S PROXY.REG
```

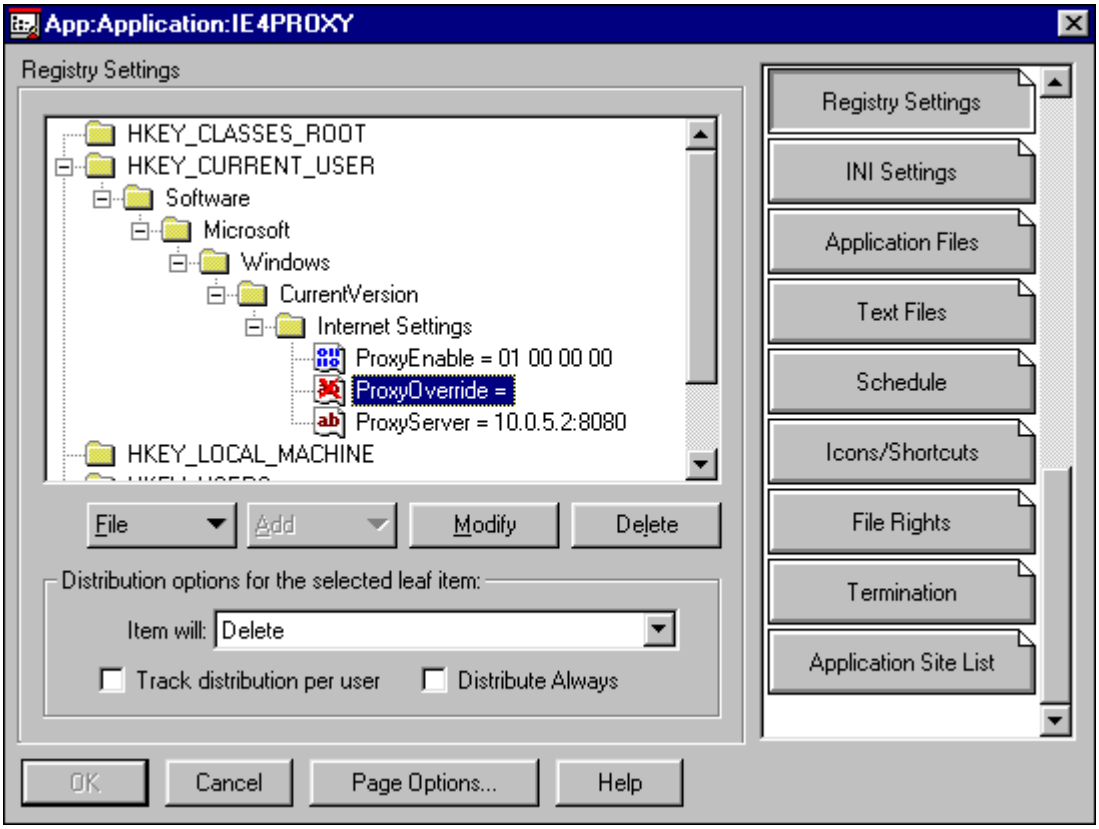
The PROXY.REG file itself is:

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings]
"ProxyServer"="<your proxy IP address>:8080"
"ProxyEnable"=dword:00000001
"ProxyOverride"="<local>"
```

Change <your proxy IP address> to the private IP address of your HTTP Proxy, and <local> to 127.0.0.1 or any combination of URL's for which you want to bypass the proxy. (I advise you to experiment with this for a while to get the syntax done correctly).

Push Registry Change in ZENWorks Application



The screenshot shown above shows a ZENworks application object setting for changing Internet Explorer 4.0 to use an HTTP Proxy at IP address 10.0.5.2, using TCP port 8080.

Netscape

See the AppNote by Anders Gustafsson at this URL:

http://developer.novell.com/research/appnotes/1999/february/02/

See also the notes on using a PROXY.PAC file in the Miscellaneous chapter later in this book.

I have also put up a tip at my web site http://www.craigjconsulting.com covering several methods for setting the browsers up to use HTTP proxy.

VPN & Modems Tip

You must disable or at least release all the IP addresses from your LAN card if you want to be able to use the VPN through the modem.

VPN Client with LAN Connection

Question: I have my Client-to Site VPN working beautifully, in all my workstation configurations, but I need a bit of advise/knowledge with a small problem

Some of my mobile users have a Xircom adapter which has the modem and the network connector on it. In order to get the VPN working I have to run "IPCONFIG /RELEASE" to drop the IP address on the network card.

What I want to know is if there is a way to do this thru API before running the Dial VPN. We would like to be able to have a single icon on the desktop to start the VPN. Can we do this via Visual Basic or something like that?

Answer 1: Here is a work-around.

- Create a batch file which runs "IPCONFIG /RELEASE" followed by the VPNLOGIN.EXE.
- Remove the shortcut on the desktop put there by the VPN install and replaced it with a shortcut to the batch file, changing the icon to be the one for VPN Client.

Answer 2: In the VPN login screen you can specify an 'Application to Launch'. Just add:

Win95/98 PCs: 'c:\windows\winipcfg /release_all'

or

WinNT4/2k/XP PCs: 'c:\winnt\system32\ipconfig /release nic'.

VPN with Client 4.7x for NT

To get our Client-to-Site VPN working, I had to do the following:

1. Use an older version (4.60.202) of the NetWare client, instead of the newer 4.71 version. The Novell support person I've been working with was unable to get into our VPN server using the 4.71 client, but was able to get in with the older client, and therefore concluded that the 4.71 client has a bug that breaks the VPN client. I didn't go back and try using the newer client again after solving problems 2, 3 & 4 though, so I can't confirm that the 4.71 client won't work.
2. Contrary to the BM3VPD08 readme file, which clearly states that the NetWare client should be installed first and the VPN client installed second, I found that installing the two clients in that order did not allow the VPN to work. However, installing them in the opposite order (VPN client first, NetWare client second) did allow a successful VPN connection.
3. Use an older version of the NT Service Pack. The SP4 or SP5 patches allowed the VPN to work, but SP6a would break it.

4. Use a different client PC with NT freshly installed. The VPN works fine on a fresh PC, but still doesn't work on an employee's original PC. The original PC has had a lot of software installed, upgraded, and removed in the several years that it's been in use, so who knows what is breaking the VPN on it.

Citrix Setting for NAT

If you are using Static NAT to access an internal Citrix server, you will have to set up an alt address in the Citrix box so it can tell the client what address to reply to. This is set up at the Citrix box with the command:

```
altaddr /set xxx.xxx.xxx.xxx
```

Where xx.xx.xx.xx is the public IP address on the BorderManager server. Then you will have to configure the client "use alternate address on firewall" from the firewall button on the connection page in settings.

HOSTS File Tip

There appears to be a bug in how PROXY.NLM reads the SYS:\ETC\HOSTS file. The last line needs to be blank and not be an entry otherwise that entry is ignored. So add a return after the last line and see if it works once the proxy rereads SYS:\ETC\HOSTS. Proxy checks the file on a regular basis and will reload it.

Load Balancing Internal Web Servers

If you define more than one web server as the origin server for your reverse proxy, it does appear that the BM server will load balance across those two servers. I did just that, added two web servers in as the origin servers, saved the changes, then took option 17 from the Proxy Console screen, and sure enough, it said "Load balancing cache fills from xx.xx.xx.xx".

Note I wonder how useful this actually is, since the static cache content still comes only from the one BorderManager server.

SSL Logout Page Location

The BMEE35 SSL Proxy Authentication logout page is:

http://172.16.30.14:1959/cmd/BM-Logout

Where the IP address is the address of the BorderManager server.

You can point your browser to this location and clear your proxy authentication. This can be useful when testing proxy authentication changes, particularly when setting up SSL Proxy Authentication. (Run DWNTRUST to stop CLNTRUST first).

St. Bernard Software / Open File Manager – Don't Use On BorderManager

St. Bernard's Open File Manager software will cause problems on a BorderManager server, particularly if used on cache volumes. Do not use this software on a BorderManager server.

The same problems might occur with any of the other variations of open file manager backup software. You should beware of any open file agent software running on a BorderManager server. Such programs might have file names like OFA or OFM.

Setting Browser Proxy Settings

There are a number of ways to set a browser to use the HTTP Proxy. There is an AppNote by Novell that discusses a number of methods. See the April 2002 AppNotes at http://developer.novell.com.

- You can manually go to each PC and configure the settings.
- You can produce instructions and have the users change their own settings. (This works amazingly well, do don't discount this approach).
- You can use ZENworks to push the browser settings via a Forced-Run application.
- For Internet Explorer, you can push the changes to the users in a login script, by running REGEDIT.EXE /S SETPROXY.REG, when SETPROXY.REG is an exported registry setting containing the proper proxy settings. Here is an example

```
#REGEDIT /S Z:\PUBLIC\SETPROXY.REG

where SETPROXY.REG is a text file containing the following case-sensitive entries:

REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings]
"ProxyEnable"=dword:00000001
"ProxyServer"="192.168.10.252:8080"
```

- You can use an autoconfiguration (PROXY.PAC) file, launched from a web server, the BorderManager mini-web

server, or a local file. (The problem here is that you have to configure the browser for this setting to start with).

- You can use an administrator's toolkit for either Internet Explorer or Netscape to produce a configuration file that you then force down to the desktop in the proper directory. For Internet Explorer, search the Microsoft web site for information on the IEAK (Internet Explorer Administration Kit). For Netscape, search for Client Customization Kits at the Netscape web site. Netscape has different kits for different versions of Netscape.
- You can use DHCP to force the proxy settings. See Novell TID 2953490 and some helpful Microsoft instructions at http://www.microsoft.com/TechNet/IE/reskit/ie5/part3/ch13sser.asp

Using an Autoconfiguration Program to Set Proxy Settings

A common way to set the browser proxy settings is by use of a PROXY.PAC file. There are numerous examples of such files on the Internet, and they can be quite flexible, and quite complex. The idea is to point the browser to the appropriate .PAC file, which is usually available via a web server, and the .PAC file tells the browser when to use a proxy server. Two examples are shown below.

Serving up the PROXY.PAC File from BorderManager

Use the BorderManager mini web server to deliver the PROXY.PAC file. Place the PROXY.PAC file in the SYS:\ETC\PROXY\DATA directory. Set the browser autoconfig setting to

http://myserver.domain.com:1959/data/PROXY.PAC

Serving up the PROXY.PAC File as a Local File

You can copy a PROXY.PAC file to the local PC and launch it from there. This is useful if you have a laptop that moves from one LAN to another, where one LAN has no proxy and the other LAN does. The appropriate PROXY.PAC file can instruct the browser to use a proxy only when on a certain TCP/IP subnet.

The syntax for launching PROXY.PAC from a local file is different between Internet Explorer and Netscape. Here are the settings I use, for IE 6.0 and Netscape 4.79.

Internet Explorer: **file://c:/windows/proxy.pac**

Netscape: **file:///c|/windows/proxy.pac**

Simple PROXY.PAC Example

This is the simplest configuration example I can think of, but also one for which there seem to be no examples on the Internet, outside of my web site. In this example, the PROXY.PAC file tests to see if the PC has an address on a certain subnet, and if so, sets the browser to use a proxy server. If the PC is NOT on that subnet, the browser will not use a proxy server. This example is useful to run as a local file on laptops that travel between a LAN with a proxy server and one without a proxy server.

```
function FindProxyForURL(url, host)
{
 if (isInNet(myIpAddress(), "192.168.1.0",
"255.255.255.0"))
 return "PROXY 192.168.1.1:8080";
 else
 return "DIRECT";
}
```

Change the 192.168.1.0 to your IP subnet, with appropriate mask, and change the 192.168.1.1:8080 to your BorderManager HTTP Proxy address and port number.

More Complex PROXY.PAC Version

I have had a number of occasions where I needed to bypass the http proxy for a particular web site. This is easily done with a PROXY.PAC file, by putting in an IF statement with the proper syntax. (You can have lots of IF statements if you want to do this for multiple web sites.)

Here is an example that bypasses proxy for a particular web site (principia.mo.techpaths.com) that was giving grief when going to it through the HTTP Proxy:

```
function FindProxyForURL(url, host)
{
if (shExpMatch(url, "http://principia.mo.techpaths.com*")) {
    return "DIRECT";
    }
 if (isInNet(myIpAddress(), "192.168.1.0", "255.255.255.0"))
  return "PROXY 192.168.1.1:8080";
  else
  return "DIRECT";
}
```

Using PROXY.PAC to Bypass Proxy for Multiple URL's

In the following example, several URL's are configured to be accessed by a browser without going through the proxy. Variables are used for the proxy address or for bypassing the proxy, and it is easy to add more URL's to this example, or set up a second proxy address as a variable for some of the URL's.

```
function FindProxyForURL(url, host)
{
// variable strings to return
var proxy_yes = "PROXY 192.168.1.1:8080";
var proxy_no = "DIRECT";

if (shExpMatch(url, "http://www.mycompanywebsite.com*")) { return proxy_no; }
if (shExpMatch(url, "http://www.myotherwebsite.com*")) { return proxy_no; }
if (shExpMatch(url, "http://www.my3rdlocalsite.com*")) { return proxy_no; }
if (shExpMatch(url, "http://192.168.1.100*")) { return proxy_no; }
// Proxy if PC is on local LAN
if (isInNet(myIpAddress(), "192.168.1.0", "255.255.255.0"))
  return proxy_yes;
  else
  return proxy_no;
}
```

Round-Robin PROXY.PAC Example

(Thanks to Shaun Pond for providing this sample).

Put the following java into a text file called "PROXY.PAC" or BROWSERCONFIG.PAC" (or whatever)

Put the file in the BorderManager server under SYS:\ETC\PROXY\DATA directory.

Set your autoconfigure setting in Internet Explorer or Netscape to **http://proxy.internal.com:1959/data/browserconfig.pac**

Change all addresses and domain names to match your internal structure.

The 10. address allows browsing to direct internal addresses (use your own addressing scheme here!)

Set your internal DNS to round robin "proxy.internal.com" to the two internal addresses if you want to share use between two servers cheaply, otherwise amend the script accordingly to just one proxy server.

```
function FindProxyForURL(url, host)
{
 // Direct connections to local domain
 if (isPlainHostName(host) ||
     dnsDomainIs(host, ".internal1.com") ||
     dnsDomainIs(host, ".internal2.com") ||
     dnsDomainIs(host, ".somewhereelse.co.uk") ||
     dnsDomainIs(host, ".playdomain.uk") ||
     dnsDomainIs(host, "127.0.0.1") ||
     dnsDomainIs(host, "10.") ||
     dnsDomainIs(host, ".nothere.int"))
     return "DIRECT";
 // Otherwise use proxy
 else
 return "PROXY 10.119.208.11:8080; " +
        "PROXY 10.119.208.10:8080";
}
```

BorderManager and NetWare Cluster Services

Some explanation provided courtesy of Evan Mintzer and Michael Prentice. See also a Novell AppNote I helped to write from September 2003, at the following URL:

http://developer.novell.com/research/appnotes/2003/septembe/03/a030903.htm

Natively, BorderManager is not truly clusterable. However, it is possible to have BorderManager services running in a cluster. This will give the administrator fault tolerance to both hardware and software problems.

NetWare Cluster Services (NWCS) is a product by Novell that allows from two to thirty-two servers to share applications. This sharing is setup in such a way that if one server goes down the rest of the servers pick up the applications that were running on that server so it is transparent to the users.

Here are some definitions for NetWare Cluster Services:

Cluster – The entire package of servers, shared drives, and software.

Node – Each server that takes part in a cluster.

Resource – An application that takes part in a cluster. A resource is transferable between nodes.

Script – It is analogous to an NCF file for a resource. A Load Script is used to activate the resource while an Unload Script deactivates it. Both are used when migrating (transferring) the resource to another node.

For a resource to be truly clusterable it has to be loaded by an NWCS script and fail over to other nodes without intervention. Within BorderManager, only proxy services are truly clusterable, however, there are ways to fail over some of the other BorderManager services.

Even though proxy is clusterable, it is not clusterable in an active-active cluster. This means that you cannot run proxies on both servers so that you get a load balancing solution. Also, to fail over your BorderManager logs and cache, an NSS external shared storage subsystem is needed.

Note If you don't mind losing your build up of cache and storing the HTTP logs of both servers independently, then it isn't necessary to configure the BorderManager resource to use a shared storage subsystem. The benefits of this include; faster cache performance (NSS volumes are about 30% slower than Netware Partitions), and a large savings in money. Saving the HTTP logs on each server's separate volumes is not an issue as some log analysis programs can easily coalesce multiple logs into one report for you.

Dynamic NAT is easy to run on all nodes – simply turn it on. However, static NAT is a little different. Since there are two parts to creating static NAT, it is possible to fail it over. First, configure your static NAT in INETCFG on all nodes. Normally, you would type **ADD SECONDARY IPADDRESS x.x.x.x** (x.x.x.x being the public IP address to be added) at the command prompt, or in the AUTOEXEC.NCF file, to activate it. Instead, create a script that has that line to load all the secondary public IP addresses and **DEL SECONDARY IPADDRESS x.x.x.x** to unload them. This will allow your static NAT to easily transfer to other nodes. Deleting the secondary IP addresses on one node during a failover will allow you to more easily do maintenance on it while the both nodes are running.

Since your firewall is the boundary between the Internet and your network, you would usually want to point all your internal devices to it as a default gateway. Which server becomes your default gateway in a cluster? Simply create a secondary private IP address that is your default gateway. Create a script similar to your static NAT script and your default gateway will fail over as well.

Firewall services are used to filter external traffic from your network. All nodes in your cluster are firewalls since they are all connected to the Internet. When making changes on one firewall, make sure you make the same changes on the others. When making multiple changes you can simply copy the SYS:\ETC\FILTERS.CFG file to the other nodes. Just remember to change the public and private IP addresses of the BorderManager server in the file before activating the other nodes.

You can avoid having to manually edit the FILTERS.CFG file between copying it to each server in a two-node setup by carefully making use of IP subnetting as follows:

Configure your primary server node with even numbered IP addresses such as Private=10.1.1.2 and Public=4.1.1.2. Configure your secondary node with the next IP address number in sequence (Primary=10.1.1.3 Public=4.1.1.3). Once you do this, on your primary node, change each of the packet filter exceptions that are based on the IP address of the server to a network address, using a mask of 255.255.255.254. That subnet mask will only allow for two valid IP addresses within the subnet range, and will be valid for both nodes. Be sure you understand subnet addressing well before using this technique. Copy the FILTERS.CFG file to the secondary node and it should work for that server also.

Example (Using the above IP addresses)

Change the following default packet filter exception:

```
Source Interface :      Public
Destination Interface:  Public
Packet Type:            ANY (IP)
Source Addr Type:       Host
Src IP Address:         4.1.1.2
Dest Addr Type:         Any Address
```

To:

```
Source Interface :      Public
Destination Interface:  Public
Packet Type:            ANY (IP)
Source Addr Type:       Network
Src IP Address:         4.1.1.2/255.255.255.254
Dest Addr Type:         Any Address
```

Note The 255.255.255.254 subnet mask discussed above is not an error – it works for the filtering module to limit the filter exception to two valid addresses. Using that subnet mask would not work for IP address assignment, but it works fine for restricting filter exception addresses.

Common Log File Format

The Common Log file is stored in the following format:

Field	Example
IP Address	10.1.1.2
Authenticated User Name	.admin.acme
Date	03/Aug/1999
Time	12:07:41
Timezone	+0000
HTTP Request	GET
URL	http://support.novell.com/images/support_nav_bar.gif
HTTP Version	HTTP/1.0
Completion Code	200
File Size	3264

IP Address

This is the private IP address used by the client accessing the BorderManager server.

Authenticated User Name

The name of the user accessing the BorderManager server including the user's common name (CN) and full context. This will only be present if the user authenticates by SSO or SSL.

Date

The date on which the request was made.

Time

The (local) time of day at which the request was made.

Timezone

The timezone on the server at which the request was made.

HTTP Request

HTTP requests commonly seen in logs are :

HTTP Request	Meaning
GET	Read a page or entity within a page
HEAD	Obtain the header information for a page
POST	Submit the results of a form

See RFC 1945 (HTTP 1.0) and RFC 2616 (HTTP 1.1) for information about the full set of requests supported by the HTTP protocol.

URL

The URL of the site being accessed including the domain name and the full path within the site.

Status Code

The HTTP status code is defined as one of the following, according to the HTTP 1.0 standard:

HTTP Status Code	Meaning
200	OK
201	Created
202	Accepted
301	Moved Permanently
302	Moved Temporarily
304	Not Modified
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error
501	Not Implemented
502	Bad Gateway
503	Service Unavailable

For HTTP 1.1 the following status codes are recognized:

HTTP Status Code	Meaning
100	Continue
101	Switching Protocols
200	OK
201	Created
202	Accepted
203	Non-Authoritative Information
204	No Content
205	Reset Content
206	Partial Content
300	Multiple Choices
301	Moved Permanently
302	Found
303	See Other
304	Not Modified
305	Use Proxy
306	Unused
307	Temporary Redirect
400	Bad Request

401	Unauthorized
402	Payment Required
403	Forbidden
404	Not Found
405	Method Not Allowed
406	Not Acceptable
407	Proxy Authentication Required
408	Request Timeout
409	Conflict
410	Gone
411	Length Required
412	Precondition Failed
413	Request Entity Too Long
414	Request-URI Too Long
415	Unsupported Media Type
416	Requested Range Not Satisfiable
417	Expectation Failed
500	Internal Server Error
501	Not Implemented
502	Bad Gateway
503	Service Unavailable
504	Gateway Timeout
505	HTTP Version Not Supported

See RFC 1945 (HTTP 1.0) and RFC 2616 (HTTP 1.1) for the full definitions of the HTTP protocol standards. These documents can be found at http://www.w3.org/Protocols/. For further information about the Common Log format, see http://www.w3.org/Daemon/User/Config/Logging.html

This brief log excerpt shows activity for two users, using IP addresses 10.1.1.4 and 10.1.1.2. The user at IP address 10.1.1.4 was authenticated as john.sales.acme and has accessed http://www.altavista.com/ while the user at IP address 10.1.1.2 was authenticated as .admin.acme and has accessed http://support.novell.com/.

