

Novell BorderManager®

3.8.2

July 26, 2004

INSTALLATION AND ADMINISTRATION
GUIDE

www.novell.com



Novell®

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

Copyright © 1997-1998, 2001, 2002-2003, 2004 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

U.S. Patent No. 5,349,642; 5,572,528; 5,608,903; 5,671,414; 5,677,851; 5,719,786; 5,758,069; 5,758,344; 5,781,724; 5,784,560; 5,818,936; 5,828,882; 5,832,275; 5,832,483; 5,832,487; 5,870,561; 5,870,739; 5,873,079; 5,878,415; 5,884,304; 5,913,025; 5,933,503; 5,933,826; 5,946,467; 5,956,718; 5,983,234; 5,991,810; 6,016,499; 6,029,247; 6,061,740; 6,065,017; 6,081,900; 6,092,200; 6,105,062; 6,105,132; 6,108,649; 6,112,228; 6,115,039; 6,119,122; 6,167,393; 6,219,676; 6,275,819; 6,286,010; 6,308,181; 6,330,605; 6,345,266; 6,345,266; 6,424,976; 6,459,809; 6,519,610; 6,539,381; 6,542,967; 6,578,035; 6,615,350; 6,629,132. Patents Pending.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.

www.novell.com

Novell BorderManager 3.8.2 Installation and Administration Guide
[July 26, 2004](#)

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

BorderManager is a registered trademark of Novell, Inc. in the United States and other countries.

Client32 is a trademark of Novell, Inc.

ConsoleOne is a registered trademark of Novell, Inc. in the United States and other countries

DirXML is a registered trademark of Novell, Inc. in the United States and other countries

eDirectory is a trademark of Novell, Inc.

Internetwork Packet Exchange and IPX are trademarks of Novell, Inc.

LANalyzer is a registered trademark of Novell, Inc. in the United States and other countries

NCP is a trademark of Novell, Inc.

NDS is a registered trademark of Novell, Inc. in the United States and other countries

NetWare is a registered trademark of Novell, Inc. in the United States and other countries.

NMAS is a trademark of Novell, Inc.

NetWare Loadable Module and NLM are trademarks of Novell, Inc.

Novell is a registered trademark of Novell, Inc. in the United States and other countries.

Novell Client is a trademark of Novell, Inc.

Third-Party Materials

All third-party trademarks are the property of their respective owners.

About This Guide 11

Part I Installing Novell BorderManager

1	Installing Novell BorderManager	15
	Upgrade Scenarios	15
	System Requirements	16
	Server Hardware	16
	Server Software	17
	End User License Agreement	17
	Documenting Your Environment	17
	Prerequisites to Installing Novell BorderManager 3.8	18
	NICI 2.6 (only for NetWare 5.1 and NetWare 6)	18
	Netnlm32.nlm	18
	TCP/IP (Only for VPN)	18
	Downloading Novell BorderManager 3.8	19
	Installing Novell BorderManager 3.8	19
	Moving from Trial to Production	24
	Installing iManager 2.0.1 Snap-Ins	24
	NetWare 5.1 SP6	24
	NetWare 6 SP3	25
	NetWare 6.5 with iManager 2.0	25
	What's Next	26
	Setting Up Login Policies	27
	Identity Management	28

Part II Proxy

2	Setting Up Proxy Services	31
	Proxy Services Prerequisites	32
	Setting Up the DNS Resolver	32
	Setting Up Microsoft Internet Explorer to Use a Web Proxy	33
	Setting Up Netscape Navigator to Use a Web Proxy	33
	Setting Up an HTTP Proxy Server	34
	Setting Up an HTTP Accelerator Server	35
	Blocking Virus Requests in HTTP Accelerator	36
	Command Line Configuration	36
	Adding and Deleting Virus Request Patterns	36
	Updating the Database via a Script (NCF File)	37
	Enabling and Configuring Auto Update	37
	Adding New Virus Keywords	38
	Monitoring the Virus Pattern Recognition Feature	38
	Effect on Performance	38
	Setting Up an FTP Proxy Server	38
	Setting Up an FTP Accelerator Server	39
	Setting Up a Mail Proxy Server	40
	Setting Up a News Proxy Server	41
	Setting Up a Generic Proxy Server	41
	Setting Up DNS Proxy	42
	Setting Up RealAudio and RTSP Proxies	42
	Setting Up the SOCKS Client (Upstream)	43
	Setting Up HTTP Transparent Proxy	44
	Setting Up Telnet Transparent Proxy	44
	Setting Up Proxy Authentication	45
	Setting Up HTTP Proxy Authentication	45
	Session Failover	46

Setting Up HTTP Transparent Proxy Authentication	46
Setting Up Telnet Transparent Proxy Authentication	47
Completing Advanced Setup, Configuration, and Management Tasks	47
3 Managing Proxy Services	49
Setting Up HTTP Proxy Services Logging	49
Monitoring Proxy Cache Realtime Activity	50
Viewing User Statistics	51
Viewing Host Statistics	52
Exporting Data	53
Exporting HTTP Audit Log Proxy Records	54
Exporting Audit Logs for All Other Proxies	55
Export File Subdirectories	55
Managing Virus Pattern Recognition	60
The Virus Pattern Configuration Screen	60
Choosing a Proper Threshold	61
Miscellaneous Tasks	61
Mail Proxy	62
Mail Proxy Transparency	62
Mail Proxy Process Multiple MX Records	62
Mail Proxy Multi-domain Support	63
Additional POP3 Server	63
Additional Flags	64
Authentication	64
MAC OS SSL Authentication	64
MAC Block HTTP Tunnel Requests	64
HTTPS Transparent Proxy	65
Terminal Server Authentication	65
Proxy Configuration Dump Tool	66
Splash Screen Settings	66
4 Advanced Configuration of Proxy Services	67
Configuring Cache Parameters	67
Configuring Cache Aging Parameters	67
Configuring Cache Control Parameters	68
Configuring Cache Location Parameters	69
Configuring Cacheable Object Control Parameters	69
Specifying Batch Downloading of Sites or URLs	70
Configuring Caching Hierarchies	71
Configuring Session Failover	73
Setting up Auth agent:	73
Starting Auth Agent:	74
Configuring Proxy Agent	74
Starting Proxy Agent:	75
Specifying Transport Timeout Parameters	75
Specifying DNS Parameters	75
5 HTTP Proxy Logging Using Nsure™ Audit	77
Nsure Audit Overview	77
Configuring Novell BorderManager 3.8 for Nsure Audit	79
Novell BorderManager 3.8 Event Data	79
Viewing Events in Nsure Audit Report	80
Other Nsure Audit Capabilities	81
6 Setting Up Access Control	83
Setting Up a URL-Based Rule	83
6 Novell BorderManager 3.8.2 Installation and Administration Guide	

Setting Up a Rule to Allow Access through an Application Proxy	84
Setting Up a Rule to Allow VPN Clients to Access VPN Servers	86
Setting Up a Rule to Allow the Server to Resolve Hostnames	86
Setting Up Time Restrictions for Access Rules	87
Viewing All Rules That Apply to an Object	88
Completing Advanced Setup, Configuration, and Management Tasks	88
7 Managing Access Control	89
Viewing User Statistics	89
Viewing Host Statistics	91
Exporting Data	92
Exporting Data from the Access Control Users Statistics Window	92
Exporting Data Using the Export Logs Option	93
8 Setting Up Alert Notification	95
Setting Up Alert E-Mail Notification	95
Completing Advanced Setup, Configuration, and Management Tasks	97
9 Managing Alert Messages	99
Viewing Alerts Sent as E-Mail Messages	99
Viewing Alerts in Audit Trail Log File	100
Displaying Audit Trail Log Records with the Audit Trail Utility	100
Archiving the Audit Trail Log File	100
Viewing Alerts in the Control Log	101
Responding to Alerts	101
Server Performance Alerts	102
License Acquisition Alerts	103
Security Alerts	103
Proxy Alerts	105
Part III Filters	
10 Setting Up Packet Filters	109
Packet Filter Prerequisites	109
Setting Up the Default Filters	110
Using Novell iManager for Filter Configuration	110
Using FILTCFG for Filter Configuration	113
Setting Up Outbound Packet Filter Exceptions	113
Setting Up Inbound Packet Filter Exceptions	117
Defining Custom Stateful Packet Types	117
Saving Filters to a Text File	118
Enabling Global IP Packet Logging	118
Completing Advanced Setup, Configuration, and Management Tasks	119
11 Managing IP Packet Filters	121
Modifying Default IP Logging Parameters	121
Viewing IP Packet Log Information	122
12 Packet Filtering Using Novell iManager	125
Configuring the Packet Forwarding Filter	127
Configuring the Service Type	132
Configuring an Incoming RIP Filter	134
13 Backing Up and Restoring Filters	139
Backing Up eDirectory Filters to LDIF	139
Restoring Filters to eDirectory from LDIF	140
Backing Up eDirectory Filters to Text Files	140

Restoring Filters to eDirectory from Text Files	140
14 Advanced Configuration of IP Packet Filters Using FILTCFG	141
Choosing between Stateful or Static Packet Filters	141
Setting Up an HTTP Filter	141
Setting Up a Stateful HTTP Filter	142
Setting Up Static Filters for HTTP	142
Setting Up an FTP Filter	143
Setting Up a Stateful FTP Filter	143
Setting Up Static Filters for FTP	144
Setting Up a Telnet Filter	144
Setting Up a Stateful Telnet Filter	145
Setting Up Static Filters for Telnet	145
Setting Up an SMTP Filter	145
Setting Up a Stateful SMTP Filter	146
Setting Up Static Filters for SMTP	146
Setting Up a POP3 Filter	146
Setting Up a Stateful POP3 Filter	147
Setting Up a Static POP3 Filter	147
Setting Up a DNS Filter	147
Setting Up a Stateful DNS Filter	147
Setting Up Static Filters for DNS	148
Setting Up VPN Filters	148
Filtering IP Packets that Use the IP Header Options Field	148
15 NBM Filter Management	151
Features of Easy Filter Configuration	151
Configuring Filters using Easy Filter Configuration	151
On Server Service Exceptions	153
Off Server Service Exceptions	155
Filter Maintenance	156
List All Firewall Policies	157
Setting Up Public Interface	158
Troubleshooting: Possible Installation Scenarios	158
The Off Server Service Fields Appear Disabled	158
Roles and Tasks Do Not Appear on the Left Pane	159
Part IV Virtual Private Network	
16 Certificate-Based Authentication	163
Automated Creation of eDirectory Certificates or Objects	164
Creating Server Certificates	164
Exporting Root Certificates from the Server Certificate	169
Creating Trusted Root Containers	171
Creating the Trusted Root Object	172
Creating a User Certificate	173
Exporting User Certificates	175
Third-Party Certificate Server	177
17 Configuring VPN Services	179
Setting Up VPN Services	179
VPN Server Configuration	179
Virtual Private Network Prerequisites	183
Site-to-Site VPN Prerequisites	184
Client-to-Site VPN Prerequisites	185
Setting Up VPN Filters	185

On VPN Master Site	187
On VPN Slave Site	188
Exceptions required to keep a Client-toSite and a Site-to-Site Connection Up	190
Client-to-Site Configuration	191
General	192
Traffic Rules	193
Authentication Rules	199
Remote LDAP Configuration	202
DNS/SLP Configuration	203
Final Client-to-Site Page	204
Attaching a Client-to-Site Service to the VPN Server	205
Site-to-Site Configuration	207
Configuring a VPN Server As a Master Server	208
Configuring a VPN Server As a Slave Server	210
Modifying a Site-to-Site Service	213
Removing Site-to-Site Members	217
VPN Policy	218
Default Values for Client-to-Site Authentication Rules	219
Default Values for Client-to-Site Traffic Rules	219
Default Values for Site-to-Site Traffic Rules	220
18 Upgrading Virtual Private Networks	221
VPN Migration	221
Upgrading a VPN from a Previous Version	222
General Guidelines for Upgrading	222
Upgrade Procedure	223
19 Monitoring Virtual Private Networks	227
Logging into NetWare Remote Manager	227
Checking the VPN Real-Time Monitor	229
Checking the Audit Log on a VPN Server	233
Checking the Activity of a VPN Server	236
20 Virtual Private Network Client	239
GUI changes for VPN Client	239
VPN Client Features	239
X.509 Certificate Authentication Mode	240
NMAP Authentication Mode	240
NMAP LDAP Authentication Mode	241
Backward Compatibility Mode	241
Pre-shared Authentication Mode	241
X-AUTH hybrid mode	241
X-AUTH PSK Mode	241
VPN Client Integration with the Novell Client	242
Use NICI for Encryption	242
Selecting Dial-Up Entries	242
Automatic Creation of a Novell VPN Dial-Up Entry	243
Password Expiry Notice	243
VPN Server Hosts List	243
Policy	243
VPN Connections through NAT	243
VPN Client Installation	244
VPN Client Silent Install	244
Part V Network Address Translation	
21 Setting Up NAT	249

NAT Prerequisites	249
Setting Up NAT on a Single Interface	250
Setting Up NAT with Multihoming	251
Completing Advanced Setup, Configuration, and Management Tasks	252
22 Advanced Configuration of NAT	253
23 Managing Network Address Translation	257
A SET Parameters	259
Configuration Using SET Options	259
IKE debugmask	259
IKE Certificate Request Payload.	259
IKE Dump All IKE SAs	259
IKE exponent_size for DH Group 1	260
IKE exponent_size for DH Group 2	260
IKE Pre-shared Key	260
IKE Retransmit Timeout	260
IPsec Encryption Algorithm for Pre-shared Key Authentication Mode in C2S	260
IPsec Hash Algorithm For Pre-shared Key Authentication Mode in C2S	261
IPsec Use Policy	261
VPN NCF Check Interval	261
VPN Over NAT	261
VPN Requires NCF	262
Pre-shared Key	262
B Cool Solutions and AppNotes on Novell BorderManager	263
C Important TIDs on Novell BorderManager	265
Novell BorderManager Glossary	267

About This Guide

Novell® BorderManager® 3.8 includes premier firewall and VPN technologies that safeguard your network and help you build a secure identity management solution. With the powerful directory-integrated features in Novell BorderManager, you can monitor users' Internet activities and control their remote access to corporate resources.

Moreover, Novell BorderManager provides Internet access control and supports numerous content-filtering solutions. These features protect your network from undesirable Internet content, including programs that destroy or steal data, games that waste users' time, and Web pages that expose your company to legal liability.

Novell BorderManager includes firewall and VPN technologies that protect networks and resources, while ensuring end-user productivity.

This documentation presents an introduction to installing and managing Novell BorderManager 3.8. The audience for this documentation is experienced network administrators.

It includes the following sections:

- ◆ [“Installing Novell BorderManager” on page 13](#)
- ◆ [“Proxy” on page 29](#)
- ◆ [“Filters” on page 107](#)
- ◆ [“Virtual Private Network” on page 161](#)
- ◆ [“Network Address Translation” on page 247](#)
- ◆ [Appendix A, “SET Parameters,” on page 259](#)
- ◆ [Appendix B, “Cool Solutions and AppNotes on Novell BorderManager,” on page 263](#)
- ◆ [Appendix C, “Important TIDs on Novell BorderManager,” on page 265](#)

Documentation Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

Also, a trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.



Installing Novell BorderManager

This section discusses Novell[®] BorderManager[®] installation.

- ◆ [Chapter 1, “Installing Novell BorderManager,” on page 15](#)

1

Installing Novell BorderManager

This section provides instructions for installing the Novell[®] BorderManager[®] 3.8 software:

- ◆ “Upgrade Scenarios” on page 15
- ◆ “System Requirements” on page 16
- ◆ “End User License Agreement” on page 17
- ◆ “Documenting Your Environment” on page 17
- ◆ “Prerequisites to Installing Novell BorderManager 3.8” on page 18
- ◆ “Downloading Novell BorderManager 3.8” on page 19
- ◆ “Installing Novell BorderManager 3.8” on page 19
- ◆ “Moving from Trial to Production” on page 24
- ◆ “Installing iManager 2.0.1 Snap-Ins” on page 24
- ◆ “What’s Next” on page 26
- ◆ “Setting Up Login Policies” on page 27
- ◆ “Identity Management” on page 28

Upgrade Scenarios

Follow this table to see which scenarios are supported by Novell BorderManager 3.8. In the table, BMEE refers to the earlier product name BorderManager Enterprise Edition, and NBM refers to the more recent Novell BorderManager.

Base Operating System	Current version of BorderManager	Upgrade to Operating System	Upgrade to Novell BorderManager 3.8	Further Upgrade (optional)
NetWare 5.1 CSP9 or greater	BMEE 3.6 SP2a	NetWare 5.1 CSP9	Yes	Nil
NetWare 5.1 CSP9 or greater	NBM 3.7 SP2	NetWare 5.1 CSP9	Yes	Nil
NetWare 5.1 CSP9 or greater	BMEE 3.6 SP2a	NetWare 5.1 CSP9	Yes	NetWare 6 CSP9
NetWare 5.1 CSP9 or greater	NBM 3.7 SP2	NetWare 5.1 CSP9	Yes	NetWare 6.5
NetWare 6 CSP 9 or greater	BMEE 3.6 SP2a	NetWare 6 CSP9	Yes	Nil
NetWare 6 CSP9 or greater	NBM 3.7 SP2	NetWare 6 CSP9	Yes	Nil

Base Operating System	Current version of BorderManager	Upgrade to Operating System	Upgrade to Novell BorderManager 3.8	Further Upgrade (optional)
NetWare 6 CSP9 or greater	BME 3.6 SP2a	NetWare 6 CSP9	Yes	NetWare 6.5
NetWare 6 CSP9 or greater	NBM 3.7 SP2	NetWare 6 CSP9	Yes	NetWare 6.5

For a detailed explanation on Novell BorderManager 3.8 upgrades for VPN Services see [Chapter 18, “Upgrading Virtual Private Networks,”](#) on page 221.

IMPORTANT: If you are upgrading BorderManager from an earlier version of the product, stop all running BorderManager services before installing Novell BorderManager 3.8.

System Requirements

Novell BorderManager 3.8 can be installed on a NetWare server and is administered using Novell iManager 2.0.1 and NetWare Administrator (for Proxy) from a client Windows* 98, Windows 2000, Windows NT*, or Windows XP workstation.

The Novell BorderManager software comes with a Companion CD containing the prerequisites for installing Novell BorderManager 3.8. The Companion CD Readme is available at the root of the CD at Documents > ReadMes > Companion. The products are:

- ◆ Novell eDirectory™ 8.7.1
- ◆ NICI 2.6 (NetWare 5.1, NetWare 6)
- ◆ Netlm32.nlm 5.5.8 dated June 04, 2003
- ◆ TCPIP
- ◆ ICE Patch
- ◆ iManager 2.0.1 - Windows (2000, XP)
- ◆ NIS

See the Readme for more details on the Companion CD products and instructions on how to install them.

Server Hardware

- ◆ PC with an Intel* Pentium* II or higher processor
- ◆ Minimum of 256 MB of RAM above OS requirements
- ◆ Minimum of 300 MB of disk space, with an additional 40 MB available during installation (Novell BorderManager needs approximately 150 MB, and NMAST™ needs an additional 40 MB).
- ◆ CD drive that can read ISO 9660 formatted disks
- ◆ Super VGA or higher resolution display adapter
- ◆ Two or more network interfaces
- ◆ PS/2 or serial mouse
- ◆ DOS partition with at least 250 MB
- ◆ 4 GB sys volume recommended

- ♦ Minimum 2 GB of free drive space for the creation of a dedicated cache volume if you want to use Novell BorderManager 3.8 as a proxy server

Server Software

The following prerequisites must be installed in this order:

- ♦ Operating System: NetWare 6.5 or NetWare 5.1 SP6 or NetWare 6 SP3
- ♦ The installation server and all servers holding a copy of the partition where the Novell BorderManager 3.8 Server object resides should have Novell eDirectory 8.6.2 or 8.7.1. The recommended version is 8.7.1. Novell BorderManager 3.8 must be installed on a NetWare server that holds an eDirectory read/write replica of the partition containing that server's object.
- ♦ NCI 2.6
- ♦ Netlm32.nlm version 5.5.8 dated June 04, 2003

Special Requirements:

- ♦ TCP/IP secure version (required for VPN only)
- ♦ If you are using eDirectory 8.6.2 and extending the VPN schema using SSL, copy the files under the ICE patch directory from the Companion CD to sys:/system.

End User License Agreement

Before installing Novell BorderManager 3.8, you need to read the End User License Agreement (EULA). The EULA is present in the relevant language directory at the root of the product directory > \EULA.

Documenting Your Environment

There are a number of parameters that you might need to note before installing Novell BorderManager 3.8.

- ♦ Location of license diskettes or path to the license file
- ♦ Public and private interfaces and their IP address bindings
- ♦ Domain Name System host name
- ♦ IP addresses for up to three DNS name servers on the network
- ♦ Domain Name for Mail Proxy and whether you want to proxy an internal mail server or external mail server or both
- ♦ Server certificates if secure LDAP is to be used for schema extension
- ♦ Default gateway
- ♦ If you are installing VPN services, document the following:
 - ♦ Server certificate to be used for the VPN server
 - ♦ Trusted Root Certificate name
 - ♦ Trusted Root Object names

Refer to [Chapter 16, "Certificate-Based Authentication," on page 163](#) and [Chapter 17, "Configuring VPN Services," on page 179](#) for more details.

Prerequisites to Installing Novell BorderManager 3.8

NICI 2.6 (only for NetWare 5.1 and NetWare 6)

Novell International Cryptography Infrastructure 2.6 is present in the Companion CD at `nici\nwserver`. To install NICI 2.6:

- 1** Create a local copy of NICI 2.6 on the server on which you are installing Novell BorderManager 3.8 (Unzip the `nici_u0.exe` on that server).
- 2** Go to `NWCONFIG > Product Options`, select `Install A Product Not Listed`, then specify the path where you have copied NICI 2.6.
- 3** Restart the server after installation.

Netnlm32.nlm

Check if you have version 5.5.8 dated June 04, 2003 on your machine. This version is required to start NMAS 2.2. If your server does not have the minimum required version of this NLM™, copy the `netnlm32.nlm` file from the `netnlm32` directory on the Companion CD to the `sys:\system` directory of your server.

The latest version of the NLM can be downloaded from [support.novell.com](http://support.novell.com/support.novell.com/cgi-bin/search/searchtid.cgi?/2966367.htm) (<http://support.novell.com/cgi-bin/search/searchtid.cgi?/2966367.htm>). Download and extract `nwlib5.exe` on the server. The DSAPI directory will be available in the extract. Copy `netnlm32.nlm` from the DSAPI directory to the `sys:\system` directory.

TCP/IP (Only for VPN)

TCP/IP is available on the Companion CD and can be installed by running a Perl script (`tinstall.pl`) on the server. This is done as follows:

From the CD:

- 1** Insert and mount the Companion CD.
- 2** At the server console, enter

```
perl NBM38CCD:\TCPIP\tinstall.pl [-f]
```

Provide the `-f` option if you have null encryption versions of this NLM software on the server.
- 3** Restart the server

From the Web:

- 1** Unzip the Novell BorderManager 3.8 Companion CD on a drive that is accessible from your server.
- 2** At the server console, enter

```
perl <Companion CD Path>\TCPIP\tinstall.pl [-f] [-p path]
```

Provide the `-f` option if you have null encryption versions of this NLM software on the server.
Provide the `-p` option to give the name of the directory where the Companion CD is unzipped.
- 3** Restart the server

Downloading Novell BorderManager 3.8

This step is needed only if you are downloading the product from the Web. If you are downloading the product, go to the Web site beta.novell.com (<http://beta.novell.com/login.html>), download the zip file, then unzip it on a drive that is accessible from your server.

Installing Novell BorderManager 3.8

To install Novell BorderManager 3.8 on the server:

- 1** Run INETCFG before you install Novell BorderManager 3.8.
- 2** Unzip Novell BorderManager 3.8 on a drive that is accessible from your server.
or
If you are using a product CD, mount the Novell BorderManager 3.8 CD on the server by entering **CDROM** at the server console.
- 3** On the server side, go to the X-Server Graphical Console. If the X-Server Graphical Console is not loaded, enter **STARTX** at the server console.
If STARTX is already loaded, press Ctrl+Esc and select the option for X-Server Graphical Console.
- 4** Click the Novell logo, then select Install to display the list of currently installed products.
- 5** Click Add, then browse to the root of the Novell BorderManager 3.8 directory and select product.ni, which is displayed in the right frame.
- 6** On the Welcome page, click Next.
- 7** Read the license agreement. If you accept the terms of the agreement, click I Accept.
The next page shows the Novell BorderManager 3.8 services that will be installed. The services are:
 - ◆ Novell BorderManager Firewall/Caching Services
 - ◆ Novell BorderManager VPN Services
 - ◆ Novell Modular Authentication Services (NMAS). This will be installed by default.Trial Licenses are selected by default.
- 8** Select either the Shipping License or select the Skip License Install check box and click Next so that the licenses can be installed later.
Trial and Shipping licenses are located in the licenses directory at the root of the CD. You can install the system files without installing the license; however, Novell BorderManager 3.8 services will not load until a valid license is installed.
NOTE: You can install the trial license only once per tree.
- 9** The Minimum Requirements page displays Review the Results column to verify whether the minimum system requirements are met, then click Next to proceed.

Figure 1 Sample Minimum Requirements Page. NetWare 6.5. For NetWare 5.1 and NetWare 6, the rows display the respective requirements.

Product	Installed Version	Minimum Require...	Result
NetWare	6.5	6.5	<input checked="" type="checkbox"/>
NICL	2.6.0	2.6.0	<input checked="" type="checkbox"/>
eDirectory	87.0.1	86.0.2	<input checked="" type="checkbox"/>
LDAP	87.0.0	86.0.1	<input checked="" type="checkbox"/>
Novell BorderManager	-	-	<input checked="" type="checkbox"/>
PKI	2.5.2	2.2.0	<input checked="" type="checkbox"/>
SAS	1.6.0	1.6.0	<input checked="" type="checkbox"/>
NETNLM32.NLM	5.5.8	5.5.8	<input checked="" type="checkbox"/>
TCP/IP Modules (opti...	Null Encryption	Domestic Encryption	<input type="checkbox"/>
Novell iManager (opti...	2.0.0	2.0.0	<input checked="" type="checkbox"/>

Buttons: Cancel, Help, < Back, Next >

If any of the minimum requirements except TCPIP modules or iManager 2.0 is not met, the install will abort. Meet the requirements according to the table above and restart the installation. If the base requirements for the TCPIP modules are not met, a warning is displayed. You can ignore the warning and install, but you need to copy the right TCP/IP modules later (see [“TCP/IP \(Only for VPN\)”](#) on page 18) if you want to use VPN services.

If iManager 2 is not installed, the plug-ins for Novell BorderManager Firewall Configuration and Novell BorderManager VPN Configuration are not installed. If that is the case, install iManager 2 after Novell BorderManager installation to automatically install the Novell BorderManager Firewall Configuration and Novell BorderManager VPN Configuration plug-ins.

- 10** In the login dialog box, log in to the eDirectory tree with a fully distinguished name (FDN, with administrative rights).

Either provide the FDN or provide only the name and then the context in the Context field.

You must have administrative rights to the root of the eDirectory tree. This requirement applies to any user who is a trustee with Supervisor rights at a container at the same level as the server. Administrative rights are required to extend the eDirectory schema, install product licenses, and configure Novell BorderManager 3.8 for the first time.

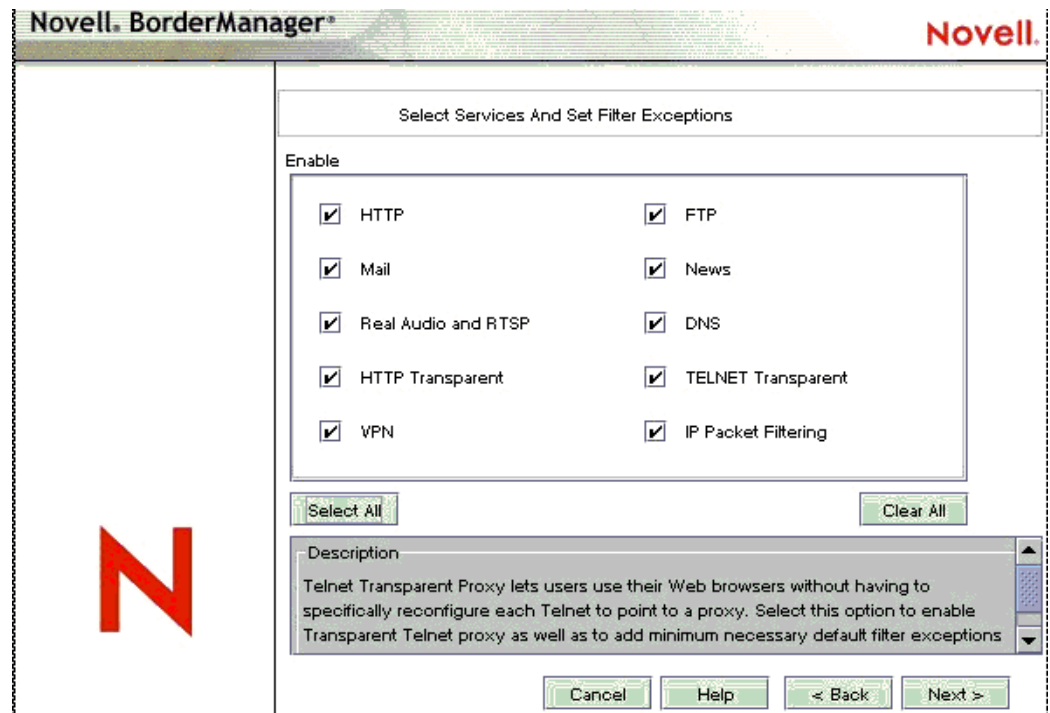
- 11** Select the NMAS login methods you want to install, then Click Next.

- 12** Radius components and ConsoleOne® snap-ins for NMAS are installed by default. For an upgrade you might select Migrate Radius Components and fill in the details.

If this is an upgrade, the next page prompts you to provide details for the VPN services. Skip to [Step 22](#) or continue with the next step.

- 13** If you are installing Novell BorderManager firewall/caching services or Novell BorderManager VPN services, review the list of network interfaces and their IP bindings. Specify each interface as public, private, or both for proxy and firewall services.
- For firewall and caching services, you must specify a public IP address to secure the network border. Public IP addresses specify server interfaces to a public network, typically the Internet. Private IP addresses specify server interfaces to a private network or intranet.
- 13a** Select either a public IP address or a private IP address or both.
- 13b** Specify the default gateway.
- 13c** By default, the iManager snap-ins for Firewall are selected. Deselect the check box if you do not want to install the snap-ins.
- 14** Click Next
- 15** Select the check boxes for the services that you want to enable. Filter exceptions for these services will be created on the public interface. Click Next.

Figure 2 Novell BorderManager Services and Filter Exceptions



On a single interface machine, filter exceptions are created but the filters are not enabled. Filter exceptions corresponding to the selected services are created on the public interface. Filter exceptions are activated along with the filters if IP Packet Filtering is selected. IP packet filtering is not enabled if only one interface is available. If this is an upgrade, existing filters are preserved. Deny All Filters is not set on public interfaces.

- 16** (Optional) If you selected Mail, select either or both of the External/Internal check boxes in order to set appropriate filter exceptions, depending on whether you want to proxy internal mail servers, external mail servers, or both. Specify the name of one domain for the mail proxy.

NWAdmn displays only the DNS name of the mail proxy. See [“Mail Proxy” on page 62](#) for more details.

- 17** (Optional) NetWare 6.5 provides the facility to create cache volumes automatically. If HTTP, FTP, HTTP Transparent is selected in the Proxy and Filter Exception page, click Create Volume and provide the required details to create traditional volumes for caching. You can also use existing traditional volumes for caching.

If you do not create a volume or select a traditional volume for caching, the `sys:\etc\proxy\cache` directory is used.

TIP: If you do not create a volume or select a traditional volume for caching, the `sys:\etc\proxy\cache` directory is used.

To create a new cache volume follow these steps:

- ◆ Copy the directory CCRT from the UNSUPPORTED directory of the NBM 3.8 CD into the `sys: volume` of a NetWare server.
- ◆ On the console prompt type `sys:\CCRT\crt`
- ◆ Follow the directions that appear on the screen.

In case there is no free space available in the system, and there are volumes/partitions which you want to delete to recover space, follow the steps below:

- ◆ Open Novell Remote Manager (NRM) and from a browser type `https://IPAddress:8009`
- ◆ After logging in, the left panel shows Partition Disks under Manage Server.
- ◆ Click on Partition Disks.
- ◆ Delete the partitions/volumes which are not required. To delete a partition, dismount the volumes in the partition first > then delete the volumes in the partition > delete the partition and restart the server before running the utility.

NOTE: If any partition label has non-ascii characters in it, this utility will not work. Free space will be shown as 0 even if there is free space on the server. Labels can have non-ascii characters if some disk imager is used to restore disk images. The partition label can be seen through NSSMU on the server. (Load NSSMU.NLM > Partitions > Partition Information - Label) Partiton label can be viewed/modified using NRM. Open `https://IpAddress:8009` from a browser. Manager server > Partition Disks. On the right panel all the partition and volumes will be shown. Partition labels are shown against the partition names. Click on an existing label to change it.

- 18** The check box for Access Control is enabled by default. We recommend that you accept the default. Access control enforces additional security by denying all proxy services traffic.

Access control rules can be set using the NetWare Administrator utility. Access rules are used to allow or deny access from any source or to any destination. This option comes up only if you selected Proxy Services on the previous page.

- 19** Specify a unique DNS domain name for your network, then click Next.

- 20** Click Add to specify at least one or up to three DNS server IP addresses. By default the existing DNS entry is used.

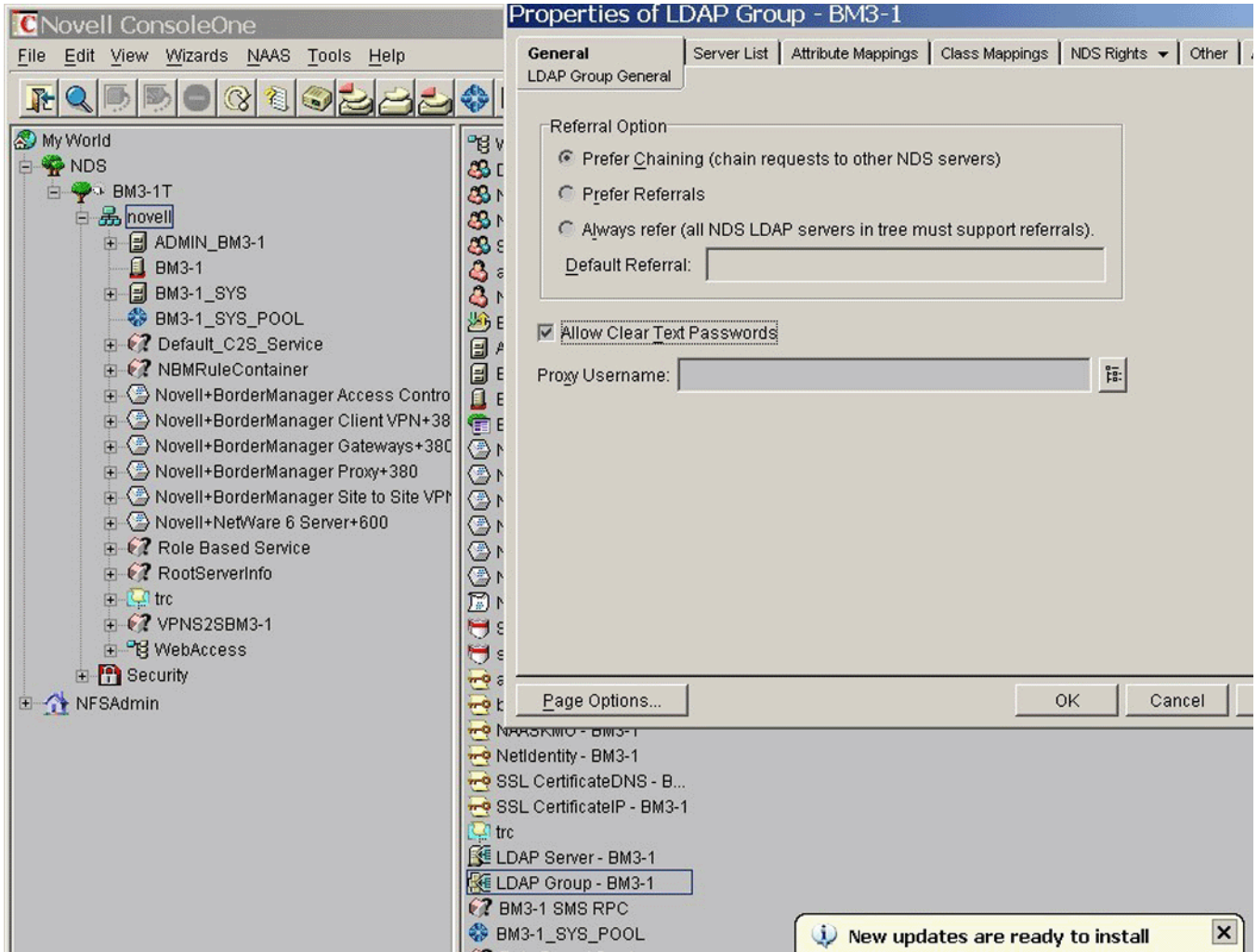
- 21** If you selected VPN, select the Allow Clear Text Password option so the VPN schema extension can use clear text passwords. Or to use SSL to encrypt your password, select Use SSL for Schema Extension.

To enable clear text passwords, log in to ConsoleOne, double-click the context of the server on which you are installing Novell BorderManager 3.8, then select LDAP Group Object and right-click > Properties. As applicable, either select Allow Clear Text Password (for

eDirectory 8.6.2) or deselect Required TLS for Simple Bind with Password (for eDirectory 8.7.1).

To use SSL: For Schema Extension to succeed in this mode, you must have a valid Server Trusted Certificate, usually a DER file present in the sys:\public directory of your server. Browse to the file or enter its name in the field.

Figure 3 Enabling Clear Text Passwords in ConsoleOne.



By default the iManager snap-ins for VPN are selected. Deselect the box if you do not want the snap-ins to be installed.

If the install is an upgrade from BMEE 3.6 or Novell BorderManager 3.7, the Migrate VPN Configuration option is selected. Deselect this option if you do not want to migrate the VPN configuration.

Do not change the port on which LDAP is listening unless LDAP is listening on a non-standard port.

If nldap.nlm is not loaded, a message box will pop up asking you to configure the LDAP server.

22 Click Finish if you are done, or click Back to return to previous pages and modify your selections.

23 Do one of the following:

- ◆ Click Reboot for Novell BorderManager 3.8 services to come up.
- ◆ Click Close to complete the installation and return to the GUI screen.
- ◆ Click Readme to view the Readme.

The install summary is available in `sys:\ni\data\nbm_instlog.csv`. The Readme is available at the root of the CD under Documents > ReadMes > enu.

NOTE: Novell BorderManager 3.8 provides the option to recover from a failed install. The Install program pops up an option after the authentication dialog box ([Step 10 on page 20](#)). To recover from a failed install, select the Fresh Install Option or select the Upgrade option. Continuing with the Fresh Install option with a working Novell BorderManager 3.8 server may give unexpected results, particularly with existing filter exceptions. After using this option, review your NWAdmn settings and filter exceptions.

Moving from Trial to Production

If you want to move from the trial Novell BorderManager 3.8 product to the production version, you do not need to re-install Novell BorderManager 3.8. Follow these steps instead:

- 1** Install the Production License from the `licenses\regular` directory on the product CD, using NWAdmn or iManager.
- 2** Uninstall the trial VPN client. Install the production version of the VPN client from the product CD (`cl_inst\vpn\exes\setupe.exe`).
- 3** Uninstall the trial NCF. Install the production version of the NCF from the product CD (`cl_inst\ncf\ncfInstall.exe`).

Installing iManager 2.0.1 Snap-Ins

iManager is a Windows-based configuration utility that helps you configure virtual private networks and filters on Novell BorderManager 3.8 machines. You need to do some configuration if BorderManager is running on any of the following platforms:

- ◆ [“NetWare 5.1 SP6” on page 24](#)
- ◆ [“NetWare 6 SP3” on page 25](#)
- ◆ [“NetWare 6.5 with iManager 2.0” on page 25](#)

NetWare 5.1 SP6

To configure Novell BorderManager 3.8 VPN and Filter services on NetWare 5.1 SP6:

- 1** Install iManager 2.0.1 on a Windows 2000 or XP machine. To do so, run `iManagerInstall.exe` located under `imanager20\installs\win` on the Companion CD.
- 2** Configure iManager 2.0.1 by following the steps in the iManager install.
- 3** To install iManager snap-ins for Novell BorderManager, run `NBM_IM2_Snapin_Install.exe`, located under `cl_inst\snapins` on the main product CD.
- 4** Launch iManager. Go to the specific IP address of the Windows machine (`https://<ip address>/nps/iManager.html`). Authenticate and select VPN or Filtering from the left pane.

NetWare 6 SP3

To configure Novell BorderManager 3.8 VPN and Filter services on NetWare 6 with SP3, do either of the following:

- 1 Install iManager 2.0.1 on a Windows 2000 or XP machine as mentioned in “[NetWare 5.1 SP6](#)” on page 24, and run the NBM_IM2_Snapin_Install.exe.

or

- 1 Install eDirectory 8.7.1 and JVM 1.4.1 if you do not have them installed already. eDirectory 8.7.1 and JVM 1.4.1 are available on the Companion CD.
- 2 Install iManager 2.0.1 on this machine. iManager 2.0.1 for NetWare 6 is available in the Companion CD under IMANAGER20\installs\NW6 directory.
- 3 Install the Novell BorderManager 3.8 snap-ins manually. See “[NetWare 6.5 with iManager 2.0](#)” on page 25 for details.

NetWare 6.5 with iManager 2.0

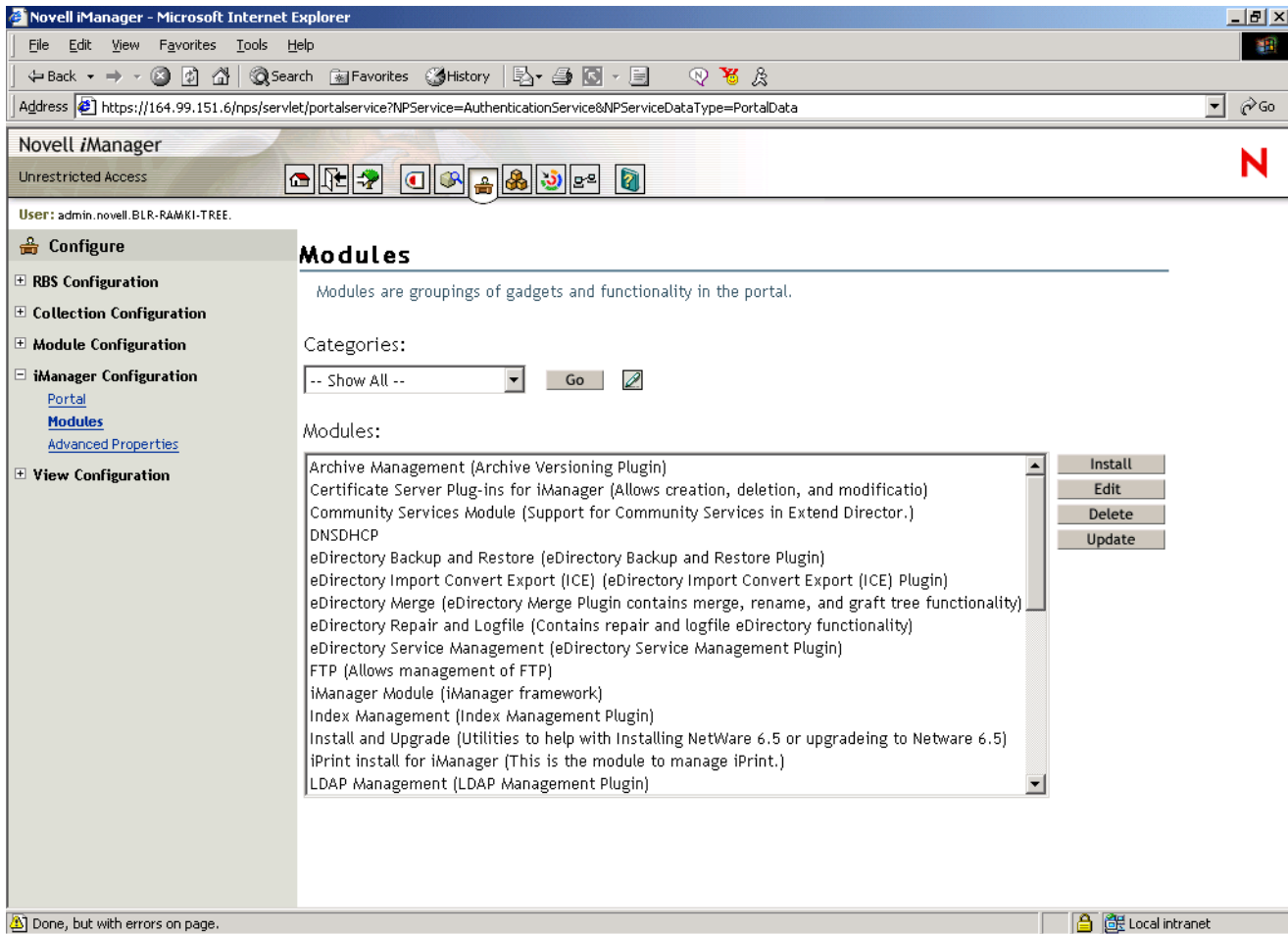
NetWare 6.5 comes with iManager 2.0 by default. To work with Novell BorderManager 3.8, either select the snap-ins during Novell BorderManager 3.8 installation, manually install them later, or use a iManager 2.0.1 on a Windows machine.

To use a Windows machine, see “[NetWare 5.1 SP6](#)” on page 24.

To manually install the snap-ins:

- 1 Launch iManager 2.0 on the browser. Go to the specific IP address of the NetWare 6.5 machine (<https://<ip address>/nps/iManager.html>).
- 2 Click the Configure tab on the top of the iManager interface, then select iManager Configuration > Modules on the left pane. The page will look like this:

Figure 4 iManager Modules



- 3 Click Install, then select the VPN snap-in NPM file. The VPN snap-in is available in the VPN directory at the root of the main product download. The name of the snap-in is vpn.npm.

NOTE: To install Firewall snap-ins, follow the steps mentioned above but select BM.NPM from the Border directory at the root of this Web download.

- 4 Restart Tomcat on the NetWare 6.5 server.

What's Next

After Novell BorderManager 3.8 is installed, you can use the services. Use the following table for details.

What	Where
Proxy Services	Chapter 2, "Setting Up Proxy Services," on page 31
Filters	Chapter 10, "Setting Up Packet Filters," on page 109
VPN Services	Chapter 18, "Upgrading Virtual Private Networks," on page 221
Network Address Translation	Chapter 21, "Setting Up NAT," on page 249

Setting Up Login Policies

All users logging in to services through Novell BorderManager 3.8 must be authenticated. The type of authentication required for a user to log in and access network services through Novell BorderManager 3.8 is stored in Novell eDirectory in a Login Policy object. Because of this, you must set up a generic login policy to enable users to access Novell BorderManager 3.8 services. Until a policy is set up, no user access is allowed. There can be only one Login Policy object in an eDirectory tree. This object holds the login policies for all Novell BorderManager 3.8 servers and services in the tree.

NOTE: The policies stored in the Login Policy object apply only to Novell BorderManager 3.8 services. Previous versions of Novell BorderManager 3.8 use hard-coded default policies. To manage login policies for all Novell BorderManager 3.8 services using the Login Policy object, you must upgrade previous versions of BorderManager to Novell BorderManager 3.8.

To create a Login Policy object and set up generic policy rules that allow users to access network services through each of the various Novell BorderManager 3.8 services with an eDirectory password, complete the following steps:

- 1** In NetWare Administrator, select the Security container object in your eDirectory tree.
The Login Policy object can only be created in the Security container object.
- 2** From the Object menu, click Create > Login Policy, then click OK.
- 3** To configure a login policy rule, click Rules, then click Add.
- 4** To configure a rule for Novell BorderManager 3.8 Authentication Services, select the Object name radio option from the Service Type dialog box, browse to select the Dial Access System object associated with that service, select the Enabled check box.

If this is a new installation of Novell BorderManager 3.8 Authentication Services, you will need to create a Dial Access System object.
- 5** Select the Users tab, click Add, then browse to select the user, group, or container objects to enable access.
- 6** Select the Methods tab, click Add, then select the Login Method enabled check box.
- 7** In the Method Types dialog box, select Novell eDirectory Passwords.
- 8** In the Method Enforcement dialog box, select Mandatory, click OK, then click Add.
- 9** To configure a rule for Proxy Services, select the Predefined option button from the Service Type dialog box, select Proxy, then select the Enabled check box.
- 10** To configure a rule for SOCKS, select the Predefined option button from the Service Type dialog box, select SOCKS, then select the Enabled check box.
- 11** To configure a rule for VPN, select the Predefined radio button from the Service Type dialog box, select VPN, check the Enabled check box.

Because NDS[®] or eDirectory passwords are a prerequisite for VPN authentication, you only need to define additional method types and enforcement policies if you want users to be authenticated by additional means such as token devices. (VPN users are always required to specify their NDS or Novell eDirectory passwords.)

- 12** Exit the utility.

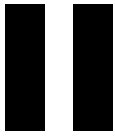
Identity Management

Novell BorderManager features such as VPNs and Proxy Services are dependent upon sound identity management. Many organizations today house identity data in multiple directories. For example, your organization might keep user account information in one tree for authentication purposes and in another tree to reflect organizational structures. In this case, you face the challenge of ensuring that data synchronization is both timely and accurate. An identity management solution can help ensure the integrity of user data by automating data synchronization. Additionally, an identity management solution can also automate the provisioning of resources and data access based on policy.

Novell DirXML[®] is an identity management solution that distributes new and updated information across directories, databases, and critical applications on the network and across firewalls to partner systems. Based on business rules you define, DirXML can ensure that when a new employee is hired or a new partner is brought onto a team, that person will have immediate access to the resources required to get their work moving.

For example, using DirXML, you could define rules that provide immediate eDirectory account creation in both your authentication tree and your hierarchical tree when employee data is entered in your Human Resources database. Based on certain attributes, such as the value of a job title or department, you also could provide access to data held in various internal Web sites while preventing access to data held on other sites. Finally, when this employee or partner leaves the organization, data access would be revoked immediately.

For more information about how DirXML can help you address identity management challenges, refer to the [DirXML Product Page \(http://www.novell.com/products/dirxml/\)](http://www.novell.com/products/dirxml/).



Proxy

The following sections of the *Novell® BorderManager® 3.8 Installation and Administration* guide provide information on how to use the Proxy Services. They also discuss access controls, alerts, and authentication services.

- ♦ [Chapter 2, “Setting Up Proxy Services,” on page 31](#) describes the procedures you need to set up a proxy server.
- ♦ [Chapter 3, “Managing Proxy Services,” on page 49](#) explains how to set up proxy logging and describes the information found in the Proxy Services logs.
- ♦ [Chapter 4, “Advanced Configuration of Proxy Services,” on page 67](#) describes the procedures you need to set up a proxy cache server beyond the basic configuration, and configure various advanced Proxy Services features and parameters.
- ♦ [Chapter 5, “HTTP Proxy Logging Using Nsure™ Audit,” on page 77](#) Novell BorderManager 3.8 is instrumented to use Nsure Audit for HTTP proxy logging. Nsure Audit provides secure logging, reporting, monitoring and notification capabilities.

The following sections describe how to manage the proxy server access control log file:

- ♦ [Chapter 6, “Setting Up Access Control,” on page 83](#) provides the basic steps to set up the proxy server access log file.
- ♦ [Chapter 7, “Managing Access Control,” on page 89](#) provides information on how to view the proxy server access log file

The following sections describe the basic information you need to set up Novell BorderManager 3.8 alerts:

- ♦ [Chapter 8, “Setting Up Alert Notification,” on page 95](#) provides basic steps on how to set up alerts on the proxy server.
- ♦ [Chapter 9, “Managing Alert Messages,” on page 99](#) provides information on how to manage the proxy server alert messages.

2

Setting Up Proxy Services

Proxy Services uses caching to accelerate Internet performance and optimize WAN bandwidth use. Proxy Services also allow protocol filtering and improves security by hiding private network domain names and addresses, and sending all requests through a single gateway.

You can use the service as an application proxy for the following services:

- ◆ HTTP, Gopher, FTP, Simple Mail Transfer Protocol (SMTP), Domain Name System (DNS), RealAudio*, and Real Time Streaming Protocol (RTSP).
- ◆ As a protocol filter to prevent certain kinds of user connections.
- ◆ As a gateway to hide the names and addresses of internal systems so that the gateway is the only hostname known outside the system.

This section explains the tasks you complete to set up Novell® BorderManager® 3.8 Proxy Services.

- ◆ “Proxy Services Prerequisites” on page 32
- ◆ “Setting Up an HTTP Proxy Server” on page 34
- ◆ “Setting Up an HTTP Accelerator Server” on page 35
- ◆ “Blocking Virus Requests in HTTP Accelerator” on page 36
- ◆ “Setting Up an FTP Proxy Server” on page 38
- ◆ “Setting Up an FTP Accelerator Server” on page 39
- ◆ “Setting Up a Mail Proxy Server” on page 40
- ◆ “Setting Up a News Proxy Server” on page 41
- ◆ “Setting Up a Generic Proxy Server” on page 41
- ◆ “Setting Up DNS Proxy” on page 42
- ◆ “Setting Up RealAudio and RTSP Proxies” on page 42
- ◆ “Setting Up the SOCKS Client (Upstream)” on page 43
- ◆ “Setting Up HTTP Transparent Proxy” on page 44
- ◆ “Setting Up Telnet Transparent Proxy” on page 44
- ◆ “Setting Up Proxy Authentication” on page 45
- ◆ “Completing Advanced Setup, Configuration, and Management Tasks” on page 47

NOTE: This section describes the tasks required to set up an initial implementation of Proxy Services. For planning and conceptual information about Proxy Services, refer to [Novell BorderManager 3.8 Overview and Planning Guide \(http://www.novell.com/documentation/lg/nbm38\)](http://www.novell.com/documentation/lg/nbm38).

Proxy Services Prerequisites

Before you set up Proxy Services, ensure that you have the following information at hand:

- ◆ The IP addresses of your server's IP interfaces, and which ones are considered private or public access
- ◆ The port number (8080 by default) and the hostname or IP address of the Novell BorderManager 3.8 proxy server

To prepare the proxy server for Internet access, verify that the following prerequisites have been met:

- ◆ DNS Resolver setup has been performed to provide a valid domain name for the DNS and an IP address of at least one DNS name server to resolve IP hostnames. You should have done this during the Novell BorderManager 3.8 product installation.

- ◆ Packet filtering has been set up to allow DNS query and response packets.

The default installation sets packet filtering to block all incoming and outgoing traffic.

To modify the packet filtering setup, refer to [Chapter 10, "Setting Up Packet Filters," on page 109](#).

- ◆ Corporate users who will use Proxy Services to access Internet Web sites have set up their Web browsers to use the Novell BorderManager 3.8 proxy server, as described in the following sections:

["Proxy Services Prerequisites" on page 32](#)

You can also use the Novell BorderManager 3.8 HTTP Transparent proxy feature to set up background, automatic proxy services. With HTTP Transparent proxy, users are not required to configure their browsers to use a proxy; it is done invisibly for them.

For more information about using HTTP Transparent proxy, refer to ["Setting Up HTTP Transparent Proxy" on page 44](#).

- ◆ Novell Public Key Infrastructure (PKI) Services and Secure Authentication Service (SAS) should be installed on the server to support Secure Sockets Layer (SSL) authentication of SOCKS 5 clients.

PKI and SAS are installed automatically during Novell BorderManager 3.8 installation if the services have not been previously installed.

After SAS and PKI are installed, you must use the PKI snap-in to NetWare[®] Administrator to perform following SSL-related administrative tasks:

- ◆ Importing certificates signed by an external Certificate Authority (CA)
- ◆ Creating and managing Key Material Objects (KMOs) used to store key pairs in NDS[®] or Novell eDirectory[™]
- ◆ Creating an NDS or eDirectory tree CA to sign certificates used on a private network

Refer to the Novell PKI online help in NetWare Administrator for the procedures to create and manage NDS or eDirectory tree CAs and KMOs.

Setting Up the DNS Resolver

To set up the DNS Resolver, complete the following steps at the server console:

- 1** Enter **LOAD INETCFG**, then select Configure NIAS > Protocols and Routing > Protocols > TCP/IP and DNS Resolver Configuration.
- 2** Specify the DNS domain name for your corporation or organization.
Your Internet Service Provider (ISP) typically supplies this name. Domain names usually take the form company_name.com or organization.org, for example, novell.com or acme.org.
- 3** Specify the IP addresses of up to three DNS name servers in the Name Server fields.
ISPs often provide access to multiple DNS name servers.
- 4** Press Esc to select Yes to update the TCP/IP configuration.
- 5** Press Esc until you return to the Internetworking Configuration menu, then select Reinitialize System and exit INETCFG.

Setting Up Microsoft Internet Explorer to Use a Web Proxy

To specify the Novell BorderManager 3.8 proxy server on a Microsoft* Internet Explorer Web browser:

- 1** Launch Internet Explorer, then select the following menu paths, based on the software version.
 - ◆ For Internet Explorer 5.5, select Tools > Internet Options > Connections > LAN Settings > Use a Proxy Server
- 2** Specify the port number (8080 by default) and hostname or IP address of the Novell BorderManager 3.8 proxy server in the proxy field.
- 3** Click Apply.

To use the advanced option where you can set the same proxy for all applications:

- 1** Launch Internet Explorer, then select the following menu paths, based on the software version.
 - ◆ For Internet Explorer 5.5, select Tools > Internet Options > Connections > LAN Settings > Use a Proxy Server > click Advanced > select the check box Use the Same Proxy for All Protocols.
- 2** Specify the port number (8080 by default) and hostname or IP address of the Novell BorderManager 3.8 proxy server in the proxy field.
- 3** Click Apply.

Setting Up Netscape Navigator to Use a Web Proxy

To specify the Novell BorderManager 3.8 proxy server on a Netscape Navigator* 3.x Web browser:

- 1** Launch Netscape Navigator, then select Options > Network Preferences > Proxies > Manual Proxy Configuration.
- 2** Click View.
- 3** Specify the port number (8080 by default) and hostname or IP address of the Novell BorderManager 3.8 proxy server in the proxy field.
- 4** Click OK.

To specify the Novell BorderManager 3.8 proxy server on a Netscape Navigator 4.x Web browser:

- 1 Launch Netscape Navigator, then select Edit > Preferences > Advanced > Proxies > Manual Proxy Configuration > View.
- 2 Specify the URL of the Novell BorderManager 3.8 proxy server in the URL field.
- 3 Click OK.

Setting Up an HTTP Proxy Server

HTTP proxy resolves URL requests on behalf of Web clients on your network. This is also known as forward proxy. These requests are cached, if possible, on the proxy server to increase the speed of delivering the same content the next time the same information is requested.

The proxy server can also be set up as an HTTP accelerator (reverse proxy) to accelerate Web server requests from Internet users for your Web servers on your intranet. You can set up a server to be an HTTP proxy server, an HTTP accelerator server, or both.

To set up an HTTP proxy server:

- 1 In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2 From the Application Proxy tab, select the HTTP Proxy check box.
- 3 Click Details or double-click the HTTP Proxy service.
- 4 Click the HTTP tab > specify the number of the HTTP listening port.

This is the port on which the proxy server listens for incoming URL requests from browser clients. The default is 8080.

NOTE: The HTTP proxy listens on interfaces identified as Private or Both, but not on interfaces identified as Public.

- 5 Specify your preferences:
 - ♦ **Ignore Refresh Requests from the Browser:** If you select this option, the proxy does not access the Web server for a URL when a user specifies to reload or refresh from the browser. All user requests are filled from the cache.
 - ♦ **Filter Cookies:** If you select this option, the cookie header is not forwarded to the origin server, and pages with the Set-Cookie header are not cached. Enable this option to increase security.
 - ♦ **Enable Persistent Connections to Browsers:** If you select this option, the connection between a browser and a proxy server remains active even if there is no data flow.
 - ♦ **Enable Persistent Connections to Origin Servers:** If you select this option, the connection between the origin server and the proxy remains active even if there is no data flow.
 - ♦ **Enable or Disable Java Applet Stripping from HTML Files:** When enabled, Java* applets are stripped from the HTML file before the file is displayed in the browser window.
- 6 Click OK, then click OK again from the Novell BorderManager 3.8 Setup page.

To set up authentication for an HTTP proxy server, refer to [“Setting Up Proxy Authentication” on page 45](#).

Setting Up an HTTP Accelerator Server

HTTP acceleration is also known as reverse proxy. In this case, the server acts as the front end to your Web servers on your Internet or intranet. Heavily loaded servers benefit from off-loading frequent requests to the proxy server. Security is also increased when the IP addresses of your Web servers are hidden from the Internet.

You need at least one private and one public address to use the proxy server. You can, however, use a single address as both a public address and a private address. The HTTP accelerator listens on interfaces identified as Public or Both, but not on interfaces identified as Private. The best security involves two interfaces.

You can set up a server to be an HTTP accelerator server, an HTTP proxy server, or both.

To set up an HTTP accelerator server:

- 1** In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2** Click the Acceleration tab, select the HTTP Acceleration check box.
- 3** Click Details or double-click the HTTP Acceleration service.
- 4** Click Add to add a new acceleration server to the HTTP Accelerator list:
 - 4a** Specify whether to enable this HTTP accelerator server after you have set it up.

The default is Disabled. Specify to disable the server if you are setting up for multiple accelerations. You can disable one or more servers without affecting the other accelerated sites.
 - 4b** Specify whether to enable authentication for this accelerator.
 - 4c** Specify the accelerator server name.

If reverse proxy authentication is enabled the accelerator server name must be the DNS domain name of the Web site that is being accelerated. The DNS domain name entry should be the same for both inbound and outbound configurations.
 - 4d** Specify the port number the origin Web server is listening on for incoming connections.

The default is 80 for HTTP.
 - 4e** Click Add, then specify a Web server name or IP address.
 - 4f** Click Add, then select one or more public proxy IP addresses.

These are the addresses the accelerator will listen on for incoming connections from the Internet.

You can associate one or several public IP addresses with a particular domain name, but the combination of the IP address and the port must be unique.

For example, you have a Web server `www1.myco.com` and two proxy IP addresses (1.2.3.4 and 1.2.3.5), and the Web server is listening on port 80. You can configure an accelerator entry for `www1.myco.com` with port 80 and two proxy IP addresses (1.2.3.4 and 1.2.3.5).

As another example, you have multiple Web servers and several proxy IP addresses. You can configure two entries: one for `www1.myco.com` with port 80 and IP address 1.2.3.4, and another for `www2.myco.com` with port 80 and IP address 1.2.3.5.
 - 4g** Specify whether to accelerate on a different port, and specify an accelerator port number.

All internal Web server links must be relative URLs.

5 Click OK, then click OK again from the Novell BorderManager 3.8 Setup page.

To set up authentication for an HTTP accelerator server, refer to [“Setting Up Proxy Authentication” on page 45](#).

Blocking Virus Requests in HTTP Accelerator

For Web servers that are being accelerated by Novell BorderManager 3.8's reverse proxy capability, Novell has added a new Virus Pattern Recognition feature to Novell BorderManager 3.8 that can help protect against such attacks. This enhancement includes features to facilitate its configuration and monitoring.

To enable this feature, you must have the latest version of proxy.nlm.

You also need the following lines in the sys:\etc\proxy\ proxy.cfg file, which is used to initialize the Novell BorderManager Proxy Server at startup:

```
[Extra Configuration]

ScanVirusPatterns=1

[Virus Pattern Configuration]

NoOfVirusPatterns=0

PatternSize=16

PatternStartOffset=1

EnablePatternAutoUpdate=1
```

If you don't have these lines in the proxy.cfg file when you start the Proxy Server, you will receive a "virus command not found" message on the system console when you try to specify any of the console commands described below.

Command Line Configuration

Configuration of the Virus Pattern Recognition feature is accomplished via console commands that are run from the system console. As with most console-based systems, responses to commands are written back to the system console and recorded in a log file (in this case, proxy.log).

NOTE: The command syntax below is specified in BNF (Backus-Naur Format) notation, a formal system of notation developed in the 1960s to describe the syntax of a given command set or computer programming language.

Adding and Deleting Virus Request Patterns

After the Proxy Server is up and running with its initial pattern database loaded, you can add new patterns while the server is running. The console command syntax for adding a new virus pattern is as follows:

```
virus add -p pattern -o origLength
```

where *pattern* is a 16-byte character string located at offset 1 in the HTTP GET request, and *origLength* is the original size of the request in bytes. These are mandatory option-value pairs. The string value for *pattern* should be enclosed in quotation marks; the value for *origLength* is given as an integer. For example:

```
virus add -p "default.ida?NNNN" -o 385
```

The Proxy Server looks at the specified offset in each incoming request and reads the next 16 bytes. If that string matches any of the patterns in the existing database, the request is considered a virus request and is blocked.

NOTE: The pattern size and start offset are set to 16 and 1, respectively, by default. You can change these values in the proxy.cfg file, but do so with caution. They are global parameters that apply to all entries in the pattern database.

To delete a pattern from the database, use the same syntax but replace the add command with del. For example:

```
virus del -p "default.ida?NNNN" -o 385
```

Updating the Database via a Script (NCF File)

Another aspect of the Virus Pattern Recognition feature is the capability to update the database in a script-like fashion by placing a list of virus add commands in an NCF file and running the file on the console. This enables you to update the virus pattern database without having to bring the Proxy Server down.

You can use the following command to write all existing entries in the database into an NCF file:

```
virus dump
```

The name of the dump file is sys:\etc\proxy\virpat.ncf. This NCF file can be run as part of the Proxy Server restart process, or you can run it manually after the Proxy Server has been loaded.

Enabling and Configuring Auto Update

Novell BorderManager 3.8 provides an Auto Update feature that automatically detects virus requests and adds their patterns to the database. This feature's heuristic (self-learning) request examination method is especially useful in detecting frequently changing virus request patterns.

The heuristics look at the incoming request distribution within a specified amount of time. For these heuristics to work, two parameters must be properly configured:

Threshold: This parameter defines the number of new requests that hash to the same value that is allowed within the time interval before those requests are considered suspect. The default value is 250; this can be changed via the virus -t *threshold* console command.

Refresh Time Interval: This parameter defines the amount of time, in seconds, after which identical requests received beyond the threshold value are checked for virus pattern content. The default value is 10 seconds; this can be changed via the virus -r *time interval* console command.

When more than the threshold number of identical requests are received within the specified time interval, that request is considered suspect and is scheduled for further analysis via a background process. In the meantime, the Proxy Server continues to receive all requests so that valid requests are never blocked.

The Virus Pattern Configuration screen provides information that can help you adjust these parameters for your particular system. See [“Choosing a Proper Threshold” on page 61](#) for details.

There are two ways to enable this Auto Update feature. One is by entering the following command at the system console: **virus -e 1**

NOTE: Specifying a value of 0 (zero) in this command disables Auto Update.

The other way to enable this feature is to place the following option in the proxy.cfg file:

```
[Virus Pattern Configuration]
```

```
EnablePatternAutoUpdate=1
```

Adding New Virus Keywords

Virus request patterns of the same virus type contain keywords or character strings that can be used to identify the request.

For example, all URLs with Code Red virus requests contain the string `cmd.exe`. Because the presence of this string identifies the URL as a virus request, "`cmd.exe`" is a keyword.

NOTE: In this Code Red example, adding `*CMD.EXE*` as a filter rule in routers blocks all requests containing this keyword.

Keywords come into play only after a request has been labelled as suspect through the heuristics described above. At that point, the suspect request is checked for the presence of certain keywords. If a match is found, the request is labelled a virus request and its pattern is added to the database. Any future requests containing that keyword are automatically blocked.

To add a new keyword to the list of existing keywords, enter the following command at the system console:

```
virus add -k keyword
```

where *keyword* is a character string that determines whether a suspect request is a humble request or a virus request.

Monitoring the Virus Pattern Recognition Feature

Because the effectiveness of a feature can be best understood through monitoring, the Novell BorderManager Proxy Server includes a Virus Pattern Configuration screen. All virus pattern-related configuration and statistical information is tracked and displayed on this separate server console screen.

Effect on Performance

Because there is very little overhead involved in checking incoming HTTP requests, enabling the Virus Pattern Recognition feature does not adversely affect Novell BorderManager Proxy Server performance.

Setting Up an FTP Proxy Server

You can use an FTP proxy server to control access to FTP sites. This enforces centralized control over Internet or intranet access. You can also use an FTP proxy server to cache data for anonymous users to enable faster downloads.

NOTE: The proxy server can also be set up as an FTP accelerator to accelerate FTP requests from Internet or intranet users to your FTP servers. You can set up a server to be an FTP proxy server, an FTP accelerator server, or both. If the server is set up for both, you must have separate public and private addresses.

To set up an FTP proxy server:

- 1 In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2 From the Application Proxy tab, select the FTP Proxy check box.
- 3 Click Details or double-click the FTP Proxy service.
- 4 Specify a username and password separator.

The username/password separator is used to separate the NDS or eDirectory username, FTP username, and FTP hostname in the USER command; and the NDS or eDirectory user password and FTP password in the PASS command. The user enters these commands when connecting to the FTP proxy. The default is the dollar sign (\$).

