

Novell BorderManager

3.9

April 5, 2007

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.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 1997-2007 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.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the [Novell Legal Patents Web page \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

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

Online Documentation: To access the latest online documentation for this and other Novell products, see [the Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

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

Contents

About This Guide	11
Part I Proxy	13
1 Proxy Services Prerequisites	15
1.1 Setting Up the DNS Resolver	15
1.2 Configuring Web Browsers to Use Novell BorderManager	16
1.2.1 Setting Up Mozilla Firefox to Use a Web Proxy	16
1.2.2 Setting Up Microsoft Internet Explorer to Use a Web Proxy	18
1.2.3 Setting Up Netscape Navigator to Use a Web Proxy	18
2 Configuring Proxy Services	19
2.1 Configuring Application Proxies	19
2.1.1 Configuring an HTTP Proxy	19
2.1.2 Configuring an FTP Proxy	21
2.1.3 Configuring FTP Proxy in Active Mode	22
2.1.4 Configuring a Mail Proxy	22
2.1.5 Configuring RealAudio and RTSP Proxies	24
2.1.6 Configuring a DNS Proxy	24
2.1.7 Configuring a Generic TCP Proxy	25
2.1.8 Configuring a Generic UDP Proxy	26
2.2 Configuring Proxy Acceleration	27
2.2.1 Configuring HTTP Acceleration	27
2.2.2 Blocking Virus Requests in the HTTP Accelerator	29
2.2.3 Configuring FTP Reverse Proxy	32
2.3 Configuring Transparent Proxies	33
2.3.1 Configuring an HTTP Transparent Proxy	33
2.3.2 Configuring Telnet Transparent Proxy	34
2.4 Configuring Authentication	35
2.4.1 Configuring Proxy Authentication	35
2.4.2 Configuring Terminal Server Authentication	37
2.5 Configuring Session Failover	38
2.5.1 Overview of Session Failover	39
2.5.2 Configuring Session Failover	43
2.6 Configuring the SOCKS V4 or V5 Gateway	45
2.6.1 Configuring the SOCKS Server	46
2.6.2 Configuring the SOCKS Client	48
3 Advanced Proxy Configurations	49
3.1 Configuring Caching Hierarchies	49
3.1.1 Configuring Cache Hierarchy Server	49
3.1.2 Configuring Cache Hierarchy Client	51
3.1.3 Configuring Cache Hierarchy Routing	52
3.2 Configuring Cache Parameters	53
3.2.1 Configuring Cache Aging Parameters	53
3.2.2 Configuring Cache Control Parameters	54
3.2.3 Configuring Cache Location Parameters	55

3.2.4	Configuring Cachable Object Control Parameters	56
3.3	Configuring IP Addresses	58
3.4	Configuring DNS Transport Parameters	58
3.5	Configuring Transport Timeout Parameters	59
4	Managing Proxy Services	61
4.1	Configuring Proxy Logging	61
4.1.1	Configuring Logging for an HTTP Proxy	61
4.1.2	Configuring Logging for an HTTP Accelerator	62
4.2	Monitoring Proxy Statistics	63
4.2.1	Monitoring Proxy Cache Real-time Activity	64
4.2.2	Monitoring HTTP Statistics	64
4.2.3	Monitoring FTP Statistics	65
4.2.4	Monitoring Mail (SMTP/POP3) Statistics	66
4.2.5	Monitoring Gopher Statistics	67
4.2.6	Monitoring RealAudio Statistics	68
4.2.7	Monitoring SOCKS Statistics	69
4.2.8	Monitoring Generic Statistics	69
4.2.9	Monitoring ICP Statistics	70
4.2.10	Monitoring Client FTP Statistics	70
4.3	Monitoring Cache Statistics	71
4.3.1	Monitoring General Cache Statistics	71
4.3.2	Monitoring DNS Cache Statistics	72
4.3.3	Monitoring Connection Cache Statistics	73
4.3.4	Monitoring Download Cache Statistics	74
4.4	Proxy Configuration Dump Tool	74
4.5	Splash Screen Settings	74
5	Using Novell Audit for HTTP Proxy Logging	75
5.1	Configuring Novell BorderManager for Novell Audit	75
5.2	Understanding the Novell BorderManager Event Data	76
5.3	Viewing Events in Novell Audit Report	77
5.4	Configuring the Audit Server	78
6	Configuring Access Rules	79
6.1	Configuring a Rule to Allow Access through an Application Proxy	79
6.2	Configuring URL-Based Access Rules	80
6.2.1	Configuring a URL-Based Access Rule for FTP or HTTP Proxy	80
6.2.2	Modifying the Existing Access Rules as URL-based Access Rules	81
6.2.3	Modifying the Existing URL-Based Access Rules	81
6.3	Configuring Third-Party Filtering Solutions	81
6.4	Configuring Time Restrictions for Access Rules	82
6.5	Configuring Access Rule Ordering	82
6.6	Viewing All Access Rules that Apply to an Object	83
7	Configuring Alert Notification	85
7.1	Configuring E-Mail Alert Notification	85
8	Managing Alert Messages	89
8.1	Viewing Alerts Sent as E-Mail Messages	89

8.2	Viewing Alerts in Audit Trail Log File	90
8.2.1	Displaying Audit Trail Log Records with the Audit Trail Utility	90
8.2.2	Archiving the Audit Trail Log File	91
8.3	Viewing Alerts in the Control Log	91
8.4	Responding to Alerts	91
8.4.1	Server Performance Alerts	92
8.4.2	License Acquisition Alerts	93
8.4.3	Security Alerts	93
8.4.4	Proxy Alerts	95
Part II Filters		97
9 Setting Up Packet Filters		99
9.1	Packet Filter Prerequisites	99
9.2	Setting Up the Default Filters	100
9.3	Using FILTCFG for Filter Configuration	100
9.3.1	Setting Up Outbound Packet Filter Exceptions	101
9.3.2	Setting Up Inbound Packet Filter Exceptions	105
9.3.3	Defining Custom Stateful Packet Types	105
9.4	Saving Filters to a Text File	106
9.5	Enabling Global IP Packet Logging	106
9.6	Completing Advanced Setup, Configuration, and Management Tasks	107
10 Using Novell iManager for Filter Configuration		109
10.1	Before you Begin	109
10.2	Setting Up Public Interface	110
10.3	Easy Filter Configuration	110
10.3.1	Configuring Filters for Novell BorderManager services	111
10.3.2	Configuring On-Server Service Exceptions	112
10.3.3	Configuring Off-Server Service Exceptions	114
10.4	Filter Maintenance	116
10.5	Legacy Filter Configuration	116
10.5.1	Configuring the Packet Forwarding Filter	118
10.5.2	Configuring the Service Type	123
10.5.3	Configuring an Incoming RIP Filter	125
10.5.4	Configuring an Outgoing RIP Filter	128
10.5.5	Configuring an Incoming EGP Filter	132
10.5.6	Configuring an Outgoing EGP Filter	135
10.5.7	Configuring an OSPF Filter	138
10.6	List All Firewall Policies	141
10.7	Troubleshooting: Possible Installation Scenarios	142
10.7.1	The Off Server Service Fields Appear Disabled	142
10.7.2	Roles and Tasks Do Not Appear on the Left Pane	143
11 Managing IP Packet Filters		145
11.1	Modifying Default IP Logging Parameters	145
11.2	Viewing IP Packet Log Information	146
12 Backing Up and Restoring Filters		149
12.1	Backing Up eDirectory Filters to LDIF	149

12.2	Restoring Filters to eDirectory from LDIF	149
12.3	Backing Up eDirectory Filters to Text Files	150
12.4	Restoring Filters to eDirectory from Text Files	150
13	Advanced Configuration of IP Packet Filters Using FILTCFG	151
13.1	Choosing between Stateful or Static Packet Filters	151
13.2	Setting Up an HTTP Filter	151
13.2.1	Setting Up a Stateful HTTP Filter	151
13.2.2	Setting Up Static Filters for HTTP	152
13.3	Setting Up an FTP Filter	153
13.3.1	Setting Up a Stateful FTP Filter	153
13.3.2	Setting Up Static Filters for FTP	154
13.4	Setting Up a Telnet Filter	154
13.4.1	Setting Up a Stateful Telnet Filter	155
13.4.2	Setting Up Static Filters for Telnet	155
13.5	Setting Up an SMTP Filter	156
13.5.1	Setting Up a Stateful SMTP Filter	156
13.5.2	Setting Up Static Filters for SMTP	156
13.6	Setting Up a POP3 Filter	157
13.6.1	Setting Up a Stateful POP3 Filter	157
13.6.2	Setting Up a Static POP3 Filter	157
13.7	Setting Up a DNS Filter	157
13.7.1	Setting Up a Stateful DNS Filter	158
13.7.2	Setting Up Static Filters for DNS	158
13.8	Setting Up VPN Filters	158
13.9	Filtering IP Packets that Use the IP Header Options Field	158
Part III	Virtual Private Network	161
14	Pre-Shared Key Support	163
14.1	PSK Use Cases and Error Messages	163
14.2	Use Case Scenarios of Novell BorderManager 3.8 Master and Slaves	164
14.3	Use Case Scenarios in Mixed Environment	165
14.4	Communication Between Two Novell BorderManager 3.9 Slaves	167
15	Certificate-Based Authentication	171
15.1	Automated Creation of eDirectory Certificates or Objects	172
15.2	Creating Server Certificates	172
15.3	Exporting Root Certificates from the Server Certificate	178
15.4	Creating Trusted Root Containers	179
15.5	Creating the Trusted Root Object	180
15.6	Creating a User Certificate	180
15.7	Exporting User Certificates	182
15.8	Third-Party Certificate Server	183
16	Configuring VPN Services	185
16.1	Setting Up VPN Services	185
16.2	VPN Server Configuration	186
16.2.1	Adding a New VPN Server	186

16.2.2	Deleting a VPN Server Configuration	189
16.3	Virtual Private Network Prerequisites	189
16.3.1	Site-to-Site VPN Prerequisites	190
16.3.2	Client-to-Site VPN Prerequisites	191
16.3.3	Setting Up VPN Filters	192
16.3.4	On VPN Master Site	193
16.3.5	On VPN Slave Site	194
16.3.6	Exceptions required to keep a Client-toSite and a Site-to-Site Connection Up. . . .	195
16.4	Client-to-Site Configuration	196
16.4.1	Creating a New Client-to-Site Configuration	196
16.4.2	General	197
16.4.3	Traffic Rules	197
16.4.4	Authentication Rules	201
16.4.5	Remote LDAP Configuration	203
16.4.6	DNS/SLP Configuration	204
16.4.7	Final Client-to-Site Page	204
16.5	Attaching a Client-to-Site Service to the VPN Server	204
16.6	Site-to-Site Configuration	204
16.6.1	Configuring a VPN Server As a Master Server	205
16.6.2	Configuring a VPN Server As a Slave Server	207
16.6.3	Modifying a Site-to-Site Service	208
16.6.4	Removing Site-to-Site Members	211
16.7	VPN Policy	213
16.7.1	Default Values for Client-to-Site Authentication Rules	213
16.7.2	Default Values for Client-to-Site Traffic Rules	214
16.7.3	Default Values for Site-to-Site Traffic Rules	214
 17 Upgrading Virtual Private Networks		215
17.1	Upgrading a VPN from a Previous Version	215
17.1.1	General Guidelines for Upgrading	215
17.1.2	Upgrade Procedure	216
 18 Monitoring Virtual Private Networks		219
18.1	Logging into NetWare Remote Manager	219
18.2	Checking the VPN Real-Time Monitor	221
18.3	Checking the Audit Log on a VPN Server	224
18.4	Checking the Activity of a VPN Server	227
 19 Virtual Private Network Client		229
19.1	VPN Client Features	229
19.1.1	X.509 Certificate Authentication Mode	229
19.1.2	NMAS Authentication Mode	230
19.1.3	NMAS LDAP Authentication Mode	230
19.1.4	Pre-Shared Key Authentication Mode	230
19.1.5	VPN Client Integration with the Novell Client	230
19.1.6	Use NICI for Encryption	231
19.1.7	Selecting Dial-Up Entries	231
19.1.8	Automatic Creation of a Novell VPN Dial-Up Entry	231
19.1.9	Password Expiry Notice	231
19.1.10	VPN Server Hosts List	232
19.1.11	Policy	232
19.1.12	VPN Connections through NAT	232

Part IV Network Address Translation	233
20 Setting Up NAT	235
20.1 NAT Prerequisites	235
20.2 Setting Up NAT on a Single Interface.	236
20.3 Setting Up NAT with Multihoming.	237
20.4 Completing Advanced Setup, Configuration, and Management Tasks	238
21 Advanced Configuration of NAT	239
22 Managing Network Address Translation	243
A SET Parameters	245
A.1 Configuration Using SET Options.	245
A.1.1 IKE debugmask	245
A.1.2 IKE Certificate Request Payload	245
A.1.3 IKE Dump All IKE SAs	245
A.1.4 IKE exponent_size for DH Group 1	245
A.1.5 IKE exponent_size for DH Group 2	246
A.1.6 IKE Pre-shared Key	246
A.1.7 IKE Retransmit Timeout.	246
A.1.8 IPsec Encryption Algorithm for Pre-shared Key Authentication Mode in C2S	246
A.1.9 IPsec Hash Algorithm For Pre-shared Key Authentication Mode in C2S.	247
A.1.10 IPsec Use Policy	247
A.1.11 VPN Over NAT.	247
A.1.12 Pre-shared Key	247
Novell BorderManager Glossary	249

About This Guide

Novell® BorderManager® 3.9 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 3.9. The audience for this documentation is experienced network administrators.