The Common Log File Format information is from an as yet unpublished article by Marcus Williamson, 'Understanding BorderManager Logging.

Chapter 34 - iManager 2.0

This chapter is intended to provide details on installing and configuring iManager 2.0 on Windows for the purpose of configuring BorderManager 3.8 VPN services.

Background Information

IManager 2.0 for Windows is included on the BorderManager 3.8 Companion CD for the sole purpose of configuring the new BorderManager 3.8 VPN services on NetWare 5.1 or 6.0 servers. NetWare 6.5 ships with iManager 2.0, and the BorderManager 3.8 installation gives you the option to install the VPN snapins for it.

If you do not have access to a NetWare 6.5 server, you will need to install iManager 2.0 on a Windows PC (or server), configure it to access a NetWare server, and add the VPN snapins.

Note IManager 2.0.1 is also available to be installed on NetWare 6.0 servers. However, there are dependencies on newer Java code that require a major upgrade to Java on NetWare 6.0. The newer Java will cause many older Java applications on the server to fail, and I do not recommend trying to install iManager 2.0 on a NetWare 6.0 server unless you have thoroughly tested it on a non-production server first! This chapter only shows an iManager installation on Windows.

IManager 2.0 uses LDAP to authenticate to a NetWare server, and read and write VPN configuration to NDS. The iManager server does not have to be in the same NDS tree as the server being configured. Indeed, a Windows PC installation of iManager is not in a tree at all.

On the NetWare server, you may need to enable Clear Text Passwords in the LDAP Group object for the server.

The iManager 2.0 installation for Windows will install Apache2 and Tomcat services to Windows 2000 or XP. Once installed, these services may need to be stopped and restarted to pick up configuration changes. The software will be found in the C:\Program Files\Novell subdirectory.

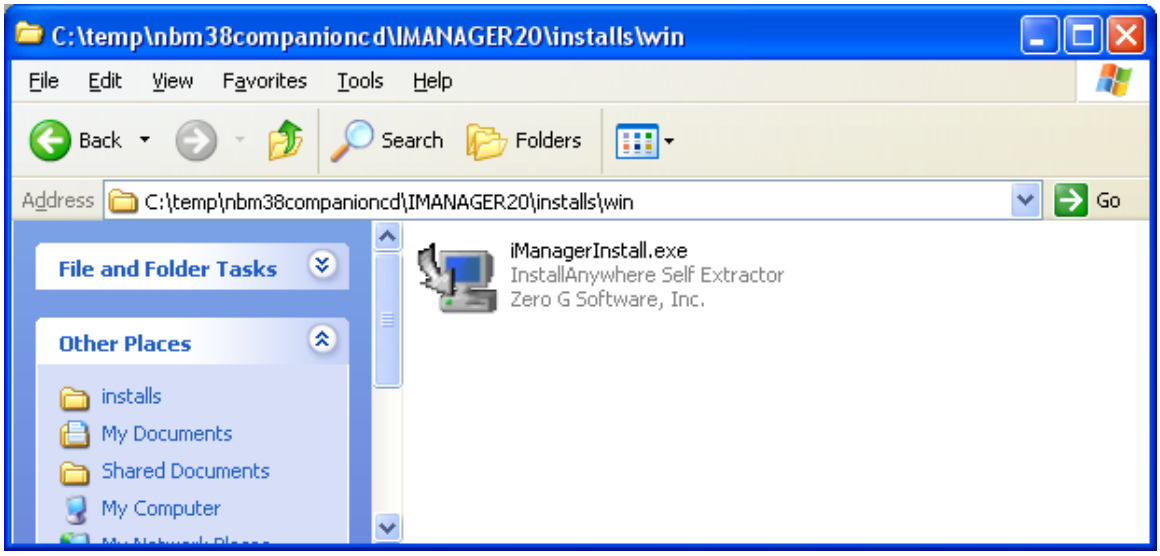
Install iManager Components

This documentation assumes that you already have a Sun version of JAVA installed on a Windows XP PC. However, the iManager installation will install a working version of JAVA for you, should a suitable JAVA version not be installed already.

Start by installing the Windows iManager components, which are supplied on the BorderManager 3.8 companion CD. You will generally want to have LDAP clear text passwords enabled on a NetWare server that you intend to use for communicating to the network via iManager. That server should be one that is intended to be in place for a while (not a temporary server), and it should be the BorderManager 3.8 server, since you are installing iManager here primarily to configure VPN services on that server.

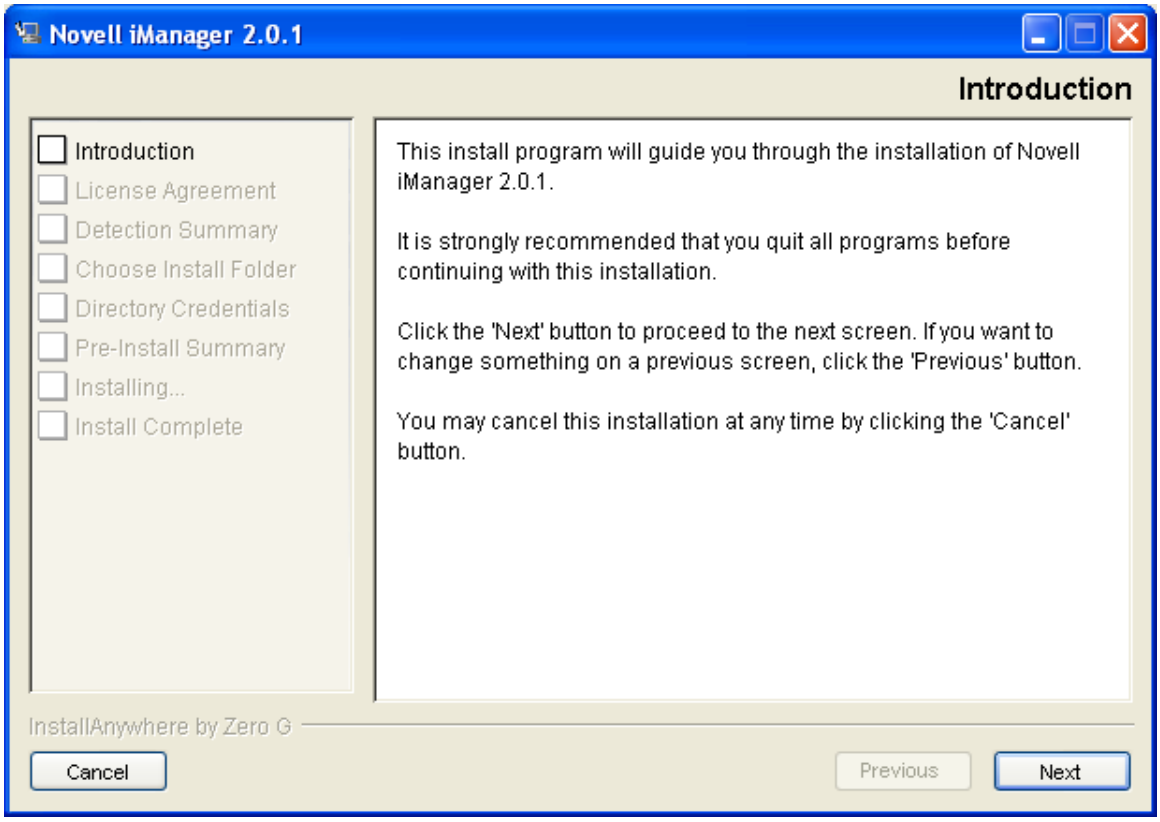
In the Companion CD, you should find a directory called IMANAGER20. Within that directory, you should find a directory called INSTALLS. Within the INSTALLS directory, there are directories containing the Windows version (WIN) and a NetWare 6.0 version (NW6) of iManager 2.0. These instructions show the procedure for installing iManager on Windows, in order to configure a Novell network.

From the Windows 2000 or XP client to be used for iManager, insert the Companion CD, or map a drive letter to a location where the Companion CD has been copied to a server.



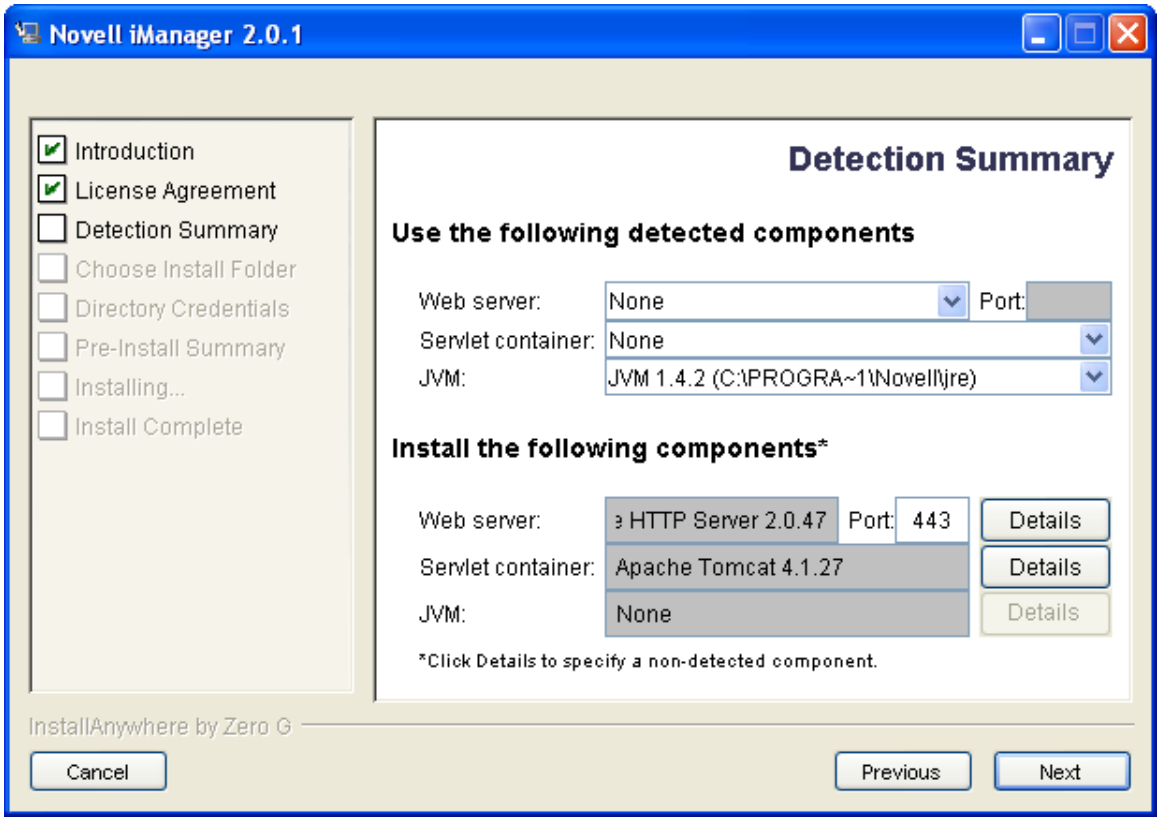
Go to the \IMANAGER\INSTALLS\WIN directory, and launch the program iManagerInstall.exe on a Windows 2000 or Windows XP PC.

When the installation routine gets to the iManager splash screen, select the desired language and click on the **OK** button.



At the Introduction menu, click **Next**.

At the Novell Software License Agreement menu, Select the **radio button to accept the terms** of the license, and click **Next**.



In a new installation, the installation routine should not detect any previously installed components. It should then suggest installing the following components:

Web Server: HTTP Server 2.0.46, using port 443

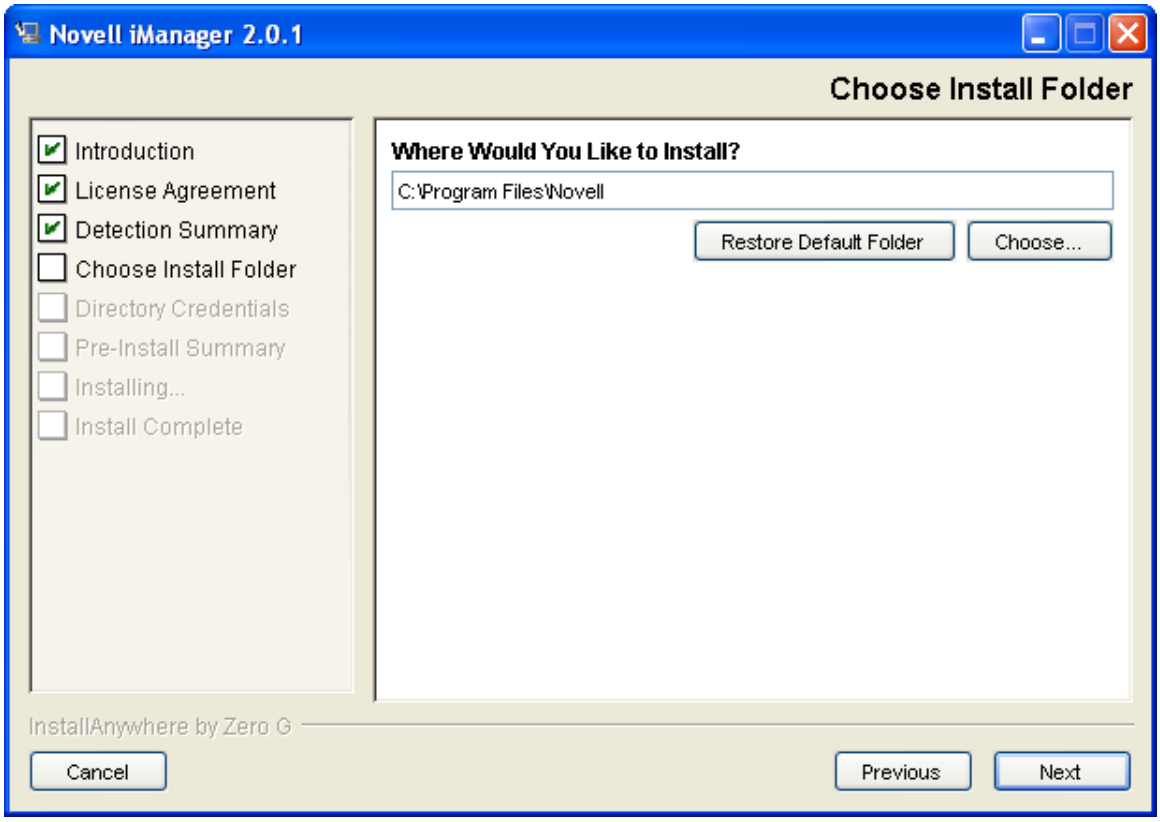
Servlet Container: Apache Tomcat 4.1.24

JVM: Sun JRE 1.4.2

The installation routine checks to see if you have required components already installed on your PC, and will install what is missing.

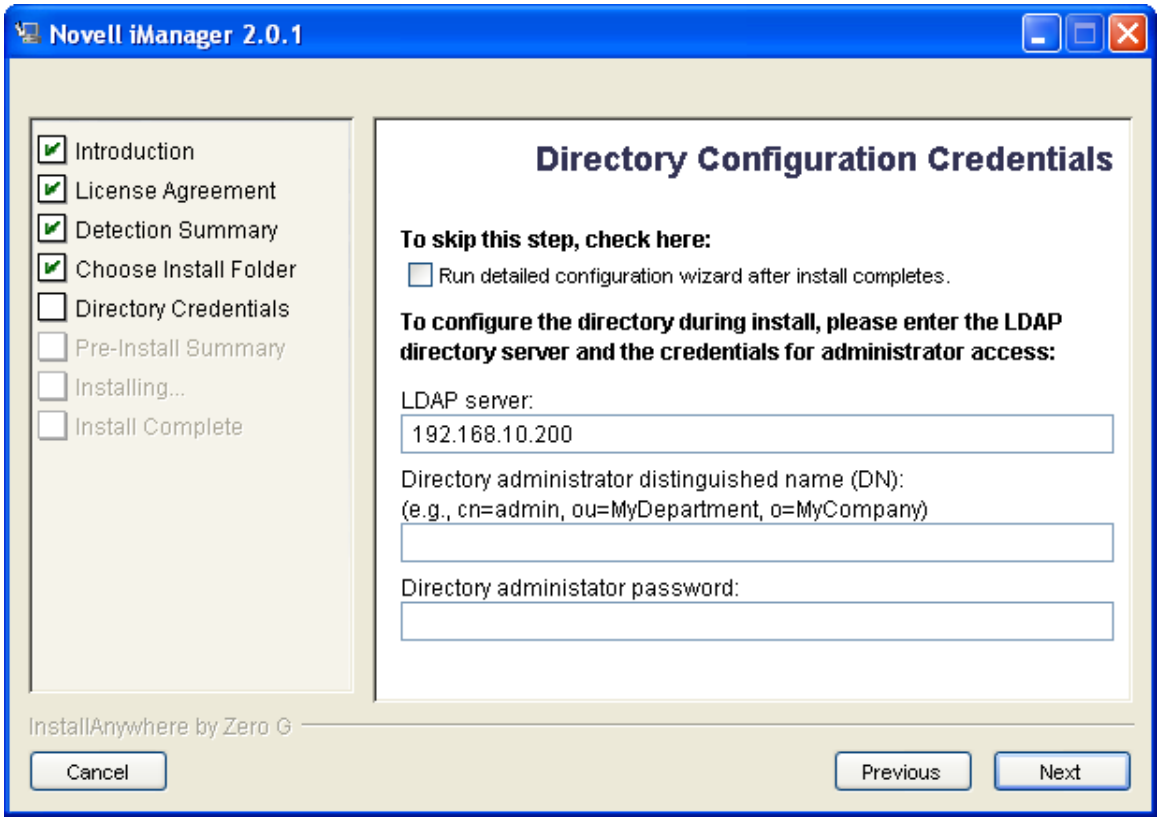
In this example, SUN's JAVA Virtual Machine (JVM) 1.4.2 has already been installed, and so the installation will skip the JVM component installation.

Click **Next** to continue.

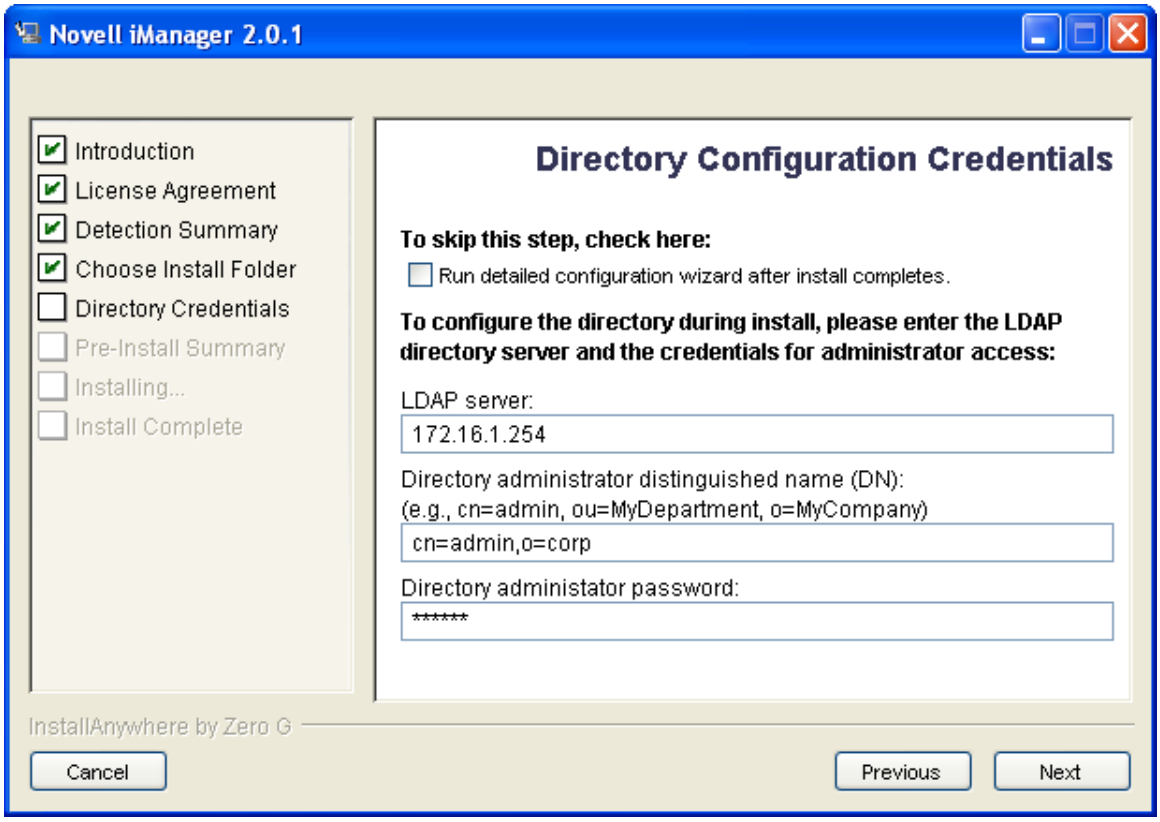


The installation routine will ask where you want to have the files installed on the Windows PC. The default is **C:\Program Files\Novell**. I recommend using the default settings unless you have good reason to change them.

Click **Next** to continue.



At the **Directory Configuration Credentials** screen, you need to change the options to point to your BorderManager server's IP address, and enter the admin ID and password.