For example, enter the following at the user and pass prompts:

```
user>john_smith.novell$anonymous$ftp.novell.com
pass> xxxxx$yyyyy
```

where john_smith.novell is the NDS or eDirectory username, anonymous is the FTP username, ftp.novell.com is the FTP host, xxxxx is the NDS or eDirectory password for john_smith, and yyyyy is the FTP password for anonymous users at ftp.novell.com.

- 5 Specify an anonymous FTP e-mail address or keep the default.

This is the e-mail address used as the password for the anonymous FTP login by the FTP client of the proxy server. The default is NovellProxyCache@.

- 6 Select a method of user authentication among the following: none, clear text username and password, or single sign-on.
 - ♦ **None:** The user is not required to specify the FTP proxy username and password when accessing the FTP server, and needs to supply only the FTP hostname and password.
 - ♦ **Clear Text Username/Password:** The user must specify a fully distinguished NDS or eDirectory username, FTP username, and FTP hostname at the user prompt; and an NDS or eDirectory password and FTP password at the pass prompt.
 - ♦ **Single Sign-On:** If a user is logged in to NetWare through the latest Novell Client™, the user is not prompted to authenticate to the proxy.

- 7 Click OK, then click OK again from the Novell BorderManager 3.8 Setup page.

To also set up the server as an FTP accelerator as well, refer to [“Setting Up an FTP Accelerator Server” on page 39](#).

Setting Up an FTP Accelerator Server

FTP acceleration is also called FTP reverse proxy. The server acts as the front end to your FTP servers on your Internet or intranet. Frequent requests can be off-loaded from heavily loaded origin FTP servers to the proxy server. Security is increased when the IP addresses of your FTP servers are hidden from the Internet or intranet.

NOTE: You can set up a server to be an FTP accelerator server, an FTP proxy server, or both. If the server is set up for both, you must have separate public and private addresses.

To set up an FTP accelerator server:

- 1 In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2 From the Acceleration tab, select the FTP Acceleration check box.
- 3 Click Details or double-click an FTP Acceleration service.
- 4 Click Add:
 - 4a Specify whether to enable the FTP accelerator server after you have set it up.
 - 4b Specify the hostname of the origin FTP server.
 - 4c Select one or more public proxy IP addresses from the list.

These are the addresses the accelerator will listen on for incoming connections from the Internet.

You can associate one or several public IP addresses with a particular domain name, but the combination of the IP address and the port must be unique.

For example, you have an FTP server ftp://ftp1.myco.com and two IP addresses (1.2.3.4 and 1.2.3.5), and the FTP server is listening on port 21. You can configure an accelerator entry for ftp1.myco.com with port 21 and two IP addresses (1.2.3.4 and 1.2.3.5).

As another example, you have multiple FTP servers and several IP addresses. You can configure two entries: one for ftp1.myco.com with port 21 and IP address 1.2.3.4, and another for ftp2.myco.com with port 21 and IP address 1.2.3.5.

- 5 Click OK, then click OK again from the Novell BorderManager 3.8 Setup page.

Setting Up a Mail Proxy Server

A Mail proxy server provides secure SMTP mail services for incoming and outgoing mail. It can also be used to hide internal domain names and mail hosts for scanning incoming mail. You can use the Mail proxy between the existing intranet mail server and the Internet, or directly between the intranet and the Internet without an intranet mail server.

If Mail Proxy is selected during install, the DNS name of the server is available in NWAdmn. Enter the IP address manually.

To set up a Mail proxy server:

- 1 In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2 From the Application Proxy tab, select the Mail Proxy check box.
- 3 Click Details or double-click the Mail Proxy service.
- 4 Specify values for the following Mail proxy parameters:
 - ♦ **Spool Directory:** The directory in which the mail files are temporarily stored.
This must be an absolute path on the server, including the volume name, for example, sys:\etc\proxy\spool.
 - ♦ **Spool Directory Max Size:** The maximum size (in MB) of the mail spool directory.
 - ♦ **Max Mail Size:** The maximum size (in MB) of a mail item.
 - ♦ **Failed Mail Retry Intreval:** The maximum number of minutes before the next attempt by the Mail proxy to forward undeliverable mail.
 - ♦ **Failed Mail Retry Count:** The maximum number of times the Mail proxy attempts to forward undeliverable mail.
 - ♦ **Primary Mail Domain Name:(Optional)** The domain name that is used to substitute the From address in an e-mail message. This name replaces the internal domain name in outbound mail headers and hides the internal network architecture. If this parameter is unspecified, the local DNS domain name is used as the primary mail domain name. If the local DNS domain name is not configured as well, the From address remains as is.
 - ♦ **Internal Mail Server Name:** The Mail eXchange (DNS MX record) name or internal mail domain name of the mail server on the internal network.
 - ♦ **POP3 Mail Server Name:** The name or IP address of the server running the Post Office Protocol 3 (POP3) software.

- 5 Click OK, then click OK again from the Novell BorderManager 3.8 Setup page.

Setting Up a News Proxy Server

A News proxy server accesses Usenet news on the Internet and provides secure Network News Transfer Protocol (NNTP) news services for transferring news articles in both directions between the intranet and the Internet. A News proxy server can also selectively filter out unwanted news groups. However, a News proxy server cannot cache news articles.

To set up a News proxy server:

- 1 In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2 From the Application Proxy tab, select the News Proxy check box.
- 3 Click Details or double-click the News Proxy service.
- 4 (Optional) Specify the primary news domain name.

This is the domain name that is used to substitute the From address in posted news articles. This name replaces the internal originating hostnames in outbound news article header lines and hides the internal network architecture. If this parameter is unspecified, the News proxy uses the DNS domain name in the From address.

- 5 (Optional) Specify the server name or IP address of the private (internal) news servers to which the incoming news articles are forwarded.

If you do not specify this information, the proxy server does not accept the connections from the public news servers to forward or retrieve articles from the private news servers.

- 6 Click Add and specify the DNS hostnames or IP addresses of the public (external) news servers from which news articles are retrieved.

You must specify at least one server for the News proxy to work if a private news server is set up. The proxy connects to the first public news server on the list, and all queries from the private news server and readers are forwarded to that server. If the connection to the first server on the list fails, the News proxy will use the next server on the list, and so on.

- 7 Click OK from the Novell BorderManager 3.8 Setup page.

Setting Up a Generic Proxy Server

Use a Generic proxy server to access multiple protocols if the application proxy you need (for example, Telnet and rlogin) is not already defined in Novell BorderManager 3.8. Generic proxy tunnels data without caching it.

To set up a Generic TCP or UDP proxy server:

- 1 In NetWare Administrator, select the BorderManager Setup page for the server.
- 2 From the Application Proxy tab, select the Generic TCP Proxy or the Generic UDP Proxy check box.
- 3 Click Details, or double-click the Generic TCP Proxy service or the Generic UDP Proxy service.

NOTE: The following steps are the same for setting up a Generic TCP or UDP proxy server.

- 4 Click Add to add a server to the Forward List:
 - 4a Specify whether to enable the Generic proxy server after you have set it up.

4b Specify the hostname of the origin server.

4c Specify the port number, to the origin server as the origin server is listening on for incoming connections.

The default is 0 for Generic proxy.

4d Select one or more public proxy IP addresses of the proxy server.

These are the addresses you want the proxy to listen on for incoming connections from the Internet.

4e Specify the port number for the proxy server.

The default is 0.

You can associate one or several public IP addresses with a particular domain name, but the combination of the IP address and the port must be unique.

4f Click OK.

5 Click OK from the Novell BorderManager 3.8 Setup page.

Setting Up DNS Proxy

DNS proxy acts as a DNS name server for clients on the intranet. The DNS proxy caches DNS records.

NOTE: The intranet client must have the private IP address of the DNS proxy configured as the address of the DNS name server.

For servers, you can set up the IP addresses of the DNS name servers and the domain name in the `sys:\etc\resolv.cfg` file.

To enable DNS proxy:

- 1** In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2** From the Application Proxy tab, select the DNS proxy check box.
- 3** Click Details, or double-click the DNS proxy service.
- 4** Click OK from the Novell BorderManager 3.8 Setup page.

Setting Up RealAudio and RTSP Proxies

RealAudio and RTSP proxies access a RealAudio server on the Internet and enable an intranet user to download and play back audio and video information in real time.

To enable RealAudio and RTSP proxies:

- 1** In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2** From the Application Proxy tab, select the RealAudio and RTSP Proxies check box.
- 3** Click Details, or double-click the RealAudio and RTSP Proxies service.
- 4** Click OK, then click OK again from the Novell BorderManager 3.8 Setup page.

Setting Up the SOCKS Client (Upstream)

This feature enables a proxy to authenticate through a SOCKS 4 or SOCKS 5 firewall. SOCKS is a circuit-gateway type of protocol. With SOCKS, hosts behind a firewall can gain full access to the Internet without full IP reachability. When SOCKS support is enabled, all requests sent to the Internet are forwarded to a SOCKS 5 server and the proxy is used for caching only.

When the proxy receives a request, it checks its cache. If the requested object is not in the cache, the proxy makes a TCP connection to the SOCKS server and redirects the request from the intranet to the SOCKS server, allowing for more secure Internet access. The SOCKS server then connects to the origin server and retrieves the object. Null and username/password authentication are supported.

Setting up HTTP or FTP proxy support through SOCKS has the following steps:

- 1** In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2** From the Application proxy tab, select HTTP or FTP proxy.
- 3** Click SOCKS Client, then select the Enable SOCKS check box.
- 4** Specify the IP address of the SOCKS server.
- 5** Specify the port number of the SOCKS server.

The default is 1080.

- 6** Click Username/Password, then specify a username and password that the proxy will use to authenticate with the SOCKS server.

If you select No Authentication and do not specify a username and password, null authentication is used. The username and password must match the username and password configured for the SOCKS server or at the third-party SOCKS server.

If you configure null authentication, make sure that the SOCKS server is set up to allow null authentication.

- 7** Click OK to close the SOCKS Client page.
- 8** If you are not using a third-party SOCKS server:

NOTE: The following steps apply only if the upstream SOCKS server is running Novell BorderManager 3.8.

- 8a** Click the Gateway tab.
- 8b** Select the SOCKS V4 and V5 check box, then click Details.
- 8c** (Optional) Specify the port number of the SOCKS server.

The default is 1080.

- 8d** Select SOCKS V5 or SOCKS V4.

Select V5 if the server must work with the Novell BorderManager 3.8 SOCKS client. If you select V5, select single sign-on and specify an authentication scheme. If you select SSL as an authentication scheme, select a key ID.

NOTE: Use the NetWare Administrator PKI Services to change and create key IDs in an NDS or eDirectory tree.

- 8e** Select an authentication method.
- 8f** Click OK.

- 8g** Select the Users setup page and specify the username and password of the SOCKS client.
The username and password must match the username and password you configured for the SOCKS.
- 8h** Click OK.
- 9** Click OK from the Novell BorderManager 3.8 Setup page.
- 10** To use a browser from a workstation, open the configuration window for the browser. In the field provided to specify the location of the HTTP proxy, specify the IP address or DNS hostname of the server running Novell BorderManager 3.8.
This allows requests from the browser to be sent to the SOCKS client operating with Novell BorderManager 3.8 Proxy Services, then forwarded to the SOCKS server if the requested information is not found in the proxy cache.

Setting Up HTTP Transparent Proxy

HTTP Transparent proxy enables you to use an HTTP proxy server without reconfiguring each of the user's browsers. Use HTTP Transparent proxy to require users to send requests through the proxy server.

When you use HTTP Transparent proxy, the clients must use the proxy's private IP address as the TCP/IP gateway address. IP forwarding must be enabled on the server.

To set up HTTP Transparent proxy:

- 1** In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2** From the Transparent Proxy tab, select the Transparent HTTP Proxy check box.
- 3** Click Details or double-click the Transparent Proxy service.
- 4** Click Add and specify a port for monitoring.
For example, specify 80 for HTTP traffic.
- 5** In the Exception IP Address List, click Add and specify a local IP address.
- 6** Click OK from the Novell BorderManager 3.8 Setup page.

To set up authentication for HTTP Transparent proxy, refer to [“Setting Up Proxy Authentication” on page 45](#).

Setting Up Telnet Transparent Proxy

Telnet Transparent proxy enables you to use a Telnet proxy server without manually connecting to a proxy server.

When you use Telnet Transparent proxy, the clients must either use the proxy's private IP address as the TCP/IP gateway address or the proxy server must be in the routing path. IP forwarding must be enabled on the server.

To set up Telnet Transparent proxy:

- 1** In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2** From the Transparent Proxy tab, select the Transparent Telnet Proxy check box.
- 3** Click Details or double-click the Transparent Telnet service.

- 4 Click Add and specify a port for monitoring.
For example, specify 23 for Telnet traffic.
- 5 In the Exception IP Address List, click Add and specify a local IP address.
- 6 Click OK page.

To set up authentication for Telnet Transparent proxy, refer to [“Setting Up Proxy Authentication” on page 45](#).

Setting Up Proxy Authentication

IMPORTANT: An additional method of authentication is available for proxy server users. Proxy server users can use security devices such as hardware tokens in addition to using an NDS or eDirectory password. Login policies defining the authentication rules and access methods required for remote users to authenticate are stored in the NDS or eDirectory Login Policy object.

The following section provides information about setting up proxy authentication:

[“Setting Up Proxy Authentication” on page 45](#)

Setting Up HTTP Proxy Authentication

Proxy authentication for HTTP proxy and HTTP acceleration (reverse and forward HTTP proxy) can be accomplished in the following ways:

- ♦ **Single Sign-on for Novell Client32 Clients:** If a user is logged in to NetWare through the latest Novell Client software and uses the browser, the user is not prompted to authenticate again to the proxy.
- ♦ **SSL Proxy Authentication:** The user is not prompted to authenticate to the proxy if he or she is already logged in to NDS or eDirectory.

You can enable HTTP proxy NDS or eDirectory authentication and require all users to authenticate with their browsers before they access the proxy server and the Internet.

Proxy authentication consists of a username and a password. The proxy authentication password is the same as a user's NDS or eDirectory authentication password. Any type of browser client can be authenticated: Windows 98, Windows 2000, Windows XP, Windows Me, Windows NT, UNIX, OS/2*, or Macintosh*.

If proxy authentication is enabled and both single sign-on and SSL are enabled, the proxy server will first try to authenticate the user through single sign-on. If the single sign-on attempt fails or is not enabled, the proxy server will attempt authentication using SSL.

Single sign-on is successful only when the client machine is running the Novell Client 32 software and has logged in to NDS or eDirectory. The client machine must also be running `dwntrust.exe` and `clntrust.exe`. These files are located in the `sys:public` directory on the server.

To set up HTTP proxy authentication:

- 1 In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2 Click Authentication Context.
- 3 From the Authentication tab, select the Enable HTTP Proxy Authentication check box.
- 4 Select an authentication scheme: single sign-on or SSL.
- 5 For single sign-on, specify the time to wait for a single sign-on reply.

- 6** For SSL:
 - ◆ **SSL Listening Port:** Specify the port used for authentication. You might need to change the port number to prevent reverse proxy traffic from running into SSL traffic. Both reverse proxy and SSL traffic default to port 443.
 - ◆ **Key ID:** Specify the key ID exchanged between the client and server for authentication. Use the NetWare Administrator PKI Services to change and create key IDs in an NDS or eDirectory tree.
 - ◆ **Notification Method:** Specify whether to send authentication notification in HTML form or as a Java applet.
 - ◆ **Idle Time:** Specify the length of time a connection can remain idle before a new login is required.
- 7** Specify whether to authenticate only when the user attempts to access a restricted page.
- 8** Click the Context tab.
- 9** Click Add, then specify the user's default NDS or eDirectory context and tree name.

Specify a fully distinguished NDS or eDirectory container name (sales.my_org, for example). The NDS or eDirectory container name can have up to 256 characters. This entry is optional and makes logging in easier for users. Users in the specified container can log in by typing only their login names without the complete context string.
- 10** Click OK from the Novell BorderManager 3.8 Setup page.

Session Failover

This new feature allows multiple proxies to share the user's authentication information. Therefore the user need not log into different proxies whenever he switches proxies.

When multiple NBM 3.8 proxies were deployed under load balancing using L4 switches, clusters, DNS round robin etc., authenticated sessions were not shared. If authentication is enabled, switching between proxies required the user to re-authenticate himself with the new proxy server.

This problem is solved with Novell BorderManager 3.8.4 release whereby, proxy now provides session fail-over support for SSL authentication. For session fail-over, all the proxies should be in a single tree, or identical trees with common username for proxy authentication.

For Configuration details of the agent components refer [“Configuring Session Failover” on page 73](#)

Setting Up HTTP Transparent Proxy Authentication

- 1** In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2** Click Authentication Context.
- 3** From the Authentication tab, select the Enable HTTP Proxy Authentication check box.
- 4** Click the Context tab.
- 5** Click Add and specify the user's default NDS or eDirectory context and tree name.

Specify a fully distinguished NDS or eDirectory container name (sales.my_org, for example). The NDS or eDirectory container name can have up to 256 characters. This entry is optional

and makes logging in easier for users. Users in the specified container can log in by typing only their login names without the complete context string.

- 6 Click OK from the Novell BorderManager 3.8 Setup page.

Setting Up Telnet Transparent Proxy Authentication

- 1 In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2 Click Authentication Context.
- 3 From the Authentication tab, select the Enable Transparent Telnet Proxy Authentication check box.
- 4 Click the Context tab.
- 5 Click Add, then specify the user's default NDS context and tree name.

Specify a fully distinguished NDS or eDirectory container name (sales.my_org, for example). The NDS or eDirectory container name can have up to 256 characters.

This entry is optional and makes logging in easier for users. Users in the specified container can log in by typing only their login names without the complete context string.

- 6 Click OK from the Novell BorderManager 3.8 Setup page.

Completing Advanced Setup, Configuration, and Management Tasks

In addition to the basic setup procedures described in this chapter, there are several advanced setup, configuration, or management procedures you might need to complete, depending on your specific configuration.

Advanced tasks are available in [Chapter 4, “Advanced Configuration of Proxy Services,” on page 67](#) and include the following:

- ◆ Configuring cache parameters
- ◆ Specifying batch downloading
- ◆ Configuring caching hierarchies
- ◆ Configuring session failover
- ◆ Specifying transport timeout parameters
- ◆ Specifying DNS parameters
- ◆ Setting up HTTP proxy services logging
- ◆ Monitoring proxy cache real-time activity
- ◆ Viewing host statistics
- ◆ Displaying records
- ◆ Viewing host record entries
- ◆ Viewing user statistics
- ◆ Viewing user log entries
- ◆ Viewing usage trends

- ◆ Exporting data

3

Managing Proxy Services

The following sections explain the tasks you complete to manage Novell® BorderManager® 3.8 Proxy Services:

- ◆ “Setting Up HTTP Proxy Services Logging” on page 49
- ◆ “Monitoring Proxy Cache Realtime Activity” on page 50
- ◆ “Viewing User Statistics” on page 51
- ◆ “Viewing Host Statistics” on page 52
- ◆ “Exporting Data” on page 53
- ◆ “Managing Virus Pattern Recognition” on page 60
- ◆ “Mail Proxy” on page 62
- ◆ “Authentication” on page 64
- ◆ “Proxy Configuration Dump Tool” on page 66
- ◆ “Splash Screen Settings” on page 66

Setting Up HTTP Proxy Services Logging

You can set up proxy logging for the HTTP server or HTTP acceleration at any time.

Logging does not appreciably slow access to Internet services and locally cached information. You can, therefore, leave logging enabled for an extended period of time.

The following types of logging are available:

- ◆ Common format: Logs the remote hostname, user's remote login name, authenticated username, date, request line from client, status, and length of data in bytes.
- ◆ Extended format: Logs the common format information plus cached status, date, time, client IP address, URL method, and URL.
- ◆ Indexed format: Also referred to as the audit log. Logs the common and extended format information plus when access was allowed or denied, the IP address that initiated an access attempt, the destination, the HTTP command used, and the result of the attempt (hit or miss).

In addition to setting up common format, extended format, or indexed format logging for an HTTP server or HTTP acceleration using this procedure, you can also set up indexed format logging for FTP, Mail, News, Generic, Domain Name System (DNS), and RealAudio and Real Time Streaming Protocol (RTSP) proxy services from the individual proxy configuration dialogs. Refer to the individual proxy service configuration procedures in <<*name of book*>> for more information.

To set up HTTP proxy logging, complete the following steps:

- 1** In NetWare Administrator, double-click the Server object representing the Novell BorderManager 3.8 server and select Novell BorderManager 3.8 Setup.
- 2** Complete any one of the following:
 - ◆ For HTTP, select HTTP proxy from the Application Proxy page, then click Details.
 - ◆ For HTTP acceleration, select HTTP proxy from the Acceleration page, then click Details. From the HTTP Acceleration list, double-click an accelerator or click Add.
- 3** Click the Logging tab, then select one or more of the logging formats (common, extended, or indexed).
- 4** If you have selected common or extended logging, click the format name and specify the following parameters for each format:
 - ◆ Log File Directory: Directory to which the common or extended format log file is written.
 - ◆ Log Rollover: How often the file is overwritten (rolls over) by time (days or hours) or by size (KB or MB).
 - ◆ Old Log Files: Whether old log files are deleted because of their age or because of the number of old log files that are retained in the database.
 - ◆ Stop Services If Logging Fails: When enabled, stops all proxy services when the log file is full and log rollover is not specified.
- 5** Click OK, then click OK again from the Novell BorderManager 3.8 Setup page.

Monitoring Proxy Cache Realtime Activity

To display the Proxy Cache Monitor window and view proxy cache activity information:

- 1** In NetWare Administrator, click the Server object representing the Novell BorderManager 3.8 server.
- 2** Select Novell BorderManager 3.8 from the Tools menu.
- 3** Click Proxy Cache, then select Monitor Realtime Activity from the Object menu.

The Proxy Cache Monitor window displays, providing the following information about proxy activity:

- ◆ Sites Cached: Number of proxy sites currently in the cache.
- ◆ Bytes Cached: Number of bytes cached on the proxy server.
- ◆ Bytes Transferred: Number of bytes transferred to the proxy server.
- ◆ Cache Misses: Number of times the cache was unable to serve a client request.
- ◆ Cache Hits: Number of times the cache was able to serve a client request.
- ◆ Hostname: Name of the Web server, including the name of the service (HTTP, for example) and the DNS domain name of the server.
- ◆ Connections: Number of TCP connections required for a direct connection to the host server. This number represents the number of connections the proxy cache has saved its clients, because Proxy Services has cached the site.
- ◆ Bytes from Cache: Number of bytes transferred from the cache.
- ◆ Bytes from Host: Number of bytes transferred from the host to the cache.

- ◆ Bytes from Neighbors: Number of bytes transferred from the nearest neighbors to the cache.

Viewing User Statistics

To display user statistics in the proxy services audit log:

- 1** In NetWare Administrator, click the Server object representing the Novell BorderManager 3.8 server.
- 2** Select Novell BorderManager 3.8 from the Tools menu.
- 3** Click Proxy Cache, then select View Audit Log from the Object menu.
- 4** Double-click the entry for that host in the first list in the User Statistics window to display a window with the the Number of Users list and the Hosts Accessed list.

Click the column heading of either list box to sort the entries in that column in ascending or descending order. The sorting order is reversed each time you click the column heading.

The Number of Users list provides the following information about Proxy Services activity:

- ◆ Username: NDS or Novell eDirectory name or IP address of the user. For an IP address, the DNS domain name will be displayed if it exists in the local DNS list.

The local DNS list is built automatically each time the WHO IS or DNS Hostname command is invoked using the right-click menu.

- ◆ Hosts Accessed: Number of hosts accessed for the specified period of time.
- ◆ Hit Volume: Total number of times data was found in the cache for all hosts accessed.
- ◆ Miss Volume: Total number of times data was not found in the cache for all hosts accessed.
- ◆ Hit Size: Total amount of data that was found in the cache for all hosts accessed.
- ◆ Miss Size: Total amount of data that was not found in the cache for all hosts accessed.

The Hosts Accessed list box provides the following information about Proxy Services activity:

- ◆ Protocol: Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
- ◆ Hostname: DNS domain name or IP address of the accessed host.
- ◆ Hit Volume: Number of times data was found in the cache for this host.
- ◆ Miss Volume: Number of times data was not found in the cache for this host.
- ◆ Hit Size: Amount of data that was found in the cache for the accessed host.
- ◆ Miss Size: Amount of data that was not found in the cache (misses) for the accessed host.

- 5** To display additional types of user information, complete any one of the following:

- 5a** To display all the connections made by a user, double-click a username in the Number of Users list box.

The User Log Entries window displays, providing the following information about Proxy Services activity:

- ◆ Entry Time: Time connection was established.

- ◆ Username: NDS or eDirectory name or IP address of the user.
- ◆ Status: Whether the proxy server found the requested data in the cache (hit or miss).
- ◆ Protocol: Protocol string representing the port number used for the connection, such as HTTP, FTP or HTTPS. For example, HTTP represents a connection made using port 80.
- ◆ Hostname: DNS domain name or IP address of the accessed host.
- ◆ Data Length: Amount of data transferred from the cache or the original host.
- ◆ Command: Commands used such as Get, Post, or Passthrough.

5b To view usage trends graphs, click Usage Trends > select the category of usage trend data.

You can view the following categories of usage trend data by time of day in one-hour increments:

- ◆ Number of users: Bar graph showing the number of unique users allowed to connect to a host.
- ◆ Number of hosts accessed: Bar graph showing the number of hosts accessed.
- ◆ Amount of hit and miss data (volume): Bar graph showing the number of cache hits and misses.
- ◆ Number of hosts accessed and amount of hit and miss data (volume): Combination line and bar graph showing the number of hosts accessed, cache hits, and cache misses.

All graphs can be saved to disk, copied to the clipboard, or printed.

Viewing Host Statistics

- 1** In NetWare Administrator, click the Server object representing the Novell BorderManager 3.8 server.
- 2** Select Novell BorderManager 3.8 from the Tools menu.
- 3** Click Proxy Cache, then select View Audit Log from the Object menu.

The HTTP Proxy Host Statistic window displays the Number of Hosts list and the User Accessed list.

Click the column heading of either list to sort the entries in that column in ascending or descending order. The sorting order is reversed each time you click the column heading.

The Number of Hosts list provides the following information about Proxy Services activity:

- ◆ Protocol: Protocol string representing the port number used for the connection, such as HTTP, FTP or HTTPS.
For example, HTTP represents a connection made using port 80.
- ◆ Hostname: DNS domain name or IP address of a host.
- ◆ Users Accessed: Number of users who have requested information from the selected host.
- ◆ Hit Volume: Number of times the requested information has been successfully delivered from the proxy server cache.
- ◆ Miss Volume: Number of times the requested information was not found in the cache.

- ◆ Hit Size: Total amount of data the proxy server has retrieved from its cache to satisfy user requests.
- ◆ Miss Size: Total amount of data the proxy server did not find in its cache.

The User Accessed list provides the username, using the NDS or Novell eDirectory name or IP address of the user, or the DNS domain name or the IP address.

- 4 To display the records for a set of connections from a specific user to a specific host, click Display Records and specify a time range for the records you want displayed.

or

For a U.S. English system, the dates are entered in the order of month, day, and year. The order is year, month, and day for a Japanese system; and day, month, and year for European language systems.

or

To see a list of connections for users who have accessed a particular host, double-click an entry in the Hosts Statistics window.

The Hosts Records Entries window displays, providing the following information about Proxy Services activity:

- ◆ Entry Time: Time the connection was established.
- ◆ Username: NDS or eDirectory name or IP address of the user.
- ◆ Status: Whether the proxy server found the requested data in the cache (hit or miss).
- ◆ Protocol: Protocol string representing the port number used for the connection such as HTTP, FTP or HTTPS, and so on. For example, HTTP represents a connection made using port 80.
- ◆ Hostname: DNS domain name or IP address of the accessed host.
- ◆ Data Length: Amount of data transferred from the cache or the origin Web server.
- ◆ Command: Commands used such as Get, Post, or Passthrough.

Exporting Data

The proxy audit logs are generated by enabling indexed format logging for the HTTP, FTP, Mail, News, Generic, DNS and RealAudio and RTSP proxy services. The proxy audit logs are stored in a Btrieve* file on the Novell BorderManager 3.8 server and are maintained by CSAUDIT.NLM.

The proxy audit logs cannot be edited or manipulated from the server; however, the data can be exported for analysis. The format of the exported data is compatible with trend analysis software packages, such as WebTrends*. This section describes how to export proxy audit logs and lists the data exported for the HTTP, FTP, Mail, News, Generic, DNS, and RealAudio and RTSP proxy services.

NOTE: Logging information for Telnet Transparent proxy is provided in the Generic TCP audit log.

The following are two ways to export the proxy audit logs from NetWare Administrator:

- ◆ Export the data from the HTTP Proxy Hosts Statistics window.
- ◆ Select Export Logs from the Novell BorderManager 3.8 menu.

To export audit logs for all proxies other than HTTP, you must use the second method. If you use the second method, you can also combine the audit log files from other Novell BorderManager 3.8 services with the proxy audit log into a single ASCII file.

For additional information, refer to the following sections:

- ♦ “Exporting HTTP Audit Log Proxy Records” on page 54
- ♦ “Exporting Audit Logs for All Other Proxies” on page 55
- ♦ “Export File Subdirectories” on page 55

Exporting HTTP Audit Log Proxy Records

To export HTTP audit log proxy records from the HTTP Proxy Hosts Statistics window:

- 1** In NetWare Administrator, click the Server object representing the Novell BorderManager 3.8 server.
- 2** Select Novell BorderManager 3.8 from the Tools menu.
- 3** Click Proxy Cache and select View Audit Log from the Object menu.
- 4** Click Display Records, specify the dates for the records you want to display, and then click OK.
- 5** In the HTTP Proxy Hosts Statistics window, click Export Data and specify the path and filename, or click Browse to select the destination of the export file.
- 6** Select one of the following sort formats under Information Output Selection, then click OK:
 - ♦ Time entry (connection by connection): Sorts records from earliest entry time to latest entry time. This is the default.
 - ♦ Access by users: Sorts records in alphabetic order based on the user's NDS or eDirectory name.
 - ♦ Access by hosts: Sorts records in ascending order (for IP addresses) or alphabetic order (for DNS hostnames).
- 7** (Conditional) If the export filename already exists under the directory path selected, you are prompted to replace the file. Click Yes to overwrite the file or click No to specify the destination as described in [Step 5](#).

The record fields are written to disk with a tab as the delimiter. Each record ends with a carriage return and line feed. The exported HTTP proxy data has the following format:

- ♦ Entry Time: Time the connection was established.
- ♦ Username: Typeless NDS or eDirectory name or IP address of user.
- ♦ Status: Whether the proxy server found the requested data in the cache (hit or miss).
- ♦ Protocol: Protocol string representing the port number used for the connection such as HTTP, FTP or HTTPS. For example, HTTP represents a connection made using port 80.
- ♦ Hostname: DNS domain name or IP address of host accessed.
- ♦ Data Length: Amount of data transferred from the cache or the original host.

Exporting Audit Logs for All Other Proxies

Use the Export Logs selection from the Novell BorderManager 3.8 menu to export all the proxy audit logs.

This procedure extracts the same data from the Btrieve database, but offers additional export options that cannot be activated from the HTTP Proxy Hosts Statistics window. More important, the audit logs for all other proxies (FTP, Mail, News, Generic, DNS, and RealAudio and RTSP) can only be accessed this way.

To export an audit log for any proxy:

- 1** In NetWare Administrator, click the Server object representing the Novell BorderManager 3.8 server.
- 2** Select Novell BorderManager 3.8 from the Tools menu.
- 3** From the Novell BorderManager 3.8 menu, select Export Logs.
- 4** Click Set Range, then specify the date range.

This is the range of dates comparable to the dates used to display records in the Access Control Users Statistics window. The default range is the current server date.

- 5** Click Browse to select the drive mapped to the destination for the export file.

This is the path and filename for the export file. The default destination is a:\yyyymmdd.log, where *yyyy* is the current year, *mm* is the current month, and *dd* is the current day. If you change the filename from the default format, the filename will not reflect the current server date. For example, if you change the filename format to *mmdyyy*.log, the next time you try to export logs on another day, the log filename will not have incremented to the current date.

- 6** (Optional) If the default filename is unacceptable, specify a new filename in the File field.
- 7** (Optional) If you want to combine the proxy audit log with audit logs from other Novell BorderManager 3.8 services, select the Combine Log Files check box. This feature allows log files from different Novell BorderManager 3.8 services to be combined into a single output file. When log files are combined, they are appended to one file, service by service.
- 8** Under Log Selection, select one or more boxes for the proxy type.
If the Combine Log Files feature has been selected, check all the services you want combined into the export log file.
- 9** (Optional) If you have selected Combine Log Files in [Step 7 on page 55](#), under Log Selection, select all other Novell BorderManager 3.8 services audit log files to be combined with the Access Control Log (ACL) file.

- 10** Click OK.

The proxy audit logs are exported to an ASCII file. The record fields are written with a tab as the delimiter.

Each record ends with a carriage return and line feed. The ASCII file format depends on which proxy audit log is exported.

Export File Subdirectories

If the Combine Log Files feature is *not* selected and you select one or more services under the Log Selection field, a separate export file is created for each service under a subdirectory of the export destination path.

The export subdirectories used are shown in the following table.

Log Type	Export Subdirectory
HTTP Proxy	HTTP
FTP Proxy	FTP
NNTP Proxy	NNTP
Mail Proxy	SMTP
RealAudio and RTSP Proxies	RAUDIO
DNS Proxy	DNS
Generic Proxy	GENERIC
Telnet Transparent Proxy	GENERIC
SOCKS Client	SOCKS
IPX Gateway	IPXGW
VPN	VPN
ACL (access control)	ACL

For example, if you specified an export destination of `vol1:logs\19981019.log`, and did not select the Combine Log Files feature, and did select HTTP proxy and access control, the following logs would result:

- ◆ `vol1:logs\http\19981019.log`
- ◆ `vol1:logs\ipxgw\19981019.log`
- ◆ `vol1:logs\acl\19981019.log`

For more information:

- ◆ [“Exported HTTP Proxy Data” on page 56](#)
- ◆ [“Exported FTP Proxy Data” on page 57](#)
- ◆ [“Exported NNTP Proxy Data” on page 57](#)
- ◆ [“Exported Mail Proxy Data” on page 58](#)
- ◆ [“Exported RealAudio and RTSP Proxy Data” on page 58](#)
- ◆ [“Exported DNS Proxy Data” on page 58](#)
- ◆ [“Exported Generic Proxy Data” on page 59](#)
- ◆ [“Exported SOCKS Client Data” on page 59](#)

Exported HTTP Proxy Data

The exported HTTP proxy data has the following fields:

- ◆ Keyword: HTTP. If the Combine Log Files option was selected, the keyword is at the beginning of each HTTP proxy audit log line.

- ◆ Date
- ◆ Time
- ◆ Source: Typeless NDS or eDirectory name and context, such as mlira.pubs.novell, or IP address
- ◆ Destination: DNS domain name or IP address
- ◆ Bytes received
- ◆ Command: Command used, such as Get, Head, Put, Post, Connect, or Delete
- ◆ Status of the command: Status of command used, such as Cache Hit, Cache Miss, IC Hit, ICP Miss, or Passthrough
- ◆ Protocol: Protocol used, such as HTTP

Exported FTP Proxy Data

The exported FTP proxy data has the following fields:

- ◆ Keyword: FTP. If the Combine Log Files option was selected, the keyword is at the beginning of each FTP proxy audit log line.
- ◆ Date
- ◆ Time
- ◆ Source: IP address
- ◆ Destination: IP address
- ◆ File length
- ◆ Proxy username: Name used to log in to the FTP proxy
- ◆ FTP username: Name used to log in to the FTP session
- ◆ File: Full path of the file transferred using FTP
- ◆ Cache status: Hit or Miss
- ◆ Status of the FTP request, such as Success, ACL rejection, DNS domain name resolution failure, FTP protocol error, and Connect failure

Exported NNTP Proxy Data

The exported Network News Transfer Protocol (NNTP) or News proxy data has the following fields:

- ◆ Keyword: NNTP. If the Combine Log Files option was selected, the keyword is at the beginning of each NNTP proxy audit log line.
- ◆ Date
- ◆ Time
- ◆ Source: IP address of client
- ◆ Destination: IP address of news server
- ◆ Status of the NNTP request, such as Success; Connect failure; ACL: news group denied; ACL: user/group posting not allowed; and NNTP protocol error # *number*, where error numbers are per RFC 977

Exported Mail Proxy Data

The exported Mail proxy data has the following fields:

- ◆ Keyword: MAIL. If the Combine Log Files option was selected, the keyword is at the beginning of each Mail proxy Audit Log Line.
- ◆ Date
- ◆ Time
- ◆ Source IP address
- ◆ Destination IP address
- ◆ User: Typeless NDS or eDirectory name or IP address of user
- ◆ Protocol: Simple Mail Transfer Protocol (SMTP) or Post Office Protocol 3 (POP3)
- ◆ Status of the SMTP or POP3 request, such as Success, ACL check failure, Spool creation error, Failed connection, Spool size limitation, Protocol and transport failure, and Resource allocation failure
- ◆ Command: SMTP or POP3 command used
- ◆ Source domain: DNS domain name (for SMTP use only)
- ◆ Recipients: First 256 bytes of comma-separated list in user@domain format (for SMTP use only)
- ◆ Process step: Examples of process steps, such as Incoming, Spool processing, and Forwarding (for SMTP use only)

Exported RealAudio and RTSP Proxy Data

The exported RealAudio and RTSP proxy data has the following fields:

- ◆ Keyword: RAUDIO. If the Combine Log Files option was selected, the keyword is at the beginning of each RealAudio proxy audit log line.
- ◆ Date
- ◆ Time
- ◆ Source: IP address
- ◆ Destination: IP address
- ◆ Destination port: Port number of the host
- ◆ RealAudio mode: TCP or UDP
- ◆ Status of the RealAudio request, such as Success, ACL failure, Connection error, and DNS domain name resolution error

Exported DNS Proxy Data

The exported DNS proxy data has the following fields:

- ◆ Keyword: DNS. If the Combine Log Files option was selected, the keyword is at the beginning of each DNS proxy audit log line.
- ◆ Date
- ◆ Time

- ◆ Source: IP address
- ◆ Destination: IP address of DNS name server
- ◆ Resource record type: Decimal number indicating the record type that was transferred. Valid record types are 1 through 16, 252, and 253.
- ◆ Resource record class: Decimal number from 1 through 3. A 1 indicates Internet, a 2 indicates CHAOS, and a 3 indicates Hesiod.
- ◆ Resource record name: Text string of up to 64 characters
- ◆ Transport: UDP or TCP
- ◆ Cache status: Hit, Miss, or Tunnel
- ◆ Status of the DNS request, such as Success, DNS packet data format error, Connect error, Name error, and Unable to resolve request

Exported Generic Proxy Data

Logging information for Telnet Transparent proxy is provided in the Generic TCP audit log.

The exported Generic proxy data has the following fields:

- ◆ Keyword: GENERIC. If the Combine Log Files option was selected, the keyword is at the beginning of each Generic proxy audit log line.
- ◆ Date
- ◆ Time
- ◆ Source: IP address
- ◆ Destination: IP address
- ◆ Destination port: Port number of the host
- ◆ Transport: UDP or TCP
- ◆ Cache status: Hit, Miss, or Tunnel
- ◆ Status of the Generic request, such as Success, ACL failure, and Connection error

Exported SOCKS Client Data

The exported SOCKS client data has the following fields:

- ◆ Keyword: SOCKS. If the Combine Log Files option was selected, the keyword is at the beginning of each Generic proxy audit log line.
- ◆ Date
- ◆ Time
- ◆ Source: IP address of client
- ◆ Destination: IP address of destination host
- ◆ Destination port: Port number of the host
- ◆ Transport: TCP or UDP
- ◆ Cache status: Hit, Miss, or Tunnel
- ◆ Status of the SOCKS request, such as Success, DNS resolution failed, Server connect failed, Server authentication failed, Server ACL failed, and General server failure

Managing Virus Pattern Recognition

For Web servers that are being accelerated by the Novell BorderManager 3.8 reverse proxy capability, Novell has added a new Virus Pattern Recognition feature that can help protect against such attacks.

The Virus Pattern Configuration Screen

The Virus Pattern Configuration screen is a console-based screen dedicated to virus pattern configuration and monitoring. This screen is reached by entering 23 on the Proxy Console screen. The information displayed is periodically refreshed for monitoring.

The following information describes each section of this screen, the parameters, their meaning, and, where applicable, their default values and configuration methods.

Configuration

The items in the Configuration section of the screen are as follows:

Number of Patterns: The current number of patterns in the database. This value is not configurable. It starts at 0 and is incremented each time a new pattern is successfully added to the database.

Pattern Size: The size of the pattern, in bytes. The default setting is 16. This is a global setting that is used for all patterns, so modify it with care.

Pattern Start Offset: Indicates where the virus pattern starts, as a byte offset from the actual beginning of the request.

The default setting is 1. This is a global setting that is used for all patterns, so modify it with care.

Refresh Interval: Specifies the time interval when the incoming request distribution is studied for Auto Update heuristic purposes.

The default value is 10 seconds. The value can be modified using the virus *-r interval* command.

Hit Threshold: The threshold upon which the automatic detection of new virus patterns is based.

The default value is 250. The value can be modified using the virus *-t threshold* command.

Virus Auto Update: Indicates whether or not the Auto Update feature is enabled.

The default value is 0 (disabled). The Auto Update feature can be enabled using the virus *-e 1* command.

Monitoring

The items in the Monitoring section of the screen are as follows:

Virus Requests: The number of incoming requests that have matched a virus pattern. This value is not configurable. It starts at 0 and is incremented each time a pattern match is detected.

Non Virus Requests: The number of incoming requests that did not match a virus pattern. This value is not configurable. It starts at 0 and is incremented each time a pattern match fails.

Recommend Threshold: A recommended value for the Auto Update threshold parameter. After the server has been up for a while, this gives a good lower limit for the hit threshold.

Maximum Non Virus Hit Rates: The maximum or peak number of incoming humble (non-virus) requests received in one time interval.

Average Virus Hit Rates: The average number of incoming virus requests received over all the time intervals crossed so far.

Average Non Virus Hit Rates: The average number of incoming humble (non-virus) requests. The threshold setting must be greater than this value.

Virus Source IP Address

This section displays the last ten IP addresses of sources that sent virus requests.

Last Predicted Request.

This section displays the last request that was made a suspect.

Choosing a Proper Threshold

The configuration section of the Virus Pattern Configuration screen contains a Hit Threshold parameter that gives the current threshold value.

The following rules of thumb can be used for arriving at an appropriate new threshold value:

- ◆ The Threshold value must be always greater than the average Non Virus Hit Rate.
- ◆ The Recommend Threshold gives a possible threshold value. However, you can use this value as a new threshold only if it is considerably higher than the Ave Non Virus Hit Rate value.

You can change the threshold value by executing the following command at the system console:

```
virus -t threshold
```

The threshold and refresh time interval settings are tightly coupled. If you raise the threshold, you need to increase the time interval accordingly, and vice versa. You can change the refresh time interval value by executing the following command at the system console:

```
virus -r time interval
```

Miscellaneous Tasks

This section outlines how to perform various tasks involved in the day-to-day operation of the Virus Pattern Recognition feature.

Specifying a Maximum Number of Patterns

Each pattern added to the database takes up 64 bytes of RAM. For memory and performance reasons, you might want to set a limit on the number of patterns allowed in the virus pattern database. To do this, specify the following command at the system console:

```
virus -m max virus patterns
```

where *maximum virus patterns* is an integer specifying the maximum number of patterns allowed in the database. This value should be set below 256.

Clearing Existing Virus Patterns

To clear all existing patterns from the database, type the following command at the system console:

```
virus -c
```

Viewing Online Help

To display online help and usage information, type the following command at the system console:

```
virus -? or virus -h
```

Verifying the Blocking of Virus Requests

To verify whether the Virus Pattern Recognition feature is working, select the proxy.log file (located in sys:\etc\proxy) for dropped request.

The following is an example of a dropped request:

```
63.146.66.41 - - [09/Aug/2001:04:47:27 -0600] "(bad request line)
GET%00/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX (truncated)" 400 2248
```

Disabling the Virus Pattern Recognition Feature

To disable the Virus Pattern Recognition feature, change the value of the ScanVirusPatterns parameter in proxy.cfg to 0 and restart the Proxy Server.

[Extra Configuration]

```
ScanVirusPatterns=0
```

Mail Proxy

This section covers the following:

- ◆ “Mail Proxy Transparency” on page 62
- ◆ “Mail Proxy Process Multiple MX Records” on page 62
- ◆ “Mail Proxy Multi-domain Support” on page 63
- ◆ “Additional POP3 Server” on page 63
- ◆ “Additional Flags” on page 64

Mail Proxy Transparency

This feature of Mail proxy works for outgoing mails. Enable the feature when the internal mail domain is public and should not be overwritten by the public domain of the proxy.

This feature is enabled by setting the following flag in the \etc\proxy\proxy.cfg file

[Extra Configuration]

```
Mailproxysupportstransparency=1
```

Mail Proxy Process Multiple MX Records

Mail proxy can now process multiple MX records. If there is a list of MX records in the DNS requests for the mail domain, proxy can now go to the next record in case of a failover at the first instance using the following parameter in proxy.cfg.

The previous proxy -m has been moved to the proxy.cfg file.

[Extra Configuration]

ProcessMultipleMXRecordsOfDomain=1

Mail Proxy Multi-domain Support

This feature enables the Novell BorderManager 3.8 Mail proxy to proxy multiple domains. Enabling this feature of mail proxy protects networks with multiple mail domains. The feature works for both incoming and outgoing e-mails. For incoming e-mail you can have multiple internal mail servers proxied by the mail proxy retaining their respective public domains, while outgoing e-mail from private internal domains is proxied with the respective public domains.

For mail proxy multi-domain support the first primary domain is taken from the NWAdmn Mail proxy primary domain. Other primary domain names and corresponding mail server names are added in the sys:\etc\proxy\proxy.cfg file under the section.

To enable the feature change, the value of the MultiDomain line to as many mail proxies as you want to configure (N is the value of the integer).

[Multiple Domain Support]

MultiDomain1=InternalMailServerName1/PrimaryDomain1

MultiDomain2=InternalMailServerName2/PrimaryDomain2

MultiDomainN=InternalMailServerNameN/PrimaryDomainN

For incoming multiple domain support, enable the following line in the file:

[Extra Configuration]

IncomingMultiDomainSupport=1

Additional POP3 Server

With this feature, the proxy's secondary IP address is added as a secondary IP address (automatically bound) to the server and the POP3 servers listen in all the mentioned addresses at port 110. This means that multiple POP3 servers can be proxied at the same time. To enable this feature, add the following to proxy.cfg.

[POP3 Additional Servers]

server1=31.0.0.2/164.99.146.124

server2=31.0.0.3/10.0.0.2

server3=31.0.0.4/10.0.0.3

server4=31.0.0.5/10.0.0.4

server5=31.0.0.6/10.0.0.5

server6=31.0.0.7/10.0.0.6

server7=31.0.0.8/10.0.0.7

server8=31.0.0.9/10.0.0.8

server9=31.0.0.10/10.0.0.9

Additional Flags

The following flags for mail Proxy server can be enabled. BM_Incoming_Relay should be set to 1 to prevent incoming e-mails from being relayed. If Primary Mail Domain is not configured through NWAdmn set, the BM_Domain to Primary Domain through sys:\etc\proxy\proxy.cfg. BM_Domain is a mandatory parameter.

```
[BM Mail Proxy]
BM_Incoming_Relay=1
BM_Domain=PrimaryDomain
BM_Proxy_Domain=Proxy Domain Name
```

The following flag is used to prevent looping when an e-mail is sent to the proxy IP address:

```
[Extra Configuration]
RejectMailToProxyIPAddress=1
```

Authentication

This section covers the following:

- ◆ [“MAC OS SSL Authentication” on page 64](#)
- ◆ [“MAC Block HTTP Tunnel Requests” on page 64](#)
- ◆ [“Terminal Server Authentication” on page 65](#)

MAC OS SSL Authentication

The MAC OS SSL authentication feature enables the first redirect to the login page to be of a small size so that it can go through and the MAC browser works fine with it. The problem was that the first redirect to the login page was big and didn't go in one packet. This caused the MAC IE browser to fail on responding to a HTTP 302 redirect.

The function is changed to SendHTMLRedirect(). To enable this set the below parameter in proxy.cfg.

```
[Extra Configuration]
new302Redirect=1
```

The default value is 0. Setting it to 1 causes the Novell BorderManager 3.8 proxy to send a simplified 302 redirect page. You must set the value to 1 for it to work properly with the MAC IE browser.

MAC Block HTTP Tunnel Requests

MAC Block HTTP Tunnel Requests disables the MAC IE browser from using the tunnelling mode. This prevents it from skipping the access control checks. Tunneling is disabled by default. The AllowHTTPTunneling flag has been added to the proxy.cfg file.

```
[Extra Configuration]
AllowHTTPTunneling=1
```

The default value is 0. A value of 1, allows HTTP tunneling.

HTTPS Transparent Proxy

The FTTP transparent proxy feature allows transparent proxy of secure HTTP sites.

The ports in the Transparent HTTP monitored list can now be either used for plain http or https access. For Transparent HTTPS access, specify the ports in the proxy.cfg file:

```
[TransparentHTTPS]
HTTPSPort1=<value>
HTTPSPort2=<value>
HTTPSPortn=<value>
```

If the proxy.cfg file is changed, ensure that proxy.nlm is unloaded and reloaded for the changes to take effect.

Terminal Server Authentication

The terminal server authentication feature solves the problem of authenticating users from clients with the same address, such as clients behind a NAT, from a Citrix server, or from any other terminal server. Now this solution also includes HTTPS sites. The feature provides the capability to differentiate users from client with the same address, and also from different addresses. Users coming from clients with the same address are shown a different authentication scheme.

To enable the feature, set the following parameters in proxy.cfg file on the server:

```
[Extra Configuration]
EnableTerminalServerAuthentication=1
RedirectHTTPSRequest=1
```

For terminal server authentication, 1 enables the feature and 0 disables the feature. The default is Disabled.

For redirecting HTTPS requests, 1 enables a redirect through JavaScript* and 0 disables the redirect through Javascript. The default is Enabled.

The authentication address sections shown below are used to limit the addresses for which the new authentication scheme applies.

```
[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
```

Authenticate all clients identified from the subnets, addresses, and address ranges. Make sure you keep the configuration as small as possible to avoid performance overhead. Optimum performance is gained if each entry in the above section occurs in a separate Network ID of CLASSed internet addresses.

Proxy Authentication for Clients with the Same Address

- 1 Log in to the Novell BorderManager 3.8 proxy.
- 2 On logging in successfully, a prompt is displayed. Copy the number displayed in the script prompt, copy it to the Clipboard, then click OK.
- 3 Paste the number in the username or the password field of the browser's proxy authentication dialog box.

From now on, any Web access from the same window or from a window launched using Ctrl-N does not require you to authenticate again.

- 4 Set the browser configuration to use proxy server IP address. Use port 8080 for all protocols.
- 5 Disable the Bypass Proxy Server for Local Addresses option on the browser. If needed, specify the local Web server IP addresses in the Exception List under the Advance button.
- 6 To make the second login automatic, run pxyauth.exe (located at border/public in the product CD) on the Citrix server or on clients behind NAT. This installs browser plug-ins on the system.

Browser plugins are available only for IE on Windows XP/2000 and Netscape 6 on Windows.

Proxy Configuration Dump Tool

The Proxy configuration dump tool is available as `cfgdump.nlm` in the unsupported directory of the product CD. This tool enables you to dump the proxy configuration to a file.

To run this NLM file, unload `proxy.nlm` and enter `cfgdump filename` on the system console.

If the filename is not specified, the file is dumped to `sys:\etc\proxy\dump.txt`.

Splash Screen Settings

The splash screen settings

```
[Extra Configuration]
```

```
SplashScreenEnabled=1
```

4

Advanced Configuration of Proxy Services

This section contains the following procedures to enhance the Novell[®] BorderManager[®] 3.8 Proxy Services performance:

- ♦ [“Configuring Cache Parameters” on page 67](#)
- ♦ [“Specifying Batch Downloading of Sites or URLs” on page 70](#)
- ♦ [“Configuring Caching Hierarchies” on page 71](#)
- ♦ [“Specifying Transport Timeout Parameters” on page 75](#)
- ♦ [“Specifying DNS Parameters” on page 75](#)
- ♦ [“Configuring Session Failover” on page 73](#)

See the [Chapter 2, “Setting Up Proxy Services,” on page 31](#) for information on how to set up Proxy Services.

Configuring Cache Parameters

The following sections describe how to configure advanced cache parameters for Novell BorderManager 3.8:

- ♦ [“Configuring Cache Aging Parameters” on page 67](#)
This section includes configuration of HTTP, FTP, and Gopher revalidation times.
- ♦ [“Configuring Cache Control Parameters” on page 68](#)
This section includes configuration of maximum cached file size and whether Java applets are stripped from HTML files.
- ♦ [“Configuring Cache Location Parameters” on page 69](#)
This section includes configuration of the cache directory and volume.
- ♦ [“Configuring Cachable Object Control Parameters” on page 69](#)
This section includes configuration of non-cachable URL patterns.

Configuring Cache Aging Parameters

- 1** In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2** Select an HTTP or FTP proxy or acceleration service, then click Caching.
- 3** From the Cache Aging tab, specify the following HTTP cache aging values:
 - ♦ **HTTP Maximum Revalidation Time:** The maximum number of hours or days HTTP data is cached before it is revalidated with the origin Web server.

This overrides the Time to Expire specified by the origin Web server if it is greater than this value.

- ◆ HTTP Default Revalidation Time: The number of hours or minutes HTTP data is cached before it is revalidated with the origin Web server. The data is revalidated if the origin Web server does not specify the Time to Expire.
- ◆ HTTP Minimum Revalidation Time: The minimum number of hours or minutes HTTP data is cached by the server. This overrides the Time to Expire specified by the origin Web server if the time specified is less than this value.

This parameter does not override the No Cache or Must Revalidate directives from the origin Web server.

- ◆ FTP Revalidation Time: The number of hours or days FTP data is cached before it is revalidated with the origin Web server.
- ◆ Gopher Revalidation Time: The number of hours or days Gopher data is cached before it is revalidated with the origin Web server.
- ◆ HTTP Failed Request Cache Time: The number of seconds or minutes after which HTTP will return a failure for the requested pages that the proxy server could not retrieve from the origin Web server.
- ◆ Maximum Hot Unreferenced Time: How long a node (or page) stays hot, or in a state where it can be more quickly accessed by the browser again after it has accessed the node once. The default is 20 minutes, after which the node is closed and the information is removed from memory. It takes longer for the proxy to access a node in cold state.

This parameter works in conjunction with the Maximum Number of Hot Nodes parameter on the Cache Control tab. Refer to [“Configuring Cache Parameters” on page 67](#) for more information.

- 4 Click OK, then click OK again from the Novell BorderManager 3.8 Setup page.

Configuring Cache Control Parameters

These parameters let you specify the maximum cached file size for each protocol, as well as the cache hash table size, number of hot nodes, and age ratio of the cache size to deleted files.

To configure cache control parameters:

- 1 In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2 Select an HTTP or FTP proxy or acceleration service, then click Caching.
- 3 From the Cache Control tab, specify the following:
 - ◆ Maximum size of the file that is cached for each URL protocol request type: Specify this value in megabytes. Any file larger than the specified size is not cached. The default is 30 MB.
 - ◆ Size of the cache hash table: The table is used by the proxy to locate a URL in its cache. Its size determines the speed of the information lookup. The default is 128,000 entries, or 51 KB of memory.

Increasing the maximum number of hot nodes might enhance performance more than increasing the size of the cache hash table.

- ◆ Maximum number of hot nodes or objects that can be cached: This is the number of nodes or pages that are hot, or in a state to be more quickly accessed by the browser again after

it has accessed the node once. This parameter works in conjunction with the Maximum Hot Unreferenced Time parameter on the Cache Aging tab.

NOTE: The maximum number of hot nodes must always be less than the maximum number of open files in NetWare. If you increase the maximum number of hot nodes from the default, make sure you also increase the maximum number of open files, up to a maximum of 100,000.

- ◆ Maximum age ratio of the cache size to deleted files: This value determines how much space on the volume is used for caching and how many deleted files remain on the volume.
- ◆ Whether Read-ahead is enabled and whether the proxy should read ahead for embedded images or page links: Read-ahead signals the proxy to cache the data and examine the HTML page to locate all embedded objects, including images and links to other pages.

When Read-ahead is enabled, the browser recognizes requests ahead of time.

- 4 Click OK, then click OK again from the Novell BorderManager 3.8 Setup page.

Configuring Cache Location Parameters

You can specify a different location for the cache.

- 1 In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2 Select an HTTP or FTP proxy or acceleration service, then click Caching.
- 3 From the Cache Location tab, specify the following:

- ◆ A server pathname as a cache storage directory: The default is `\etc\proxy\cache`.

The volume name is optional. If you do not specify a volume name, the default `sys:` is used.

For improved stability and performance, we recommend that you set up a separate volume other than `sys:` for the proxy cache directory, with compression and suballocation disabled, no long namespace support, and block size set to 16K.

- ◆ (After clicking Add) A volume name to the Volume list: This specifies a different cache location. Make sure you include a colon at the end of the volume name.
- ◆ The number of directories available per volume.

- 4 Click OK, then click OK again from the Novell BorderManager 3.8 Setup page.

- 5 Stop and restart the proxy server for the changes to take effect.

The cache on the `sys:` volume will not be moved to the new volume name.

Configuring Cachable Object Control Parameters

These parameters let you control which URL patterns are not cached, as well as what happens with objects that have a question mark (?) in the URL, `/cgi` in the pathname, or a no-cache reply header.

You can specify whether to cache URLs and objects with certain predefined patterns or access them directly without caching by the proxy server (be noncachable).

When no caching is specified, the proxy server simply forwards the request from the server to the requesting client. Objects with a question mark (?) in the URL, `/cgi` in the pathname, or a no-cache reply header are not cached by default unless you specify otherwise.

To configure cachable object control parameters, complete the following steps:

- 1** In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2** Select an HTTP or FTP proxy or acceleration service, then click Caching.
- 3** Click the Cachable Object Control tab.
- 4** Click Add to specify a list of URL patterns that will not be cached.
 - 4a** Specify the following information:
 - ◆ Scheme: Specify a scheme type of HTTP, FTP, Gopher, or HTTPS.
 - ◆ Hostname: Specify any hostname or specify a specific hostname that must be matched.

You can also select the check box to match any hostname that ends with the specified domain.
 - ◆ Port: Specify any port number or specify a specific port number.
 - ◆ Path: Specify any path or specify a specific pathname.

You can also select the check box to match any path that begins with the specified name.
 - ◆ Extension: Specify any extension or specify a specific extension.
 - 4b** Click OK.

If you specify a long list of patterns, the proxy server performance is affected.
- 5** Specify the actions taken for the following objects:
 - ◆ Objects with a question mark (?) in their URL
 - ◆ Objects with /cgi in their paths
 - ◆ Objects with a no-cache reply header

These objects are not cached by default. Specify to cache these objects if you are setting up an accelerator. You can also specify to not cache and send replies to all browsers that request the information at the same time. This reduces how often the proxy must retrieve information from the origin Web server.

Specify to not cache or split requests that have a cookie to avoid sending different replies to different users for the same request.
- 6** Click OK, then click OK again from the Novell BorderManager 3.8 Setup page.

Specifying Batch Downloading of Sites or URLs

Use batch downloading to keep the Novell BorderManager 3.8 cache of objects up to date for your users. You can schedule downloads of HTTP files from a Web site to the local cache. You can download a URL, multiple URLs up to a specified number of links, or an entire Web site. You can specify batch downloading for both forward and reverse HTTP proxies. Reverse proxy, however, does not download links that are external to a site.

Schedule downloads for low network usage times to conserve your network resources.

To specify batch downloading:

- 1** In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2** Select an HTTP proxy or acceleration service, then click Caching.

- 3** Click the Scheduled Download tab, then click Enable Scheduled Downloads and specify whether to perform the downloads sequentially.
- 4** Click Add from the Download List, then specify the following download parameters:
 - ◆ Enable this particular download.
 - ◆ HTTP URL: A URL, the number of levels to download in that URL, and whether to follow links from that URL to other hosts.
 - ◆ Maximum number of concurrent requests: The number of concurrent downloads to perform.
 - ◆ Maximum number of objects to download: The number of objects that can be downloaded during a session.
 - ◆ Maximum amount of data to download: The maximum size of data (in MB) that can be downloaded during a session.
- 5** Click the Frequency tab and specify the following parameters:
 - ◆ One time only: The date and time for a single download event.
 - ◆ Once a day at: The start time for a daily download.
 - ◆ Daily from: The interval and frequency for multiple daily downloads. Also, whether to perform the downloads only on certain days of the week.
- 6** Click OK then click OK again from the Novell BorderManager 3.8 Setup page.

Configuring Caching Hierarchies

If several proxy servers are serving the network, you can set up a hierarchy of proxy caches. If a proxy server does not find the requested page in its cache, it queries its peers and parents for the information.

The queried peers and parents can then, in turn, query additional peers and parents for the requested information. The origin server is queried as the last resort.

The Novell BorderManager 3.8 proxy server is compatible with other Internet Cache Protocol (ICP)-based proxy servers that exist on the Internet. You can set up these proxy servers as peers (neighbors), parents, or both.

You can configure a CERN hierarchy, a cache hierarchy (ICP), or both. If both are configured, the cache hierarchy takes precedence and the CERN hierarchy is used as a backup. CERN hierarchies have only parents, whereas cache hierarchies have both parents and peers.

To configure a hierarchical cache:

- 1** In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2** From the Application Proxy tab, select the HTTP Proxy service, then click Details.
- 3** Click the Cache Hierarchy Server tab, then select the Enable Cache Hierarchy Server check box.
- 4** Specify the following, then click OK:
 - ◆ Whether to enable source round-trip time: This parameter is used by the proxy to determine whether to send a request to the parent or to the origin server. The proxy uses the route that returns the shortest round-trip time.

- ◆ Whether to enable ICP ACL: This enables the cache hierarchy or ICP access control on the server.
 - ◆ ICP listening port number: The UDP port on which the cache listens for queries from other caches.
 - ◆ (After clicking Add) One or more multicast IP addresses for the multicast group list: Multicast addresses on which the cache hierarchy server receives multicast cache hierarchy queries.
 - ◆ (After clicking Add) One or more hostnames or IP addresses for the access control list: The hostnames or IP addresses on this list are used to verify whether proxies can send a request. The clients on this list are allowed to send a cache hierarchy request.
- 5** Click the Cache Hierarchy Client tab, then select the Enable Cache Hierarchy Client check box.
- 6** Specify the following:
- ◆ Must Only Forward Through Hierarchy: Deselect this option if you want the proxy server to retrieve the requested objects directly from the origin server.
 - ◆ Cache Neighbor Timeout value: The number of seconds or minutes the proxy server waits for a response to a cache hierarchy request from another proxy server.
Do not specify a value if you are configuring a CERN client.
 - ◆ (After clicking Add) One or more neighbors for the Neighbors List, with the following information specified:
Name of the nearest host server neighbor.
Port number of the neighbor HTTP proxy.
Port number of the neighbor cache hierarchy client: Do not specify a value if you are configuring a CERN client.
Type of neighbor: peer, parent, or CERN: Select peer or parent if you are configuring a cache hierarchy client; select CERN if you are configuring a CERN client.
Priority for each neighbor, from 1 (lowest) to 10 (highest): You can prioritize a set of parents or neighbors. A cache hierarchy client chooses the fastest responding hierarchy cache with the highest priority to service a request. CERN uses pure priority routing without querying.
Domains that the cache hierarchy client will serve: The default is null, or all neighbors receive all queries. CERN also supports domain routing.
 - ◆ (After clicking Add) One or more unicast addresses or names and port numbers for the multicast responder list: This is a list of all acceptable neighbors (unicast) that can respond to a multicast query. This list lets the cache hierarchy client verify that the responses are from a valid neighbor. Do not specify a value if you are configuring a CERN client.
- 7** Click OK.
- 8** Click the Cache Hierarchy Routing tab, then specify the following:
- NOTE:** Use cache hierarchy (ICP) routing when the parent cannot contact the origin server.
- ◆ Whether a URL's home site is used as a peer cache (not recommended).

- ◆ (After clicking Add) The local domain name for origin Web servers that are in close proximity: The proxy server prefers to query for a URL that it cannot resolve from these servers instead of from the cache hierarchy.
 - ◆ (After clicking Add) One or more stop patterns for which the cache must query the origin Web server directly: Specify patterns for which the delays caused by hierarchical caching are unacceptable, for example, static pages that change frequently.
- 9 Click OK, then click OK again from the Novell BorderManager 3.8 Setup page.

Configuring Session Failover

This solution has two components namely, Auth agent and Proxy Agent. Auth agent collects information from multiple Proxy Agents and distributes the same to all Proxy Agents. This will ensure sharing of authentication information amongst all proxies that are configured to use the Auth Agent, even if the user is authenticated to only one proxy. Proxy Agents run on each NBM box and share the information with Auth Agent. This need to be configured for each NBM Proxy.

User password is never exchanged between Proxy Agent and Auth agent. Run Auth agent on a separate box.

The Auth agent, a java application, is the central repository of authenticated user information, for all the proxies in the setup. The Auth agent can run on NetWare, Windows or a Linux Server, with a Java Virtual Machine (version 1.4). For better reliability, the Auth Agent should run on a separate machine.

NOTE: The Auth agent failover will be supported in the next release.

Proxy agent is the new authchk.nlm, running in each of the proxy servers configured for Session failover. The Proxy agent part of authchk talks to the Auth agent and keeps the central repository in sync with the local proxies. The activities that could trigger a communication between the Proxy agent and the Auth agent would be - new user logs in, logs out, inactivity timeout, etc.

The trust between the Proxy agent and the Auth agent is established by the configuration file.

Setting up Auth agent:

1. Copy bmauth.jar to the system where you intend to run the Auth Agent.
2. Create auth.cfg in /ETC/PROXY directory (SYS:/ETC/PROXY/ for NetWare).
(copy sample auth.cfg file from SYS:/ETC folder).
3. Edit the proxy agents section.

Proxy agents section contains the list of Proxy agents (proxy servers) wanting to share authenticated session information. Format is: <unique_proxyID>=<ProxyAgent_IP_Address>

To ensure that the ProxyID and IPaddress mapping is unique across all your Proxies, it is recommended to edit one auth.cfg with all the relevant information and copy it to the Auth agent and Proxy agent boxes.

A sample auth.cfg file (in auth agent box) is:

```
[proxy agents]
1=10.10.10.1
2=10.10.10.2
```

```
[auth]
ipport1=10.10.10.3:9023

[debug]
Level=1

File=auth.log
```

In the sample, 1 and 2 are unique Proxy Ids.

The Auth agent is listening at 10.10.10.3 port 9023. The debug section is for debugging and logging purposes. Recommended Level is 1. Level 1 gives details on the information exchanged between the proxies and the auth agent, in the log file. The log file name is configurable via the 'File' entry under debug section. The log is available with the Auth agent in /etc/proxy directory.

Starting Auth Agent:

To start auth agent:

- 1 Run the following command in the Auth Agent server .

```
java -classpath <full path of bmauth.jar>
      com.novell.bordermanager.proxy.auth.AuthDB<location of config
      file>
```

Location of config file is optional and you can use this if auth.cfg file is stored in a different location other than /etc/proxy. eg. java -classpath sys:\public\bmauth.jar com.novell.bordermanager.proxy.auth.AuthDB

Configuring Proxy Agent

Ensure that the Auth Agent is configured (as described above) and running.

- 1 Copy sample auth.cfg file to sys:/etc/proxy folder from SYS/ETC folder of the NBM Server.
- 2 In the Proxy Agents section, edit the entry for this proxy server, by changing the IP address to 'localhost' (without quotes).

This is similar to the config file for Auth Agent except that <ProxyID>=<Proxy Agent IP Address>. Entry for the local server should be localhost instead of IP address.

The auth section should mention the IP address and port of the Auth agent, as shown below.

See a sample auth.cfg file, for Proxy Agent configuration on 10.10.10.1 machine:

```
[proxy agents]
1=localhost
2=10.10.10.2

[auth]
ipport1=10.10.10.3:9023

[debug]
Level=1

File=auth.log
```

Starting Proxy Agent:

Run stopbrd and startbrd to restart NBM Services.

Proxy Agent supports the following command to initiate a sync request to Auth Agent:

```
authchk_send_sync_to_agent
```

This is useful when the Proxy Agent and Auth Agent go out of sync due to network failures. Run the above command in the proxy box, once the connection with auth agent is established.

NOTE: Make sure that Proxy Agents and Auth Agents are able to communicate with each other [reachable] through the configured interfaces / IP addresses.

Specifying Transport Timeout Parameters

You can fine-tune various transport-related timeout parameters that are used by the Novell BorderManager 3.8 proxy server for connections. Do not change the defaults unless you are certain of the outcomes. You might need to change the parameters based on your network load.

To specify transport timeout parameters:

- 1** In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2** Click Transport > specify values for any of the following TCP timeout parameters you want to set:
 - ◆ **Establish Connection Timeout:** The number of seconds or minutes the proxy server attempts to establish a connection before timing out because the other side has not responded.