It includes the following sections:

- ◆ Part I, "Proxy," on page 13
- ◆ Part II, "Filters," on page 97
- ◆ Part III, "Virtual Private Network," on page 161
- ◆ Part IV, "Network Address Translation," on page 233
- ◆ Appendix A, "SET Parameters," on page 245

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *Novell BorderManager 3.9 Installation Guide*, visit the [Novell Documentation Site \(http://www.novell.com/documentation/nbm39/index.html\)](http://www.novell.com/documentation/nbm39/index.html).

Additional Documentation

This Administration Guide is a part of documentation set for Novell BorderManager 3.9. The other documents include:

- ◆ *Novell BorderManager 3.9 Proxy and Firewall Overview and Planning Guide*
- ◆ *Novell BorderManager 3.9 Installation Guide*
- ◆ *Novell BorderManager 3.9 Virtual Private Network Client Installation Guide*
- ◆ *Novell BorderManager 3.9 Troubleshooting Guide*
- ◆ *Novell BorderManager 3.9 Virtual Private Network Deployment Frequently Asked Questions*

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.

Proxy

The following sections of the Novell® BorderManager® 3.9 Administration guide provide information on how to use the Proxy Services. It also discusses the access control rules, alerts, and authentication services.

The following sections describe how to configure proxy services and access control lists:

- ◆ [Chapter 1, “Proxy Services Prerequisites,” on page 15](#)
- ◆ [Chapter 2, “Configuring Proxy Services,” on page 19](#)
- ◆ [Chapter 3, “Advanced Proxy Configurations,” on page 49](#)
- ◆ [Chapter 4, “Managing Proxy Services,” on page 61](#)
- ◆ [Chapter 5, “Using Novell Audit for HTTP Proxy Logging,” on page 75](#)
- ◆ [Chapter 6, “Configuring Access Rules,” on page 79](#)
- ◆ [Chapter 7, “Configuring Alert Notification,” on page 85](#)
- ◆ [Chapter 8, “Managing Alert Messages,” on page 89](#)

Proxy Services Prerequisites

1

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

- ◆ DNS Resolver setup was performed at the time of Novell® BorderManager® installation, to provide a valid domain name for the DNS, and an IP address of at least one DNS name server to resolve the IP hostnames. For more information on setting up the DNS Resolver, see [Section 1.1, “Setting Up the DNS Resolver,” on page 15](#).
- ◆ Packet filtering is configured 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 9, “Setting Up Packet Filters,” on page 99](#).
- ◆ Corporate users who want to use Proxy Services to access Web sites have set up their Web browsers to use the Novell BorderManager proxy server. For more information, see [Section 1.2, “Configuring Web Browsers to Use Novell BorderManager,” on page 16](#)
- ◆ 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 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.

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

- ◆ The IP addresses of your server’s IP interfaces with the private or public interfaces identified.
- ◆ The port number (8080 by default) and the hostname or IP address of the Novell BorderManager proxy server.

This section has the following information:

- ◆ [Section 1.1, “Setting Up the DNS Resolver,” on page 15](#)
- ◆ [Section 1.2, “Configuring Web Browsers to Use Novell BorderManager,” on page 16](#)

1.1 Setting Up the DNS Resolver

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

- 1 Enter `INETCFG`, then select *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 `example.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.

1.2 Configuring Web Browsers to Use Novell BorderManager

Corporate users who use the Proxy Services to access Web sites have to set up their Web browsers to use the Novell BorderManager server.

You can also use the Novell BorderManager 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 [Section 2.3.1, “Configuring an HTTP Transparent Proxy,” on page 33](#).

This section has the following information:

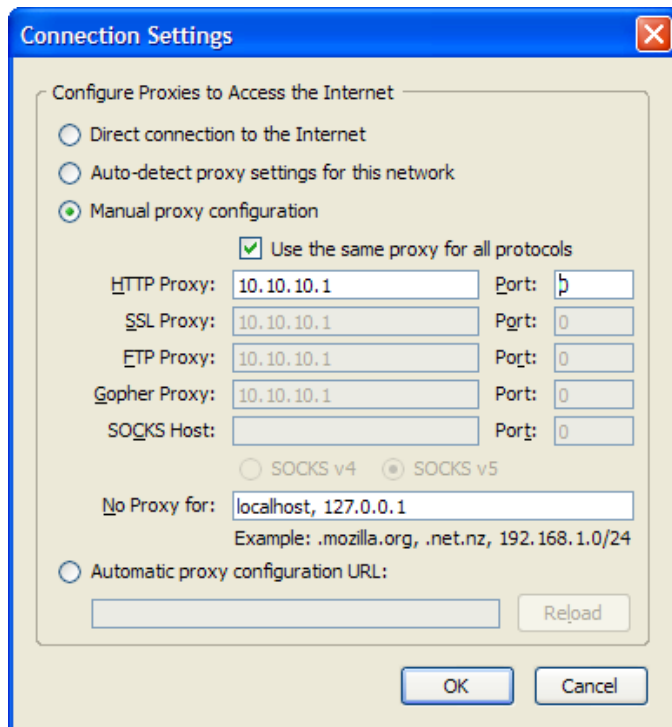
- ♦ [Section 1.2.1, “Setting Up Mozilla Firefox to Use a Web Proxy,” on page 16](#)
- ♦ [Section 1.2.2, “Setting Up Microsoft Internet Explorer to Use a Web Proxy,” on page 18](#)
- ♦ [Section 1.2.3, “Setting Up Netscape Navigator to Use a Web Proxy,” on page 18](#)

1.2.1 Setting Up Mozilla Firefox to Use a Web Proxy

To specify the Novell BorderManager server on a Mozilla* Firefox* browser:

- 1 Launch Mozilla Firefox browser, then select *Tools > Options* or *Edit > Preferences*, depending on the browser version.

- 2 Click the *General* tab, then click *Connection Settings*.

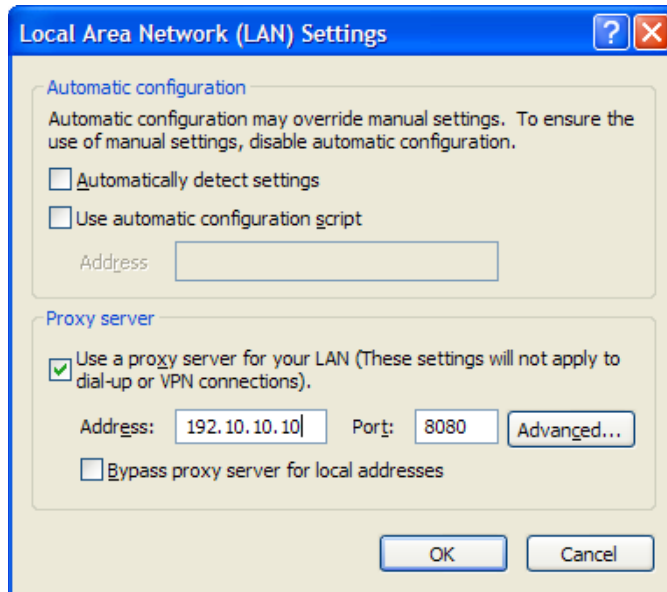


- 3 Select *Manual Proxy Configuration*.
- 4 Select *Use the same proxy for all protocols*.
- 5 Specify the port number (8080 by default) and hostname or IP address of the Novell BorderManager proxy server in the proxy field.
- 6 Click *OK*.

1.2.2 Setting Up Microsoft Internet Explorer to Use a Web Proxy

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

- 1 Launch Internet Explorer, then 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 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 *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 proxy server in the proxy field.
- 3 Click *Apply*.

1.2.3 Setting Up Netscape Navigator to Use a Web Proxy

To specify the Novell BorderManager 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 proxy server in the URL field.
- 3 Click *OK*.

Configuring Proxy Services

2

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

This section has the following information:

- ◆ [Section 2.1, “Configuring Application Proxies,” on page 19](#)
- ◆ [Section 2.2, “Configuring Proxy Acceleration,” on page 27](#)
- ◆ [Section 2.3, “Configuring Transparent Proxies,” on page 33](#)
- ◆ [Section 2.4, “Configuring Authentication,” on page 35](#)
- ◆ [Section 2.5, “Configuring Session Failover,” on page 38](#)
- ◆ [Section 2.6, “Configuring the SOCKS V4 or V5 Gateway,” on page 45](#)

2.1 Configuring Application Proxies

You can use the 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 has the following information:

- ◆ [Section 2.1.1, “Configuring an HTTP Proxy,” on page 19](#)
- ◆ [Section 2.1.2, “Configuring an FTP Proxy,” on page 21](#)
- ◆ [Section 2.1.3, “Configuring FTP Proxy in Active Mode,” on page 22](#)
- ◆ [Section 2.1.4, “Configuring a Mail Proxy,” on page 22](#)
- ◆ [Section 2.1.5, “Configuring RealAudio and RTSP Proxies,” on page 24](#)
- ◆ [Section 2.1.6, “Configuring a DNS Proxy,” on page 24](#)
- ◆ [Section 2.1.7, “Configuring a Generic TCP Proxy,” on page 25](#)
- ◆ [Section 2.1.8, “Configuring a Generic UDP Proxy,” on page 26](#)

2.1.1 Configuring an HTTP Proxy

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

To set up an HTTP proxy server:

- 1 Log in to iManager.

- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Click *HTTP* in the *Forward Proxy* section. The HTTP Proxy page is displayed.

HTTP Cache Hierarchy Server Cache Hierarchy Client Cache Hierarchy Routing Logging

Enable this proxy

Listening port:

Ignore Refresh Requests from Browser

Filter Cookies

Enable Persistent Connections to Browsers

Enable Persistent Connections to Origin Servers

Enable Java Applet Stripping

OK Cancel

- 5 Select *Enable this Proxy*, to enable the proxy.
- 6 Specify the HTTP listening port number in the *Listening Port* field.

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

The HTTP proxy listens on interfaces identified as Private or Both, but not on interfaces identified as Public.
- 7 Specify information in the following fields:
 - Ignore Refresh Requests from 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. You can 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 Java Applet Stripping:** When this option is enabled, Java* applets are stripped from the HTML file before the file is displayed in the browser window.
- 8 Click *OK*.
- 9 Click *Apply Changes* to save the changes.

2.1.2 Configuring an FTP Proxy

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.

To set up an FTP proxy server:

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Click *FTP*, in the *Forward Proxy* section. The FTP proxy configuration page is displayed.

Enable this proxy

Username/Password Separator:

Anonymous FTP Email Address:

User Authentication

None

Clear Text User(or)Password

Single Sign On

Enable Indexed Format Logging

OK Cancel

- 5 Select *Enable this proxy*, to enable the proxy.

- 6 Specify a username and password separator in the *Username/Password Separator* field.

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[Inbrk]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`.

- 7 Specify an anonymous FTP e-mail address in the *Anonymous FTP E-Mail Address* field.

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@`.

- 8 Select a user authentication method from the following:

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 User (or) 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.

- 9 Select *Enable Indexed Format Logging* to enable indexed format logging for the FTP proxy server.

You can view data from the FTP indexed format (audit) log only by exporting the log.

- 10 Click *OK*.
- 11 Click *Apply Changes* to save the changes.

2.1.3 Configuring FTP Proxy in Active Mode

With this release, Novell BorderManager has added the capability to the FTP proxy to connect in active mode to the origin FTP server.