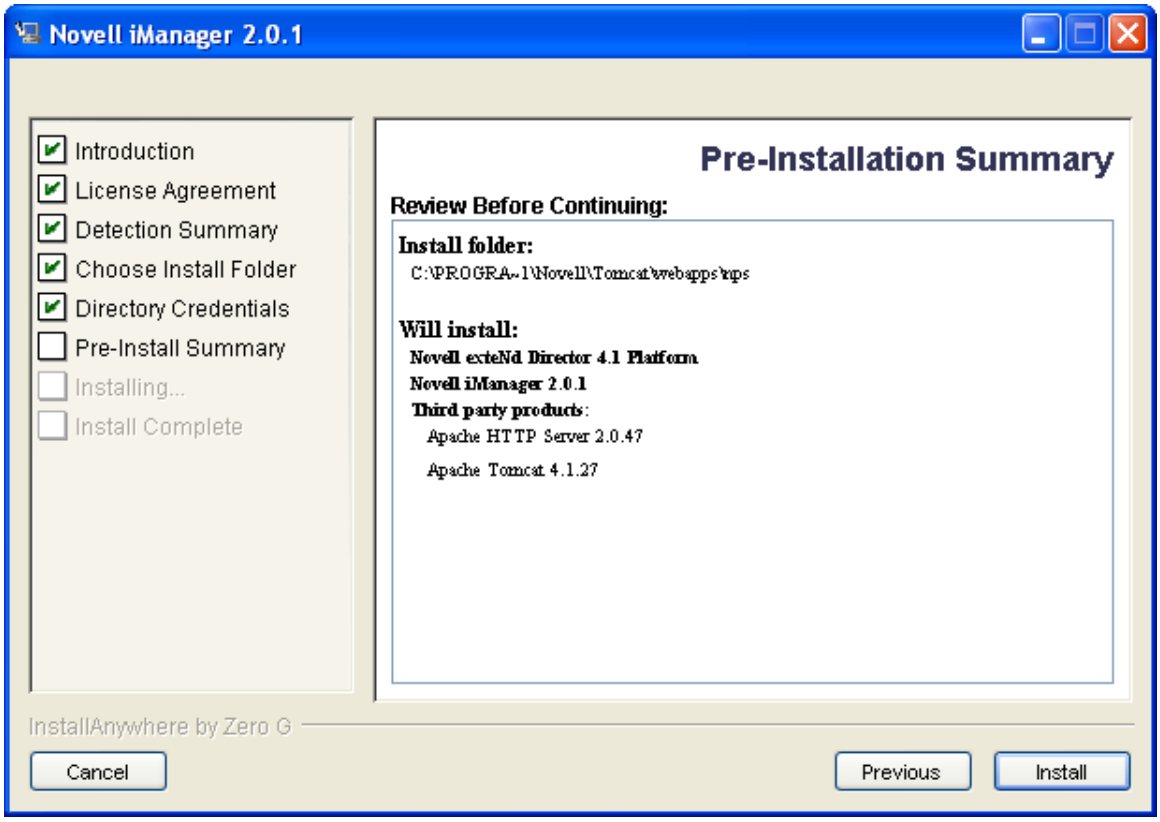


Enter the **IP address** of the server, which should be the BorderManager server, but could also be any server in the same NDS tree as BorderManager, and that has clear text passwords enabled in the LDAP Group object.

Enter **the distinguished name of the admin user ID, in LDAP syntax**. LDAP syntax uses commas between entries instead of periods. (That is, admin.corp in NDS syntax should be enter as cn=admin,o=corp in LDAP syntax).

Enter the admin **password.**

Click **Next**.

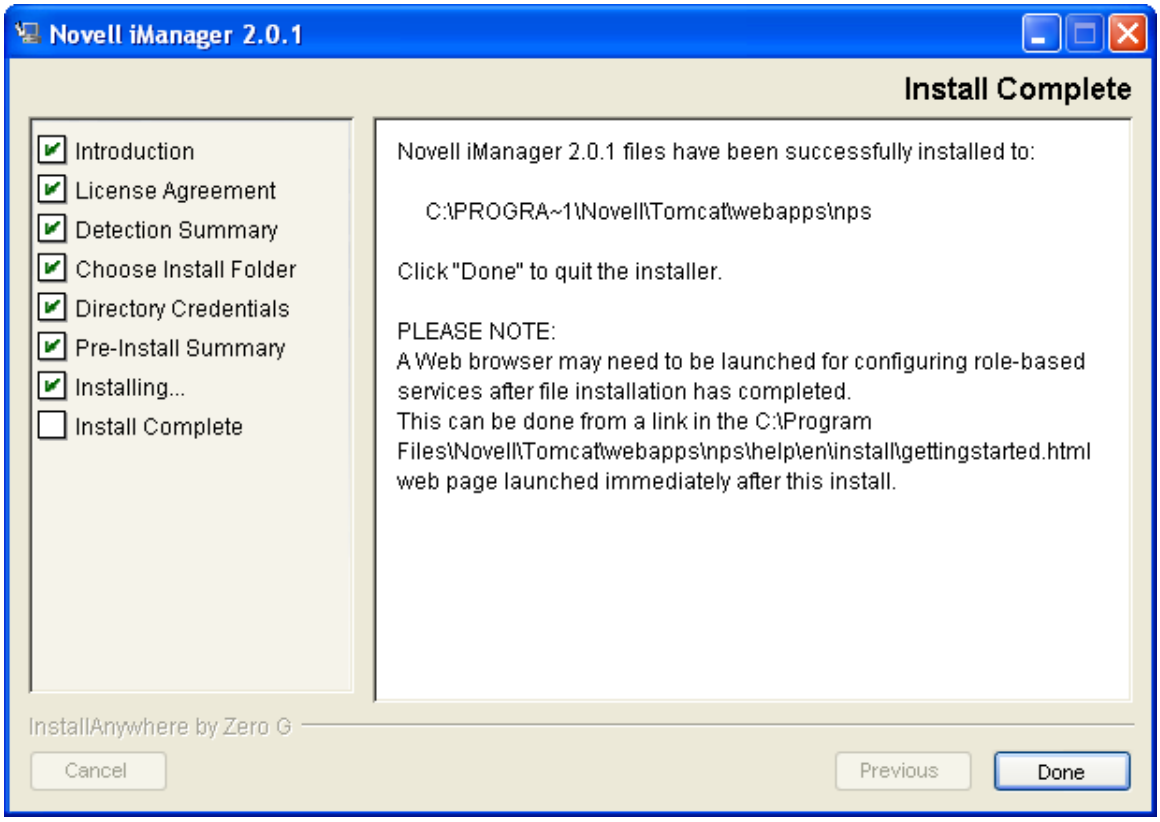


A **Pre-Installation Summary** screen will show the components to be installed and the location for the Tomcat install folder.

Click **Install** to continue.

The installation routine will begin copying files to the PC and configuring the services.

DOS windows may open and close during the procedure.



An **Install Complete** screen should show a message that Novell iManager 2.0 was successfully installed.

When the Install Complete screen appears, you are not done. As it mentions in the screen, you still have to launch a web browser and complete the configuration steps needed to install objects into NDS that will control how the browser looks, and what options are available (including BorderManager VPN configuration).

You should at this point see a small red and white icon for Apache services in your system tray. Before you can start the iManager configuration steps, you may need to stop and restart the Apache and Tomcat services from the Services menu. (There is a link in the Apache icon in the system tray to Services. Otherwise, you can run 'services.msc' as a run command, or browse to the Services configuration menu through Control Panel.)

Once you have stopped and restarted Apache and Tomcat on the PC, you may need to open the following file in a web browser:

C:\program files\novell\tomcat\webapps\nps\help\en\install\gettingstarted.html

There is a link in that html file to the configuration URL for iManager on your PC.

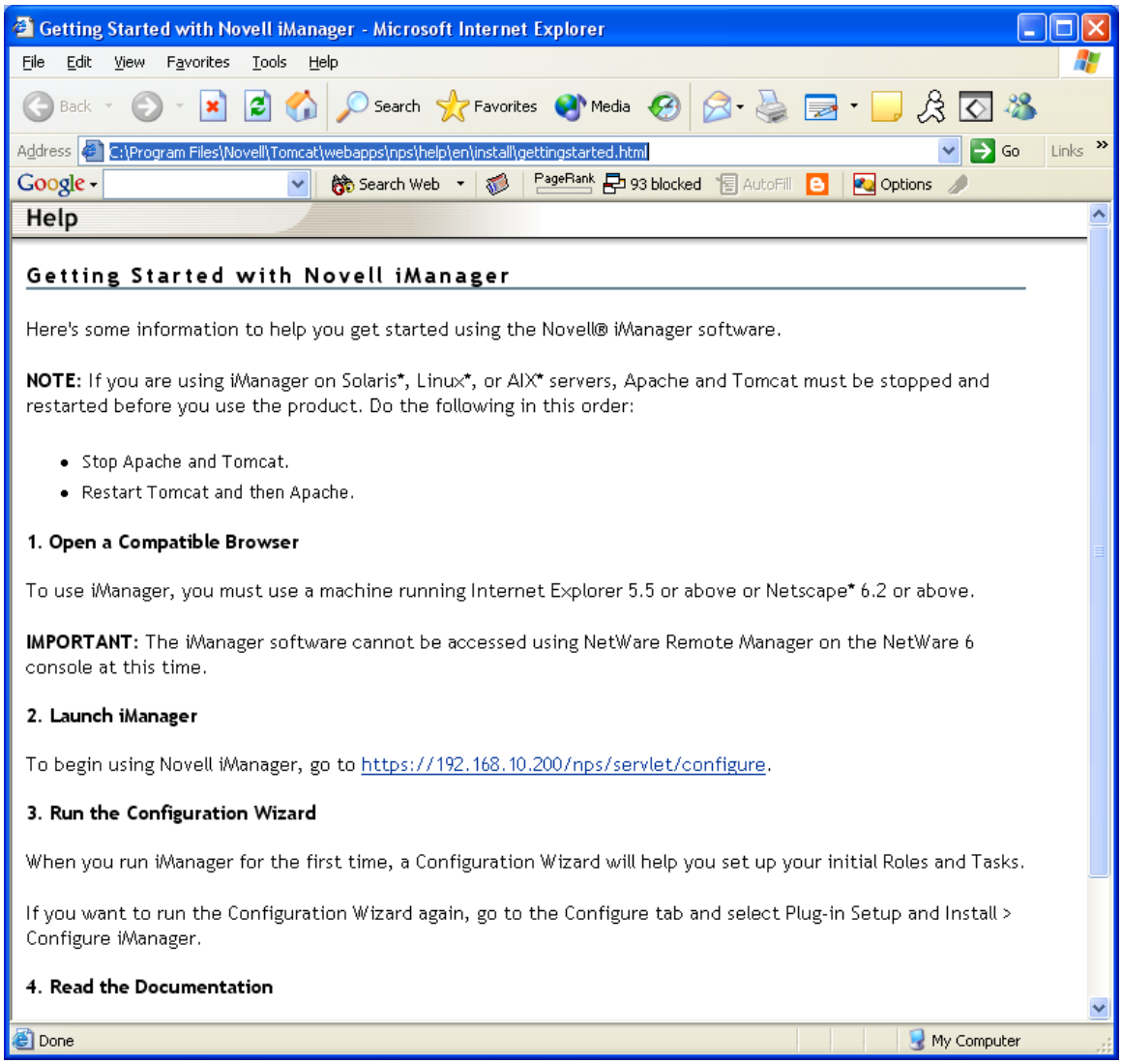
Click **Done** to continue.

Configuring iManager 2.0 the First Time

Immediately upon a successful installation, a web browser should open to the following URL:

```
C:\Program Files\Novell\Tomcat\webapps\nps\help\en\install\gettingstarted.html
```

However, you will need to stop and restart Apache2 and Tomcat services on the PC in order to access iManager 2.0.



You now need to go to the

https://192.168.10.200/nps/servlet/configure

URL and configure the VPN services at least once.

Note Substitute your PC's IP address, or use LOCALHOST instead of the IP address. You should not use a proxy setting in your browser for these steps, particularly if you want to use LOCALHOST.

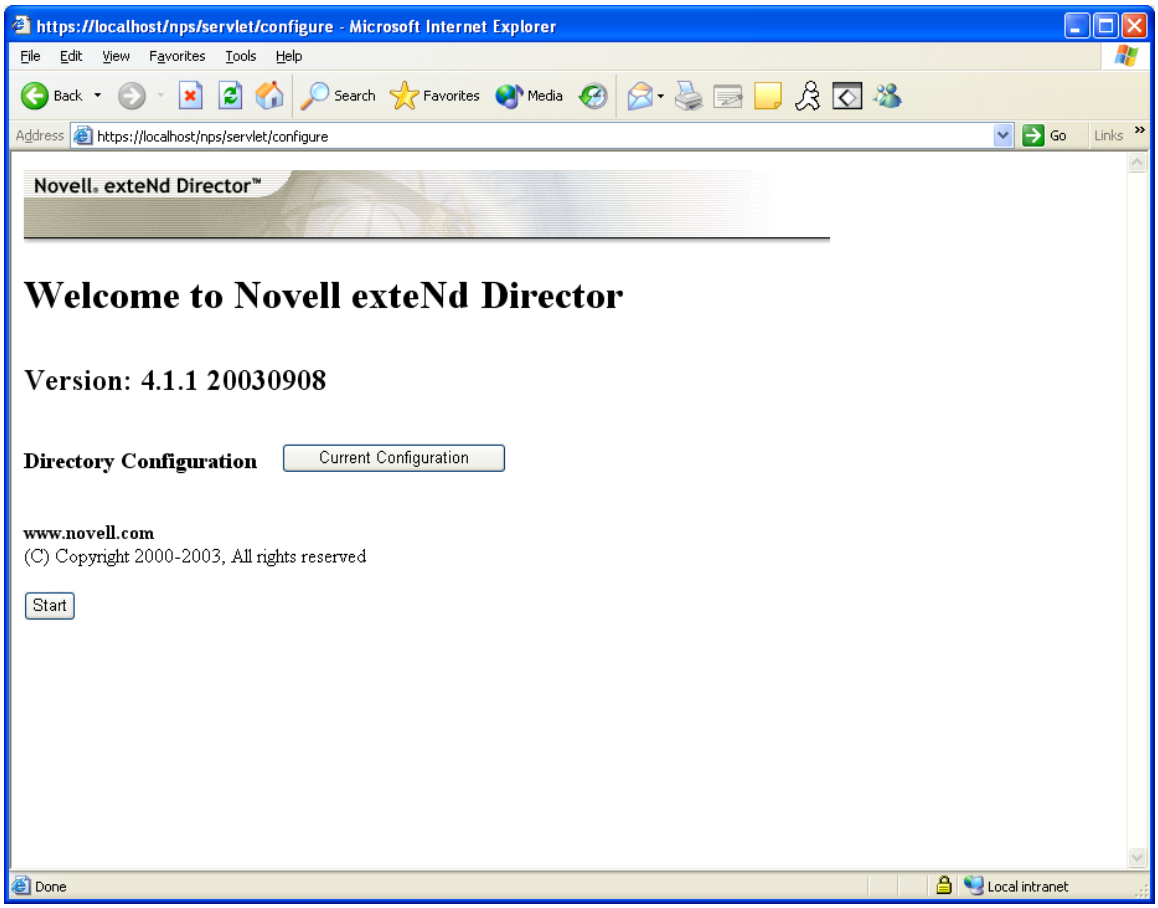
At this point, you need to stop and restart Apache2 and Tomcat services on the PC, and then return to the above URL. You should bookmark the URL.

Configuring Portal Properties

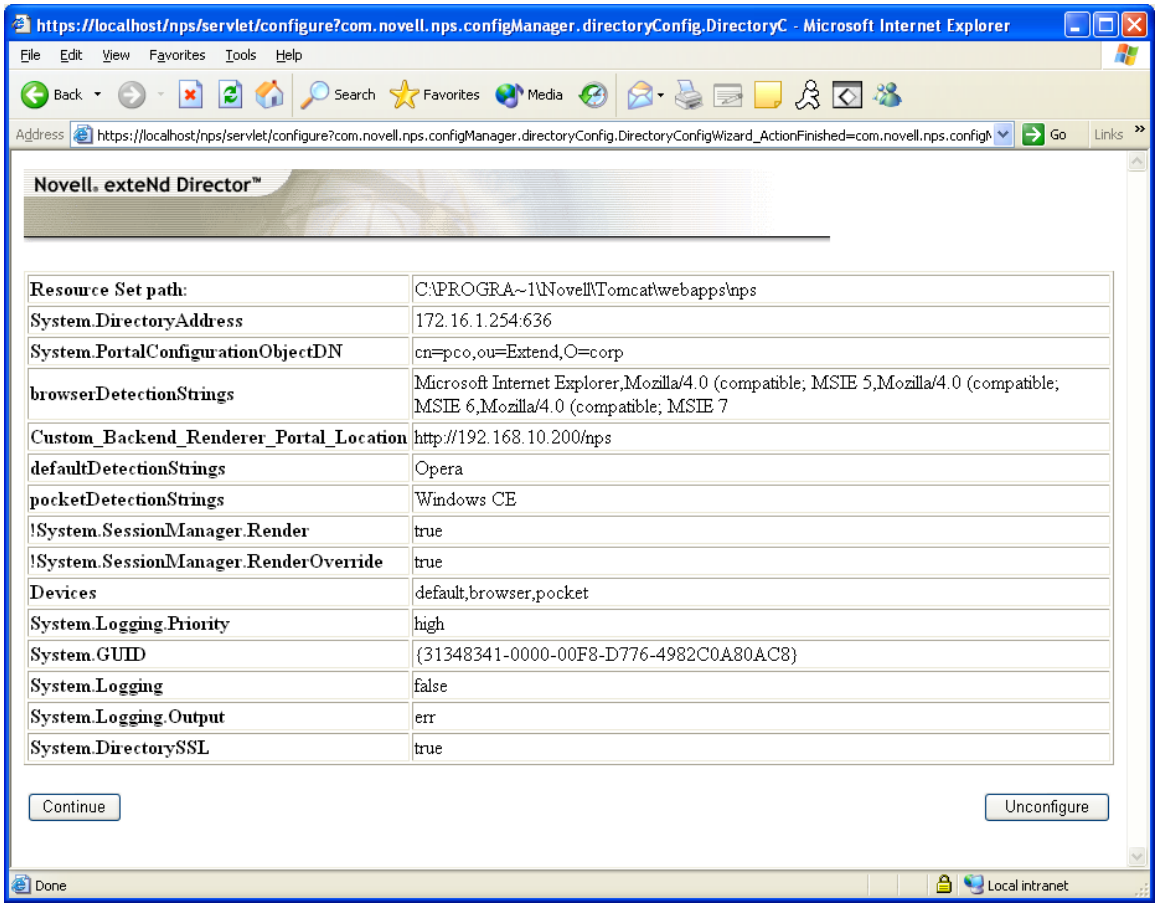
From the

https://localhost/nps/servlet/configure

URL, you should see the following menu:



Click **Current Configuration**.



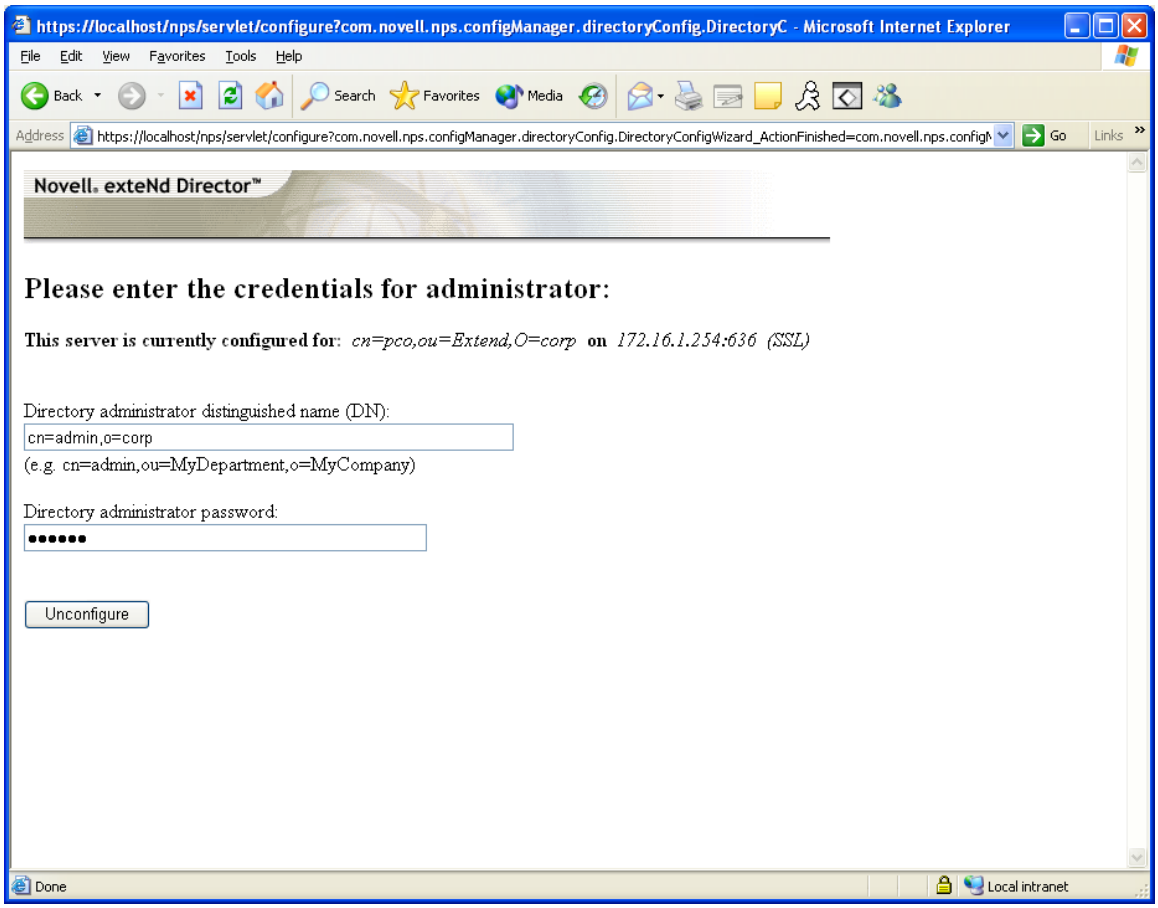
You should see a screen similar to the above. Note the System Directory Address, which is the eDirectory server address (and secure LDAP port 636) that you entered in the beginning of the iManager installation.

If you want to change this, click the Unconfigure button in the lower right.

Otherwise click Continue.