You might want to increase this value if you notice that the remote server is reachable (the ping succeeds) but the load is heavy.
 - ◆ **Connection Keepalive Interval:** The number of minutes or hours a connection is idle before the proxy server queries to check if the other server is still responding.
 - ◆ **Data Read Timeout:** The number of seconds or minutes the proxy server waits for expected data to begin arriving before it times out. You might want to increase this value if you notice that the browser receives incomplete data or the connection is disconnected in the middle of data transfer.
 - ◆ **Idle Server Persistent Connection Timeout:** The number of minutes or hours the proxy server keeps the TCP connection between the browser and the proxy server active, even if there is no data flow.
 - ◆ **Idle Client Persistent Connection Timeout:** The number of seconds or minutes the proxy server keeps the connection to the origin Web (or FTP or Gopher) server or another proxy server active, even if there is no data flow.
- 3** Click OK, then click OK again from the Novell BorderManager 3.8 Setup page.

Specifying DNS Parameters

You can fine-tune some of the parameters used by the Domain Name System (DNS) Resolver of the Novell BorderManager 3.8 proxy server.

To change DNS parameters:

- 1** In NetWare Administrator, select the Novell BorderManager 3.8 Setup page for the server.
- 2** Click DNS then specify TCP or UDP (the default) as the transport protocol used by the DNS Resolver to query the DNS name server.

If you select UDP and notice an increase in Bad Gateway error messages while the origin Web server is running, you might want to increase the DNS Resolver Timeout value.

- 3** For UDP, specify the DNS Resolver Timeout value.

This value indicates how long the proxy server waits before timing out after it sends a request to a DNS name server to resolve a domain name.

- 4** Specify values for the following parameters:

- ◆ **Negative DNS Lookup:** How long a failed DNS lookup domain name remains in the proxy server cache. If the proxy server cannot resolve a domain name, it stores that information in its cache for the specified amount of time.

If the proxy server receives requests for that domain name within this period, it will send a Bad Gateway error message to the browser and will not resolve the domain name again.
- ◆ **Maximum DNS Entry TTL:** The maximum amount of time that DNS entries are cached before they expire. This is the maximum value, regardless of the value returned by the DNS name server.
- ◆ **Minimum DNS Entry TTL:** The minimum amount of time that DNS entries are cached before they expire. This is the minimum value, regardless of the value returned by the DNS name server.
- ◆ **Maximum DNS Entry Threshold:** The maximum number of DNS cache entries. When this number is reached, the proxy server deletes old entries to make room for newer ones. The default is 2,500.

- 5** Click OK, then click OK again from the Novell BorderManager 3.8 Setup page.

5

HTTP Proxy Logging Using Nsure™ Audit

Novell BorderManager 3.8 is instrumented to use Nsure Audit for HTTP proxy logging.

Nsure Audit provides secure logging, reporting, monitoring and notification capabilities. Through integration with Nsure Audit, the BorderManager 3.8 HTTP proxy supports logging of all events previously reported in the Common and Extended log formats, plus the categorizations of each Web request as provided by third party URL database products from partners such as SurfControl* and N2H2*.

Nsure Audit is an additional logging method. The legacy Common, Extended and Indexed Logging still exist in BorderManager 3.8. However, Nsure Audit has several key advantages, including:

- ◆ **Security**—Nsure Audit events are signed and chained, which means that you have forensically viable evidence of all HTTP proxy activity. Nsure Audit guarantees that no log data has been deleted or modified.
- ◆ **Log Data Aggregation**—The Nsure Audit Secure Logging Server allows you to collect log data from multiple BorderManager 3.8 proxy servers into one data store. Reports may then be generated that reflect Web activity for an entire organization, not just one server.
- ◆ **Performance**—Nsure Audit is very fast and scalable. It allows you to do comprehensive logging with minimal impact on proxy performance. Note: For maximum performance when using Nsure Audit, legacy proxy logging methods should be disabled in NetWare® Administrator.

Nsure Audit Overview

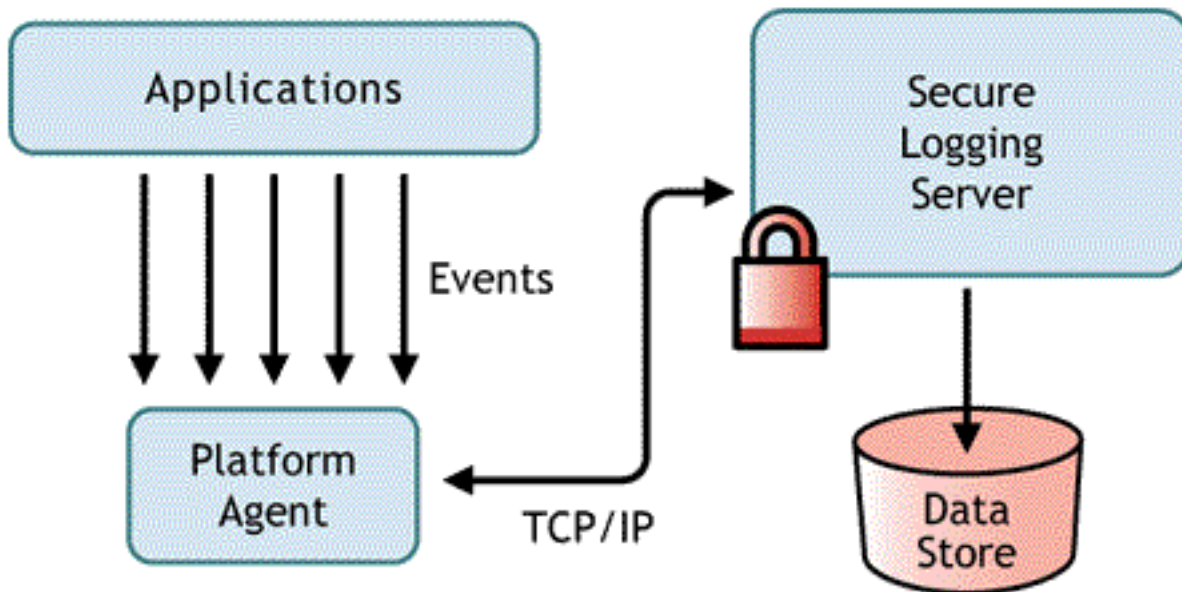
Nsure Audit is a centralized, cross-platform logging service that can log data from multiple applications to a centralized data store. After event data is logged, you can run detailed reports, do custom queries and trigger notifications based on logged events.

Nsure Audit consists of two primary components:

- ◆ Platform Agent
- ◆ Secure Logging Server

The following figure illustrates the high-level architecture of Nsure Audit:

Figure 5 NBM 3.8 as one of the applications that uses the platform agents to report events to Nsure Audit Secure Logging Server



In this illustration, BorderManager 3.8 is one of the applications which uses the Platform Agent to report events to the Nsure Audit Secure Logging Server.

The Platform Agent runs on the same server as BorderManager 3.8 and communicates events to the Secure Logging Server. The Secure Logging Server is the component that receives event data from BorderManager 3.8 and other applications. The Secure Logging Server may be installed on the same NetWare server as BorderManager 3.8 or on a different server.

The Secure Logging Server supports the following platforms:

- ◆ Novell NetWare 5.1 SP6 and higher
- ◆ Novell NetWare 6.0 SP3
- ◆ Novell NetWare 6.5 and NetWare 6.5 SP1
- ◆ Microsoft Windows* 2000 SP4
- ◆ Solaris* 8 and 9
- ◆ SuSE® Linux* Enterprise Server 8
- ◆ Red Hat* Linux 7.3 and 8.0

The Secure Logging Server can log events to MySQL*, Oracle*, Java* applications and several other data stores, including a flat file. Nsure Audit includes a tool called Nsure Audit Report that is designed to query the data store for event data. A data store with an ODBC connector is required to use this advanced reporting tool.

Nsure Audit is included with NetWare 6.5 and can be installed during the NetWare 6.5 server installation. If NetWare 6.5 has already been installed, you can return to the NetWare Install later and add the “Nsure Audit Starter Pack” component.

For other platforms, the Nsure Audit Starter Pack may be downloaded from [Starter Pack \(http://download.novell.com\)](http://download.novell.com). A Quick Start Card for each platform is provided in the download files.

Full product documentation for Nsure Audit may be found at [Product Description \(http://www.novell.com/documentation/lg/nsureaudit\)](http://www.novell.com/documentation/lg/nsureaudit). Please consult this documentation for detailed information on the configuration of Nsure Audit components.

Configuring Novell BorderManager 3.8 for Nsure Audit

Novell BorderManager 3.8 is not enabled for Nsure Audit by default. In order to use Nsure Audit with BorderManager 3.8, follow these steps:

- 1** Ensure that Nsure Audit is properly installed and configured as per the Nsure Audit Quick Start Card. This includes installing a Secure Logging Server and installing the NetWare Platform Agent on each BorderManager 3.8 proxy server that will be reporting events to Nsure Audit.
- 2** Ensure that the Platform Agents are correctly configured to communicate with the Secure Logging Server. On each BorderManager 3.8 proxy server that will be reporting events to Nsure Audit, check for the file `sys:\etc\logevent.cfg`. Change the value of the `LogHost` parameter to the IP address or DNS name of your Secure Logging Server.
- 3** Prepare the Secure Logging Server to receive data from BorderManager 3.8. This only needs to be done once, no matter how many BorderManager 3.8 proxy servers will be reporting events to Nsure Audit. To simplify setup, an NCF file is provided that prepares Nsure Audit to receive BorderManager 3.8 events. This file is located at `sys:\etc\proxy\audit\runaud.ncf` on any server where BorderManager 3.8 has been installed. Open this file in a text editor and enter a valid user name and password with Admin rights to the Secure Logging Server. Use the example format shown in the NCF file.
- 4** If the Secure Logging Server is set up on the same machine where the edited version of `runaud.ncf` exists, go to the server's System Console, type `sys:\etc\proxy\audit\runaud.ncf` and press Enter.

Secure Logging Server on Another NetWare server: Copy `sys:\etc\proxy\audit\runaud.ncf` to the NetWare server where the Secure Logging Server is installed and run the NCF file from the System Console.

Secure Logging Server on Windows: Copy `sys:\etc\proxy\audit\runaud.ncf` to the Windows server where the Secure Logging Server is installed. Rename the file to `runaud.bat` and run it.

Secure Logging Server on Other Platforms: See the Nsure Audit product documentation for instructions to set up new applications on other platforms supported by the Secure Logging Server.

- 5** Restart the Secure Logging Server.
- 6** On each BorderManager 3.8 proxy server that will be reporting events to Nsure Audit, using a text editor, add the following in the `sys:\etc\proxy\proxy.cfg` file:

```
[Extra Configuration]
EnableNsureAuditLogging=1
```

- 7** Restart the BorderManager 3.8 server(s).

Novell BorderManager 3.8 Event Data

Before you can run queries or build reports that display proxy log data in a useful fashion, it is important to understand the nature of the data reported by the Novell BorderManager 3.8 HTTP proxy.

For the purposes of Nsure Audit, each URL request through the BorderManager 3.8 HTTP proxy generates three “events”. The Nsure Audit event information for BorderManager 3.8 is shown in the following table.

Event ID	Description	Data Fields
00040001	Proxy Common Log Data	IP Address, Authenticated User Name, Date, Time, Time Zone, HTTP Request, URL, HTTP Version, Status Code, File Size
00040002	Proxy Extended Log Data	cached, [date-time], c-ip, cs-method, cs-uri
00040005	3rd Party Categorization	url, username, url-category, vendor-ID

For descriptions of the data fields in the Common and Extended Log Data events, please see an article by Marcus Williamson in the January, 2002, Novell AppNotes® [Understanding Novell BorderManager’s HTTP Logs \(http://developer.novell.com/research/appnotes/2002/january/02/a020102.htm\)](http://developer.novell.com/research/appnotes/2002/january/02/a020102.htm)

Capture of the 3rd Party Categorization data is unique to BorderManager 3.8’s support for Nsure Audit. Descriptions of the 3rd Party Categorization data fields follow:

Data Field	Description
url	The URL of the Web content being requested
username	The name of the user requesting that URL
url-category	The categorization of the URL, based on the 3rd party categorization product being used on the proxy server that handled the request
vendor-ID	1 – CyberPatrol* (This is not officially supported on BorderManager 3.8.) 3 – SurfControl Content Database 4 – N2H2 Category Server 7 – Connectotel LinkWALL*

The IP address of the BorderManager 3.8 proxy server that reported the event is also included in each event record.

Viewing Events in Nsure Audit Report

Nsure Audit Report is a Windows-based, ODBC-compliant application that can use SQL query statements or Crystal Reports* to query Oracle and MySQL data stores (or any other database that has ODBC driver support).

Follow the instructions in the Nsure Audit product documentation to set up Nsure Audit Report.

To generate a simple query, do the following:

- 1** In the Nsure Audit Report Workspace, click the Events tab, then expand the BorderManager folder. This list contains all predefined BorderManager events. Double-click any event in the list to view event properties.
- 2** To query for events, right-click the event in the Workspace and select Define Query.

- 3** When the Query Expert appears, specify a time frame and verify the event.
- 4** To run the query, select the Query tab in the Workspace, right-click the query name, then select Run.

Queries can also be created using SQL statements.

Other Nsure Audit Capabilities

For information on how to use Nsure Audit to create reports, generate alerts, monitor Internet activity in real time, or output data to various formats for processing by other applications, please consult the Nsure Audit product documentation.

6

Setting Up Access Control

Access control is the process by which user access to Internet and intranet services is regulated and monitored. Specifically, the Novell® BorderManager® 3.8 access control software allows or denies access requests made through the Proxy Services, or a Virtual Private Network (VPN) client.

When you enabled the Novell BorderManager 3.8 HTTP proxy for all private interfaces during the software installation, access control was enabled by default. All HTTP proxy traffic through the private interface is denied until you configure an access rule to specifically allow users to access the HTTP proxy.

When access control is enabled, the Access Control List (ACL)—comprising the access rules—also applies to the application proxies, and VPN clients attempting to connect to a VPN server.

An access rule can be created for a Country (C), Organization (O), Organizational Unit (OU), or Server object.

This section explains how to set up basic access control so users can use the Novell BorderManager 3.8 services you enabled.

- ◆ [“Setting Up a URL-Based Rule” on page 83](#)
- ◆ [“Setting Up a Rule to Allow Access through an Application Proxy” on page 84](#)
- ◆ [“Setting Up a Rule to Allow VPN Clients to Access VPN Servers” on page 86](#)
- ◆ [“Setting Up a Rule to Allow the Server to Resolve Hostnames” on page 86](#)
- ◆ [“Setting Up Time Restrictions for Access Rules” on page 87](#)
- ◆ [“Viewing All Rules That Apply to an Object” on page 88](#)
- ◆ [“Completing Advanced Setup, Configuration, and Management Tasks” on page 88](#)

NOTE: This section describes the tasks required to set up an initial implementation of access control.

For planning and conceptual information about access control, refer to the *Novell BorderManager 3.8 Overview and Planning Guide*, available in the online documentation.

Make sure you understand this information before setting up and configuring access control.

Setting Up a URL-Based Rule

URL-based access rules apply to users accessing Web content through the HTTP proxy. If you enabled the HTTP proxy for all private interfaces during the installation, the simplest way to allow users to access the HTTP proxy is to create a rule that allows any source on the private network to access any destination.

To create an access rule for a URL:

- 1** In NetWare[®] Administrator, right-click the object where the access rules are to be created, then select Details.
- 2** Select the Novell BorderManager 3.8 Access Rules page, then click Add.
- 3** In the Access Rule Definition page, specify Allow (the default) for Action.
- 4** For Access Type, select URL.
- 5** Under Source, specify Any to apply the rule to all NDS[®] or Novell eDirectory[™] objects, Domain Name System (DNS) hostnames, IP addresses, and subnets. Otherwise, select users, groups, or hosts as follows:
 - 5a** Click Specified, then click Browse.
 - 5b** Specify an NDS or eDirectory object, a DNS hostname, an IP address or range of addresses, or a subnet, including its subnet mask, then click Add.

For DNS hostname specifications, you can use the wildcard character (*) in your entry.
 - 5c** Add additional sources.
 - 5d** After you have added the sources you want, click OK.
- 6** Under Destination, specify Any to apply the rule to any URL, otherwise, select Specified and do the following:
 - 6a** Click Browse > Add.
 - 6b** Specify the *unqualified* URL (www.novell.com, for example), then click OK.
 - 6c** Repeat this process to add additional URLs, if necessary.

NOTE: You can use wildcards in the URLs. However, be aware that the HTTP proxy enforces rules with wildcards differently. The HTTP proxy enforces a rule with a wildcard in the hostname of a URL.
- 7** (Optional) If you want the server to record all access attempts that match the rule, click Enable Rule Hit Logging.

Logging access attempts can affect server performance; however, we recommend that you do so to detect unauthorized activity.
- 8** Click OK, as necessary, to return to the Novell BorderManager 3.8 Access Rules page, then click OK to update the access rules.

Setting Up a Rule to Allow Access through an Application Proxy

When a user is accessing an application proxy, these rules are ignored. If you want similar rules to apply to users accessing these services through an application proxy, you must set up access rules for the individual application proxies.

To create an access rule for an Proxy Services, complete the following steps:

- 1** In NetWare Administrator, right-click the object where the access rules are to be created, then select Details.
- 2** Select the Novell BorderManager 3.8 Access Rules page, then click Add.
- 3** In the Access Rule Definition page, specify Allow (the default).
- 4** For Access Type, select Application Proxy.
- 5** For Access Details, select a proxy from the Proxy drop-down menu.

The port number information is automatically filled in for you. If you selected the News proxy, a drop-down menu is added that allows you to specify the direction: Posting or Reading.

- 6** Under Source, accept Any to apply the rule to all NDS or eDirectory objects, DNS hostnames, IP addresses, and subnets. Otherwise, select users, groups, or hosts as follows:

6a Click Specified, then click Browse.

6b If you did not select the SMTP Mail or News proxy earlier, specify an NDS or eDirectory object, a DNS hostname, an IP address or range of addresses, or a subnet, including its subnet mask, then click Add.

For DNS hostname specifications, you can use the wildcard character (*) in your entry.

If you selected the RealAudio, Generic TCP, Generic UDP, or Telnet proxy, you can specify an IP address or a subnet address only.

6c If you selected the SMTP Mail proxy earlier, specify an e-mail user name or an e-mail domain name to specify all users in the domain, then click Add.

6d If you selected the News proxy earlier and selected Posting for the direction, specify an e-mail username, then click Add.

6e Add additional sources by repeating the following steps:

[Step 6a on page 85](#)

[Step 6b on page 85](#)

[Step 6c on page 85](#)

[Step 6d on page 85](#)

6f When you have added the sources you want, click OK.

- 7** Under Destination, accept Any to apply the rule to any destination; otherwise select destinations as follows:

7a Click Specified, then click Browse.

7b If you did not select the SMTP Mail or News proxy earlier, specify a DNS hostname, an IP address or range of addresses, or a subnet, including its subnet mask, then click Add.

For DNS hostname specifications, you can use the wildcard character (*) in your entry.

7c If you selected the SMTP Mail proxy earlier, specify an e-mail username or an e-mail domain name to specify all users in the domain, then click Add.

7d If you selected the News proxy earlier, specify a news group name, then click Add.

7e Add additional destinations by repeating the following steps:

[Step 7a on page 85](#)

[Step 7b on page 85](#)

[Step 7c on page 85](#)

[Step 7d on page 85](#)

7f After you have added all the destinations, click OK.

IMPORTANT: If you create a rule that allows access to any destination whose hostname must be resolved by a DNS name server, you must create another rule that allows the Novell BorderManager 3.8 server to resolve the hostname.

For information, refer to [“Setting Up a Rule to Allow the Server to Resolve Hostnames” on page 86](#).

- 8** (Optional) If you want the server to record all access attempts that match the rule, click Enable Rule Hit Logging.

Logging access attempts can affect server performance; however, we recommended that you do so to detect unauthorized activity.

- 9** Click OK, as necessary, to return to the Novell BorderManager 3.8 Access Rules page, then click OK to update the access rules.

Setting Up a Rule to Allow VPN Clients to Access VPN Servers

Access rules for VPN clients apply to both VPN LAN clients and to VPN clients that are attempting to connect to a VPN server using a dial-in connection.

To create an access rule for a VPN client:

- 1** In NetWare Administrator, right-click the object where the access rules are to be created and select Details.
- 2** Select the Novell BorderManager 3.8 Access Rules page, then click Add.
- 3** In the Access Rule Definition page, specify Allow (the default).
- 4** For Access Type, select VPN Client.
- 5** Under Source, accept Any to apply the rule to all NDS or eDirectory objects, DNS hostnames, IP addresses, and subnets. Otherwise, select users, groups, or hosts as follows:
 - 5a** Click Specified, then click Browse.
 - 5b** Click Add, select from among the available objects in the NDS or eDirectory tree, then click OK.
 - 5c** Add additional sources.
 - 5d** When you have added the sources you want, click OK.
- 6** Under Destination, accept Any to apply the rule to any VPN server in the NDS or eDirectory tree; otherwise select destinations as follows:
 - 6a** Click Specified, then click Browse.
 - 6b** Click Add, select from among the available server objects in the NDS or eDirectory tree, then click OK.
 - 6c** Add additional destinations.
 - 6d** After you have added all the destinations, click OK.
- 7** (Optional) If you want the server to record all access attempts that match the rule, click Enable Rule Hit Logging.

Logging access attempts can affect server performance; however, we recommended that you do so to detect unauthorized activity.
- 8** Click OK, as necessary, to return to the Novell BorderManager 3.8 Access Rules page, then click OK to update the access rules.

Setting Up a Rule to Allow the Server to Resolve Hostnames

If you create any rules that allow access to hostname destinations that must be resolved by a DNS name server, you must create another rule at the Organization (O) or Organizational Unit (OU)

object that contains the Novell BorderManager 3.8 server to allow the server to resolve the hostname.

To create an access rule to allow the server access a DNS host to resolve a hostname:

- 1** In NetWare Administrator, right-click the object where the access rules are to be created and select Details.
- 2** Select the Novell BorderManager 3.8 Access Rules page, then click Add.
- 3** In the Access Rule Definition page, specify Allow (the default value).
- 4** For Access Type, select DNS.

The port number 53 appears in the Port field. Allowing outbound access to port 53 enables the Novell BorderManager 3.8 server to issue a DNS query.

- 5** Under Source, accept Any.
- 6** Under Destination, accept Any to allow any DNS name server to resolve the hostname; otherwise, select destinations as follows:
 - 6a** Click Specified, then click Browse.
 - 6b** Specify a DNS hostname, then click Add.

For DNS hostname specifications, you can use the wildcard character (*) in your entry.
 - 6c** Add additional destinations.
- 7** After you have added all the destinations, click OK.
- 8** (Optional) If you want the server to record all access attempts that match the rule, click Enable Rule Hit Logging.

Logging access attempts can affect server performance; however, we recommend that you do so to detect unauthorized activity.

- 9** Click OK, as necessary, until you return to the Novell BorderManager 3.8 Access Rules page, then click OK to update the access rules.

Setting Up Time Restrictions for Access Rules

By default, access rules you create are enforced 24 hours a day, every day. If you want to specify when access rules are enforced, you can set up a time restriction for each rule so it is effective only during a part of the day or week.

To specify time restrictions for an access rule:

- 1** In NetWare Administrator, right-click the object where the access rule has been created and select Details.
- 2** Select the Novell BorderManager 3.8 Access Rules page.
- 3** In the access rules list, select the Access Rule for which you want to specify time restrictions. Click Time Restrictions, then click Specified.
- 4** In the grid, click and drag through the days and times that you want the access rule to be in effect.

A highlighted area means the access rule applies to the source only during that time. To revert to enforcing the rule at all times, click None.

- 5 Click OK to return to the Novell BorderManager 3.8 Access Rules page, then click OK to update the access rules.

Viewing All Rules That Apply to an Object

Because access rules can be applied to different object classes in an NDS or eDirectory tree, more than one rule can affect a single object. The effective rules of an object are all access rules, in order of execution, from the Server object up to the root of the NDS or eDirectory tree.

To view the effective rules of an object:

- 1 From an administrator workstation, log in to the NDS or eDirectory tree where the Novell BorderManager 3.8 server is located and start the NetWare Administrator utility.
- 2 Locate the source object for which you want to view access rules in the NDS or eDirectory tree > right-click the object > select Details.

The object must be a Server, Organization, Organizational Unit, or Country.

- 3 Select the Novell BorderManager 3.8 Access Rules page.
- 4 Click Effective Rules.

A new window displays all access rules in the order they are applied.

NOTE: New access rules are not displayed in the effective rules list until the server is updated (Refresh Server) because they are not yet saved in NDS or eDirectory.

Completing Advanced Setup, Configuration, and Management Tasks

In addition to the basic setup procedures described in this section, there are several advanced setup, configuration, or management procedures you might need to complete, depending on your specific configuration. Advanced tasks are available in [Chapter 7, "Managing Access Control,"](#) on page 89 and include the following:

- ♦ Viewing user statistics
- ♦ Viewing user log entries
- ♦ Viewing rule descriptions
- ♦ Viewing host statistics
- ♦ Viewing host record entries
- ♦ Viewing usage trends
- ♦ Exporting data

7

Managing Access Control

The following sections explain the tasks you must complete to manage Novell® BorderManager® 3.8 access control by checking the access control log:

- ♦ “Viewing User Statistics” on page 89
- ♦ “Viewing Host Statistics” on page 91
- ♦ “Exporting Data” on page 92

See the Setting Up Access Control section in the Novell BorderManager 3.8 Install Guide for information on how to set up access control files.

Viewing User Statistics

To display the User Statistics window:

- 1** In NetWare® Administrator, click the Server object representing the Novell BorderManager 3.8 server.
- 2** Click Tools > Novell BorderManager 3.8, then click View Access Control.

The Access Control Users Statistics window has two list boxes: the Number of Users list box and the Hosts Accessed by User list box. Initially, the list boxes are empty.

- 3** To display the records for a set of connections from a specific user to a specific host, select Display Records and specify a time range for the records you want displayed.

For a U.S. English system, the dates are entered in the order of month, day, and year. The order is year, month, and day for a Japanese system; and day, month, and year for European language systems.

While the records are being read, a dialog box displays the number of records processed, the date and time of the last record that was read, and a status bar showing the portion of the records read based on the range of dates specified. Click Cancel to cancel the query process. Records that have been read are displayed in the Access Control Users Statistics window.

You can click the column heading of either list box to sort the entries in that column in ascending or descending order. The sorting order is reversed each time you click the column heading.

The number of users list box provides the following information about activity through access control:

- ♦ Username: NDS® or eDirectory™ name or IP address of the user. For an IP address, the Domain Name System (DNS) domain name is displayed if it exists in the local DNS list. The local DNS list is built each time the WHO IS command or DNS Hostname is invoked using the right-click menu.
- ♦ Hosts Accessed: Number of hosts accessed for the specified period of time.

- ◆ Connections: Total number of connections used to access hosts.

The Hosts Accessed by number of Users list box provides the following information about activity through access control:

- ◆ Protocol: Protocol string representing the port number used for the connection, such as HTTP, FTP or HTTPS. For example, HTTP represents a connection made using port 80.
- ◆ Hostname: DNS name or IP address of the accessed host.
- ◆ Allowed: Total number of connections granted access to the host for a user.
- ◆ Denied: Total number of connections denied access to the host for a user.

4 To display additional types of user information:

- 4a** To display all the connections made by a user, double-click a username in the Number of Users list box.

The Access Control Log window displays the following information about the user's activity through access control:

- ◆ Entry Time: Time connection was established.
- ◆ Username: NDS or eDirectory name or IP address of user.
- ◆ Access: Action specified in the access rule for this connection.
- ◆ Protocol: Protocol string representing the port number used for the connection, such as HTTP, FTP, or HTTPS. For example, HTTP represents a connection made using port 80.
- ◆ Hostname: DNS name or IP address of the accessed host.
- ◆ Service: Service used to access the host, such as Proxy Services.
- ◆ Rule Number: ID number of the rule that grants or denies access to hosts.

- 4b** To see a description of the rule for a connection between a user and a host, double-click the connection entry in the Access Control Log window.

The Rule Description window provides the following information about activity through access control:

- ◆ Rule Number: ID number of the rule that grants or denies access to hosts.
- ◆ Date of Creation: Day and time the rule was created.
- ◆ Action: Whether the connection is allowed or denied.
- ◆ Source: IP address, hostname, or interface name of the connection source to which the rule is applied.
- ◆ Destination: IP address, hostname, or interface name of the connection destination to which the rule is applied.
- ◆ Access Specification: Any protocol, URL, or SurfControl* rule that determines connection access or denial.

- 4c** To view usage trend graphs, click Usage Trends in the User Statistics window, then select any of the following graphs to view usage trend data by time of day in one-hour increments:

- ◆ Users: Bar graph showing the number of unique users allowed to connect to a host.
- ◆ Hosts Accessed: Bar graph showing the number of hosts accessed.

- ◆ Access Volume: Line graph showing the number of allowed and denied connections.
- ◆ Access Allowed: Bar graph showing the number of allowed connections.
- ◆ Access Denied: Bar graph showing the number of denied connections.
- ◆ Users, Hosts, and Access Volume: Combination line and bar graph showing the number of users, hosts accessed, and total connections.

All graphs can be saved to disk, copied to the clipboard, or printed.

Viewing Host Statistics

To display specific host information:

- 1** In NetWare Administrator, click the Server object representing the Novell BorderManager 3.8 server.
- 2** Click Tools > Novell BorderManager 3.8, then click View Access Control.
- 3** To display the records for a set of connections from a specific user to a specific host, click Display Records and specify a time range for the records you want displayed.
- 4** To see which users have accessed a host, double-click the entry for that host in the Hosts Accessed by User list box in the User Statistics window.

The Access Control Hosts window displays two list boxes: the Number of Hosts list box and the User Access list box. As in the User Statistics window, the entries can be sorted by selecting the column headings.

The Number of Hosts list box provides the following information:

- ◆ Protocol: Protocol string representing the port number used for the connection such as HTTP, FTP, or HTTPS. For example, HTTP represents a connection made using port 80.
- ◆ Hostname: DNS name or IP address of a host.
- ◆ Users Accessed: Number of users who have accessed the selected host.
- ◆ Connections: Number of connections that have been allowed access.

The User Access list box provides the following information:

- ◆ Username: IP address or DNS name of the user who accessed the host.
- ◆ Allowed: Number of connections granted access to the host.
- ◆ Denied: Number of connections denied access to the host.

- 5** To see a list of connections for users who have accessed a host, double-click the entry for the host in the Host Statistics window.

The Access Control Log window for the selected host is displayed. The Rules Description window can be viewed by double-clicking an entry.

The Access Control Log list box provides the following information about activity for the selected host through access control:

- ◆ Entry Time: Time the connection was established.
- ◆ Username: NDS or eDirectory name or IP address of the user.
- ◆ Access: Action specified in the access rule for this connection: either Allowed or Denied.

- ◆ Protocol: Protocol string representing the port number used for the connection such as HTTP, FTP or HTTPS. For example, HTTP represents a connection made using port 80.
- ◆ Hostname: DNS domain name or IP address of the accessed host.
- ◆ Service: Select Proxy Services as the service used to access the host.
- ◆ Rule Number: ID number of the rule that grants or denies access to the hosts.

Exporting Data

The access control log is stored in a Btrieve file on the Novell BorderManager 3.8 server and is maintained by csaudit.nlm. The access log cannot be edited or manipulated from the server; however, the data can be exported for analysis. The format of the exported data is compatible with trend analysis software packages, such as WebTrends.

There are two ways to export the access control log from NetWare Administrator:

- ◆ [“Exporting Data from the Access Control Users Statistics Window” on page 92](#)
- ◆ [“Exporting Data Using the Export Logs Option” on page 93](#)

If you use the second method, you can also combine the audit log files from other Novell BorderManager 3.8 services with the access control log into a single ASCII file.

Exporting Data from the Access Control Users Statistics Window

- 1** In NetWare Administrator, click the server object representing the Novell BorderManager 3.8 server.
- 2** Click Tools > Novell BorderManager 3.8, then click View Access Control.
- 3** Click Display Records, specify the dates for the records you want to display, then click OK.
- 4** In the Access Control Users Statistics window, click Export Data and specify the path and filename.
or
Click Browse to select the destination of the export file.
- 5** Select one of the following sort formats under Information Output Selection, then click OK.
 - ◆ Entry Time (connection by connection): (Default selection) Sorts records from the earliest entry time to latest entry time.
 - ◆ Access by users: Sorts records in alphabetic order based on the user's NDS or eDirectory username.
 - ◆ Access by hosts: Sorts records in ascending order (for IP addresses) or alphabetic order (for DNS hostnames).
- 6** If the export filename already exists under the directory path selected, you are prompted to replace the file. Click Yes to overwrite the file or No to specify the destination as described in [Step 4 on page 90](#).

The record fields are written to disk with a tab as the delimiter. Each record ends with a carriage return and line feed. The exported data has the following format:

- ◆ Entry Time: Time connection was established.
- ◆ Username: NDS or eDirectory name or IP address of the user.

- ◆ Access: Either Allowed or Denied as the action specified in the access rule for this connection.
- ◆ Protocol: Protocol string representing the port number used for the connection, such as HTTP, FTP, or HTTPS. For example, HTTP represents a connection made using port 80.
- ◆ Hostname: DNS name or IP address of the accessed host.
- ◆ Service: Service used to access the host: Proxy Services.
- ◆ Rule Number: ID number of the rule that grants or denies access to the hosts.

Exporting Data Using the Export Logs Option

The procedure to export access control data using the Export Logs option from the Novell BorderManager 3.8 menu extracts the same data from the Btrieve database, but offers additional export options that cannot be activated from the Access Control Users Statistics window.

To export the access control log:

- 1** In NetWare Administrator, click the server object representing the Novell BorderManager 3.8 server.

- 2** Click Tools > Novell BorderManager 3.8, then click Export Logs.

- 3** Click Set Range to specify the date range.

This is the range of dates comparable to the dates used to display records in the Access Control Users Statistics window. The default range is the current server date.

- 4** Click Browse to select the drive mapped to the destination for the export file.

This is the path and filename for the export file. The default destination is a:\yyyymmdd.log, where *yyyy* is the current year, *mm* is the current month, and *dd* is the current day. If you change the filename from the default format, the filename does not reflect the current server date. For example, if you change the filename format to *mmddyyyy.log*, the next time you try to export logs on another day, the log filename would not have incremented to the current date.

- 5** (Optional) If the default filename is unacceptable, specify the filename in the File field.

- 6** (Optional) If you want to combine the access control log with audit logs from other Novell BorderManager 3.8 services, select the Combine Log Files check box.

This feature allows log files from different services to be combined into a single output file. When log files are combined, they are appended to one file, service by service.

- 7** Under Log Selection, select the box for ACL.

If the Combine Log Files feature has been selected, select all the services whose data will be combined into the export log file.

- 8** (Optional) If you selected Combine Log Files in **Step 6**, under Log Selection, select all other Novell BorderManager 3.8 services audit log files to be combined with the access control log file.

- 9** Click OK.

The access control log is exported to an ASCII file. The record fields are written with a tab as the delimiter. Each record ends with a carriage return and line feed. The exported access control data has the following fields:

- ◆ Keyword: ACL. If the Combine Log Files option was selected, the keyword is at the beginning of each line from the access control list (ACL) audit log.

- ◆ Date.
- ◆ Time.
- ◆ Source: Typeless eDirectory name and context, such as mlira.pubs.novell, or an IP address.
- ◆ Destination: Domain name or IP address.
- ◆ Bytes received.
- ◆ Status: Allow or Deny.
- ◆ Protocol: Protocol used, such as HTTP or FTP.
- ◆ Service: Service used to access the host: Proxy Services.
- ◆ Rule ID: An 8-digit hexadecimal number that identifies the rule associated with the allowed or denied access.

If the Combine Log Files feature is *not* selected and you select one or more services under the Log Selection field, a separate export file is created for each service under a subdirectory of the export destination path.

The export subdirectories used are shown in the following table.

Log Type	Export Subdirectory
HTTP Proxy	HTTP
FTP Proxy	FTP
NNTP Proxy	NNTP
Mail Proxy	SMTP
RealAudio* and Real Time Streaming Protocol (RTSP) Proxies	RAUDIO
DNS Proxy	DNS
Generic Proxy	GENERIC
SOCKS Client	SOCKS
IPX Gateway	IPXGW
VPN	VPN
ACL (access control)	ACL

For example, if you specified an export destination of `vol1:logs\19981019.log`, did not select the Combine Log Files feature, and selected the boxes for HTTP Proxy, SOCKS client, and ACL, the following log files would result:

- ◆ `vol1:logs\http\19981019.log`
- ◆ `vol1:logs\socks\19981019.log`
- ◆ `vol1:logs\acl\19981019.log`

8

Setting Up Alert Notification

Novell® BorderManager® 3.8 Alert monitors server performance, security, and reports potential or existing server problems that affect the performance of configured Novell BorderManager 3.8 services.

Novell BorderManager 3.8 Alert reports server events indicating a potential problem with any of the following:

- ◆ Server performance
- ◆ License acquisition, excluding Novell BorderManager 3.8 Authentication Services licenses; Novell BorderManager 3.8 Alert does not report a problem with a Novell BorderManager 3.8 Authentication Services license
- ◆ Security
- ◆ Proxy server connections

Novell BorderManager 3.8 Alert monitors a predefined set of server events. However, you can select the individual events for which you want to receive notification.

When an alert is triggered on a Novell BorderManager 3.8 server, the default notification includes the following:

- ◆ An e-mail message (sent to all e-mail addresses in the E-mail Alert list)
- ◆ An entry in the server's audit trail log file
- ◆ A server console message

NOTE: Novell BorderManager 3.8 Alert output supports automatic paging from your e-mail system. This requires additional configuration and the process varies depending on the e-mail software you use. Consult your e-mail software documentation to determine if this option is configurable for your system.

This section explains the tasks you need to complete to set up an initial implementation of Novell BorderManager 3.8 Alert e-mail notification. It contains the following sections:

- ◆ [“Setting Up Alert E-Mail Notification” on page 95](#)
- ◆ [“Completing Advanced Setup, Configuration, and Management Tasks” on page 97](#)

NOTE: This section describes the tasks required to set up an initial implementation of Novell BorderManager 3.8 Alert.

For planning and conceptual information about Novell BorderManager 3.8 Alert, refer to the *Novell BorderManager 3.8 Overview and Planning Guide*, available in the online documentation. Make sure you understand this information before setting up and configuring Novell BorderManager 3.8 Alert.

Setting Up Alert E-Mail Notification

To set up Novell BorderManager 3.8 e-mail notification:

- 1** In NetWare[®] Administrator, locate the object in the NDS[®] or Novell eDirectory[™] tree where the alert configuration will be specified > right-click the object > select Details.

An alert can be configured only for an Organization (O), Organizational Unit (OU), or Server object.

- 2** Click the Novell BorderManager 3.8 Alert page.

- 3** Select one of the following notification schemes:

- ◆ **Inherit (default):** Specifies that an alert configuration is obtained from a container higher up in the NDS or eDirectory tree. An alert configured for a Server object cannot be inherited by another container or Server object.

Inherit disables the E-mail Alert and E-mail Servers lists for the selected NDS or eDirectory object. If these lists have been previously configured, the recipients and servers in the lists are deleted after you click OK.

To view the inherited information, click Effective Configuration. The Effective Configuration information is read-only. To change the alert information, identify the NDS or eDirectory container in the Location of Specification field and open the Novell BorderManager 3.8 Alert page from that container's Details page.

- ◆ **Send Alert:** Enables the E-mail Alert and E-mail Servers lists you configure for the selected NDS or eDirectory object. To specify e-mail recipients and servers, continue with Step 4.
- ◆ **None:** Disables the alert service. No event or error notification will occur. However, selecting None preserves your configuration; recipients and servers are only inactive.

- 4** (Optional) If you selected Send Alert earlier, specify the alert conditions for which you want notification as given in the following steps.

- 4a** Click Alert Conditions.

- 4b** Click Specific (the default is All).

- 4c** Select the alert conditions.

- 4d** Click OK.

- 5** Specify E-mail Alert Recipients and E-mail Servers.

NOTE: The Novell BorderManager 3.8 server must be configured with at least one e-mail server. Otherwise, alert notification will fail.

- 5a** Click Add for the E-mail Alert field and specify the e-mail address of the person to be notified by Novell BorderManager 3.8 Alert.

Add as many e-mail recipients as necessary. There is no upper limit on the number of recipients that can be added.

- 5b** (Optional) To remove a recipient from the list, select the recipient's e-mail address and click Delete for the E-mail Alert field.

- 5c** Click Add for the E-mail Server's field and specify the e-mail server name or IP address for the recipients added in Step 5a.

The first server in the list is the primary e-mail server. The primary server receives alert messages and routes them to other e-mail servers on the network, if necessary.

All other servers in the list act as backup e-mail servers if the primary server fails to route the e-mail. This can occur if e-mail forwarding has been disabled on the primary server or if the primary server is down.

Add as many e-mail servers as necessary. Although there is no upper limit on the number of backup servers that can be added, Novell BorderManager 3.8 Alert sends alerts to only one e-mail server on the list.

TIP: To increase the performance of Novell BorderManager 3.8 Alert, specify the IP addresses of e-mail servers. When IP addresses are used, the Novell BorderManager 3.8 server is not required to process Domain Name System (DNS) lookups to resolve the DNS hostnames of e-mail servers.

- 5d** (Optional) To remove an e-mail server or servers from the list, highlight the e-mail server name or IP address, then click Delete for the E-mail Server field.
- 5e** (Optional) To change an e-mail server's status as a primary or backup server, click the up-arrow or down-arrow to move the e-mail server's name or IP address up or down the list.
- 6** Click OK to save the configuration and exit the Details page.

Clicking OK saves the configuration changes in NDS or eDirectory and notifies brdsrv.nlm that a configuration change has occurred. Alert configurations are updated on each NDS or eDirectory replica during normal NDS or eDirectory synchronization.

If you enabled an alert configuration for an entire organization, it might take a while for all Novell BorderManager 3.8 servers to be notified of the configuration change in NDS or eDirectory.

- 7** (Optional) If you enabled an alert configuration for an entire organization and want a specific server to use the alert configuration immediately, rather than after NDS or eDirectory synchronization occurs, complete the following substeps:
 - 7a** Double-click the Server object representing the Novell BorderManager 3.8 server you want to begin using the alert configuration immediately.
 - 7b** From the Server object's Details page, click Novell BorderManager 3.8 Alert to view the Novell BorderManager 3.8 Alert page for the server.
 - 7c** Click Refresh Server.

IMPORTANT: When you first open the Novell BorderManager 3.8 Alert page, the Refresh Server button is available. Clicking Refresh Server causes brdsrv.nlm to read the new alert configuration for this server only. It does not trigger a full NDS or eDirectory synchronization. If you modify the alert configuration for this Server object, the Refresh Server button is inactive and no longer an option.

Completing Advanced Setup, Configuration, and Management Tasks

In addition to the basic setup procedures described in this section, there are several advanced setup, configuration, or management procedures you might need to complete, depending on your specific configuration. Advanced tasks are available in the [Chapter 9, "Managing Alert Messages," on page 99](#) and include the following:

- ◆ Viewing alerts sent as e-mail messages
- ◆ Viewing alerts in the audit trail log file
- ◆ Viewing alerts in the console log
- ◆ Responding to alerts

9

Managing Alert Messages

The following sections describe how to view alert messages generated by Novell® BorderManager® 3.8 Alert and how to respond to them:

- ♦ “Viewing Alerts Sent as E-Mail Messages” on page 99
- ♦ “Viewing Alerts in Audit Trail Log File” on page 100
- ♦ “Viewing Alerts in the Control Log” on page 101
- ♦ “Responding to Alerts” on page 101

See Chapter 8, “Setting Up Alert Notification,” on page 95 for information on how to set up alerts.

Viewing Alerts Sent as E-Mail Messages

All e-mail notifications triggered by Novell BorderManager 3.8 Alert contain a time stamp, the name of the server where the event occurred, the service affected, and an error message.

NOTE: When the message is sent to a pager, the time stamp, server name, and error message appear first, followed by the sender, recipient, and subject. This is done to accommodate paging services that limit the amount of alphanumeric text that is displayed.

In the sample e-mail message that follows, substitute your own Domain Name System (DNS) domain name for novell.com:

From: *nbmalert@novell.com*

To: *admin_1@novell.com admin_2@novell.com*

Subject: The system is short on disk space and operations may fail

Time: 7-17-98 9:45:07am

Server: SJ-NW5

Service: NetWare Operating System

The system is short on disk space and operations might fail

NOTE: If a loaded NetWare® Loadable Module™ (NLM™) causes the alert, the e-mail message might not always identify the offending NLM because the NLM that detected the error might be reported instead. Therefore, load monitor.nlm to check any unusual statistics if the cause of the alert is not clearly evident.

If Novell BorderManager 3.8 Alert has been configured and e-mail notification fails to occur when alerts are displayed on the server console, verify the following:

- ♦ The alert condition has been enabled for notification in NetWare Administrator.
- ♦ All e-mail addresses configured for the Novell BorderManager 3.8 server are for valid accounts.
- ♦ The primary and backup e-mail servers have e-mail forwarding enabled.

- ◆ The primary e-mail server or at least one backup e-mail server is up and running.
- ◆ All NDS[®] or Novell eDirectory[™] partitions have been synchronized if the alert configuration was recently changed.

A delay in synchronization can mean that your server has not been updated with the latest configuration, especially if the alert configuration applies to an entire organization.

- ◆ A route to the mail server has been established. Ping the mail server from the Novell BorderManager 3.8 server and inspect the trace on the route.
- ◆ There are no filters on routers between the Novell BorderManager 3.8 server and the mail server that deny Simple Mail Transfer Protocol (SMTP) traffic.

Viewing Alerts in Audit Trail Log File

Novell BorderManager 3.8 Alert logs server events in the audit trail log file. The alert record contains information such as the type of alert, a description of the event, the name of the server that generated the alert, and a time stamp. Use the audit trail log file to check for anomalies or suspicious activities that affect routing and security on your network.

The audit trail log file, `csaudit.log`, is maintained by `csaudit.nlm`. The audit trail log file is managed with the CSLIB audit trail utility. Use this utility to view records in the audit trail log and configure a schedule for archiving the log. The active audit trail log file is located in `sys:\system\cslib`. Archived audit log files are located in `sys:\system\cslib\logs`.

This section contains the following procedures:

- ◆ [“Displaying Audit Trail Log Records with the Audit Trail Utility” on page 100](#)
- ◆ [“Archiving the Audit Trail Log File” on page 100](#)

Displaying Audit Trail Log Records with the Audit Trail Utility

To view the audit trail log file:

- 1** To run the CSLIB audit trail utility from the server console, enter
CSAUDIT

- 2** Click Display Audit Trail Records.

The currently active log file is displayed. If the current log file has the record you need, you are done. Otherwise, to view an archived log file, continue with Step 3.

- 3** Press Insert to view the other display options.
- 4** Click the Display Options menu > Select from Archived File List.
- 5** Use the Up-arrow and Down-arrow to locate the archived log file to view.
- 6** Click Specify to view the records in the log file.
- 7** Press Esc until you are prompted to exit the audit trail utility.

Archiving the Audit Trail Log File

As with most log files, the audit trail log file can grow rapidly. It is important to archive it and rotate the archived log files on a regular basis, because the audit trail log file is stored on the `sys:` volume.

To configure the frequency of archiving and the number of archived log files:

- 1** From the server console, enter
CSAUDIT
- 2** Click Audit Trail Configuration.
- 3** Press Enter in the Archive Hour field and select the hour at which the audit trail log file should be archived.
- 4** In the Archive Interval field, specify the number of days for which the active audit log file records data.
- 5** In the Archive Files Retained field, specify the number of audit log files to be archived before the first archived file is overwritten.
- 6** Press Esc, then select Yes to save the changes.
- 7** Press Esc until you are prompted to exit the audit trail utility.

Viewing Alerts in the Control Log

The alert message is also saved in `sys:\etc\console.log`, because Novell BorderManager 3.8 Alert sends alert messages to the server console, if conlog is running on the server.

To view the console log at the server console, specify the following:

```
LOAD EDIT SYS:ETC\CONSOLE.LOG
```

Responding to Alerts

Novell BorderManager 3.8 Alert monitors server performance, license acquisition for licensed Novell BorderManager 3.8 services, security, and Proxy Services availability.

For information on specific alerts:

- ◆ [“Server Performance Alerts” on page 102](#)
- ◆ [“License Acquisition Alerts” on page 103](#)
- ◆ [“Security Alerts” on page 103](#)
- ◆ [“Proxy Alerts” on page 105](#)

The following table describes some recommended responses to the Novell BorderManager 3.8 alerts:

Alert	Recommended Actions
Disk space shortage	Reduce the size and number of log files. Add more disk space, if necessary.
Memory shortage	<p>Check server resources using <code>monitor.nlm</code> to determine whether a module is using excessive memory. Add more memory, if necessary. Depending on the bus type, some NetWare servers do not register all the memory present unless a REGISTER MEMORY statement exists in the <code>startup.ncf</code> file. More information about REGISTER MEMORY is located in the NetWare 5 online documentation at the following path:</p> <p>Reference > Utilities Reference (under the General Reference heading) > Utilities > REGISTER MEMORY</p>

Alert	Recommended Actions
ECB shortage	Check server resources using monitor.nlm to determine which NLM uses the most event control blocks (ECBs). Increase the maximum packet receive buffers on the server if server memory allows.
License error	Verify the current licenses installed for the server and check for license conflicts or expired trial licenses. Install additional licenses, if necessary.
Loading or unloading a security-sensitive NLM	This alert is primarily informational. Verify that the server console is secure and all remote sessions are authorized. Reload or unload the NLM, if necessary.
Oversized ping packet	Use a packet sniffer to capture packets and determine the source IP address. Configure a TCP/IP packet forwarding filter to block pings originating from that source.
SYN packet flooding	Use a packet sniffer to capture packets and determine the source IP address. Configure a TCP/IP packet forwarding filter to block TCP packets originating from that source.
Oversized UDP packet	Use a packet sniffer to capture packets and determine the source IP address. Configure a TCP/IP packet forwarding filter to block UDP packets originating from that source.
Cache hierarchy parent (ICP parent) down	Ping the parent server to check if there is a routing problem. Verify that the parent server for the cache hierarchy is down and bring the server back up. Note that if the cache hierarchy has multiple parents configured, proxy servers lower in the hierarchy will use the other parent servers while this server is down.
SOCKS server down	Ping the SOCKS server to check if there is a routing problem. Verify that the SOCKS server is down and bring the server back up.
POP3 or SMTP server down	Ping the Post Office Protocol 3 (POP3) or SMTP server to check if there is a routing problem. Verify that the POP3 server or internal mail server is down. You might not be able to resolve this problem if the POP3 server is administered by someone who is outside your organization.

Server Performance Alerts

Server performance alerts notify you of potential problems with server parameters or operations that can cause Novell BorderManager 3.8 services to underperform or fail.

The server performance alerts are as follows:

- ◆ Disk space shortage

A disk space shortage warning indicates that the shortage of disk space is severe enough to potentially cause server operations to fail.
- ◆ Memory shortage

A memory shortage warning indicates that the shortage of memory is severe enough to potentially cause server operations to fail.
- ◆ Event Control Block (ECB) shortage (out of receive buffers or no ECBs available)

An ECB shortage warning indicates that the packet receive buffer or ECB shortage is severe enough to potentially cause network input or output to degrade or fail.

License Acquisition Alerts

A license alert indicates that a Novell BorderManager 3.8 service was unable to acquire the license it needs to operate.

Novell BorderManager 3.8 Alert monitors license acquisition for the following:

- ◆ Proxy Services
- ◆ Virtual Private Network (VPN) servers and clients
- ◆ Access control

Security Alerts

Security alerts notify you of possible security breaches. The causes of these alerts should be investigated further because your server might be the target of a denial-of-service attack.

Denial-of-service attacks commonly plague servers connected to the Internet and are initiated by someone without authorized access to servers. A denial-of-service condition can be caused by a bombardment of packets sent to a server in order to consume significant memory or CPU processing time. After these server resources have been allocated to handle the packets, connection requests made by legitimate users cannot be processed effectively.

As with computer viruses, new denial-of-service attacks are launched on the Internet community without warning. Many of the known denial-of-service attacks are documented on various Web sites.

The Novell BorderManager 3.8 security alerts include the following:

- ◆ Loading or unloading a security-sensitive NLM

Security-sensitive modules are those that can potentially compromise network or server security when they are loaded or unloaded.

The modules that are considered security-sensitive are as follows:

- ◆ ds.nlm
 - ◆ ftpserv.nlm
 - ◆ ipxipgw.nlm
 - ◆ proxy.nlm
 - ◆ remote.nlm
 - ◆ tftpserv.nlm
 - ◆ vpninf.nlm
 - ◆ vpmaster.nlm
 - ◆ vpslave.nlm
- ◆ Oversized ping packet

An oversized ping packet warning can indicate that malicious activity is occurring on the server. This alert is generated when the server receives and discards ping packets that have more than 10,240 bytes of data. The server is enabled to discard these packets by default.

For certain situations that require your server to receive larger ping packets, such as router stress tests, specify the following SET commands at the server console to change the largest ping packet size or disable packet discarding:

SET LARGEST PING PACKET SIZE=*N*

SET DISCARD OVERSIZED PING PACKETS=OFF

The variable *n* is a decimal number representing the number of bytes allowed. Never specify a number with commas.

To re-enable packet discarding, enter the following command at the server console:

SET DISCARD OVERSIZED PING PACKETS=ON

NOTE: You should know your network topology before changing the largest ping packet size, because packet sizes are limited by the type of media used. For Ethernet only, the oversized ping packet alert is not generated if the largest ping packet size is set between 35,541 and 65,535 bytes. However, alerts are generated for packets smaller than 35,541 bytes. The acceptable packet size ranges for other media differ and depend on each medium's maximum transmission unit (MTU), which is the largest packet size a medium can transport without fragmentation.

◆ SYN packet flooding

A TCP SYN packet flood warning can indicate that malicious activity is occurring on the server, which can cause a denial-of-service condition. TCP connections require a three-way handshake between the server and client:

- ◆ The client sends a packet in which the SYN flag is set in the TCP header.
- ◆ The server sends a SYN/ACK (acknowledgment) packet.
- ◆ The client sends an ACK packet so data transmission can begin. A denial-of-service condition occurs when the client fails to send the last ACK packet and intentionally sends successive TCP connection requests to the server to fill up the server's buffer.

After the server's buffer is full, other clients cannot establish a connection, resulting in a denial-of-service condition.

IMPORTANT: Novell BorderManager 3.8 Alert detects only SYN packet floods for socket applications, such as FTP.

Because of the importance of defending your server against SYN packet floods, the detection of SYN packet floods should always be enabled. However, for extreme troubleshooting measures, use the following SET command to disable detection if necessary:

SET TCP DEFEND SYN ATTACKS=OFF

Re-enable detection with the following command:

SET TCP DEFEND SYN ATTACKS=ON

◆ Oversized UDP packet

An oversized UDP packet warning can indicate that the malicious activity is occurring on the server. This alert is generated when the server receives and discards UDP packets larger than 16,384 bytes. The server is enabled to discard these packets by default.

If necessary, specify the following SET commands at the server console to change the largest UDP packet size or disable packet discarding:

SET LARGEST UDP PACKET SIZE=*n*

SET DISCARD OVERSIZED UDP PACKETS=OFF

The variable *n* is a decimal number representing the number of bytes allowed. Never specify a number with commas.

To re-enable packet discarding, specify the following command at the server console:

SET DISCARD OVERSIZED UDP PACKETS=ON

NOTE: You should know your network topology before changing the largest UDP packet size, because packet sizes are limited by the type of media used. For Ethernet only, the oversized UDP packet alert is not generated if the largest UDP packet size is set between 35,541 and 65,535 bytes. However, alerts are generated for packets smaller than 35,541 bytes. The acceptable packet size ranges for other media differ and depend on each medium's MTU, which is the largest packet size a medium can transport without fragmentation.

Many other documented denial-of-service attacks can be detected by Novell BorderManager 3.8 Alert, although attacks are not identified by name.

Proxy Alerts

Proxy alerts generally indicate that a proxy server has not been configured correctly or is down.

The proxy alerts are as follows:

- ◆ Cache hierarchy parent (ICP parent) down

A cache hierarchy parent down warning indicates a problem with the parent proxy cache server in a configured cache hierarchy. If the cache hierarchy client is enabled on the proxy server and the proxy fails to connect to the parent, the alert is triggered.

If the option to forward all requests through the hierarchy has been selected and the parent is down, requests that cannot be fulfilled through the cache can result in an error because the parent is not available to access the source information.

- ◆ SOCKS server down

A SOCKS server down warning indicates that the SOCKS server to which the proxy cache server connects as a client is down. If the SOCKS client is enabled on the proxy server and the proxy fails to make a connection, the alert is triggered. Because a SOCKS server is often used as a firewall, requests that cannot be fulfilled through the cache can result in an error because the proxy cannot forward requests through the firewall.

- ◆ POP3 or SMTP server down

A POP3 server down warning indicates that there is a problem with a POP3 server or an internal SMTP mail server.

The mail proxy enabled on the Novell BorderManager 3.8 server cannot forward outgoing mail to the POP3 server or deliver incoming mail to the SMTP server.



Filters

Novell® BorderManager® 3.8 delivers filter configuration based on Novell iManager. FILTCFG can still be used to configure filters. For more information refer to [“Installing iManager 2.0.1 Snap-Ins” on page 24](#).

Novell BorderManager 3.8 extends the directory schema to add attributes to server objects for IP packet filtering. The filter configuration is stored in Novell eDirectory™. This allows the use of either FILTCFG or Novell iManager on a Novell BorderManager 3.8 server, and also provides a natural backup of the firewall configuration. Changes in Novell iManager are automatically moved out to the server and put into effect.

During the installation of Novell BorderManager 3.8, if packet filtering is already configured on the server, the existing configuration is imported into eDirectory. By storing the firewall configuration in eDirectory, Novell BorderManager 3.8 extends the functionality. See the following sections for more information:

- ♦ [Chapter 10, “Setting Up Packet Filters,” on page 109](#) provides information on the basic steps to set up filters on Novell BorderManager 3.8 servers.
- ♦ [Chapter 11, “Managing IP Packet Filters,” on page 121](#) provides information on the configuration parameters for the IP packet filter log and the standard IP packet filter log format.
- ♦ [Chapter 12, “Packet Filtering Using Novell iManager,” on page 125](#) provides information on setting up RIP, EGP, OSPF, and Packet Forwarding Filters.
- ♦ [Chapter 13, “Backing Up and Restoring Filters,” on page 139](#) provides information on NDS® or Novell eDirectory.
- ♦ [Chapter 14, “Advanced Configuration of IP Packet Filters Using FILTCFG,” on page 141](#) provides information on setting up HTTP, FTP, Telnet, SMTP, POP3, and DNS filters.
- ♦ [Chapter 15, “NBM Filter Management,” on page 151](#) provides information on configuring filters and exceptions the easiest way. The role, previously named as “NBM Access Management“ is renamed “NBM Filter Management.

10

Setting Up Packet Filters

Packet filters provide network-layer security to control the types of information sent between networks and hosts. Novell® BorderManager® supports Routing Information Protocol (RIP) filters, External Gateway Protocol (EGP), and packet forwarding filters to control the service and route information for the common protocol suites, including Internetwork Packet Exchange™ (IPX™) software and TCP/IP.

If you chose to secure the public interfaces of your Novell BorderManager 3.8 server during installation, a set of default filters was configured at that time. If you performed an upgrade, the existing filters were retained and the default filters were added to the filter list.

The default filters block all traffic through the public interfaces except for the traffic being forwarded to and from an enabled Novell BorderManager 3.8 service. Novell BorderManager 3.8 creates exceptions to allow some selected services during installation. This section explains the tasks you must complete to configure packet filtering to allow additional services to be routed through the Novell BorderManager 3.8 server.

With Novell BorderManager 3.8 the TCP/IP filters can also be configured through Novell iManager.

This section describes the tasks required to set up an initial implementation of Novell BorderManager 3.8 packet filtering. For planning and conceptual information about packet filtering, refer to the *Novell BorderManager 3.8 Overview and Planning Guide*, available in the online documentation. Make sure you understand this information before setting up and configuring packet filtering.

The following sections are discussed here:

- ◆ “[Packet Filter Prerequisites](#)” on page 109
- ◆ “[Setting Up the Default Filters](#)” on page 110
- ◆ “[Using Novell iManager for Filter Configuration](#)” on page 110
- ◆ “[Using FILTCFG for Filter Configuration](#)” on page 113

Packet Filter Prerequisites

Before you begin to configure packet filters for your Novell BorderManager 3.8 server, you should have the following information at hand:

- ◆ **Your company security policy.** The security policy should define the communication allowed with external sources and between various segments of the corporate intranet.
- ◆ **Your current network topology.** You need to know the physical layout of the network components.

- ◆ **Information about other firewall components.** You need to know what other security measures are in place (or will be in place) so that you do not inadvertently circumvent or disable those measures.

Setting Up the Default Filters

If you did not choose to secure the public interfaces of Novell BorderManager 3.8 during installation, you can do so at any time. This process secures the public interface of your machine and only the traffic to and from a Novell BorderManager service is allowed.

To set up default filters:

- 1** At the server console prompt, enter
`LOAD BRDCFG`
- 2** When prompted, select Yes to configure the set of default filters and press Enter.
- 3** When prompted to launch INETCFG, select No, then press Enter.
- 4** From the Filter Configuration Options menu, select Setup Filters on the PublicInterface then press Enter.
- 5** Select the Public Interface from the list, then press Enter.
- 6** Follow the prompts to enable and configure the default filters.

The default filter settings block all IPX and IP traffic except to and from the Proxy Services, and Virtual Private Networks (VPNs). Filter support for both IPX and TCP/IP are automatically enabled when the default filters are enabled.

To manually enable or disable the Filter Support option for the TCP/IP protocol:

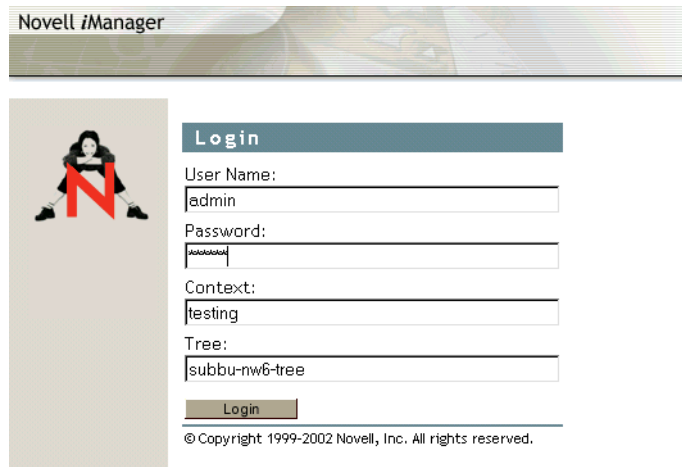
- 1** At the server console prompt, enter
`LOAD INETCFG`
- 2** Select Protocols > TCP/IP > Filter Support > Status.
- 3** Select Enabled or Disabled, then press Enter.

NOTE: When Filter Support is disabled, the protocol operates as if the filter module is not loaded, and no filtering occurs. When Filter Support is enabled, changes to the filter configurations take effect immediately without reinitializing the server.

Using Novell iManager for Filter Configuration

These sections tell you how to use Novell iManager for filter configuration. The Novell BorderManager Access Management role and Packet Filtering configuration tasks are automatically plugged into Novell iManager during Novell BorderManager 3.8 installation. By default, this role is assigned to the administrator only.

Log in to Novell iManager to use the Packet Filtering Configuration Task.

Figure 6 Novell iManager Login Screen


Novell iManager

Login

User Name:
admin

Password:
[password]

Context:
testing

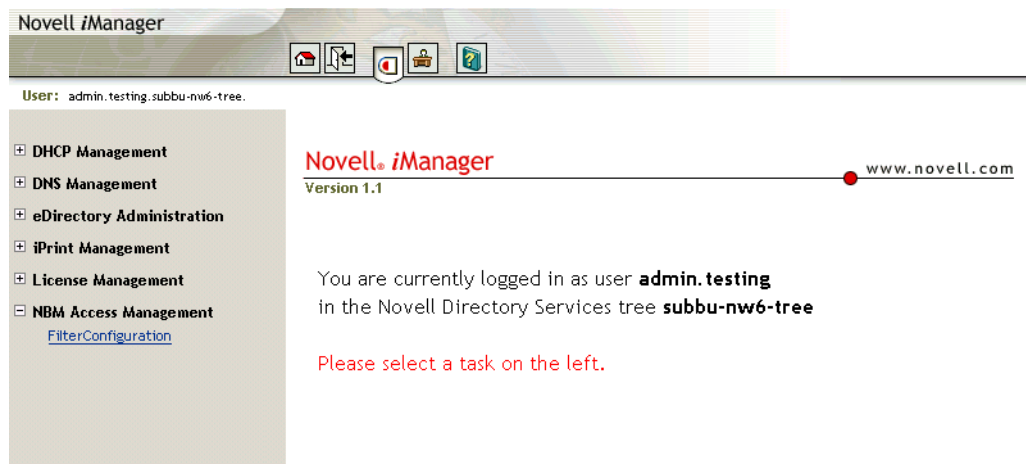
Tree:
subbu-nw6-tree

Login

© Copyright 1999-2002 Novell, Inc. All rights reserved.

When you log in to the Novell iManager, you can see the NBM Access Management role in the left pane.

Click NBM Access Management to see the Filter Configuration task.

Figure 7 Novell BorderManager Access Management Pane


Novell iManager

User: admin.testing.subbu-nw6-tree.

DHCP Management
 DNS Management
 eDirectory Administration
 iPrint Management
 License Management
 NBM Access Management
 [FilterConfiguration](#)

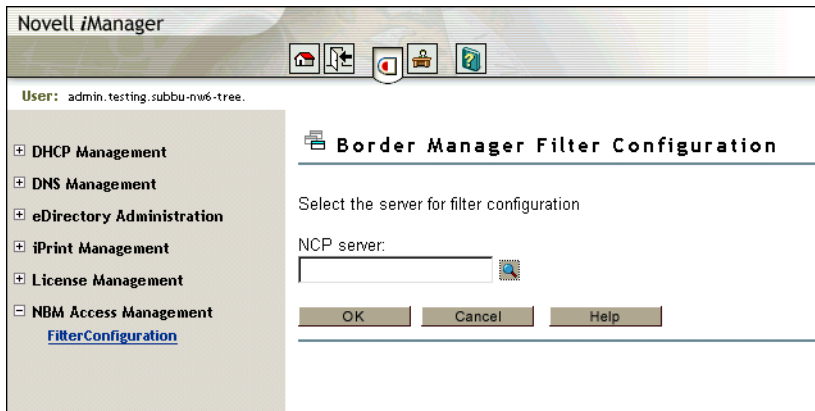
Novell iManager
Version 1.1 www.novell.com

You are currently logged in as user **admin.testing**
in the Novell Directory Services tree **subbu-nw6-tree**

Please select a task on the left.

Click the Filter Configuration task to see the Novell BorderManager Server Selection option.

Figure 8 Server Selection Option Page



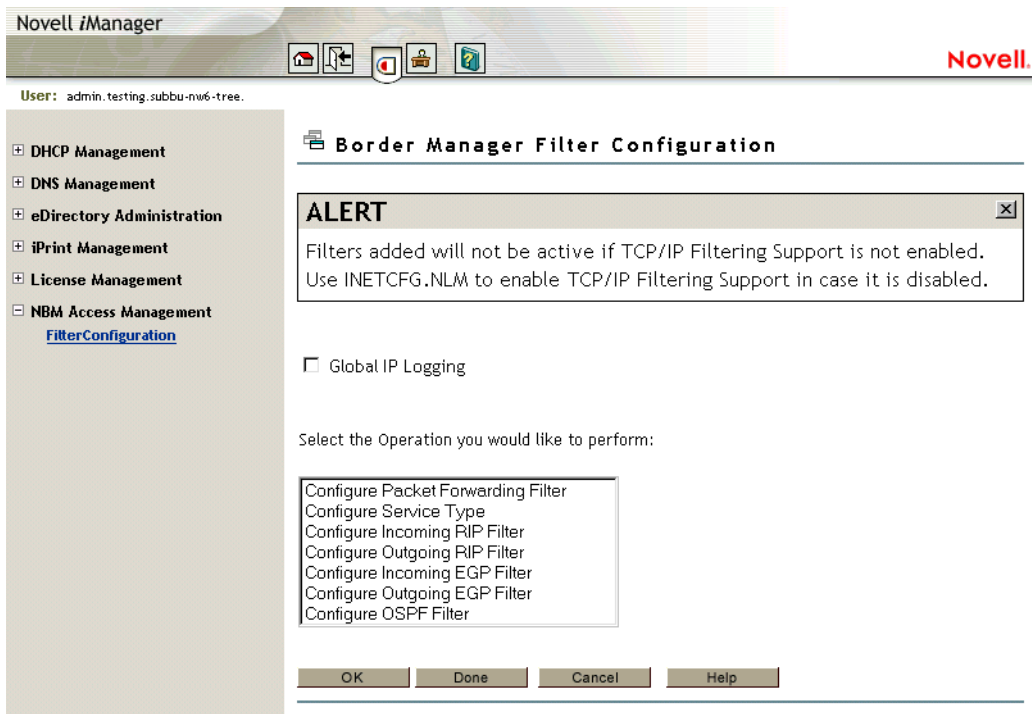
Click the object selector icon to find the server you want to select.

Click the server icon.

The selected server is shown on the main page.

Click OK.

Figure 9 Task List Box



Select the task you want to perform from the list.

Click OK.