- 1 Open the `proxy.cfg` proxy configuration file located in `SYS:\ETC\PROXY`.
- 2 Add the following line in the `[Extra Configuration]` section:

```
EnableActiveFTP=1
```

NOTE: Add the `[Extra Configuration]` section, if your configuration file does not already have it.

- 3 Save the `proxy.cfg` file.
- 4 Restart the proxy.
- 5 To disable this feature, remove the line from the file or set `EnableActiveFTP=0`.

2.1.4 Configuring a Mail Proxy

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 iManager. Specify the IP address manually.

To configure the mail proxy server:

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.

4 Click *Mail* in the *Forward Proxy* section. The mail proxy configuration page is displayed.

Enable this proxy

Spool Directory:	<input type="text" value="SYS:\ETC\PROXY\SPPOOL"/>	
Spool Directory Max Size:	<input type="text" value="10"/>	MB
Max Mail Size:	<input type="text" value="1"/>	MB
Failed Mail Retry Interval:	<input type="text" value="10"/>	Min
Failed Mail Retry Count:	<input type="text" value="10"/>	
Primary Mail Domain Name:	<input type="text"/>	
Internal Mail Server Name:	<input type="text"/>	
POP3 Mail Server Name:	<input type="text"/>	

Enable Index Format Logging

5 Select the *Enable this proxy* check box, to enable the proxy.

6 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 Interval:** 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.

7 Select *Enable Indexed Format Logging* to enable indexed format logging for the Mail proxy server.

You can view data from the Mail proxy indexed format (audit) log only by exporting the log.

8 Click *OK*.

9 Click *Apply Changes* to save the changes.

2.1.5 Configuring 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 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Click *RealAudio and RTSP* in the *Forward Proxy* section. The RealAudio and RTSP configuration page is displayed.

Enable this proxy

Enable Index Format Logging

- 5 Select the *Enable this proxy* check box to enable the RealAudio and RTSP proxy.
- 6 Select *Enable Indexed Format Logging* to enable indexed format logging for the RealAudio or RTSP proxy server.
You can view data from the RealAudio or RTSP indexed format (audit) log only by exporting the log.
- 7 Click *OK*.
- 8 Click *Apply Changes* to save the changes.

2.1.6 Configuring a DNS Proxy

The 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 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.

- 4 Select *DNS* in the *Forward Proxy* section. The DNS proxy configuration page is displayed.

Enable this proxy

Enable Index Format Logging

OK Cancel

- 5 Select the *Enable this proxy* check box to enable the RealAudio and RTSP proxy.
- 6 Select the *Enable Indexed Format Logging* check box to enable indexed format logging for the DNS proxy server.
You can view the logged data from the DNS indexed format (audit) log by exporting the log.
- 7 Click *OK*.
- 8 Click *Apply Changes* to save the changes.

2.1.7 Configuring a Generic TCP Proxy

This proxy is a circuit-level passthrough proxy used to serve multiple protocols for which an application proxy is not available.

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

To set up a Generic TCP proxy server:

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Select *Generic TCP Proxy* in the *Forward Proxy* section. The Generic TCP Proxy page is displayed.

Enable this proxy

Forward List						
New...					Delete	0 item(s)
<input type="checkbox"/> Origin Server Hostname	Origin Server Port	Proxy IP Address	Proxy Port	Status		
No items						

Enable Index Format Logging

OK Cancel

- 5 Select *Enable this proxy* to enable the Generic TCP proxy.
- 6 To add a server to the *Forward List*, click *New*.
- 7 Specify the following information in the New dialog box:

Enable This Particular Proxy: Select this check box to specify whether to enable the Generic proxy server after you have set it up.

Origin Server Hostname: Specify the hostname of the origin server.

Origin Server Port: Specify the port number for the origin server as that origin server is listening on for incoming connections. The default port number is 0.

Proxy IP address: 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.

Proxy Port: Specify the port number for the proxy server. The default port number is 0. You can associate one or several public IP addresses with a particular domain name, but make sure you have a unique IP address and the port number combination.

8 Click *OK* to add the new server to the *Forward List*.

9 Select *Enable Indexed Format Logging* to enable indexed format logging for the Generic TCP proxy server.

You can view data from the Generic TCP proxy indexed format (audit) log only by exporting the log.

10 Click *OK*.

11 Click *Apply Changes*.

2.1.8 Configuring a Generic UDP Proxy

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

To set up a Generic UDP proxy server:

1 Log in to iManager.

2 Select *Novell BorderManager > Proxy Services*.

3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.

4 Select *Generic UDP Proxy* in the *Forward Proxy* section. The Generic UDP Proxy page is displayed.

Enable this proxy

Forward List						
New...					Delete	0 item(s)
<input type="checkbox"/>	Origin Server Hostname	Origin Server Port	Proxy IP Address	Proxy Port	Status	
No items						

Enable Index Format Logging

5 Select *Enable this proxy* to enable the Generic UDP proxy.

6 To add a server to the *Forward List*, click *New*.

7 Specify the following information in the New dialog box:

Enable This Particular Proxy: Select this check box to specify whether to enable the Generic proxy server after you have set it up.

Origin Server Hostname: Specify the hostname of the origin server.

Origin Server Port: Specify the port number for the origin server as that origin server is listening on for incoming connections. The default port number is 0.

Proxy IP address: 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.

Proxy Port: Specify the port number for the proxy server. The default port number is 0. You can associate one or several public IP addresses with a particular domain name, but make sure you have a unique IP address and the port number combination.

8 Click *OK* to add the new server to the *Forward List*.

9 Select the *Enable Indexed Format Logging* check box to enable indexed format logging for the Generic UDP proxy server.

You can view data from the Generic UDP proxy indexed format (audit) log only by exporting the log.

10 Click *OK*.

11 Click *Apply Changes* to save the changes or *Cancel Changes* to cancel the changes.

2.2 Configuring Proxy Acceleration

In proxy acceleration or reverse proxy, 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.

This section contains the following information:

- ♦ [Section 2.2.1, “Configuring HTTP Acceleration,” on page 27](#)
- ♦ [Section 2.2.2, “Blocking Virus Requests in the HTTP Accelerator,” on page 29](#)
- ♦ [Section 2.2.3, “Configuring FTP Reverse Proxy,” on page 32](#)

2.2.1 Configuring HTTP Acceleration

An HTTP Reverse Proxy is also known as an HTTP accelerator. The HTTP reverse proxy listens on interfaces identified as Public or Both, but not on interfaces identified as Private. The best security involves two interfaces.

To set up an HTTP Reverse Proxy:

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Select *HTTP* in the *Reverse Proxy* section.

5 Select *Enable this proxy*.

Enable this proxy

HTTP Accelerator List

New | Delete

<input type="checkbox"/> Accelerator Name	Web Server Port	Proxy IP Address	Logging	Status
<input type="checkbox"/> www.example.com	80	10.1.1.1	No	Enabled

OK Cancel

6 Click *New* to add a server to the *HTTP Accelerator List*.

HTTP Accelerator **Logging**

Enable this particular accelerator

Enable authentication for this particular accelerator

Accelerator Name:

Web Server Port:

Web Servers

New ▾ | Delete

<input type="checkbox"/> Name/IP Address	Port
<input type="checkbox"/> www.example.com	80

Proxy IP Addresses

New ▾ | Delete

<input type="checkbox"/> IP Address	Port
<input type="checkbox"/> 10.1.1.1	80

Accelerate on a different port

OK Cancel

Specify the following information:

Enable This Particular Accelerator: Select this check box to enable the configured server. You can disable the server if you are configuring multiple accelerations. You can disable one or more servers without affecting the other accelerated sites.

Enable Authentication For This Particular Accelerator: Specify whether you want to enable the accelerator for authentication.

Accelerator Name: 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.

Web Server Port: Specify the port number the origin Web server is listening on for incoming connections. The default is 80 for HTTP.

Web Servers: To add a new Web server, click *Add*, specify either the Web server name or the IP Address, then click *OK*. To delete a Web Server, select the check box next to the Web server, then click *Delete*.

Proxy IP Addresses: These are the addresses the accelerator will listen on for incoming connections from the Internet. To add a new proxy IP address, click *Add*, select the IP address that you want to add, then click *Add*.

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`.

To delete an IP address, select the check box next to the Proxy IP address, then click *Delete*.

Accelerate on a Different Port: Select this check box if you want to accelerate on a different port. Specify a different accelerator port number.

All internal Web server links must be relative URLs.

7 Click *OK* to add the new server to the *HTTP Accelerator List*.

8 Click *Apply Changes* to save the changes.

2.2.2 Blocking Virus Requests in the HTTP Accelerator

Novell BorderManager has a Virus Pattern Recognition feature that can help protect the Web servers that are being accelerated by Novell BorderManager. This enhancement includes features to facilitate its configuration and monitoring.

Configuration of the Virus Pattern Recognition feature is accomplished using the 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`).

This section has the following information:

- ♦ “Monitoring the Virus Pattern Recognition Feature” on page 30
- ♦ “Effect on Performance” on page 30
- ♦ “Adding and Deleting Virus Request Patterns” on page 30
- ♦ “Enabling and Configuring Auto Update” on page 31
- ♦ “Adding New Virus Keywords” on page 31

Monitoring the Virus Pattern Recognition Feature

The Novell BorderManager Server includes a Virus Pattern Configuration screen. All virus pattern configuration and statistical information is tracked and displayed on this separate server console screen.

Effect on Performance

Enabling the Virus Pattern Recognition feature does not adversely affect Novell BorderManager Proxy Server performance.

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=0PatternSize=16PatternStartOffset=1Ena  
blePatternAutoUpdate=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.

NOTE: The command syntax in this section 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 following syntax:

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

For example:

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

Enabling and Configuring Auto Update

Novell BorderManager 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, the following 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.

There are two ways to enable this Auto Update feature.

- ♦ Enter the following command at the system console:

```
virus -e 1
```

NOTE: To disable the Auto Update feature, specify 0 (zero) in the command.

- ♦ Add the following line to 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.

Let us assume that all URLs with Code Red virus requests contain the string `cmd.exe`. Here, `cmd.exe` is a keyword, because the presence of this string identifies the URL as a virus request. If `cmd.exe` is added as a filter rule in routers, all requests containing this keyword are 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.

When a request is labeled as the suspect through the heuristics described above, the suspect request is checked for the presence of certain keywords. If a match is found, the request is labeled as a virus request and its pattern is added to the database. Any future requests containing that keyword are automatically blocked.

2.2.3 Configuring FTP Reverse Proxy

An FTP Reverse Proxy is also known as an FTP accelerator. 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.

To configure an FTP Reverse Proxy server:

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Select *FTP* in the *Reverse Proxy* section.
- 5 Select *Enable this proxy*.

Enable this proxy

FTP Accelerator List				
New ▾ Delete				
<input type="checkbox"/> FTP Server Name	FTP Server Control Port	Proxy IP Address	Proxy Port	Status
<input type="checkbox"/> www.example.com	21	10.1.1.1	21	Enabled

OK Cancel

- 6 Click *New*, then specify the following information:
 - Enable This Particular Accelerator:** Select this check box to enable the accelerator.
 - FTP Server Hostname:** Specify the hostname of the origin FTP server.
 - Proxy IP Addresses:** These are the addresses the accelerator will listen on for incoming connections from the Internet. Select one or more public proxy IP addresses from the list.

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.
- 7 Click *OK* to add the new server to the *HTTP Accelerator List*.
- 8 Click *Apply Changes* to save changes.

2.3 Configuring Transparent Proxies

A transparent proxy enables you to use a proxy server without reconfiguring each of the user's browsers. This section has the following information.

- ♦ [Section 2.3.1, “Configuring an HTTP Transparent Proxy,” on page 33](#)
- ♦ [Section 2.3.2, “Configuring Telnet Transparent Proxy,” on page 34](#)

2.3.1 Configuring an HTTP Transparent Proxy

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

Pre-requisites

- ♦ Clients must use the private IP address of proxy as the TCP/IP gateway address.
- ♦ IP forwarding must be enabled on the server.
- ♦ Make sure port 80 is free as the HTTP transparent proxy listens on port 80.

NOTE: If the Apache Web server is listening on port 80, make sure you change it to any other free port before you begin configuring the HTTP transparent proxy.

To configure an HTTP Transparent proxy:

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Select *HTTP* in the *Transparent Proxy* section.
- 5 Select *Enable this proxy*.