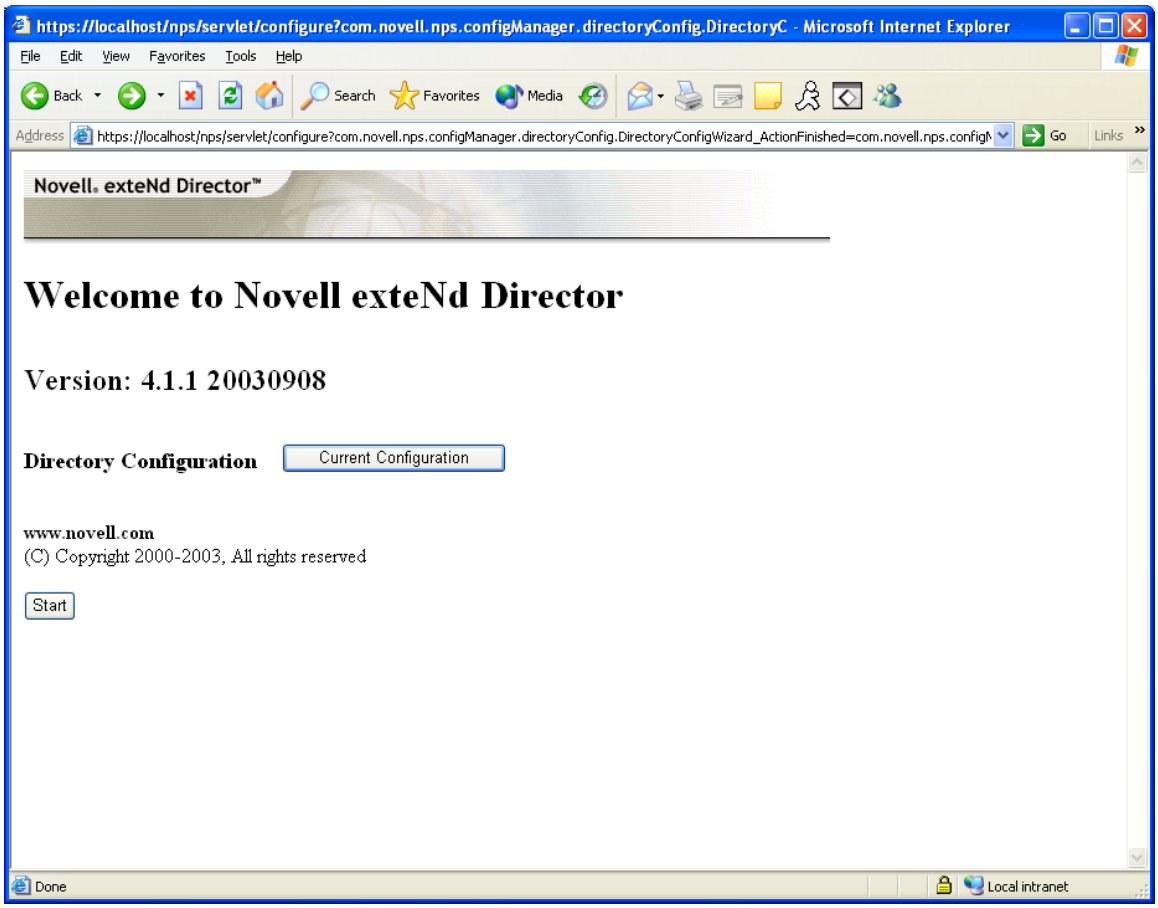
Unconfigure Option (optional)

This option should only be used if you want to reconfigure the portal settings to start over from a previous configuration. Skip this step if configuring iManager for the first time!



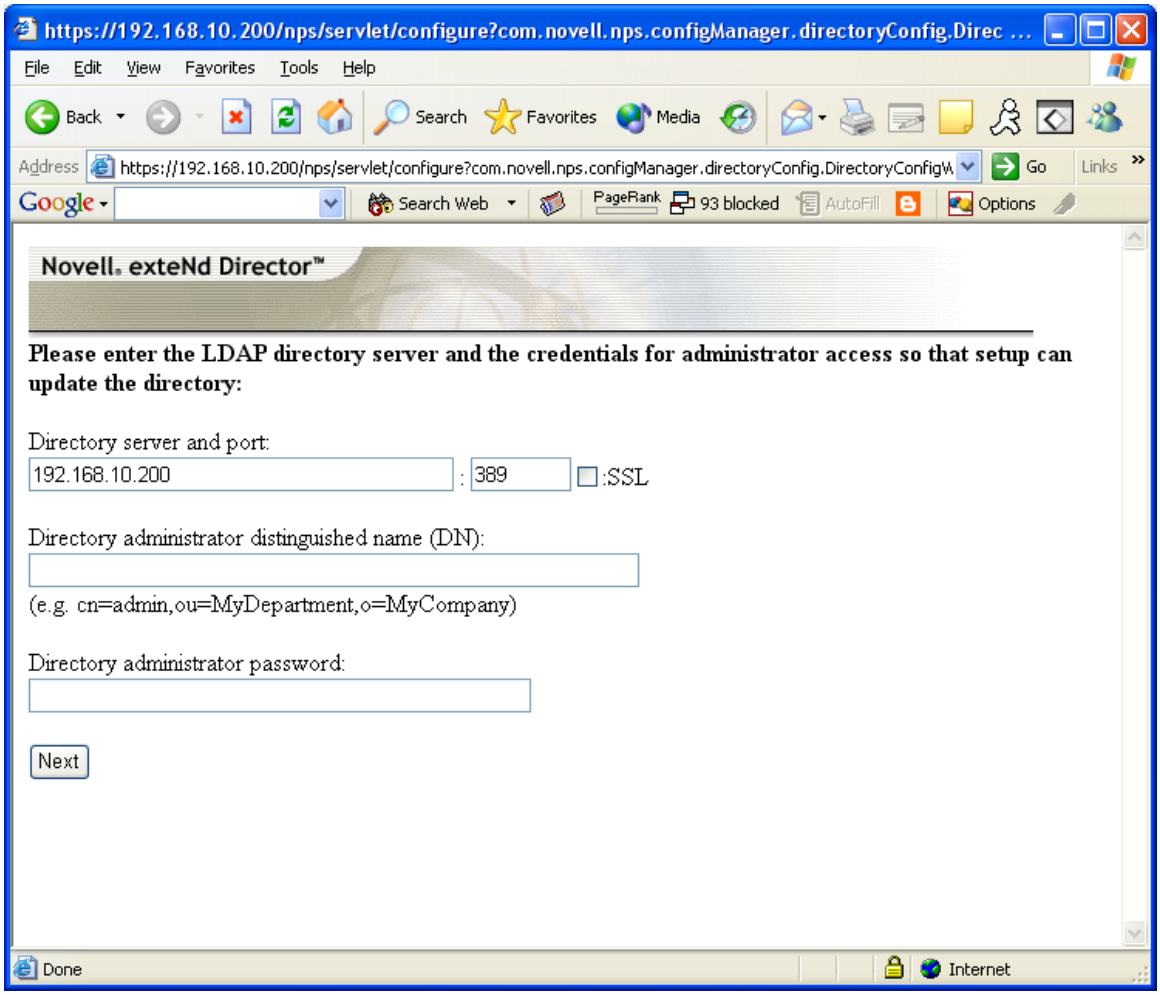
Clicking the Unconfigure option allows you to change configuration used by iManager installation. This may be useful when setting the system to access a different server. Enter the admin ID / password, and click Unconfigure. Your settings will be reset to defaults, and you can start over. The same end can be accomplished by editing the portal.properties file as described later in this chapter.

Configure Portal



Click on **Start** to begin configuring iManager.

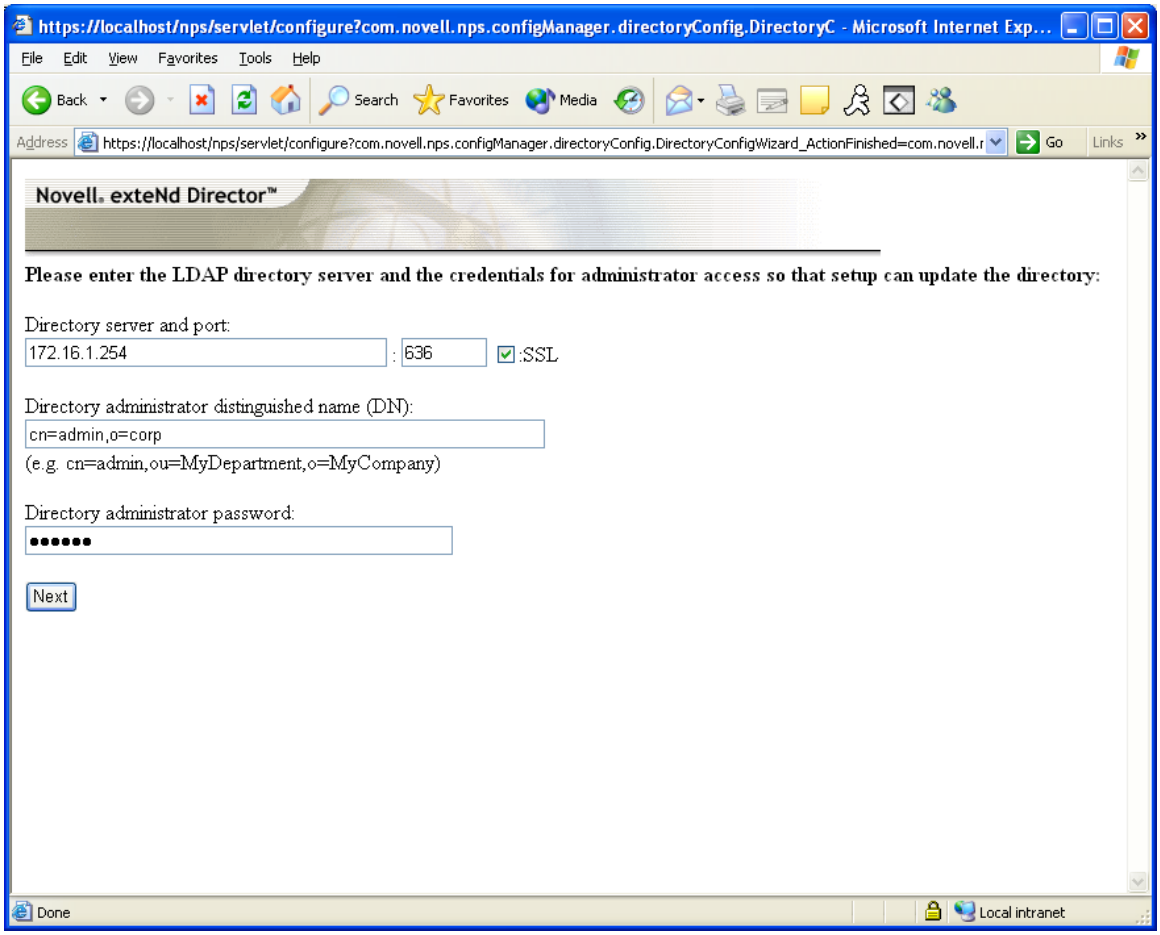
These next steps tell iManager what LDAP server to authenticate to, and get iManager set up with snapins.



iManager starts by pointing to the IP address of the PC it is running on.

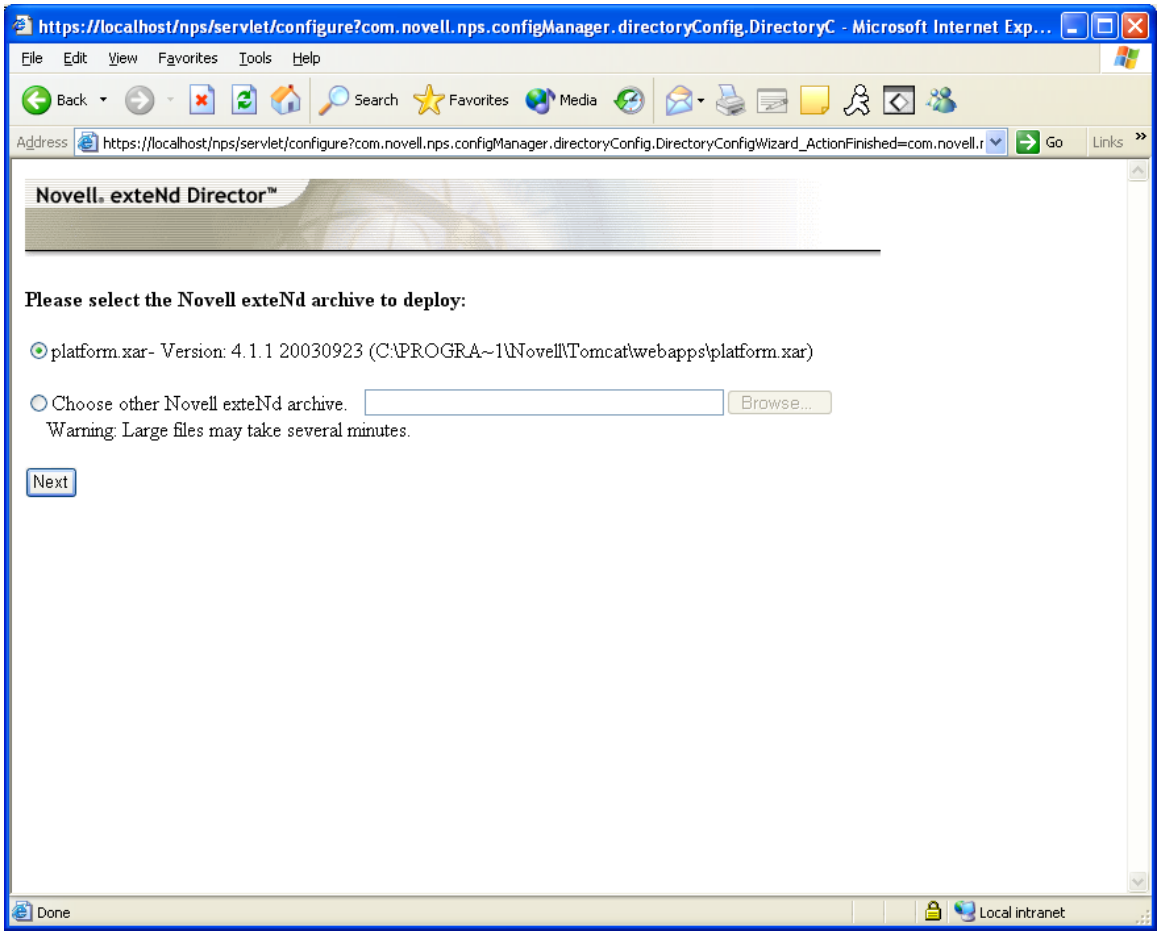
We must change the **Directory server and port** IP address to point to a NetWare server.

It is best to leave the port at 636, with SSL enabled, but if you have a problem authenticating to LDAP, you may want to change to port 389 and uncheck SSL. (Assumes clear text passwords are enabled in the LDAP Group object on the server).



In this example, I will point to the IP address (172.16.1.254) of a NetWare 6.0 server running BorderManager 3.8, with an Admin user located in the DD Organization container. (E.G. cn=admin,o=dd is the LDAP syntax for .admin.dd).

Click **Next** to continue

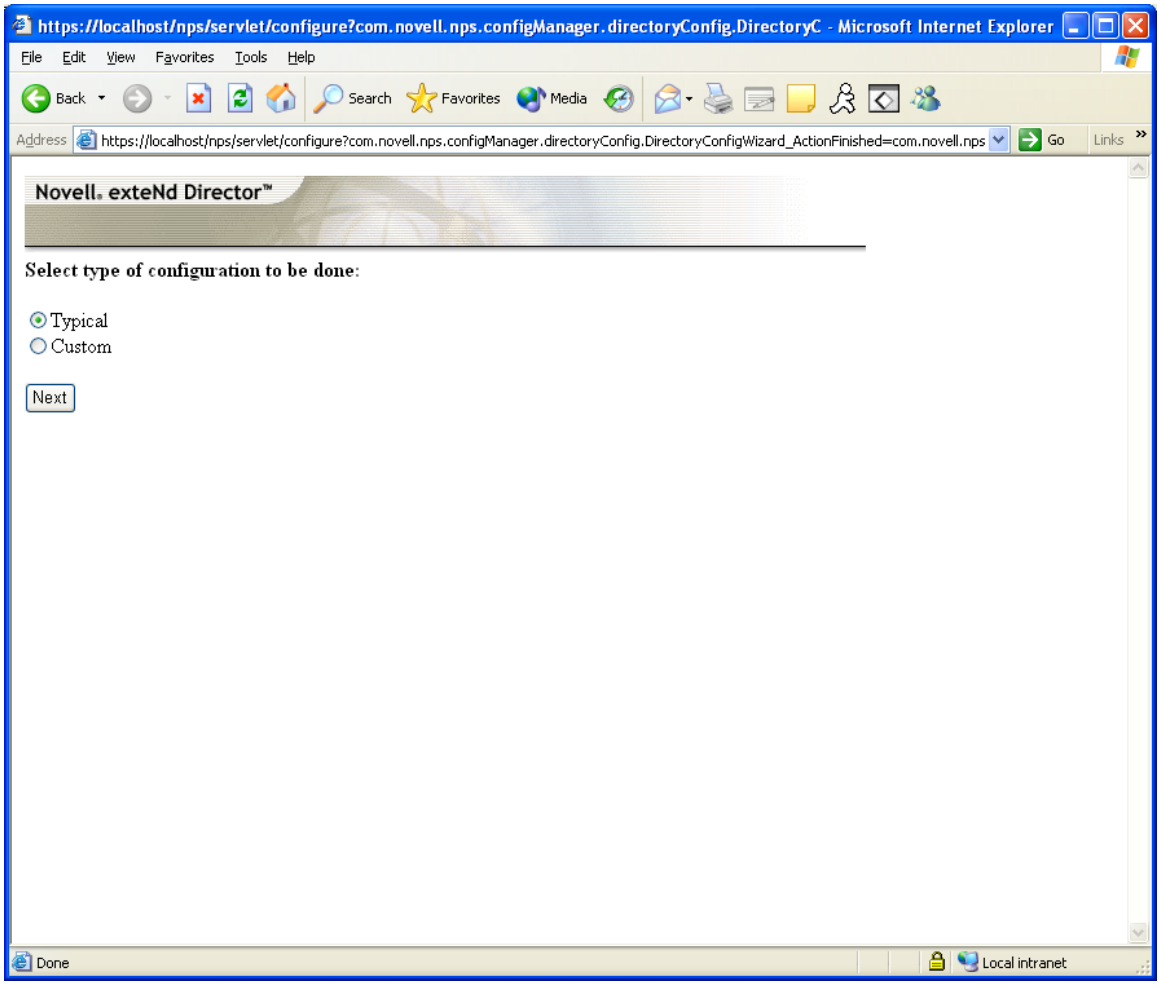


You are given the choice of selecting a default archive to deploy, or select a custom archive.

Select the default (first) option **'platform.xar'**

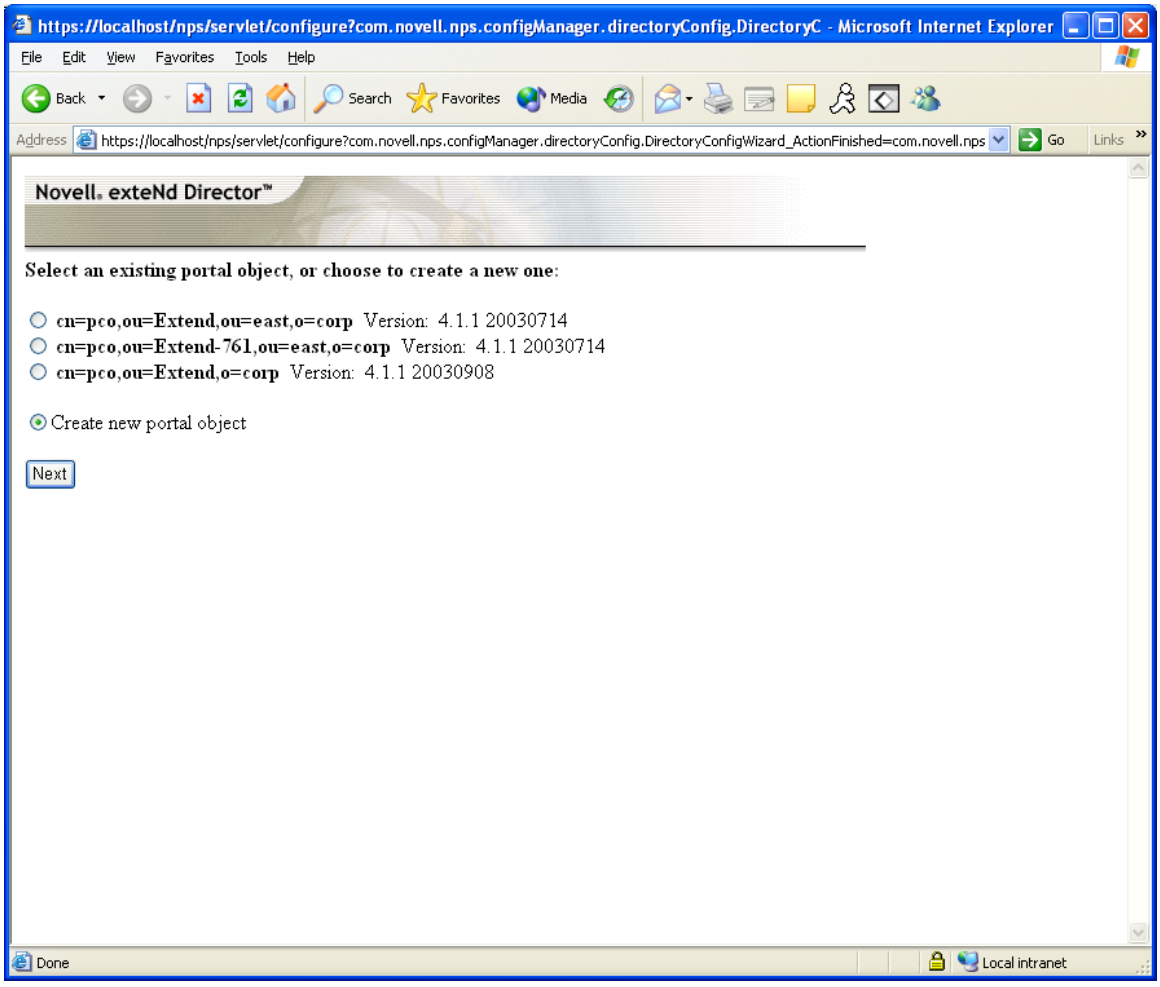
Press **Next** to continue.