Using FILTCFG for Filter Configuration

These sections tell you how to use FILTCFG on a Novell BorderManager 3.8 server:

- ◆ “Setting Up Outbound Packet Filter Exceptions” on page 113
- ◆ “Setting Up Inbound Packet Filter Exceptions” on page 117
- ◆ “Defining Custom Stateful Packet Types” on page 117
- ◆ “Saving Filters to a Text File” on page 118
- ◆ “Enabling Global IP Packet Logging” on page 118
- ◆ “Completing Advanced Setup, Configuration, and Management Tasks” on page 119

Setting Up Outbound Packet Filter Exceptions

Because the default filters don't automatically allow certain packet types to cross the firewall, you might also need to enable filter exceptions to enable other services.

The system-defined packet types enable you to configure stateful packet filter exceptions for the following services:

- ◆ DNS over UDP
- ◆ DNS over TCP
- ◆ FTP
- ◆ Ping
- ◆ POP3
- ◆ Simple Mail Transfer Protocol (SMTP)
- ◆ Telnet
- ◆ HTTP
- ◆ HTTPS

With stateful (dynamic) packet filtering, you only need to define the exceptions that allow specific types of outbound traffic going to specific destinations to be forwarded by the Novell BorderManager 3.8 server. Stateful packet filtering monitors each connection and creates a temporary (time-limited) filter exception for the inbound connection. This allows you to block incoming traffic originating from a particular port number and address, while still allowing return traffic from that same port number and address.

Stateful packet filters track the outgoing packets allowed to pass and allows only the corresponding response packets to return. When the first packet is transmitted to the public network (Internet), a reverse filter is dynamically created. To be counted as a response, the incoming packet must be from the same host and port to which the outbound packet was originally sent.

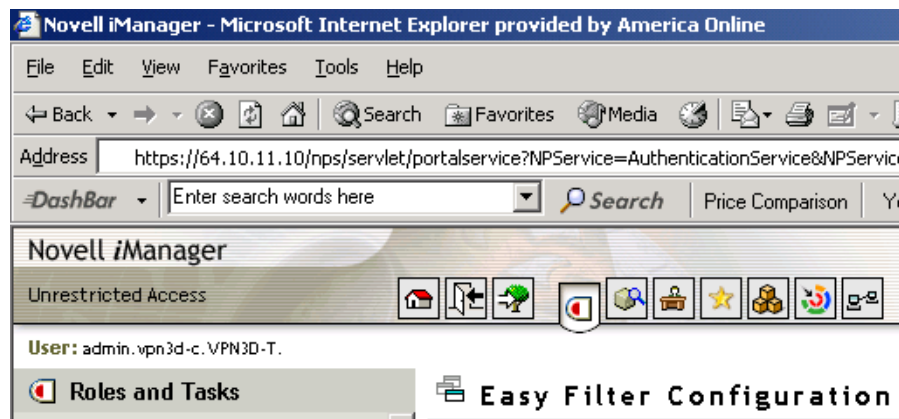
To configure stateful packet forwarding exceptions to forward outbound traffic through the Novell BorderManager 3.8 server:

- 1 At the server console prompt, enter

```
LOAD FILTCFG
```

- 2** From the Filter Configuration Available Options menu, select Configure Interface Options, then press Enter.
- 3** Select an interface from the list, then press Tab to switch between Public and Private.
Any interface listed can be designated as either a public (external) interface or a private (internal) interface.
- 4** Press Esc, then select Configure TCP/IP Filters, then Packet Forwarding Filters.
The screen displayed should appear similar to the following.

Figure 10 Packet Forwarding Filters Screen



- 5** Complete the following steps:
 - ◆ If the status is Disabled, press Enter, select Enabled, then press Enter again. Any TCP/IP filters previously configured become active immediately.
 - ◆ If the action is Permit Packets in Filter List, press Enter, select Deny Packets in Filter List, then press Enter again. Packets matching the types listed in the filter list will not be forwarded by the Novell BorderManager 3.8 server.
- 6** Select Filters, then press Enter to display the filter list.
A default filter set up during installation blocks all inbound IP packets coming from the public interface.
- 7** Press Esc.
- 8** Select Exceptions, then press Enter to display the exceptions list.
A default filter exception that is set up during installation allows all outbound IP packets to be routed through the public interface.
Other filter exceptions permit the following inbound packet types through the public interface:
 - ◆ Secure Sockets Layer (SSL) authentication: TCP port 443.
 - ◆ Dynamic TCP: TCP ports 1024 to 65535.
 - ◆ Dynamic UDP: UDP ports 1024 to 65535.
 - ◆ VPN master or slave (IPX/TCP): TCP port 213.
 - ◆ VPN client authentication: TCP port 353.

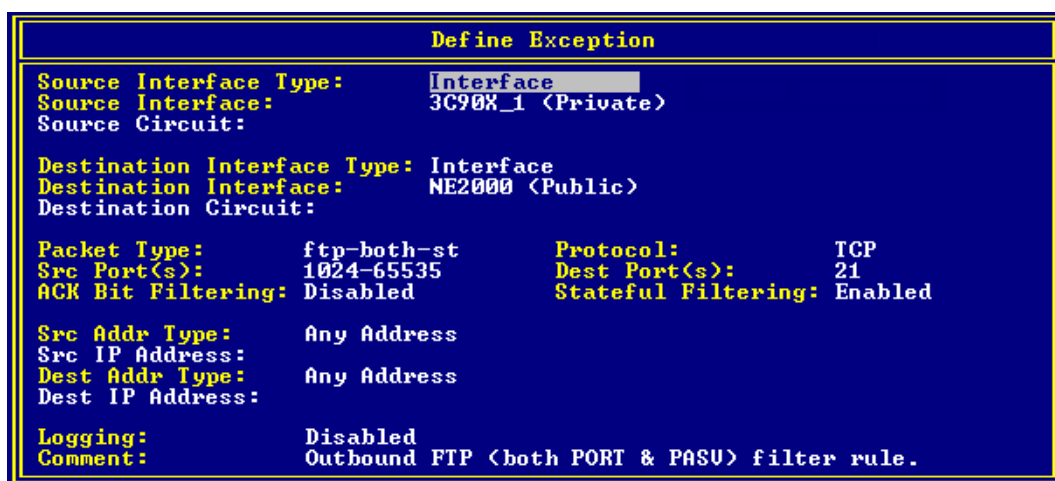
- ◆ VPN keep-alive: UDP port 353.
- ◆ VPN Simple Key Management for Internet Protocol (SKIP) Protocol 57.
- ◆ Web proxy cache (WWW-HTTP): TCP port 80.

Although the default filter exceptions allow certain VPN-related packets to be forwarded, the default VPN exceptions do not allow encrypted packets to be routed from one VPN member to another. The filters for the VPN tunnels must be updated each time you configure a VPN server. For more information, refer to [“Completing Advanced Setup, Configuration, and Management Tasks”](#) on page 119, and VPN Overview and Planning.

- 9 Press **Ins** to define a new outbound packet forwarding filter exception.

The Define Exception screen is displayed, similar to the following screen:

Figure 11 Define Exception Screen



- 10 Select Source Interface, Type, then press **Enter**.
- 11 Select Interface or Interface Group, then press **Enter**.
- 12 Select Source Interface, then press **Enter**.
- 13 Select the Novell BorderManager 3.8 server's private interface or interface group, then press **Enter**.
- 14 If you selected a WAN interface, select Source Circuit, then press **Enter** to define the following circuit information that applies to the interface:
 - ◆ Local Frame Relay DLCI # (for frame relay): The data-link connection identifier (DLCI) circuit number used for calls.
 - ◆ Remote System ID (for PPP, X.25, or ATM): The name of the remote system server or remote peer associated with this circuit.
 - ◆ Circuit Parameter Type (for X.25 or ATM): The type of virtual circuit used to establish a connection.
 - ◆ Remote DTE Address (for X.25): The X.121 data terminal equipment (DTE) address assigned to the specific remote DTE.

- ♦ Remote ATM Address (for ATM): The address assigned to the specific remote Asynchronous Transfer Mode (ATM).
- 15** Select Destination Interface Type, then press Enter.
 - 16** Select Interface or Interface Group, then press Enter.
 - 17** Select Destination Interface, then press Enter.
 - 18** Select the Novell BorderManager 3.8 server's public interface or interface group, then press Enter.
 - 19** If you selected a WAN interface, select Destination Circuit, then press Enter to define the following circuit information that applies to the interface:
 - ♦ Local Frame Relay DLCI # (for frame relay): The DLCI circuit number used for calls.
 - ♦ Remote System ID (for PPP, X.25, or ATM): The name of the remote system server or remote peer associated with this circuit.
 - ♦ Circuit Parameter Type (for X.25 or ATM): The type of virtual circuit used to establish a connection.
 - ♦ Remote DTE Address (for X.25): The X.121 DTE address assigned to the specific remote DTE.
 - ♦ Remote ATM Address (for ATM): The address assigned to the specific remote ATM.
 - 20** Select Packet Type, then press Enter.

The Defined TCP/IP Packet Types window is displayed.

You can select any of the following predefined stateful packet forwarding filters:

Name	Packet Type	Transport Type	Destination Port	Stateful Filtering
dns/tcp-st	DNS	TCP	53	Enabled
dns/udp-st	DNS	UDP	53	Enabled
ftp-pasv-st	FTP	TCP	21	FTP_PASV
ftp-port-st	FTP	TCP	21	FTP_PORT
ftp-port-pasv-st	FTP	TCP	21	Enabled
ping-st	PING	ICMP	N/A	Enabled
pop3-st	POP3 Mail	TCP	110	Disabled
smtp-st	SMTP	TCP	25	Enabled
telnet-st	Telnet	TCP	23	Enabled
www-http-st	HTTP	TCP	80	Enabled
www-https-st	HTTPS	TCP	443	Enabled

- 21** For Src Addr Type, select Any Address, Host, or Network.

You should select Any Address unless you want the exception to be valid only for a specific host or network on your private network.

- 22** If you selected Host or Network, select Src IP Address, then specify the host or network address.
 - 23** For Dest Addr Type, select Any Address, Host, or Network.
You should select Any Address unless you want the exception to be valid only for packets addressed to a specific host or network outside the private network.
 - 24** If you selected Host or Network, select Dest IP Address, then specify the host or network address.
 - 25** (Optional) For Logging, then press Enter and change the status from Disabled to Enabled.
 - 26** (Optional) Specify a comment in the Comment field describing the purpose of the filter. Press Esc, then select Yes to save the filter. Press Esc until you are prompted to exit FILTCFG.
- IMPORTANT:** If you enabled logging for a filter exception, you must also enable global logging for TCP/IP. Both global logging and logging for the specific filter exception must be enabled for logging to occur.

Setting Up Inbound Packet Filter Exceptions

If you elected to secure the public interface Novell BorderManager 3.8 server and support SOCKS clients, you might be required to enable inbound packet filter exceptions to allow them to connect through the public interface. SOCKS clients connect through TCP port 1080.

To configure packet forwarding exceptions to forward SOCKS traffic, go through the following Novell BorderManager 3.8 server's public interface:

- 1** At the server console prompt, enter
LOAD FILTCFG
- 2** Select Configure TCP/IP Filters and Packet Forwarding Filters.
- 3** Select Exceptions, then press Enter to display the exceptions list.
- 4** Press Ins to define a new inbound packet forwarding filter exception.
- 5** Configure the exception for SOCKS clients.
- 6** Press Esc until you are prompted to exit FILTCFG.

Defining Custom Stateful Packet Types

The Novell BorderManager 3.8 firewall has many static packet types defined in addition to the stateful packet types listed in [“Setting Up Outbound Packet Filter Exceptions” on page 113](#).

Static packet types are those without -st in their names. A static packet type is used to define a filter operating on traffic in one direction only. For example, instead of creating a stateful packet filter in one direction and relying on the system to enable the time-limited filter in the reverse direction, you can create two static packet filters, one for packets flowing in each direction. However, stateful packet filters provide more security than static packet filters.

If the stateful packet types already defined by the Novell BorderManager 3.8 server do not include a packet type you want to filter, and you are hesitant to use static packet filters, you can create a custom stateful packet type.

To define a custom stateful packet type:

- 1** In the Defined TCP/IP Packet Types window, press Insert.
- 2** Specify the name of the new packet type in the Name field.

- 3** For the Protocol field, press Insert and select IP, ICMP, IGMP, TCP, or UDP.
- 4** If you selected TCP or UDP, specify the source and destination port number or range of port numbers.
- 5** Do not change the default setting of Disable for ACK Bit Filtering.

You don't need to enable ACK bit filtering separately, because ACK bit filtering automatically occurs when stateful packet filtering is enabled. The software does not allow you to enable both ACK bit filtering and stateful packet filtering for the same filter.

- 6** Enable stateful filtering by selecting one of the following stateful filtering modes:
 - ◆ Enabled
 - ◆ Enabled for Active FTP only (PORT)
 - ◆ Enabled for Passive FTP only (PASV)

NOTE: The last two stateful filtering modes apply only to FTP packet types (port 21). If you want stateful filtering for both Active FTP and Passive FTP, select Enabled.

- 7** (Optional) Specify a comment to describe the packet type.

The TCP/IP packet type definition will look similar to the following.

Figure 12 Define TCP/IP Packet Type

```

Define TCP/IP Packet Type
Name:          stateful-email
Protocol:      TCP
Source Port(s): 1024-65535
Destination Port(s): 25
ACK Bit Filtering: Disabled
Stateful Filtering: Enabled
Comment:       User-defined filter for e-mail (SMTP) service.
  
```

- 8** Press Esc to add the packet to the Defined TCP/IP Packet Types list.

After the packet type has been added to the list, you can set up a stateful packet filter using this packet type definition.

Saving Filters to a Text File

To document the filters and exceptions you enabled for your server:

- 1** At the server console prompt, enter
LOAD FILTCFG
- 2** Select Save Filters to a Text File.
- 3** Specify the filename to which the filters will be saved.
- 4** Press Esc to exit FILTCFG.

Enabling Global IP Packet Logging

The Global Logging flag allows you to turn logging on and off for all filters within a specific protocol, such as TCP/IP. If this flag is not enabled, no logging will occur, even if the log flag has been enabled for a specific filter or exception.

Packet logging records the activity of the individual filters specified in the filter lists or the exception lists.

NOTE: Logging options can slow server performance. Consider disabling logging after you have tested your filters and exceptions.

To enable global IP logging:

- 1 At the server console prompt, enter

LOAD FILTCFG

- 2 Select Filter Configuration Available Options > Configure TCP/IP Filters > Global IP Logging and Status.

- 3 Select Enabled, then press Enter.

NOTE: When Global IP Logging is enabled, logging activity will start. If you want to log the activity of a particular filter, you must enable both Global IP Logging and the packet logging option for that filter.

- 4 Press Esc until you are prompted to exit FILTCFG.

Completing Advanced Setup, Configuration, and Management Tasks

In addition to the basic setup procedures described in this section, there are several advanced setup, configuration, or management procedures you might need to complete, depending on your specific configuration. Advanced tasks include the following sections:

- ♦ Setting up an HTTP filter
- ♦ Setting up an FTP filter
- ♦ Setting up a Telnet filter
- ♦ Setting up an SMTP filter
- ♦ Setting up a POP3 filter
- ♦ Modifying default IP packet logging parameters
- ♦ Viewing IP packet log information

11

Managing IP Packet Filters

The following sections describe how to manage Novell® BorderManager® 3.8 IP packet filters used as part of your firewall. Refer to [Table 1, “ippktlog.cfg Configuration Parameters,” on page 121](#) for the logging configuration parameters in ippktlog.cfg.

- ♦ [“Modifying Default IP Logging Parameters” on page 121](#)
- ♦ [“Viewing IP Packet Log Information” on page 122](#)

Modifying Default IP Logging Parameters

If global logging for IP has been enabled, IP packets are automatically logged to a text file located in the sys:\etc\logs\ippktlog directory on the server. The configuration file, sys:\etc\ippktlog.cfg, specifies the logging parameters.

IMPORTANT: IP packets that match a specific packet filtering rule are not logged unless logging has been explicitly enabled for the filter.

For more information on logging configuration parameters in ippktlog.cfg, refer to the following table:

Table 1 ippktlog.cfg Configuration Parameters

Parameter	Default Value	Available Settings
LOG_FILE_TYPE	1	1 = Sequential log file.
LOG_FILE_LOCATION	sys:\etc\logs\ippktlog	Any directory.
LOG_FILE_ROLL_METHOD	3	1 = Roll log file every <i>n</i> hours, where <i>n</i> is the value assigned to LOG_FILE_ROLL_METHOD_VALUE. 2 = Roll log file every <i>n</i> days, where <i>n</i> is the value assigned to LOG_FILE_ROLL_METHOD_VALUE. 3 = Roll log file when the log file size exceeds <i>n</i> KB, where <i>n</i> is the value assigned to LOG_FILE_ROLL_METHOD_VALUE.
LOG_FILE_ROLL_METHOD_VALUE	100	Any value representing hours when LOG_FILE_ROLL_METHOD is 1. Any value representing days when LOG_FILE_ROLL_METHOD is 2. Any value representing KB when LOG_FILE_ROLL_METHOD is 3.

Parameter	Default Value	Available Settings
LOG_FILE_DELETE_METHOD	2	1 = Do not delete log files. 2 = Begin deleting log files when the number of log files reaches the limit specified by LOG_FILE_DELETE_METHOD_VALUE. 3 = Begin deleting log files when the age of the log files reaches <i>n</i> hours, where <i>n</i> is the value assigned to LOG_FILE_DELETE_METHOD_VALUE.
LOG_FILE_DELETE_METHOD_VALUE	512	Any value representing the number of files when LOG_FILE_DELETE_METHOD is 2. Any value representing the number of hours when LOG_FILE_DELETE_METHOD is assigned a value of 3. The value assigned should be greater than LOG_FILE_ROLL_METHOD_VALUE if LOG_FILE_ROLL_METHOD is assigned a value of 1.
LOG_CACHE_BUFFER_SIZE	80	Any value representing the size in KB. The value assigned should not exceed the available memory on the server.
DATE_TIME_FORMAT	2	1 = Do not insert a date and time stamp for each entry to the log file. 2 = Insert a date and time stamp for each entry to the log file. The date and time have the format of MM/DD/YYYY, HH:MM:SS +/- TimeZoneOffset, where MM is the month, DD is the day, and YYYY is the year.

If global logging for IP has been enabled, the Novell BorderManager 3.8 server is also configured by default to shut down the public interface when logging fails to occur. A logging failure can occur when the server experiences a shortage of disk space. If you want to disable the automatic shutdown of the public interface when logging fails, at the server console enter

```
SET SHUTDOWN PUBLIC INTERFACE ON LOG FAILURE = OFF
```

To re-enable the automatic shutdown of the public interface, enter

```
SET SHUTDOWN PUBLIC INTERFACE ON LOG FAILURE = ON
```

Viewing IP Packet Log Information

The IP packet filter logs stored in the `sys:\etc\logs\ippktlog` directory can be viewed with any text editor. The data in the log file can be imported by most third-party applications for analysis, because the log file conforms to the Microsoft standard format.

Each entry in the log file contains the following fields:

- ◆ Date
- ◆ Time
- ◆ Source IP Address
- ◆ Destination IP Address

- ◆ Protocol
- ◆ Source Port
- ◆ Destination Port
- ◆ TCP Flags
- ◆ Access: 1 indicates accept; 0 indicates deny
- ◆ IP Header
- ◆ IP Payload

NOTE: A dash (-) appearing in any of the fields indicates that the information was unavailable or did not apply to the type of packet that was logged.

12 Packet Filtering Using Novell iManager

Novell® BorderManager® 3.8 comes with a Packet Filtering Configuration Task based on Novell iManager for configuring TCP/IP filters. The Novell BorderManager Access Management Role and Packet Filtering Configuration Task is automatically plugged into Novell iManager during Novell BorderManager 3.8 installation.

For more details regarding filter configuration see [AppNotes on Filter Configuration \(http://developer.novell.com/research/appnotes/2002/june/04/a020604.htm\)](http://developer.novell.com/research/appnotes/2002/june/04/a020604.htm).

Make sure that Novell iManager is up and working on the NetWare® or Windows machine. For more information refer to [“Installing iManager 2.0.1 Snap-Ins” on page 24](#).

To log in to Novell iManager:

- 1** In Internet Explorer go to `https://<ipaddress>/nps/iManager.html` or use `https://<DNS>/nps/iManager.html`
- 2** Log in to Novell iManager to use the Packet Filtering Configuration Task.
- 3** When you log in to Novell iManager, you can see the role of NBM Access Management on the left pane. Click NBM Access Management to see the Filter Configuration task.
- 4** Click the Filter Configuration task to see the NBM Server Selection option.
- 5** Select the Novell BorderManager 3.8 server.

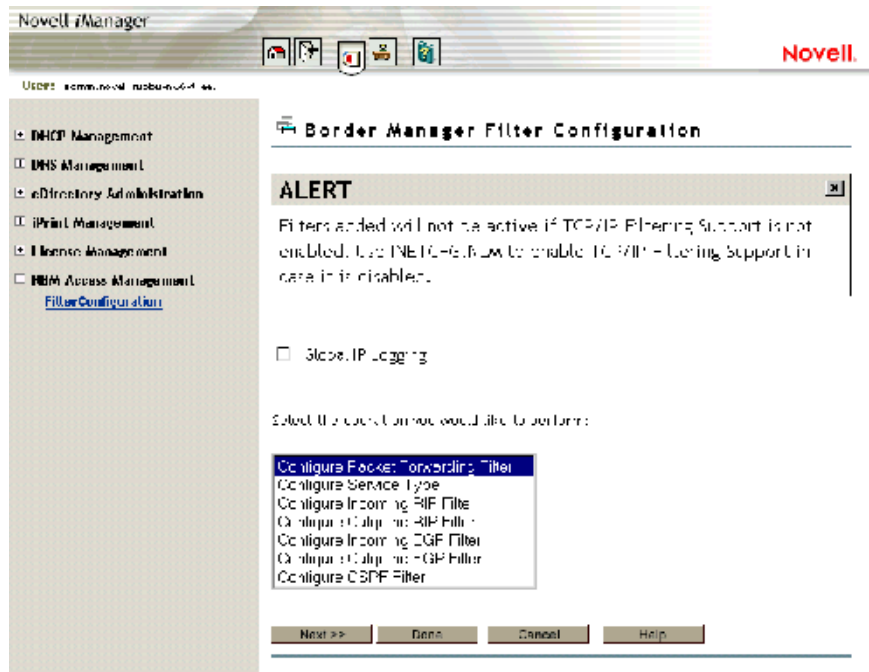
To set up the Packet Filtering Configuration Task, refer to [Chapter 12, “Packet Filtering Using Novell iManager,” on page 125](#).

To ensure that the configured filters are active, check to see that you have enabled filter support using INETCFG.

After you have reached the filter configuration task, the following seven types of configuration can be seen:

- ◆ Configure Packet Forwarding Filter
- ◆ Configure Service Type
- ◆ Configure Incoming RIP Filter
- ◆ Configure Outgoing RIP Filter
- ◆ Configure Incoming EGP Filter
- ◆ Configure Outgoing EGP Filter
- ◆ Configure OSPF Filter

Figure 13 Configuration Menu



The global logging status for all filter types can be enabled or disabled from the configuration menu.

Select any one of the following for configuration:

- ◆ **Configuring Packet Forwarding Filter:** TCP/IP Packet Forwarding Filters allow the router to selectively filter packets based on their packet type, source, and destination.
- ◆ **Configuring Service Type:** Service Type includes the System and User defined packet types used for configuring Packet Forwarding filters.
- ◆ **Routing Information Protocol (RIP) Filter:** RIP filters are used to control the propagation of routing information by this router. They provide a low level of security by hiding the existence of specific IP networks from other routers. There are two types of routing filters, incoming and outgoing.
 - Incoming RIP filters restrict the acceptance of routing information from the adjacent routers.
 - Outgoing RIP filters restrict the routing information advertised by the router to its adjacent routers.
- ◆ **EGP Filter:** The routes that the router can share with the EGP peers are defined with EGP filters. There are two types of EGP filters: Incoming and Outgoing.
 - Incoming EGP filters restrict what routes can be accepted from an EGP peer.
 - Outgoing EGP filters restrict what routes learned from RIP, OSPF, or static routes can be propagated to EGP peers.
- ◆ **Configuring OSPF Filter:** The router can use OSPF to exchange routing information within its Autonomous System. OSPF External Route Filters define the route and the source of the source of the route that will be propagated into the OSPF domain.

Select an operation from the list and click Next to continue.

Click Done if you want to save changes to IP logging and exit Filter Configuration.

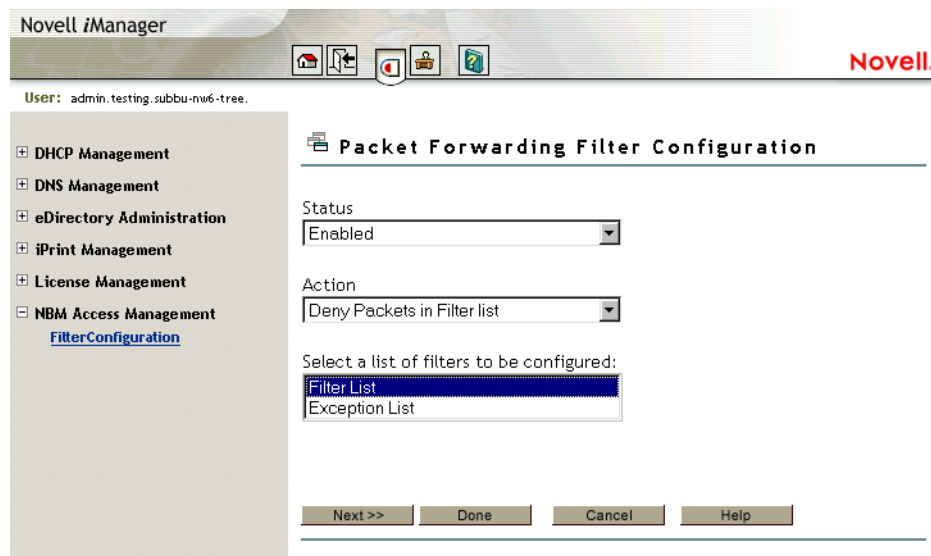
Click Cancel to exit Filter Configuration.

The next three sections contain information about configuring filter types:

- ◆ “Configuring the Packet Forwarding Filter” on page 127
- ◆ “Configuring the Service Type” on page 132
- ◆ “Configuring an Incoming RIP Filter” on page 134

Configuring the Packet Forwarding Filter

Figure 14 Packet Forwarding Filter Configuration



This page helps you to set the properties of the selected filter type:

Status: Choose between Disabling or Enabling the selected filters. If Filtering Support has been enabled in inetcfg.nlm for this protocol, altering the status will cause configured filters to immediately become active (Enabled) or inactive (Disabled).

Action: Choose between Denying and Permitting packets on the filter list. Specify the action taken when a packet matches a filter in the Filter List. If the filters in the Exception List overlap with the filters in the Filters List, the Exception List is used.

Select the list of Filters to be Configured: Select the list of filters to be configured; choose between the Filter List or the Exception List.

Filter List: Displays all configured filters. You can add new filters, or delete or modify existing filters. The data packets that match any filter are either permitted or denied depending on the setting of the Action parameter. Data packets that match any filter in the Exceptions List are not filtered, even if they match a filter in the Filters List.

Exception List: Displays the exceptions to the filters defined in the Filters List, and allows you to specify additional exceptions. Exception filters take priority over filters in the Filter List. If a packet does not match an exception filter, it is checked against the Filters List. The packet is filtered if it matches any filter.

- 1 From the BorderManager Filter Configuration page in iManager, select Configure Packet Forwarding Filter from the list of tasks
- 2 Select Filter List or Exception List and click Next to configure filters in that list.
- 3 Select or change properties for the filters, then click Done to save changes to the status or action of this filter type and return to the filter configuration menu.
- 4 Click Cancel to discard changes to the status or action and return to the filter configuration menu.

Figure 15 Packet Forwarding Filter Configuration - Packets Denied

Novell iManager

User: admin.testing.subbu-nw6-tree.

Packet Forwarding Filter Configuration

Packets Denied

Select	Source	Circuit	Packet Type	Destination	Circuit
<input type="checkbox"/>	CE100B	-	Any	All Interfaces	-
<input type="checkbox"/>	All Interfaces	-	Any	CE100B	-
<input type="checkbox"/>	CE100B	-	IP	All Interfaces	-
<input type="checkbox"/>	All Interfaces	-	IP	CE100B	-
<input type="checkbox"/>	All Interfaces	-	ftp	All Interfaces	-
<input type="checkbox"/>	CE100B	-	IP	All Interfaces	-
<input type="checkbox"/>	All Interfaces	-	IP	CE100B	-

<< Previous Add Modify Delete Done Cancel Help

This page gives you a summary of packet forwarding filters.

You can add new filters, or delete or modify existing filters. The data packets that match any filter are either permitted or denied depending on the setting of the Action parameter. Data packets that match any filter in the Exceptions List are not filtered, even if they match a filter in the Filters List.

Click Done to return to the beginning of Packet Forwarding Filter configuration.

Click Cancel to return to the filter configuration menu.

Figure 16 Packet Forwarding Filter Configuration - Add or Modify

This page helps you to add or modify your filter properties.

Name: Gives you the name of the packet filter. This is the name of the filter object that would be created in Novell eDirectory.

Service Type: Defines the service type to be filtered. Click the button to view a list of defined TCP/IP service types. You can select an entry for the filter being edited. If you want to add or modify or delete user-defined service types, go to the Configure Service Type option on the configuration menu. See [Figure 13, "Configuration Menu,"](#) on page 126.

Comment: Specify a short comment in this field, to save in the database along with the other entries in the form.

Logging: Choose to enable or disable this option.

- ◆ Enable: The header of the packet that matches the options in the filters or exceptions are logged as long as the global logging status and the filters/exception logging status are enabled. The Log file is a Btrieve database file (csaudit.log) located at sys:\etc\logs\ippktlog directory.
- ◆ Disable: Packets that match the options in filters or exceptions are not logged. Data logging slows down the server's performance and you should turn it on for a short time only. The local logging status can be enabled or disabled from the filter/exception definition menu.

Specify a name in the Name dialog box, then click Next.

If you have modified the settings, click Done to save changes to the filter and return to the Packet Forwarding Filter Summary.

Click Cancel to discard any changes to the filter and return to the Packet Forwarding Filter Summary.

Figure 17 Packet Forwarding Filter Configuration - Type of Information

The screenshot shows the Novell iManager web interface in Microsoft Internet Explorer. The browser address bar shows the URL: `https://164.99.158.58:2200/eMFrame/webacc?taskId=dev.Empty&merge=fw.Main&User.context=rlukMlnskdAm`. The page title is "Novell iManager" and the user is logged in as "admin.pxy1b.PXYT1B".

The main content area is titled "Packet Forwarding Filter Configuration". It contains the following configuration fields:

- Source Interface Type:** A dropdown menu with "Interface" selected.
- Source Interface:** A dropdown menu with "CE100B_1" selected.
- Source Circuit:** A text input field containing "-NA-".
- Source Address Type:** A dropdown menu with "Host" selected.
- Source IP Address:** Four input fields containing "164", "99", "158", and "58" respectively.
- Source Subnet Mask:** Four empty input fields.

At the bottom of the configuration area, there are four buttons: "Previous", "Next >>", "Cancel", and "Help".

The Windows taskbar at the bottom shows the Start button, several open applications (Novell GroupWise - Mailbox, Adobe Photoshop), and the system tray with the time "10:22 AM".

This page helps you to alter the source information for the filter.

Source Interface Type: Select the source interface type of the TCP/IP packet forwarding filter. The available source types are Interface and Interface Group.

Source Interface: Select a source interface.

Source Circuit: Specify the information about the circuit to be configured. The source circuit is valid only if the source interface is of WAN media type. The default source circuit value is All Circuits.

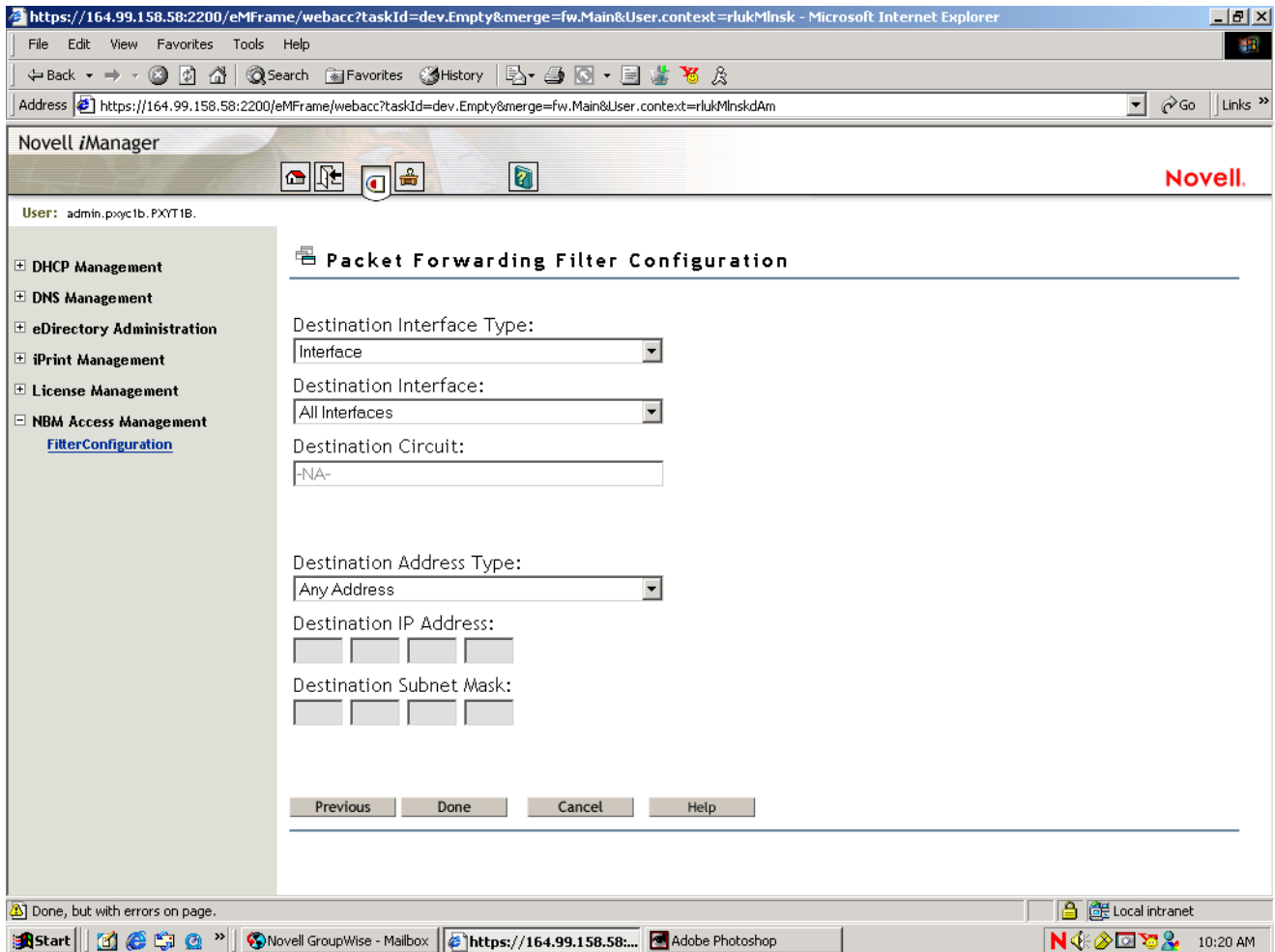
Source Address Type: Select the Source Address Type of the TCP/IP packet forwarding filter. The available source types are Network, Host, or Any Address.

Source IP Address: Gives the IP address of your network or host.

Source Subnet Mask: Gives the subnetwork mask of your network.

Click Next.

Figure 18 Packet Forwarding Filter Configuration - Information



This page helps you to alter the destination information for the filter.

Destination Interface Type: Select the destination interface type of the TCP/IP packet forwarding filter. The available source types are Interface and Interface Group.

Destination Interface: Select the destination interface.

Destination Circuit: Specify the information about the circuit to be configured. The destination circuit is valid only if the destination interface is of WAN media type. The default destination circuit value is All Circuits.

Destination Address Type: Select the Destination Address Type of the TCP/IP packet forwarding filter. The available types are Network, Host, Multicast, or Any Address.

Destination IP Address: Gives the Network, Host or Multicast address.

Destination Subnetwork Mask: Gives the subnetwork mask of your network.

Click Done.

Configuring the Service Type

Figure 19 Service Type Configuration

The screenshot displays the 'Service Type Configuration' page in a web browser. The page title is 'Service Type Configuration' and it shows a list of 'Defined TCP/IP Service Types'. The list has columns for 'Select', 'Name', 'Protocol', 'Src Port(s)', 'Dst Port(s)', and 'Comment'. There are 'Add', 'Modify', and 'Delete' buttons above the table. The status bar at the bottom indicates 'Done, but with errors on page.' and 'Local intranet'.

Select	Name	Protocol	Src Port(s)	Dst Port(s)	Comment
<input type="checkbox"/>	Any	IP	-	-	All TCP/IP Services
<input type="checkbox"/>	Accel-Auth	TCP	All	443	Accelerator Authentication
<input type="checkbox"/>	aurp	UDP	All	387	AppleTalk AURP
<input type="checkbox"/>	bootpc	UDP	All	68	Bootstrap Protocol Client
<input type="checkbox"/>	bootps	UDP	All	67	Bootstrap Protocol Server
<input type="checkbox"/>	bordergw	UDP	All	179	Border Gateway Protocol
<input type="checkbox"/>	chargin	TCP	All	19	Character Generator
<input type="checkbox"/>	chargin/udp	UDP	All	19	Character Generator over UDP
<input type="checkbox"/>	cmd	TCP	All	514	Remote Command Execution
<input type="checkbox"/>	csaudit	TCP	All	2000	Novell CSAudit logging Protocol
<input type="checkbox"/>	discard	TCP	All	9	
<input type="checkbox"/>	discard/udp	UDP	All	9	Discard Over UDP
<input type="checkbox"/>	dns/tcp-st	TCP	All	53	Stateful DNS Over TCP
<input type="checkbox"/>	dns/udp	UDP	53	53	Domain Name Server
<input type="checkbox"/>	dns/udp-st	UDP	All	53	Stateful DNS Over UDP
<input type="checkbox"/>	domain	UDP	All	53	Domain Name Server
<input type="checkbox"/>	domain/tcp	TCP	All	53	Domain Name Server Over TCP

This page gives you a summary of defined TCP/IP service types.

You can add new service types, or delete or modify only User Service types.

Figure 20 Service Type Configuration - TCP/IP

Novell iManager

User: admin.testing.subbu-nw6-tree.

Service Type Configuration

Add New Service Type:

Name:

Protocol:

Select from list

Specify protocol id

Source Port:

Destination Port:

ACK Bit Filtering:

Disabled
 Enabled

Stateful Filtering:

Comment:

This page helps you to configure the TCP/IP service types.

Name: Name of the TCP/IP service type.

Protocol: Either select from a list of commonly used internet protocols or specify a valid protocol ID between 0 - 255.

Source and Destination Port: Define a single TCP/IP port or range of ports separated by a hyphen for the TCP or UDP protocols. Valid port numbers range from 1 to 65535. If not defined, the default value for this field is All.

ACK Bit Filtering: This field is enabled only if the protocol selected is TCP. If the TCP ACK Bit filtering is enabled in a filter route, only the packets with the ACK Bit set are allowed through. This will effectively block all the connections being initiated, in the direction defined by the filter rule. TCP ACK Bit filtering is often applied to all inbound TCP packets in a network.

Stateful Filtering: If stateful filtering is enabled in a filter rule, a dynamic filter is also created in the reverse of the direction that is defined by the filter rule. The reverse filter is created with the information such as source IP address, source interface, source port, destination IP address, destination interface, and destination port. This information is stored in a table that will later be used to compare against the reply. If it is not a reply to the original request packet, stateful filtering will not allow the packet through.

Stateful filtering supports both connection and connectionless protocols. For ICMP packets, only the reply ICMP messages are allowed. ICMP redirect messages will not be allowed. Stateful filtering is slower than the current static filtering but it is more secure. It does not open up all the

ports as static filters do; instead, dynamic filters are created with more specific information on the IP address, source, and destination ports.

Comment: Specify a short comment in this field to save in the database along with the other entries in the form.

- 1 On the Service Type Configuration page in iManager, click Any.
- 2 Make the configuration changes you want.
- 3 Click OK.

Configuring an Incoming RIP Filter

The following sections contain an overview of the Incoming RIP Filter Configuration pages. Use the same information for other configurations, such as the following:

- ◆ Configuring an outgoing RIP filter
- ◆ Configure an incoming EGP filter
- ◆ Configuring an outgoing EGP filter
- ◆ Configuring an OSPF filter

Figure 21 Incoming RIP Configuration

This page helps you to set the properties of the selected filter type.

Status: Choose between disabling or enabling the selected filters. If Filtering Support has been enabled in inetcfg.nlm for this protocol, altering the status causes configured filters to immediately become active (Enabled) or inactive (Disabled).

Action: Choose between Denying and Permitting packets on the filter list. Specify the action taken when a packet matches a filter in the Filter List. If the filters in the Exception List overlap with the filters in the Filters List, the Exception List is used.

Select the List of Filters to Be Configured: Select the list of filters to be configured. Choose between the Filter List or the Exception List.

Filter List: Displays all configured filters. You can add new filters, or delete or modify existing filters. The data packets that match any filter are either permitted or denied depending on the setting of the Action parameter. Data packets that match any filter in the Exceptions List are not filtered, even if they match a filter in the Filters List.

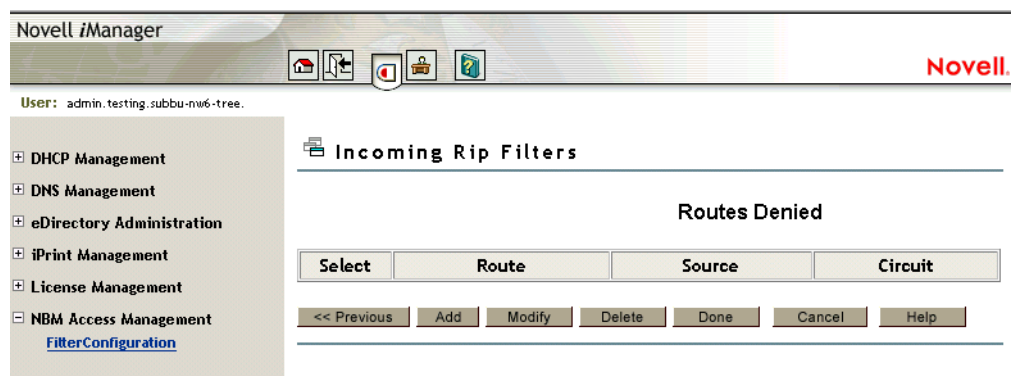
Exception List: Displays the exceptions to the filters defined in the Filters List, and allows you to specify additional exceptions. Exception filters take priority over filters in the Filter List. If a packet does not match an exception filter, it is checked against the Filters List. The packet is filtered if it matches any filter.

Select Filter List or Exception List and click Next to configure filters in that list.

Click Done to save changes to Status and/or Action of this filter type and return to the filter configuration menu.

Click Cancel to discard changes to Status and/or Action and return to the filter configuration menu.

Figure 22 Incoming RIP Configuration - TCP/IP



This page displays the configured TCP/IP incoming (route acceptance) RIP filters.

The filters are in Deny or Permit mode depending on what you have selected in the Action field. If the Action is deny, then the RIP routes that match the criteria of a filter in the Filter List are not accepted by the router. All other RIP routes are not accepted. If the Action is Permit, then the RIP routes that match the criteria of a filter in the Exception List are always accepted by the router, even if another filter in the Filter List is configured to do the opposite.

You can add new filters, or delete or modify the filters in the list. After you save the changes, TCP/IP dynamically updates to the new configuration. The action taken on routes matching filters in this list is described in the Action field. You can select the Route and Source parameters from the list of defined values.

Click Done to return to the beginning of Incoming RIP Filter configuration.

Click Cancel to return to the filter configuration menu.

Figure 23 Incoming RIP Configuration

Novell iManager

User: admin.testing.subbu-nw6-tree.

Incoming RIP Filter Configuration

Incoming RIP Filter Name:

Filtered Route:
 Route to Network or Host:

Do Not Accept Route From:
 Source Type:

Comment:

Logging:

This page helps you to configure an incoming RIP filter.

Incoming RIP Filter Name: Specify the name of the RIP filter. This name becomes the distinguished name of the filter in the eDirectory.

Route to Network or Host: Specify the host, route, or network to be filtered.

Source Type: Specify the source type that the router will accept or block the route to. Select from the list. The available types are Host, Interface, Interface Group, and Network.

Comment: Specify a short comment in this field to save in the database along with the other entries in the form.

Logging: Choose to enable or disable this option.

- ◆ Enabled: the header of the packet that matches the options in the filters or exceptions is logged as long as the global logging status and the filters/exception logging status are enabled. The Log file is a Btrieve database file (csaudit.log) located at sys:\etc\logs\ippktlog directory.
- ◆ Disabled: Any packet that matches the options in filters or exceptions is not logged. Data logging slows down the server's performance and you should turn it on for a short time only. The local logging status can be enabled or disabled from the filter/exception definition menu.

Figure 24 Incoming RIP Configuration - information

Novell iManager

User: admin.testing.subbu-nm6-tree.

Incoming RIP Filter Configuration

Filtered Route:
Route to Network or Host: All Routes

Do Not Accept Route From:
Source Type: Interface
Source Interface: CE100B_1
Source Circuit: -NA-

<< Previous Done Cancel Help

This page helps you to alter the type of information regarding the filter.

Filtered Route

IP Address of Network/Host: Specify a four-byte IP address in dotted decimal notation. For example: 130.57.172.0.

NOTE: When configuring RIP filters for IP networks you should be aware of the fact that depending on the network topology, RIP broadcasts on a particular interface might only advertise the networks even if the network has been divided into several subnetworks. Configuring a filter for a subnetwork of a network, in this case, will not stop information about the network itself from being included in the RIP broadcast. This means that you might need to configure a filter for the network and not the subnetwork to prevent the subnetwork information from being advertised on an interface. You can configure filters for subnetworks to prevent those subnetworks being advertised on other subnetworks of the same network, but be aware that their effectiveness will be influenced by the routing topology.

Subnetwork Mask: Specify a four-byte mask in dotted decimal format. 255.255.255.255 is invalid. The mask must also cover the nature mask.

Address Type of Routing Peer

Source Type: Specifies whether the source is a Host, Interface, Interface Group, or Network.

Source Interface: If your Source Type is Interface or Interface Group, select a source location from the list of network interfaces.

Source Circuit: If the current source is of type Interface or Interface Group and is of WAN Media Type, specify the destination circuit parameters.

Source IP Address: If your Source Type is Network or Host, specify the IP address.

Subnetwork Mask: If your Source Type is Network, specify the subnetwork mask.

13

Backing Up and Restoring Filters

Novell® BorderManager® 3.8 features filtering based on NDS® or Novell eDirectory™. All the stored filters are created under the container NBMRuleContainer. The container NBMRuleContainer is created at the same level as the NCP™ server object of the server where Novell BorderManager 3.8 is installed. To back up or restore IP filters in NDS or eDirectory, you can use any one of the tools that supports the LDAP Import/Export utility.

The following sections discuss how to back up or restore filters using the ConsoleOne® NDS Import or Export utility.

- ♦ “Backing Up eDirectory Filters to LDIF” on page 139
- ♦ “Restoring Filters to eDirectory from LDIF” on page 140
- ♦ “Backing Up eDirectory Filters to Text Files” on page 140
- ♦ “Restoring Filters to eDirectory from Text Files” on page 140

NOTE: Before using this utility, make sure that you have enabled the Allow Clear Text Passwords option of the LDAP Group object. To do so, in ConsoleOne, select the LDAP Group > right-click the LDAP Group > Properties > enable Allow Clear Text Passwords.

Backing Up eDirectory Filters to LDIF

- 1** Create a dummy file anywhere on the server. This is required because the utility does not allow you to create the file online.
- 2** Start ConsoleOne, then authenticate yourself.
- 3** Select Wizards, click NDS, then click Import/Export.
- 4** Select the Export LDIF File (the file you created in Step 1) option button, then click Next.
- 5** Specify the Server DNS name/IP address.
- 6** Specify the Port: 389.
- 7** Select Authenticated Login.
- 8** Specify the User Distinguished Name and password in LDIF format, then click Next. An example of the entries could be cn=admin, o=novell.
- 9** Specify the Distinguished Name of the NBMRuleContainer as the Base Distinguished Name. For example, cn=NBMRuleContainer, O=novell
- 10** Select One Level as the scope, then Click Next.
- 11** Select the Destination LDIF File, click Next, then click Finish.

Restoring Filters to eDirectory from LDIF

- 1 Start ConsoleOne and authenticate yourself.
- 2 Select Wizards, click NDS, then click Import/Export.
- 3 Select Import LDIF File option button then click Next.
- 4 Select Source LDIF File then click Next.
- 5 Specify the Server DNS name/IP address.
- 6 Specify the Port: 389.
- 7 Select Authenticated Login.
- 8 Specify the User Distinguished Name and password in LDIF format, click Next, then click Finish. For example, one of the entries could be `cn=admin, o=novell`.

Backing Up eDirectory Filters to Text Files

- 1 Ensure that `filtsrv.nlm` is loaded. If it is not, load `filtserv.nlm`.
- 2 Go to the system console and enter `filtsrv_backup_filters filename`
- 3 The filters are backed up to the filename provided earlier. If no filename is provided, the filters are backed up to `sys:\etc/filters.bak`.

Restoring Filters to eDirectory from Text Files

- 1 Ensure that `filtsrv.nlm` is unloaded. If it is not, unload `filtserv.nlm`.
- 2 Rename the text file from which you want to restore to `filters.cfg` and place it in the `sys:etc` directory.
- 3 On the system console, enter `load filtsrv migrate`
- 4 Unload `filtsrv`.

14

Advanced Configuration of IP Packet Filters Using FILTCFG

The following sections describe how to configure exceptions using FILTCFG to allow specific IP services through the Novell® BorderManager® 3.8 firewall when the action of the filters is to deny packets in the filter list. A server SET command to filter packets that have IP header options is also described.

- ♦ [“Choosing between Stateful or Static Packet Filters” on page 141](#)
- ♦ [“Setting Up an HTTP Filter” on page 141](#)
- ♦ [“Setting Up an FTP Filter” on page 143](#)
- ♦ [“Setting Up a Telnet Filter” on page 144](#)
- ♦ [“Setting Up an SMTP Filter” on page 145](#)
- ♦ [“Setting Up a POP3 Filter” on page 146](#)
- ♦ [“Setting Up a DNS Filter” on page 147](#)
- ♦ [“Setting Up VPN Filters” on page 148](#)
- ♦ [“Filtering IP Packets that Use the IP Header Options Field” on page 148](#)

Choosing between Stateful or Static Packet Filters

Stateful packet filters are more secure because they allow only the packets in response to requests to pass through the firewall. For this reason, the procedures in this section describe how to configure stateful packet filters. However, static packet filters offer faster performance, so a list of equivalent static filters is provided, should you choose to configure them.

If you choose to configure static filters for the TCP protocol, you should enable ACK bit filtering so that all inbound packets that do not have the TCP ACK bit set are dropped by the server.

Setting Up an HTTP Filter

You can set up an HTTP filter on your server’s public interface to filter HTTP packets in the inbound or outbound direction. An inbound HTTP filter might be required to allow public access to specific Web servers in your private network. An outbound HTTP filter might be required to allow certain users to bypass proxy services and connect directly to origin Web servers.

This section contains the following tasks, complete the following steps:

- ♦ [“Setting Up a Stateful HTTP Filter” on page 142](#)
- ♦ [“Setting Up Static Filters for HTTP” on page 142](#)

Setting Up a Stateful HTTP Filter

- 1** Select Configure TCP/IP Filters > Packet Forwarding Filters, then click Exceptions.
- 2** Press Ins to define a new exception.
- 3** If you are creating an inbound exception, complete the following:
 - 3a** Specify All Interfaces for the Source Interface parameter.
 - 3b** Specify the server's public interface for the Destination Interface parameter.
 - 3c** Press Enter for Packet Type, then select www-http-st.
The www-http-st packet type is for HTTP over TCP. This packet type will not work for HTTP over UDP.
 - 3d** If you want the server to forward HTTP packets only from certain public hosts, specify Host or Network for the Src Addr Type parameter, then specify the IP address for the Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.
 - 3e** If you want the server to forward HTTP packets only addressed to certain private hosts, specify Host or Network for the Dest Addr Type parameter, then specify the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.
 - 3f** Press Esc select Yes to save the filter.
- 4** If you are creating an outbound exception, complete the following:
 - 4a** Specify the server's private interface for the Source Interface parameter.
 - 4b** Specify the server's public interface for the Destination Interface parameter.
 - 4c** Press Enter for Packet Type then select www-http-st.
 - 4d** If you want the server to forward HTTP packets from certain private hosts only, specify Host or Network for the Src Addr Type parameter then specify the IP address for Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.
 - 4e** If you want the server to forward HTTP packets addressed to certain public hosts only, specify Host or Network for the Dest Addr Type parameter then specify the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.
 - 4f** Press Esc, then select Yes to save the filter.

IMPORTANT: The outbound stateful HTTP filter does not allow packets for Domain Name System (DNS) name resolution to be forwarded to a DNS server on the public network. DNS names in URLs cannot be resolved unless you set up a DNS filter.

Setting Up Static Filters for HTTP

If you do not want to configure a stateful HTTP exception, you can create static filters instead. In the direction that HTTP requests will be sent, create one or both of the following static packet filter exceptions:

- ◆ www-http (for HTTP over TCP)
- ◆ www-http/udp (for HTTP over UDP)

Most browsers are configured to use HTTP over TCP, but they can also use HTTP over UDP. If you support browsers using HTTP over UDP, you should create both filters.

In the direction that HTTP responses will be sent, create one or both of the following static packet filter exceptions:

- ♦ `dynamic/tcp` (for HTTP over TCP)
- ♦ `dynamic/udp` (for HTTP over UDP)

The exceptions you create depend on which exceptions you created for the opposite direction of packet flow. If you have created exceptions for both `www-http` and `www-http/udp`, you should create filter exceptions for both `dynamic/tcp` and `dynamic/udp`. The dynamic port range is 1024 to 65,535.

IMPORTANT: These filters do not allow packets for DNS name resolution to be forwarded.

Setting Up an FTP Filter

You can set up an FTP filter on your server's public interface to filter FTP packets in the inbound or outbound direction. An inbound FTP filter might be required if public users connect to an FTP server in your private network. An outbound FTP filter might be required to allow certain users to bypass proxy services and connect directly to FTP servers on the public network.

When you set up an FTP filter, you can configure it to inspect for active FTP connections, passive FTP connections, or both. For tighter security, some administrators allow only active FTP connections in the inbound direction so the data connection is always on port 20. In contrast, passive FTP connections use any dynamic ports that are available.

This section contains the following tasks:

- ♦ [“Setting Up a Stateful FTP Filter” on page 143](#)
- ♦ [“Setting Up Static Filters for FTP” on page 144](#)

Setting Up a Stateful FTP Filter

- 1** Select Configure TCP/IP Filters, click Packet Forwarding Filters, then click Exceptions.
- 2** Press `Ins` to define a new exception.
- 3** If you are creating an inbound exception, complete the following:

- 3a** Specify All Interfaces for the Source Interface parameter.
- 3b** Specify the server's public interface for the Destination Interface parameter.
- 3c** Press `Enter` for Packet Type, then select `ftp-port-pasv-st`.

The packet type `ftp-port-pasv-st` allows both active and passive FTP connections. To allow active FTP connections only, select `ftp-port-st`. To allow passive FTP connections only, select `ftp-pasv-st`.

- 3d** If you want the server to forward FTP packets from certain public hosts only, specify Host or Network for the Src Addr Type parameter, then specify the IP address for the Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.
- 3e** If you want the server to forward FTP packets addressed to certain private hosts only, specify Host or Network for the Dest Addr Type parameter, then specify the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.
- 3f** Press `Esc`, then select Yes to save the filter.

4 If you are creating an outbound exception:

4a Specify the server's private interface for the Source Interface parameter.

4b Specify the server's public interface for the Destination Interface parameter.

4c Press Enter for Packet Type, then select ftp-port-pasv-st.

The packet type ftp-port-pasv-st allows both active and passive FTP connections. To allow active FTP connections only, select ftp-port-st. To allow passive FTP connections only, select ftp-pasv-st.

4d If you want the server to forward FTP packets from certain private hosts only, specify Host or Network for the Src Addr Type parameter and specify the IP address for the Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.

4e If you want the server to forward FTP packets addressed to certain public hosts only, specify Host or Network for the Dest Addr Type parameter, then specify the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.

4f Press Esc, then select Yes to save the filter.

IMPORTANT: The outbound stateful FTP filter does not allow packets for DNS name resolution to be forwarded to a DNS server on the public network. Users establishing an FTP connection to an FTP server must use the FTP server's IP address unless you set up a DNS filter.

Setting Up Static Filters for FTP

If you do not want to configure a stateful FTP exception, you can create static filters instead.

To allow public hosts to establish active FTP connections to a server in the private network, configure the following inbound and outbound filter exceptions:

- ♦ ftp (the control channel)
- ♦ ftp-data (the data channel)

If you want to allow users in your private network to establish passive FTP connections to public servers, configure additional filter exceptions for dynamic/tcp in both directions so that dynamic ports can be used as the data channel instead of port 20. Enable ACK bit filtering for the dynamic/tcp exceptions.

IMPORTANT: These filters do not allow users to establish FTP connections using the FTP server's DNS name. A DNS filter is required.

Setting Up a Telnet Filter

You can set up a Telnet filter on your server's public interface to filter Telnet packets in the inbound or outbound direction. An inbound Telnet filter might be required if public users establish Telnet sessions to a server in your private network. An outbound Telnet filter might be required to allow users to establish a Telnet session on the public network.

This section contains the following tasks:

- ♦ [“Setting Up a Stateful Telnet Filter” on page 145](#)
- ♦ [“Setting Up Static Filters for Telnet” on page 145](#)

Setting Up a Stateful Telnet Filter

- 1** Select Configure TCP/IP Filters, click Packet Forwarding Filters, then click Exceptions.
- 2** Press Ins to define a new exception.
- 3** If you are creating an inbound exception:
 - 3a** Specify All Interfaces for the Source Interface parameter.
 - 3b** Specify the server's public interface for the Destination Interface parameter.
 - 3c** Press Enter for Packet Type, then select telnet-st.
 - 3d** If you want the server to forward Telnet packets from certain public hosts only, specify Host or Network for the Src Addr Type parameter, then specify the IP address for the Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.
 - 3e** If you want the server to forward Telnet packets addressed to certain private hosts only, specify Host or Network for the Dest Addr Type parameter, then specify the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.
 - 3f** Press Esc, then select Yes to save the filter.
- 4** If you are creating an outbound exception, complete the following:
 - 4a** Specify the server's private interface for the Source Interface parameter.
 - 4b** Specify the server's public interface for the Destination Interface parameter.
 - 4c** Press Enter for Packet Type, then select telnet-st.
 - 4d** If you want the server to forward Telnet packets from certain private hosts only, specify Host or Network for the Src Addr Type parameter, then specify the IP address for the Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.
 - 4e** If you want the server to forward Telnet packets addressed to certain public hosts only, specify Host or Network for the Dest Addr Type parameter, then specify the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.
 - 4f** Press Esc, then select Yes to save the filter.

IMPORTANT: The outbound stateful Telnet filter does not allow packets for DNS name resolution to be forwarded to a DNS server on the public network. Users establishing a Telnet session must use IP addresses unless you set up a DNS filter.

Setting Up Static Filters for Telnet

If you do not want to configure a stateful Telnet exception, you can create static filters instead. Simply create a static Telnet filter exception in both the inbound and outbound directions. Make sure you enable ACK bit filtering for the exception in the inbound direction.

IMPORTANT: These filters do not allow users to establish Telnet sessions using a server's DNS name. A DNS filter is required.

Setting Up an SMTP Filter

You can set up a Simple Mail Transfer Protocol (SMTP) exception on the server's public interface to allow SMTP mail servers or SMTP gateways in your private network to send and receive mail through the Novell BorderManager 3.8 firewall.

This section contains the following topics:

- ◆ [“Setting Up a Stateful SMTP Filter” on page 146](#)
- ◆ [“Setting Up Static Filters for SMTP” on page 146](#)

Setting Up a Stateful SMTP Filter

- 1** Select Configure TCP/IP Filters, click Packet Forwarding Filters, then click Exceptions.
- 2** Press Ins to define a new exception.
- 3** If you want private SMTP servers or gateways to be able to send mail through the firewall, specify the server’s private interface as the Source Interface.

or

If you want public SMTP servers to be able to send mail to the SMTP server in your private network, and you have not enabled the Mail proxy, specify the server’s public interface as the Source Interface.

- 4** If you want private SMTP servers or gateways to be able to send mail through the firewall, specify the server’s public interface as the Destination Interface.

or

If you want public SMTP servers to be able to send mail to the SMTP server in your private network, and you have not enabled the Mail proxy, specify the server’s private interface as the Destination Interface.

- 5** Press Enter for Packet Type, then select smtp-st.
- 6** Press Enter, then select Yes to save the filter.

IMPORTANT: The outbound stateful SMTP filter does not allow domain names to be resolved by a DNS server on the public network.

Setting Up Static Filters for SMTP

If you do not want to configure a stateful SMTP exception, you can create static filters instead. Simply create a static SMTP filter exception in both the inbound and outbound directions. Make sure you enable ACK bit filtering for the exception in the inbound direction.

IMPORTANT: These filters do not forward requests for domain name resolution. A DNS filter is required.

Setting Up a POP3 Filter

You can set up a Post Office Protocol 3 (POP3) exception on the server’s public interface to allow public clients to access a private POP3 server behind the Novell BorderManager firewall.

This section contains the following topics:

- ◆ [“Setting Up a Stateful POP3 Filter” on page 147](#)
- ◆ [“Setting Up a Static POP3 Filter” on page 147](#)

IMPORTANT: These filters do not forward requests for domain name resolution by a DNS server in your private network. A DNS filter is required.

Setting Up a Stateful POP3 Filter

- 1 Select Configure TCP/IP Filters, click Packet Forwarding Filters, then click Exceptions.
- 2 Press Ins to define a new exception.
- 3 Specify All Interfaces for the Source Interface parameter.
- 4 Specify the server's public interface for the Destination Interface parameter.
- 5 If you want the server to forward mail from certain public hosts only, specify Host or Network for the Src Addr Type parameter, then specify the IP address for the Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.
- 6 If you want the server to forward mail addressed to certain private hosts only, specify Host or Network for the Dest Addr Type parameter, then specify the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.
- 7 Press Enter for Packet Type, then select pop3-st.
- 8 Press Esc, then select Yes to save the filter.

Setting Up a Static POP3 Filter

If you do not want to configure a stateful POP3 exception, you can create a static filter instead. Make sure you enable ACK bit filtering for the exception in the inbound direction.

Setting Up a DNS Filter

TCP/IP connections to a server can be made by specifying the server's IP address, but most servers, particularly those connected to the Internet, are accessed by their DNS names.

This section contains the following topics:

- [“Setting Up a Stateful DNS Filter” on page 147](#)
- [“Setting Up Static Filters for DNS” on page 148](#)

Setting Up a Stateful DNS Filter

To set up a stateful DNS exception to allow users to use DNS names to connect to servers accessed through the Novell BorderManager 3.8 server's public interface, complete the following steps from the main FILTCFG menu:

- 1 Select Configure TCP/IP Filters, click Packet Forwarding Filters, then click Exceptions.
- 2 Press Ins to define a new exception.
- 3 Specify the server's private interface for the Source Interface parameter.
- 4 Specify the server's public interface for the Destination Interface parameter.
- 5 Press Enter for Packet Type, then select dns/udp-st.
- 6 Press Esc, select Yes to save the filter.

IMPORTANT: If applications are configured to use DNS over TCP, you can also configure a stateful DNS exception for DNS over TCP. In [Step 5](#), select the dns/tcp-st packet type instead of the dns/udp-st packet type.

Setting Up Static Filters for DNS

If you do not want to configure a stateful DNS exception, you can create static filters instead.

In the direction that DNS queries will be sent, create the following static packet filter exception:

- ◆ dns/udp

In the direction that DNS responses will be sent, create the following static packet filter exception:

- ◆ dynamic/udp

Setting Up VPN Filters

To set filter exceptions to allow VPN traffic refer to [“Setting Up VPN Filters” on page 185](#).

Filtering IP Packets that Use the IP Header Options Field

In addition to containing 32-bit source IP address and destination IP address fields, IP packets also contain an options field. This field can be used for the following purposes:

- ◆ Security restrictions: United States Department of Defense basic and extended security options to identify classification levels and security information.
- ◆ Record route: List of IP addresses to identify each router that forwarded the packet.
- ◆ Time stamp: List of IP addresses and time stamps to identify each router that forwarded the packet.
- ◆ Source routing: List of IP addresses to which the packet must be routed.

Although the NetWare TCP/IP stack does not process these options, it can be a security risk to forward packets with these options specified. In particular, the source routing option can force all packets that are routed from your network to be forwarded to an untrustworthy host in the public network.

When you install Novell BorderManager 3.8 firewall/caching services, a server SET command is automatically enabled to drop packets with IP header options enabled.

To view the current setting for your server, complete the following steps:

- 1** At the server console, enter

```
SET
```

- 2** Select option 1 (Communications).

- 3** Verify that the SET command displays as

```
SET FILTER PACKETS WITH IP HEADER OPTIONS = ON
```

It is best not to change the default setting, but under certain circumstances you might need to turn this setting off. For example, you could use the source routing option to specify the routers that must handle the traffic from your network.

IMPORTANT: Because routers often do not support IP header options, be sure to verify the capability of your routers before disabling the filtering to perform such tests.

To disable the filtering of packets that use IP header options from the server console, enter

```
SET FILTER PACKETS WITH IP HEADER OPTIONS = OFF
```

To re-enable the filtering from the server console, enter

```
SET FILTER PACKETS WITH IP HEADER OPTIONS = ON
```


15

NBM Filter Management

In NBM Filter Management, the Easy Filter Configuration task lets you easily configure filters and exceptions without having an extensive knowledge of services and protocols.

The following sections describe how to configure filters and exceptions using Easy Filter Configuration to allow specific IP services through the Novell[®] BorderManager[®] 3.8 firewall.

- ◆ “Features of Easy Filter Configuration” on page 151
- ◆ “Configuring Filters using Easy Filter Configuration” on page 151
- ◆ “On Server Service Exceptions” on page 153
- ◆ “Off Server Service Exceptions” on page 155
- ◆ “Filter Maintenance” on page 156
- ◆ “List All Firewall Policies” on page 157
- ◆ “Troubleshooting: Possible Installation Scenarios” on page 158

Features of Easy Filter Configuration

- ◆ All NBM/On Server (NSBS)/Off Server services are logically grouped together and listed as services
- ◆ Falling back to default filters is possible
- ◆ Clearing all kinds of filters and exceptions on the selected server is easier
- ◆ All policies are listed in one page
- ◆ Creation of service-based exceptions is easier

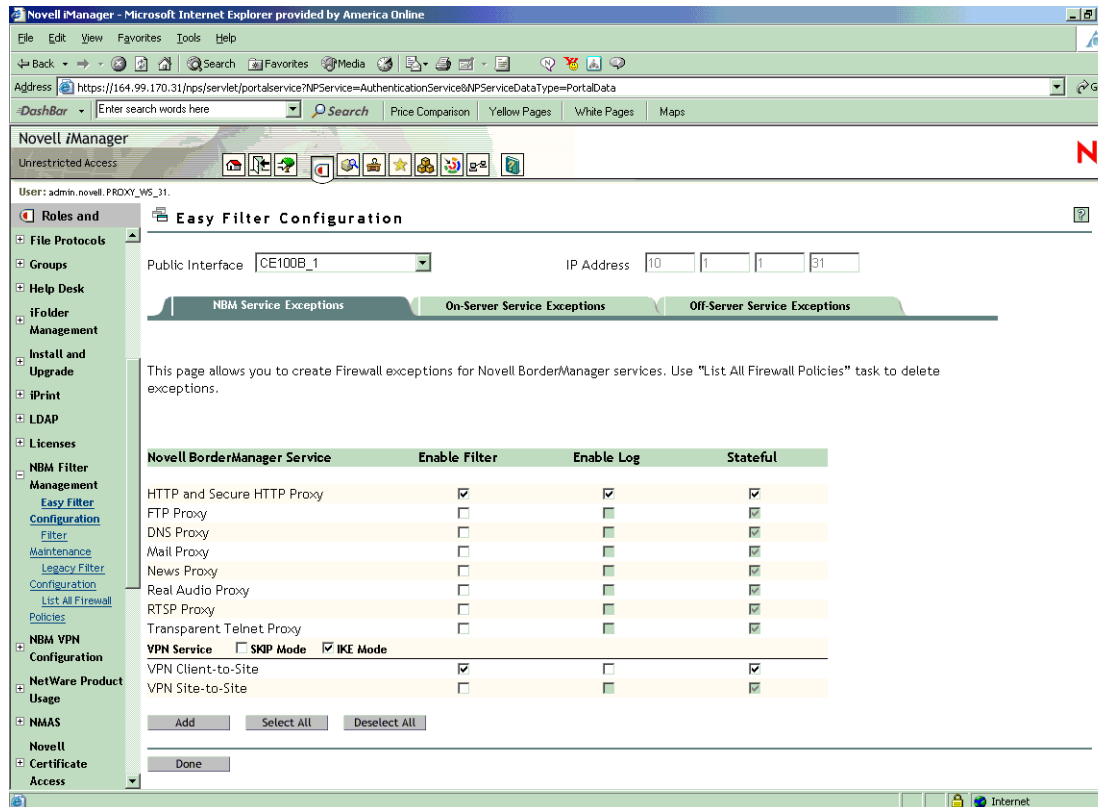
Configuring Filters using Easy Filter Configuration

You can configure filters and exceptions for the following NBM services:

- ◆ HTTP and Secure HTTP Proxy
- ◆ FTP Proxy
- ◆ DNS Proxy
- ◆ Mail Proxy
- ◆ News Proxy
- ◆ Real Audio Proxy
- ◆ RTSP Proxy
- ◆ Transparent Telnet Proxy

- 1** Click the Easy Filter Configuration task under NBM Filter Management.
- 2** From the list, select the server where the filters are to be configured by clicking the icon and then click OK.