Enable this proxy

Exception IP Address List
New... | Delete 0 item(s)
 IP Addresses
No items

Ports Monitored
New... | Delete 0 item(s)
 Ports
No items

OK Cancel

- 6 In the *Exception IP Address List* section, click *New*, specify a local IP address, then click *OK*.
- 7 In the *Ports Monitored* section, click *New*, specify a port for monitoring, then click *OK*.
Specify 80 for HTTP traffic.
- 8 Click *OK*.
- 9 Click *Apply Changes* to save the changes.

To configure authentication for HTTP transparent proxy, refer to [Section 2.4, “Configuring Authentication,” on page 35](#).

2.3.2 Configuring 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 private IP address of proxy 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 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Select *Telnet* in the *Transparent Proxy* section.
- 5 Select *Enable this proxy*.

Enable this proxy

Exception IP Address List

New... | Delete 0 item(s)

IP Addresses

No items

Ports Monitored

New... | Delete 0 item(s)

Ports

No items

- 6 In the *Exception IP Address List* section, click *New*, specify a local IP address, then click *OK*.
- 7 In the *Ports Monitored* section, click *New*, specify a port for monitoring, then click *OK*.
For example, specify 23 for Telnet traffic.

- 8 Click *OK*.
- 9 Click *Apply Changes* to save the changes.

To set up authentication for a Telnet transparent proxy, refer to [Section 2.4, “Configuring Authentication,” on page 35](#).

2.4 Configuring Authentication

You can enable NDS or eDirectory authentication to an HTTP proxy or Telnet proxy, and mandate the users to authenticate before they access the proxy server through the Internet.

Proxy authentication consists of a username and a password. This could be the NDS or eDirectory authentication username and password.

If you have enabled proxy authentication and selected both single sign-on and SSL as your authentication scheme, then proxy server first attempts to authenticate the user through single sign-on. If single sign-on fails, the proxy tries to authenticate using SSL.

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

IMPORTANT: Proxy server users can use security devices such as hardware tokens to authenticate, in addition to the 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 configuring authentication:

- ♦ [Section 2.4.1, “Configuring Proxy Authentication,” on page 35](#)
- ♦ [Section 2.4.2, “Configuring Terminal Server Authentication,” on page 37](#)

2.4.1 Configuring Proxy Authentication

To configure proxy authentication:

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.

- 4 Select *HTTP* from the *Authentication Context* section.

Authentication Context Terminal Server Authentication Session FailOver

Enable HTTP Proxy Authentication

Authentication Schemes

Single Sign On

Time to wait for Single Sign On reply: seconds

SSL

SSL Listening Port:

Key ID:

For Authentication page, send notification in

HTML Form JAVA Applet

Maximum idle time before requiring a new login:

Authenticate Only when user attempts to access a restricted page

Enable Transparent Telnet Proxy Authentication

- 5 Select the *Authentication* tab, then select *Enable HTTP Proxy Authentication*.
- 6 To specify Single Sign on as the authentication scheme, do the following:
 - 6a Select *Single Sign On*.
 - 6b Specify the time in seconds in the *Time to wait for Single Sign on reply* field.
- 7 To specify SSL as the authentication scheme, do the following:
 - 7a Select the *SSL* check box.
 - 7b Specify the following information:

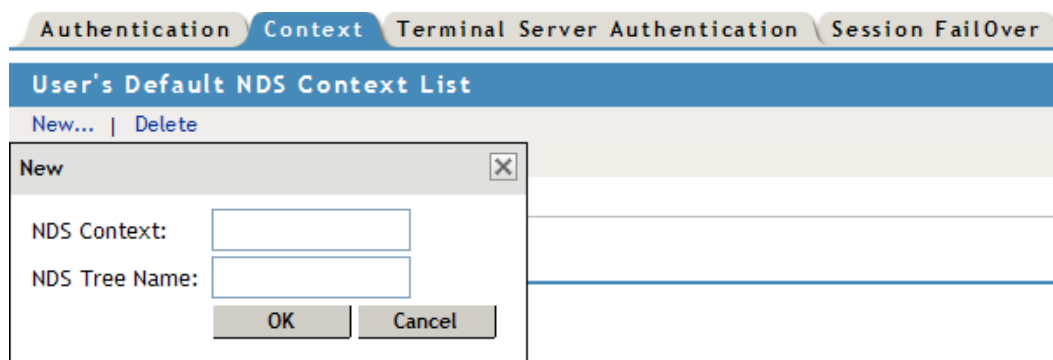
SSL Listening Port: Specify the port used for authentication. You might need to change the port number to prevent reverse proxy traffic from running into SSL traffic. Both reverse proxy and SSL traffic default to port 444.

Key ID: Browse to and select the key ID exchanged between the client and server for authentication.

For Authentication Page, Send Notification In: Specify whether to send authentication notification in HTML form or as a Java applet.

Maximum Idle Time Before Requiring a New Login: Specify the length of time a connection can remain idle before a new login is required.
- 8 Select *Authenticate Only when the user attempts to access a restricted page* if required.
- 9 Select *Enable Transparent Telnet Proxy Authentication* to enable authentication for transparent proxy
- 10 Click the *Context* tab.

- 11 Click *New* in the *User's Default NDS Context List* section, 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.

- 12 Click *OK*.
- 13 Click *Apply Changes* to save changes.

2.4.2 Configuring Terminal Server Authentication

Terminal server authentication provides the capability to differentiate users from client with the same address, such as clients using a Terminal Server or the clients behind NAT; and also from different addresses. Users coming from clients with the same address are provided with a different authentication scheme.

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Complete [Step 4 to Step 12 in Section 2.4.1, “Configuring Proxy Authentication,” on page 35](#), to configure proxy authentication.
- 5 Select the *Terminal Server Authentication* tab.

6 Select *Enable Terminal Server Authentication*.

Authentication Context **Terminal Server Authentication** Session FailOver

Enable Terminal Server Authentication
 Redirect HTTPS Request

Authentication Subnets List
New... | Delete
 ID Subnet Address Subnet Mask
No items

Authentication Ranges List
New... | Delete
 ID Start IP Address End IP Address
No items

Authentication Addresses List
New... | Delete
 ID IPV4 Address
No items

- 7 Select *Redirect HTTPS Request* to enable HTTPS request redirection using the JavaScript*.
- 8 Specify an authentication subnet in the *Authentication Subnets List* to authenticate all clients identified from the specified subnet range. To add a new subnet to the list, click *New*, then specify the ID, subnet address, subnet mask, then click *OK*.
- 9 Specify a range of IP addresses to authenticate all clients identified from the specified address range, in the *Authentication Ranges List*.
- 10 Specify an IP address to authenticate all clients identified from that addresses.
- 11 Click *OK*.
- 12 Click *Apply Changes* to save changes.

NOTE: For the new configuration to take effect, enter the following command to at the console to restart proxy:

- ◆ stopbrd
 - ◆ startbrd
-

2.5 Configuring Session Failover

The Novell® BorderManager® 3.9 proxy provides session failover support for SSL authentication. This ensures that you can switch between two proxies, or transfer the connection request from one proxy to the other, when connection fails, without re-authenticating. If you have deployed more than one proxy server and the session failover feature is enabled, the authentication details are shared across the proxy servers.

This section provides the following information on Session Failover:

- ◆ [Section 2.5.1, “Overview of Session Failover,” on page 39](#)
- ◆ [Section 2.5.2, “Configuring Session Failover,” on page 43](#)

2.5.1 Overview of Session Failover

The session failover of proxy servers involves two components, the AuthAgent and the ProxyAgent. The AuthAgent collects authentication information from ProxyAgents, which run on individual Novell BorderManager server. The authentication information is then shared among all the proxies even if the user is authenticated to only one proxy. The users' password is never shared during the process.

- ◆ [“ProxyAgent” on page 39](#)
- ◆ [“AuthAgent” on page 39](#)
- ◆ [“Requirements” on page 39](#)
- ◆ [“Session Failover Process Using an L4 Switch” on page 40](#)
- ◆ [“AuthAgent Failover” on page 40](#)
- ◆ [“Session Failover Solution Across a WAN” on page 42](#)

ProxyAgent

The ProxyAgent (authchk.nlm) is configured on each Novell BorderManager proxy server and shares information with the [“AuthAgent” on page 39](#). The ProxyAgent keeps the central repository in sync with all the local proxies.

The following activities could trigger a communication between the ProxyAgent and the AuthAgent:

- ◆ New user login
- ◆ User logout
- ◆ Inactivity timeout

AuthAgent

The AuthAgent is a Java application and acts as a central repository of authenticated user information, for all the proxies in the setup. It ensures sharing of authentication information among all the proxies that are configured, even if the user authenticates to only one proxy. The AuthAgent can run on NetWare, Windows, or Linux servers with a Java Virtual Machine (version 1.4).

For better reliability, the AuthAgent should run on a separate machine.

Requirements

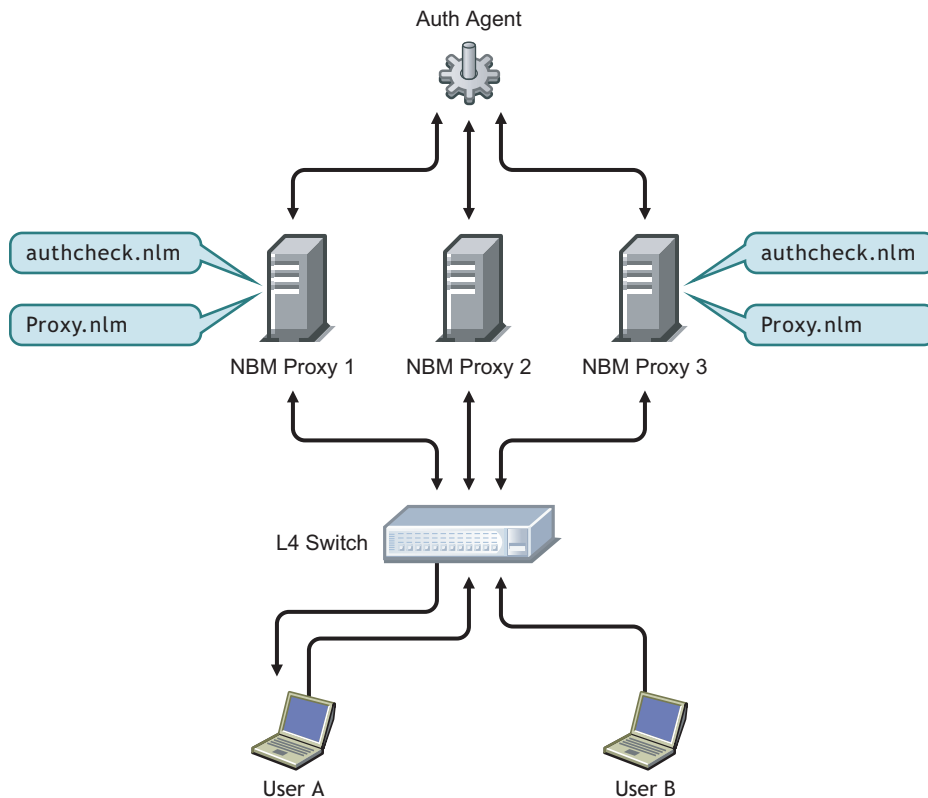
- ◆ All Novell BorderManager proxies should be in a single tree or identical trees with a common username for proxy authentication.

NOTE: A separate machine might be required for better reliability. For more information, see [“AuthAgent” on page 39](#).

- ◆ All proxies should be time synchronized.
- ◆ The TCP port on which AuthAgent listens should be opened if a firewall exists between the proxy and the AuthAgent. The default port is 9023. For more information, see [“Overview of Session Failover” on page 39](#).

Session Failover Process Using an L4 Switch

Figure 2-1 Session Failover Using L4 Switches



The session failover process among Novell BorderManager proxy servers using an L4 switch is shown in [Figure 2-1](#).

1. The user attempts to access the Internet through a Web browser.
2. The L4 switch routes the request to NBM Proxy 1.
3. Proxy 1 requests for authentication (if authentication is enabled).
4. After receiving the credentials, Proxy 1 stores the details in the database and shares the information with the AuthAgent, if authentication is successful.

NOTE: The user password is not shared in this process.