A license agreement screen appears. Click on the **radio button to accept** the terms of the license agreement, then click **Next** to continue.



You should see an option to do Typical or Custom. Either will work, but Typical is easier, so choose **Typical**.

Click **Next** to continue.

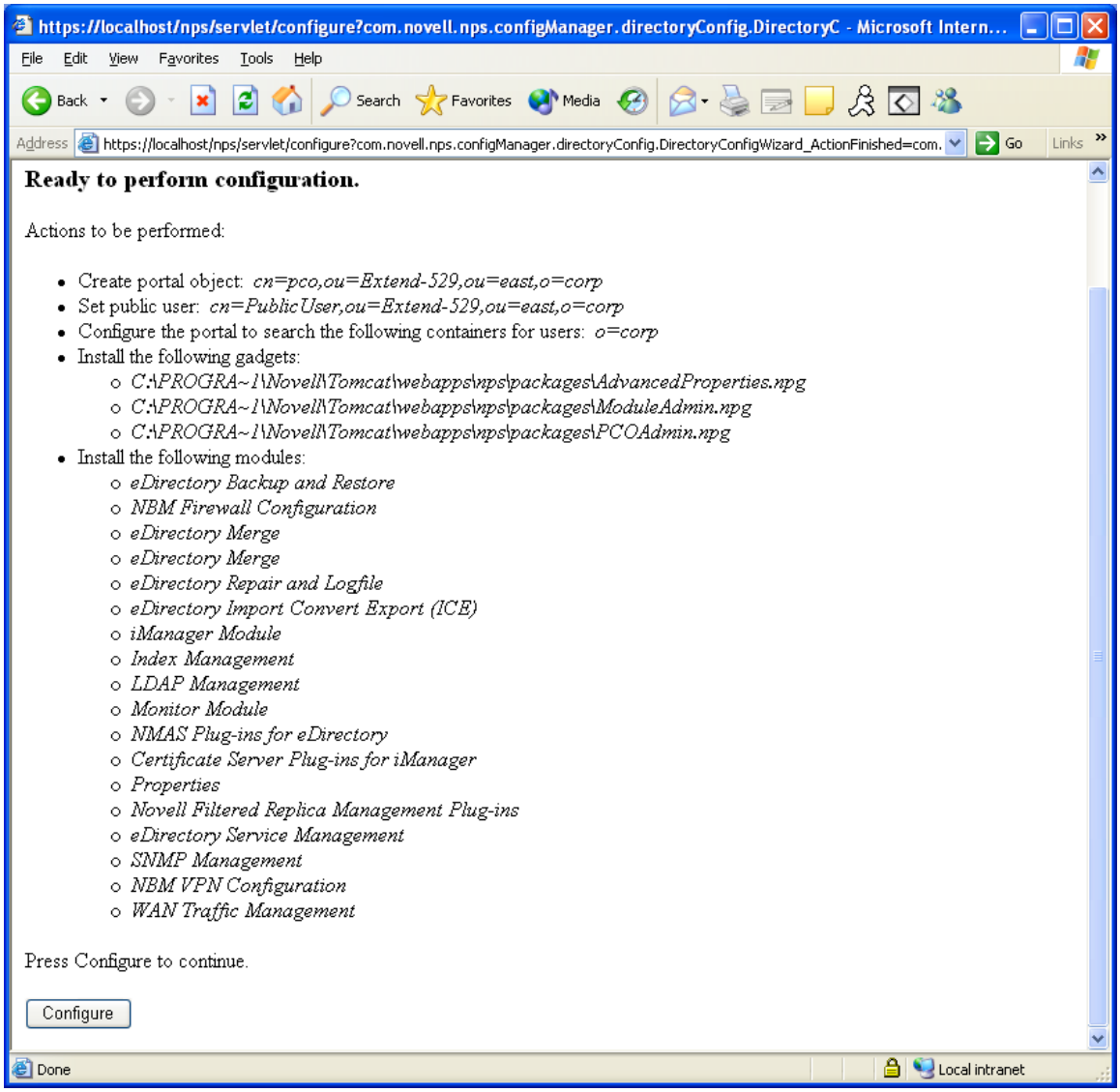


You can now either configure an existing portal object, or create a new one. If you select an existing object, you must know the password seed to modify it.

In the example above, there are several choices (partly because I have installed iManager on other PC's and chose to create a new object each time).

Choose **Create new portal object**.

Click **Next**.



You should then see a **Summary** screen.

Press **Configure** to continue.

iManager will then configure several modules. The configuration process will create a new Extend-xxx OU in the eDirectory tree, and create various objects within that OU.

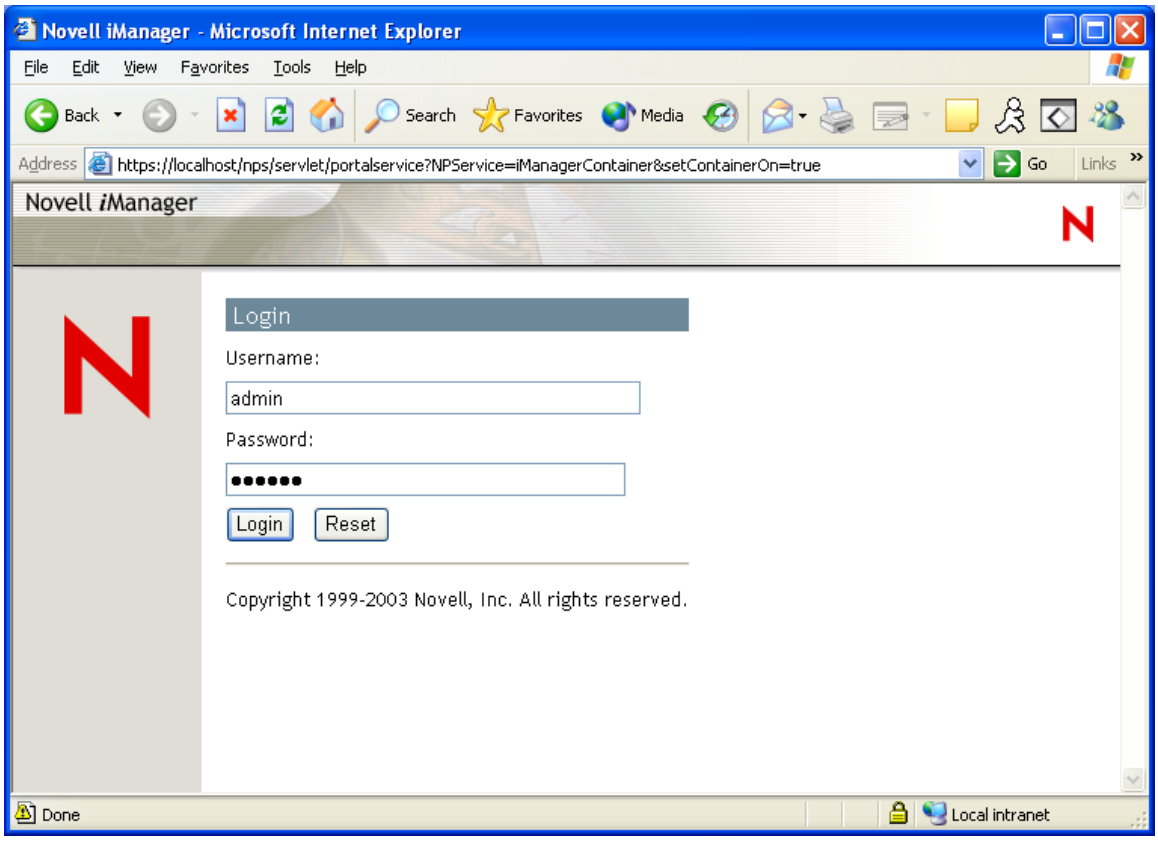
When configuration is done, press **Continue**,

At this point, you must **stop and restart the Tomcat service** to pick up the new settings and modules, and iManager should log in and be ready for basic use.

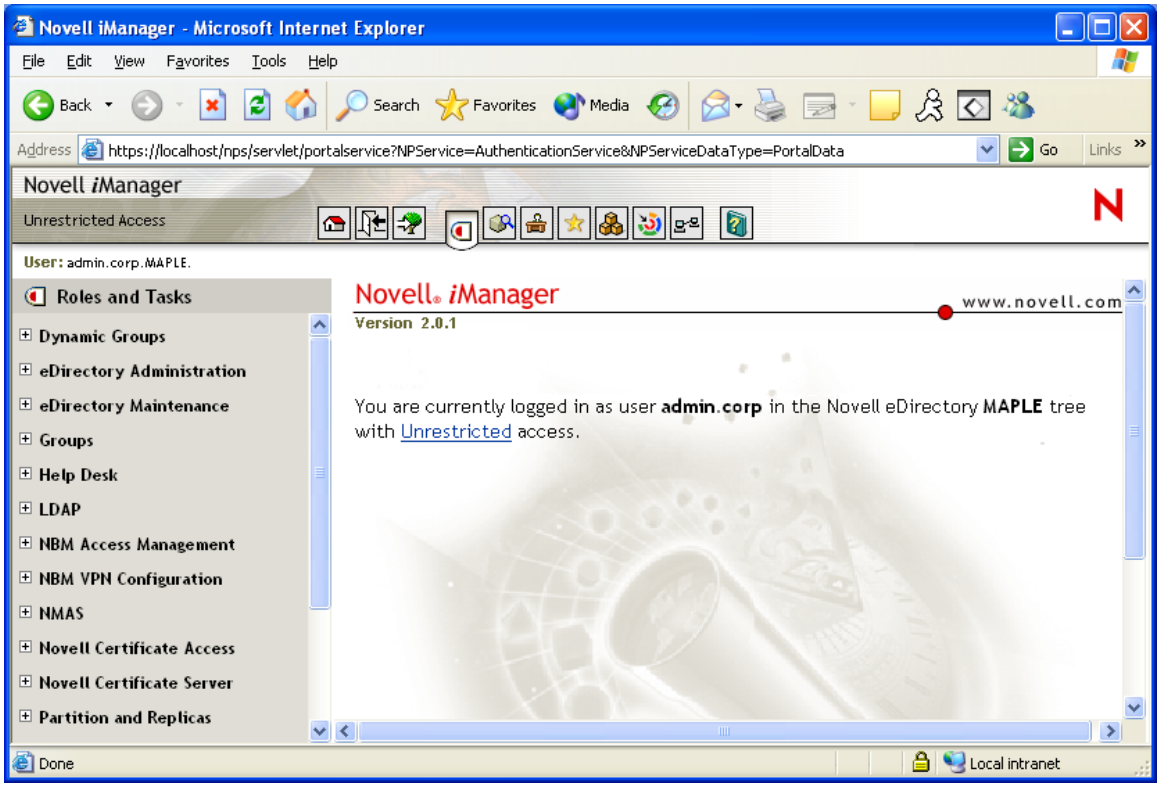
Adding VPN Snapins to iManager 2.0

You will need to log in to iManager 2.0, and add the VPN snapins.

Log in using https://localhost/nps/iManager



A login screen should appear, and you can log in as Admin.



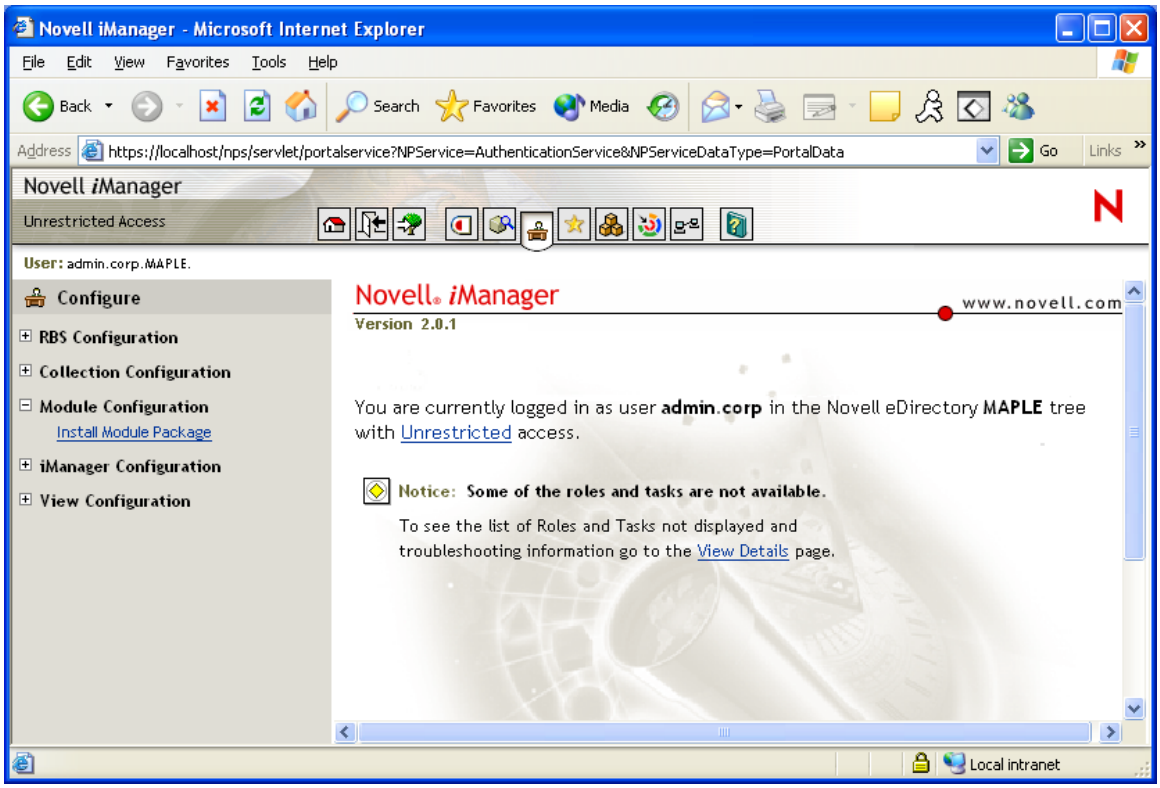
At this point you should see many **Roles and Tasks** in the left panel, but you may not see the BorderManager filtering or VPN options.

If you do NOT see the NBM VPN Configuration option under Roles and Tasks, you need to add the VPN snapins at this point.

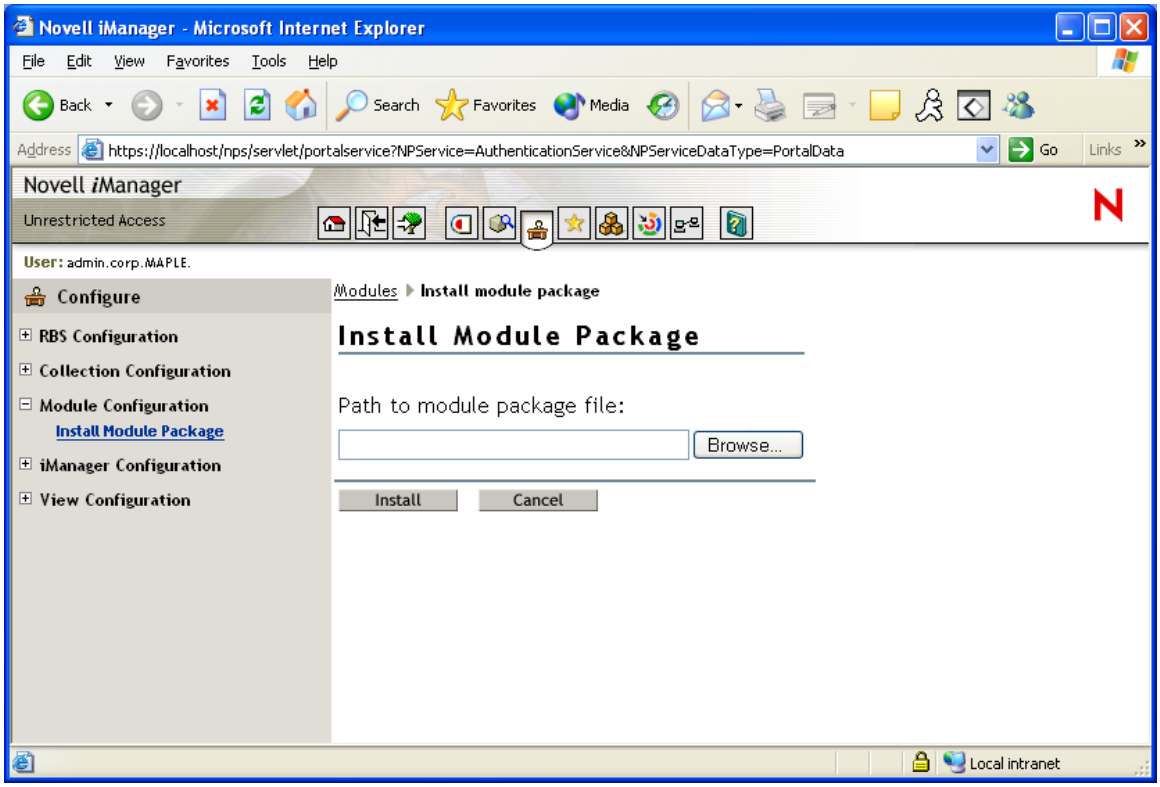
If you see the **NBM VPN Configuration** option in the left panel, you are ready to configure BorderManager 3.8 VPN services. If you do not, you must install the BorderManager 3.8 VPN module for iManager.

In order to have an option to configure BorderManager 3.8 VPN features, you need to install the VPN.NPM module into iManager 2.0. The file is located within the BorderManager installation files (CD or uncompressed download), in the VPN subdirectory.

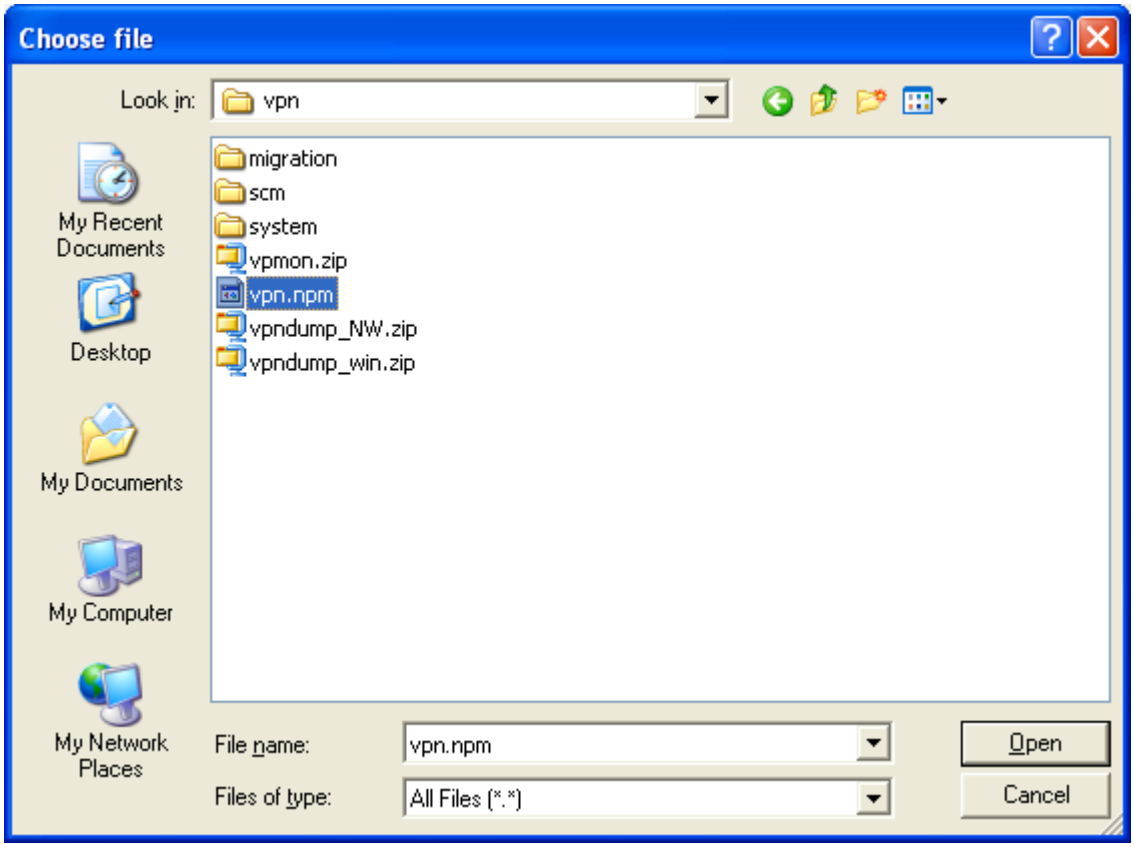
Log into iManager 2.0, and click on the **Configure** button. The configure button looks like a man sitting behind a desk.



Open the **Module Configuration** link on the left panel, and choose **Install Module Package**.