Figure 25 Easy Filter Configuration



3 From the drop-down list, select the public interface of the server where the filters/exceptions are to be configured.

4 To enable the filter for a service, select the corresponding check box under Enable Filter.

If you enable exceptions for HTTP and secure HTTP proxy with the Stateful option, it creates two default filters to deny all incoming and outgoing connections, thus creating exceptions to allow only HTTP and HTTPS traffic.

5 To enable the log for a service, select the corresponding check box, under Enable Log.

IMPORTANT: When you enable this option, the header of the packet that match the options in the filters or exceptions is logged if you have enabled both global logging status and filters/exception logging status. This is placed in the directory `sys:\etc\logs\lppktlog`. If you disable the option, the packets that match the options in filters or exceptions are not logged. Datalogging slows down the server's performance and should be kept on only for a short time.

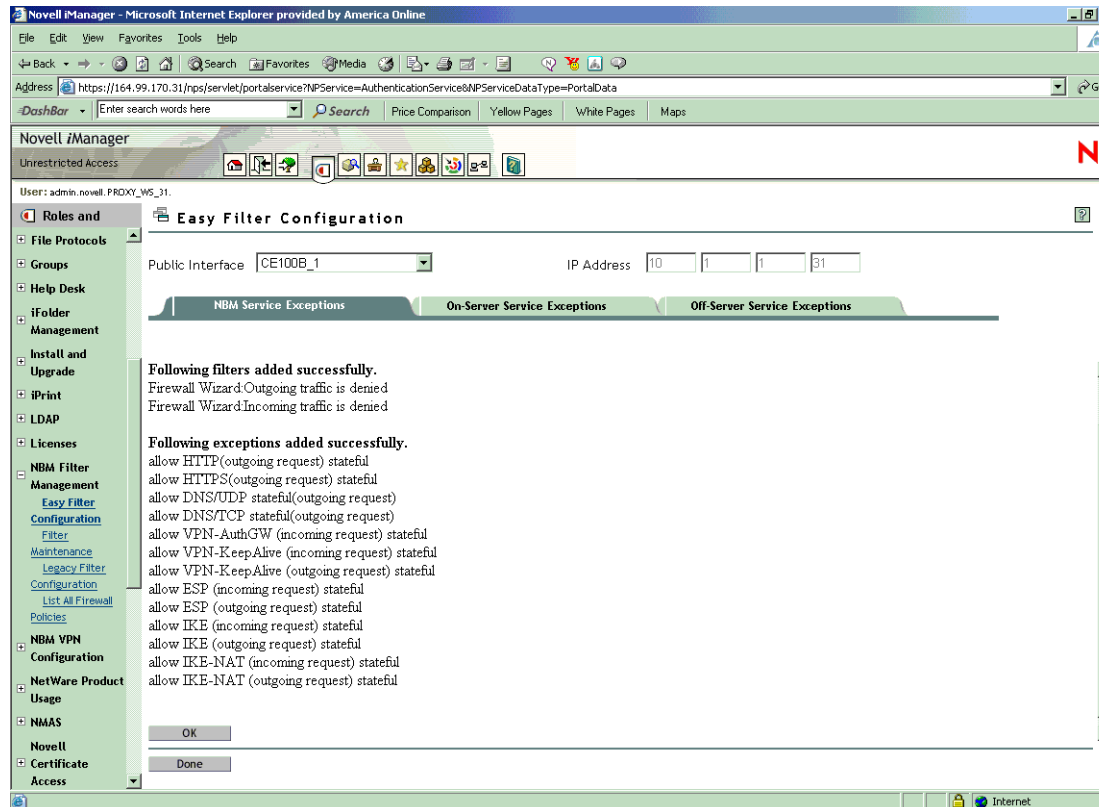
6 To enable the stateful filter for a service, select the corresponding check box under Stateful.

If stateful filtering is enabled in a filter rule, a dynamic filter is also created in the reverse direction. The reverse filter is created with the information such as source IP address, source interface, source port, destination IP address, destination interface, and destination port. This information is stored in a table which is later used to compare against the reply.

7 Click Add.

The following page is displayed:

Figure 26 Filters successfully created



NOTE: If you want to delete the exceptions, use [“List All Firewall Policies”](#) on page 157.

On Server Service Exceptions

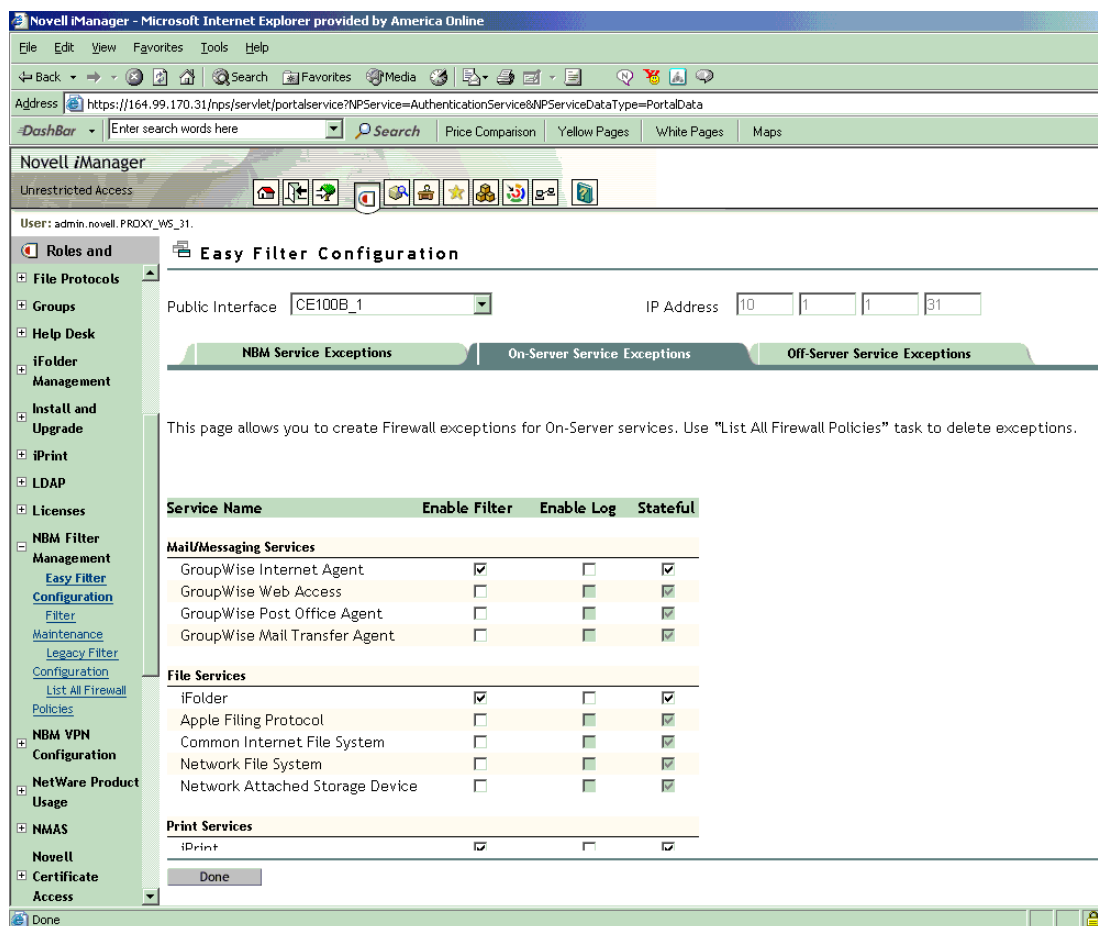
All Novell Small Scale Business Suite (NSBS) services are grouped and listed under On Server Services. On Server is the server where all the services and firewall are running. You can configure exceptions to the On Server Services here.

The On Server services (NSBS) are grouped into five main service headings, under which various services are available:

- ◆ Mail Messaging Services
 - ◆ Groupwise[®] Internet Agent
 - ◆ Groupwise Web Access
 - ◆ Groupwise PO Agent
 - ◆ Groupwise Mail Transfer Agent
- ◆ File Services
 - ◆ iFolder[®]
 - ◆ Apple* Filing Protocol
 - ◆ Common Internet File System
 - ◆ Network File System

- ◆ Network Attached Storage Device
- ◆ Print Services
 - ◆ iPrint
 - ◆ Line Printer Daemons
 - ◆ Novell Distributed Print Services™ (NDPS®)
- ◆ Network Management
 - ◆ ZENworks® for Desktop 3
 - ◆ ZENworks for Server 2
 - ◆ ZENworks for Server 3.2
- ◆ Miscellaneous
 - ◆ iManager
 - ◆ WebServer
 - ◆ Remote Debugger

Figure 27 On Server Exceptions



To configure filters and exceptions for On Server Services, complete the following steps:

- 1 Select the check box corresponding to each service filters and logs you want to enable.

IMPORTANT: When you select enable log, it creates a log where the header of the packet that matches the options in the filters or exceptions is logged. Data logging slows down the server's performance and you should turn it on only for a short period.

- 2** Select the check box under Stateful to enable a stateful filter.
- 3** Click Add.

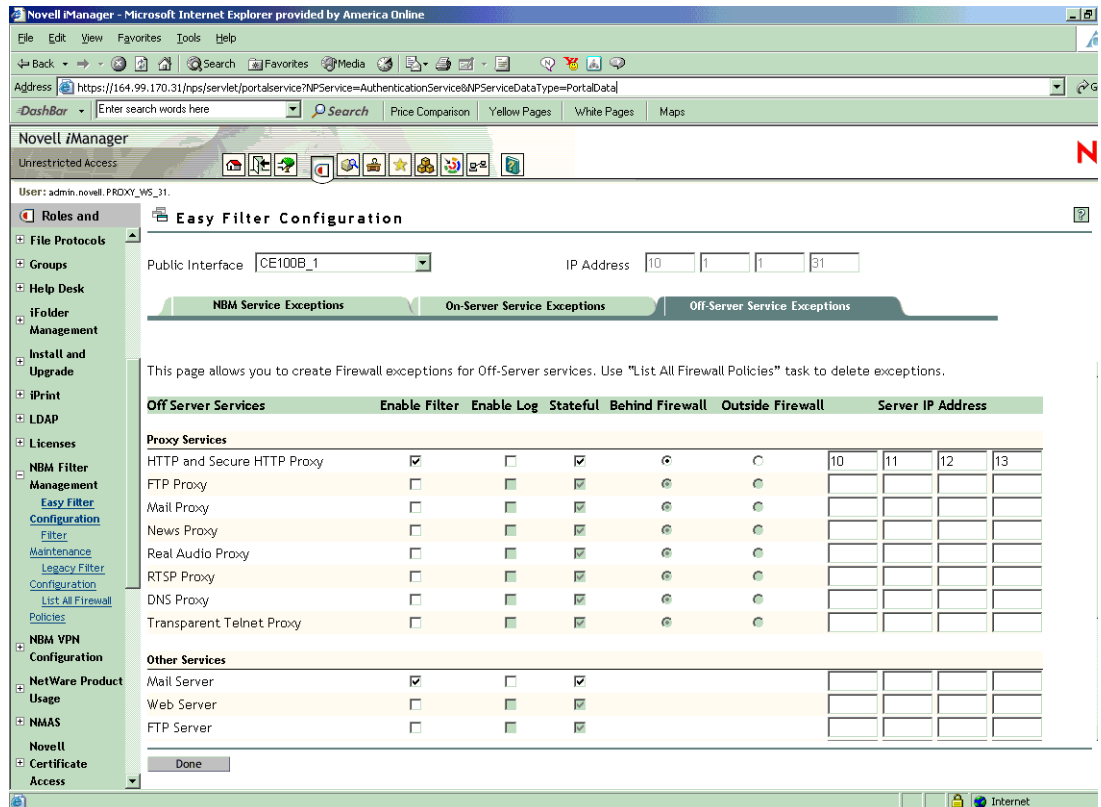
The results page is displayed.

Off Server Service Exceptions

Off Server Services (where firewall and services run on different machines) exceptions are classified into two main categories, under which various services are available.

- ◆ Proxy Services
 - ◆ HTTP and Secure HTTP Proxy
 - ◆ FTP proxy
 - ◆ Mail Proxy
 - ◆ News Proxy
 - ◆ Real Audio Proxy
 - ◆ RTSP proxy
 - ◆ DNS Proxy
 - ◆ Transparent Telnet Proxy
- ◆ Other Services
 - ◆ Mail Server
 - ◆ Web Server
 - ◆ FTP Server
 - ◆ DNS Server

Figure 28 Off Server Service Exceptions



To configure Off Server service exceptions, complete the following steps:

- 1** Select the Public Interface where the exceptions are to be created.

This is either the LAN or WAN interface that connects your server to the Internet or other public network.
- 2** Indicate whether the exceptions should be stateful or stateless.

If stateful filtering is enabled in a filter rule, a dynamic filter is also created in the reverse direction that is defined by the filter rule.
- 3** Indicate whether the proxy server is behind or outside the firewall by selecting the respective radio buttons.
 - ◆ Select Behind Firewall if the service is behind the firewall and the traffic to the Internet has to pass through the firewall.
 - ◆ If the service exists before the firewall and the traffic coming from the Internet has to pass through the proxy and the firewall, then select Outside Firewall.
- 4** Type the server IP address of the proxy where the services are running, then click Add.

Filter Maintenance

Use this task if you want to retain the default filters or if the existing filters on the servers need to be deleted.

- 1** Click the filter maintenance task, then select the server for filter maintenance.

2 On the next page, select one of the following operations:

- ◆ Restore Default Filters
- ◆ Clear Filter Configuration

Restore Default Filters adds the default filters to the services on a particular interface. Clear Filter Configuration deletes all the existing filters and exceptions on the selected server.

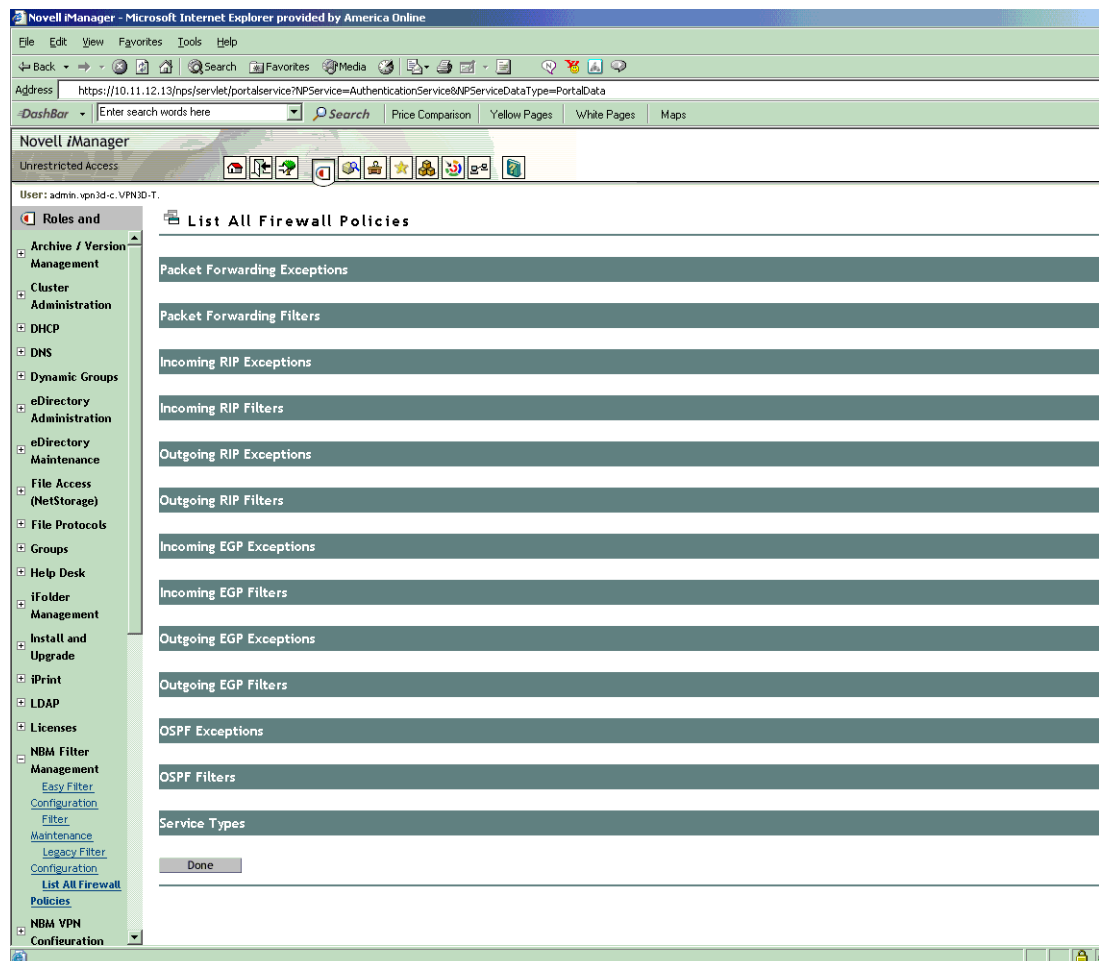
Restore Default Filters has the same functionality as brdcfg.nlm available in the Legacy Filter configuration. For more information, see [“Using Novell iManager for Filter Configuration” on page 110](#).

3 On the next page, select Public Interface and click OK

List All Firewall Policies

When you select this task, the following page is displayed listing all the firewall policies:

Figure 29 List All Firewall policies



When you expand any item in the list, all the filters/exceptions which fall under it are listed.

Each filter/exception can be modified or deleted. New filters can also be defined and added.

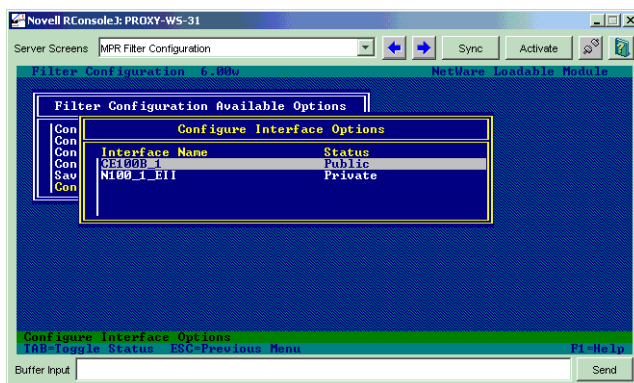
Filter Modification: When you click this icon, all the filters and exceptions listed under each heading is displayed. To modify a filter, click its name, make your changes on the screens that follow, and then click Done.

Service Type Modification: Only those services which are nonstandard or user created appear hyperlinked and can be modified. For more details, refer “Configuring the Service Type” on page 132.

Setting Up Public Interface

- 1 Load `filtcfg.nlm`, then select Configure Interface.

Figure 30 Configuring Public Interface



- 2 Press Tab to select the configuration as Public or Private.
- 3 Enter `Reinitialize system` at the server console and refresh iManager.

Troubleshooting: Possible Installation Scenarios

The Off Server Service Fields Appear Disabled

If this occurs, install the `bm` module package manually by completing the following steps:

- 1 Click the Configure icon in the top pane of iManager.
 - 1a For a description of each icon, mouse over it.
- 2 Click Module Configuration > Install Module Package.
- 3 Map the NetWare[®] `sys` volume directory.
 - 3a The path of the directory : `sys:\tomcat\4\webapps\nps\packages\bm.npm`
- 4 Browse `bm.npm` file.
- 5 Click Install.
- 6 Enter the following commands at the Netware console:

```
java -exit
tomcat4
```

Roles and Tasks Do Not Appear on the Left Pane

Refresh the page or log in again.

IV

Virtual Private Network

A Virtual Private Network (VPN) is used to transfer sensitive information across the Internet in a secure fashion by encapsulating and encrypting the data. A VPN can also be deployed in intranets where data security is required between departments.

The Novell BorderManager 3.8 VPN features, including integration with Novell eDirectory, give remote and mobile employees secure access to network resources they are entitled to use. This means that they can enjoy direct, secure access to all the services such as file, print, and e-mail applications they need, from wherever they're working.

Novell BorderManager 3.8 supports open standards and authenticates the users with any fully compliant Lightweight Directory Access Protocol (LDAP) directory or Novell eDirectory. Novell BorderManager 3.8 traffic rules enable you to manage users' access at a granular level by client-to-site or site-to-site service, node, network address, and more.

For greater authentication flexibility in this release of Novell BorderManager 3.8, the BorderManager Authentication Services (BMAS) authentication is replaced with Novell Modular Authentication Services (NMAS™) mechanism. Novell BorderManager supports more than 50 advanced authentication methods. As a result, your mobile employees can use tokens, smart cards, X.509 certificates, and other supported methods—alone or in combination—to securely access data via the VPN. Novell BorderManager 3.8 can interoperate with third-party servers using standard based protocols such as IKE and IPsec.

The following sections of the *Novell® BorderManager® 3.8 Installation and Administration* guide provide information on how to set up and use VPN. Novell BorderManager 3.8 provides an entirely new iManager-based VPN configuration.

- ◆ **Chapter 16, “Certificate-Based Authentication,” on page 163** provides information on the prerequisites for setting up the new VPN services.
- ◆ **Chapter 17, “Configuring VPN Services,” on page 179** describes how to set up the VPN services and use Novell iManager to configure and use policies on the VPN Server.
- ◆ **Chapter 18, “Upgrading Virtual Private Networks,” on page 221** provides basic information on how to upgrade to the new VPN.
- ◆ **Chapter 19, “Monitoring Virtual Private Networks,” on page 227** describes how to monitor the VPN services through the NetWare Remote Manager framework.
- ◆ **Chapter 20, “Virtual Private Network Client,” on page 239** describes the basic functionality of the VPN client and the procedure to install it. The VPN client is released along with Novell BorderManager 3.8.

For more information on some of the terms used in this section refer to the Glossary at the end of this book.

16 Certificate-Based Authentication

Novell® BorderManager® 3.8 Virtual Private Network (VPN) services are significantly different from the VPN services of all earlier versions of the software. The VPN services are enabled for iManager 2.0.1. For details see [“Installing iManager 2.0.1 Snap-Ins” on page 24](#). VPN services provide extensive facilities to set up and configure site-to-site and client-to-site services. This section discusses how to get the certificates to set up the VPN services.

Certificates, trusted root objects, and trusted root containers are needed to log into VPN services and configure client-to-site and site-to-site services. Some of these entities can be automatically created and are available by default. See [“Automated Creation of eDirectory Certificates or Objects” on page 164](#) to understand which items you do not need to create.

NOTE: Although an administrator can create certificates for any user using the ConsoleOne® or the iManager snap-ins, only the user can export those certificates into a file. However, an administrator can export a user certificate using the PKI Certificate Console. If the administrators needs to export the certificates, they must inform the user before exporting the certificates

- ◆ [“Automated Creation of eDirectory Certificates or Objects” on page 164](#)
- ◆ [“Creating Server Certificates” on page 164](#)
- ◆ [“Exporting Root Certificates from the Server Certificate” on page 169](#)
- ◆ [“Creating Trusted Root Containers” on page 171](#)
- ◆ [“Creating the Trusted Root Object” on page 172](#)
- ◆ [“Creating a User Certificate” on page 173](#)
- ◆ [“Exporting User Certificates” on page 175](#)
- ◆ [“Third-Party Certificate Server” on page 177](#)

The following list explains the entities required to configure the site-to-site and client-to-site services:

- ◆ For Site-to-Site
 - ◆ Server Certificate
 - ◆ Trusted Root Container in the eDirectory context of the Master VPN server
 - ◆ Trusted Root Objects in Trusted Root Container
- ◆ For Client-to-Site
 - ◆ Server Certificate
 - ◆ Trusted Root Container in the eDirectory context of the server
 - ◆ Trusted Root Objects in the Trusted Root Container
 - ◆ User Certificate(s)

Also see the [Novell Certificate Server \(http://www.novell.com/documentation/lg/crt203ad/\)](http://www.novell.com/documentation/lg/crt203ad/) documents for more details.

IMPORTANT: We recommend using iManager on a different server than on which the site-to-site VPN services are running.

Automated Creation of eDirectory Certificates or Objects

You can also create the server certificate and trusted root container automatically using VPN server configuration through iManager. In that case you need not follow the manual steps described in “[Creating Server Certificates](#)” on page 164 and “[Creating Trusted Root Containers](#)” on page 171. After creating the Server Certificate and the Trusted Root Container, export the Trusted Root from the server certificate using steps in “[Exporting Root Certificates from the Server Certificate](#)” on page 169, and create a Trusted Root object in the Trusted Root container using the steps in “[Creating the Trusted Root Object](#)” on page 172.

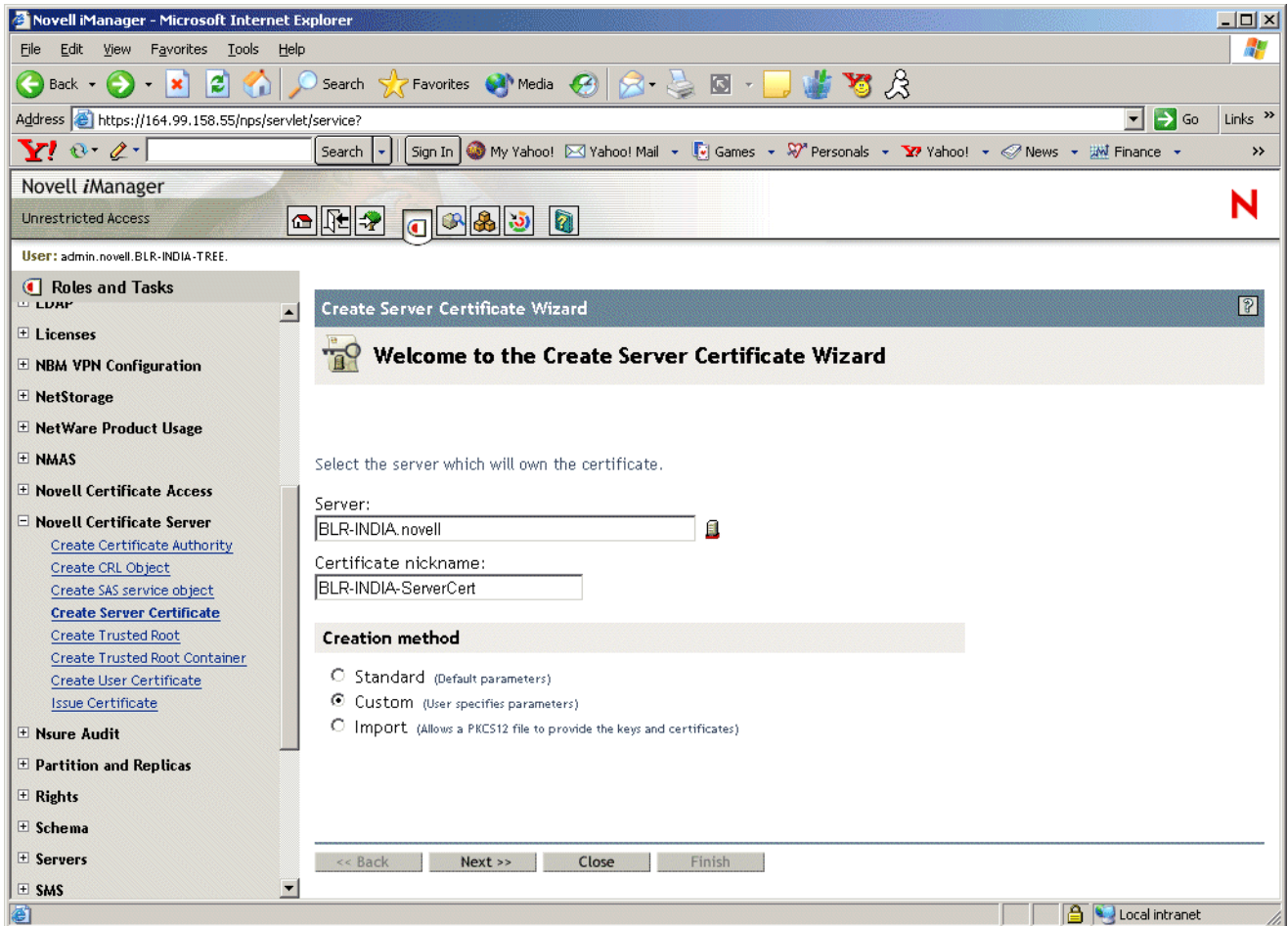
Creating Server Certificates

- 1 Log in to iManager. On a Windows XP or 2000 machine connected to a NetWare[®] server, go to (<https://ipaddress/nps/iManager.html>), where *ip address* is the IP address of a NetWare 6 or NetWare 6.5 server running Novell BorderManager 3.8.

NOTE: You can run iManager from a NetWare server to configure other Novell BorderManager 3.8 servers.

- 2 Type the username and password. Click Login. The username and password are the Novell eDirectory login details. Specify the non-fully-distinguished name.
- 3 In the left pane, select Novell Certificate Server, then select Create Server Certificate.

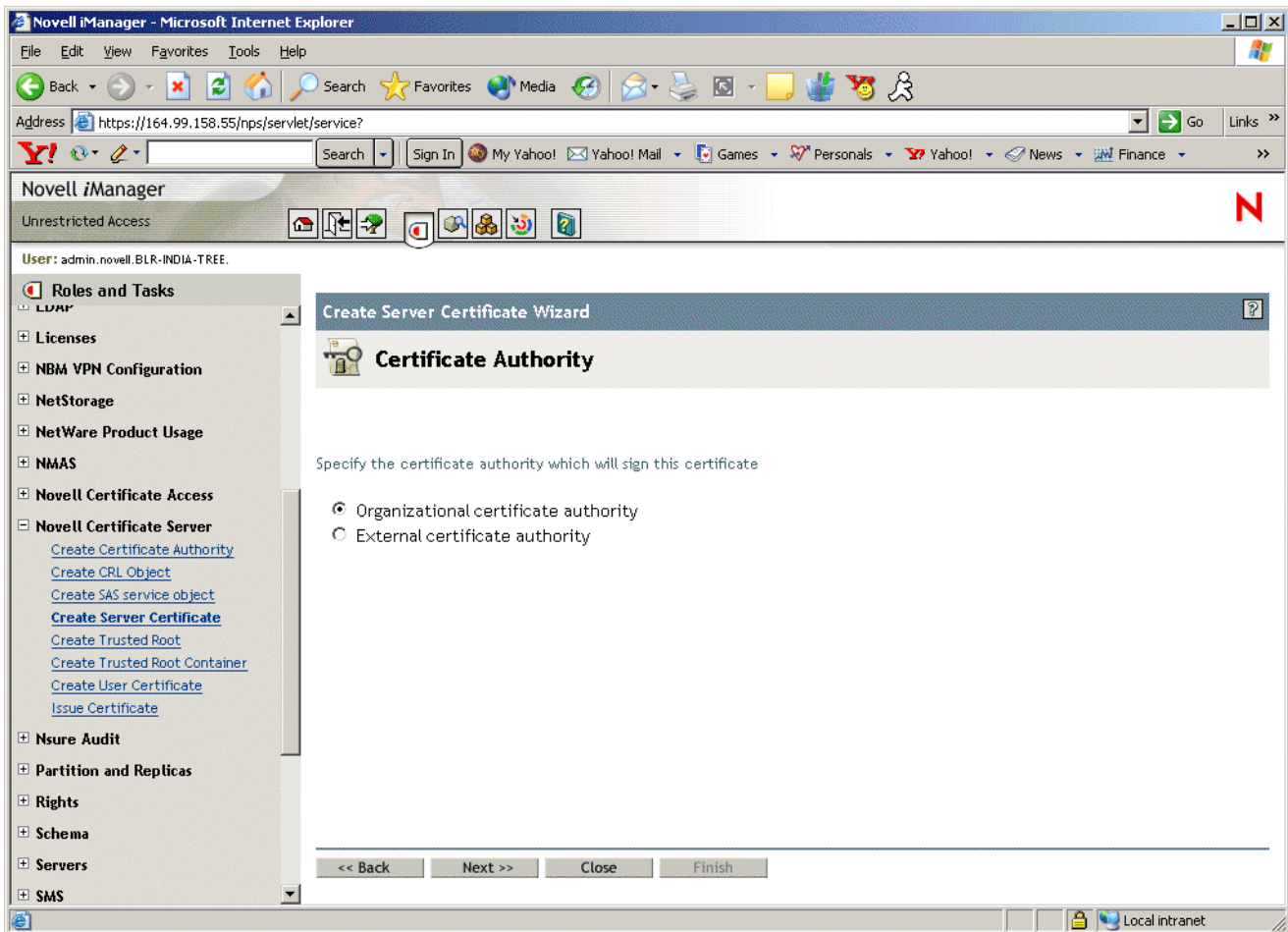
Figure 31 Create Server Certification Wizard



- 4 Specify the server name and the nickname for the certificate, or use the Browse button to select the server object that will be one of the underlined objects in iManager. The wizard will indicate which objects it is looking for. Select the Custom check box and specify the details of the certificate, then click Next.

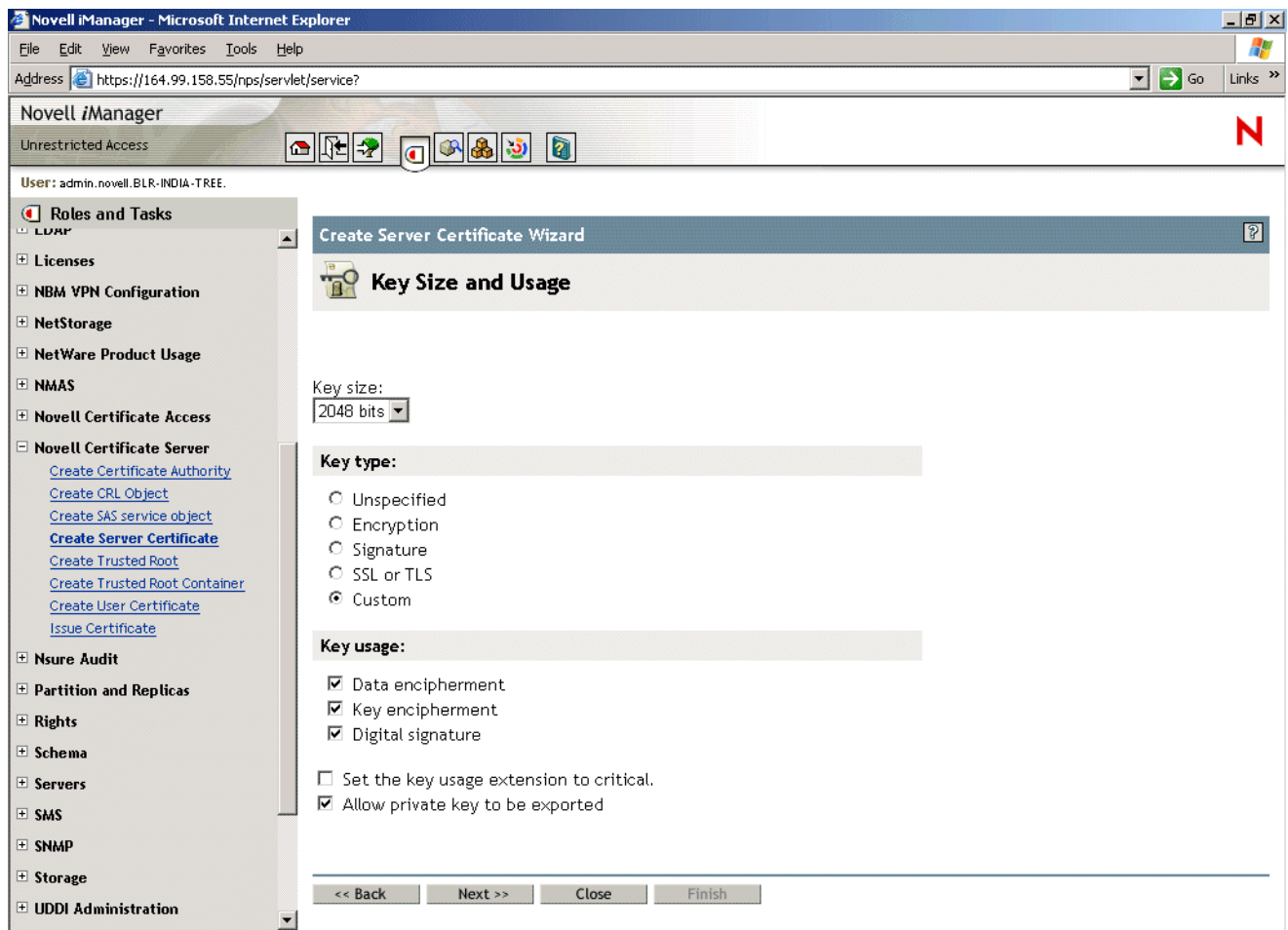
NOTE: While creating server certificates, the custom check box must be selected, and the key usage should be set to data encipherment and digital signature. For user certificates, creating a standard certificate will suffice. We recommend that you use the Custom option. If you use the Standard option, client-to-site services will work but there might be some problems with site-to-site services.

Figure 32 Certificate Authority



5 Select Organizational Certificate Authority, then click Next.

Figure 33 Key Size and Usage



6 Specify the Key Type and Key Usage, then click Next.

Figure 34 Certificate Parameters

Novell iManager - Microsoft Internet Explorer

Address: https://164.99.158.55/nps/servlet/service?

Novell iManager

Unrestricted Access

User: admin.novell.BLR-INDIA-TREE.

Roles and Tasks

- LDAP
- Licenses
- NBM VPN Configuration
- NetStorage
- NetWare Product Usage
- NMAS
- Novell Certificate Access
- Novell Certificate Server
 - Create Certificate Authority
 - Create CRL Object
 - Create SAS service object
 - Create Server Certificate
 - Create Trusted Root
 - Create Trusted Root Container
 - Create User Certificate
 - Issue Certificate
- Nsure Audit
- Partition and Replicas
- Rights
- Schema
- Servers
- SMS
- SNMP
- Storage
- UDDI Administration

Create Server Certificate Wizard

Certificate Parameters

Specify the certificate parameters.

Subject name:

NDS name:

Include NDS alternative name

Signature algorithm:

Validity period:

Effective date:

Expiration date:

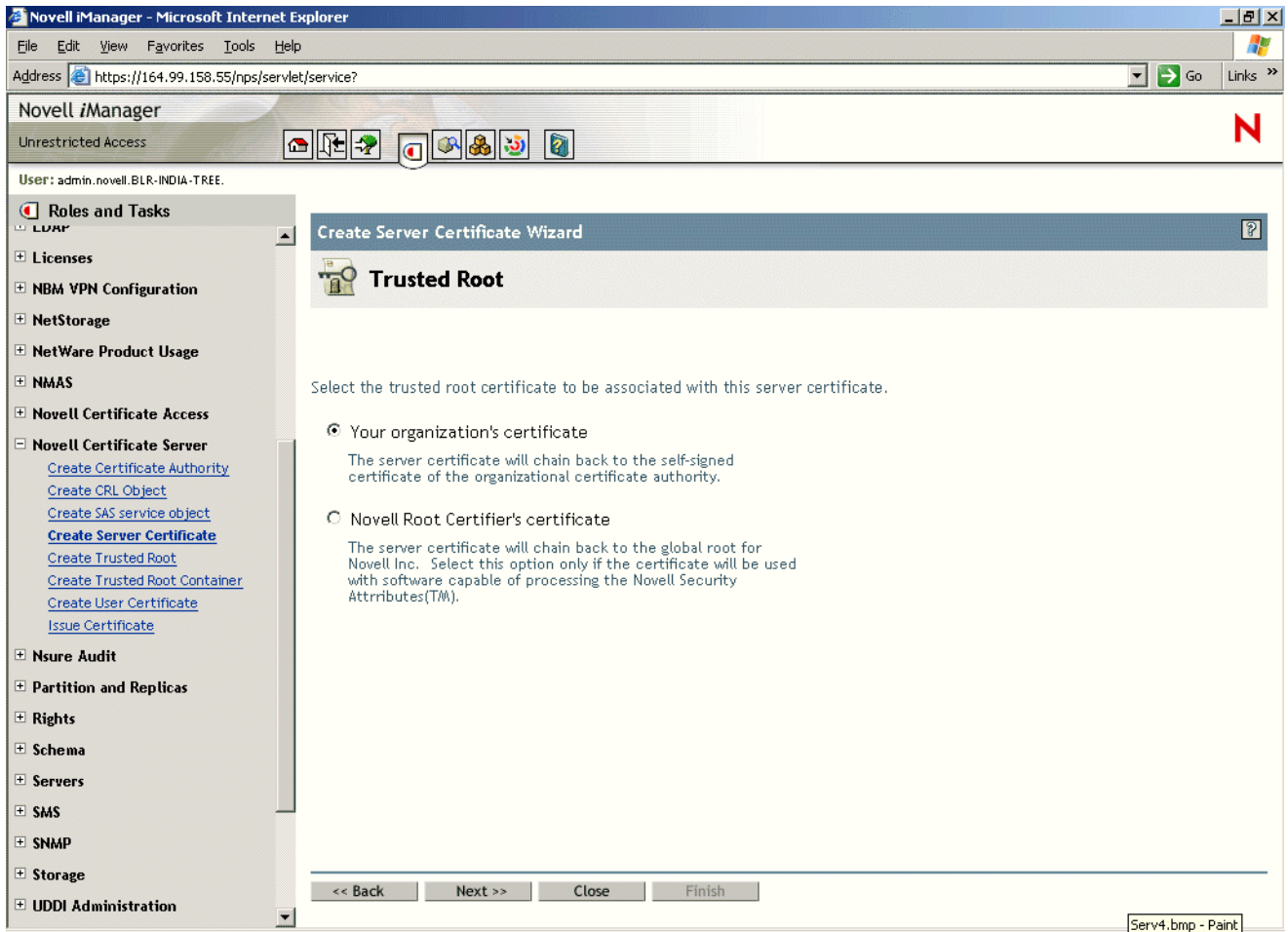
<< Back Next >> Close Finish

No notifications.

7 Specify the parameters of the certificate, specify the dates, then click Next.

Entering the exact time for validity has the advantage that if there is a timing issue with the server the entry won't be invalid.

Figure 35 Trusted Root



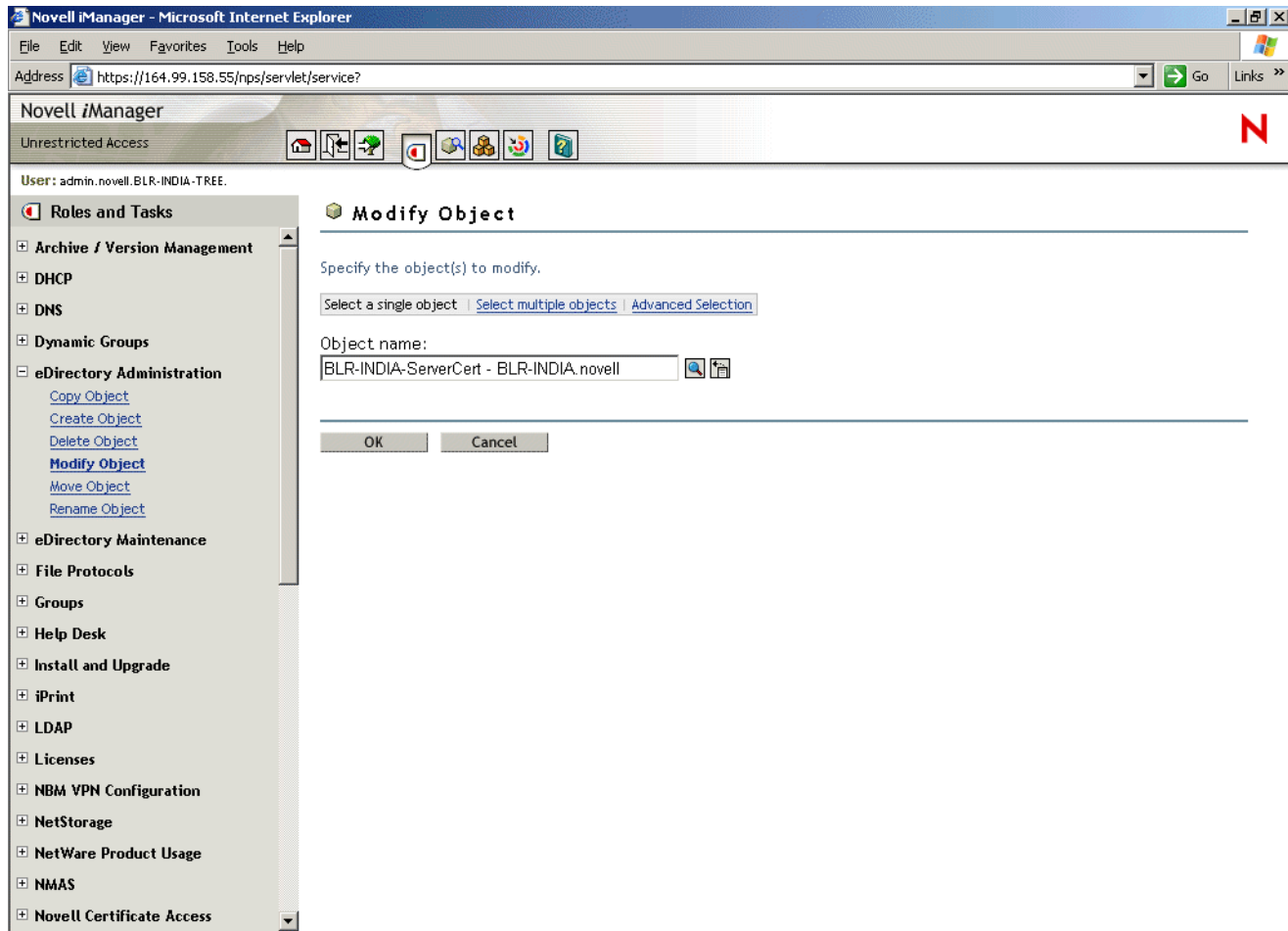
- 8 Select the relevant text box to specify the trusted root for the certificate, then click Next.
- 9 The summary page shows the complete details of the certificate chosen. If the information is correct, click Next. If it is not correct, then go back and make changes.

The certificate is created and you see a Success message.

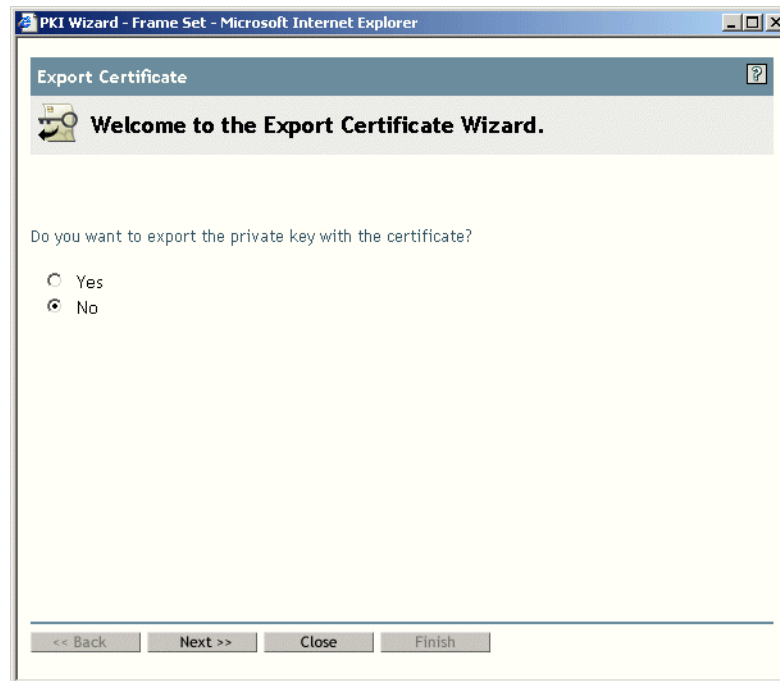
Exporting Root Certificates from the Server Certificate

- 1 Click Modify Object under Novell eDirectory Administration

Figure 36 Modify Object



- 2** Select Single Object, then specify the name of the object. This object is the server certificate itself.
- 3** Click OK.
- 4** Click Certificates, then select Trusted Root Certificate and view the details of the certificate.
- 5** Click Export, then click OK to launch the Certificate Export Wizard.

Figure 37 Export Certificate Wizard

6 Select the option button, depending on whether you want to export the key or not.

7 Select the Binary DER format or the Base64 format.

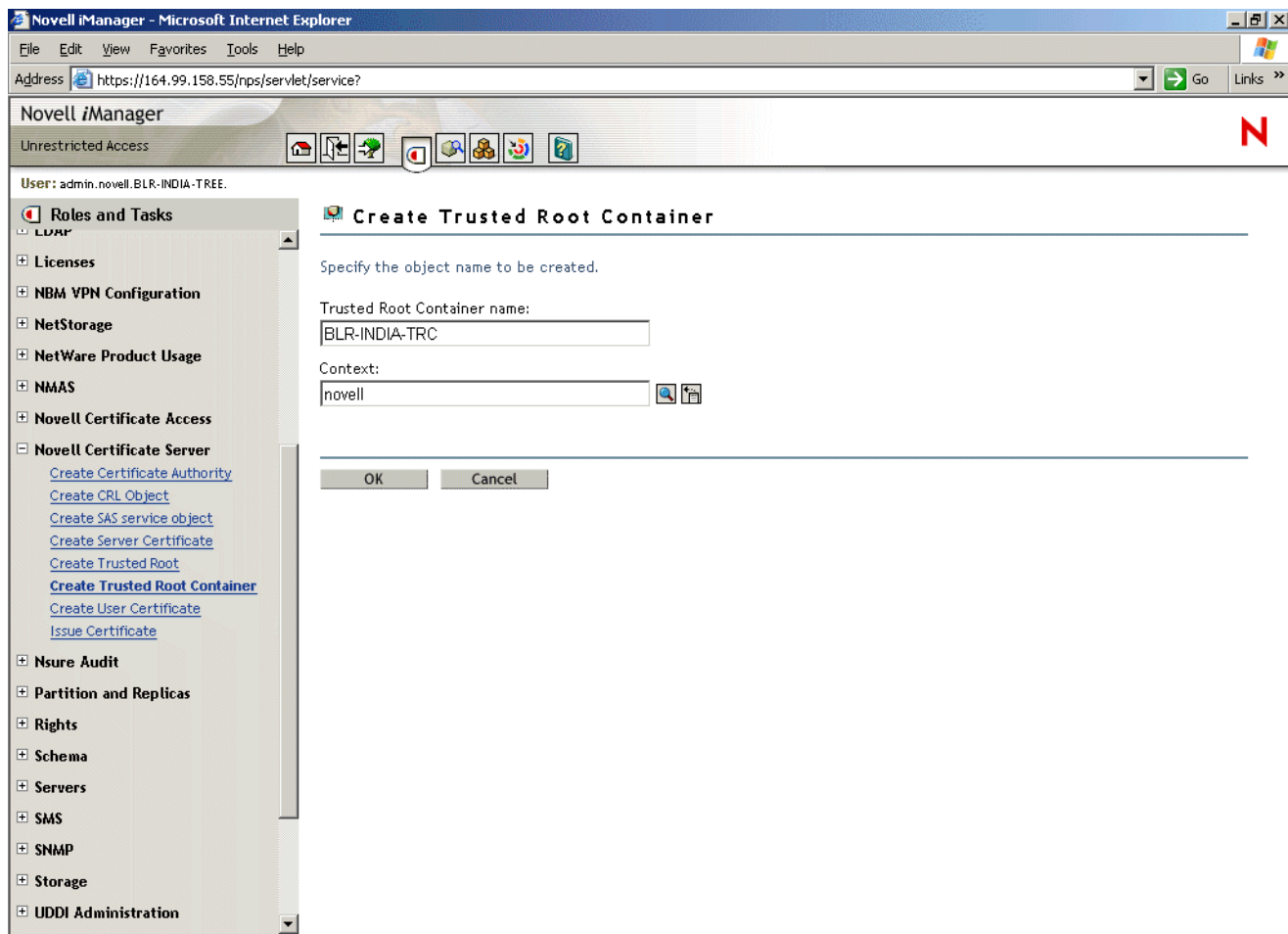
The next page displays a message indicating the export was successful and prompts you to save it as a file or not.

If you choose to save the certificate, you are prompted to save it on the local machine.

Creating Trusted Root Containers

1 Click Create Trusted Root Containers under Novell Certificate Server.

Figure 38 Create Trusted Root Container



2 Specify the Trusted Root Container name and context, then click OK.

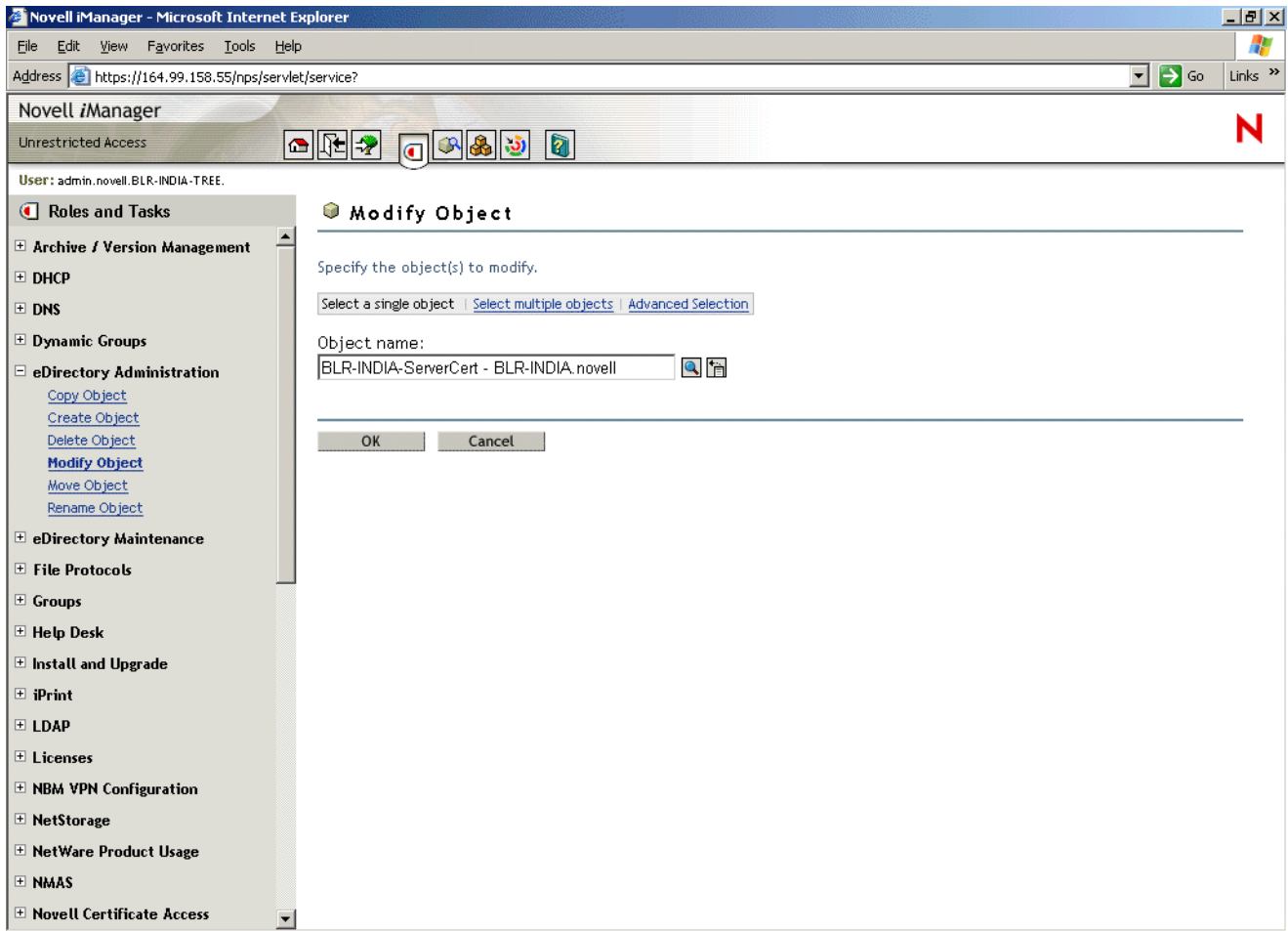
In the next page, you can create new containers or modify existing containers.

Creating the Trusted Root Object

1 Click Modify Object under eDirectory Administration.

Select the Server Certificate.

Figure 39 Modify Object



- 2 Specify the certificate name, the container, and the complete location of the file you exported in [“Exporting Root Certificates from the Server Certificate” on page 169](#), then click OK.

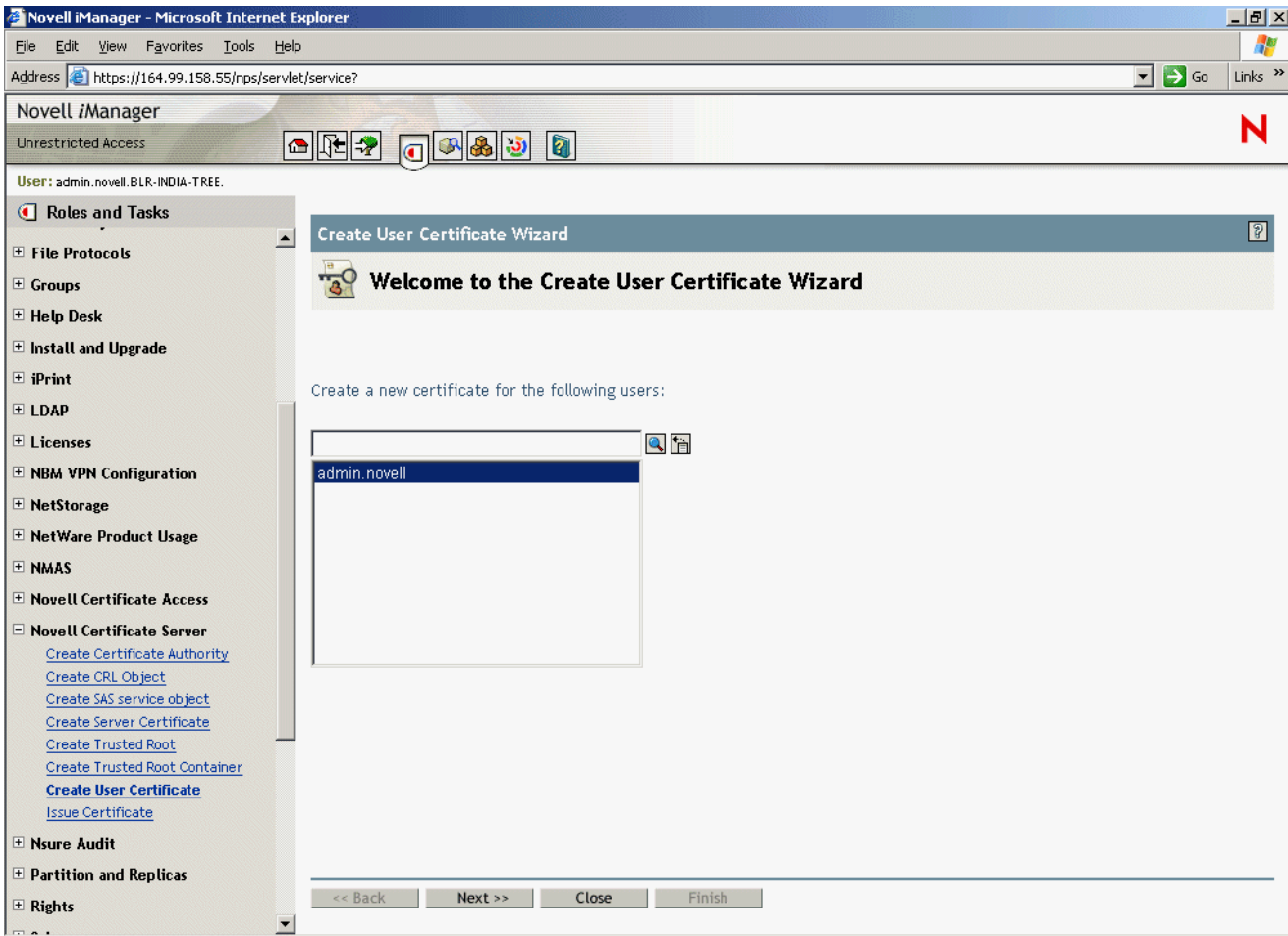
The next page will show the successful creation of the certificate.

Creating a User Certificate

Before you begin, ensure that you have administrative or equivalent rights for creating user certificates.

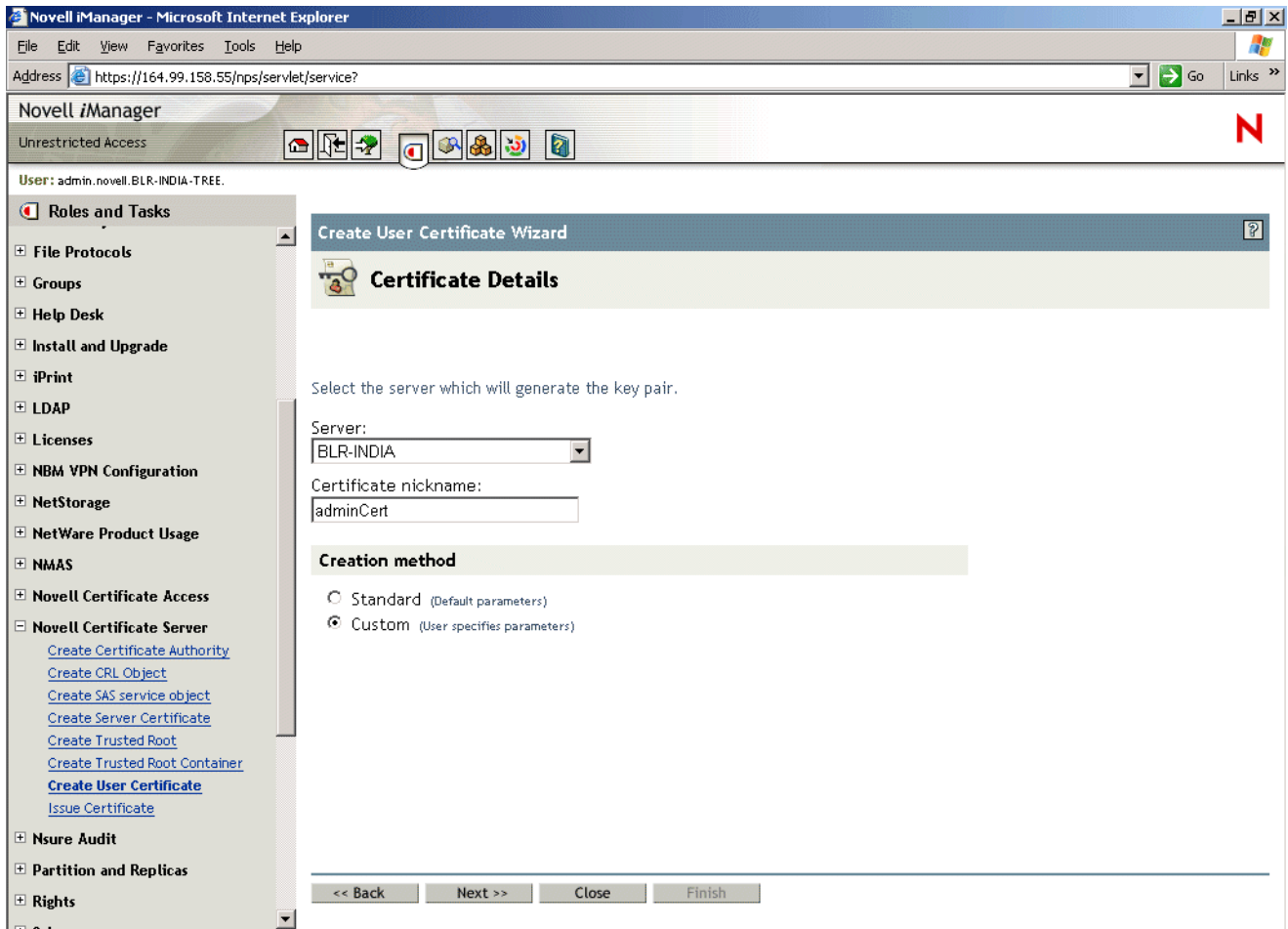
- 1 Click Create User Certificate under Novell Certificate Server.

Figure 40 Create User Certificate Wizard



2 Click Browse to find the user for whom you are creating the certificate.

Figure 41 Certificate Details



- 3 Specify the name of the server and the nickname for the certificate. Select the option button according to whether you want to specify parameters (Custom) or whether you want the certificate to have default parameters (Standard).
- 4 Specify the Key Size (2048) and Usage details, then click Next.
- 5 Specify the Certificate parameters and click Next.
- 6 The summary page shows you the summary of the certificate you just created. If the information is correct, click Next. If it is not correct, click Back and modify any details as necessary.

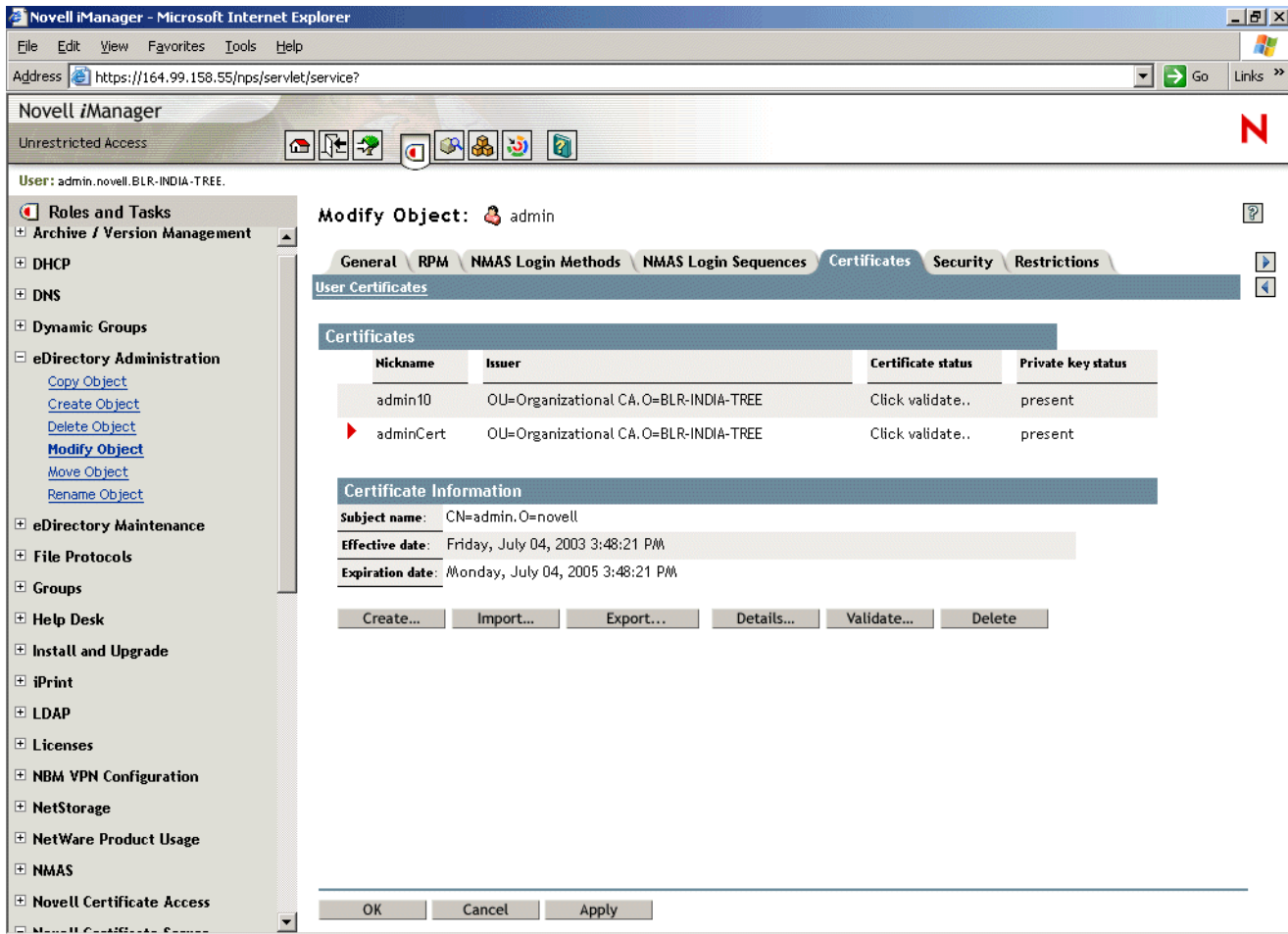
The user certificate will be created and you see a Success message.