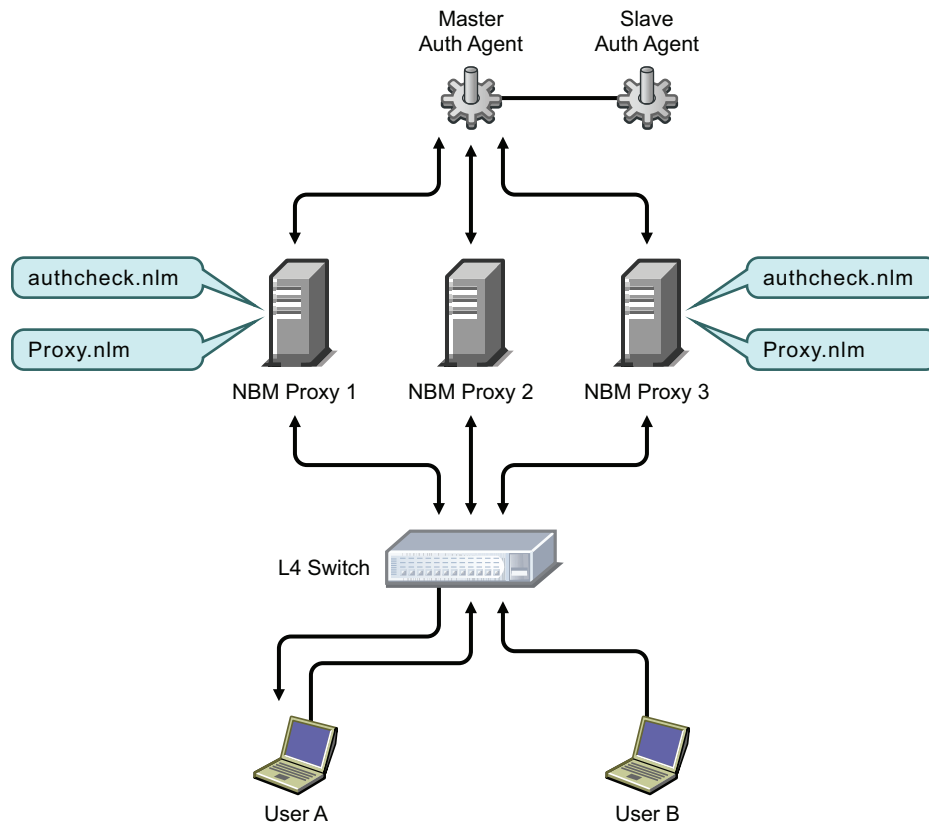
5. The AuthAgent stores the authentication details and sends them to NBM Proxy 2 and NBM Proxy 3.
6. If NBM Proxy 1 goes down, the L4 switch routes all the connection requests to NBM Proxy 2 or NBM Proxy 3.
7. The user is allowed access without providing any authentication credentials, if the next access request comes within the maximum allowed idle time.

AuthAgent Failover

The session failover with a single AuthAgent works as long as the AuthAgent is up and functional. But if the AuthAgent goes down, the session failover solution becomes nonfunctional until the

AuthAgent comes up again. To resolve this issue, you can use AuthAgent failover. With AuthAgent failover, a slave AuthAgent backs up the master AuthAgent.

Figure 2-2 *AuthAgent Failover*



As shown in [Figure 2-2](#), A1 is the Master AuthAgent and A2 is the Slave AuthAgent. AuthAgent failover between these two agents occurs as follows:

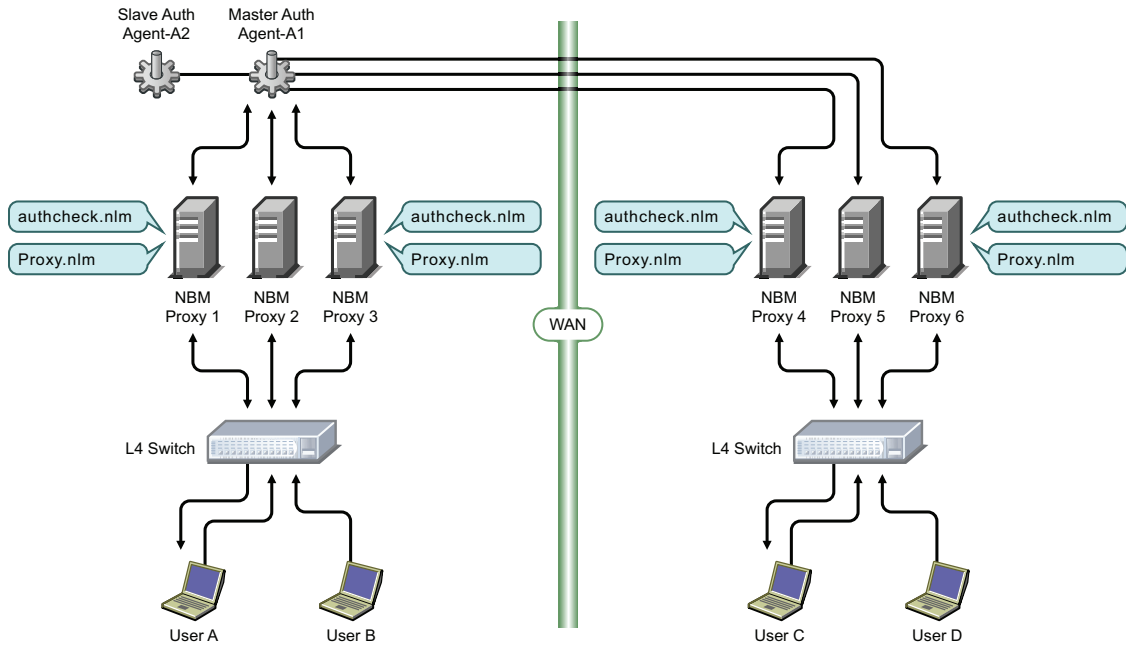
1. A1, which comes up first becomes the master AuthAgent and accepts connections and serves the ProxyAgents.
2. When A2 comes up, it tries to connect to A1 for a fixed number of times at a regular interval. This ensures that, even if A1 and A2 come up simultaneously, the probability of a race condition (when both A1 and A2 become primary AuthAgents at the same time) is minimized. If any attempt of A1 is successful, A2 becomes the slave AuthAgent served by A1. It does not accept any connections but keeps updating its cache as long as A1 is up.
3. If all the attempts of A2 to connect to A1 fail, A2 takes over as the master AuthAgent and starts serving the incoming requests. When ProxyAgents realize that their connection with A1 is down, they try connecting to A2. If the connection is successful, they start interacting with A2 as the master AuthAgent.
4. Meanwhile, if A1 comes up, it serves as the slave AuthAgent and takes over when A2 goes down. All the ProxyAgents are connected only to the master AuthAgent.

NOTE: The assumption is that both the AuthAgents do not go down at the same time. If both the AuthAgents go down, the solution is nonfunctional again.

Session Failover Solution Across a WAN

If the network is spread across multiple locations (WAN) and each location (LAN) has a few proxy servers with one AuthAgent serving all the proxies, the bandwidth of WAN is considerably used for sharing the session information.

Figure 2-3 Session Failover Across WAN

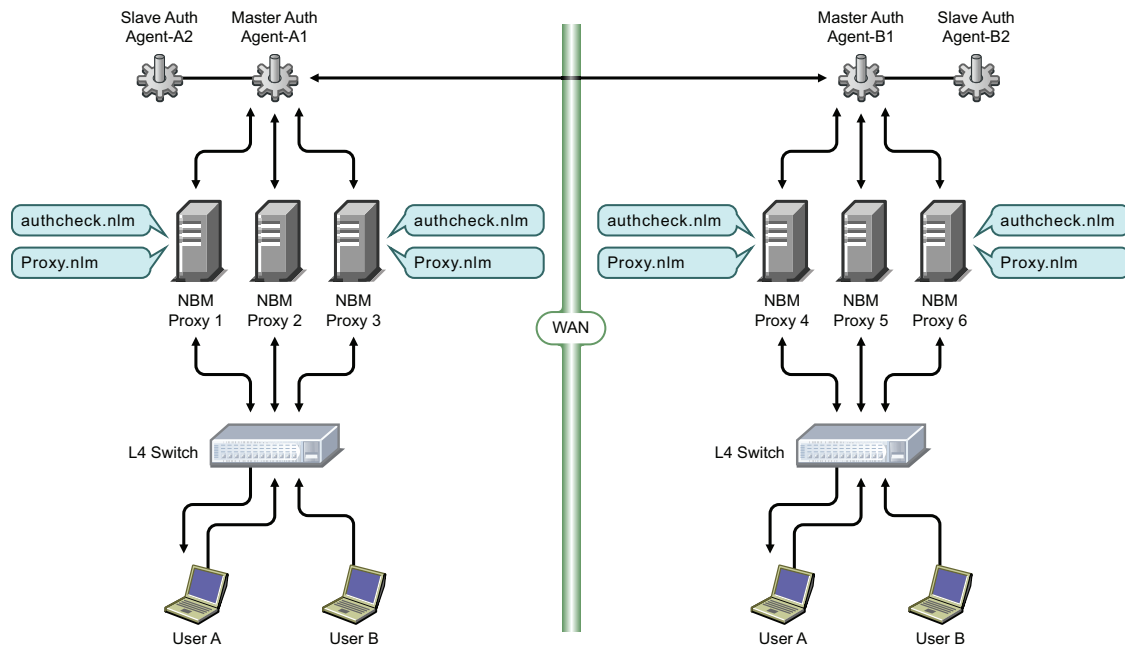


This can be minimized, by configuring AuthAgents at each location, which in turn can interact and share the session information across the WAN. Currently, Novell BorderManager supports communication between two such AuthAgents.

Consider a scenario where A1 and A2 are two AuthAgents supporting each other on one side of the WAN, and B1 and B2 are AuthAgents supporting each other on the other side of WAN. A1 considers A2, which runs either on the same machine or on a different machine in the same LAN, as a local AuthAgent. B1 considers B2 as a local AuthAgent. A1 and A2 consider B1 and B2 as remote

AuthAgents, similarly, B1 and B2 consider A1 and A2 as remote AuthAgents as they are running on either side of the WAN.

Figure 2-4 AuthAgent Sending Session Information to Remote AuthAgent



Session Failover across a WAN happens as follows:

1. Session failover at individual LAN locations occurs as explained in section “[Session Failover Process Using an L4 Switch](#)” on page 40.
2. A1 (or A2, which is the master at LAN-1) sends session information related to its LAN to its peer remote AuthAgent (B1 or B2, depending on which agent is the master at LAN-2), which in turn propagates that information to its ProxyAgents and slave AuthAgent. Similarly, B1 sends session information to A1.
3. If B1 goes down and B2 takes over as the master, the local proxies and the remote AuthAgent is connected to B2.

NOTE: If both B1 and B2 go down at the same time, the remote AuthAgent continues to try to connect to them.

2.5.2 Configuring Session Failover

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.

- 4 Select HTTP from the *Authentication* section, then select the *Session Failover* tab.

The screenshot shows the configuration interface for Session Failover. It includes a navigation bar with tabs for Authentication, Context, Terminal Server Authentication, and Session FailOver. The Session FailOver tab is active. Below the tabs, there are several configuration options: a checked checkbox for 'Enable Session FailOver', an unchecked checkbox for 'Enable Logging', a 'Log Level' dropdown menu set to '1', a 'Logging Path' text box containing '/etc/proxy', and a 'Statistics Interval' text box containing '0'. Below these options are two empty tables: 'AuthAgent List' and 'ProxyAgent List'. Each table has a header with columns for ID, Address, Port, and Type, and a 'No Items' message below the header.

- 5 Select *Enable Session Failover*.
- 6 Select *Enable Logging* to enable logging and debugging information to be saved. Specify the following information:
 - Log Level:** There are three log levels.
 - ♦ **Level 0:** The Log file contains minimum details such as the name of the application and the time started.
 - ♦ **Level 1:** In addition to the information contained in Level 0, the log file also contains information exchanged between the proxies and the AuthAgent.
 - ♦ **Level 2:** In addition to the information contained in Level 1, the log file also contains information such as hash key values, which are useful for developers for debugging.
 - Logging Path:** Specify the directory to which the common or extended format log file is written.
 - Statistics Interval:** Specify the interval between two successive log entries by the AuthAgent. The AuthAgent logs information, such as the number of users currently authenticated, and the number of session timeouts at regular intervals.
- 7 Click *New* in the *AuthAgent List* section to add a new AuthAgent. Specify the ID, IP address, and port number. Specify if the AuthAgent is a local agent or a remote agent, then click *OK*.
- 8 Specify a list of ProxyAgents that want to share authenticated session information. Click *New* in the *ProxyAgent List* section to add a new ProxyAgent. Specify the ID and IP address, then click *OK*.
- 9 Click *OK*.
- 10 Click *Apply Changes* to save the changes.