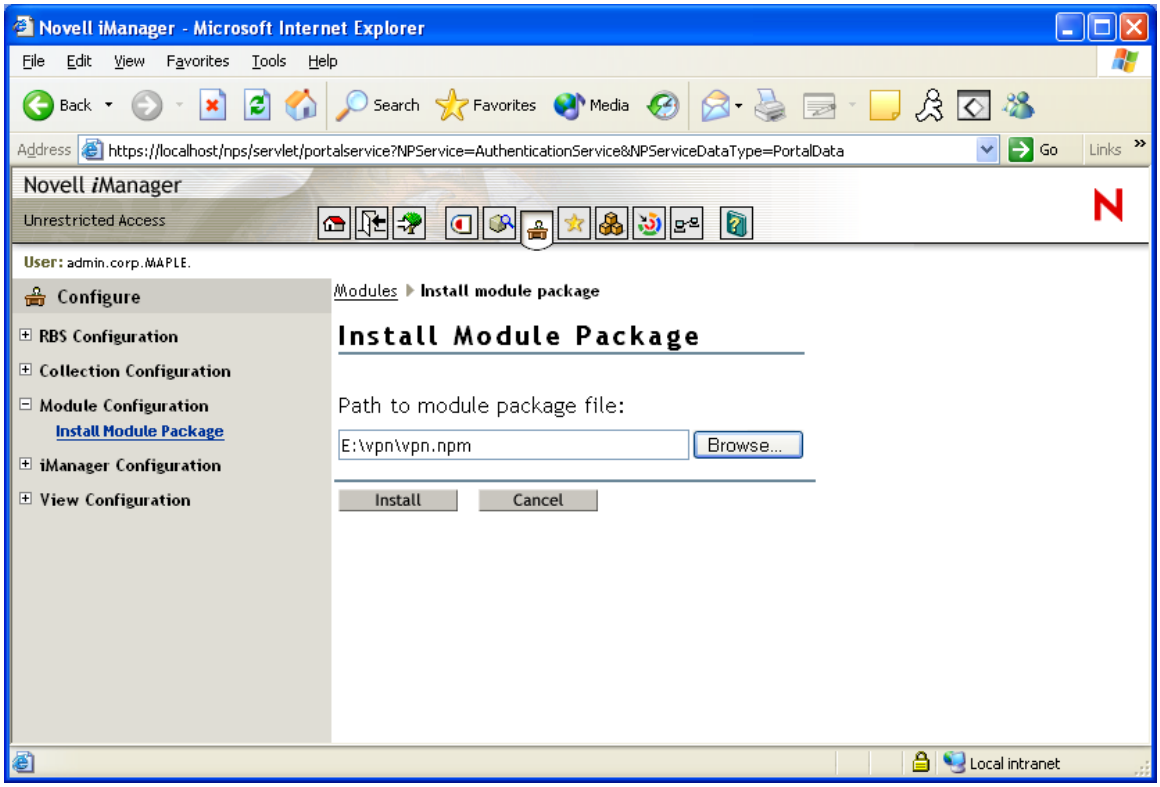


Click on **Browse**.

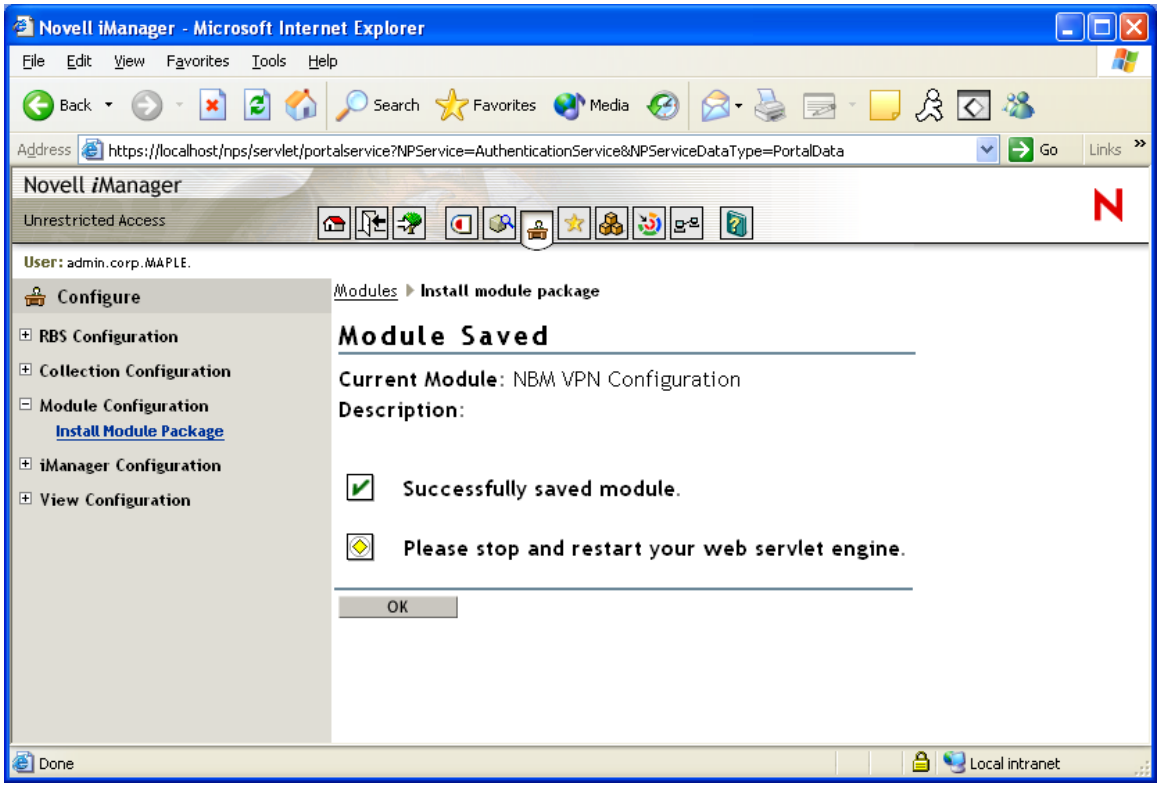


Browse to the BorderManager 3.8 product CD (not Companion CD), VPN directory.

Select the **VPN.NPM** file, and click Open.



Click **Install** to install that module package file.

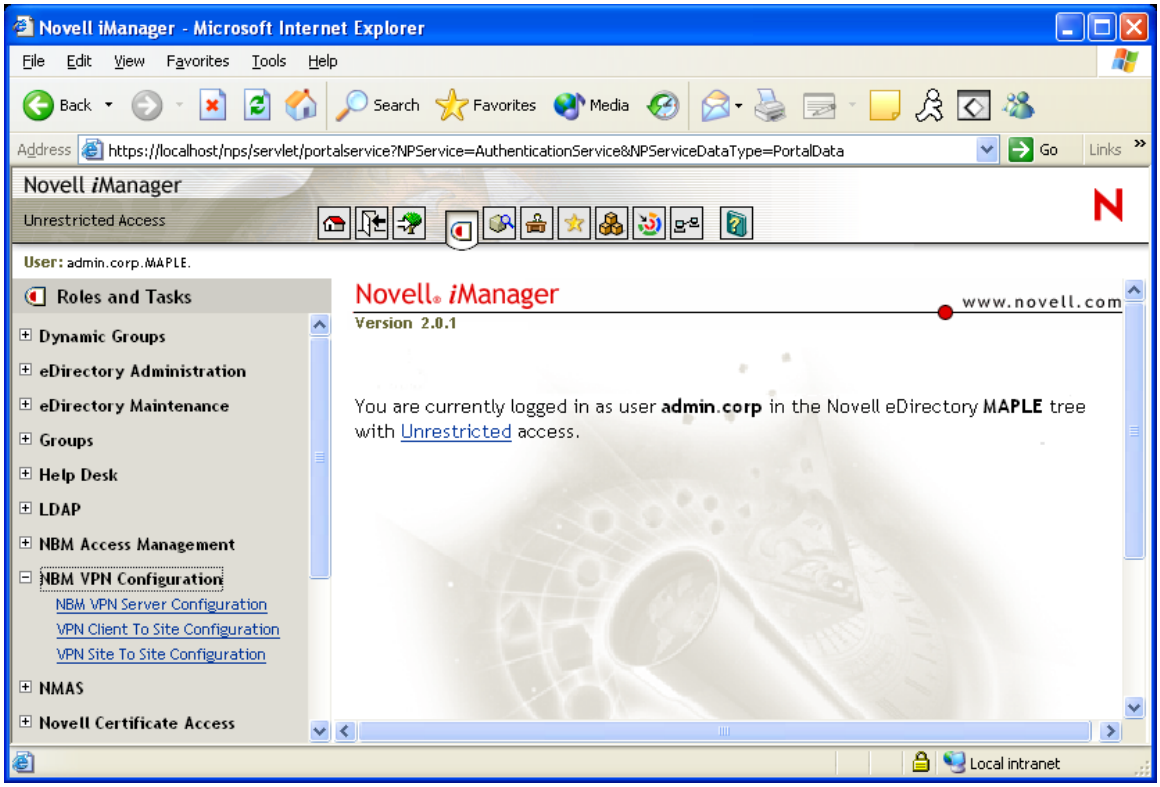


When the module has been saved, click **OK**.

Stop and restart the Tomcat service on the iManager PC.

Then click **OK** to continue.

You may have to log in again. Do so.



Now you should have a **NBM VPN Configuration** option in the left panel.

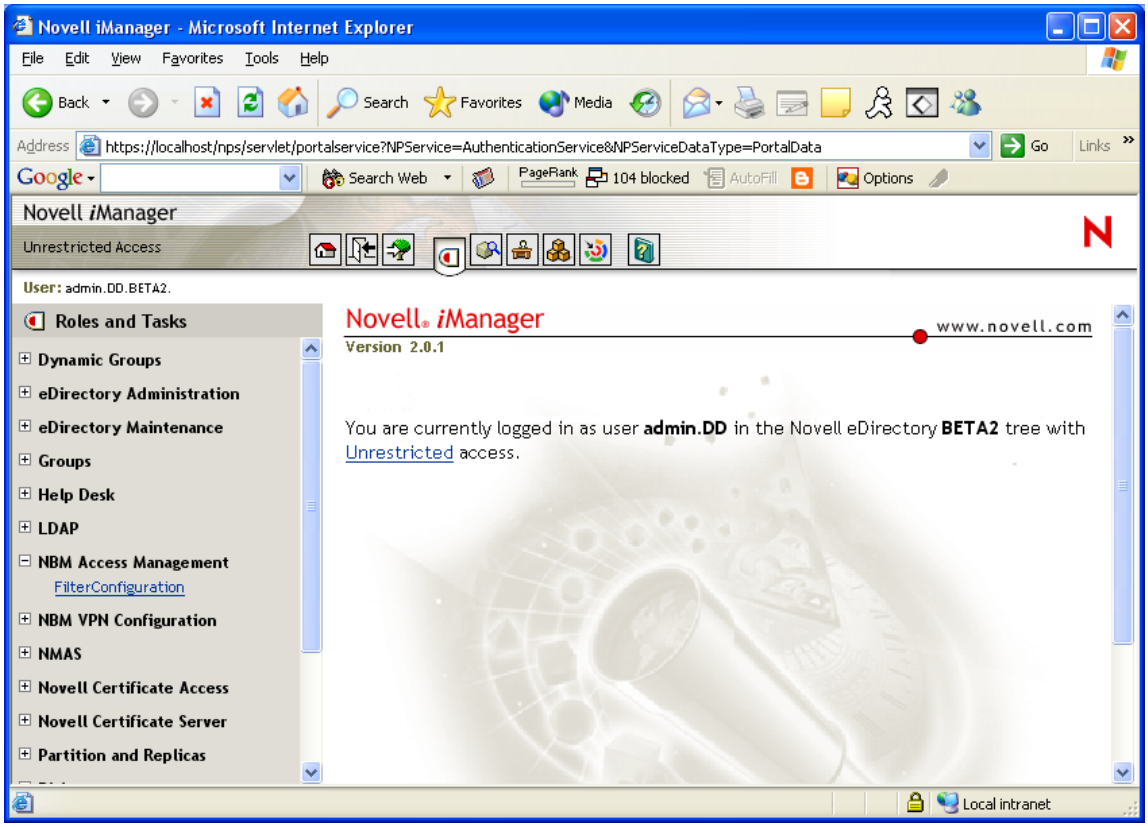
Adding Filtering Configuration Option to iManager 2.0 on Windows

In order to use iManager 2.0 on Windows to manage BorderManager 3.7 or 3.8 filters, you **may** need to install the BorderManager snapins for iManager.

The snapins are installed using a setup file located on the BorderManager 3.8 product CD, in the CL_INST/SNAPINS directory. Launch the **NBM_IM2_SNAPIN_INSTALL.EXE** file there and follow the prompts.

Once the snapin installation program has completed, **stop and restart the Apache2 and Tomcat services** on the Windows PC.

Log in to the local iManager on the Windows PC.



You should now have a **NBM Access Management** option, with a **FilterConfiguration** menu entry for managing filters from your browser.

Resetting the iManager Configuration File

Should iManager quit working, because it is no longer able to connect to a LDAP server, you may need to reset the configuration to point to a different server. Perhaps the server's IP address has changed, or the server has been removed.

But you may first have to remove the old configuration so that iManager doesn't try to log in to the old server first.

You may need to modify the PORTAL.PROPERTIES file in the following (default) directory:

C:\Program Files\Novell\Tomcat\webapps\nps\WEB-INF

That file looks something like this:

```
#eXtend
#Thu Nov 13 17:16:02 MST 2003
System.DirectoryAddress=172.16.1.254\:636
browserDetectionStrings=Microsoft Internet Explorer,Mozilla/4.0 (compatible;
MSIE 5,Mozilla/4.0 (compatible; MSIE 6,Mozilla/4.0 (compatible; MSIE 7
System.PortalConfigurationObjectDN=cn\=pco,ou\=Extend-
529,ou\=east,o\=corp
Custom_Backend_Renderer_Portal_Location=http\://127.0.0.1/nps
pocketDetectionStrings=Windows CE
defaultDetectionStrings=Opera
\!System.SessionManager.Render=true
\!System.SessionManager.RenderOverride=true
System.Password=rllinmlmcorhmockl
Devices=default,browser,pocket
System.Logging.Priority=high
System.GUID={33762A40-0000-00F8-D797-0740C0A80AC8}
System.Logging=false
System.Logging.Output=err
System.DirectorySSL=true
```

Notice the **System.DirectoryAddress** entry. This is the IP address and LDAP port number of the server you are trying to contact via LDAP.

Notice the **System.PortalConfigurationObjectDN** entry. This is the eDirectory object that iManager is using to interface to eDirectory.

If you want to start the iManager configuration process again, to point to another server and create a new portal object, simply remark out these two lines, and restart Apache/Tomcat. Then go through the configuration steps shown earlier in this chapter.

On a NetWare 6.5 server, the same settings are contained in **sys:\tomcat\4\webapps\nps\WEB-INF\ PortalServlet.properties.**

<This page intentionally left blank. This is to facilitate putting in chapter tabs in a ring binder for double-sided printing. The main chapters should start on an odd-numbered page.>

Errata & Revisions

This book was first released in beta versions, with some corrections and additions made to the book before release as First Edition. The following changes were made as compared to previous revisions.

Beta 2.0

Page 399: Figure was incorrect. Figure on page 200 was correct. Updated figure to deny all SMTP traffic in access rule.

Miscellaneous typos corrected.

Beta 3.0

Updated descriptive test for Generic TCP and UDP proxy examples for pcANYWHERE.

Added example for WS_FTP in FTP Proxy section

Numerous small wording changes and several corrections to typographical errors.

Added mention of BorderManager 3.6 throughout.

Added sections for Client-to-Site VPN using pure IP login and VPN over NAT.

Corrected mention of Portal where Web Manager was meant.

Updated section on patches to reflect more recent patches.

Updated BMON.NCF and BMOFF.NCF examples

Updated troubleshooting section with additional information.

First Edition

Page 35, “TCP port 8080 traffic will come to the BorderManager server HTTP proxy, and the BorderManager server will then use standard HTTP (TCP port 80) to access web browser.” should be “TCP port 8080 traffic will come to the BorderManager server HTTP proxy, and the BorderManager server will then use standard HTTP (TCP port 80) to access web servers.” (Change browsers to servers).

Page 39, Figure, lower right corner. 'Site A BorderManager server protects network 192.168.11.0…" should have been 'Site B BorderManager server protects network 192.168.11.0…"

Several changes were made to the both the Site-to-Site and Client-to-Site VPN chapters to clarify meaning.

Notice about the ability for BorderManager 3.6 to handle NAT on the client side of Client-Site VPN was added to a few pages in the Client-to-Site VPN chapter.

Some duplicate wording was removed in the Client-to-Site VPN chapter.

Added mention of the use of the HOSTS file in addition to the NWHOST file for replacing SLP information with Client-to-Site VPN.

Chapter 19, added VPN debug options.

The headers were changed to include the chapter / section titles, and the book title was moved to the footer.

Version 1.01

Page 260, paragraph two, sentence three read "You will have to specific source and destination values to limit inbound and outbound traffic as desired.". It should have read "You will have to specify source and destination values to limit inbound and outbound traffic as desired."

Page 427, the first sentence of the paragraph titled "Deny All Ports for Troubleshooting Purposes " read "In the same way that the last rule logged URL denials, this rule logs Port denials to the Access Control Log ", and it should have read "In the same way that the next rule logs URL denials, this rule logs Port denials to the Access Control Log."

Second Edition

Changes from Beta 1

Some spelling errors were corrected throughout the book.

Some blank pages were added to cause Chapter 1 through the Index to start on odd-numbered pages, in order to make facilitate adding section tabs in a ring binder if you print the book double-sided.

A cable modem scenario was added in Chapter 2

NDS design configuration information was added regarding BorderManager 3.7 and the NBMRuleContainer in Chapter 3.

Patch information was updated in Chapter 3.

One of the screenshots in Chapter 3 on configuring access rule enforcement during a BorderManager 3.7 installation was incorrect. It was replaced with the correct screenshot.

The example configuration for Transparent Proxy in Chapter 7 was enhanced to add exception IP addresses for any reverse proxies or static NAT secondary addresses that might be on the server. This change will help to keep transparent proxy from looping traffic back to itself.

Page 255 conflicted with 248 and was corrected in Chapter 9. To use an internal POP3 mail client with Mail Proxy configured for an external POP3 server, you need to connect to the private IP address of the Mail Proxy server, not the Internet address of the external POP3 server.

Additional information on configuring protected networks for the master VPN server was added in Chapter 17.

Some general updates were added for Client-to-Site VPN in Chapter 18.

A new section in the Chapter 20 was added to show examples of how to allow some hosts to use the HTTP Proxy without having to authenticate through proxy authentication. This section makes use of the '**Authenticate Only when user attempts to access a restricted page**' option in the Authentication Context menu.

A new screenshot of the Access Rules menu was added to Chapter 20, along with an example of using N2H2 filtering on BorderManager 3.7. The option to use N2H2 is only available for BorderManager 3.7, and only after adding a patch that adds the capability in the Access Rules menu.

An access rule example for LinkWall was added in Chapter 20.

A section on configuring the N2H2 Sentian Category Server was added to chapter 21.

A section on installation and configuration of LinkWall was added to Chapter 21.

The CRONTAB example for starting CSP_LIST for SurfControl in Chapter 21 was incorrect. There was an extra asterisk before the command to be executed.

An example of real-time monitoring using RTMonitor was added in Chapter 26.

The PROXY.CFG file, and information relating to it, was updated in Chapter 30.

Third Edition

Changes from Beta 1

This book was on sale in a beta version from November 2003 until April 2004. I have made the following changes in this revision since that version.

- Corrected various typographical errors pointed out to me by readers. (Thanks Karim Kronfli and Cary Stanton!)
- Changed the example for NMAS Client-to-Site Authentication rule to call out 'Logged' instead of 'Password', because setting the value to 'Password' was causing 'Failed receiving server DH public value' errors at the VPN client.
- Updated the installation section with latest patches available as of late April, 2004.
- Added considerable troubleshooting information on BorderManager 3.8 Client-to-Site and Site-to-Site VPN in the Troubleshooting chapter.
- Added installation and troubleshooting tips for iManager 2.0.1 on NetWare 6.0 in the Troubleshooting chapter.
- Updated many sections of the BorderManager 3.8 VPN chapters with some new information.
- Removed the example to send data through the Client-to-Site VPN unencrypted to iFolder. That was a mistake. Choosing unencrypted mode bypasses the VPN entirely, instead of sending it unencrypted through the VPN.
- Removed the statement that NMAS LDAP Client-to-Site VPN won't work over a PAT/NAT connection. Turns out LDAP NAMS authentication to the test server I was using doesn't work with or without PAT/NAT, and I am trying to find out why.
- Added a non-BorderManager Site-to-Site VPN configuration example, using a Linksys VPN router connecting to a BorderManager 3.8 server.
- Added information on connecting to a BorderManager 3.8 VPN server in backwards compatibility mode.
- Added a new PROXY.PAC example.
- Updated the PROXY.CFG file example.
- Updated SurfControl information in various places (Installation & patch sequence, Access Rules, SurfControl sections) for the Service Pack 3 version of SurfControl.

- Updated the RTMonitor information to reflect a newer version.
- Updated LinkWall information
- Changed references to www.caledonia.net to my website to reflect the fact that I am now selling my books directly instead of through Caledonia.
- Added the CFGDUMP.NLM utility into the section on documenting your server.
- Mentioned the VPN schema addition, removal and migration tools (now supplied on the BorderManager 3.8 Product CD) in the Troubleshooting chapter.
- Mentioned the CALLMGR utility (now supplied on the BorderManager 3.8 companion CD) in the Troubleshooting chapter.
- Mentioned the PKTSCAN packet sniffing and capture tool (now supplied on the BorderManager 3.8 companion CD) in the Troubleshooting chapter.

Third Edition, Revision 1

Changes from Third Edition

This book was on sale between April 30 and May 19 before I noticed that I had forgotten to show the Linksys VPN router configuration in the Site-to-Site VPN chapter. I have added those pages into Revision 1.