Exporting User Certificates

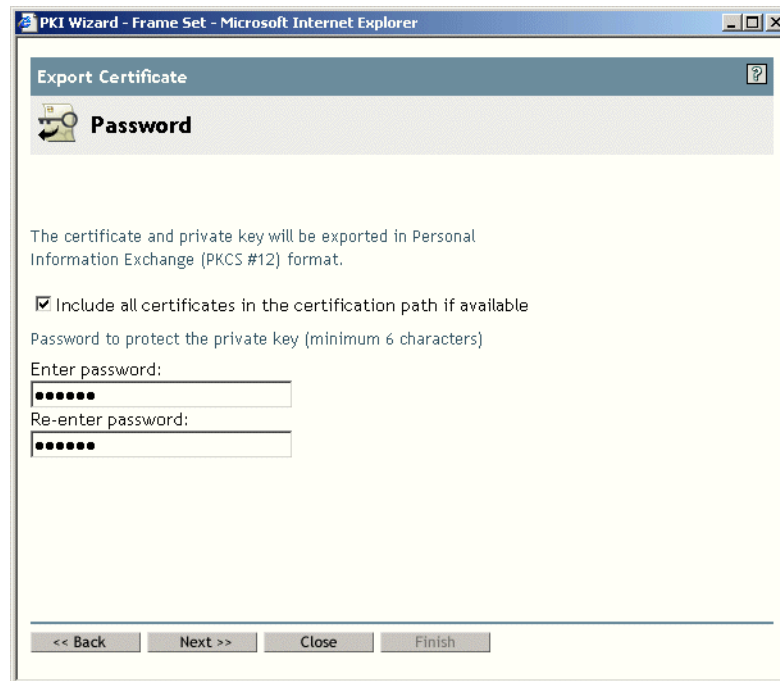
- 1 Click Modify Object under Novell eDirectory Administration, then select Single Object and then select specific User Object or specify the object distinguished name.

NOTE: To export the private key with the user certificate, log in as the same user in iManager.
- 2 On the next page, select the Certificates tab.

Figure 42 Modify Object: Certificates



- 3 Click Export, then click Ok to launch the Certificate Export Wizard.
- 4 Mark the options according to whether you want to export the key or not. If you chose to export the personal key, provide the password.

Figure 43 Password for Export Key

- 5** The next page displays a message indicating the export was successful, and prompts you to save it as a file or not.
- 6** If you choose to save the certificate, you are prompted to save it on the local machine.

Third-Party Certificate Server

If you are using a third-party server for certificate validation, the following items are to be configured manually:

- ◆ Key Size: 2048 bits
- ◆ Key Type: Unspecified, Encryption, Signature, SSL or TLS
- ◆ Key Usage: Data Encipherment, Key Encipherment or Digital Signature. All three are needed.

If the certificate issue path is `server_certificate > intermediate_certificate > trusted_root_certificate`, the intermediate server certificate along with the certificate chain (the public key certificate as well as the trusted root certificate of the intermediate certificate) should be imported into the TRO, and this should be configured as the issuer. The same holds for the client issuer name list, which is specified in the authentication rules.

17

Configuring VPN Services

The new VPN server software for Novell® BorderManager® 3.8 is based on Novell iManager 2.0.1. This change is significant and overrides all earlier versions of the software. The VPN services provide extensive facilities to set up and configure site-to-site and client-to-site services. Configure the VPN server before configuring the client-to-site or site-to-site services.

- ♦ “Setting Up VPN Services” on page 179
- ♦ “VPN Server Configuration” on page 179
- ♦ “Virtual Private Network Prerequisites” on page 183
- ♦ “Client-to-Site Configuration” on page 191
- ♦ “Attaching a Client-to-Site Service to the VPN Server” on page 205
- ♦ “Site-to-Site Configuration” on page 207
- ♦ “VPN Policy” on page 218

IMPORTANT: The software does not validate individual entries in the fields, so make sure your entries are correct and validate them manually. Also not all the diagrams presented have consistent server names and IP addresses. The naming is merely indicative and not to be followed in absolute terms.

Setting Up VPN Services

- 1** Log in to iManager-based VPN Services. On a Windows XP or 2000 machine connected to a NetWare® server, go to (<https://ipaddress/nps/iManager.html>). Here the *ip address* is the IP address of a NetWare 6 or NetWare 6.5 server running Novell BorderManager 3.8.
NOTE: You can run iManager from a NetWare server to configure other Novell BorderManager 3.8 servers.
- 2** Type the username and password, then click Login. The username and password are the Novell eDirectory™ login details. Specify the non-fully-distinguished name.
- 3** In the left pane, click the NBM VPN Configuration role to see the three kinds of configuration options available.
 - ♦ NBM VPN Server Configuration: Click this to set up the server as a VPN server.
 - ♦ VPN Client-to-Site Configuration: Click this to configure client-to-site services. You can also configure a new client-to-site service.
 - ♦ VPN Site-to-Site Configuration: Click this to modify or delete site-to-site services. You can also configure a new site-to-site service.

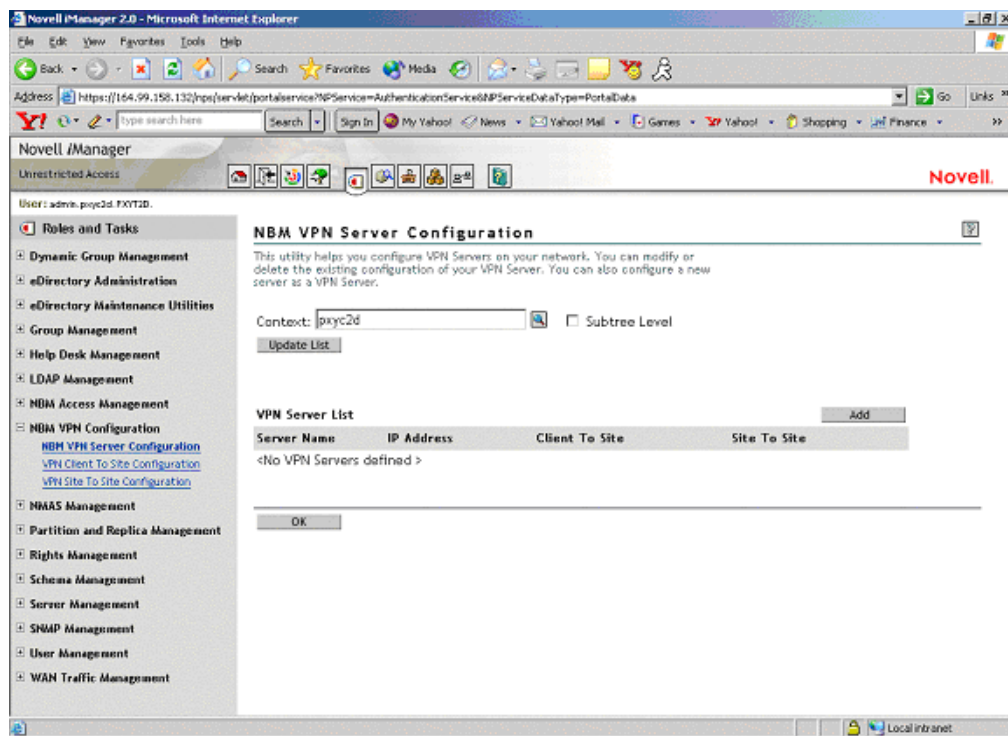
VPN Server Configuration

The VPN server can be used to modify or delete existing configuration. You can also configure a new server as a VPN server. The pre requisites to configuring a VPN server are:

- ◆ Trusted Root Container (TRC, referred to as Trusted Root in the iManager and in Novell eDirectory). If you want to create the Container see [“Creating Trusted Root Containers” on page 171](#). If you want the VPN configuration utility to create the Container automatically, skip the Creating Trusted Root Containers section.
- ◆ Key Material Object (KMO) for the server. If you want to create the KMO manually, see [“Creating Server Certificates” on page 164](#), and export the KMO using the steps in [“Exporting Root Certificates from the Server Certificate” on page 169](#). If you want the VPN configuration to create the KMO automatically, you need not refer to Creating Server Certificates, but after it is created you need to export it using the steps in [“Exporting Root Certificates from the Server Certificate” on page 169](#).
- ◆ Trusted Root Object (TRO) under the Trusted Root Container see [“Creating the Trusted Root Object” on page 172](#).

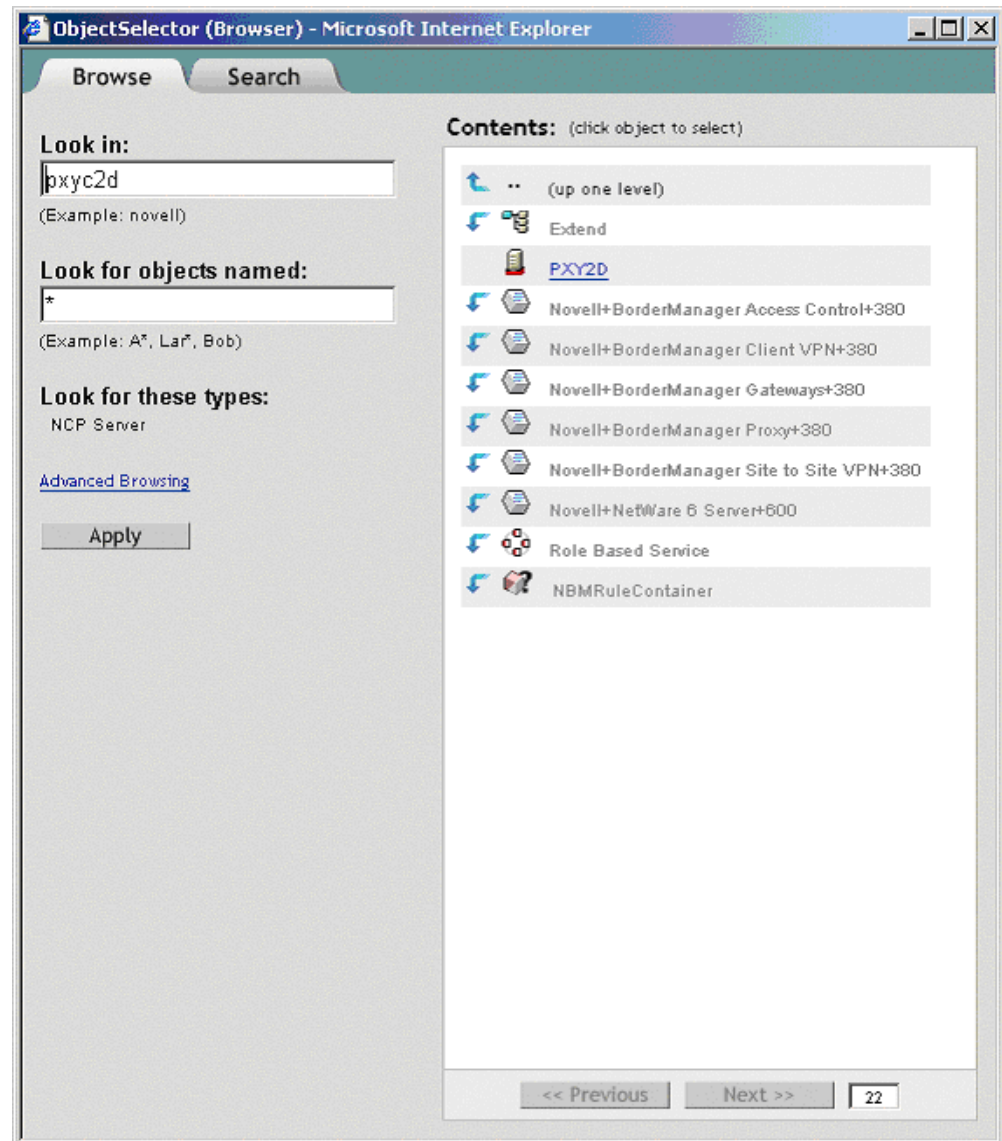
Click the NBM VPN Server Configuration role to display the following page:

Figure 44 NBM VPN Server Configuration



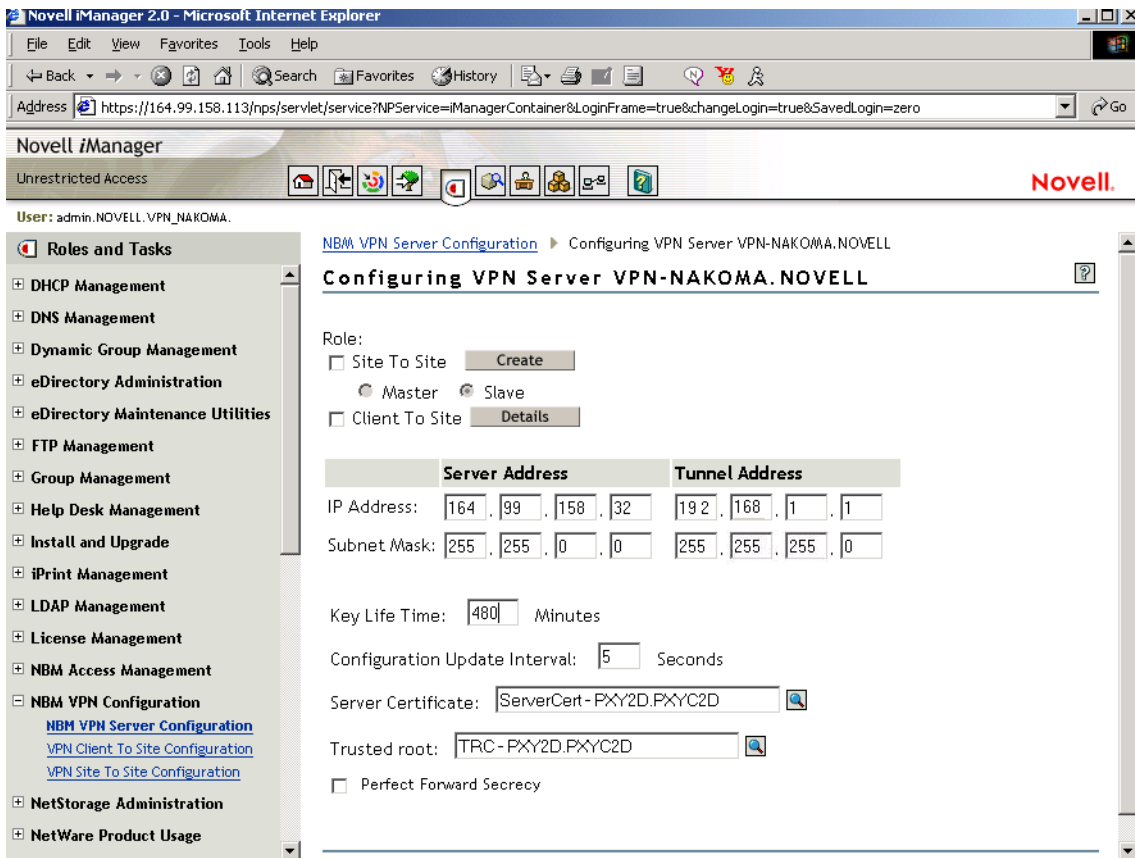
- 1 The page is currently blank. The list of VPN servers is empty until a VPN server is configured. After a server is added, the list shows the server, its IP address, and whether it is hosting a client-to-site or a site-to-site service. Use the Context text box to select the Novell eDirectory context in which you would want to view the already configured VPN servers. Select Subtree Level for a detailed context check. The Subtree Level search shows all VPN servers residing in all subcontexts. To change the context, click the Browse button and select the context. After selecting the context, click Update List. Click Add to add a VPN server.
- 2 Click the Browse button next to the field and choose a server in the tree.

Figure 45 VPN Server Selection



- 3 Select a server from the list (it should be one of the underlined objects), then click Next. The selected server is reflected on the original page.

Figure 46 VPN Server Page



4 Specify the details on the next page.

- ◆ **IP Address and Subnet Mask (Server):** Public IP address and subnet mask of the VPN server. This is the public IP address bound to the NetWare server.
- ◆ **IP Address and Subnet Mask (Tunnel):** Novell BorderManager 3.8 server's virtual tunnel IP address and subnet mask. This should have an encrypted tunnel and not a real IP address bound to an interface.
- ◆ **WAN Client IPX Network Address:** Specifies the IPX™ network address that dialing clients will use for IPX connectivity. This is applicable only when you select the client-to-site check box.
- ◆ **Key Life Time:** The IKE Key Life Time in minutes. The default is set to 480 minutes. This is the lifetime for which the IKE key is valid. If the time period is reduced, the overhead increases and the performance is impacted. However, it provides higher security.
- ◆ **Configuration Update Interval:** The interval at which the VPN server will look for updates to the configuration.
- ◆ **Server Certificate:** Use the default value if you want to automatically create and use the server certificate (Key Material Object). If you want to use a server certificate that you have already created using the steps in **“Creating Server Certificates” on page 164**, select the Key Material Object from Novell eDirectory by using the Browse button.
- ◆ **Trusted Roots:** The Trusted Root Container object that will contain all the Trusted Root objects for this VPN Server. Use the default value if you want to automatically create and

use the Trusted Root Container. If you want to use a Trusted Root Container that you have already created using the steps mentioned in [“Creating Trusted Root Containers” on page 171](#), select the Trusted Root Container for eDirectory using the Browse button (trusted root is one of the underlined items).

- ◆ **Perfect Forward Secrecy:** Indicates whether to enable or disable PFS in IKE Quick Mode. Enable this if you want higher level of security of IKE keys. For more information, refer to RFC: 2409.
- ◆ **Trusted Master Server Certificate Subject Name:** Specify the certificate subject name of the trusted master. If the master is in the same tree as the slave, browse to select the master's certificate instead of entering the certificate subject name.

NOTE: : If the VPN server is assigned a site-to-site role and is acting as a slave, the trusted master for this slave needs to be configured. The Trusted Master Server Certificate Subject Name field will be visible.

- 5** This page shows both the client-to-site and site-to-site services as disabled. These services are currently disabled on this VPN Server. To enable either or both of them, click the server name link.
- 6** Use the button with an X to delete a VPN server configuration from a particular Novell BorderManager 3.8 server.
- 7** Click the server name link to modify the VPN server information. When you modify a server, you can choose to either modify the VPN server parameters or you can enable (attach) a site-to-site or a client-to-site service.

TIP: The Synchronize feature is available when you modify VPN server information. Click Synchronize to reload the configuration information. The Synchronize feature saves the configuration information and increments or decrements the Configuration Update interval by a second.

VPN Server Behind NAT

The VPN server can also be configured behind NAT. To do so, use the nat.nlm shipped with Novell BorderManager 3.8. The nat.nlm is available in filtersv\system directory on the product CD. For more details on NAT, see [Chapter 21, “Setting Up NAT,” on page 249](#).

In case of static NAT, the site-to-site tunnel cannot be established between Novell BorderManager 3.7 and Novell BorderManager 3.8. So once the server is behind NAT all SKIP capabilities of that server will not work.

Shipping versions of NetWare 6.5 do not work properly if they are not patched with the bsdsock.nlm version 6.51o or later for NetWare 6.5. The domestic stack that is available in the Companion CD resolves this issue.

Virtual Private Network Prerequisites

Before you start to set up the VPN component of the Novell BorderManager 3.8 software, you must meet the prerequisites described in this section.

This section contains the following topics:

- ◆ [“Site-to-Site VPN Prerequisites” on page 184](#)
- ◆ [“Client-to-Site VPN Prerequisites” on page 185](#)
- ◆ [“Setting Up VPN Filters” on page 185](#)
- ◆ [“On VPN Master Site” on page 187](#)

- ♦ [“On VPN Slave Site” on page 188](#)
- ♦ [“Exceptions required to keep a Client-toSite and a Site-to-Site Connection Up” on page 190](#)

Site-to-Site VPN Prerequisites

Before you set up a site-to-site VPN, your network must meet the following requirements:

- ♦ The NetWare routing software must be installed and configured on each VPN server. Configuring the routing software includes, but is not limited to, setting up the LAN or WAN links to the other VPN members, and configuring static or dynamic routing for Internet Packet Exchange™ (IPX) and IP packets.

Verify connectivity between your VPN servers as required by your selected VPN topology. Any associated firewall software should be configured and connectivity should be verified before the VPN software is installed and before each VPN server is attached to the private networks it will protect.

- ♦ If your VPN sites are not on the same intranet, each VPN server must have a connection to the Internet, either directly or indirectly. If your VPN server is connected directly to the Internet, obtain the public IP address provided by your Internet Service Provider (ISP) to use when connecting to the Internet. Each VPN server uses the public IP address to exchange encrypted information with other VPN servers.

Obtain the public IP address before you set up the VPN. The ISP connection should also be tested before the VPN software is installed and before the VPN server is attached to any private networks. In the case of an intranet VPN, an ISP connection is not required.

- ♦ If your VPN server is connected directly to the Internet, you must obtain a permanent IP address for the ISP connection.
- ♦ The VPN server must have only one connection to the Internet. Otherwise, you risk sending and receiving your confidential data unencrypted if your data is routed to the other connection.
- ♦ If you are configuring a VPN server for the first time in an NDS® or Novell eDirectory tree, you must be able to log in to the server's NDS or eDirectory tree with administrative rights in order to extend the Server object schema.
- ♦ If the VPN server is also the firewall machine that protects your private network from the Internet, select the Setup Novell BorderManager 3.8 for Secure Access to the Public Interface option during the initial Novell BorderManager 3.8 installation and configuration. Otherwise, load BDRCFG to configure the required filters.
- ♦ If your VPN server is behind a firewall, be sure to configure the firewall with the proper packet forwarding filters, as determined by your security policy.

If the firewall is also running the Novell BorderManager 3.8 software, select the Setup Novell BorderManager 3.8 for Secure Access to the Public Interface option during the initial Novell BorderManager 3.8 installation and configuration to automatically configure firewall filters.

These firewall filters must then be altered as determined by your security policy. In general, the filters must be altered to allow VPN members to communicate with each other and allow encrypted packets to pass through. Refer [“Setting Up VPN Filters” on page 185](#).

The filters listed in can be used as a guideline for how the firewall filters should be altered for VPN. The filters might also have to be altered to allow communication with other Novell BorderManager 3.8 services.

The firewall filters can also be configured after installation by loading BDRCFG. If the firewall is not running the Novell BorderManager 3.8 software, you must configure these

filters manually as described in the documentation provided with the third-party firewall product.

- ◆ If you have set up two VPN servers on the same network, or the hop count between the two VPN servers is one, you must use FILTCFG to prevent all private network routes from being advertised through the public interfaces.
- ◆ If your network uses Open Shortest Path First (OSPF) dynamic routing, your VPN server must be located on a pure OSPF backbone area.

Client-to-Site VPN Prerequisites

Before you install the VPN client software, verify that the following pre requisites have been met:

- ◆ The workstation must be running Windows 98, Windows 2000, Windows XP, Windows Me or Windows NT.
- ◆ If the VPN client will be using a dial-up connection, Microsoft Dial-Up Networking must be installed before installing the VPN client software. Refer to the VPN client Readme for limitations.
- ◆ If you are using the VPN client with the Novell Client™ software, Novell Client version 4.83 or later is recommended.
- ◆ If you are using the VPN LAN client, you must have an Ethernet adapter.
- ◆ If you are using Windows NT, you must use an Intel-based workstation. The VPN client does not support Alpha workstations.
- ◆ If you are using Windows NT, use the latest support pack Windows NT SP4.
- ◆ If you are using Windows NT, you must log in to Windows NT as a user with administrative rights in order to install the VPN client.
- ◆ The VPN server must have only one connection to the Internet. Otherwise, you may risk sending and receiving your confidential data unencrypted if your data is routed to the other connection.
- ◆ If your VPN server is behind a firewall, be sure to configure the firewall with the proper packet forwarding filters, as determined by your security policy. If the firewall is also running the Novell BorderManager 3.8 software, select the Setup Novell BorderManager 3.8 for Secure Access to the Public Interface option during the initial installation and configuration to automatically configure firewall filters.

These firewall filters must then be altered as determined by your security policy. In general, the filters must be altered to allow VPN clients to communicate with the server and allow encrypted packets to pass through. The filters listed in the following table can be used as a guideline for how the firewall filters should be altered. The filters might also have to be altered to allow communication with other Novell BorderManager 3.8 services.

The firewall filters can also be configured after installation by loading BDRCFG. If the firewall is not running the Novell BorderManager 3.8 software, you must configure these filters manually as described in the documentation provided with the third-party firewall product.

Setting Up VPN Filters

These tables provide details on exceptions required for a Novell BorderManager 3.8 in a BorderManager server to keep different types of VPN connections up.

Client-to-Site

Source Address	Source Port (Service Type)	Destination Address	Destination Port (Service Type)	Protocol
Any	Any	Public IP Address	353 (VPN-AuthGW-st)	TCP(6)
Any	Any	Public IP Address	353 (VPN-KeepAlive)	UDP(17)
Any	Any	Public IP Address	(VPN-SKIP)	SKIP(57)*
Any	Any	Public IP Address	(ESP-st)	ESP(50)
Any	Any	Public IP Address	500 (IKE-st)	IKE(UDP)

Site-to-Site

Source Address	Source Port (Service Type)	Destination Address	Destination Port (Service Type)	Protocol
Public IP Address	Any	Any	213 (ipx/tcp-st)	TCP(6)
Any	Any	Public IP Address	(VPN-SKIP)	SKIP(57)*
Public IP Address	Any	Any	(VPN-SKIP)	SKIP(57)*
Any	Any	Public IP Address	2010 (VPTUNNEL-st)	UDP(17)
Public IP Address	Any	Any	2010 (VPTUNNEL-st)	UDP(17)
Any	Any	Public IP Address	213 (ipx/tcp-st)	TCP(6)
Any	Any	Public IP Address	(ESP-st)	ESP(50)
Public IP Address	Any	Any	(ESP-st)	ESP(50)
Any	Any	Public IP Address	500 (IKE-st)	IKE(UDP)
Public IP Address	Any	Any	500 (IKE-st)	IKE(UDP)

Special cases: Behind NAT

S No	Source Address	Source Port (Service Type)	Destination Address	Destination Port (Service Type)	Protocol
1	Any	Any	Public IP Address	2010 (VPTUNNEL-st)	UDP(17)**
2	Public IP Address	Any	Any	2010 (VPTUNNEL-st)	UDP(17)**
3	Public IP Address	Any	Any	4500 (IKE-NAT-st)	IKE-NAT-ST
4	Any	Any	Public IP Address	4500 (IKE-NAT-st)	IKE-NAT-ST

* Required only for backward compatibility with Novell BorderManager 3.7 VPN servers.

** Required only for backward compatibility with Novell BorderManager 3.7 VPN servers for client-to-site connections.

Serial number 3 & 4 are applicable when servers are behind NAT in a site-to-site connection, they are required in place of destination port 500 (IKE-st) in the site-to-site table. Only serial number 4 is required when servers/client is behind NAT for a client-to-site connection, it is required in place of destination port 500 (IKE-st) in the client-to-site table.

NOTE: When IKE completes use KeepAlive port (udp 353) to indicate that the connection is through from the client side to the server side. It can also be used to indicate to the server that the connection timeouts have to be reset, whenever we start traffic from the client end. For these reasons, we will have to keep this port enabled, even for NMAS/IKE and even when keepalives are disabled.

On VPN Master Site

Following are the list of filters that need to be opened on the Firewall to allow the Incoming packets

Protocol ID	Source Address: Port	Destination Address: Port	Remarks
TCP(6)	Any: Any	Any: 353	NAT-ed and non-NAT-ed VPN clients connect to this port so as to authenticate the user to authgw.nlm. The destination address could be made more specific by specifying as the VPN public IP address.
TCP(6)	Any: 213	Any: Any	VP Slave responds to VP Master through this port after VP Master makes the connection on VP Slave at port 213. The destination address could be made more specific by specifying as the VPN public IP address.

Protocol ID	Source Address: Port	Destination Address: Port	Remarks
SKIP (57)	Any: Any	Any: Any	Allow any packets with protocol ID = 57. These are SKIP/IPsec VPN packets and IANA has assigned protocol ID of 57 for SKIP. This is for Site-to-Site as well as non-NAT-ed Client-to-Site tunnel.
UDP (17)	Any: Any	Any: 2010	The VPN sites communicate over this UDP port to handshake a VPN connection disconnect. NAT-ed Client-to-Site uses this port for tunnel. The destination address could be made more specific by specifying it as the VPN public IP address.
UDP (17)	Any: Any	Any: 353	This port is used by the (NAT-ed and non-NAT-ed) VPN client and authentication gateway (authgw.nlm) for keep alive and disconnect packets.

Following are the list of filters that need to be opened on the Firewall to allow the Outgoing packets.

Protocol ID	Source Address: Port	Destination Address: Port	Remarks
TCP(6)	Any: 353	Any: Any	Authgw communicates with (NAT-ed and non-NAT-ed) VPN clients over this port during the authentication of the user. The VPN client first connects to authgw on this port. The source address could be made more specific by specifying as the VPN public IP address.
TCP(6)	Any: Any	Any: 213	VP Master connects to VP Slave on this port to resynchronize or receive activity updates. The source address could be made more specific by specifying as the VPN public IP address.
SKIP (57)	Any: Any	Any: Any	Allow any packets with protocol ID = 57. These are SKIP/IPsec VPN packets and IANA has assigned protocol ID of 57 for SKIP. This is for Site-to-Site as well as non-NAT-ed Client-to-Site Tunnel.
UDP (17)	Any: 2010	Any: Any	The VPN sites communicates over this UDP port to handshake a VPN connection disconnect. NAT-ed Client-to-Site uses this port for Tunnel. The source address could be made more specific by specifying as the VPN public IP address.
UDP (17)	Any: 353	Any: Any	This port is used by the (NAT-ed and non-NAT-ed) VPN client and authentication gateway (authgw.nlm) for keep alive and disconnect packets.

On VPN Slave Site

Following are the list of filters that need to be opened on the Firewall to allow the Incoming packets.

Protocol ID	Source Address: Port	Destination Address: Port	Remarks
TCP(6)	Any: Any	Any: 353	NAT-ed and non-NAT-ed VPN clients connect to this port so as to authenticate the user to authgw.nlm. The destination address could be made more specific by specifying as the VPN public IP address.
TCP(6)	Any: Any	Any: 213	VP Master connects to this port to communicate to VP Slave. VP Slave will be listening on this port. The destination address could be made more specific by specifying as the VPN public IP address.
SKIP (57)	Any: Any	Any: Any	Allow any packets with protocol ID = 57. These are SKIP/IPsec VPN packets and IANA has assigned protocol ID of 57 for SKIP. This is for Site-to-Site as well as non-NAT-ed Client-to-Site Tunnel.
UDP (17)	Any: Any	Any: 2010	The VPN sites communicate over this UDP port to handshake a VPN connection disconnects. Nated Client-to-Site uses this port for Tunnel. The destination address maybe made more specific by specifying as the VPN public IP address.
UDP (17)	Any: Any	Any: 353	This port is used by the (NAT-ed and non-NAT-ed) VPN client and authentication gateway (authgw.nlm) for keep alive and disconnect packets.

Following are the list of filters that need to be opened on the Firewall to allow the Outgoing packets

Protocol ID	Source Address: Port	Destination Address: Port	Remarks
TCP(6)	Any: 353	Any: Any	AUTHGW communicates with (NAT-ed and non-NAT-ed) VPN clients over this port during the authentication of the user. The VPN client first connects to authgw on this port. The source address could be made more specific by specifying as the VPN public IP address.
TCP(6)	Any: 213	Any: Any	VP Slave responds to VP Master on this port after VP Master connects to VP Slave listening on this port. The source address could be made more specific by specifying as the VPN public IP address.
SKIP (57)	Any: Any	Any: Any	Allow any packets with protocol ID = 57. These are SKIP/IPsec VPN packets and IANA has assigned protocol ID of 57 for SKIP. This is for Site-to-Site as well as non-NAT-ed Client-to-Site Tunnel.

Protocol ID	Source Address: Port	Destination Address: Port	Remarks
UDP (17)	Any: 2010	Any: Any	The VPN sites communicate over this UDP port to handshake a VPN connection disconnects. NAT-ed Client-to-Site uses this port for Tunnel. The source address maybe made more specific by specifying as the VPN public IP address.
UDP (17)	Any: 353	Any: Any	This port is used by the (NAT-ed and non-NAT-ed) VPN client and authentication gateway (authgw.nlm) for keep alive and disconnect packets.

Exceptions required to keep a Client-toSite and a Site-to-Site Connection Up

Source Address	Source Port (Service Type)	Destination Address	Destination Port (Service Type)	Protocol	Description
Any	Any	Public IP Address	353	TCP(6)	VPN-Authgw
Any	Any	Public IP Address	353	UDP(17)	VPN-Authgw
Any	213	Public IP Address	Any	TCP(6)	
Any	Any	Public IP Address	Any	SKIP(57) *	
Public IP Address	Any	Any	Any	SKIP(57) *	
Any	Any	Public IP Address	2010	UDP (17)	
Public IP Address	Any	Any	2010	UDP (17)	
Public IP Address	Any	Any	213	TCP(6)	
Any	Any	Public IP Address	Any	AH (51)	
Public IP Address	Any	Any	Any	AH (51)	
Any	Any	Public IP Address	Any	ESP (50)	
Public IP Address	Any	Any	Any	ESP (50)	
Any	Any	Public IP Address	500	IKE (UDP)	

Source Address	Source Port (Service Type)	Destination Address	Destination Port (Service Type)	Protocol	Description
Public IP Address	Any	Any	500	IKE (UDP)	
Public IP Address	Any	Any	4500	IKE-NAT-ST	
Any	Any	Public IP Address	4500	IKE-NAT-ST	

Client-to-Site Configuration

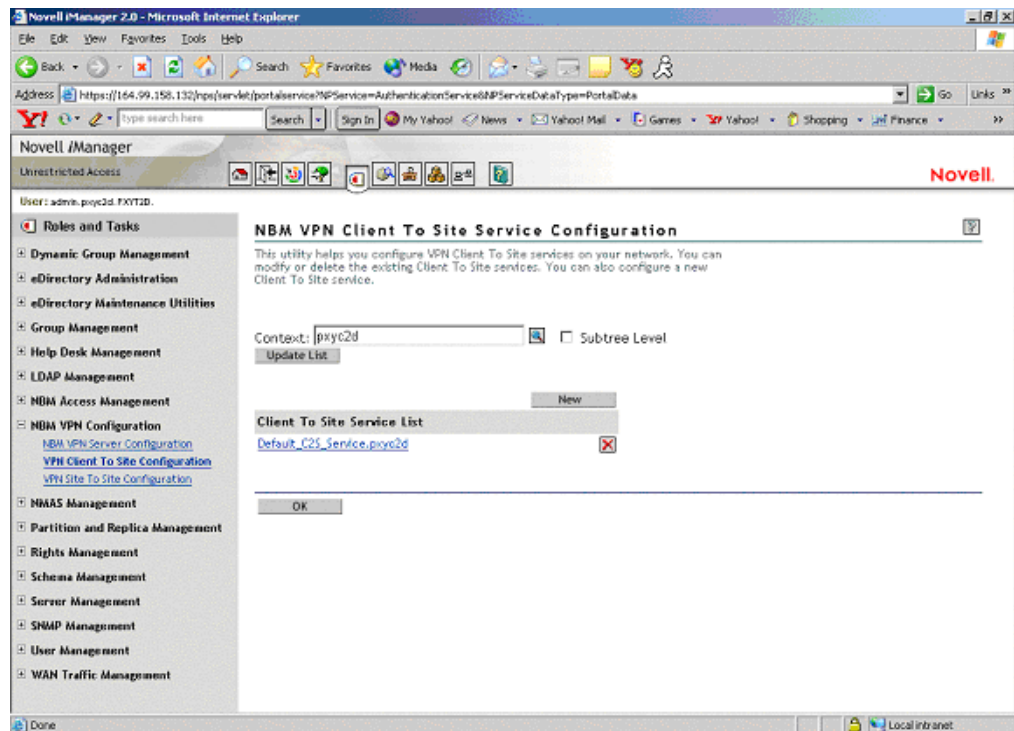
This utility helps you configure VPN client-to-site services on your network. You can modify or delete the existing client-to-site services. You can also configure a new client-to-site service.

Prerequisites:

- ◆ **Trusted Root Container:** The same as the server (on which you want to host the client-to-site service) trusted root container. Referred to as Trusted Root in the pages and in Novell eDirectory.
- ◆ **Server Trusted Root Object:** Under the Trusted Root Container mentioned above.

On this page you can view the configured client-to-site services. A default client-to-site service is created when you configure a server as a VPN Server.

Figure 47 New Client-to-Site Configuration



- 1 Use the Context list to select the Novell eDirectory context in which you want to view the already configured VPN client-to-site services. Select Subtree Level for a detailed context check. The Subtree Level search shows all VPN servers residing in all subcontexts. To change the context, click the Browse button and select the context. After selecting the context, click Update List.
- 2 Click New to add a new client-to-site service.
- 3 Click OK to go back to the main configuration page.

You can configure any one of the following parameters:

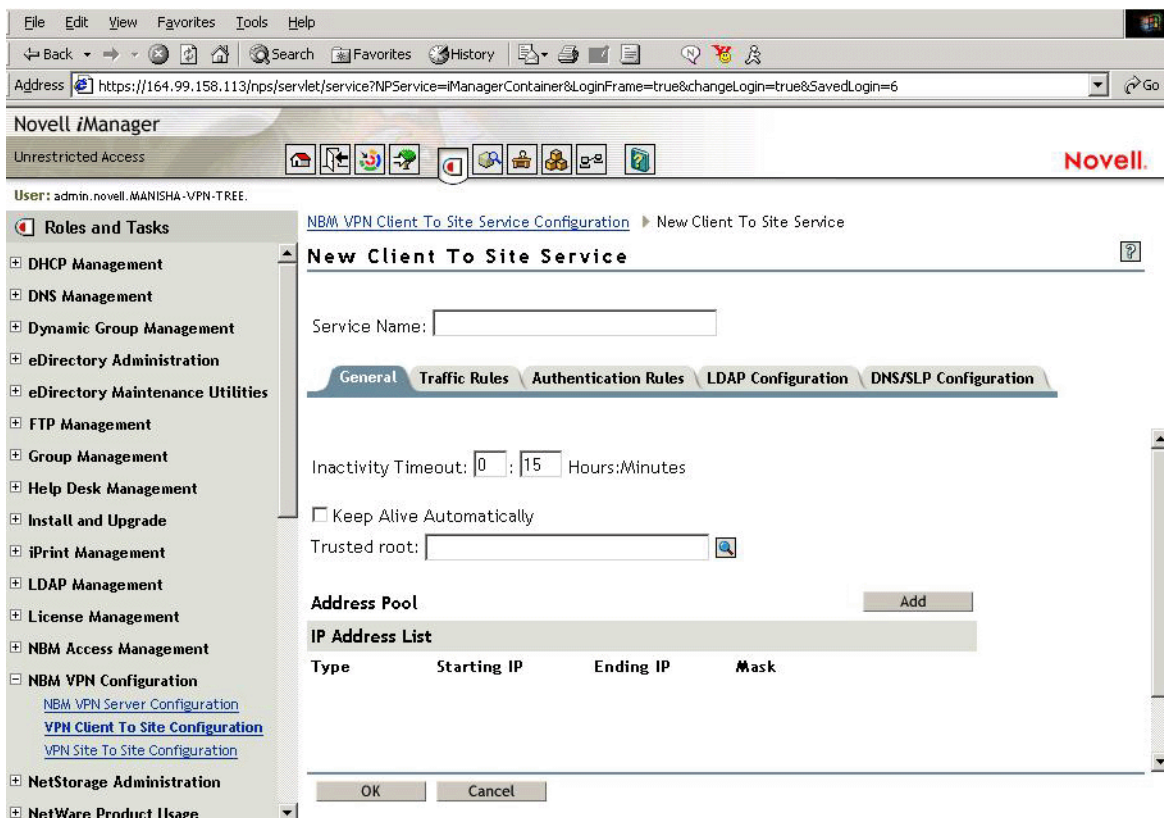
- ◆ “General” on page 192
- ◆ “Traffic Rules” on page 193
- ◆ “Authentication Rules” on page 199
- ◆ “Remote LDAP Configuration” on page 202
- ◆ “DNS/SLP Configuration” on page 203
- ◆ “Final Client-to-Site Page” on page 204

General

These are the general properties of the client-to-site service. Make sure to click Apply button if you’ve made any modifications to the general parameters.

The following illustration reflects the default values.

Figure 48 Default Values for a New Client-to-Site Service.



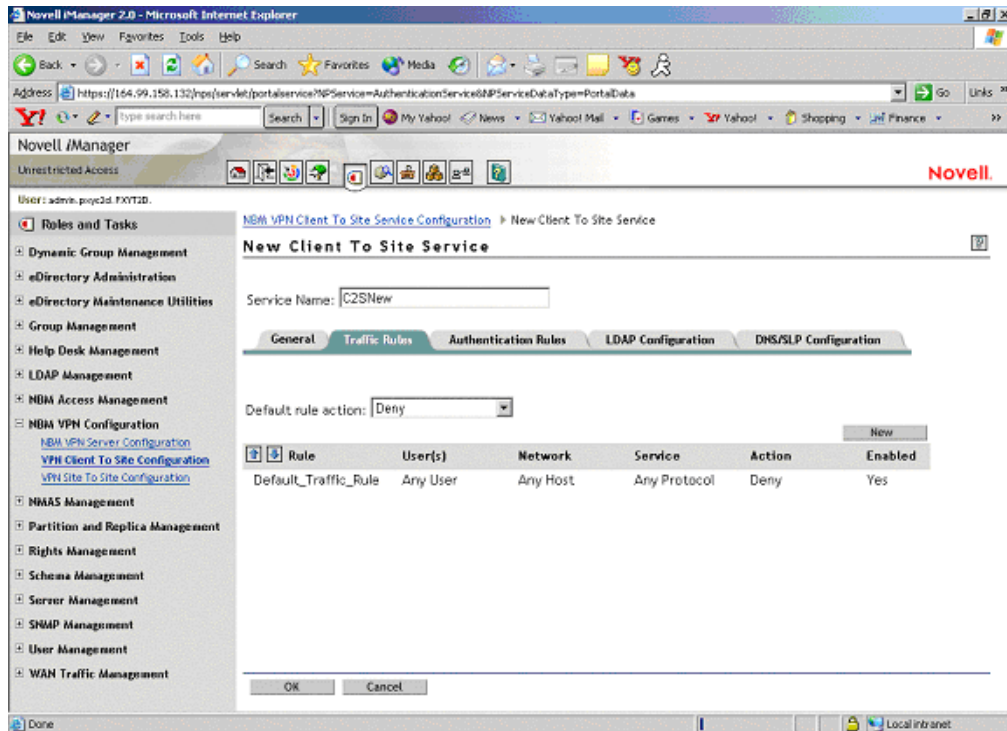
- 1** Choose the Trusted Root Container for the client-to-site service. You can configure one or more of the following:
 - ◆ **Inactivity Timeout:** Specifies amount of time that a connection to a VPN client remains up if no encrypted data is received by the server from the client. The default value is 15 minutes.
 - ◆ **Keep Alive Automatically:** A connection from a VPN client remains up indefinitely even if no data is sent or received. The default is Disabled. Enable this if you want to keep the connection alive indefinitely.
 - ◆ **Address Pool:** This is to assign a private address to the VPN client. The administrator must assign an address pool in the client-to-site service and this address pool should not fall within any protected network behind this server, or the tunnel IP assigned to the server. This facility avoids an IP address conflict for two different clients having same IP address while residing two different NATs. During a session, after the IP address assignment is done, the client can access resources beyond VPN server if these resources have the VPN server's IP address as their default gateway. At least one address pool entry needs to be configured. The default client-to-site is associated with a network range 1.0.0.0 - 255.0.0.0. This does not work if the address pool is assigned on the same subnet as the VPN server interface.
- 2** Specify the client-to-site service name, then click Apply if you have made any changes to the general parameters. Click OK if you want to save and exit this configuration.

Traffic Rules

Traffic Rules are policies that govern accessibility for a user through a VPN connection. You can add, modify, or delete traffic rules for the client-to-site service. You can also change the priority of a traffic rule by moving it the up or down the list. The traffic rule at the top of the list has the highest priority.

TIP: A default traffic rule is automatically created. The default action of this traffic rule is to deny all packets. You need to modify the action of this default traffic rule.

Figure 49 Expanded View



1 Click New to add a new traffic rule.

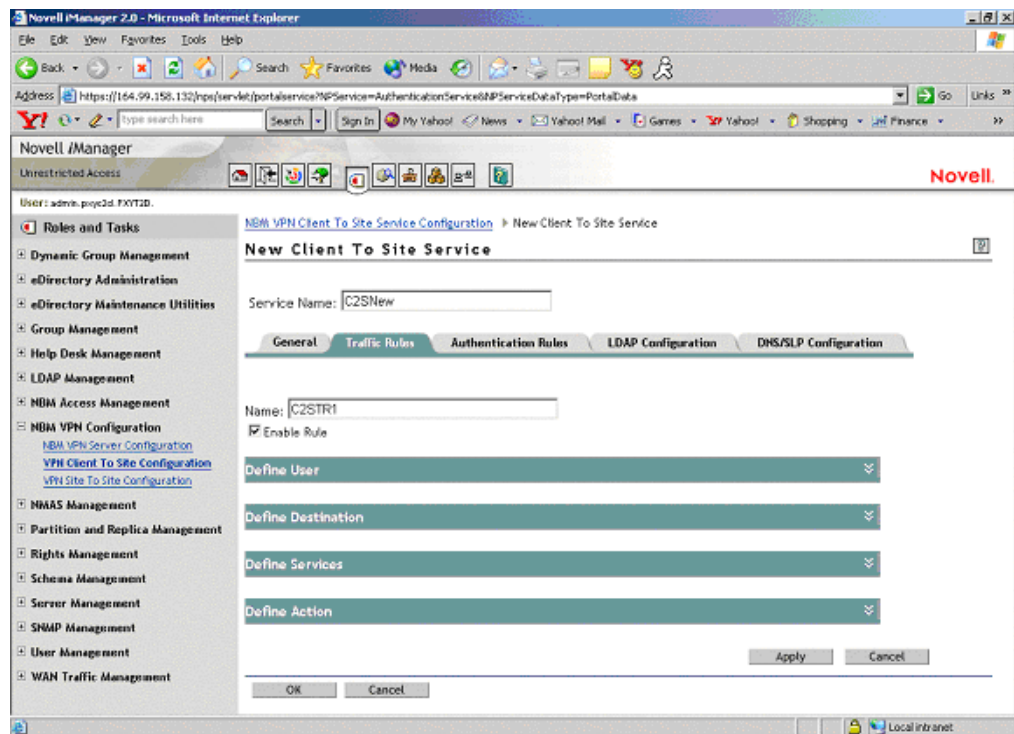
2 You can configure any one if the following in a traffic rule.

- ◆ **Define User:** Users to whom this traffic rule will apply.
- ◆ **Define Destination:** Destinations to which the rule will apply. These are the protected networks that can be reached.
- ◆ **Define Services:** Services to which the rule will be applied
- ◆ **Define Action:** Action that must be performed.

TIP: The service provides the facility to configure and store your entries as profiles that can be used later when you log in to the service.

On entering the name and expanding the up or down button, the following view is available.

Figure 50 Expanded View



On expanding each of the rules, the following can be configured.

- ◆ “Define User” on page 195
- ◆ “Define Destination” on page 197
- ◆ “Define Services” on page 197
- ◆ “Define Action” on page 198

Define User

Use this page to define the users to whom this rule will apply. Click Define User to see this page. The values shown on the page are the default values. You can modify them.

You can apply this rule to any user, or you can specify a list of users or certificate users.

If you want to select a user list to which you want to apply this rule, select the Only User List option button. You can create a list of users or certificate users. To add users, click Add. To add certificate users, click Add Certificate User. This service also provides for selection of user groups or a group of users with a shared context.

The following two kinds of users can be selected here:

- ◆ “A User” on page 195
- ◆ “A Certificate User” on page 196

A User

Click Add and select the user from the page. It should be one of the underlined items.

Click Browse to find the User. The User might be in a context. Click the Context down-arrow to search for a User within a context.

The page displays the user list after an Administrator user is selected from the list.

NOTE: This is for the NMAS-NDS user.

A Certificate User

Click Add Certificate User to open the dialog box.

TIP: Specify the Certificate Subject Name of the user. Subject Alternative Names can also be specified. Specify the same Certificate Subject Name that you provided while creating User Certificates in ConsoleOne.

The certificate subject name should be in the format cn=admin.o=novell or o=novell.cn=admin. For exact subject name, view the certificate subject name from the user certificate.

To view the certificate subject name go to ConsoleOne and right-click the User Object > Properties > Security > Certificate. Select the certificate from the list, then click Details.

Select the Add Another One check box if you want to add another Certificate User. Click OK. If you have selected the Add Another One check box, the same dialog box will appear again; if not, the next page is displayed.

LDAP User

The LDAP Group or User name allows the administrator to specify the user or group identities that are allowed to use the LDAP form of authentication for VPN. When the user authenticates using the LDAP mode, the LDAP NMAS™ method associates one of the configured user or group names from this list as the user's identity. If a user's name as well as his group name is present in the list, that username is selected as the identity. This list is unordered. Otherwise, if a user belongs to any of the groups in the list, that group name is chosen as the user's authenticating identity. Later, the authenticating identity will be compared against the traffic rules to match the policy to be applied for this client-to-site connection.

For example:

The client-to-site LDAP group or username list contains the following LDAP distinguished names:

cn=group1,o=xyz

cn=group2,o=xyz

cn=user1,o=xyz

The client-to-site traffic rules contains the following LDAP identity-based rules, in the following priority order:

Rule1: cn=group2, o=xyz - Encrypt

Rule2: cn=user1,o=xyz - Bypass

Rule3: cn=group1,o=xyz - Deny

If a user cn=user1,o=xyz (who is also a member of group1 and group2) authenticates, the identity is assigned as cn=user1,o=zyx, and the Rule2 is applied for traffic.

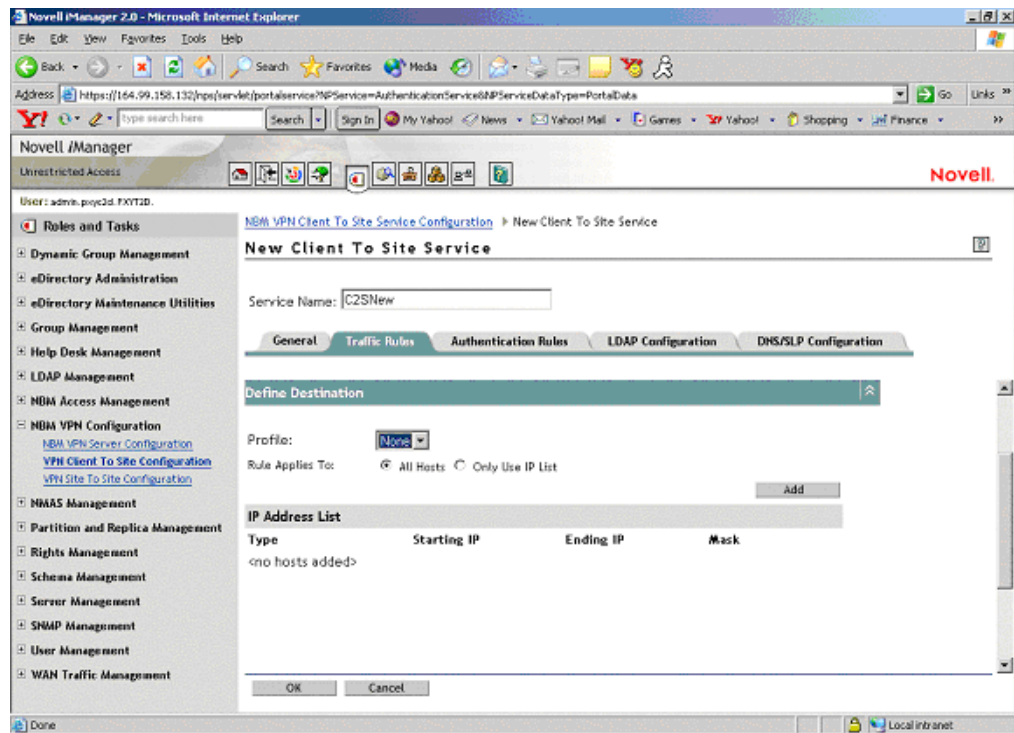
If a user cn=user2,o=novell (who is also a member of group1 and group2) authenticates, the identity is ascertained by comparing the user's groups with the LDAP group or user list during authentication. The one that matches is assigned as the identity. The same identity (either group1

or group2) is later used to select the traffic rule to be applied. If a user belongs to multiple groups, the identity might match the traffic rules based on any one of the groups.

Define Destination

Use this page to define destinations to which the rule will apply. Click Define Destination to see this page. The values shown on the page are the default values. You can modify them.

Figure 51 Traffic Rules



- ◆ You can apply this rule to any host or you can specify a list of address ranges or networks.
- ◆ If you want to select a destination IP Address List to apply this rule to, select the Only Use IP List option button. You can create a list of IP Address ranges or networks. Click Add to create a list.
- ◆ If you want to add a network to the destination list, select the network in the Type drop-down list and specify the network number (IP address) and subnet mask. Click OK.
- ◆ If you want to add a network to the destination list, select the network in the Type drop-down list and specify the start and end values for the range. Click OK.

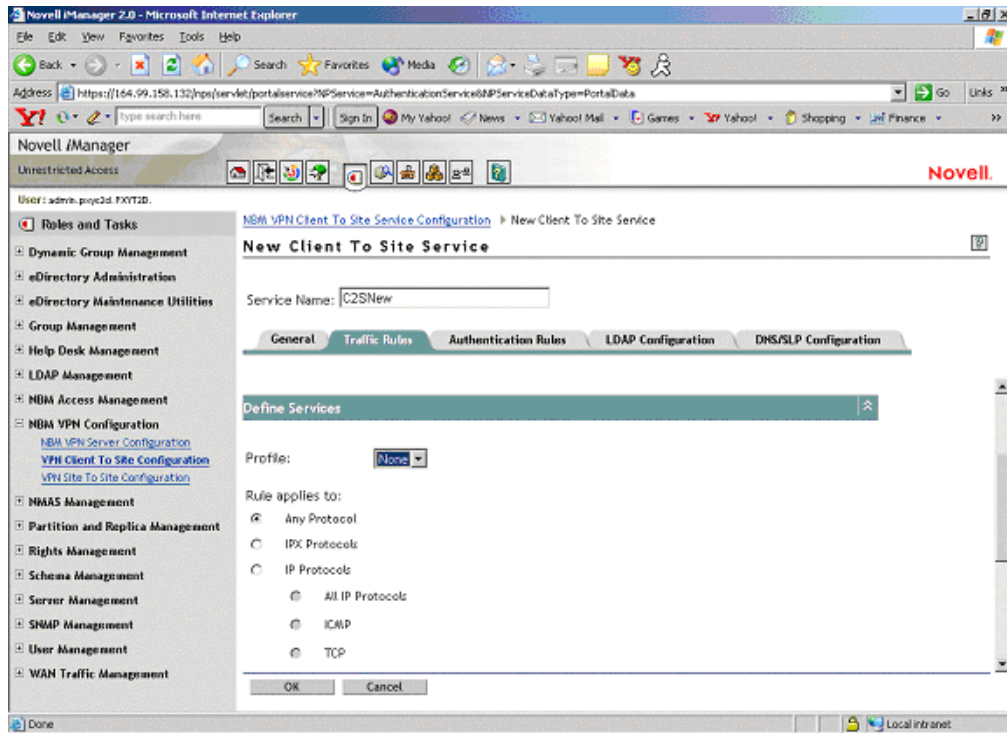
NOTE: You can specify only one address range or network entry per rule.

Define Services

Use this page to define the services to which the rule is applied.

Click Define Service to see this page. The values shown on the page are the default values. You can modify them.

Figure 52 Traffic Rules



The default service is Any Protocol. You can select the protocol to which the traffic rule is applied. For TCP protocols less than 1024, you can also specify the service port.

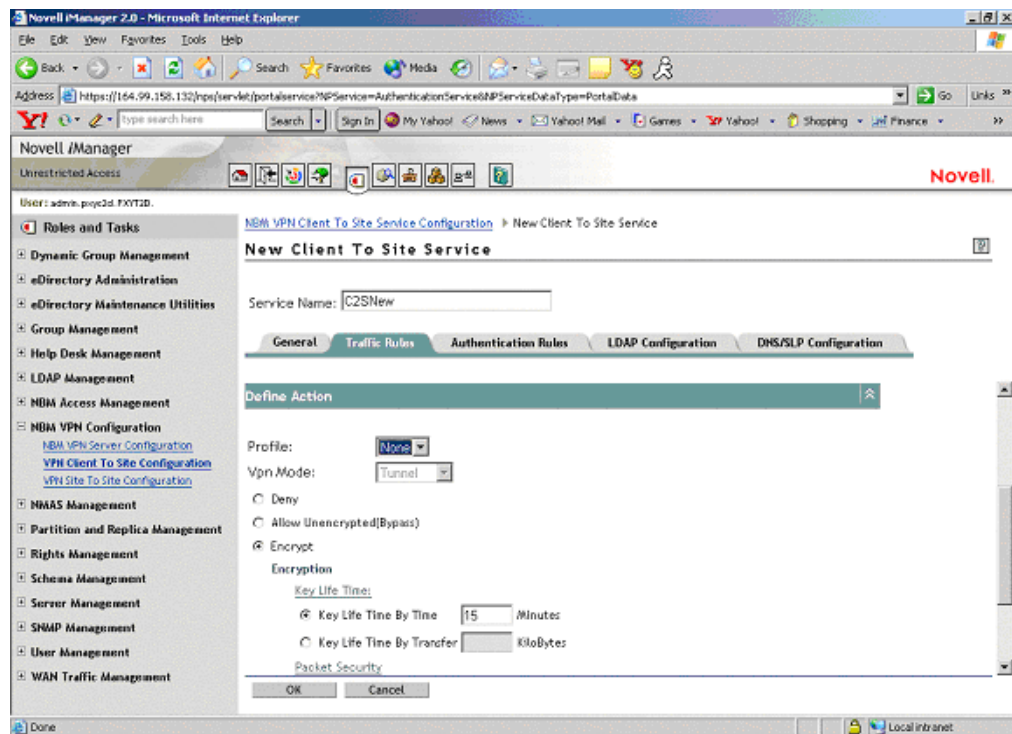
NOTE: You can specify one port at a time. If you want to set up more ports, specify new traffic rules for each port.

Define Action

Use this page to define the action that has to be performed.

Click Define Action to see this page. The values shown on the page are the default values. You can modify them.

Figure 53 Traffic Rules: Default Values



- ◆ Select Deny if you want to discard all packets that match this traffic rule. Select Allow Unencrypted if you want to bypass the tunnel for the packets that match this traffic rule. Select Encrypt if you want to encrypt the packets matching this traffic rule according to the encryption options that you have configured as shown in the next page.
- ◆ The default Action is Encrypt with an IKE key lifetime of 120 minutes. Default encryption and authentication algorithms are 3DES/HMAC-MD5.

You can choose to discard, bypass (allow unencrypted), encrypt the packets that match this traffic rule. If the action is Encrypt, you can also configure the encryption and authentication algorithms and the IKE lifetime.

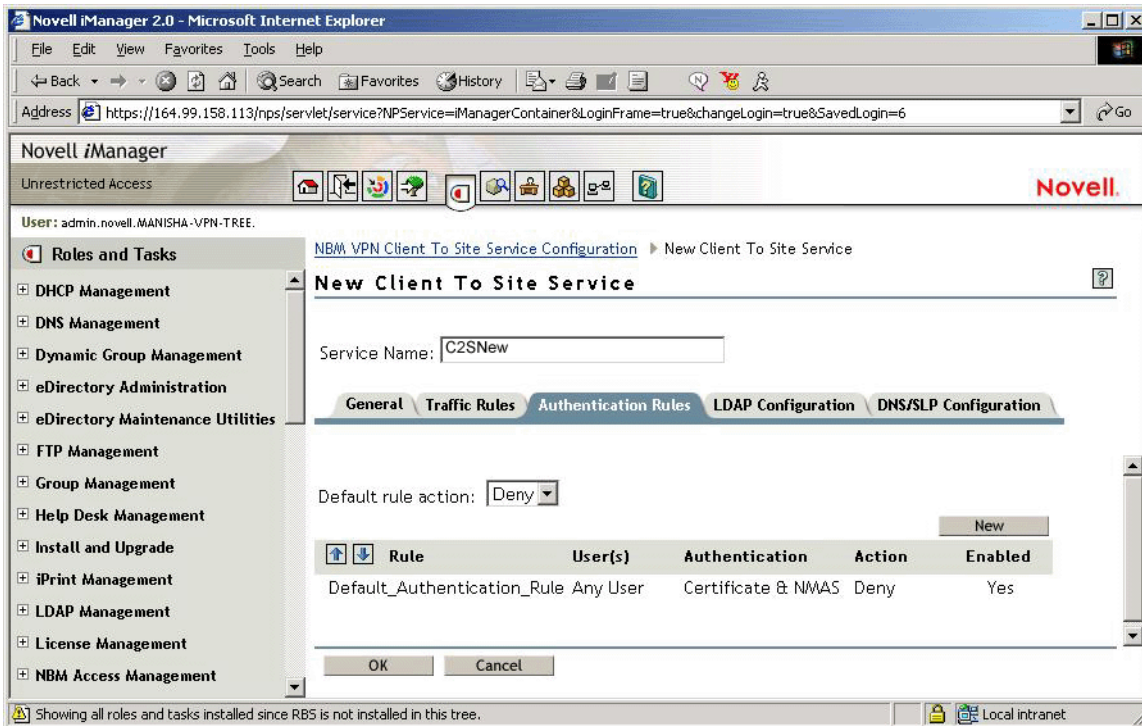
Authentication Rules

Authentication Rules are policies that govern authentication of a user to a VPN server.

You can add, modify, or delete authentication rules for the client-to-site service. You can also change the priority of an authentication rule by moving it up or down the list. The authentication rule at the top of the list has the highest priority.

TIP: A default authentication rule is automatically created. The default action of this authentication rule is to deny all users. The default authentication rule always has the lowest priority in the authentication rule list.

Figure 54 Authentication Rules



1 You can configure any of the following in an authentication rule:

- ◆ Users to whom this rule will apply.
- ◆ Type of authentication to be performed.
- ◆ Allow/Deny Action: If the action is set to Deny, the user cannot authenticate.

TIP: The service provides the facility to configure and store your entries as profiles that can be used later when you log in to the service.

2 Specify the name of the traffic rule. The following are discussed here:

- ◆ [“Define User” on page 200](#)
- ◆ [“Authentication Condition” on page 200](#)
- ◆ [“Allow/Deny Action” on page 201](#)
- ◆ [“Example of a Default NMAAS Configuration” on page 201](#)

Define User

Use this page to define the users to whom this rule will apply. Click Define User to see this page. The values shown on the page are the default values. You can modify them.

You can apply this rule to any user, or you can specify a list of users or certificate users. See Traffic Rules > Define User for details on this page.

Authentication Condition

Use this page to define the type of authentication to be performed. Click Authentication Condition to see this page. In Novell BorderManager 3.7, you could use `vpncfg` to verify the authentication data of the server shown during VPN client login. With Novell BorderManager 3.8, the

authentication data of the server for the NMAS mode of authentication cannot be checked on the server side. Checking authentication data works only for the backward compatibility mode.

There are no default values for this condition.

To define an authentication type:

- 1** You can select either Certificate Authentication or NMAS Authentication. If you select Certificate Authentication, you must configure one or more trusted roots. For NMAS Authentication, you can also configure the clearance level (Minimum Allowed Authentication Grade). For more details refer to the [NMAS documentation \(http://www.novell.com/documentation/lg/nmas22/index.html\)](http://www.novell.com/documentation/lg/nmas22/index.html).
- 2** Select Allow Certificate Authentication, then click Add to open the next page.
- 3** Select Trusted Root Object from the list.
- 4** If you selected Allow NMAS Authentication, you can configure the clearance level as shown in the illustration above. In this page, Password has been selected as the clearance level.

NOTE: Unless you have already configured a default security clearance for the users to a clearance level other than the one available while logging in, keep the minimum allowed authentication as logged in (which is the default).

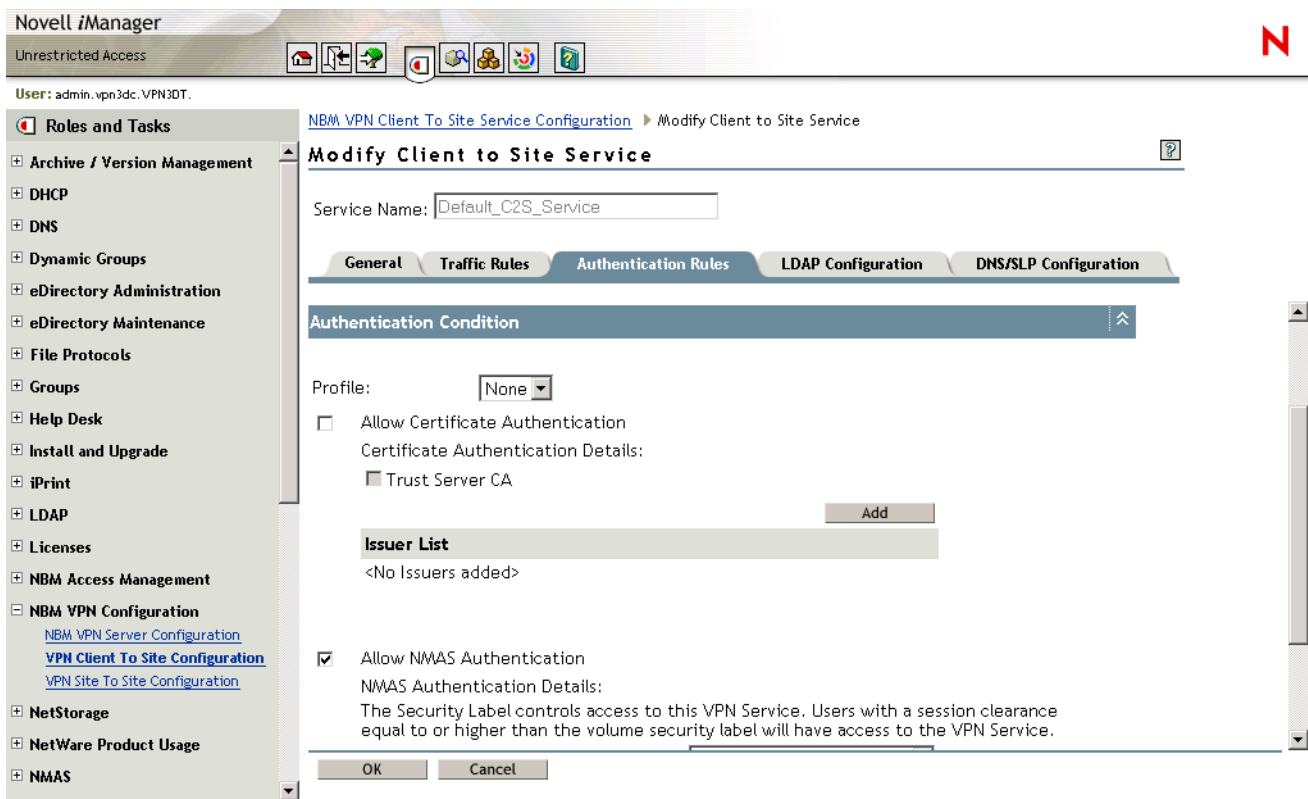
Allow/Deny Action

- 1** Click Allow/Deny Action to see this page. Allow is the default action.
- 2** You can select either the Allow or the Deny action for this rule.

Example of a Default NMAS Configuration

- 1** Log into the iManager server.
- 2** Choose the VPN client-to-site configuration on the VPN server under NBM VPN Configuration.
- 3** Select the client-to-site service on the service list.
- 4** Go to Authentication Rules > Click New.
- 5** Provide the Rule Name.
- 6** Select Define User, and click All Users radio button.
- 7** Select Authentication Condition, the following screen will be displayed.

Figure 55 Authentication Condition Example



- 8 Check Allow NMAS Authentication as shown in the figure.
- 9 Select Allow/Deny Users, and check the Allow check box.
- 10 Click Apply > and then OK.

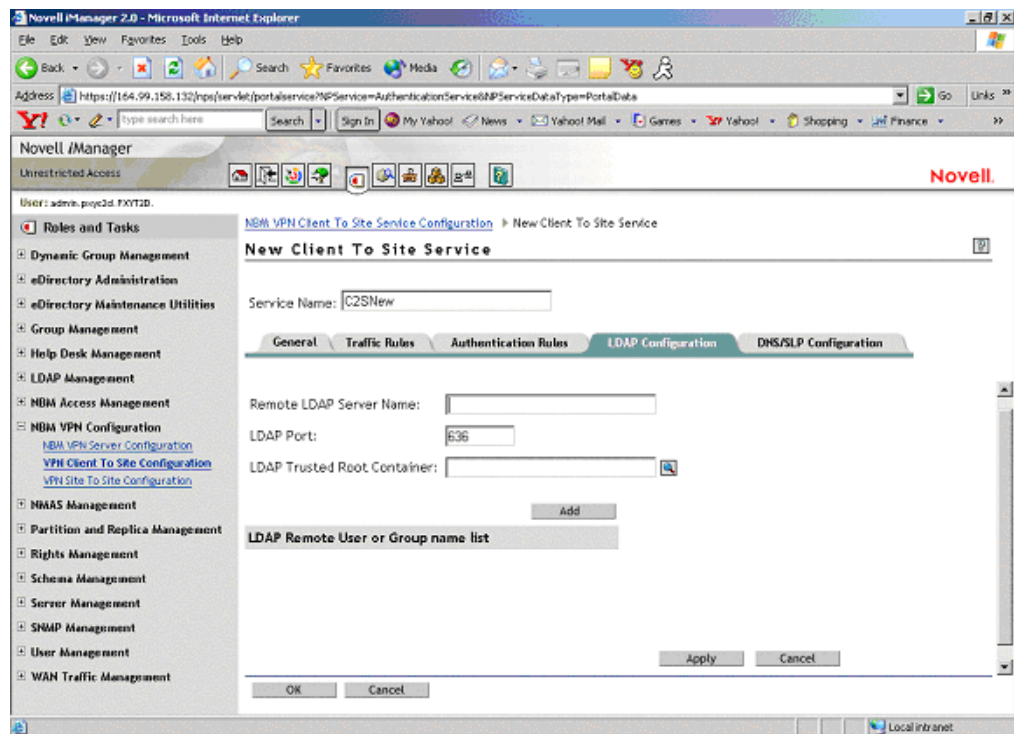
Remote LDAP Configuration

Configure LDAP to enable a remote authoritative directory for NMAS authentication using LDAP methods.