Starting the AuthAgent

This section contains the following information:

- ♦ [“Single AuthAgent” on page 44](#)
- ♦ [“AuthAgent Failover” on page 45](#)

Single AuthAgent

To start the AuthAgent, run the following command at a command prompt:

```
java -classpath full path of bmauth.jar
com.novell.bordermanager.proxy.auth.AuthDB
```

Example:

```
java -classpath sys:\public\bmauth.jar
com.novell.bordermanager.proxy.auth.AuthDB
```

AuthAgent Failover

To run the Master AuthAgent (indicated by the command line argument "1"), use the following command:

```
java -classpath <fully qualified name of bmauth.jar>
com.novell.bordermanager.proxy.auth.AuthDB 1
```

For example:

```
java -classpath sys:/public/bmauth.jar
com.novell.bordermanager.proxy.auth.AuthDB 1
```

To run the Slave AuthAgent, use the following command:

```
java -classpath <fully qualified name of bmauth.jar>
com.novell.bordermanager.proxy.auth.AuthDB 2
```

For example:

```
java -classpath sys:/public/bmauth.jar
com.novell.bordermanager.proxy.auth.AuthDB 2
```

NOTE: AuthAgent has been tested on Netware and Linux only.

Starting the ProxyAgent

- 1 Ensure that the AuthAgent is up and running.
- 2 Run the `stopbrd` and `startbrd` commands to restart Novell BorderManager Services.

The ProxyAgent supports the following command to initiate a sync request to AuthAgent:

```
authchk_send_sync_to_agent
```

This is useful when the ProxyAgent and AuthAgent are of sync because of network failures. Run the `authchk_send_sync_to_agent` command on the proxy machine, when the connection with the AuthAgent is established.

NOTE: Make sure that ProxyAgents and AuthAgents can communicate with each other [reachable] through the configured interfaces and IP addresses.

2.6 Configuring the SOCKS V4 or V5 Gateway

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 the full IP reach. 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.

- ◆ [Section 2.6.1, “Configuring the SOCKS Server,” on page 46](#)
- ◆ [Section 2.6.2, “Configuring the SOCKS Client,” on page 48](#)

2.6.1 Configuring the SOCKS Server

To configure a SOCKS V4 or V5 gateway:

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Select *SOCKS V4 and V5* from the *Gateway* section.

Enable Socks Server.

Service Port

SOCKS V5 Authentication

Single Sign On


Supported Authentication Scheme

None

Clear Text User/Password

NDS User/Password

SSL

KEY ID 

SOCKS V4 User Verification

LOG

Logging Format

Common

Indexed

Log Level

- 5 Select *Enable Socks Server* to enable SOCKS server.
- 6 (Optional) Specify the port number of the SOCKS server.
The default is 1080.
- 7 Select *Single Sign-On* to enable single sign-on for SOCKS 5 clients.

When you select this option, if a user is already authenticated to NDS, the gateway performs its authentication in the background and the user is not required to supply a username and password before accessing resources through the gateway. If single sign-on authentication is not enabled, the gateway authenticates users by using any of the authentication schemes that have been selected.

- 8 Select the authentication scheme from the *Supported Authentication Scheme* section. You can select more than one option for authentication and encryption for SOCKS 5 client and server. For the authentication options, the highest priority selection that can be used by both the client and the server as the type of authentication that is used. You have the following SOCKS 5 authentication schemes:

None: No authentication. However, data is encrypted if the Secure Sockets Layer (SSL) option is also selected.

Clear Text User/Password: During Novell IP Gateway user authentication, the user's password is transmitted across the wire in clear text without encryption. The password is checked against the password stored in NDS, but this is not the same as NDS authentication. However, if SSL is also selected, the password is encrypted before being sent.

NDS User/Password: The user is authenticated using the NDS username and password with a scheme that protects the secrecy of the password. However, data is not encrypted unless the SSL option is also selected. This option works only if the SOCKS 5 client software supports NDS authentication.

SSL: The SSL option requires that an SSL connection between the client and the server be established before the Novell IP Gateway can authenticate a user by using any of the other authentication schemes. Enabling this option also ensures the encryption of all data transmitted between the client and the server.

Key ID: If you select the SSL authentication scheme, you must also select a Key ID from the drop-down list. At least one Key ID must be created for the server in NDS prior to the selection of SSL. Novell Public Key Infrastructure (PKI) Services must be installed on your server.

NOTE: If you enable both SSL and access control, you must also select either *NDS User/Password* or *Clear Text User/Password* as a SOCKS 5 authentication method. This is because SSL does not authenticate a user to NDS.

- 9 Select *SOCKS V4 User Verification* if clients on your network support SOCKS 4. With user verification, the username is verified, but the user is not authenticated with a password before being allowed access to resources through the gateway.

- 10 Select one of the following logging format options:

Common: The common log format records standard information including a time stamp, source address, destination address, and the TCP/IP service used.

Indexed: A Novell audit-log format. The information recorded depends on the Novell BorderManager component from which information is collected.

- 11 Specify a number between 0 and 3 to indicate the type of information logged by the server.

0: No information.

1: Internet access information. The server records the user's fully distinguished NDS name; the access protocol, such as HTTP; and the destination such as www.novell.com.

2: Error codes, such as NDS errors. Level 2 information can help you determine why a user cannot access a particular service.

3: Debugging information and internal server communications, such as socket calls. Level 3 information is typically of interest only to software developers.

Each log level is additive, so, level 1 information is also logged at level 2.

- 12** Click *OK*.
- 13** Click *Apply Changes* to save changes.

2.6.2 Configuring the SOCKS Client

To configure HTTP or FTP proxy support through SOCKS:

- 1** Log in to iManager.
- 2** Select *Novell BorderManager > Proxy Services*.
- 3** Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4** Select *SOCKS V4 and V5* from the *Gateway* section.

Enable Socks Client

V5 V4

SOCKS Server IP Address

Port

Authentication Method

No Authentication

User Name/Password

User Name

Password

Changes made on this panel must be applied or scheduled from the [Configuration Panel](#).

- 5** Select *Enable Socks Client* to enable socks client.
- 6** Specify the IP address of the SOCKS server in the *SOCKS Server IP Address* field.
- 7** (Optional) Specify the port number of the SOCKS server in the *Port* field.
The default is 1080.
- 8** Specify whether you want to authenticate. If you want to authenticate, specify the username and password for authentication.
- 9** Click *OK*.
- 10** Click *Apply Changes* to save changes.

This section contains the following procedures to enhance the Novell® BorderManager® 3.9 Proxy Services performance:

- ♦ [Section 3.1, “Configuring Caching Hierarchies,” on page 49](#)
- ♦ [Section 3.2, “Configuring Cache Parameters,” on page 53](#)
- ♦ [Section 3.3, “Configuring IP Addresses,” on page 58](#)
- ♦ [Section 3.4, “Configuring DNS Transport Parameters,” on page 58](#)
- ♦ [Section 3.5, “Configuring Transport Timeout Parameters,” on page 59](#)

3.1 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 proxy server is compatible with other proxy servers on the Internet that are based on the Internet Cache Protocol (ICP). 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.

This section contains the following information on caching hierarchies:

- ♦ [Section 3.1.1, “Configuring Cache Hierarchy Server,” on page 49](#)
- ♦ [Section 3.1.2, “Configuring Cache Hierarchy Client,” on page 51](#)
- ♦ [Section 3.1.3, “Configuring Cache Hierarchy Routing,” on page 52](#)

3.1.1 Configuring Cache Hierarchy Server

To configure a cache hierarchy server:

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Click *HTTP* in the *Forward Proxy* section.
- 5 Select the *Cache Hierarchy Server* tab.

- 6 Select *Enable Cache Hierarchy Server* to enable the cache hierarchy server.

The screenshot shows a configuration window with the following elements:

- Navigation tabs: HTTP, **Cache Hierarchy Server**, Cache Hierarchy Client, Cache Hierarchy Routing, Logging
- Options:
 - Enable Cache Hierarchy Server
 - Enable Source Round Trip Time
 - Enable ICP ACL
- ICP Listening Port: 3130
- Access Control List section:
 - Buttons: New... | Delete
 - Access Control list
 - No items
- Multicast Group List section:
 - Buttons: New... | Delete
 - Multicast Group List
 - No items
- Buttons: OK, Cancel

- 7 Select *Enable Source Round-Trip Time* to enable proxy to use the route that returns the shortest 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.
- 8 Select *Enable ICP ACL* to enable the cache hierarchy or ICP access control on the server.
- 9 In the *ACL Listening Port* field, specify the UDP port on which the cache listens for queries from other caches.
- 10 *Access Control List* consists of a list of hostnames or IP addresses that are used to verify whether proxies can send a request. The clients on this list are allowed to send a cache hierarchy request. You can perform one of the following actions in this section:
 - New:** To add a new IP address, click *New*, specify the hostname or IP address, then click *OK*.
 - Delete:** To delete an IP address, select the check box next to the IP address, then click *Delete*
- 11 *Multicast Group List* consists of a list of multicast addresses on which the cache hierarchy server receives multicast cache hierarchy queries. You can perform one of the following actions in this section:
 - New:** To configure a new multicast address, click *New*, specify the Multicast IP address, then click *OK*.
 - Delete:** To delete a multicast IP address, select the check box next the IP address, then click *Delete*.
- 12 Click *OK*.
- 13 Click *Apply Changes* to save changes.

3.1.2 Configuring Cache Hierarchy Client

To configure a cache hierarchy client:

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Click *HTTP* in the *Forward Proxy* section.
- 5 Select the *Cache Hierarchy client* tab.
- 6 Select *Enable Cache Hierarchy Server* to enable the cache hierarchy server.

The screenshot shows the configuration window for the Cache Hierarchy Client. At the top, there are tabs for HTTP, Cache Hierarchy Server, Cache Hierarchy Client (selected), Cache Hierarchy Routing, and Logging. Below the tabs, there are several options: a checked checkbox for 'Enable Cache Hierarchy Client', an unchecked checkbox for 'Must Only Forward Through Hierarchy', and a 'Cache Neighbor Timeout' field set to '2' with a dropdown menu set to 'Seconds'. Below these are two empty tables: 'Neighbors List' and 'Multicast Responder List'. The 'Neighbors List' table has columns for Neighbor Hostname, Proxy Port, ICP Port, Type, Priority, and Domain. The 'Multicast Responder List' table has columns for UnicastAddress/Name and Proxy Port. At the bottom of the window are 'OK' and 'Cancel' buttons.

- 7 Select *Enable Cache Hierarchy Client*.
- 8 Select *Must Only Forward Through Hierarchy* if you do not want the proxy server to retrieve the requested objects directly from the origin server.
- 9 In the *Cache Neighbor Timeout* value field, specify the number of seconds or minutes the proxy server waits for a response to a cache hierarchy request from another proxy server.

NOTE: Do not specify a value if you are configuring a CERN client.

- 10 The *Neighbor List* consists of one or more neighbors for the Neighbors List, with the following information specified:

Neighbor Hostname: Specifies the name of the nearest host server neighbor.

Proxy Port: Port number of the neighbor HTTP proxy.

ICP Port: Port number of the neighbor cache hierarchy client.

NOTE: Do not specify a value if you are configuring a CERN client.

Type: Specify the type of neighbor as peer, parent, or CERN. Select peer or parent if you are configuring a cache hierarchy client, or select *CERN* if you are configuring a CERN client.

ICP Routing Priority: You can prioritize a set of parents or neighbors in a scale of 1 to 10. 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.

Domain Restriction: Specify domains that the cache hierarchy client will serve. Click *Add* to add new domains or click *Delete* to delete existing domains.

To add a new neighbor, click *New* and specify details in all the fields, then click *OK*.

To delete an existing neighbor, select the check box next to the neighbor that you want to delete, then click *Delete*.

- 11 The *Multicast Responder List* 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. You can perform one of the following actions in this section:

New: To add a new unicast, click *New*, specify the unicast name or IP address, specify a proxy port, then click *OK*.

NOTE: Do not specify a value if you are configuring a CERN client.