<This page intentionally left blank. This is to facilitate putting in chapter tabs in a ring binder for double-sided printing. The main chapters should start on an odd-numbered page.>

Index

128-bit..... 224, 225, 236, 243, 500, 789
3DES.....642, 643
3rd party.....631
3rd-party 83, 169, 631, 639, 641
40-bit..... 224, 225, 236, 237, 243
56-bit..... 109, 224, 500, 789
ABEND 1123, 1149
acceleration.....33, 216, 913
Acceleration..... 32, 33, 259, 415, 417, 425, 426, 910, 1094
Access Control Log 881, 894, 896, 906, 933, 934, 1025, 1027, 1048, 1049, 1052, 1053, 1054, 1210
access rule..18, 28, 33, 42, 50, 55, 61, 65, 73, 82, 110, 129, 151, 177, 179, 211, 218, 221, 229, 246, 251, 253, 254, 265, 308, 316, 317, 318, 319, 321, 333, 335, 337, 339, 342, 345, 346, 347, 348, 349, 350, 351, 357, 359, 360, 361, 363, 365, 367, 371, 375, 377, 380, 382, 383, 384, 385, 391, 394, 400, 401, 404, 405, 407, 411, 412, 413, 419, 424, 425, 428, 429, 434, 435, 436, 440, 441, 442, 447, 497, 503, 504, 510, 512, 548, 549, 555, 612, 727, 728, 729, 730, 739, 791, 795, 838, 843, 847, 869, 870, 871, 873, 874, 876, 880, 881, 882, 883, 884, 885, 886, 887, 889, 891, 892, 900, 902, 903, 908, 912, 925, 926, 928, 929, 930, 931, 932, 935, 936, 938, 939, 941, 946, 948, 951, 953, 955, 956, 957, 959, 960, 961, 965, 984, 985, 986, 987, 989, 990, 998, 999, 1025, 1042, 1045, 1047, 1068, 1070, 1090, 1092, 1115, 1117, 1155, 1158, 1209, 1211
Access Rule31, 32, 33, 34, 64, 65, 110, 129, 151, 212, 218, 221, 222, 244, 259, 307, 308, 316, 322, 323, 327, 330, 339, 345, 347, 348, 349, 360, 361, 366, 367, 383, 385, 391, 394, 400, 401, 405, 412, 424, 425, 428, 429, 435, 436, 440, 441, 503, 504, 509, 529, 795, 869, 871, 873, 875, 888, 896, 900, 912, 915, 921, 925, 935, 938, 941, 946, 947, 948, 952, 961, 967, 970, 978, 982, 983, 986, 987, 994, 1049, 1117, 1122, 1158, 1211, 1213
ACK bit filtering.....423
ACLCHECK.....33, 946
ACLDUMP.....21, 1158
ACLDUMP.NLM.....21, 1158
alert..... 783, 1021, 1022, 1023, 1024
Alert..... 1022, 1023, 1024
antivirus 783, 871, 951, 1094
Apache.182, 379, 386, 1126, 1136, 1138, 1139, 1179, 1184, 1206
ARP table.....66, 176, 1008
Audit Log.855, 860, 861, 863, 865, 1034, 1063, 1128, 1131
authentication 27, 29, 32, 65, 177, 188, 191, 192, 193, 199, 218, 220, 221, 222, 223, 226, 227, 229, 243, 244, 246, 250, 251, 252, 253, 254, 268, 269, 270, 271, 299, 300, 316, 319, 321, 322, 323, 330, 332, 416, 419, 424, 429, 435, 436, 440, 441, 444, 446, 475, 477, 515, 524, 525, 527, 528, 529, 530, 533, 534, 548, 549, 553, 554, 642, 717, 719, 727, 729, 734, 766, 768, 769, 770, 791, 796, 803, 804, 805, 806, 807, 808, 814, 821, 838, 848, 850, 853, 870, 871, 889, 903, 906, 951, 955, 956, 957, 958, 960, 982, 1067, 1095, 1104, 1133, 1149, 1150, 1164, 1211, 1213
Authentication19, 29, 31, 33, 155, 218, 219, 220, 221, 224, 229, 236, 243, 244, 249, 250, 251, 252, 253, 298, 316, 317, 318, 319, 322, 323, 325, 326, 330, 332, 434, 435, 441, 442, 443, 515, 524, 525, 529, 549, 629, 642, 643, 719, 764, 765, 766, 767, 768, 803, 807, 826, 838, 840, 842, 846, 847, 871, 885, 889, 1095, 1104, 1133, 1150, 1211, 1213
Authentication Rule 719, 764, 765, 826, 838
BEFSX41 .....21, 549, 642
Blacklist 997
Block Selected Downloads..... 891
BMAS 30, 31
BORDER1 .. 57, 58, 59, 61, 62, 63, 83, 213, 215, 216, 217, 262, 277, 301, 304, 324, 327, 409, 410, 474, 493, 512, 513, 515, 519, 524, 855, 875, 876, 881, 882, 883, 914, 920, 921, 922, 979, 1022
BORDER2 ..... 57, 58, 59, 61, 62, 277, 301, 304, 484, 487, 488, 490, 493, 512, 523, 526, 534, 535
BorderManager 2.1 ... 31, 41, 111, 176, 186, 221, 431, 432, 978
BorderManager 3.0 ... 18, 29, 31, 41, 58, 64, 108, 109, 111, 163, 167, 172, 173, 174, 189, 194, 198, 213, 214, 219, 220, 231, 233, 250, 287, 289, 293, 298, 299, 309, 310, 313, 325, 332, 363, 364, 366, 367, 416, 432, 497, 512, 513, 515, 517, 520, 523, 524, 539, 546, 791, 795, 894, 923, 979, 1021, 1022, 1023, 1069, 1090, 1093, 1119
BorderManager 3.5 ... 58, 64, 102, 104, 106, 111, 163, 172, 184, 187, 193, 214, 219, 220, 234, 250, 251, 264, 289, 293, 299, 300, 310, 311, 313, 322, 326, 332, 342, 348, 363, 365, 367, 368, 378, 408, 512, 523, 526, 533, 539, 544, 924, 929, 990, 992, 1021, 1023, 1024, 1090, 1095, 1113, 1114, 1120, 1121, 1122, 1125, 1148, 1159
BorderManager 3.6 ..... 18, 28, 61, 64, 82, 97, 98, 100, 101, 111, 112, 170, 171, 172, 176, 192, 221, 307, 346, 359, 380, 420, 497, 511, 512, 525, 546, 1094, 1125, 1156, 1209, 1210
BorderManager 3.7 . 19, 20, 23, 29, 30, 31, 33, 37, 61, 64, 67, 82, 83, 89, 91, 93, 94, 95, 96, 97, 99, 100, 101, 102, 103, 105, 106, 110, 140, 142, 145, 147, 148, 149, 150, 157, 162, 165, 166, 168, 169, 170, 171, 172, 181, 182, 184, 191, 192, 195, 200, 201,

202, 205, 207, 209, 224, 246, 250, 251, 252, 255, 304, 307, 311, 346, 352, 353, 355, 416, 425, 429, 447, 448, 497, 498, 546, 722, 727, 855, 860, 935, 961, 962, 963, 964, 975, 986, 990, 994, 1068, 1095, 1118, 1119, 1121, 1122, 1123, 1124, 1125, 1132, 1143, 1150, 1156, 1205, 1211
BorderManager 3.8 . 18, 19, 20, 21, 29, 30, 31, 32, 56, 60, 61, 62, 64, 66, 67, 72, 80, 82, 83, 87, 88, 89, 90, 91, 92, 93, 97, 111, 112, 114, 116, 117, 124, 133, 136, 137, 157, 161, 166, 182, 183, 189, 190, 202, 212, 224, 248, 260, 335, 341, 342, 343, 347, 416, 447, 497, 498, 512, 546, 547, 548, 549, 550, 551, 552, 553, 554, 613, 614, 631, 632, 633, 641, 687, 695, 703, 717, 718, 720, 722, 723, 727, 757, 772, 783, 784, 785, 789, 791, 792, 795, 796, 800, 803, 806, 809, 820, 821, 823, 850, 852, 860, 861, 862, 864, 869, 920, 929, 961, 990, 991, 1060, 1066, 1118, 1119, 1120, 1122, 1123, 1126, 1129, 1130, 1132, 1133, 1137, 1148, 1150, 1156, 1175, 1176, 1192, 1198, 1201, 1205, 1213, 1214
BRDCFG150, 181, 195, 196, 199, 200, 201, 203, 259, 448, 463, 546, 1124
BRDSRV 164, 167, 979
Btrieve 81, 283, 284, 907, 1025, 1031
bug ...89, 91, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 104, 106, 107, 188, 225, 236, 287, 772, 785, 888, 1069, 1070, 1093, 1119, 1120, 1121, 1133, 1134, 1148, 1162, 1163
cable modem... 45, 55, 56, 60, 61, 497, 512, 544, 615, 1211
cache 20, 28, 33, 58, 61, 64, 67, 72, 80, 126, 137, 138, 139, 146, 169, 179, 182, 255, 256, 259, 260, 262, 263, 264, 274, 277, 279, 284, 286, 288, 289, 290, 291, 292, 293, 294, 300, 301, 303, 304, 305, 308, 312, 415, 428, 871, 889, 907, 951, 965, 1035, 1045, 1047, 1068, 1069, 1070, 1071, 1073, 1075, 1076, 1082, 1084, 1085, 1086, 1098, 1103, 1120, 1143, 1144, 1145, 1146, 1150, 1163, 1164, 1169
Cache80, 126, 137, 139, 275, 276, 277, 278, 279, 285, 286, 288, 293, 300, 301, 303, 304, 305, 907, 973, 1033, 1034, 1035, 1039, 1071, 1075, 1082, 1084, 1085, 1097, 1098, 1143, 1144, 1145, 1148
Cache Aging 285
cache control.....286
Cache Hash Table 286, 1145
cache hierarchy . 58, 61, 279, 300, 301, 303, 304, 305, 871, 889, 951, 965, 1073, 1086
cache location 169, 288, 289
CALLMGR.....185, 1129, 1214
CERN...32, 58, 59, 277, 300, 301, 302, 303, 304, 305, 981, 1073, 1084, 1085, 1086, 1101
Certificate Authentication..... 768, 820, 838, 841, 843
CFGDUMP.NLM 21, 1130, 1156, 1214
CFM.....291
Chat.....925
Cisco VPN 548
Citrix..... 250, 251, 1049, 1163
clear cache 377, 407
Client-to-Site VPN..... 18, 21, 28, 32, 55, 59, 64, 172, 173, 176, 181, 201, 448, 452, 474, 497, 498, 499, 501, 502, 504, 505, 507, 509, 510, 511, 512, 515, 519, 521, 523, 533, 534, 536, 537, 538, 539, 540, 544, 546, 548, 554, 562, 717, 720, 721, 722, 771, 772, 776, 777, 780, 782, 783, 784, 791, 794, 795, 796, 804, 838, 850, 869, 873, 920, 922, 1124, 1133, 1135, 1162, 1209, 1210, 1211, 1213
CLNTRUST 19, 108, 109, 218, 219, 220, 221, 224, 226, 227, 228, 229, 245, 249, 250, 251, 322, 326, 372, 432, 435, 436, 517, 871, 887, 951, 1095, 1164
common log. 73, 280, 281, 282, 436, 907, 1028, 1040, 1045
Common log..... 280, 281, 434, 443, 888, 1028, 1029
Companion CD . 87, 88, 90, 91, 92, 93, 157, 552, 718, 1129, 1137, 1175, 1176, 1201
config.txt 1156, 1157, 1158
CONLOG..... 1116
ConsoleOne..... 73, 182, 225, 230, 233, 234, 236, 526, 547, 553, 554, 563, 566, 576, 588, 591, 594, 614, 619, 622, 623, 647, 648, 654, 656, 659, 670, 672, 681, 684, 685, 687, 703, 803, 804, 821, 827
CP_SETUP.EXE.....104, 105, 107, 962, 978, 979
CPFILTER..... 29, 164, 166, 945, 961, 963, 964, 965, 968, 969, 972, 973, 975, 978, 979, 980, 981
CRON 183, 184, 972, 974
CRONTAB 183, 184, 974, 1212
CSAUDIT 81, 284, 860, 1025, 1128, 1131
CSLIB 81, 283, 907, 1025
CSP_LIST .. 969, 972, 973, 974, 975, 976, 1119, 1212
CSPCONFIG.INI 965, 966, 973
custom error page.....169, 1003, 1005, 1006
CuteFTP 330, 331
CyberNOT..... 884, 894, 942, 943, 944, 945, 978, 979, 981, 1049, 1051
CyberPatrol 29, 64, 104, 105, 107, 108, 109, 110, 136, 148, 164, 883, 884, 894, 895, 899, 936, 942, 943, 944, 945, 956, 961, 962, 964, 972, 973, 978, 979, 980, 981, 994, 1003, 1049, 1050
CyberYES 978, 979
DEBUG.....74, 1116, 1117
default filters 200, 202, 354, 546, 1124
default gateway . 36, 42, 44, 47, 49, 63, 149, 178, 217, 377, 407, 501, 536, 537, 538, 722, 1117, 1170
default route 36, 37, 44, 47, 49, 58, 59, 62, 64, 66, 73, 74, 75, 78, 178, 179, 183, 308, 536, 537, 552, 616, 723, 800, 1117, 1135
Default route 178
default rule 65, 244, 351, 631, 632, 633, 638, 639, 641, 727, 730, 870, 875, 880, 933
Default rule 759
DES..... 643
DHCP..... 45, 46, 58, 60, 375, 543, 906, 951, 1165
digest..... 462, 475, 477, 478, 479, 487, 491, 502, 503, 524
DMZ.....46, 51, 53, 614, 615, 618
DNS 28, 32, 33, 34, 38, 39, 41, 42, 58, 62, 73, 74, 75, 79, 130, 132, 152, 153, 178, 183, 200, 203, 255, 256, 260, 261, 262, 263, 264, 266, 293, 302, 304, 308, 317, 318, 324, 327, 330, 339, 342, 352, 359, 363, 373, 374, 375, 390, 393, 394, 408, 410, 411,

542, 549, 717, 719, 770, 771, 772, 773, 802, 875, 934, 1010, 1011, 1012, 1016, 1022, 1070, 1074, 1082, 1083, 1099, 1115, 1120, 1122, 1123, 1133, 1134, 1144, 1168
DNS Proxy...28, 32, 39, 256, 262, 373, 374, 375, 772, 1123
DNS/SLP 719, 770, 771
do not cache 291
Domain 38, 79, 302, 339, 340, 341, 342, 350, 358, 1150
dynamic NAT 31, 36, 42, 46, 61, 64, 66, 153, 164, 263, 321, 344, 373, 501, 515, 537, 538, 539, 544, 552, 614, 615, 617, 869, 915, 1007, 1008, 1009, 1010, 1013, 1016, 1117, 1125
Dynamic NAT 32, 42, 73, 263, 321, 392, 421, 539, 1007, 1008, 1009, 1010, 1013, 1016, 1170
Effective Rules..... 244, 870, 875, 876, 879, 880
emFrame 205
Enforce Rules..... 259, 873, 1117
Enhancement Pack 102, 187
error page 424, 1003
Ethernet..... 67, 512
extended log..... 281, 282
Extended log 281, 282, 1031
Extended Log..... 282, 1031
Extended Logging..... 282
FILTCFG 30, 33, 89, 91, 92, 94, 96, 110, 162, 181, 182, 196, 198, 205, 207, 208, 336, 352, 354, 387, 420, 421, 1118, 1157
filter exception .. 20, 31, 39, 41, 42, 45, 48, 51, 52, 53, 60, 64, 65, 66, 75, 89, 91, 92, 94, 96, 110, 111, 125, 128, 150, 153, 162, 179, 181, 184, 195, 196, 198, 200, 201, 202, 203, 207, 208, 209, 228, 260, 263, 307, 321, 336, 337, 340, 344, 345, 346, 352, 353, 354, 355, 359, 373, 377, 380, 382, 384, 387, 388, 389, 392, 404, 407, 413, 416, 420, 421, 424, 425, 428, 444, 447, 546, 555, 869, 915, 917, 953, 982, 984, 985, 1007, 1008, 1009, 1010, 1011, 1012, 1013, 1014, 1015, 1016, 1017, 1018, 1019, 1020, 1088, 1116, 1119, 1121, 1123, 1131, 1155, 1157, 1170, 1171
FilterConfiguration 206, 207, 1205
Filtering 27, 31, 102, 195, 205, 389, 421, 501, 515, 896, 915, 938, 986, 997, 1008, 1009, 1116, 1118, 1128, 1205
filters 30, 33, 34, 39, 45, 51, 52, 64, 65, 74, 82, 83, 89, 91, 92, 94, 96, 110, 149, 162, 181, 182, 184, 195, 196, 199, 200, 202, 203, 208, 227, 259, 265, 307, 420, 453, 463, 464, 538, 549, 938, 1021, 1116, 1117, 1128, 1131, 1157, 1205
FILTERS.CFG 30, 33, 162, 181, 184, 205, 1157, 1170
FILTSRV .89, 91, 92, 94, 96, 110, 162, 200, 202, 207, 1119
FILTSRV MIGRATE 89, 91, 92, 94, 96, 110, 162, 200, 202, 207, 1119
firewall.....27, 29, 30, 34, 39, 50, 51, 53, 61, 195, 216, 300, 316, 332, 783, 833, 984, 1015, 1163, 1170
Firewall..... 27, 30, 32, 51, 53, 124, 172, 783, 1170
frequency 976
FTP..... 28, 32, 33, 44, 48, 49, 52, 55, 58, 64, 65, 126, 146, 200, 203, 218, 219, 221, 229, 267, 268, 270, 271, 283, 286, 288, 298, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 332, 333, 425, 426, 427, 428, 511, 870, 892, 910, 911, 912, 1015, 1080, 1102, 1209
FTP Acceleration 425, 426, 428, 910
FTP proxy 203
FTP Proxy 28, 32, 49, 65, 218, 219, 221, 268, 270, 271, 283, 298, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 332, 333, 425, 428, 870, 910, 912, 1209
FTP-PORT-PASV-ST 200
Generic Proxy 381, 384, 387, 391, 393, 399, 401, 405, 913, 918, 919, 1105
generic TCP proxy 401, 918, 919
Generic TCP Proxy . 20, 377, 378, 379, 381, 383, 384, 385, 386, 390, 392, 397, 398, 404, 405, 412, 913, 1122
Generic UDP Proxy..... 380, 404, 407, 408, 409, 410, 411, 412, 914
GroupWise 23, 61, 187, 336, 339, 344
GWIA.....336, 344
hierarchy .. 275, 279, 300, 301, 303, 1073, 1084, 1101
HOSTNAME 183
HOSTS..... 38, 39, 176, 183, 256, 261, 262, 263, 264, 304, 324, 327, 373, 374, 419, 541, 542, 544, 545, 1082, 1124, 1144, 1163, 1210
hot nodes 286, 1070, 1145
HTTP Proxy .. 32, 41, 49, 50, 61, 64, 65, 80, 126, 137, 139, 146, 169, 178, 201, 203, 204, 216, 218, 229, 244, 251, 256, 258, 259, 260, 261, 262, 263, 264, 265, 266, 268, 270, 271, 273, 274, 277, 283, 285, 287, 289, 297, 298, 299, 300, 301, 304, 305, 307, 308, 312, 368, 369, 370, 371, 372, 373, 436, 439, 870, 871, 885, 891, 907, 909, 912, 934, 951, 955, 981, 982, 984, 985, 1044, 1050, 1074, 1075, 1076, 1077, 1078, 1079, 1080, 1081, 1082, 1089, 1098, 1099, 1103, 1120, 1121, 1122, 1139, 1147, 1148, 1159, 1160, 1161, 1164, 1166, 1211
https..... 203, 205, 975, 1138, 1139, 1186, 1187, 1197
HTTPS 50, 157, 199, 201, 250, 260, 268, 270, 271, 307, 390, 415, 416, 418, 420, 422, 892, 975, 1121, 1148
ICMP..... 65, 536
ICP 32, 300, 301, 302, 303, 1073, 1086, 1101
IKE.. 29, 166, 202, 447, 497, 547, 548, 549, 615, 641, 642, 850, 1060, 1066, 1127, 1129, 1130, 1131, 1132, 1135
IKE-st..... 202
iManager 18, 20, 21, 30, 32, 33, 62, 63, 87, 88, 89, 91, 92, 93, 94, 96, 110, 116, 124, 133, 145, 157, 162, 172, 181, 182, 184, 202, 205, 206, 207, 208, 379, 380, 384, 385, 386, 447, 497, 547, 549, 552, 553, 554, 556, 561, 566, 567, 571, 575, 576, 580, 581, 585, 588, 589, 591, 594, 598, 599, 610, 620, 628, 647, 654, 655, 659, 660, 670, 672, 681, 682, 684, 687, 717, 718, 720, 724, 764, 777, 791, 795, 803, 804, 821, 827, 837, 838, 839, 869, 919, 1118, 1126, 1136, 1137, 1138, 1139, 1175, 1176, 1177,