IMPORTANT: LDAP authentication uses SSL connections for authenticating the user from the Novell BorderManager server to the LDAP server. This requires the administrator to specify the trusted root container containing the Trusted Root object of the LDAP server.

The LDAP trusted root container configured in this purpose should contain only valid LDAP trusted root certificates, because the LDAP SSL client will fail to read certificates that are not valid LDAP trusted root certificates. Sometimes the LDAP SSL client fails to read some third-party certificates. We recommend that you create a separate trusted root container for storing LDAP trusted root certificates, and use it in the client-to-site LDAP configuration.

Figure 56 LDAP Configuration

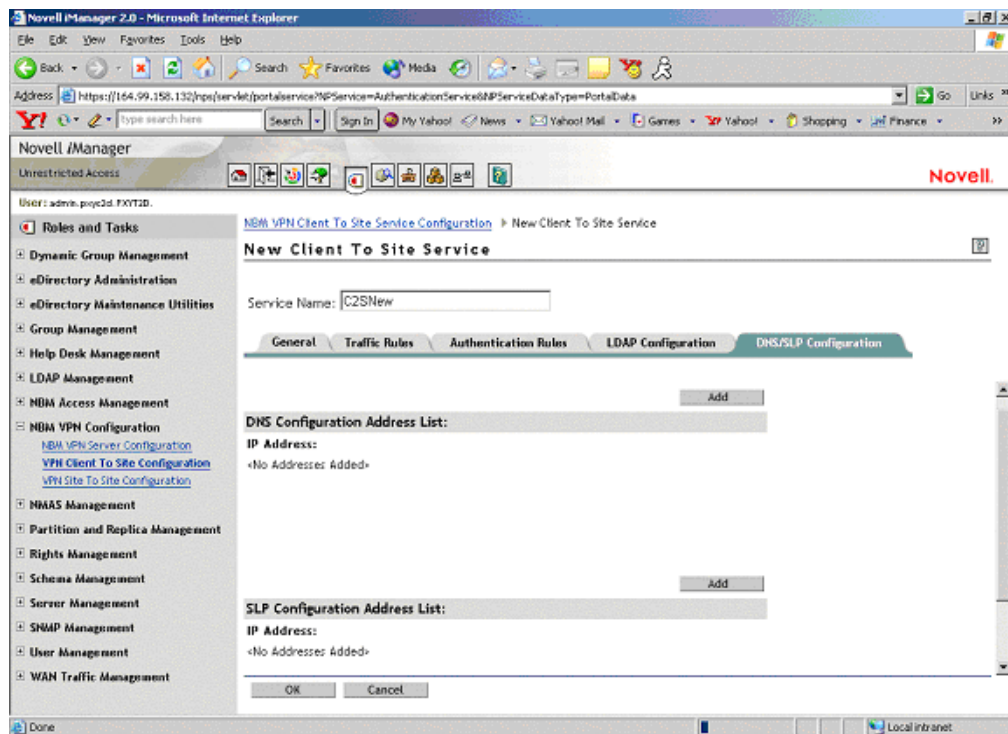


- ◆ **Remote LDAP Server Name:** The name or IP address of the remote LDAP server to which the VPN server will talk for LDAP authentication.
- ◆ **LDAP Port:** The LDAP secured port used by the VPN server to establish an SSL connection. The default value is 636.
- ◆ **LDAP Trusted Root Container:** This should contain the remote LDAP server's issuer certificate. The certificate can be created from the remote LDAP server certificate.
- ◆ **LDAP Remote User or Group Name:** The User or Group name of the remote LDAP user from the local Novell eDirectory. The names should have complete information, such as cn=admin, o=novell.

DNS/SLP Configuration

Use this page to configure DNS/SLP to be applied on Windows workstation during a VPN session.

Figure 57 DNS/SLP Configuration



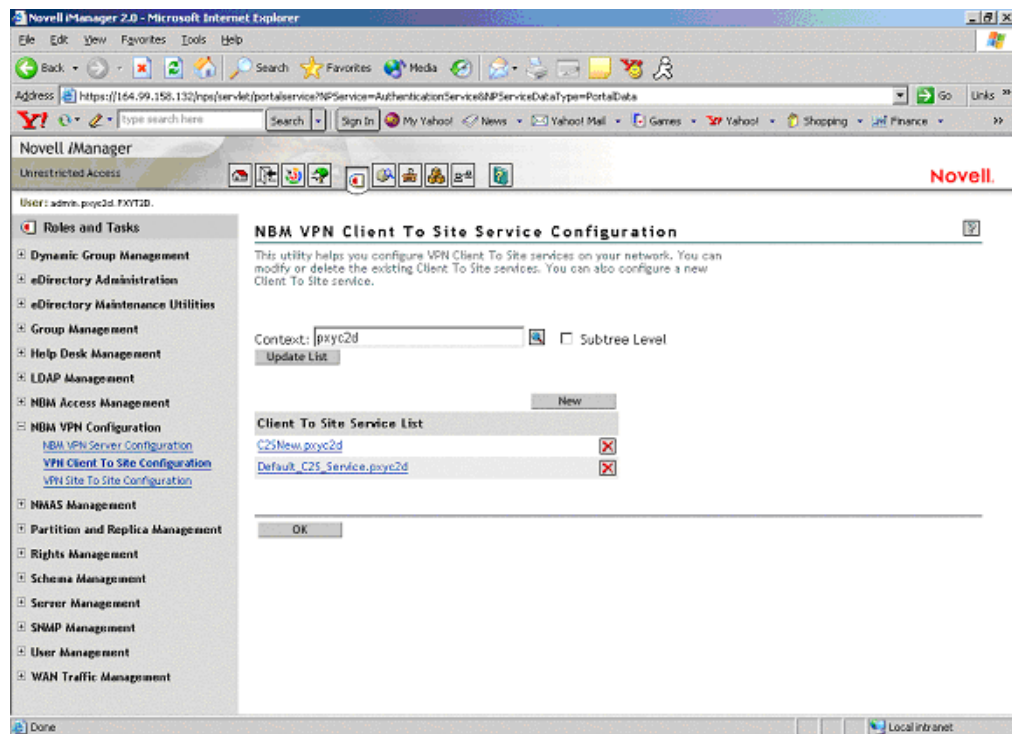
- ◆ **DNS Configuration Address List:** The address list of the DNS servers applied in the client during the VPN session. After a connection ends, the client will get back its original DNS information.
- ◆ **SLP Configuration Address List:** The address list of the directory agents applied in the client during the VPN session. This is applicable if Novell authentication is taking place during the VPN session. After a connection ends, the client will get back its original SLP information.

Final Client-to-Site Page

If all your configurations are correct, click OK on the bottom of the client-to-site service page to save the client-to-site service configuration.

The following page is displayed.

Figure 58 Final Client-to-Site Page



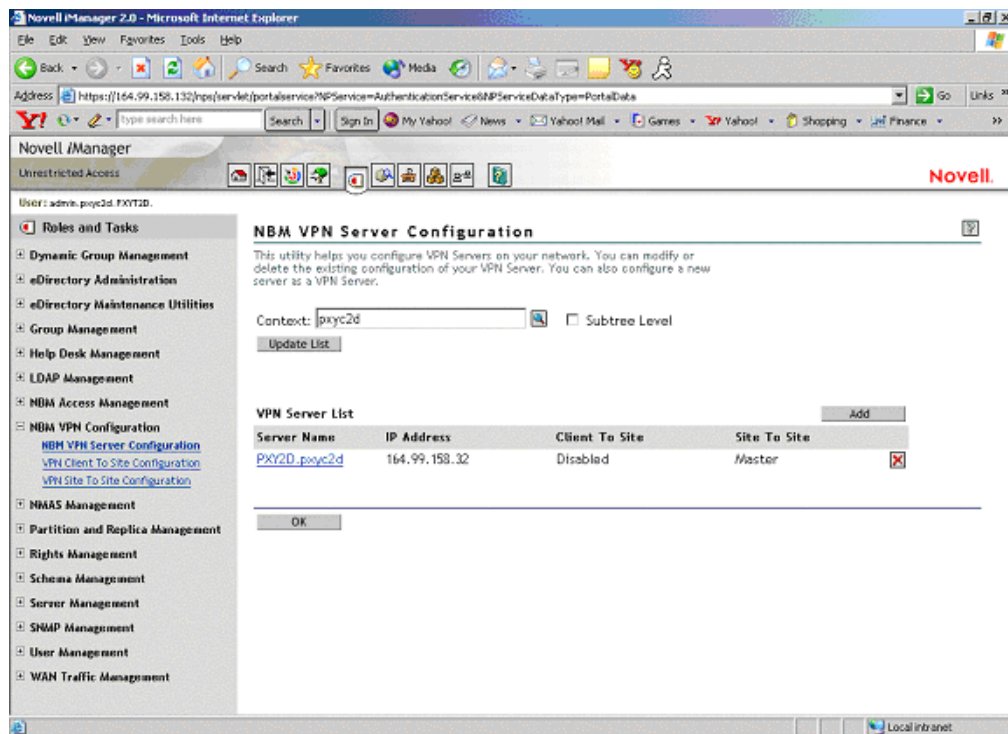
- 1 To delete the client-to-site service, click X.
- 2 Click the client-to-site service link if you want to modify any of the service properties.

Attaching a Client-to-Site Service to the VPN Server

After you configure a client-to-site service, you need to attach it to a VPN server.

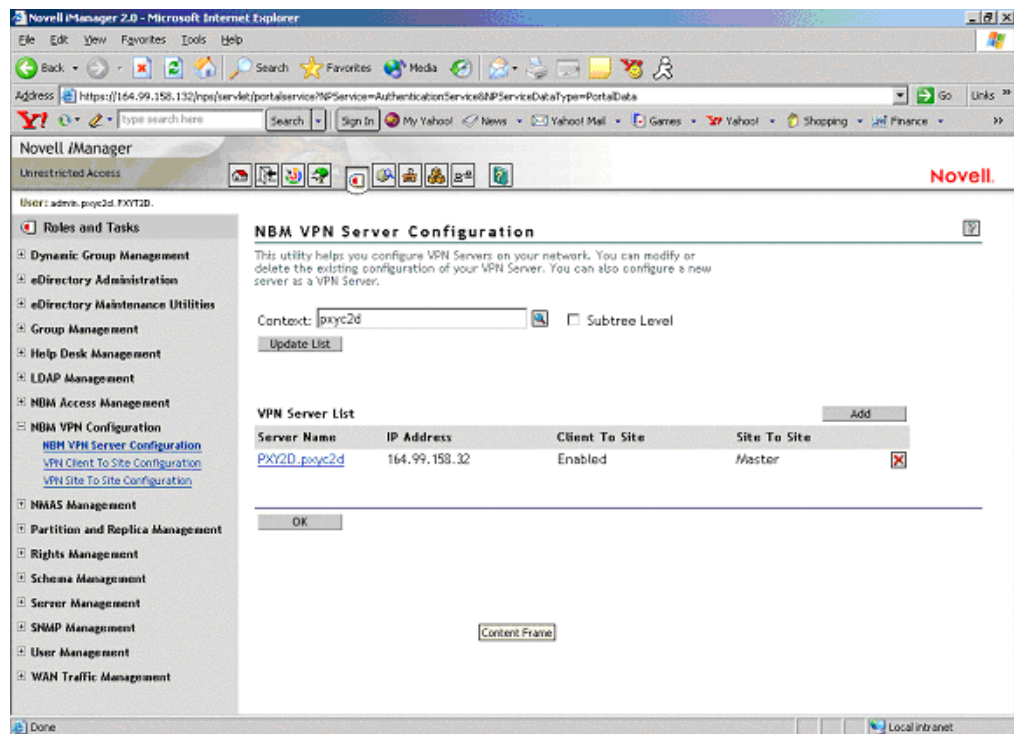
To do so, click the NBM VPN Configuration > Server Configuration in the left pane of iManager 2.0.1.

Figure 59 VPN Server Configuration



- 1 Click the VPN Server link to modify the VPN configuration. On the new page that appears, select the client-to-site check box and click Details. Click OK in the message box.
Deselect the client-to-site service to detach the service (if the service is already attached).
- 2 On the next page, click the Browse button to select the client-to-site service that you just created.
- 3 After the service is displayed, click Update.
- 4 In the next page, specify hexadecimal values in the WAN client IPX Network Address field. You can specify less than nine hexadecimal digits. This must be a unique IPX address.
- 5 Click OK to save all changes.
The final page shows the client-to-site services enabled.

Figure 60 Final Client-to-Site Attached Page



Site-to-Site Configuration

This utility helps you configure VPN site-to-site services on your network. You can modify or delete the existing site-to-site services. With a single master server you can configure single site-to-site service at a time.

Prerequisites for the Master:

- ◆ Master Trusted Root Container (referred to as Trusted Root on the pages and in eDirectory): Contains the TROs for the master and all the slaves. This was created while you were configuring the master server as a VPN server. See [“VPN Server Configuration” on page 179](#).
- ◆ Trusted Root Object for each of the members (contained in the Trusted Root Container mentioned as above):
 - ◆ TROs of the master server. You created this during VPN server configuration.
 - ◆ TROs of the slave server. You need to export the TRO from the slave’s server certificate using the steps in [“Exporting Root Certificates from the Server Certificate” on page 169](#) and create the TROs in the Trusted Root container using the steps in [“Creating the Trusted Root Object” on page 172](#).

Prerequisites for the Slave:

- ◆ Slave Trusted Root Container (referred to as Trusted Root on the pages and in eDirectory): Contains the TRO for the master. This was created while you were configuring the slave server as a VPN server. See [“VPN Server Configuration” on page 179](#)
- ◆ Trusted Root Object for the master (contained in the Trusted Root container mentioned above). You need to export the TRO from the master’s server certificate using the steps in

“Exporting Root Certificates from the Server Certificate” on page 169 and create the TROs in the Trusted Root container using the steps in “Creating the Trusted Root Object” on page 172.

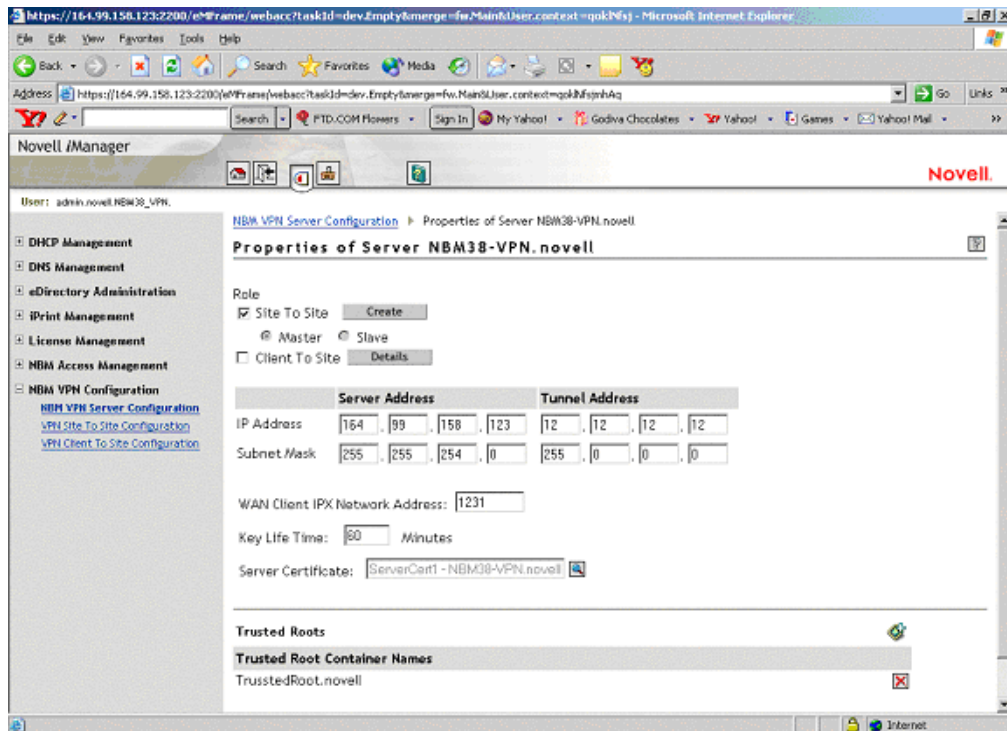
The following topics are discussed here:

- ◆ “Configuring a VPN Server As a Master Server” on page 208
- ◆ “Configuring a VPN Server As a Slave Server” on page 210
- ◆ “Modifying a Site-to-Site Service” on page 213
- ◆ “Removing Site-to-Site Members” on page 217

Configuring a VPN Server As a Master Server

A new site-to-site service can be created either while a new VPN master server is created or by modifying an already configured VPN server. To create a site-to-site service, you need to configure a VPN server as a master server. Because no site-to-site service is currently attached to this server, the site-to-site check box is deselected.

Figure 61 Site-to-Site Configuration



- 1** To create and attach a site-to-site service to a VPN server, select the site-to-site check box and select the Master option button, then click Create.
- 2** In the next page, specify the details of the master member of the site-to-site service.
 - ◆ **Issuer:** The eDirectory Distinguished Name of the Trusted Root object that has issued the certificate for the master member of the site-to-site service. Use the default value that you see on the page if you haven't already created a Trusted Root object for this server and you want to use the automatic TRO creation facility for this server. If you already have a TRO created for this server using the steps mentioned in “Creating the Trusted Root

Object” on page 172, browse and select the Trusted Root object that you have imported into the trusted root container.

- ◆ **Subject Name:** The subject name of the X.509 Server Certificate issued for the master member. The certificate subject name should be in the format shown in the following example: cn=nbm38.o=novell or o=novell.cn=nbm38. For exact subject name, view the certificate subject name from the server certificate. The certificate subject name should be exactly the same as the one that appears in the certificate.

NOTE: To view the certificate subject name, go to iManager > eDirectory Administration > Modify Object > select the Key Material Object (server certificate that you have created). Select the certificate from the list and click Details.

- ◆ **Alternative Subject Name:** These can be of three types: DNS, Mail, or IPv4. One of these three is applicable. If you choose one of these, you must provide the corresponding type of alternative subject name. For example, Mail means xxx@novell.com.
- ◆ **Protected IP Network and Hosts:** This is the list of networks or hosts that would be protected by this site-to-site master member.
- ◆ **Enable IP RIP:** The enabled RIP filter exceptions are added on the member server to restrict advertising routes via the VPTUNNEL Virtual Interface.

3 Click Apply to save this information temporarily.

Click Add to add Protected Networks/Hosts, then click OK to save this protected network.

4 The next page shows the Issuer and Subject Name information. It also shows the configured protected networks.

5 Click Apply to save the changes temporarily.

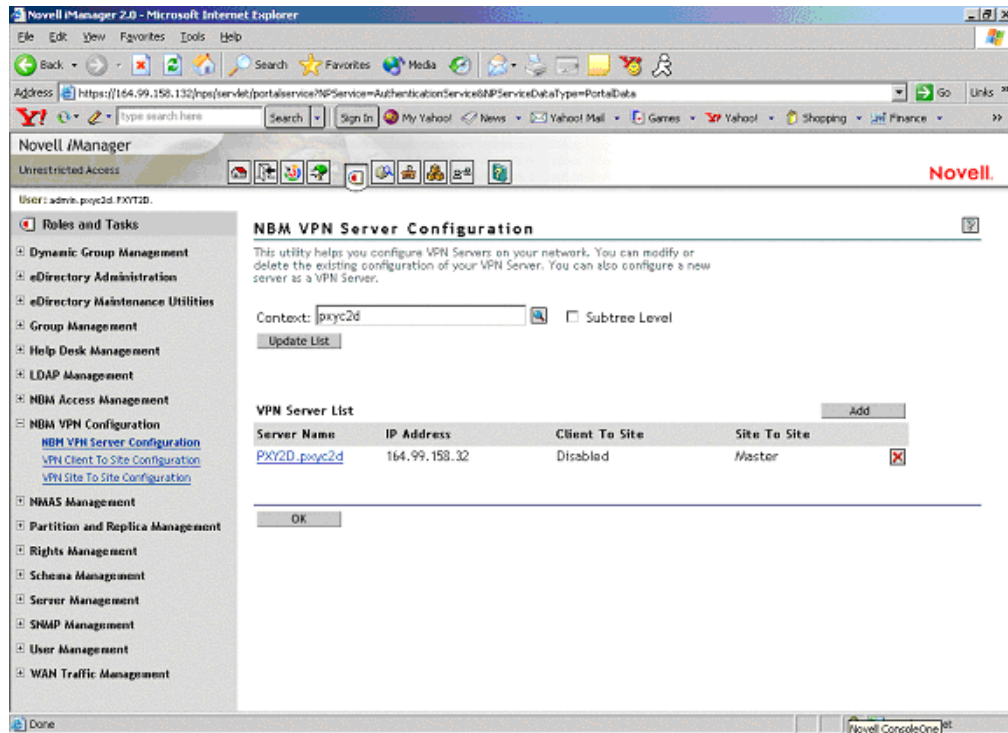
6 In the next page, click OK to save changes to eDirectory.

7 After you create a site-to-site service as above, deselect the site-to-site check box to delete and detach the service from the server and Novell eDirectory.

If the certificate issue path is server_certificate > intermediate_certificate > trusted_root_certificate, the intermediate server certificate along with the certificate chain (the public key certificate as well as the trusted root certificate of the intermediate certificate) should be imported into the TRO, and this should be configured as the issuer. The same holds for the client issuer name list, which is specified in the authentication rules.

The following page shows the status of the server after it attached to a site-to-site service. Because the server has been configured as a master server, the page shows Master in the VPN server list entry.

Figure 62 Server Attached to a Site-to-Site Service

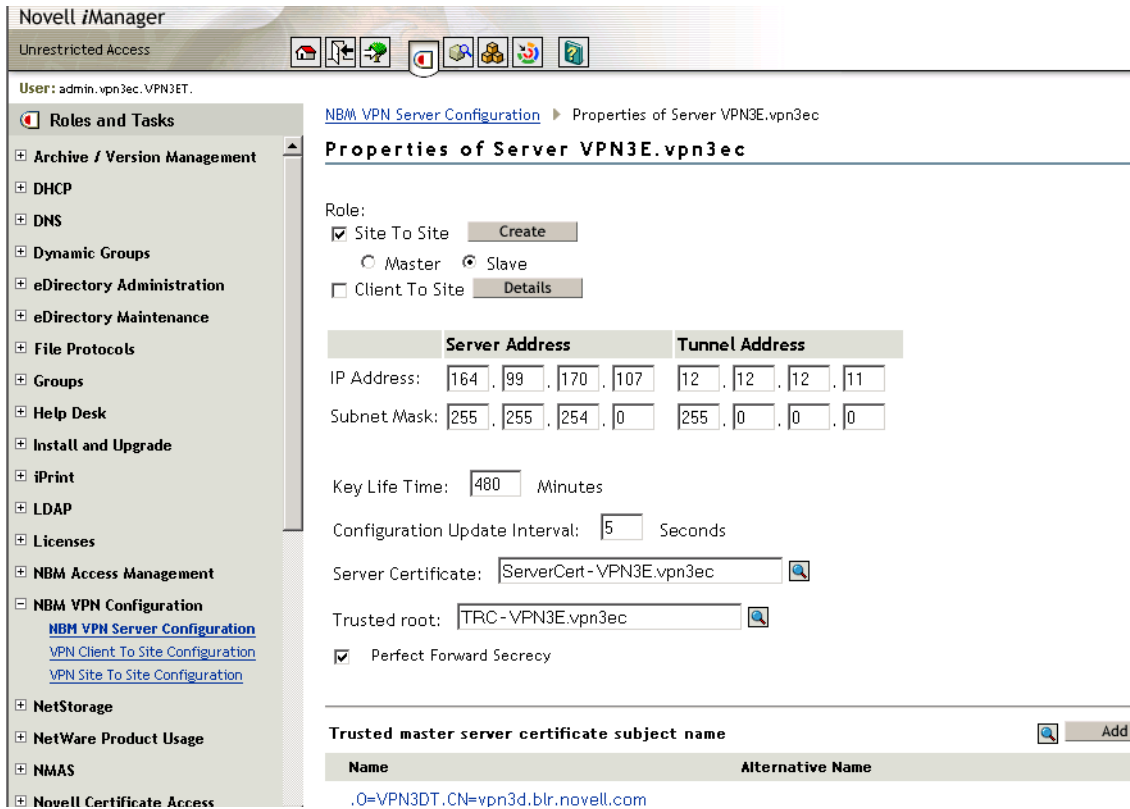


This example shows a server PXY2D.pxy2d with public IP address 164.99.158.32 configured as a VPN server with client-to-site services disabled and site-to-site services enabled. This VPN server is a master of the site-to-site service to which it belongs.

Configuring a VPN Server As a Slave Server

If you want to make a VPN server a slave member of a site-to-site service, first configure the server as a VPN server using the steps in [“VPN Server Configuration” on page 179](#). In the left pane, click NBM VPN Server Configuration, then click the configured server. Select the site-to-site service and click the Slave option button. Specify the certificate subject name of the trusted master. If the master is in the same tree as the slave, browse to select the master's certificate instead of entering the certificate subject name. If the master certificate is not in the same tree go to ConsoleOne and log into both master and slave. Go to the master server trusted root container and create a trusted root object. Provide the slave's root certificate which will be present in the sys:public directory. Repeat the process for the slave and you would have created slave trusted root object in the master, and the master trusted root object in the slave.

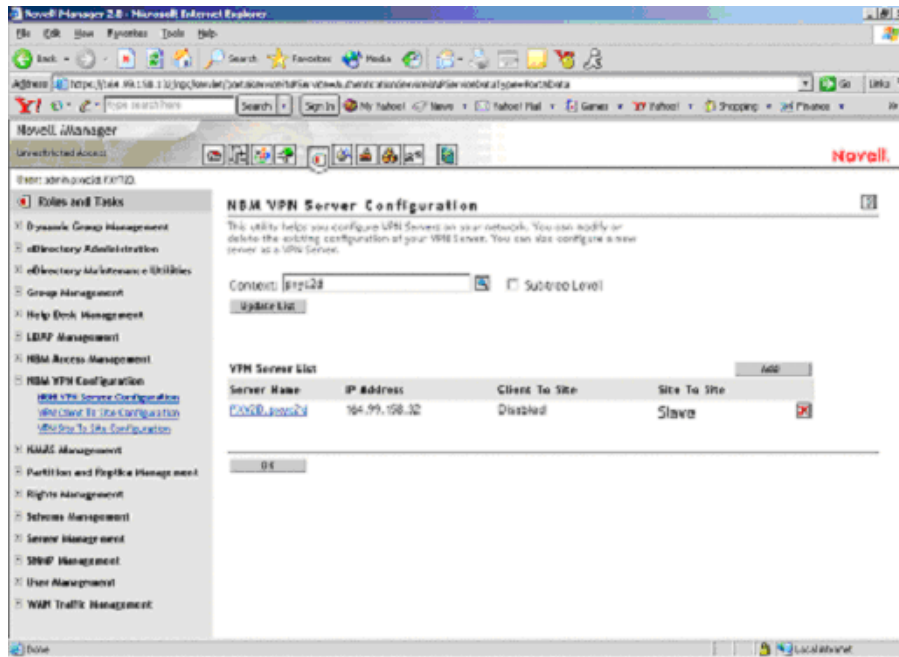
Figure 63 Configuring a VPN Server as a Slave



- 1** Click OK after entering the Subject Name if you have clicked the Add button to manually add the trusted master's server certificate subject name. If the master is in a different tree, go to ConsoleOne and then go to the master server certificate > right-click properties and see the certificate subject name. Copy and paste this name to the Add > Certificate Subject Name field.
- 2** Click OK on the main Server Modification page.

The following page shows the status of the server after it has been configured as a slave of a site-to-site service. Because the server has been configured as a slave server, the page shows Slave in the VPN server list entry.

Figure 64 Sample Page



This example shows a server PXY2D.pxyc2d with public IP address 164.99.158.32 configured as a VPN server with both client-to-site and site-to-site services enabled. This VPN server is a slave of the site-to-site service to which it belongs.

After the VPN server is configured as a slave, add this slave server's information in the member list of the site-to-site service (in the master VPN server) of which you want to make this server a slave. See ["Member List"](#) on page 214.

NOTE: A VPN server can be a slave of only one site-to-site service. A site-to-site service can have only one master.

After the Server configuration is completed on the slave, and site-to-site configuration is completed on the master, the master distributes the site-to-site configuration information to all the Slaves.

To verify whether the configuration information has reached the slaves:

- ◆ Use callmgr.nlm from the companion CD to verify that a WAN call was established with the master on the slave machines. This NLM can be used to find the status of IP/IPX WAN calls between VPN servers. To use this NLM, copy it to the sys:\system directory and load callmgr.nlm from the system console. Use the screen that pops up to check the details of existing WAN calls.
- ◆ The sys:\etc\ipwan.cfg file contains information about the master and all slaves for Mesh topology, and information about the master for Star topology.
- ◆ The VPN Monitoring NetWare Remote Manager snap-in shows the status of all the slaves as Up-to-Date.
- ◆ Data communication between the master and slaves is happening. Test this with a ping from the master to the slave.

If any of the above has not happened, you might need to force a resynchronization from the master.

- 1 Go to the VPN Monitoring snap-in in NetWare Remote Console on the master.

For more information, see [Chapter 19, “Monitoring Virtual Private Networks,”](#) on page 227.

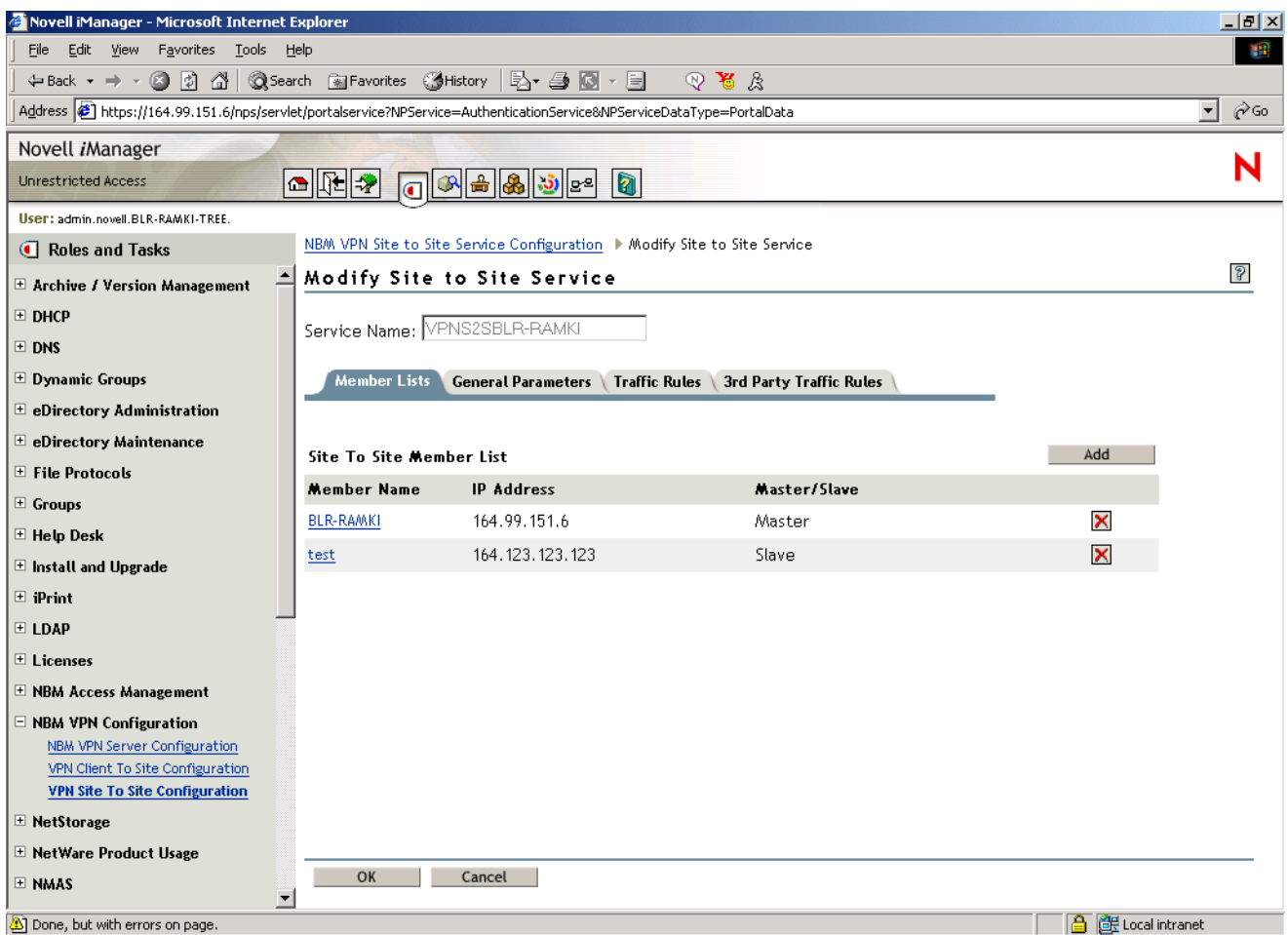
You will see the list of members.

- 2 Click Synchronize All.

Modifying a Site-to-Site Service

Click VPN site-to-site Configuration in the left panel to view a list of the configured site-to-site services. The following page shows the example site-to-site service that was created earlier.

Figure 65 Configured Site-to-Site Service



Click the name of the site-to-site service.

Use the next pages to configure the following:

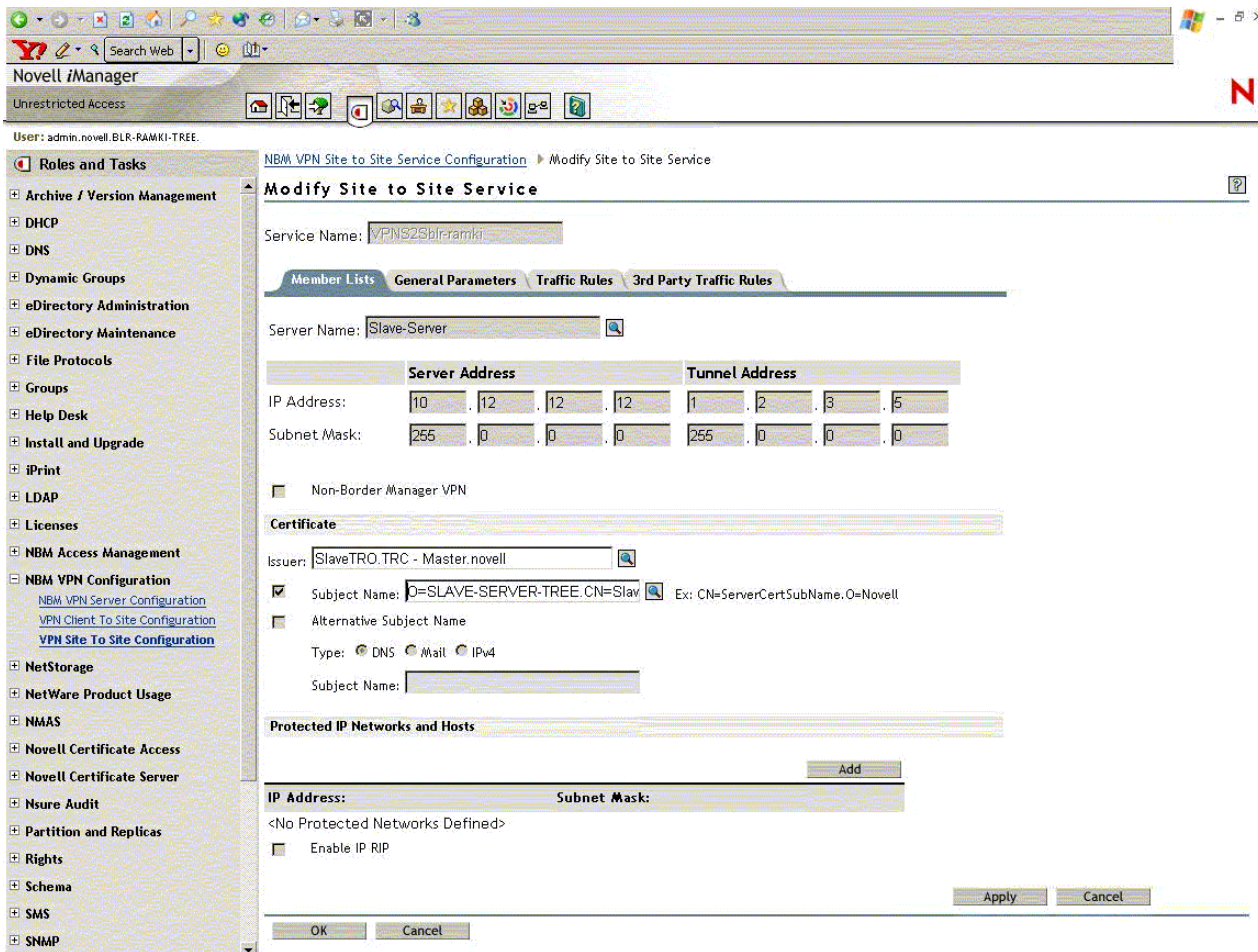
- ◆ “Member List” on page 214
- ◆ “Traffic Rules” on page 216
- ◆ “Third-Party Traffic Rules” on page 216
- ◆ “Final Site-to-Site Page” on page 217

Member List

The member list shows the master server that was configured during the creation of the site-to-site service.

- 1 Click the server name to view and modify master server details.
- 2 To add a slave server to this site-to-site service, click New.
- 3 Fill the details in the next page.

Figure 66 Site-to-Site Slave Configuration



NOTE: The slave server that you are adding to this member list should have been already configured as a slave VPN server as mentioned [“Configuring a VPN Server As a Slave Server” on page 210](#)

- ◆ **Server Name:** If the server is on the same tree, click Browse and select the server object, or specify the name of the slave server. The name you specify could be any name with which you identify the slave server.
- ◆ **Issuer:** The Novell eDirectory Distinguished Name of the Trusted Root object that has issued the certificate for the master or slave member of the site-to-site service. Browse and select the Trusted Root object that you have imported into the master’s Trusted Root container.
- ◆ **Subject Name:** The subject name of the X.509 Server Certificate issued for the master or slave member. The subject name of the certificate should be in the following format:

cn=nbm38.o=novell or o=novell.cn=nbm38. For the exact subject name, view the certificate subject name from the server certificate. The certificate subject name should be exactly the same as the one that appears in the certificate.

To view the certificate subject name, go to ConsoleOne and right-click on the Key Material Object (server certificate that you have created) > Properties > Security > Certificate. Select the certificate from the list and click Details.

- ◆ **3rd Party/Non-BorderManager VPN:** You can also add a third-party site-to-site member using this option. Select the check box to add a third-party member. For a third-party member, both the Preshared Key and Certificate modes of authentication are supported. Choose the appropriate authentication method. If Preshared Key is chosen, a Preshared Key secret must be specified. If Certificate is chosen, the issuer name and subject name must be specified.
 - ◆ **Alternative Subject Name:** These can be of three types: DNS, Mail or IPv4. One of these three is applicable. If you choose one of these, you must provide an alternative subject name.
 - ◆ **Protected IP Network and Hosts:** This is the list of networks or hosts to be protected by this site-to-site master member.
 - ◆ **Enable IP RIP:** The enabled RIP filter exceptions are added on the member server to restrict advertising routes via VPTUNNEL Virtual Interface.
 - ◆ **Trusted Master Server Certificate:** The certificate subject name of master server that you have configured as the Master Member.
- 4 Click Browse if the server that you're adding a slave is on the same tree as the master. If the slave server is on a different tree, specify the name. Specify other slave details.
 - 5 Click Apply to temporarily save the slave server information.
 - 6 The next page will show both the servers in the member list.
 - 7 You can click OK to exit after saving the member list changes to Novell eDirectory, or you can configure General Parameters/Traffic Rules for the site-to-site service.

General Parameters

The General Parameters page has the following fields:

- ◆ **Topologies:** Two topologies are supported:
 - Full Mesh:** This is the default topology. All servers are interconnected to form a web or mesh, with only one hop to any VPN member. There is communication between every member in the VPN, whether required or not. This topology is the most fault-tolerant. If a VPN member goes down, only the connection to that member's protected network is lost. Also, after the encryption keys have been established, the master server is no longer required. However, if RIP is enabled for the VPN tunnel, this topology has more routing traffic because each VPN member must send updates to every other member. Also, routing loops in a mesh topology can require a significant amount of time to be resolved. Choose the trusted root container for this site-to-site service. This trusted root container is the master's trusted root container. The illustration above shows the default values automatically assigned during the creation of the site-to-site service.
 - Star:** In this topology, all the slaves are connected only to the master, and all the communication is routed through the master. This topology has the advantage that the routing traffic is far less than the mesh topology and the connection between two slaves

is not required. This topology is not fault tolerant. If the master goes down, the VPN communication between the slaves is also affected.

NOTE: A ping between two slaves does not go through in a star topology unless the slave address is added to protected networks.

- ◆ **Update Interval:** A synchronization parameter that specifies how long the master server waits between attempts to update a slave server with the newest topology and encryption information. If the first attempt fails, the master server retries at set intervals until it updates the slave server. The default value is 15 minutes.
- ◆ **Connect Timeout:** A synchronization parameter that specifies how long the master server tries to connect to a slave server during a synchronization update. The default value is two minutes.
- ◆ **Response Timeout:** A synchronization parameter that specifies how long the master server waits for a response from a slave server before terminating the connection during a synchronization update. The default value is two minutes.

8 Click Apply to save the changes temporarily.

Traffic Rules

Traffic Rules are policies that govern what traffic can go through a VPN connection. You can add, modify, or delete traffic rules for the site-to-site service. You can also change the priority of a traffic rule by moving it up or down the list. The traffic rule at the top of the list has the highest priority. A default traffic rule is automatically created. The default action of this traffic rule is to encrypt all packets (Encryption algorithm: 3DES, Authentication algorithm: HMAC-MD5).

- 1** Click New to add a new traffic rule.
- 2** On the next page, click Define Services. Specify the details.
- 3** Click OK to save changes temporarily.
- 4** Click Define Action to configure the traffic rules.
- 5** Click Apply to save changes temporarily.
- 6** On the next page click OK to save changes to Novell eDirectory.

TIP: The service provides the facility to configure and store your entries as profiles that can be used later when you log in to the service.

Third-Party Traffic Rules

Third-party traffic rules are policies that govern accessibility for a site-to-site connection to a third-party member. You can add, modify, or delete traffic rules for the site-to-site service. You can also change the priority of a traffic rule by moving it up or down the list. The traffic rule at the top of the list has the highest priority. A default traffic rule is automatically created for each third-party server that is configured as a slave. This rule can not be modified. To create a new third-party traffic rule:

- 1** Click Add to add a new third-party traffic rule.
- 2** On the next page, click third-party Server Configuration or Novell BorderManager Server Protected Network. Specify the details.
- 3** Click OK to save changes temporarily.
- 4** Click Define Action to configure the 3rd-party traffic rules.
- 5** Click Apply to save changes temporarily.

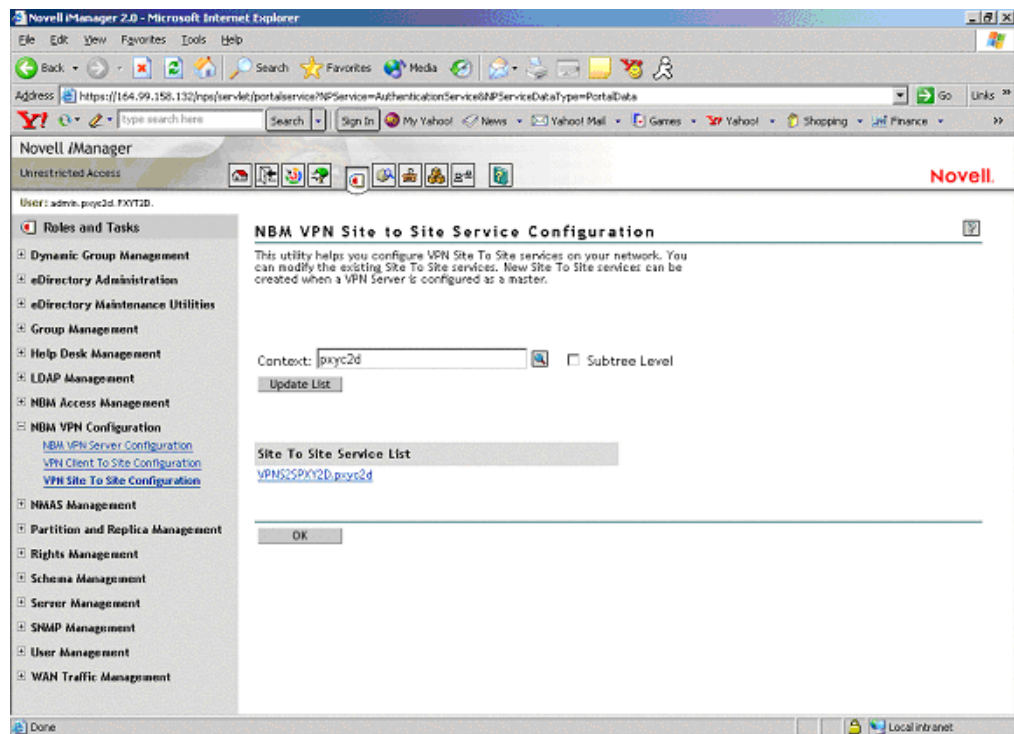
6 On the next page click OK to save changes to eDirectory.

TIP: The service provides the facility to configure and store your entries as profiles that can be used later when you log in to the service.

Final Site-to-Site Page

After you have clicked OK the final page reflects the changes.

Figure 67 Final Page



Removing Site-to-Site Members

The following scenarios are possible while removing site-to-site members:

- ◆ “Removing Slave” on page 217
- ◆ “Forcefully Removing the Slave” on page 218
- ◆ “Removing a Master” on page 218
- ◆ “Forcefully Removing a Master” on page 218

Removing Slave

- 1** Verify that the master and slaves are up and communicating with one another.
- 2** Remove the slave member from iManager. Go to Site-to-Site, select the Members tab, and delete the member you intend to remove.
- 3** The change in configuration is synchronized to all the slaves. You can check this in Novell Remote Manager or from the ipwan.cfg file. Otherwise, use Synchronize All on the monitoring pages to get the changes across.

- 4** After the slave removal is synchronized and the WAN call for the slave is removed on the master, remove the server configuration on the slave server from iManager.
- 5** When the server configuration is removed, the vpslave NLM is unloaded on the slave.

Forcefully Removing the Slave

When one or more slaves has a hardware or a network problem that prevents the master from synchronizing the changes to the slave to do a clean removal you might need to remove the slave forcefully.

- 1** Remove the slave member physically from the VPN network. If the slave is up, use iManager to remove the server configuration on the slave.
- 2** Using iManager, remove the slave member from the site-to-site members list on the Master.
- 3** Enter stopvpn to stop the VPN services on the master.
- 4** Remove the file sys:\system\vpn\member.dat, sys:\system\vpn\member.bak and sys:\etc\ipwan.cfg on the Master.
- 5** Start the VPN services on the Master, enter startvpn.

Removing a Master

- 1** Normally the master can be removed only if all the slaves are removed. Please remove all the slaves using the steps mentioned in [“Removing Slave” on page 217](#), and verify that the changes are synchronized.
- 2** Using iManager remove the VPN site-to-site configuration.

Forcefully Removing a Master

Ocasionaly, because of a problem with the master's hardware or with the network, it might be essential to replace a master from the network with another master.

- 1** Remove the existing master from the network.
- 2** From iManager, add the server configuration for the new master. Add site-to-site configuration, but don't add the other slaves to site-to-site.
- 3** For each existing slave:
 - ♦ Stop the VPN services on the slave using stopvpn.
 - ♦ Remove all the files in sys:/system/vpn/ on the slave server
- 4** Change the certificate subject names in the server configuration of all slaves to point to the new Master's server certificate. If the master server is reinitialized, you might need to configure new TRCs and TROs for all the slaves and put them under the same TRC.
- 5** In iManager, go to the new master server and add all the slaves as members in the site-to-site configuration.

VPN Policy

Novell BorderManager 3.8 VPN services provide VPN access rules that can be assigned to a particular user. The access control is categorized based on Novell eDirectory user, X.509 certificate user, Novell eDirectory usergroup, and Novell eDirectory container. The traffic rules are granularized to the level of port information.

The administrator can effectively combine the authentication and traffic rules to control all the VPN users. For example, it is possible to configure a rule to allow one particular user to access an application running on a particular TCP port and deny access to everyone else. In addition to this, the administrator can even specify the type of authentication credentials for a particular user.

VPN rules are part of either the client-to-site VPN service or the site-to-site VPN Service. The client-to-site VPN service has both authentication and traffic rules. The site-to-site VPN service has only traffic rules because there is no user authentication involved in the site-to-site VPN service. Authentication rules reside on the VPN server and are traversed only after the primary authentication is successful, then the selected set of traffic rules enforces all the traffic over the VPN tunnel for the duration of the connection. The default authentication rule is Deny All.

The following table provides an overview of the access rules.

Client-to-Site	Site-to-Site
Authentication rules are traversed	No Authentication rules
Traffic rules are indexed based on the user	No index. All traffic rules are applicable to the master and all slave servers
No specific third-party rules need to be configured. Based on the certificate user logged in, the traffic rules are enforced.	Specific traffic rules must be configured while configuring communication with the third party site-to-site server
Can specify a destination condition	No destination condition. They are covered by protected networks

The following default values are discussed here in brief:

- ◆ [“Default Values for Client-to-Site Authentication Rules” on page 219](#)
- ◆ [“Default Values for Client-to-Site Traffic Rules” on page 219](#)
- ◆ [“Default Values for Site-to-Site Traffic Rules” on page 220](#)

Default Values for Client-to-Site Authentication Rules

When a client-to-site service is created, no default authentication rule is created. In such a situation, the VPN server assumes that the default authentication action is to allow all users from eDirectory. However, if at least one authentication rule is configured, the default (no rule is matching) action is to deny the user trying to get access to the VPN network.

Default Values for Client-to-Site Traffic Rules

When a client-to-site service is created, a default traffic rule is created to drop the packet. This means that when a client-to-site service is created, the client-to-site connection goes through but all packets are dropped at the VPN client. In other words, the communication ceases to exist. For this, the administrator must have to configure the required traffic rules for different users accordingly.

Default Values for Site-to-Site Traffic Rules

When the site-to-site service is created, a default traffic rule is created for any kind of traffic to encrypt it with 3DES/HMAC-MD5 combination. This default traffic rule can be modified to include any kind of traffic or to drop the packet.

18

Upgrading Virtual Private Networks

This section explains the tasks you must complete to set up the VPN component of the Novell® BorderManager® 3.8 software for an upgrade from an earlier version of BorderManager. These steps are significantly different than they were for earlier versions. For configuration information, see [Chapter 17, “Configuring VPN Services,” on page 179](#). Refer to [Chapter 16, “Certificate-Based Authentication,” on page 163](#) for details on how to configure certificates before you launch VPN services.

This section also describes the preparatory steps required for some tasks.

- ◆ [“VPN Migration” on page 221](#)
- ◆ [“Upgrading a VPN from a Previous Version” on page 222](#)

NOTE: This section describes the tasks required to set up an initial implementation of VPN. For planning and conceptual information about VPN, refer to the *Novell BorderManager 3.8 Overview and Planning Guide*, available in the online documentation. Make sure you understand this information before setting up and configuring your VPN.

VPN Migration

The VPN configuration migration tool migrates the BorderManager Enterprise Edition 3.6 and Novell BorderManager 3.7 configuration to a Novell BorderManager 3.8 VPN configuration. This takes place when you install Novell BorderManager 3.8 over an earlier version of BorderManager. This tool also works outside of Novell BorderManager install. For that information refer to [“Upgrading a VPN from a Previous Version” on page 222](#).

The VPN migration tool reads earlier BorderManager VPN configurations from their respective locations (configuration files or eDirectory) and automatically converts the information to Novell BorderManager 3.8-compatible VPN configuration.

The tool creates the following items:

- ◆ **Master or Slave Server Configuration:** The public IP address, tunnel IP address, IPX address, and their respective IP masks are read from the configuration files and migrated. The migration tool also reads the Novell eDirectory information on the server role and enabled services and migrates them. It creates all other Novell BorderManager 3.8-compatible attributes and attaches the server certificate and trusted root container.
- ◆ **Site-to-Site Service:** The tool creates site-to-site traffic rules and migrates the protected networks and host, as well as other Novell BorderManager 3.8-compatible attributes. It migrates attributes like ServiceEnabled vpnConnProperties, pnConfigConnectTimeout, VpnConfigResponseTimeout, serviceHosts, serviceIdentifier and vpnConfigInterval. If the server is a master, the tool creates the site-to-site object and adds the site-to-site member entry. If the server is a slave, it does not create the object in the members list of the master.
- ◆ **Client-to-Site Service:** The tool creates the client-to-site object for both master as well as slave servers. It migrates the traffic rules, protected networks and creates the default

authentication rule. It also creates the other Novell BorderManager 3.8-compatible attributes.

- ◆ **Server Certificates:** The migration tool creates the server certificate with the name VpnServCert, appending the server name.
- ◆ **Trusted Root Containers:** The migration tool creates the Trusted Roots Containers with the name TrustedRoot, appending the server name.
- ◆ **Trusted Root Objects:** The migration tool creates the Trusted Root Object with the name TRO, appending the server name.
- ◆ **SCM Service Object:** The migration tool creates the SCM service object.

To implement this component, upgrade all the nodes. If only one node is upgraded, add the keys from the NWAdmn member list.

Upgrading a VPN from a Previous Version

Earlier versions of BorderManager VPN servers use SKIP for key management. They also use VPNCFG and NWAdmn for configuration. Novell BorderManager 3.8 supports industry-standard IKE for key management, but also supports backward compatibility with Novell BorderManager 3.7 in SKIP mode. This section discusses ways of upgrading an earlier version of BorderManager VPN network to a Novell BorderManager 3.8 VPN network without affecting the connectivity between these networks. If you want to migrate the VPN configuration before upgrading to Novell BorderManager 3.8, make sure that the VPN is configured.

NOTE: After initial configuration through VPBNCFG, reload vpmaster and vpslave if they are not already loaded.

General Guidelines for Upgrading

First, upgrade the master Novell BorderManager 3.8 server. Upgrade the slaves only after the master is upgraded.

When a master or slave is upgraded, automatic VPN configuration migration is supported from earlier versions of BorderManager configuration to Novell BorderManager 3.8 configuration. The actual upgrade consists of three steps:

1. Installing Novell BorderManager 3.8 over earlier versions of BorderManager.
2. During installation, selecting the Automatic Migration check box, which will automatically migrate the existing configuration.
3. Some additional manual configuration or migration is necessary for certain scenarios. These scenarios are discussed later.

After the above three steps are complete, an earlier version of a BorderManager server can be considered fully migrated to a Novell BorderManager 3.8 server.

You can upgrade the slaves one by one. When some slaves are migrated and others are running an earlier version of BorderManager, the servers communicate with each other in the SKIP mode, if SKIP is configured on both. After all the slaves are migrated remove the SKIP configuration on all the servers and retain only the IKE configuration.

The SKIP configuration needs to be done using VPNCFG and NWAdmn, as with previous versions. The IKE configuration can be done using the iManager plug-ins. The Novell BorderManager 3.8 slaves and master can be monitored through the new Netware Remote

Manager monitoring interface. For information see [Chapter 19, “Monitoring Virtual Private Networks,”](#) on page 227.

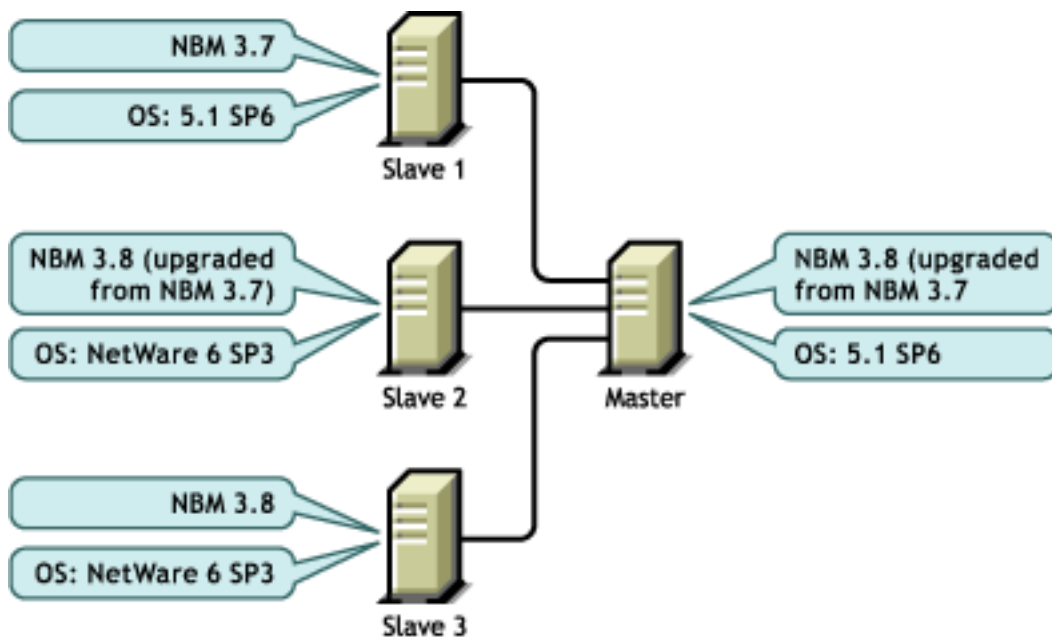
IMPORTANT: Always back up your networking configuration files before an upgrade. The files to be backed up are `\etc\tcpip.cfg`, `\etc\netinfo.cfg`, and `\etc\gateways`. In the event of an abend and subsequent file corruption, this backup will help in restoring the networking configuration.

After migrating a slave to Novell BorderManager 3.8 and configuring site-to-site for IKE mode, the two servers might still continue to communicate in the SKIP mode for a few minutes until the changes take effect. Data communication continues to happen during this period.

Example Upgrade Scenario

The following example setup consists of one master and two slaves. All of them are running an earlier version of Novell BorderManager. The focus of the upgrade is to migrate all the existing VPN servers to Novell BorderManager 3.8 and eventually have the servers using IKE for key management. These servers can then be configured and monitored using Web-based interfaces. You can also add a new Novell BorderManager 3.8 slave to the VPN site-to-site network. This will be a fresh, newly configured Novell BorderManager 3.8 slave.

Figure 68 Example Upgrade Scenario



Upgrade Procedure

The following upgrade scenarios are discussed here:

- ◆ [“Upgrading an Earlier BorderManager Master to Novell BorderManager 3.8”](#) on page 224
- ◆ [“Upgrading an Earlier BorderManager Slave to Novell BorderManager 3.8”](#) on page 224
- ◆ [“Adding a New Novell BorderManager 3.8 Slave to a Partially or Fully Upgraded Setup”](#) on page 224
- ◆ [“Adding a New BorderManager 3.7 Slave to an Existing Novell BorderManager 3.8 Setup”](#) on page 224
- ◆ [“Removing SKIP Configuration”](#) on page 225

Upgrading an Earlier BorderManager Master to Novell BorderManager 3.8

- 1** Run the Novell BorderManager 3.8 installation on the master.
- 2** On the upgrade page, make sure the Migrate check box is selected (this is selected by default).
- 3** After the master is upgraded, verify that the configuration migration is successful by viewing the server and site-to-site configuration in the iManager VPN configuration pages.
- 4** Use the VPN console option 5 to verify that the master contains information about all the slaves.

Upgrading an Earlier BorderManager Slave to Novell BorderManager 3.8

- 1** Run the Novell BorderManager 3.8 installation on the slave.
- 2** In the upgrade page, make sure the Migrate check box is selected (this is selected by default).
- 3** After the slave is upgraded, verify that the configuration migration is successful by viewing the slave server's configuration in the iManager VPN configuration page.
- 4** Using iManager, go to the slave and configure the slave for IKE.
 - 4a** Import the master's trusted root certificate as a TRO into the trusted root container of the slave
 - 4b** Add the certificate subject name of the master.
- 5** Using iManager, go to the master,
 - 5a** Import the slave's trusted root certificate as a TRO into the master's trusted root container.
 - 5b** Add the slave member to the site-to-site member configuration.

Adding a New Novell BorderManager 3.8 Slave to a Partially or Fully Upgraded Setup

- 1** Run the Novell BorderManager 3.8 installation on the slave. Because this is not an upgrade, the configuration migration does not take place.
- 2** In iManager, complete the following steps:
 - 2a** Go to the slave and configure the slave for IKE. For information, refer to [“Configuring a VPN Server As a Slave Server” on page 210.](#)
 - 2b** Go to the master and add this slave as a Novell BorderManager 3.8 slave. For information, refer to [“Configuring a VPN Server As a Slave Server” on page 210.](#)
At this point, the new slave is able to receive the configuration from the master, and also communicate with the other Novell BorderManager 3.8 slaves.
- 3** [Conditional] If this slave is required to communicate with the other earlier BorderManager slaves in a partially upgraded setup, add SKIP configuration using VPNCFG. Then add the slave as a SKIP slave using NWAdmn.

IMPORTANT: It is important for the Novell BorderManager 3.8 slave to be configured first for IKE. After that, configure the SKIP.

Adding a New BorderManager 3.7 Slave to an Existing Novell BorderManager 3.8 Setup

Although this scenario is not recommended, it is supported in this release.

Configure the earlier BorderManager slave using VPNCFG and add it as an earlier BorderManager slave using NWAdmn. After this is done, the slave is able to communicate with the master and the other BorderManager slaves configured for SKIP.

Removing SKIP Configuration

After all the earlier BorderManager slaves are upgraded to Novell BorderManager 3.8 and are configured for IKE, the SKIP configuration can be removed first from the slaves and finally from the master.

- 1** Go to NWAdmn and remove the slave from the earlier BorderManager network.
- 2** Use NWAdmn Monitoring to verify that the removal of slave has taken effect on the master.
- 3** Go to the slave and remove the SKIP configuration using VPNCFG. Repeat steps 1 to 3 for all the slaves.
- 4** When all the slaves are removed from the earlier BorderManager network, use VPNCFG to remove the master's SKIP configuration.

NOTE: Sometimes removing SKIP configuration will bring the VPN service down. Restart the VPN service with a stopvpn and startvpn sequence.

19

Monitoring Virtual Private Networks

The following sections describe the statistics used to monitor the operation of Novell® BorderManager® 3.8 Virtual Private Network (VPN). The VPN monitoring component is available through NetWare Remote Manager (NRM). This section contains information on the tasks a user can do using the NRM. For details on every field see the help on each page. The help is available on the upper right corner on each page and can be invoked using the (i) icon.

This section contains the following:

- ♦ “Logging into NetWare Remote Manager” on page 227
- ♦ “Checking the VPN Real-Time Monitor” on page 229
- ♦ “Checking the Audit Log on a VPN Server” on page 233
- ♦ “Checking the Activity of a VPN Server” on page 236

NOTE: VPN Monitoring through NRM is available only for Novell BorderManager 3.8 servers. If your site-to-site setup has both Novell BorderManager 3.8 members and BMEE 3.6/NBM 3.7 members, then VPN Monitoring through NRM will only list the BMEE 3.6/NBM 3.7 members in the member list. You can monitor only the Novell BorderManager 3.8 members using the NRM VPN Monitoring utility. For monitoring Novell BorderManager 3.7 members, you still need to use NWAdmn. The Synchronize All Servers/Synchronize Selected Servers facility provided in VPN Monitoring through NRM synchronizes only the Novell BorderManager 3.8 members. For synchronizing the BMEE 3.6/NBM 3.7 members, you still need to use the Synchronize option available in NWAdmn.

Logging into NetWare Remote Manager

- 1 Specify the IP address in the browser with port 8009 (<https://ip address:8009>)
- 2 Specify the login name and password.
- 3 From the NRM on the browser, select NBM Monitoring > VPN Monitoring in the left pane.

Figure 69 VPN Monitoring



- The member name, type, IP address, and status are displayed. You can use this framework to monitor the real time, audit log, and activity.

Figure 70 Member List

VPN Member List				
Member Name	Type	IP Address	Status	
<input type="checkbox"/> MANISHA_VPN	Master	164.99.159.247	Up-to-date	
<input type="checkbox"/> sreeni-slave	Slave	164.99.159.122	Being Configured	

Synchronize Selected Servers Synchronize All Servers

Status: Up-to-date is an indication that everything is working fine. Being Configured indicates that the configuration information has not been fully received by the slave.

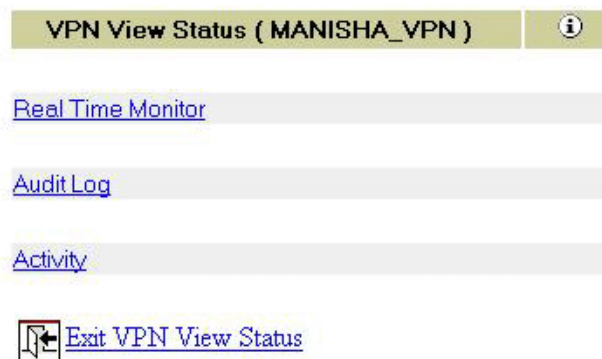
Synchronization: This is an important feature used to distribute configuration information from a master server to slaves. This feature is available only in NRM-based VPN Monitoring

and is applicable only to Novell BorderManager 3.8 servers. In order to synchronize slaves of earlier versions of BorderManager, use NWAdmn. Synchronization can be done in two ways:

- ◆ Synchronize selected servers: Click the check box to select certain servers, then click the Synchronize Selected Servers button.
- ◆ Synchronize all servers: Click the Synchronize All Servers button to synchronize all members at the same time. Synchronization of all servers pushes the information from the master server to all other servers.

IMPORTANT: This list is visible if the server is a master. If the server is a slave, the VPN View Status page is directly displayed without an Exit link.

Figure 71 VPN View Status



TIP: For a full screen view, specify the port and /VPN (https://ip address:8009/VPN). The right pane occupies the full screen and the left pane is suppressed.

Checking the VPN Real-Time Monitor

The VPN real-time monitor page displays the information of a selected VPN member and its associated VPN connections.

In the NRM VPN view status menu (see [Figure 71, “VPN View Status,” on page 229](#)) click the Real Time Monitor link for a selected member to display a page with the following information:

Figure 72 Connection Information for the Selected Member

Virtual Private Network Monitor (MANISHA_VPN) i

Active Connections 3

Packets Received 8779

Packets Sent 10492

Page Refresh Interval : Sec

Connected Node	Connection Name	Key Management Type	Connection Type
164.99.159.122	sreeni-slave	IKE	Server
164.99.167.125 (55.55.55.55)	O=novell,CN=admin	IKE	Client
164.99.145.16	admin.novell	SKIP	Client

This page provides detailed real-time information of the list of members and clients connected to the selected member.

- ◆ **Connected Node:** These are the IP addresses of the listed clients and members. They are links to detailed information for each of them. The addresses in the brackets are unique IP addresses assigned by the VPN gateway.
- ◆ **Connection Name:** For servers, the connection name is the VPN name of the server. For clients, the connection name is as follows:
 - ◆ For the Novell BorderManager 3.8 client, when the key management type is IKE the connection name is either the certificate subject name if user connects in certificate mode (for example o=novell, CN=admin), the eDirectory/NDS FDN username if the user is an NMAS user (for example admin.novell), or the LDAP FDN username if the user is an LDAP user (for example CN=admin).
 - ◆ For any earlier version of the BorderManager client or Novell BorderManager 3.8 client in backward compatibility mode, the connection name is the eDirectory/NDS FDN username (for example admin.novell).
- ◆ **Key Management Type:** The key management type of the connections could be IKE or SKIP. If the connections are behind NAT, the key management type is NATed IKE or NATed SKIP. If the key management is Unknown Type, it indicates that the connection with the associated member is lost. There is no IKE SA, but the server is still configured as a slave to the site-to-site network.
- ◆ **Connection Type:** The connections could be VPN servers (master or slave) or clients.
- ◆ **Page Refresh Interval:** The Page Refresh Interval is an editable field and can be used to alter the refresh interval. The minimum limit here is 10 seconds.

If the real-time monitor page shows a connection as type Server with the key management type as unknown, the server might be configured as a site-to-site member of the network but there might not be any active connection between the two servers.