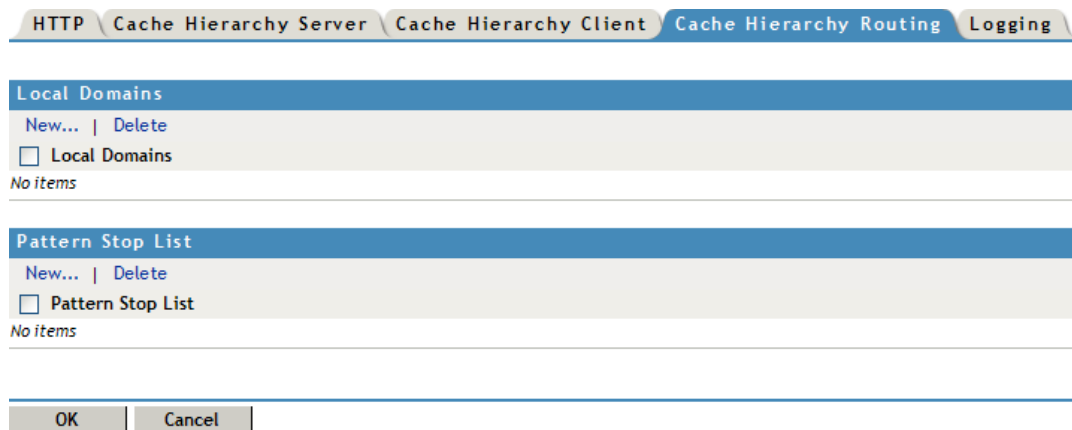
Delete: To delete a unicast, select the check box next to Unicast Name/Address, then click *Delete*.

- 12 Click *OK*.
- 13 Click *Apply Changes* to save changes.

3.1.3 Configuring Cache Hierarchy Routing

Use cache hierarchy routing when the parent cannot contact the origin server.

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Click *HTTP* in the *Forward Proxy* section.
- 5 Select the *Cache Hierarchy Routing* tab.



- 6 The *Local Domain List* consists of a list of local domain names 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. You can perform one of the following actions in this section:

New: To add a new domain name to the Local Domain list, click *New*, specify a domain name, then click *OK*.

Delete: To delete a domain, select the check box next to the domain name, then click *Delete*.

7 The *Pattern Stop List* consists of a list of 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. You can perform one of the following actions in this section:

New: To add a new pattern to the list, click *New*, specify a pattern name, then click *OK*.

Delete: To delete a pattern, select the check box next to the pattern, then click *Delete*.

8 Click *OK*.

9 Click *Apply Changes* to save changes.

3.2 Configuring Cache Parameters

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

- “Configuring Cache Aging Parameters” on page 53
- “Configuring Cache Control Parameters” on page 54
- “Configuring Cache Location Parameters” on page 55
- “Configuring Cachable Object Control Parameters” on page 56

3.2.1 Configuring Cache Aging Parameters

This section includes configuration of HTTP, FTP, and Gopher revalidation times.

1 Log in to iManager.

2 Select *Novell BorderManager > Proxy Services*.

3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.

4 Select *Caching* in the *General* section.

Parameter	Value	Unit
HTTP Maximum Revalidation Time:	7	days
HTTP Default Revalidation Time:	6	hours
HTTP Minimum Revalidation Time:	20	minutes
FTP Revalidation Time:	7	days
GOPHER Revalidation Time:	7	days
HTTP Failed Request Caching Time:	0	minutes
Maximum HOT Unreferenced Time:	30	minutes

Reset to Default

OK Cancel

- 5 Select the *Cache Aging* tab, then specify the following HTTP cache aging values:

HTTP Maximum Revalidation Time: The maximum number of hours or days that 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 that 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 that 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 that FTP data is cached before it is revalidated with the origin Web server.

Gopher Revalidation Time: The number of hours or days that 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. For more information, see [Section 3.2.2, “Configuring Cache Control Parameters,” on page 54](#).

- 6 (Optional) Click *Reset to Default* to reset values to the default.
- 7 Click *OK*.
- 8 Click *Apply Changes* to save the changes.

3.2.2 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 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Select *Caching* in the *General* section.

5 Select the *Cache Control* tab.

Cache Aging Cache Control Cache Location Cachable Object Control

Maximum Cached File Size (MB)

HTTP: FTP: Gopher:

Cache Hash Table Size: K of Entries

Maximum number of Hot Nodes:

Cache Of Deleted File Maximum Age Ratio:

Reset to Default

OK Cancel

Specify the following information:

Maximum Cached File Size (MB): Specify the maximum size in megabytes of the file that is cached for each URL protocol request type. Any file larger than the specified size is not cached. You can specify different values for HTTP, FTP and Gopher. The default is 30 MB.

Cache Hash Table Size: 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: 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.

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.

Cache of Delete File Maximum Age Ratio: This value determines how much space on the volume is used for caching and how many deleted files remain on the volume.

6 Click *OK*.

7 Click *Apply Changes* to save the changes.

3.2.3 Configuring Cache Location Parameters

You can specify a different location for the cache.

1 Log in to iManager.

2 Select *Novell BorderManager > Proxy Services*.

3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.

- 4 Select *Caching* in the *General* section.
- 5 Select the *Cache Location* tab.

Cache Directory:

Volume List	
Add...	Delete
<input type="checkbox"/> Volume	
<input type="checkbox"/> SYS:	

Number of Directories:

Specify the following information:

Cache Directory: Specify 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.

Volume List: This specifies a different cache location. To add a new volume name, click *New*, then specify a name in the *Volume Name* field. Make sure you include a colon at the end of the volume name. Click *OK*.

To delete a volume, select the check box next to the volume, then click *Delete*.

Number of Directories: Specify the number of directories available per volume.

- 6 Click *OK*.
- 7 Click *Apply Changes* to save the changes.

3.2.4 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.

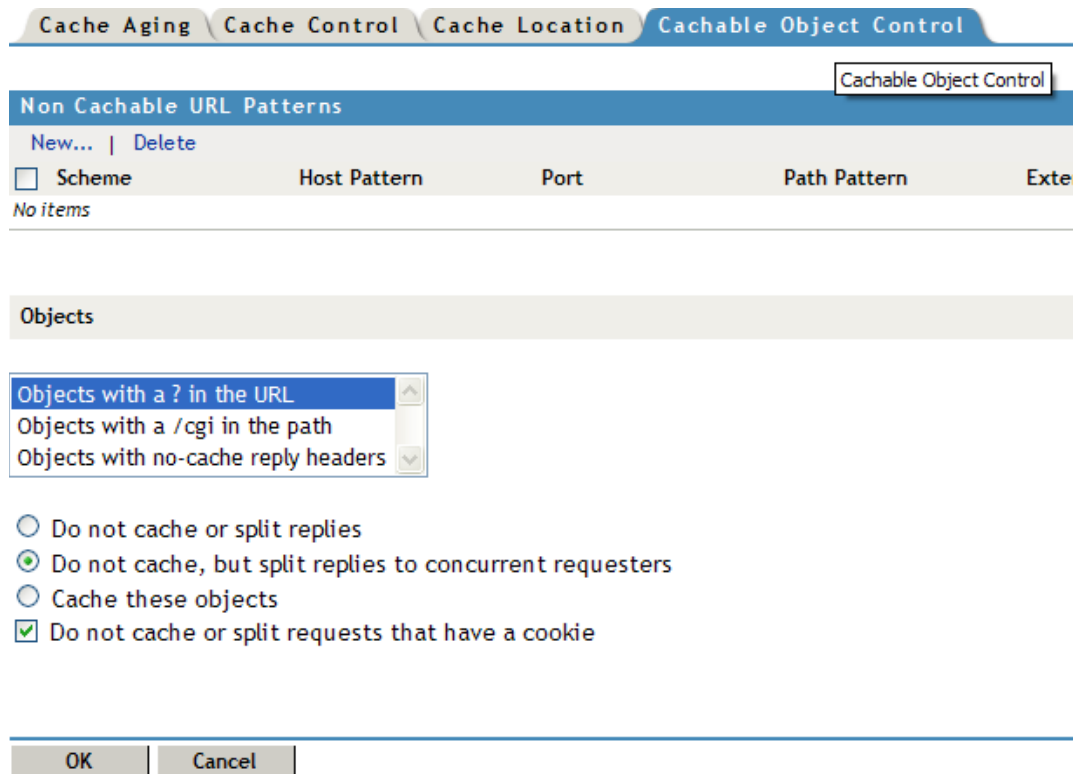
You can specify whether to cache URLs and objects with certain predefined patterns or access them directly without caching by the proxy server (be noncachable).

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:

- 1 Log in to iManager.

- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Select *Caching* in the *General* section.
- 5 Select the *Cachabel Object Control* tab.



- 6 Click *New* to add a list of URL patterns that are not be cached.
 - 6a Specify the following information:
 - Scheme Type:** 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.
 - 6b Click *OK*.

If you specify a long list of patterns, the proxy server performance is affected.
- 7 Specify the actions taken for the following objects:
 - ♦ Objects with a ? 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.

- 8 Click *OK*.
- 9 Click *Apply Changes* to save the changes.

3.3 Configuring IP Addresses

You can configure IP addresses as private, public, or as both.

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Select *IP addresses* in the *General* section.

IP Address	Subnet Mask	Usage Type
<input type="checkbox"/> 10.1.1.1	255.0.0.0	Private

- 5 Click *New* in the *Configured IP addresses* section. Specify the following information:
 - IP Address:** Specify the IP address to be configured.
 - Subnet Mask:** Specify the subnet mask.
 - Usage Type:** Specify the IP address as public, private, or both.
- 6 Click *OK*.
- 7 To delete an IP address, select the check box next to the IP address that you want to delete, then click *Delete*.
- 8 Click *Apply Changes* to save the changes.

3.4 Configuring DNS Transport Parameters

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

To configure Transport parameters:

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.

- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Select *DNS* from the *General* section.

DNS Transport Protocol

UDP

DNSResolverTimeout: :

Negative DNS LookUp: :

Maximum DNS Entry TTL: :

Minimum DNS Entry TTL: :

Maximum DNS Entry Threshold:

- 5 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 does 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.

- 6 (Optional) Click *Restore to Default* to restore the default values.
- 7 Click *OK*.
- 8 Click *Apply Changes* to save the changes.

3.5 Configuring Transport Timeout Parameters

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

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.

- 4 Select *Transport* from the *General* section.

TCP

Establish Connection Time out: 30 : Seconds

Connection KeepAlive Interval: 5 : Minutes

Data Read Time out: 2 : Minutes

Idle Server Persistent Connection Timeout: 30 : Minutes

Idle Client Persistent Connection Timeout: 10 : Minutes

Reset to Default

OK Cancel

- 5 Specify values for the following parameters:

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 can increase this value if you notice that the remote server is reachable 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.

- 6 Click *Restore to Default* to restore the default values.

- 7 Click *OK*.

- 8 Click *Apply Changes* to save the changes.

Managing Proxy Services

4

The following sections explain the tasks you complete to manage Novell® BorderManager® 3.9 Proxy Services:

- ◆ [Section 4.1, “Configuring Proxy Logging,” on page 61](#)
- ◆ [Section 4.2, “Monitoring Proxy Statistics,” on page 63](#)
- ◆ [Section 4.3, “Monitoring Cache Statistics,” on page 71](#)
- ◆ [Section 4.4, “Proxy Configuration Dump Tool,” on page 74](#)
- ◆ [Section 4.5, “Splash Screen Settings,” on page 74](#)

4.1 Configuring Proxy 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, 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.

- ◆ [Section 4.1.1, “Configuring Logging for an HTTP Proxy,” on page 61](#)
- ◆ [Section 4.1.2, “Configuring Logging for an HTTP Accelerator,” on page 62](#)

4.1.1 Configuring Logging for an HTTP Proxy

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Click *HTTP* in the *Forward Proxy* section.

- 5 Click the *Logging* tab. The HTTP logging page is displayed.

The screenshot shows a configuration dialog box with the following elements:

- Navigation tabs: HTTP, Cache Hierarchy Server, Cache Hierarchy Client, Cache Hierarchy Routing, **Logging**.
- Options:
 - Enable Logging
 - Enable Indexed Logging
 - Enable Novell Audit
- Log Directory:
- Profile Type:
- Buttons:

- 6 Select *Enable Logging* to enable HTTP logging.
- 7 If you have selected common or extended logging, click the format name and specify the following parameters for each format:
 - Log File Directory:** The 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.
- 8 Click *Apply Changes* to save the changes.

4.1.2 Configuring Logging for an HTTP Accelerator

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Click *HTTP* in the *Forward Proxy* section.

- 5 Click the *Logging* tab. The HTTP logging page is displayed.

HTTP Accelerator **Logging**

Enable Logging

Log Directory:

Logging Profile List

New... | Delete | Enable One

<input type="checkbox"/>	Name	In Use	Profile Type	Indexed Logging	Novell Audit
<input type="checkbox"/>	logprofile www example com	<input checked="" type="checkbox"/>	Common	Not Enabled	Not Enabled

OK Cancel

- 6 Select *Enable Logging* to enable HTTP logging.