1184, 1185, 1188, 1189, 1190, 1191, 1195, 1196, 1197, 1198, 1199, 1203, 1205, 1206, 1213
indexed log....283, 1045, 1148
Indexed Logging....283, 1035
INETCFG 34, 37, 39, 40, 41, 42, 74, 75, 79, 88, 90, 92, 102, 112, 123, 124, 130, 131, 149, 164, 177, 181, 183, 184, 262, 263, 321, 421, 431, 453, 476, 515, 1007, 1008, 1009, 1117, 1126, 1134, 1157, 1158, 1170
Internet Explorer... 157, 205, 250, 251, 266, 368, 372, 860, 976, 1004, 1041, 1159, 1161, 1164, 1165, 1168
Internic....35
IPFLT..74, 103, 110, 162, 224, 969, 1116, 1131, 1157
IPFLT31.NLM....103, 1116
IPSec.... 497, 547, 548, 1130, 1132
JAVA.... 84, 85, 86, 182, 1138, 1176, 1179
Java Applet Stripping....274
LDAP.....87, 133, 549, 719, 727, 729, 734, 762, 769, 770, 803, 804, 805, 806, 807, 808, 809, 810, 811, 814, 815, 816, 817, 818, 1126, 1133, 1137, 1139, 1175, 1176, 1182, 1188, 1190, 1191, 1192, 1206, 1213
LDAP Configuration..... 719, 769, 770, 803, 804, 816, 1133
license 29, 68, 116, 145, 157, 159, 168, 172, 173, 174, 175, 945, 962, 968, 1178, 1193
Linksys.21, 61, 62, 454, 548, 549, 551, 552, 614, 615, 616, 617, 618, 624, 628, 629, 630, 632, 635, 638, 639, 641, 642, 643, 644, 645, 646, 1213, 1215
LinkWall....19, 29, 105, 107, 169, 895, 899, 900, 901, 902, 903, 908, 909, 935, 938, 939, 940, 941, 961, 990, 991, 994, 995, 996, 997, 998, 999, 1000, 1001, 1044, 1211, 1212, 1214
LINKWALL.LST 940, 994, 995, 996, 997
Linux 24, 29, 60, 61, 84, 300, 548, 871, 951, 957, 982, 983, 985, 1021
LOAD PROXY –CC 292, 293, 1120
Local Secure Group 642
log....20, 33, 65, 80, 81, 118, 133, 169, 177, 223, 226, 229, 249, 251, 280, 281, 282, 283, 284, 307, 391, 416, 425, 509, 511, 519, 520, 534, 535, 539, 540, 545, 546, 589, 771, 772, 783, 785, 791, 796, 799, 819, 820, 855, 856, 865, 870, 882, 888, 897, 907, 933, 934, 942, 960, 975, 1021, 1025, 1028, 1029, 1031, 1035, 1045, 1046, 1047, 1049, 1052, 1053, 1054, 1070, 1121, 1124, 1128, 1131, 1136, 1137, 1138, 1139, 1141, 1169, 1174, 1196, 1197, 1203, 1206
Logger screen....94
logging...32, 65, 97, 99, 100, 101, 103, 105, 106, 218, 281, 283, 290, 291, 317, 319, 351, 364, 375, 409, 434, 443, 512, 536, 556, 567, 660, 772, 783, 799, 821, 827, 870, 882, 888, 907, 908, 933, 994, 995, 1000, 1021, 1034, 1045, 1049, 1052, 1124, 1148
Logging....81, 280, 281, 282, 283, 307, 435, 436, 509, 783, 888, 891, 894, 896, 906, 921, 933, 934, 939, 942, 960, 1025, 1049, 1121, 1174
loopback....272
Loopback 183
Mail Proxy 19, 20, 30, 32, 44, 48, 64, 73, 128, 150, 201, 202, 203, 335, 336, 337, 338, 339, 340, 342, 343, 344, 345, 346, 347, 348, 349, 351, 352, 353, 355, 929, 930, 931, 932, 1088, 1091, 1122, 1147, 1148, 1150, 1211
Maximum Number of Hot Nodes....286, 1145
MD5 ....642, 643
memory leak.... 1072
Microsystems 944, 979
MLA license....65, 174, 175
Mozilla 268, 269
multicast....539, 1141
N2H229, 895, 899, 900, 935, 936, 937, 938, 941, 943, 956, 961, 982, 983, 984, 985, 987, 988, 989, 990, 994, 1211, 1212
Nat.... 1015
NAT 28, 36, 41, 42, 46, 48, 62, 64, 66, 88, 90, 92, 94, 95, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 153, 164, 179, 201, 202, 216, 336, 421, 497, 512, 515, 538, 539, 546, 548, 562, 580, 586, 614, 615, 617, 625, 719, 772, 915, 1007, 1008, 1009, 1015, 1016, 1018, 1116, 1117, 1125, 1133, 1134, 1163, 1170, 1210, 1213
NBM Access Management.....206, 207, 1118, 1205
NBMRuleContainer 83, 1118, 1211
NDS-based rule 219, 222, 870, 871
NETDB 1143, 1144
NETINFO.CFG....181, 184, 474, 1117, 1156
NETINFO.CHK 184
Netscape 157, 245, 250, 251, 271, 272, 372, 386, 976, 1004, 1161, 1165, 1168
NetWare 4.11 34, 58, 67, 72, 101, 106, 108, 164, 168, 174, 194, 212, 215, 231, 233, 430, 536, 1123
NetWare 4.2 181
NetWare 5.0 58, 61, 84, 100, 104, 108, 193, 230, 231, 432
NetWare 5.1 29, 61, 62, 71, 72, 81, 82, 85, 92, 95, 98, 102, 108, 111, 137, 167, 182, 188, 189, 192, 217, 225, 230, 231, 233, 234, 387, 552, 614, 1009, 1130, 1132, 1175
NetWare 6 ... 20, 29, 40, 41, 62, 72, 73, 75, 80, 81, 84, 88, 90, 91, 93, 94, 97, 100, 103, 105, 106, 111, 112, 124, 126, 133, 137, 140, 143, 157, 164, 165, 172, 182, 189, 191, 202, 205, 209, 212, 221, 380, 386, 411, 551, 552, 580, 703, 717, 974, 991, 1119, 1136, 1137, 1138, 1142, 1145, 1175, 1176, 1192, 1207, 1213
NetWare 6.5 20, 29, 40, 41, 62, 72, 75, 80, 84, 88, 91, 93, 111, 124, 126, 133, 137, 182, 189, 212, 221, 380, 551, 552, 580, 703, 717, 974, 991, 1175, 1207
NetWare Connect 31
Network Address Translation....28, 35, 36
News Proxy 32, 150, 200, 357, 358, 359, 360, 361, 392, 393, 925, 926, 927, 928
NIAS . 27, 29, 31, 73, 97, 98, 100, 101, 181, 430, 449, 1129
NIASCFG 31, 181, 449, 450, 466
NICI 87, 88, 90, 92, 104, 108, 112, 175, 224, 703, 789, 1130, 1132

NIST 409
njclv2.jar 1137
NLS..66, 143, 163, 164, 167, 168, 169, 172, 173, 174, 189
NLS Licenses 172
NLSFLAIM 165, 167
NLSLSP 165, 172, 174
NMAS Authentication 768, 795, 796, 1133
NMAS/LDAP 803, 815
NNTP.24, 32, 35, 58, 64, 79, 198, 200, 357, 358, 359, 360, 361, 378, 379, 380, 392, 393, 394, 395, 403, 925, 928, 1013, 1014, 1109
non-cachable 1076
Notes 167
Novell Client Firewall.....21, 29, 30, 783, 784
Novell Public Forums 35, 87
Novell Remote Manager. 20, 183, 380, 381, 383, 549, 597, 860, 861, 918, 1060, 1066, 1128, 1129, 1131, 1136
NRM 183, 381, 549, 862, 1128
NTP 164, 409, 410
NWADMIN 875, 1022
NWHOST 540, 541, 542, 1210
OFA 1164
OFM 1164
Open File Manager 1164
Outbound DNS 1010
PASV 268, 270, 271, 321, 425
PASV FTP 268, 270, 271, 321
patches ...18, 20, 21, 34, 87, 88, 90, 92, 94, 95, 98, 99, 100, 101, 102, 103, 104, 105, 107, 108, 109, 115, 117, 144, 163, 167, 172, 174, 180, 186, 187, 191, 201, 212, 224, 250, 255, 260, 287, 293, 307, 313, 322, 326, 335, 336, 337, 341, 342, 347, 425, 757, 769, 772, 896, 929, 978, 1069, 1093, 1094, 1119, 1120, 1121, 1122, 1123, 1124, 1130, 1132, 1141, 1143, 1147, 1148, 1156, 1158, 1162, 1209, 1213
Patches 87, 186
pattern matching 1094
pcANYWHERE..... 46, 377, 380, 404, 405, 407, 412, 413, 915, 917, 1209
Perfect Forward Secrecy 562, 642
Phase 1 643
Phase 2 643
PING 65, 74, 453, 1115
POP3..28, 58, 128, 201, 217, 335, 336, 337, 338, 339, 340, 341, 344, 345, 346, 348, 354, 355, 932, 1108, 1211
pornography 940, 960, 961, 990
port 110 .....201, 345, 354, 932
port 119 .....200, 359, 380, 392, 394, 400, 1013, 1014
port 123...217, 380, 388, 389, 390, 391, 409, 410, 913
port 12345 ..... 217, 380, 388, 389, 390, 391, 913
port 20 .....448, 546
port 2010 .....448, 546
port 21 ..... 49, 198, 425, 427, 448, 1131
port 213 .....198, 448, 1131
port 22 ..... 380, 384, 385, 386, 404, 915, 919, 1136
port 2200 .....380, 384, 385, 386, 919, 1136
port 23 .....201, 313, 315
port 25 ..... 201, 349, 1017, 1019, 1020, 1122, 1148
port 353 .....199, 201, 448, 546
port 37 .....409, 410, 914
port 389 .....1137, 1191
port 443 ... 50, 199, 201, 203, 221, 311, 418, 423, 755, 1179
port 53 .....39, 200, 373, 375, 1010, 1011, 1012
port 554 .....201, 372
port 5631 .....404, 915, 917
port 5632 .....380, 404, 915, 916, 917
port 636 1188
port 7070 .....201, 368
port 8049, 50, 199, 201, 203, 216, 245, 259, 260, 273, 277, 300, 307, 308, 311, 369, 381, 382, 418, 420, 423, 435, 612, 753, 754, 808, 871, 975, 981, 984, 985, 1139, 1161, 1209
port 8008 381
port 8009 .....381, 382, 975
port 8080. 50, 245, 259, 273, 277, 300, 369, 435, 981, 985, 1139, 1161, 1209
port 9090 372
Portal 183, 1187, 1190, 1209
ports 1024-65535 448
PPPoE 45
PPTP 1159
private interface..... 41, 43, 45, 57, 61, 62, 63, 67, 149, 177, 178, 196, 199, 203, 308, 321, 453, 538, 915, 1011, 1012, 1013, 1014
private IP address 35, 36, 39, 41, 44, 47, 49, 61, 62, 63, 103, 157, 168, 178, 179, 199, 203, 205, 215, 217, 239, 245, 265, 271, 311, 324, 327, 330, 339, 357, 358, 373, 375, 380, 392, 416, 425, 453, 454, 502, 537, 539, 541, 544, 551, 552, 717, 772, 835, 861, 914, 975, 1125, 1132, 1134, 1139, 1160, 1170, 1172, 1211
protocol 57 .....199, 512
Protocol 57 201
Proxy authentication..... 218, 250, 415, 951, 952, 959, 1149
Proxy Authentication 19, 33, 182, 218, 219, 220, 221, 222, 223, 224, 225, 226, 229, 234, 236, 242, 243, 244, 245, 246, 248, 249, 250, 251, 252, 253, 259, 269, 271, 307, 316, 372, 419, 422, 424, 869, 870, 871, 875, 881, 887, 888, 906, 951, 960, 984, 1043, 1045, 1049, 1095, 1163, 1164, 1174
PROXY Performance Tuning 287
PROXY.CFG .. 19, 64, 89, 91, 93, 95, 96, 98, 99, 101, 104, 106, 107, 128, 184, 186, 250, 252, 253, 260, 300, 311, 339, 342, 343, 347, 348, 415, 424, 929, 931, 1005, 1071, 1094, 1095, 1120, 1121, 1122, 1147, 1148, 1212, 1213
proxy.pac.....20, 1165
PROXY.PAC 266, 267, 1161, 1164, 1165, 1166, 1167, 1168, 1213
public interface.. 35, 41, 43, 44, 45, 48, 49, 52, 57, 58, 61, 65, 77, 149, 177, 195, 196, 198, 199, 200, 321,

387, 431, 453, 476, 515, 1011, 1012, 1013, 1014, 1015, 1021
Public interface 388, 389
public IP address35, 36, 38, 39, 41, 44, 46, 48, 49, 58, 60, 66, 73, 178, 179, 196, 198, 199, 200, 201, 203, 215, 216, 217, 227, 228, 259, 307, 335, 336, 340, 345, 346, 347, 352, 354, 359, 377, 379, 380, 381, 382, 384, 386, 387, 388, 389, 404, 405, 407, 412, 413, 415, 416, 420, 425, 427, 428, 448, 453, 454, 455, 468, 476, 497, 498, 523, 536, 538, 546, 551, 552, 555, 562, 580, 586, 596, 602, 614, 618, 625, 635, 638, 642, 718, 793, 797, 816, 913, 915, 916, 917, 1007, 1010, 1013, 1015, 1016, 1018, 1117, 1121, 1122, 1125, 1128, 1132, 1163, 1170
Public IP address.....38, 216, 307, 562
Public IP Address..... 43, 48, 416, 420, 453, 476
PXYERR.HTM..... 1003, 1004, 1005, 1006
PXYHOSTS.... 261, 262, 264, 293, 1070, 1082, 1120, 1144
RADIUS 27, 30, 31, 32, 64, 73, 102, 103, 105, 106, 108, 109, 122, 155, 164, 167, 169, 529
RAM 30, 66, 67, 259, 285, 945, 964, 965, 972, 973, 1045, 1047, 1070, 1071, 1072, 1119, 1134, 1143
RCONJ.....83, 86
RDATE.....164, 409, 411, 914
read-ahead..... 287, 888, 1069, 1070, 1120
Real Audio ... 213, 214, 363, 364, 365, 366, 367, 1092
RealAudio 28, 103, 105, 106, 201, 203, 363, 364, 366, 367, 368, 371, 372, 923, 924, 1106, 1114
RealAudio Proxy.....364, 366, 923, 924
RealPlayer G2 372
real-time.....468, 472, 855, 857, 859, 900, 1040, 1062, 1212
REGEDIT 1159, 1160, 1164
REGISTER.EXE..... 945, 968, 979, 980, 981
Remote Manager.....975, 976, 1129
Remote Secure Group 642
Reverse Proxy..... 32, 33, 59, 415, 417, 418, 420, 424, 885, 910, 911, 1015, 1094, 1151
reverse proxy acceleration 44, 46, 48, 58, 262, 386, 416, 420, 1007
Reverse Proxy Acceleration..... 32, 33, 415, 417, 420, 424, 1094
Rollover 280
routing..36, 37, 41, 42, 54, 61, 62, 64, 65, 74, 75, 183, 185, 196, 256, 279, 305, 308, 392, 452, 453, 499, 501, 515, 536, 537, 538, 547, 548, 629, 717, 722, 869, 1116, 1117, 1128
RTMonitor 20, 900, 990, 1040, 1041, 1042, 1043, 1044, 1045, 1046, 1047, 1212, 1214
RTSP.....103, 105, 106, 201, 203, 213, 214, 363, 365, 367, 368, 370, 371, 372, 923, 924, 1090, 1114
rule hit logging..... 888, 942, 1049
Rule Inheritance.....870
scheduled download..... 294, 295, 296, 1112
Scheduled Tasks 972, 975
schema extension 133, 168, 1129
secondary IP address..... 40, 41, 49, 62, 164, 165, 177, 178, 179, 198, 208, 215, 216, 217, 228, 311, 387, 393, 416, 420, 421, 422, 423, 757, 772, 915, 1007, 1015, 1088, 1141, 1170
Secondary IP address 40, 217
security.. 27, 36, 37, 53, 221, 231, 243, 274, 373, 377, 389, 407, 423, 429, 430, 440, 462, 497, 500, 642, 703, 759, 800, 817, 848, 854, 976, 1015
Security . 229, 230, 231, 233, 245, 269, 271, 500, 526, 783, 858, 1063
Sentian..... 29, 936, 937, 943, 961, 982, 983, 984, 985, 987, 988, 1212
serial number.....969, 979, 1156
Service Type 208, 529
SET FILTER DEBUG=ON 1116
SET TCP IP DEBUG 74, 536, 1116, 1117
SHA 643
Shared Secret.....642, 850
Single Sign On220, 221, 243, 322, 326, 434, 442, 443
Site-to-Site VPN 21, 28, 32, 54, 58, 59, 61, 62, 63, 65, 66, 83, 163, 164, 165, 166, 172, 173, 176, 179, 181, 183, 277, 447, 449, 452, 453, 461, 465, 474, 493, 498, 500, 501, 502, 538, 539, 547, 549, 551, 552, 553, 554, 567, 569, 572, 580, 588, 597, 598, 599, 609, 610, 612, 628, 629, 630, 637, 641, 642, 648, 672, 687, 703, 719, 720, 722, 803, 841, 850, 855, 862, 864, 1123, 1124, 1126, 1127, 1128, 1129, 1130, 1131, 1135, 1213, 1215
SKIP..... 199, 201, 203, 448, 495, 497, 512, 548, 855, 1135
SLP 512, 519, 539, 540, 542, 549, 717, 719, 771, 772, 773, 774, 1124, 1133, 1134, 1142, 1210
smtp.....202, 1150
SMTP 28, 48, 58, 79, 128, 198, 201, 217, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 347, 348, 349, 350, 351, 352, 353, 355, 929, 930, 931, 932, 1016, 1017, 1018, 1019, 1020, 1021, 1024, 1107, 1122, 1148, 1209
snapins91, 93, 104, 105, 107, 124, 133, 168, 182, 189, 190, 191, 192, 193, 194, 212, 230, 526, 527, 703, 717, 1175, 1190, 1197, 1198, 1205
Snapins.....124, 1197
SOCKS..... 28, 32, 268, 270, 271, 297, 298, 299, 429, 444, 445, 446, 1067, 1089, 1110
SOCKS Client.....32, 297, 298, 1089, 1110
SOCKS Server 32
Software Virtual Server.....307, 1122
Squidguard Blacklist 940, 990, 996
SSL.. 19, 133, 182, 199, 201, 218, 220, 221, 222, 223, 224, 225, 226, 229, 234, 236, 242, 243, 244, 245, 246, 248, 249, 250, 251, 252, 253, 268, 269, 270, 271, 307, 390, 415, 418, 419, 420, 422, 424, 446, 861, 871, 887, 892, 951, 1095, 1121, 1126, 1131, 1148, 1149, 1163, 1164, 1172, 1191
SSO 221, 229, 429, 435, 436, 440, 441, 1172
STARTVPN... 597, 719, 814, 1126, 1128, 1130, 1133
STARTX..... 84, 85, 88, 90, 92, 94, 95, 112, 140
Stateful 39
stateful filtering.....200, 1131
static NAT ... 39, 44, 46, 49, 51, 58, 66, 102, 110, 164, 165, 178, 179, 184, 208, 216, 217, 307, 311, 335,

336, 377, 380, 407, 420, 421, 425, 539, 544, 549, 562, 586, 614, 615, 618, 624, 625, 717, 772, 915, 1015, 1016, 1017, 1018, 1019, 1020, 1117, 1125, 1170, 1211
Static NAT 31, 32, 46, 48, 59, 66, 217, 380, 415, 1015, 1016, 1163
static route....46, 63, 78, 110, 183, 469, 493, 550, 722, 723, 800, 806, 1135
statistics .227, 329, 333, 371, 400, 402, 410, 518, 522, 800, 801, 1039, 1069, 1070, 1071, 1073, 1074, 1075, 1076, 1077, 1078, 1079, 1080, 1081, 1082, 1085, 1086, 1089, 1090, 1092, 1093
STOPVPN 597, 719, 814, 1129, 1130, 1132, 1133
SurfControl 20, 29, 30, 64, 67, 89, 91, 93, 95, 96, 105, 107, 110, 136, 148, 166, 169, 182, 183, 184, 308, 875, 881, 894, 895, 896, 897, 898, 899, 900, 902, 903, 905, 907, 909, 935, 936, 938, 941, 943, 945, 951, 953, 956, 957, 958, 960, 961, 962, 963, 964, 965, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 978, 982, 985, 986, 990, 994, 1118, 1119, 1143, 1212, 1213
TaskMaster 976
TCPCON 37, 74, 185, 1117, 1136
TCPIP.CFG.....181, 184
telnet 203
Telnet 176
TELNET 32, 33, 65, 201, 219, 220, 221, 309, 310, 313, 314, 315, 316, 317, 318, 319, 912, 1113
Terminal Server 250, 251, 252, 1095
TID 66, 81, 87, 88, 175, 186, 189, 284, 286, 342, 348, 516, 525, 757, 907, 974, 1003, 1119, 1120, 1136, 1137, 1143, 1144, 1147, 1148, 1159, 1165
time server 164, 914
timeout 169, 229, 249, 256, 257, 858
Tomcat 182, 1136, 1137, 1139, 1175, 1179, 1183, 1184, 1185, 1186, 1196, 1203, 1205, 1206
Traffic Rule..... 21, 611, 612, 613, 630, 631, 632, 634, 639, 718, 727, 731, 739, 740, 746, 750, 756, 759, 761, 764, 765, 795, 802, 805, 806, 807, 808, 809, 814, 818, 838, 841, 844, 1133, 1135
Transparent HTTP Proxy 20, 126, 146, 201, 307, 310, 311, 1121
transparent proxy.....307, 308, 435, 1211
Transparent Proxy ... 32, 229, 260, 261, 265, 307, 308, 309, 310, 311, 312, 314, 374, 429, 432, 440, 441, 984, 1050, 1069, 1093, 1121, 1122, 1148, 1159, 1211
Transparent Telnet Proxy 201, 203, 219
transport 256, 497, 1099, 1123
Transport 34, 255, 256, 257
troubleshooting.. 19, 21, 169, 174, 452, 515, 549, 658, 802, 850, 873, 882, 1068, 1079, 1090, 1115, 1128, 1129, 1130, 1136, 1156, 1209, 1213
tuning 81, 1143
UINSTALL 88, 1120
uninstall.....99, 102, 103, 1119, 1132
Unknown System Error 1137
unload 79, 85, 169, 177, 180, 200, 287, 963, 972, 973, 994, 1082, 1116, 1141, 1148, 1150, 1156, 1170
URL Pattern 292
Usage Trends.....1038, 1053
virtual IPX network number..... 499
VNC 46, 377
VPMASTER 164, 166, 167, 474
VPN over NAT 546, 1209
VPN.NPM 1198, 1201
VPNCFG181, 224, 447, 449, 450, 455, 459, 461, 462, 463, 464, 465, 466, 467, 474, 475, 476, 487, 491, 497, 502, 553, 795, 1135, 1157, 1158
VPNRegClean.exe 21, 1132
VPSLAVE.....164, 166, 167, 474
VPTUNNEL.....196, 197, 203, 1126
VREPAIR 138, 289, 290, 1146
WAN Call Directory 1126
Warning..... 1120
Web Manager 217, 379, 380, 386, 387, 388, 389, 390, 391, 913, 1209
Webspy 281, 1028, 1031
Webtrends 20
www.yahoo.com 881, 882, 883, 884
XMGR..... 1134
ZENworks . 226, 272, 430, 431, 440, 535, 1159, 1161, 1164