Figure 73 Detailed Information for a SKIP Connection


Virtual Private Network Monitor (164.99.145.16)		
Connection Name	admin.novell	
Connection Type	Client	
Bytes Sent	132 Bytes	
Bytes Received	296 Bytes	
Connection Uptime	0 days 0: 3:11	
Encryption Type	RC5-CBC	
Key Size	128	
Key Life Time	1000	
Key Changes	0	
IP Packets Sent	1	
IP Packets Received	2	
IPX Packets Sent	0	
IPX Packets Received	0	
Authentication Type	KEYED-MD5	
Authentication Size	128	
Time to Disconnect	0 days 0:12: 1	

Figure 74 Detailed Information for an IKE Connection

Virtual Private Network Monitor (55.55.55.55)					i	
Connection Name	O=novell.CN=admin					
Connection Type	Client					
Bytes Sent	0 Bytes					
Bytes Received	0 Bytes					
Connection Uptime	0 days 0: 3:15					
IP Packets Sent	0					
IP Packets Received	0					
IPX Packets Sent	0					
IPX Packets Received	0					
Time to Disconnect	0 days 0:11:42					
PFS Enabled	Yes					
IKE Key LifeTime	3600					
IKE Key Changes	0					
IKE Authentication Method	CERTIFICATE					
IKE Encryption Algorithm	3DES CBC					
IKE Authentication Algorithm	SHA-1					
Active Policies						
Protected Networks	Protocol	Port	Key Life Time(secs)	Algorithm(enc/auth)		
Any	Any	Any	900	3DES/HMAC-MD5		
Any	Any	Any	900	3DES/HMAC-MD5		
		Refresh		Back		

IKE key management parameters like encryption algorithm, authentication algorithm, and authentication method (Certificate/Pre-shared key/NMAS) are displayed here.

Active Policies: The policies displayed in the lower box on the page are active traffic rules enforced for a connection. Click a traffic rule to see the packets passed because of this traffic rule. If a traffic rule is configured as Deny it won't be displayed here. If the same policy is displayed twice, one of the policies is about to expire and a new SA is being negotiated. The algorithm shown here is used to protect the data traffic.

Figure 75 Policy Statistics for an Active Traffic Rule

Virtual Private Network Monitor (164.99.159.122)
i

Connection Name	sreeni-slave
Connection Type	
Bytes Sent	
Bytes Received	
Connection Uptime	
IP Packets Sent	
IP Packets Received	
IPX Packets Sent	
IPX Packets Received	
Time to Disconnect	
PFS Enabled	
IKE Key LifeTime	
IKE Key Changes	
IKE Authentication Method	
IKE Encryption Algorithm	
IKE Authentication Algorithm	

Policy Statistics

IP Packets Sent	16
IP Packets Received	13
IPX Packets Sent	0
IPX Packets Received	0
Total Packets Discarded(Sent)	0
Total Packets Discarded(Recv)	0
Authentication Key Size	128
Encryption Key Size	192

Protected Networks	Protocol	Port	Key Life Time(secs)	Algorithm(enc/auth)
n/a	TCP	213	1000	3DES/HMAC-MD5
n/a	Any	Any	900	3DES/HMAC-MD5
n/a	TCP	213	1000	3DES/HMAC-MD5

Checking the Audit Log on a VPN Server

The VPN audit log enables you to view audit log messages generated by a VPN server. You can also view a detailed explanation of any message by clicking on the Audit Log messages in the box in the lower part of the page.

To display a VPN audit log, in the NRM VPN view status menu (See [Figure 71, “VPN View Status,” on page 229](#)), click the Audit Log link for a selected member to display a page with the following information.

Figure 76 Audit Log Page

Audit log information for MANISHA_VPN

Audit Log Provider
 VPN Control
 VPN Tunnel
 Authentication gateway
 IP Security
 SKIP Key Management
 IKE key management

Audit Log Level
 Error

Detailed

 Informational

Detailed

Audit Log Start
 Date

9/23/2003

 Time

03:00:03 AM

Audit Log End
 Date

9/23/2003

 Time

06:15:56 PM

Valid AuditLog Range
 Start Date/Time

9/16/2003 03:34:58 AM

 End Date/Time

9/23/2003 06:15:59 PM

Audit Log Progress
 Last Audit Date/Time

9/23/2003 06:10:54 PM

 Phase Entries

10

Audit log Messages

i	9/23/2003	06:14:30 PM	IKE	ESP SA was created successfully with 164.99.159.122
i	9/23/2003	06:14:30 PM	IKE	Received notify message of type CONNECTED : 16384 from 164.99.159.122
i	9/23/2003	06:14:30 PM	IKE	Received proxy Id : IPV4 SUBNET 0.0.0.0/0.0.0.0
i	9/23/2003	06:14:30 PM	IKE	Received proxy Id : IPV4 SUBNET 0.0.0.0/0.0.0.0
i	9/23/2003	06:14:30 PM	IKE	IPSEC SA NEGOTIATION - Peer lifetime is: 1000 My lifetime is: 1000
i	9/23/2003	06:14:30 PM	IKE	Sending proxy id : Type 4 0.0.0.0/0.0.0.0
i	9/23/2003	06:14:30 PM	IKE	Sending proxy id : Type 4 0.0.0.0/0.0.0.0
i	9/23/2003	06:12:24 PM	IKE	ESP-SA is deleted mySPI=12E538C4 peerSPI=987551D0 dst :164.99.159.122
i	9/23/2003	06:12:24 PM	IKE	Received delete msg from 164.99.159.122

This page provides detailed audit logs of the list of members and clients connected to the selected member. This is nearly same as the NetWare CSAUDIT facility.

- ◆ **Audit Log Provider:** You can enable any one or more of the Audit Log Providers in the group box to view the desired messages.
- ◆ **Audit Log Level:** The Audit Log Level in the group box can be error or informational or both. Messages are subcategorized as Detailed, Medium and User.
- ◆ **Audit Log Start and End:** The Audit Log Start and End group box can be used to set the desired start and end date and time during which the messages were logged. Set the time according to the Valid Audit Log Range.
- ◆ **Valid Audit Log Range:** The Valid Audit Long Range group box displays the valid start and end time. This sets the limit for Audit Log Start and End.
- ◆ **Audit Log Progress:** The Audit Log Progress group box provides the date and time of the currently displayed last Audit Log message. The Phase Entries field provides the number of entries displayed in the list below. This is also an editable field.

IMPORTANT: After any change to the attributes, click Acquire to see the audit log messages.

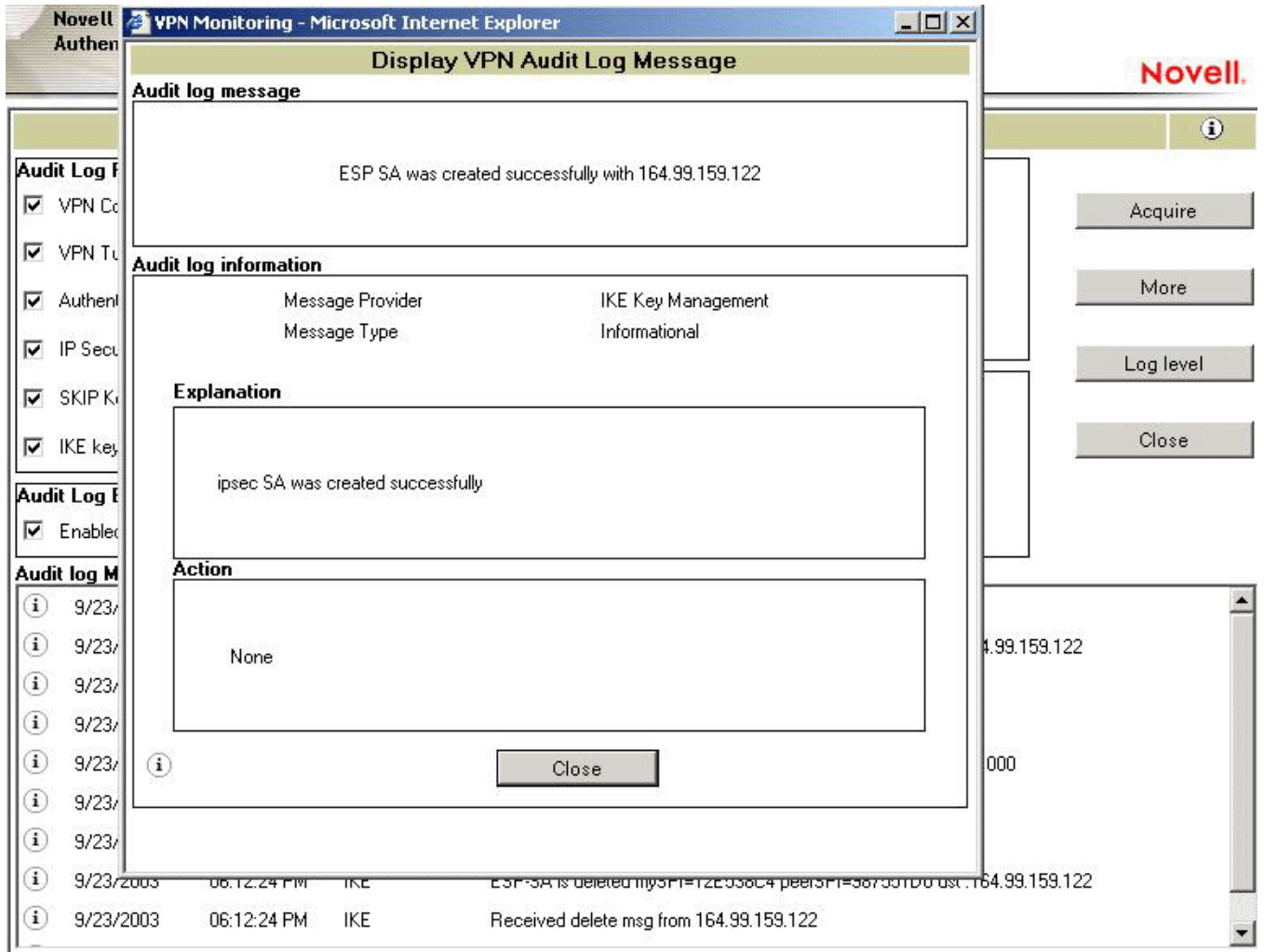
Audit Log Messages

When you click Acquire, Audit Log messages are displayed in the box towards the lower part of the page. The audit log messages show information for various activities that are taking place on

the server. The administrator can use the audit log facility to understand what went wrong for authentication failures, or what could have been the cause of failure during IKE negotiation. Click More to view messages that cannot be displayed in the available space.

You can obtain a detailed explanation of any audit log message by clicking the message. For error messages, a brief corrective action is displayed as shown below.

Figure 77 Audit Log Message Details



Log Level

In the page shown in Figure 76, "Audit Log Page," on page 234, pressing Log Level displays the dialog box shown below. This dialog box helps you set the log levels for a selected server. In the following page the user is setting the log level to log detailed error and informational messages for the selected audit log types which excludes logging of VPN Control and SKIP Key Management.

Figure 78 Log Level



Select the check boxes to provide error or informational messages of the following types:

- ◆ **VPN Control:** Provides the messages from VPMaster or VPSlave.
- ◆ **VPN Tunnel:** Provides messages related to establishment or failure of the tunnel.
- ◆ **Authentication Gateway:** Provides the messages related to client-to-site authentication (user password information).
- ◆ **IP Security:** Provides messages related to TCP/IP and IP Sec modules.
- ◆ **SKIP Key Management:** Provides key management messages related to earlier versions of the BorderManager client or the Novell BorderManager 3.8 client in backward compatibility mode.
- ◆ **IKE Key Management:** Provides key management messages for Novell BorderManager 3.8 clients.

Checking the Activity of a VPN Server

The VPN Activity page displays the activities of a selected VPN member and its associated VPN connections.

In the NRM VPN view status menu (see [Figure 71, “VPN View Status,” on page 229](#)), click the Activity link for a selected member.

Figure 79 Activities of a VPN server

VPN Member Activity : MANISHA_VPN i

<p>Associated Connections: 1</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 15%;">IPX</th> <th style="width: 15%;">IP</th> <th style="width: 70%;">Connection</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"></td> <td style="text-align: center;"></td> <td>sreeni-slave</td> </tr> </tbody> </table> <p>Associated connection details</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Associated connection</td><td>sreeni-slave</td></tr> <tr><td>Associated address</td><td>164.99.159.122</td></tr> <tr><td>Time to disconnect</td><td>Unlimited</td></tr> <tr><td>Total bytes sent</td><td>1,717,104</td></tr> <tr><td>Total bytes received</td><td>2,247,856</td></tr> <tr><td>Send packets discarded</td><td>0</td></tr> <tr><td>Receive packets discarded</td><td>0</td></tr> </table> <p>IPX associated connection details</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Connection state</td><td>Unattached</td></tr> <tr><td>Call direction</td><td>None</td></tr> <tr><td>Time active</td><td></td></tr> <tr><td>Packets sent</td><td></td></tr> <tr><td>Packets received</td><td></td></tr> </table> <p>IP associated connection details</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Connection state</td><td>Established</td></tr> <tr><td>Call direction</td><td>Outgoing</td></tr> <tr><td>Time active</td><td>3:05:46:01</td></tr> <tr><td>Packets sent</td><td>10,491</td></tr> <tr><td>Packets received</td><td>8,777</td></tr> </table>	IPX	IP	Connection			sreeni-slave	Associated connection	sreeni-slave	Associated address	164.99.159.122	Time to disconnect	Unlimited	Total bytes sent	1,717,104	Total bytes received	2,247,856	Send packets discarded	0	Receive packets discarded	0	Connection state	Unattached	Call direction	None	Time active		Packets sent		Packets received		Connection state	Established	Call direction	Outgoing	Time active	3:05:46:01	Packets sent	10,491	Packets received	8,777	<p>Global details</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Tunnel status:</td><td>Loaded</td></tr> <tr><td>Tunnel time active:</td><td>3:05:46:01</td></tr> <tr><td>IPX packets sent</td><td>0</td></tr> <tr><td>IPX packets received</td><td>0</td></tr> <tr><td>IP packets sent</td><td>12,398</td></tr> <tr><td>IP packets received</td><td>38,251</td></tr> <tr><td>Total packets sent</td><td>12,398</td></tr> <tr><td>Total packet received</td><td>38,251</td></tr> <tr><td>Total bytes sent</td><td>2,168,000</td></tr> <tr><td>Total bytes received</td><td>7,923,908</td></tr> <tr><td>Total send packet discarded</td><td>0</td></tr> <tr><td>Total received packet discarded</td><td>64</td></tr> <tr><td>IKE Status</td><td>Up</td></tr> <tr><td>Main mode attempted count</td><td>116</td></tr> <tr><td>Main mode failure count</td><td>24</td></tr> <tr><td>Quick mode attempted count</td><td>598</td></tr> <tr><td>Quick mode failure count</td><td>0</td></tr> <tr><td>Successful PSS Authentications</td><td>4</td></tr> <tr><td>Failed PSS Authentications</td><td>0</td></tr> <tr><td>Successful NMAS Authentications</td><td>n/a</td></tr> <tr><td>Failed NMAS Authentications</td><td>n/a</td></tr> <tr><td>Successful x509 Authentications</td><td>12</td></tr> <tr><td>Failed x509 Authentications</td><td>0</td></tr> <tr><td>Successful LDAP Authentications</td><td>n/a</td></tr> <tr><td>Failed LDAP Authentications</td><td>n/a</td></tr> <tr><td>Total Backward compatibility authentications</td><td>n/a</td></tr> <tr><td>Failed Backward compatibility authentications</td><td>n/a</td></tr> </table> <p>More IKE Statistics...</p>	Tunnel status:	Loaded	Tunnel time active:	3:05:46:01	IPX packets sent	0	IPX packets received	0	IP packets sent	12,398	IP packets received	38,251	Total packets sent	12,398	Total packet received	38,251	Total bytes sent	2,168,000	Total bytes received	7,923,908	Total send packet discarded	0	Total received packet discarded	64	IKE Status	Up	Main mode attempted count	116	Main mode failure count	24	Quick mode attempted count	598	Quick mode failure count	0	Successful PSS Authentications	4	Failed PSS Authentications	0	Successful NMAS Authentications	n/a	Failed NMAS Authentications	n/a	Successful x509 Authentications	12	Failed x509 Authentications	0	Successful LDAP Authentications	n/a	Failed LDAP Authentications	n/a	Total Backward compatibility authentications	n/a	Failed Backward compatibility authentications	n/a
IPX	IP	Connection																																																																																													
		sreeni-slave																																																																																													
Associated connection	sreeni-slave																																																																																														
Associated address	164.99.159.122																																																																																														
Time to disconnect	Unlimited																																																																																														
Total bytes sent	1,717,104																																																																																														
Total bytes received	2,247,856																																																																																														
Send packets discarded	0																																																																																														
Receive packets discarded	0																																																																																														
Connection state	Unattached																																																																																														
Call direction	None																																																																																														
Time active																																																																																															
Packets sent																																																																																															
Packets received																																																																																															
Connection state	Established																																																																																														
Call direction	Outgoing																																																																																														
Time active	3:05:46:01																																																																																														
Packets sent	10,491																																																																																														
Packets received	8,777																																																																																														
Tunnel status:	Loaded																																																																																														
Tunnel time active:	3:05:46:01																																																																																														
IPX packets sent	0																																																																																														
IPX packets received	0																																																																																														
IP packets sent	12,398																																																																																														
IP packets received	38,251																																																																																														
Total packets sent	12,398																																																																																														
Total packet received	38,251																																																																																														
Total bytes sent	2,168,000																																																																																														
Total bytes received	7,923,908																																																																																														
Total send packet discarded	0																																																																																														
Total received packet discarded	64																																																																																														
IKE Status	Up																																																																																														
Main mode attempted count	116																																																																																														
Main mode failure count	24																																																																																														
Quick mode attempted count	598																																																																																														
Quick mode failure count	0																																																																																														
Successful PSS Authentications	4																																																																																														
Failed PSS Authentications	0																																																																																														
Successful NMAS Authentications	n/a																																																																																														
Failed NMAS Authentications	n/a																																																																																														
Successful x509 Authentications	12																																																																																														
Failed x509 Authentications	0																																																																																														
Successful LDAP Authentications	n/a																																																																																														
Failed LDAP Authentications	n/a																																																																																														
Total Backward compatibility authentications	n/a																																																																																														
Failed Backward compatibility authentications	n/a																																																																																														

Update
Clients
Reset
Close

This page provides detailed information on activities of a selected member. This page provides information on servers or clients, depending on what you choose to display by clicking the Server/Client button on the right. By default, the page shows the associated members (servers). The icon on the lower-right side of the page indicates whether you are on the server page or client page.

IMPORTANT: The Client button in the illustration above toggles between displaying clients and servers. The Reset button is associated with the Server page, and the Disconnect button is associated with the Client page. The reset and disconnection applies to only those entities from the list that are selected using the option button on the left.

- ◆ **Associated Connections:** Shows you a count of server or client connections. The box on the upper left shows a list of connected servers or client with the status of IPX or IP. For servers, the connection name is the VPN name of the server. For clients, the connection name is the login name of the client.
 - TIP:** For details on each of the status icons, see the online help or see the associated tool tip.
- ◆ **Associated Connection Details:** Provides information about the connections between the selected VPN member and associated VPN member with respect to the tunnel connection.
- ◆ **IPX Associated Connection Details:** Provides information about the connections between the selected VPN member and associated VPN member with respect to the IPX tunnel connection.
- ◆ **IP Associated Connection Details:** Provides the connection information between the selected VPN member and associated VPN member regarding the IP tunnel connection.

- ◆ **Global Details:** Shows the global VPN connection information for the selected VPN member.

20 Virtual Private Network Client

The Novell® BorderManager®r VPN client software allows a workstation to communicate securely over the Internet to a network protected by a Novell VPN server.

The Novell BorderManager 3.8 VPN client is new and overrides all earlier versions of the VPN client.

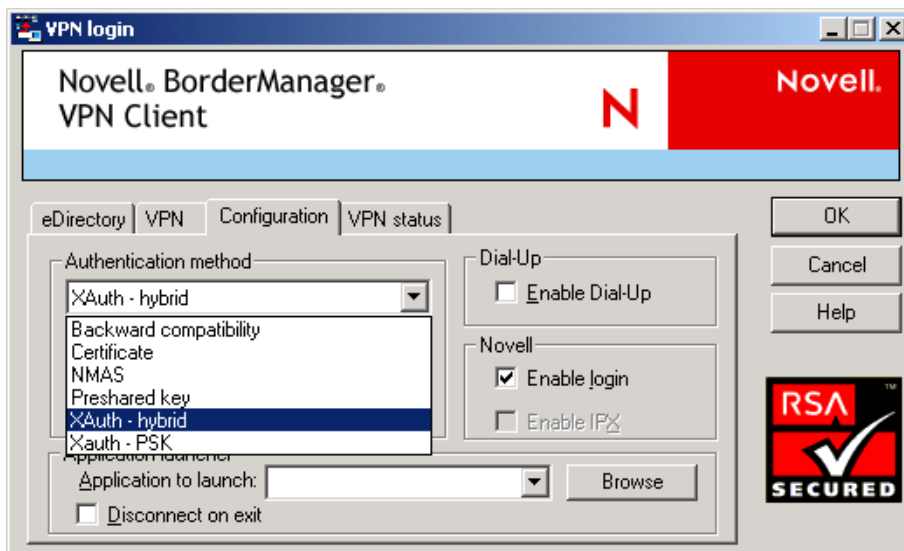
This section discusses the following:

- ♦ “GUI changes for VPN Client” on page 239
- ♦ “VPN Client Features” on page 239
- ♦ “VPN Client Installation” on page 244
- ♦ “VPN Client Silent Install” on page 244

GUI changes for VPN Client

Radio buttons used for selecting authentication mode has been replaced by dropdown boxes. See the following figure:

Figure 80 Radio buttons replaced by dropdown box for selecting authentication mode



VPN Client Features

The following features are available in the VPN client software:

- ◆ “X.509 Certificate Authentication Mode” on page 240
- ◆ “NMAP Authentication Mode” on page 240
- ◆ “NMAP LDAP Authentication Mode” on page 241
- ◆ “Backward Compatibility Mode” on page 241
- ◆ “Pre-shared Authentication Mode” on page 241
- ◆ “X-AUTH hybrid mode” on page 241
- ◆ “X-AUTH PSK Mode” on page 241
- ◆ “VPN Client Integration with the Novell Client” on page 242
- ◆ “Use NCI for Encryption” on page 242
- ◆ “Selecting Dial-Up Entries” on page 242
- ◆ “Automatic Creation of a Novell VPN Dial-Up Entry” on page 243
- ◆ “Password Expiry Notice” on page 243
- ◆ “VPN Server Hosts List” on page 243
- ◆ “Policy” on page 243
- ◆ “VPN Connections through NAT” on page 243

X.509 Certificate Authentication Mode

The Novell BorderManager 3.8 VPN client provides the user with a X.509 certificate and the server's trusted root to perform the IKE main mode of authentication. These two should be copied to the local workstation (<drive>:\novell\vpnc\certificates\users or *drive*:\novell\vpnc\certificates\trustedroot) from where VPN is to be executed.

Certificate Retrieval

The VPN client provides a feature to retrieve the user certificate from Novell eDirectory™. If the Novell Client™ is installed, this option is enabled for the user to retrieve his or her certificate. To retrieve a user certificate you must provide the username, password, context, and IP address (optional) and the user certificate name (such as adminCert). This will retrieve the user certificate and store it in *drive*:\novell\vpnc\certificates\users as AdminCert.pfx. If a user has more than one certificate it will store them as AdminCert(n).pfx (n = 1..n)

Local Policy

In the Certificate mode of authentication, the user can provide IKE and IPsec parameters by clicking the policy editor on the VPN tab. This policy will mandate to the VPN server if the server is not imposing any policy. The proposal part will take precedence if connecting to a Novell BorderManager 3.8 VPN server and the IPsec policy and traffic rule will not take effect. For third-party servers this proposal is preferred and the IPsec policy and traffic rule are applied on outgoing traffic.

NMAP Authentication Mode

Novell VPN client is integrated with Novell Modular Authentication Services (NMAP™). NMAP works with the Novell Client, so you must install the Novell Client to benefit from the NMAP functionality.

Select the NMAS option in the configuration tab and provide NMAS user information and credentials in the eDirectory tab. In the VPN tab, provide the VPN server IP address and NMAS sequence (for example, NDS/eDirectory, Universal Smart Card, Simple Password and so on). The method displays a dialog box.

When users uninstall the Novell Client 4.9, they also need to uninstall NMAS. Leave the methods installed and remove only the client.

NMAS LDAP Authentication Mode

Select NMAS and select the LDAP check box on the Configuration page. Go to the VPN page and specify the VPN server IP address and LDAP user DN (for example, CN=Admin,O=Novell). The LDAP method displays a dialog box for the credential.

Backward Compatibility Mode

Select Backward Compatibility mode on the Configuration tab. Provide eDirectory credentials on the eDirectory page. In this mode, the Novell BorderManager 3.8 Client communicates with the Novell BorderManager server (BMEE 3.6, Novell BorderManager 3.7, Novell BorderManager 3.8) in SKIP mode. The ActiveCard token authentication is enabled if NMAS is installed on the client. The ActiveCard token authentication method works if the ActiveCard token method is configured for the user in eDirectory. The VPN page requires credentials for ActiveCard token method.

Pre-shared Authentication Mode

Select Pre-shared Authentication Mode on the Configuration page. Go to the VPN page and provide the pre-shared key configured in the VPN server.

The pre-shared key (PSS) mode of authentication is supported only for the purpose of debugging and for standards compliance. Traffic rules for the pre-shared key mode cannot be set using the iManager configuration snap-ins. Instead, you can use the set parameters on the server console to specify a single traffic rule for PSS.

X-AUTH hybrid mode

Select X-Auth hybrid mode under Authentication Method in the Configuration page. Click the VPN tab and in the page provide VPN server IP address, username, and password. User need to copy the trusted root certificate corresponding to the server.

VPN Server IP Address is the the IP address of the VPN server and username need to be specified as required in the server(3rd Party Server only).

NOTE: Xauth Hybrid mode will be supported in aggressive mode only and this has to be enabled in the policy editor. The policy editor page opens on clicking the Policy Editor button in the VPN page.

X-AUTH PSK Mode

Select X-Auth PSK under Authentication Method in the Configuration page. Go to the VPN page by clicking the VPN tab and provide the VPN Server IP address, username, password and shared secret.

VPN Server IP_Address is the the IP address of the VPN server and username is the full DN name. Eg. john.novell

Shared Secret :This is used for IKE Phase1 authentication. The shared secret should be the one configured in the server.

NOTE: While connecting to NBM Server, put the IKE mode in main mode along with PFS=yes in the policy editor.

VPN Client Integration with the Novell Client

This version of the Novell VPN client will integrate into the Novell Client for Windows 98, Windows NT, Windows 2000, or Windows XP Home. Restart the machine after installing the new VPN client; during the restart, the VPN client integrates with the Novell Client. After the system comes up, the Novell Login page has a Location drop-down list. The list contains the default entry as well as an entry for the VPN capabilities. You can select any of the locations, depending on the operation to be performed.

Four new tabs are available that can be configured in a Service Instance by selecting Novell Client32 Properties. The four tabs do the following:

- ◆ Configuration: Provides the authentication mechanism for the VPN client as well as for dial-up, Novell login, the IPX option, and the launcher to launch applications after VPN connection.
- ◆ VPN: Provides credentials for the authentication type listed on the Configuration page.
- ◆ Dial-Up: Performs the dial-up operation. This option appears on the configuration page if dial-up is enabled.
- ◆ VPN Status: Displays the status of the VPN dial-up and authentication.

Use NICI for Encryption

This version of VPN client for Windows 98, Windows Me, Windows NT, Windows 2000, and Windows XP uses NICI (128-bit) encryption because there are no export restriction with NICI.

If NICI 1.7.0 (128-bit version) is not installed, the VPN Setup program installs it. This version of NICI overwrites NICI 1.5.7 (56-bit) or NICI 1.5.3 (56/128-bit), but not NICI 2.6.0. If NICI 2.6.0 is installed, NICI 1.5.7 and 2.6.0 will co-exist.

Selecting Dial-Up Entries

On Windows 98 and Windows Me, you can select a dial-up entry of any server type. Previously (with Novell BorderManager Enterprise Edition 3.0), you could only select dial-up entries of type Novell Virtual Private Network. All entries must be configured to negotiate only for TCP/IP connections. If you want to invoke the VPN client from Dial-Up Networking instead of vpnlogin.exe, then the dial-up entry that you select from Dial-Up Networking must be of server type Novell Virtual Private Network; otherwise, vpnlogin.exe is not spawned after the dial-up connection is established.

On Windows NT, you can select a dial-up entry of any server type. There is no Novell Virtual Private Network server type from the Dial-Up Networking selection on Windows NT.

If there is a dial-up requirement, install dial-up networking before you install the VPN client.

When you make your dial-up entry selection from VPNLogin.exe, choose entries that do not enable Point-to-Point Protocol (PPP) compression.

Compressing data that has been encrypted incurs unnecessary CPU overhead and does not offer any savings in the size of the packets being sent.

Install the modem, then install the VPN client.

Automatic Creation of a Novell VPN Dial-Up Entry

During VPN client installation, if you choose to use Dial-Up Networking, the VPN client installation creates a Novell VPN dial-up entry for you.

Password Expiry Notice

During VPN client login, the eDirectory user is notified if the user's eDirectory password has expired and grace logins are being used. The user is also given an option to change the eDirectory password during VPN Client login. This option is also provided via the VPN Client task bar. Users see the Change Password option only if they are using eDirectory credentials for VPN or NetWare login from the VPN client application. Change Password will fail for contextless login. It requires eDirectory user credentials.

VPN Server Hosts List

If you have a file named `vpnhost.txt` in your VPN client installation directory, the installation program will take IP addresses from this file and specify them into the workstation's registry. Each line of the `vpnhost.txt` file can contain one IP address, optionally followed by a description of the entry. For example:

```
130.1.1.1 My Corporate VPN in Bangalore.
```

Policy

The policy specified by the administrator in eDirectory is applied on the client. If a policy is changed for that particular VPN user while a VPN session is active, the changes are not reflected until the next session.

VPN Connections through NAT

NAT support on the VPN client provides IKE-NAT Traversal and UDP encapsulation in addition to the NAT support provided by earlier versions of Novell BorderManager. IKE-NAT traversal and UDP encapsulation is the standard used in the industry.

Make sure that the NAT supports the ESP protocol. If you are using Netware NAT, download the latest `nat.nlm` from the folder `filtersrv\system` directory in the product CD. This NAT supports ESP.

If the NAT gateway and any NetWare server are in the same subnet and RIP is enabled on both of them, the users can not communicate between the VPN servers.

NOTE: Because of the standard IKE support, the VPN server can be behind NAT and the VPN client can still connect to it using the IP address of the NAT instead of the server's IP address. This prevents the VPN server from being exposed to public networks.

VPN Client Installation

This section discusses the installation of the VPN client. The VPN client software is available on the Novell BorderManager 3.8 product CD.

- 1** Unzip the file on your local drive.
- 2** Follow the on-screen prompts to set up the product. The installation will configure the parameters associated with a secure connection.
- 3** When prompted, choose either or both of the following options:
 - ◆ Dial-Up VPN client
 - ◆ NMAS client

Choose one or both depending upon your need.

- 4** When prompted, choose either or both of the following NICI versions:
 - ◆ NICI 1.7.0 (128-bit)
 - ◆ NICI 2.6.0 (128-bit)

After the installation is complete, restart the machine for the VPN client software to work properly.

VPN Client Silent Install

This version of the VPN client supports the silent install feature, which allows the installation to be completed without user input. If the Dial-Up option is selected, some user intervention may be required if the workstation does not have the Dial-Up Networking or RAS components

To use this feature, you run SETUP.EXE with a switch to create a response file that contains the answers to all the questions normally asked during installation. Because this includes selection of the dial-up client, the LAN client, or both, you may need to create multiple response files based on user needs.

After creating the response file, you can then run SETUP.EXE with a different switch to use the response file so that installation requires minimal user intervention. There is also a switch to generate a log file for the silent install. This can be used to verify that the install completed successfully, or to diagnose why the installation failed. Examples on how to use these switches are given below.

You may often need to do a "silent install" on workstations that have different versions of Windows. If Windows or the Novell Client was from CD, then the VPN client install will ask for those installation CDs. In this situation, since the responses to the install prompts will depend on the version of Windows that is installed, it is best to create a response file that will query the user for these installation CDs if needed.

To create this kind of a response file:

- 1** Perform a normal install of the VPN client without creating the response file. This installation may ask for the Windows and/or Novell Client CDs. Proceed normally through the installation.
- 2** After rebooting, run SETUP.EXE again, this time creating the response file. This re-install will not query for the Windows or Novell Client install CDs, so the generated response file will not know what to answer when the user installation asks for the Windows or Novell Client

CD. Because there is no answer in the response file, the user will be queried for the Windows or Novell Client CDs if they are needed

To verify that the response file is working properly, run the installation in silent mode on a workstation that does not have VPN client installed. The install log file should show ResultCode=0.

The silent install feature only works with the SETUP.EXE under the disk1 directory. It does not work with the self-extracting exe.

The silent install feature is enabled by executing SETUP.EXE under the disk1 directory with certain command-line options. The available options for SETUP.EXE are:

- r - Run the installation and capture the response
- s - Run the installation in silent mode.

Depending on which of the two options is being used, the -f1 and -f2 options may also be used to specify names files.

To use the silent install feature:

- 1** Create a response file by issuing the following command from disk1 of the VPN client disks:

```
setup.exe -r -f1"<RESPONSE_FILE>"
```

where <RESPONSE_FILE> contains the absolute path and name of the response file. The -f1"<RESPONSE_FILE>" option may be omitted, in which case a response file named SETUP.ISS is created in the Windows or WinNT directory.

For example,

```
setup.exe -r -f1"c:\temp\setup.iss" executes the installation and saves the input to
c:\temp\setup.iss
```

NOTE: When using the -f1 and -f2 switches, do not put a space before the quote sign. For example: -f1 "filename" won't work. -f1"filename" will work.

- 2** Execute the installation based on previously captured input by issuing the following command from disk1 of the VPN client disks.

```
setup.exe -s -f1"<RESPONSE_FILE>" -f2"<LOG_FILE>"
```

where <RESPONSE_FILE> contains the absolute path and name of response file, and <LOG_FILE> contains the absolute path and name of log file.

For example, setup.exe -s -f1"c:\temp\setup.iss" -f2".\setup.log" executes the installation, taking input from setup.iss in the c:\temp directory, and records the result in the file setup.log in the same directory as setup.exe.

- 3** Verify that the silent install was successful by checking the contents of setup.log. You should see a result section with the following:

```
[ResponseResult]
```

```
ResultCode=0
```

A value of 0 for ResultCode indicates that installation was successful. A nonzero value indicates failure. The possible ResultCode values are:

- 0 Success.
- 1 General error.
- 2 Invalid mode.
- 3 Required data not found in the SETUP.ISS file.

- 4 Not enough memory available.
- 5 File does not exist.
- 6 Cannot write to the response file.
- 7 Unable to write to the log file.
- 8 Invalid path to the InstallShield Silent response file.
- 9 Not a valid list type (string or number).
- 10 Data type is invalid.
- 11 Unknown error during setup.
- 12 Dialog boxes are out of order.
- 51 Cannot create the specified folder.
- 52 Cannot access the specified file or folder.
- 53 Invalid option selected.

The most common installation error code seen is -12. An error condition usually displays an error message dialog box requiring user input, such as "Click OK" to acknowledge the error. Because the response would not be in the response file, the silent install process assumes that the response file has the dialog boxes out of order and hence reports error -12.

A batch file may be used to further automate the silent install process. For example, you could create the following INSTALL.BAT in the DISK1 subdirectory: `setup.exe -s -f1"c:\vpninst\disk1\response.txt" -f2"c:\temp\vpninst.log" rem` This assumes that the VPN client has been extracted to `c:\vpninst`. `rem` It could be on a network drive, or somewhere else. Don't put a space between `-f1` and the quotation mark. If the VPN Login icon shows up on your desktop, reboot, and the VPN client installation will be over.

V

Network Address Translation

The following sections of the *Novell® BorderManager® 3.8 Installation and Administration* guide provide the basic information you need to set up Network Address Translation (NAT).

- ♦ [Chapter 21, “Setting Up NAT,” on page 249](#) provides information on how to set up Network Address Translation.
- ♦ [Chapter 22, “Advanced Configuration of NAT,” on page 253](#) gives the procedures you need to set up and configure various NAT features and parameters.
- ♦ [Chapter 23, “Managing Network Address Translation,” on page 257](#) gives tips and guidelines for monitoring NAT functionality.

21

Setting Up NAT

Novell® BorderManager® 3.8 Network Address Translation (NAT) allows IP clients on your local network to access the Internet without requiring you to assign globally unique IP addresses to each system.

In addition, NAT acts as a filter, allowing only certain outbound connections and guaranteeing that inbound connections cannot be initiated from the public network.

NAT configuration consists of selecting one of the following three modes:

- ♦ **Dynamic only:** Dynamic-only mode is used to allow clients on your private network to access a public network, such as the Internet.
- ♦ **Static only:** Static-only mode is used to allow clients on the public network to access selected resources on your private network, or to allow specified private hosts to access public hosts. Static-only mode requires the additional configuration of a network address translation table.
- ♦ **A combination of static and dynamic:** The combination static and dynamic mode is used when functions of both the static mode and the dynamic mode are required. The combination static and dynamic mode also requires the configuration of a network address translation table for the static mode.

This section contains the following topics:

- ♦ [“NAT Prerequisites” on page 249](#)
- ♦ [“Setting Up NAT on a Single Interface” on page 250](#)
- ♦ [“Setting Up NAT with Multihoming” on page 251](#)
- ♦ [“Completing Advanced Setup, Configuration, and Management Tasks” on page 252](#)

NOTE: This section describes the tasks required to set up an initial implementation of Novell BorderManager 3.8 NAT. For planning and conceptual information about NAT, refer the *Novell BorderManager 3.8 Overview and Planning Guide*, available in the online documentation.

Make sure you understand this information before setting up and configuring NAT.

NAT Prerequisites

Before configuring NAT, verify that the following prerequisites have been met:

- ♦ A registered IP address has been obtained for each public interface on the server.
- ♦ TCP/IP has been enabled for and bound to two interface boards (the public and private interfaces).

If your Novell BorderManager 3.8 installation was successful, this prerequisite has already been satisfied for at least one board.

- ♦ For interfaces that have TCP/IP enabled, IP packet forwarding has been enabled or static routing has been enabled to use a static routing table.

To enable IP packet forwarding from the server console, load INETCFG, select Protocols > TCP/IP, and change the status of IP Packet Forwarding from Disabled End Node to Enabled Router.

To configure static routing from the server console, load INETCFG, select Protocols > TCP/IP, enable LAN Static Routing, and select LAN Static Routing Table to enter static routes.

- ◆ An Internet Service Provider (ISP) connection has been configured with enough bandwidth for the number of users on your network.

If the Novell BorderManager 3.8 server does not provide the connection to the ISP, ensure that the server has a static route configured or that the router to the ISP is in the routing path of the Novell BorderManager 3.8 server.

NOTE: It is assumed that all clients that will use the NAT-enabled interface as a default route to the Internet have already been configured with a TCP/IP stack and an IP address. The IP addresses can be registered or unregistered addresses.

Setting Up NAT on a Single Interface

To enable and set up NAT on a LAN or WAN interface, complete the following steps:

- 1** At the server console, enter

```
LOAD INETCFG
```

- 2** Select Protocols > Bindings.
- 3** Select the appropriate interface with TCP/IP bound to it.

NAT can be set up on the private interface or the public interface.

The public interface is either a LAN or WAN interface that connects your router to the Internet or other public network. NAT is most commonly used on the public interface.

- 4** Select Expert TCP/IP Bind Options.
- 5** Select Network Address Translation.
- 6** Set Status to Dynamic Only, Static and Dynamic, or Static Only.
- 7** If you set Status to Static Only or Static and Dynamic, complete the following substeps to map private IP addresses to public IP addresses:
 - 7a** Select Network Address Translation Table.
 - 7b** Press Ins to open the Network Address Translation Entry window.
 - 7c** In the Public Address field, specify the public IP address to which a private address is mapped.
 - 7d** In the Private Address field, specify the IP address of the private host that you want public hosts to access using the public IP address.
 - 7e** Press Esc to add the entry to the NAT table.
 - 7f** For address translation of inbound requests, repeat the steps for each private host to be accessed by public hosts.
 - 7g** (Optional) If you selected Static Only for address translation of outbound requests, repeat the steps for each private host that you want to have access to the Internet through the NAT-enabled interface using a public address.

The public addresses can be on the same network or subnetwork as the primary IP address, or they can be on a different network or subnetwork. If the public addresses are on the same network or subnetwork, use multihoming, as described in [“Setting Up NAT with Multihoming” on page 251](#), to add secondary addresses to the NAT-enabled interface.

Each private host address can be mapped to only one public host address. To access IP hosts using the public address within the private network, ensure that the static address pair specifies the same address for both the public and private addresses.

If NAT is connected to the Internet using multi-access WAN links, you must add static routes on your external router so that packets that are destined to one of the public addresses can be routed to the NAT interface.

- 8** If you set Status to Static Only or Static and Dynamic, configure a secondary address for each public address you configured in the network address translation table.

Refer to [“Setting Up NAT with Multihoming” on page 251](#) for instructions on how to configure a secondary address.

- 9** Press Esc until you are prompted to update your changes, then select Yes.
- 10** Press Esc until you are prompted to exit INETCFG, then select Yes.
- 11** If you want the NAT configuration to take effect immediately, bring down and restart the server.

Setting Up NAT with Multihoming

Multihoming enables a server to have multiple IP addresses. Multihoming can be achieved by adding a secondary IP address to an existing interface or by physically adding another interface to the server and binding another IP address to it.

A secondary IP address added to an existing interface must be on the same network as the IP address already bound to that interface. If there are multiple interfaces and the secondary IP address being added is not valid on any of the existing networks, the address is rejected and an error message appears on the server console.

For example, if the IP addresses 130.57.0.1 and 10.0.0.1 are bound to two interfaces and you attempt to add 172.16.1.1 as a secondary IP address, it will be rejected because it does not belong to the same network as 130.57.0.1 or 10.0.0.1.

Multihoming is required for NAT when static mode is used.

For an example of using multihoming with NAT, refer to the NAT online documentation. For information about how to set up NAT for a particular implementation with Proxy Services or the Virtual Private Network (VPN), refer to the [Chapter 2, “Setting Up Proxy Services,” on page 31](#) or [Chapter 18, “Upgrading Virtual Private Networks,” on page 221](#).

When multihoming is used with a proxy server, a VPN, NAT, or any other TCP/IP application, an administrator must configure secondary addresses from the server console.

To configure secondary IP addresses for multihoming, complete the following steps:

- 1** At the server console, enter

```
LOAD INETCFG
```

- 2** Select Protocols.

3 If TCP/IP was not configured on the public interface during installation, enable TCP/IP under Protocols, then bind one IP address to the public interface under Bindings.

4 Press Esc until you are prompted to save your changes and select Yes.

5 Select Manage Configuration and Edit autoexec.ncf.

6 Add a secondary IP address by entering the following command after the line that executes INITSYS.NCF:

```
ADD SECONDARY IPADDRESS n.n.n.n
```

where *n.n.n.n* is your server's secondary IP address.

IMPORTANT: This command will not take effect until the system is restarted. For this command to take effect immediately, enter the command at the server console.

7 To delete or display secondary IP addresses, press Alt+Esc until the server console prompt is displayed.

◆ You can delete secondary IP addresses by entering the following command:

```
DELETE SECONDARY IP ADDRESS n.n.n.n
```

where *n.n.n.n* is your server's secondary IP address.

◆ Ensure that when you delete secondary IP addresses, the corresponding commands are also removed from AUTOEXEC.NCF.

You can display secondary IP addresses by entering the following command:

```
DISPLAY SECONDARY IP ADDRESS
```

Completing Advanced Setup, Configuration, and Management Tasks

In addition to the basic setup procedures described in this chapter, there are several advanced setup, configuration, or management procedures you might need to complete, depending on your specific configuration. Advanced tasks are available in the NAT online documentation and include the following topics:

- ◆ Using NAT within a private network
- ◆ Managing NAT

22

Advanced Configuration of NAT

This section provides an example of using Novell® BorderManager® 3.8 Network Address Translation (NAT) in a private network when the network uses both registered and unregistered addresses.

See [Chapter 21, “Setting Up NAT,” on page 249](#) section for instructions on how to set up Network Address Translation.

In the following example, NAT is used to separate a segment of a private network, which uses registered addresses, from the rest of the network, which uses unregistered addresses. As shown in the following illustration, the segments of the private network that use unregistered addresses (network 10.0.0.0 and network 11.0.0.0) have an FTP server and database server that need to be accessible from the Internet.

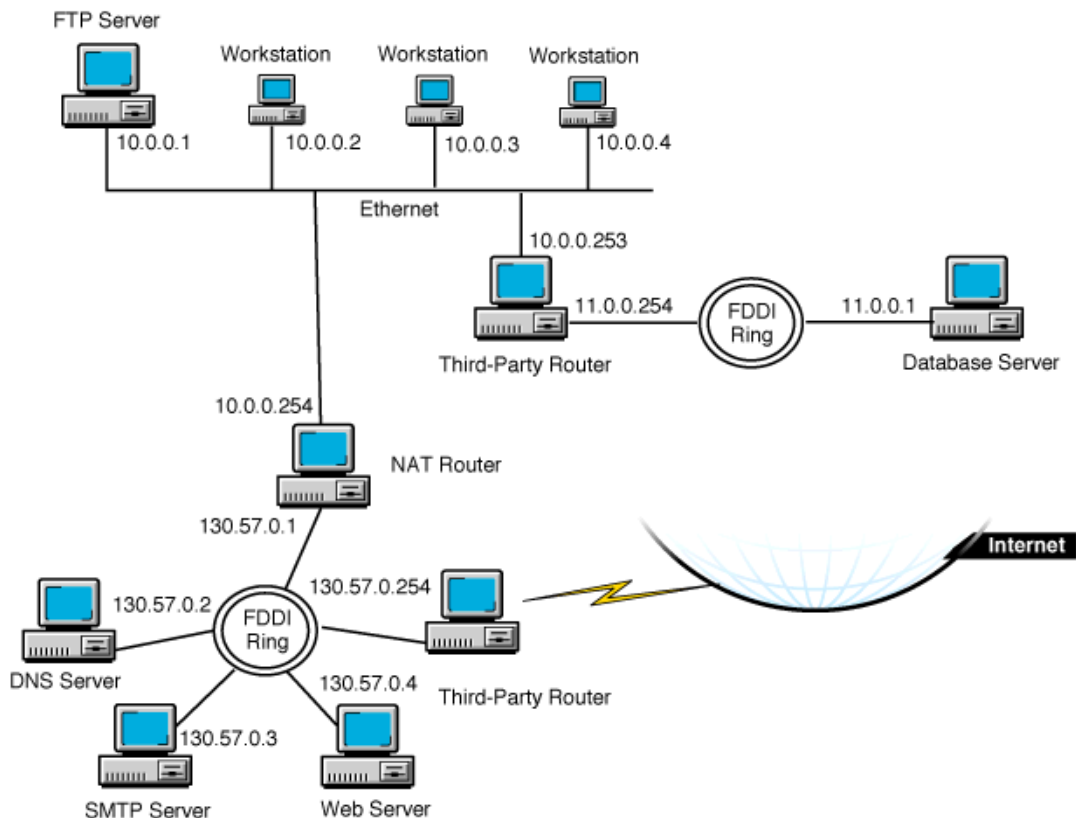
Workstations on network 10.0.0.0 should be able to access the rest of the private network and the Internet.

The segment of the private network that uses registered addresses (network 130.57.0.0) has a Web server, a Domain Name Server (DNS) server, and a Simple Mail Transfer Protocol (SMTP) gateway server that should be accessible from the workstations on the rest of the private network.

In this example, the following registered IP addresses have been obtained from an Internet Service Provider (ISP) for NAT use: 130.57.100.1, 130.57.100.2, 130.57.100.3, 130.57.100.4, and 130.57.110.1.

These addresses are to be mapped to the FTP server, database server, and workstations on the 10.0.0.0 and 11.0.0.0 networks.

Figure 81 Using NAT within a Private Network



For this example, an administrator must complete the following tasks:

- ◆ Add the secondary IP addresses on the NAT router interface that has been assigned IP address 130.57.0.1.
- ◆ Enable Network Address Translation on the NAT router interface.
- ◆ Create a Network Address Translation table mapping the secondary IP addresses to the private hosts on networks 10.0.0.0 and 11.0.0.0.
- ◆ Create static (default) routes on the routers to enable routing between the private network segments if the routers have been configured to filter Routing Information Protocol (RIP) packets.

To perform these tasks:

1 At the server console, enter

```
LOAD INETCFG
```

2 Select Protocols.

3 If TCP/IP was not configured on the NAT router interfaces, enable TCP/IP for each interface under Protocols, and bind IP addresses to the public and private interfaces under Bindings.

In this example, bind 130.57.0.1 to the public interface, and bind 10.0.0.254 to the private interface.

4 Press Esc until you are prompted to save your changes, then select Yes.

5 Select Manage Configuration > Edit AUTOEXEC.NCF.

- 6** Specify the commands to bind secondary IP addresses after the line that executes INITSYS.NCF.

In this example, enter the following lines:

```
ADD SECONDARY IPADDRESS 130.57.100.1
ADD SECONDARY IPADDRESS 130.57.100.2
ADD SECONDARY IPADDRESS 130.57.100.3
ADD SECONDARY IPADDRESS 130.57.100.4
ADD SECONDARY IPADDRESS 130.57.110.1
```

- 7** Press Esc until you are prompted to save your changes, then select Yes.
- 8** Press Esc until you return to the Internetworking Configuration menu.
- 9** Select Bindings.
- 10** Select the public interface that has a registered address bound to it.
In this example, select the interface bound to the address 130.57.0.1.
- 11** Select Expert TCP/IP Bind Options.
- 12** Select Network Address Translation.
- 13** For Status, select Static Only.
- 14** Select Network Address Translation Table, then press Ins.

Specify the following public address and private address pairs:

Public Address	Private Address
130.57.100.1	10.0.0.1
130.57.100.2	10.0.0.2
130.57.100.3	10.0.0.3
130.57.100.4	10.0.0.4
130.57.110.1	11.0.0.1

- 15** Press Esc until you are prompted to save your changes, then select Yes.
- 16** Press Esc to return to the Internetworking Configuration menu.
- 17** If the third-party router that connects the 10.0.0.0 network to the 11.0.0.0 network is filtering outgoing RIP packets, add a static route on the NAT router for the 11.0.0.0 network with a next hop of 10.0.0.253.

Also verify that each host on the 10.0.0.0 network that is allowed to access the 11.0.0.0 network has a static route to the router with the IP address 10.0.0.253.

To configure a static route on the NAT router:

- 17a** From the Internetworking Configuration menu, select Protocols > TCP/IP.
- 17b** If necessary, change the status of LAN Static Routing from Disabled to Enabled.
- 17c** Select the LAN Static Routing Table field.
- 17d** Press Ins to add a TCP/IP static route.
- 17e** For Route Type, select Network.
- 17f** For IP Address of Network/Host, enter 11.0.0.0.

- 17g** For Subnetwork Mask, accept the default, FF.0.0.0, or enter the subnet mask for your network.
 - 17h** For Next Hop Router on Route, enter 10.0.0.253.
 - 17i** Press Esc and select Yes to update the database.
 - 17j** Press Esc and select Yes to update the TCP/IP configuration.
 - 17k** Press Esc to return to the Internetworking Configuration menu.
- 18** If the NAT router is filtering incoming RIP packets, add a default static route for the 130.57.0.0 network on the third-party router that connects the 11.0.0.0 network to the rest of the network.
- Also verify that each host on the 10.0.0.0 network that is allowed to access the Internet uses 10.0.0.254 bound to the NAT interface as the default route to the 130.57.0.0 network.
- NOTE:** Because the 10.0.0.0 network is not using registered addresses, both incoming and outgoing RIP packets should always be filtered. This enables NAT to hide the 10.0.0.0 network while allowing its hosts to access the Internet.
- 19** If the third-party router that connects the 130.57.0.0 network to the Internet is filtering incoming RIP packets, add a default route to the Internet on the NAT router with a next hop of 130.57.0.254.
- Also verify that each host on the 130.57.0.0 network that is allowed to access the Internet has a default route to the router with the IP address 130.57.0.254.
- To configure a default static route on the NAT router, complete the following steps:
- 19a** From the Internetworking Configuration menu, select Protocols > TCP/IP.
 - 19b** If necessary, change the status of LAN Static Routing from Disabled to Enabled.
 - 19c** Select the LAN Static Routing Table field.
 - 19d** Press Ins to add a TCP/IP static route.
 - 19e** For Route Type, select Default Route.
 - 19f** For Next Hop Router on Route, enter 130.57.0.254.
 - 19g** Press Esc twice and select Yes to update the database.
 - 19h** Press Esc and, if prompted, select Yes to update the TCP/IP configuration.
 - If you have enabled LAN Static Routing in Step 19b, you are prompted to update the TCP/IP configuration
 - 19i** Press Esc to return to the Internetworking Configuration menu.
- 20** If you want the static routes to take effect immediately, select Reinitialize System and select Yes to activate your changes.

23

Managing Network Address Translation

This section provides tips and guidelines for monitoring the functionality of Novell® BorderManager® 3.8 Network Address Translation (NAT) on your server.

To monitor NAT functionality, verify the following:

- ◆ To see if TCP/IP routing and connectivity is established: Test IP connectivity using the `LOAD PING` command at the server console.
- ◆ To see if NAT is enabled on the public interface: Check whether NAT is enabled in `inetcfg`.
- ◆ To see if TCP/IP is bound to more than one interface: You can check the bindings in `inetcfg`.
- ◆ To see if Filters are not blocking outgoing packets: You can verify the configured filters using `filtcfg`.
- ◆ Verify the entries in the Static NAT Table are correct.
- ◆ Load `tcpip.nlm`, then issue the `SET TCP IP DEBUG=1` command:
 - ◆ The NAT server is receiving incoming packets.
 - ◆ The correct address translation is performed.
 - ◆ Discarded packets are not displayed on the console screen.
 - ◆ The connection is not being reset by the NAT router.
- ◆ TCP reset packets (RSTs) are not displayed on LAN traces.

A SET Parameters

These are some of the common SET parameters for Novell® BorderManager® 3.8. Use these parameters to change your settings.

Configuration Using SET Options

The following SET options allow you to configure certain parameters from the command line on the host. The SET options are entered at the server console as commands, and the configuration changes made this way are applied to the whole system rather than to an individual interface.

IKE debugmask

Syntax	IKE debugmask = n
Description:	2 = message header, 4 = message body, 8 = attribute
Range:	0 to 4294967295
Default:	8

IKE Certificate Request Payload

Syntax:	IKE cert request = OFF
Description:	Send certificate request payload ON=yes OFF=no
Range:	On Off
Default:	Off (disabled)

IKE Dump All IKE SAs

Syntax:	IKE DUMPSA = n
Description:	Change the number to dump all IKE SA's.
Range:	0 to 4294967295
Default:	1

IKE exponent_size for DH Group 1

Syntax:	IKE exp_size for group 1 = n
Description:	Set exponent size for DH group 1
Range:	4 to 760
Default:	760

IKE exponent_size for DH Group 2

Syntax:	IKE exponent_size for DH group 2 =n
Description:	set exponent size for DH group 2 between
Range:	4 to 1016
Default:	1016

IKE Pre-shared Key

Syntax:	IKE Pre-shared key = 2
Description:	To set the pre-shared key to be used, the number given is insignificant. The user simply needs to provide a different number than previously given. The username could be <username>.<context>. For example, admin.novell.
Range:	0 to 4294967295
Default:	1

IKE Retransmit Timeout

Syntax:	IKE Retransmit Timeout = n
Description:	Sets the IKE retransmit timeout value. This should be used and increased depending on the speed of the link.
Range:	0 to 4294967295 seconds
Default:	5 seconds

IPsec Encryption Algorithm for Pre-shared Key Authentication Mode in C2S

Syntax:	IPsec encr alg for pss
---------	------------------------

Description:	IPsec encryption for Pre-shared key IKE mode IPsec_ESP_Des :1 IPsec_ESP_DES :3 IPsec_ESP_NULL :11 To set the encryption algorithm to be used in Phase 2 negotiation if the method is preshared key authentication.
Range:	1 to 11
Default:	1

IPsec Hash Algorithm For Pre-shared Key Authentication Mode in C2S

Syntax:	IPsec hash alg for pss = 1
Description:	IPsec hash alg for preshared key IKE mode IPsec_HMAC_MD5 :1 IPsec_HMAC_SHA :2 To set the hash algorithm to be used in Phase 2 negotiation for the preshared key authentication method
Range:	1 to 4
Default:	1

IPsec Use Policy

Syntax:	IPsec use policy = 1
Description:	0 - Use a uniform policy for all traffic 1 - Use different policies for different traffic
Range:	0 to 1
Default:	1

VPN NCF Check Interval

Syntax:	set VPN NCF Check Interval = n
Description:	The VPN client check for NCF running on the client machine after every configured interval of time.
Range:	1-10 minutes
Default:	1

VPN Over NAT

Syntax:	VPN Over NAT = ON
---------	-------------------

Description:	Can be enabled or disabled over NAT
Range:	On Off
Default:	ON

VPN Requires NCF

Syntax:	VPN Requires NCF = n
Description:	VPN requires the Novell Client™ firewall on the workstation. 0=no, 1 = yes
Range:	0 to 1
Default:	0

Pre-shared Key

Syntax:	Set IKE Pre-shared Key = n
Description:	To set the user pre-shared key. Change the number everytime you want to change the secret.
Range:	1, 2, 3, 4 ...
Default:	1

B

Cool Solutions and AppNotes on Novell BorderManager

On a regular basis we post new articles on the Novell® BorderManager® Cool Solutions Web site. See the site ([Cool Solutions \(http://www.novell.com/coolsolutions/bordermag/\)](http://www.novell.com/coolsolutions/bordermag/) for the latest updates and information on other products interoperating with Novell BorderManager.

Over the last two years the BorderManager team members and external experts have actively published various AppNotes that deal with specific components and features in much greater detail. For more information, follow the links below:

- ♦ [Understanding Novell BorderManager's HTTP Proxy Logs \(http://developer.novell.com/research/appnotes/2002/january/02/a020102.htm\)](http://developer.novell.com/research/appnotes/2002/january/02/a020102.htm)
- ♦ [Blocking Virus Requests in Novell BorderManager's HTTP Accelerator \(http://developer.novell.com/research/appnotes/2002/february/02/a020202.htm\)](http://developer.novell.com/research/appnotes/2002/february/02/a020202.htm)
- ♦ [A Technical Overview of Novell TCP/IP in NetWare 6 \(http://developer.novell.com/research/appnotes/2002/april/01/a020401.htm\)](http://developer.novell.com/research/appnotes/2002/april/01/a020401.htm)
- ♦ [Interoperability of Novell BorderManager with Other Novell Services \(http://developer.novell.com/research/appnotes/2002/may/03/a020503.htm\)](http://developer.novell.com/research/appnotes/2002/may/03/a020503.htm)
- ♦ [Novell BorderManager Filter Configuration through iManager \(http://developer.novell.com/research/appnotes/2002/june/04/a020604.htm\)](http://developer.novell.com/research/appnotes/2002/june/04/a020604.htm)
- ♦ [Tuning the NetWare 6 TCP/IP Stack via SET Parameters \(http://developer.novell.com/research/appnotes/2002/july/02/a020702.htm\)](http://developer.novell.com/research/appnotes/2002/july/02/a020702.htm)
- ♦ [Monitoring Proxy Information on Novell BorderManager \(http://developer.novell.com/research/appnotes/2002/august/03/a020803.htm\)](http://developer.novell.com/research/appnotes/2002/august/03/a020803.htm)
- ♦ [Blocking Browser Ads with Novell BorderManager \(http://developer.novell.com/research/appnotes/2003/january/02/a030102.htm\)](http://developer.novell.com/research/appnotes/2003/january/02/a030102.htm)
- ♦ [IP Address Configurations and Usage for the NetWare 6.5 TCP/IP Protocol Stack \(http://developer.novell.com/research/appnotes/2003/february/01/a030201.htm\)](http://developer.novell.com/research/appnotes/2003/february/01/a030201.htm)
- ♦ [Using WebSpy Analyzer and WebSpy Live on Novell BorderManager Proxy Log Files \(http://developer.novell.com/research/appnotes/2003/march/02/a030302.htm\)](http://developer.novell.com/research/appnotes/2003/march/02/a030302.htm)
- ♦ [Running Novell BorderManager on Novell Cluster Services \(http://developer.novell.com/research/appnotes/2003/septembe/03/a030903.htm\)](http://developer.novell.com/research/appnotes/2003/septembe/03/a030903.htm)
- ♦ [Novell BorderManager with FreeSwan Client \(http://www.novell.com/coolsolutions/bordermag/features/a_vpn_freeswan_client_bm.html\)](http://www.novell.com/coolsolutions/bordermag/features/a_vpn_freeswan_client_bm.html)
- ♦ [VPN Policies on Novell BorderManager \(http://www.novell.com/coolsolutions/bordermag/features/a_vpn_policies_bm.html\)](http://www.novell.com/coolsolutions/bordermag/features/a_vpn_policies_bm.html)
- ♦ [Novell BorderManager VPN Client \(http://www.novell.com/coolsolutions/bordermag/features/a_bm38_intro_vpn_bm.html\)](http://www.novell.com/coolsolutions/bordermag/features/a_bm38_intro_vpn_bm.html)

- ◆ [Novell BorderManager with CISCO IOS 12.2\(11\)](http://www.novell.com/coolsolutions/bordermag/features/a_cisco_ios_12.2_bm.html) (http://www.novell.com/coolsolutions/bordermag/features/a_cisco_ios_12.2_bm.html)
- ◆ [Novell BorderManager with SSH Sentinel Client](http://www.novell.com/coolsolutions/bordermag/features/a_ssh_sentinel_client_bm.html) (http://www.novell.com/coolsolutions/bordermag/features/a_ssh_sentinel_client_bm.html)
- ◆ [Novell BorderManager Access Rules: Some Do's and Dont's](http://www.novell.com/coolsolutions/bordermag/features/a_bm38_access_rules_bm.html) (http://www.novell.com/coolsolutions/bordermag/features/a_bm38_access_rules_bm.html)
- ◆ [Novell BorderManager with Check Point](http://www.novell.com/coolsolutions/bordermag/features/a_bm38_with_check_point_bm.html) (http://www.novell.com/coolsolutions/bordermag/features/a_bm38_with_check_point_bm.html)
- ◆ [Novell BorderManager VPN Monitoring](http://www.novell.com/coolsolutions/bordermag/features/a_vpn_monitoring_bm.html) (http://www.novell.com/coolsolutions/bordermag/features/a_vpn_monitoring_bm.html)
- ◆ [Novell BorderManager NMAS and LDAP Authentication](http://www.novell.com/coolsolutions/bordermag/features/a_auth_users_nmas_ldap_bm.html) (http://www.novell.com/coolsolutions/bordermag/features/a_auth_users_nmas_ldap_bm.html)

C

Important TIDs on Novell BorderManager

Over the last few years the BorderManager[®] support team members have actively published a number of TIDs on the support.novell.com site. Here are some of the most important TIDs that have been published recently. These TIDs are searchable in the [Knowledgebase at Novell Support \(http://support.novell.com/search/kb_index.jsp\)](http://support.novell.com/search/kb_index.jsp). Search with either with TID number or the solution ID.

TID	Solution ID	Title
10012765	4.0.3921366.2238576	Performance, Tuning and Optimization
10080403	NOVL87343	Restoring BorderManager 3.7 default filters
10011002	3.0.328786.2205046	Novell BorderManager 3.x Client-to-Site VPN Hotstart
10070403	NOVL78024	Novell BorderManager 3.7 Filter Configuration Frequently Asked Questions
10018669	1.0.33811594.2354884	BorderManager Proxy and Cache Performance and Tuning
10059667	NOVL37374	BorderManager PROXY.CFG and PROXY.NLM Options
10083142	NOVL89406	BorderManager 3.7 Support Pack 2 (bm37sp2.exe)
10011260	4.0.1390904.2202743	How to add TCP/IP Static routing in INETCFG for LAN, WAN, & NetWare Connect
10011263	4.0.1390957.2202743	NAT FAQ; Network Address Translation
10083710	NOVL89925	Able to send SPAM e-mail though HTTP proxy
10013153	4.0.6634098.2248324	How to put BorderManager default filters back in place
10061723	NOVL45270	Advanced filter troubleshooting and filter debugging
10072002	NOVL80411	Transparent proxy is listening in all interfaces
10076524	NOVL83828	BorderManager Licenses show expiration of 12/12/02
10083405	NOVL89602	BorderManager / N2H2 content filtering solution is halted or slow and Winsock errors displayed on server console
10025666	1.0.51440661.2510819	Reinstalling NICI Files - the detailed version
10061203	NOVL43052	Login to a Windows NT/2000 (NTLM) database via HTTP Proxy
10066872	NOVL66008	Cannot access origin Web server through BorderManager
10071884	NOVL80406	NBM 3.7 filters are not working

TID	Solution ID	Title
10076512	NOVL83821	SurfControl CPFILTER.NLM will not load

Novell BorderManager Glossary

Novell provides an exhaustive glossary of technical terms. Refer to that glossary for details of most of the networking terms. For more information on the Novell Glossary see [Novell Glossary of Networking Terms \(http://www.intl.novell.com/documentation/lg/glossary\)](http://www.intl.novell.com/documentation/lg/glossary). In this section we discuss some of the key terms used in Novell BorderManager VPN services and Novell Client Firewall 2.0 product that is available along with this release.

Authentication Rules

The data receiver knows who is the data sender. User authentication allows an administrator to grant or reject access to specific users from specific IP addresses, based on their user credentials. Authentication rules and policies are defined and stored in eDirectory and are globally managed through the iManager-based VPN services.

Certificate Authority

A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be. Usually, this means that the CA has an arrangement with a financial institution, such as a credit card company, which provides it with information to confirm an individual's claimed identity. CAs are a critical component in data security and electronic commerce because they guarantee that the two parties exchanging information are really who they claim to be.

Encryption

The process of scrambling or coding data for security purposes. Through encryption we translate data into a secret code. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

Key Material Object

An eDirectory object that contains the public key, private key, certificate, and certificate chain. It is also known as a Key Material Object (KMO) or, in the eDirectory/NDS schema, as NDSPKI:Key Material.

Loopback

Is a special IP address (127.0.0.1) reserved for feedback when testing software on a node without having to dispatch the package on the network.

PKI

A system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

Password Expiry Notice

A password is a secret series of characters that enables a user to access a file, computer, or program. On multi-user systems, each user must enter his or her password before the computer will respond to commands. The password helps ensure that unauthorized users do not access the computer. The expiry notice for a password can be set so that the password is null after that period.

Plug-in

Is an independent component that can be added or removed from a software package to extend the capability of that software. The software must be designed and built to support plug-ins. Plug-in technology allows third party developers to create plug-ins specific to that software enabling the software to do many more things.

Preset

A preset in NCF is a pre-defined setting or group of settings for an event or action. A preset can apply many settings simultaneously with one mouse click. This saves time for users who would otherwise need to apply each setting manually.

Pre Shared Key

The preshared key can be an ACSII text or hexadecimal character key.

Profiles

A control file that is usually easily modified and is used to customize aspects of a program.

Public Key

A cryptographic system two keys -- a public key known to everyone and a private or secret key known only to the recipient of the message. An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key.

Referrer

Is part of the HTTP request that contains the URL of the last page visited before the request.

Spyware

Is hidden software or a concealed part of some software that is secretly or unknowingly installed on your computer. Spyware collects information (usually for marketing purposes) and sends it without the user's knowledge to the author or organization that originated the spyware

Stealth Mode

Stealth mode in NCF makes your computer invisible to hackers while letting you browse the Internet. Normally, when your computer receives a connection request from another computer, it lets that computer know that this port is closed. In stealth mode, your computer will not respond, making it seem like it is not turned on or not connected to the Internet.

Traffic Rules

Traffic Rules are policies that govern accessibility for a user through a VPN connection.

Trusted Root

An entity, usually a certification authority (CA), that a particular system recognizes and trusts to verify a public key. Any public key certificate signed by a trusted root is considered valid.

Trusted Root Certificate

A certificate that contains the public key of a trusted root.

Trusted Root Certificate Object

An eDirectory object that contains a trusted root certificate. The object's eDirectory schema name is NDSPKI:Trusted Root Object. The trusted root certificate can be exported and used as needed.

Trusted Root Container

An eDirectory object that contains Trusted Root Certificate objects. The container object's eDirectory schema name is NDSPKI:Trusted Root.

Trusted Root Object

Defines an object that holds a trusted root certificate from a trusted Certificate Authority.

Tunnel IP Address

The process of encapsulating a packet within a packet of a different protocol. Using tunneling, two networks based on the same protocol can communicate across a network based on a different protocol. Tunnel IP Address is the address used to route the encrypted traffic across the VPN network to reach the protected networks. It is the virtual Network Interface used to achieve IP/IPX tunneling and routing mechanism for site-to-site connections.

User Certificate

A user certificate provides the user the ability to prove his identity. In addition to vouching for the user's identity, the digital certificate will also enable you to encrypt and digitally sign transactions thus ensuring the confidentiality and integrity of your communications.

VPN Master

This is the NBM VPN gateway that is the Master of the site-to-site VPN network. The site-to-site configuration consisting of the site-to-site properties, VPN members, and VPN Policies are configured at the VPN Master, and the Master distributes the configuration to the VPN Slave servers. Additionally, if the site-to-site network uses Star topology, all the data traffic between the VPN Slave networks is routed through the VPN Master.

VPN Slave

The other NBM VPN gateways in a site-to-site VPN network are called VPN Slaves. The Slaves receive the site-to-site configuration including the site-to-site properties, VPN Members and the VPN Policies from the VPN Master.