- 7 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.

- 8 Click *Apply Changes* to save the changes.

4.2 Monitoring Proxy Statistics

This section has the following information:

- ◆ [Section 4.2.1, “Monitoring Proxy Cache Real-time Activity,” on page 64](#)
- ◆ [Section 4.2.2, “Monitoring HTTP Statistics,” on page 64](#)
- ◆ [Section 4.2.3, “Monitoring FTP Statistics,” on page 65](#)
- ◆ [Section 4.2.4, “Monitoring Mail \(SMTP/POP3\) Statistics,” on page 66](#)
- ◆ [Section 4.2.5, “Monitoring Gopher Statistics,” on page 67](#)
- ◆ [Section 4.2.6, “Monitoring RealAudio Statistics,” on page 68](#)
- ◆ [Section 4.2.7, “Monitoring SOCKS Statistics,” on page 69](#)
- ◆ [Section 4.2.8, “Monitoring Generic Statistics,” on page 69](#)
- ◆ [Section 4.2.9, “Monitoring ICP Statistics,” on page 70](#)
- ◆ [Section 4.2.10, “Monitoring Client FTP Statistics,” on page 70](#)

4.2.1 Monitoring Proxy Cache Real-time Activity

To view proxy cache activity information:

- 1 Log in to the Novell Remote Manager.
- 2 Select *NBM Monitoring > Proxy Monitoring*.
- 3 Click *Site Statistics*. The *Proxy Monitoring - Site Statistics* page is displayed.

Proxy Monitoring - Site Statistics

Begin Refresh Page Refresh Rate 10 seconds ▼

[\[Back to Proxy Monitoring\]](#)

Bytes Cached:0
Bytes Transferred:0
Cache Misses:0
Cache Hits:0

Site Statistics				
HostName	Connections	Bytes from Cache	Bytes from Host	Bytes from Neighbors
10.10.10.1	1	0	0	0
10.10.10.2	2	0	0	0

SitesCached:2

The following site statistics are displayed on this page:

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.

Sites Cached: Total number of proxy sites currently in the cache.

- 4 To update the statistics at a regular interval, select a value from the *Page Refresh Rate* drop-down list and click *Begin Refresh*.
- 5 To stop regular updating of statistics, click *Stop Refresh*.
- 6 To go back to the proxy monitoring page, click *Back to Proxy Monitoring*.

4.2.2 Monitoring HTTP Statistics

To view the HTTP proxy activity information:

- 1 Log in to the Novell Remote Manager.
- 2 Select *NBM Monitoring > Proxy Monitoring*.

- 3 Click *HTTP Statistics*. The *Proxy Monitoring - HTTP* page is displayed.

Proxy Monitoring - HTTP

Page Refresh Rate

[\[Back to Proxy Monitoring\]](#)

HTTP Statistics	
HTTP Server Requests:	0
HTTP Server Active Requests:	0
HTTP Server Errors:	0
HTTP Client Cache Requests:	0
HTTP Client Pass Through Requests:	0
HTTP Client Active Requests:	0
HTTP Client Retries:	0
HTTP Client Errors:	0

The HTTP statistics are displayed on this page.

- 4 To update the statistics at a regular interval, select a value from the *Page Refresh Rate* drop-down list and click *Begin Refresh*.
- 5 To stop regular updating of statistics, click *Stop Refresh*.
- 6 To go back to the proxy monitoring page, click *Back to Proxy Monitoring*.

4.2.3 Monitoring FTP Statistics

To view the FTP proxy activity information:

- 1 Log in to the Novell Remote Manager.
- 2 Select *NBM Monitoring > Proxy Monitoring*.

- 3 Click *Site Statistics*. The *Proxy Monitoring - FTP* page is displayed.

Proxy Monitoring - FTP

Page Refresh Rate

[\[Back to Proxy Monitoring\]](#)

FTP Statistics	
Active Requests:	0
Bytes Transferred:	0
Failures:	0
Successful Sessions:	0
Proxy Requests:	0
Accelerator Requests:	0
Cache Hits:	0
Cache Misses:	0
Login Failures:	0
ACL Rejections:	0

The FTP statistics are displayed on this page.

- 4 To update the statistics at a regular interval, select a value from the *Page Refresh Rate* drop-down list and click *Begin Refresh*.
- 5 To stop regular updating of statistics, click *Stop Refresh*.
- 6 To go back to the proxy monitoring page, click *Back to Proxy Monitoring*.

4.2.4 Monitoring Mail (SMTP/POP3) Statistics

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

- 1 Log in to the Novell Remote Manager.
- 2 Select *NBM Monitoring > Proxy Monitoring*.

- 3 Click *Mail (SMTP/POP3) Statistics*. The *Proxy Monitoring - Mail (SMTP/POP3)* page is displayed.

Proxy Monitoring - Mail (SMTP/POP3)

Page Refresh Rate ▼

[\[Back to Proxy Monitoring\]](#)

SMTP STATISTICS	
Messages Received:	0
Messages Stored:	0
Messages Transmitted:	0
Messages Unsent:	0

POP3 Statistics	
Bytes Transmitted:	0
Active Requests:	0
Client Authentication Errors:	0
Client Connection Errors:	0
Client Session Requests:	0

The SMTP and POP 3 statistics are displayed on this page.

- 4 To update the statistics at a regular interval, select a value from the *Page Refresh Rate* drop-down list and click *Begin Refresh*.
- 5 To stop regular updating of statistics, click *Stop Refresh*.
- 6 To go back to the proxy monitoring page, click *Back to Proxy Monitoring*.

4.2.5 Monitoring Gopher Statistics

To view gopher statistics:

- 1 Log in to the Novell Remote Manager.
- 2 Select *NBM Monitoring > Proxy Monitoring*.

- 3 Click *Gopher Statistics*. The *Proxy Monitoring - Gopher* page is displayed.

Proxy Monitoring - Gopher

Page Refresh Rate

[\[Back to Proxy Monitoring\]](#)

Gopher Statistics	
Gopher Client Cache Requests:	0
Gopher Client Active Requests:	0
Gopher Client Errors:	0
Gopher Client Local Replies:	0
Gopher Client HTML Translations:	0

The Gopher statistics is displayed on this page.

- 4 To update the statistics at a regular interval, select a value from the *Page Refresh Rate* drop-down list and click *Begin Refresh*.
- 5 To stop regular updating of statistics, click *Stop Refresh*.
- 6 To go back to the proxy monitoring page, click *Back to Proxy Monitoring*.

4.2.6 Monitoring RealAudio Statistics

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

- 1 Log in to the Novell Remote Manager.
- 2 Select *NBM Monitoring > Proxy Monitoring*.
- 3 Click *RealAudio Statistics*. The *Proxy Monitoring - RealAudio* page is displayed.

Proxy Monitoring - RealAudio

Page Refresh Rate

[\[Back to Proxy Monitoring\]](#)

RealAudio Statistics	
Bytes Transmitted:	0
Bytes Received:	0
RealAudio Sessions:	0
ACL Rejections:	0

The Real Audio statistics is displayed on this page.

- 4 To update the statistics at a regular interval, select a value from the *Page Refresh Rate* drop-down list and click *Begin Refresh*.
- 5 To stop regular updating of statistics, click *Stop Refresh*.
- 6 To go back to the proxy monitoring page, click *Back to Proxy Monitoring*.

4.2.7 Monitoring SOCKS Statistics

To view proxy cache activity information:

- 1 Log in to the Novell Remote Manager.
- 2 Select *NBM Monitoring > Proxy Monitoring*.
- 3 Click *SOCKS Statistics*. The *Proxy Monitoring - SOCKS* page is displayed.

Proxy Monitoring - SOCKS

Page Refresh Rate

[\[Back to Proxy Monitoring\]](#)

SOCKS Statistics	
TCP Requests:	0
UDP Requests:	0

The SOCKS statistics is displayed on this page.

- 4 To update the statistics at a regular interval, select a value from the *Page Refresh Rate* drop-down list and click *Begin Refresh*.
- 5 To stop regular updating of statistics, click *Stop Refresh*.
- 6 To go back to the proxy monitoring page, click *Back to Proxy Monitoring*.

4.2.8 Monitoring Generic Statistics

To view Generic proxy activity information:

- 1 Log in to the Novell Remote Manager.
- 2 Select *NBM Monitoring > Proxy Monitoring*.
- 3 Click *Generic Statistics*. The *Proxy Monitoring - Generic* page is displayed.

Proxy Monitoring - Generic

Page Refresh Rate

[\[Back to Proxy Monitoring\]](#)

Generic Statistics	
TCP Bytes Transferred:	0
UDP Bytes Transferred:	0
TCP Connections:	0
UDP Connections:	0
TCP ACL Errors:	0
UDP ACL Errors:	0

This page displays the generic statistics on in this page:

- 4 To update the statistics at a regular interval, select a value from the *Page Refresh Rate* drop-down list and click *Begin Refresh*.
- 5 To stop regular updating of statistics, click *Stop Refresh*.
- 6 To go back to the proxy monitoring page, click *Back to Proxy Monitoring*.

4.2.9 Monitoring ICP Statistics

To view ICP statistics:

- 1 Log in to the Novell Remote Manager.
- 2 Select *NBM Monitoring > Proxy Monitoring*.
- 3 Click *ICP Statistics*. The *Proxy Monitoring - ICP* page is displayed.

Proxy Monitoring - ICP

Page Refresh Rate

[\[Back to Proxy Monitoring\]](#)

ICP Statistics	
Server Hits:	0
Server Misses:	0
Server Errors:	0
Fill Cache Requests:	0
Parent Hits:	0
Sibling Hits:	0

The ICP statistics are displayed on this page.

- 4 To update the statistics at a regular interval, select a value from the *Page Refresh Rate* drop-down list and click *Begin Refresh*.
- 5 To stop regular updating of statistics, click *Stop Refresh*.
- 6 To go back to the proxy monitoring page, click *Back to Proxy Monitoring*.

4.2.10 Monitoring Client FTP Statistics

To view the client FTP statistics:

- 1 Log in to the Novell Remote Manager.
- 2 Select *NBM Monitoring > Proxy Monitoring*.

- 3 Click *Client FTP Statistics*. The *Proxy Monitoring - Client FTP* page is displayed.

Proxy Monitoring - Client FTP

Page Refresh Rate ▼

[\[Back to Proxy Monitoring\]](#)

Client FTP Statistics	
FTP Client Cache Requests:	0
FTP Client Active Requests:	0
FTP Client Errors:	0
FTP Client Directory Requests:	0
FTP Client File Requests:	0

The Client FTP statistics is displayed on this page.

- 4 To update the statistics at a regular interval, select a value from the *Page Refresh Rate* drop-down list and click *Begin Refresh*.
- 5 To stop regular updating of statistics, click *Stop Refresh*.
- 6 To go back to the proxy monitoring page, click *Back to Proxy Monitoring*.

4.3 Monitoring Cache Statistics

This section has the following information:

- ♦ [Section 4.3.1, “Monitoring General Cache Statistics,” on page 71](#)
- ♦ [Section 4.3.2, “Monitoring DNS Cache Statistics,” on page 72](#)
- ♦ [Section 4.3.3, “Monitoring Connection Cache Statistics,” on page 73](#)
- ♦ [Section 4.3.4, “Monitoring Download Cache Statistics,” on page 74](#)

4.3.1 Monitoring General Cache Statistics

To view General cache statistics:

- 1 Log in to the Novell Remote Manager.
- 2 Select *NBM Monitoring > Proxy Monitoring*.

- 3 Click *General Cache Statistics*. The *Proxy Monitoring - General Cache Statistics* page is displayed.

Proxy Monitoring - General Cache

Page Refresh Rate

[\[Back to Proxy Monitoring\]](#)

General Cache Statistics	
Total Objects In Cache:	0
Hot Objects In Cache:	0
Cold Objects In Cache:	0
Number Of Requests Serviced:	0
Hits On Hot Objects:	0
Hits On Cold Objects:	0
Cache Misses:	0
Volume In Requests Serviced(Kb):	0
Fetches From Cache:	0
Fetches From Neighbors:	0
Fetches From Source:	0

The General Cache statistics are displayed on this page.

- 4 To update the statistics at a regular interval, select a value from the *Page Refresh Rate* drop-down list and click *Begin Refresh*.
- 5 To stop regular updating of statistics, click *Stop Refresh*.
- 6 To go back to the proxy monitoring page, click *Back to Proxy Monitoring*.

4.3.2 Monitoring DNS Cache Statistics

To view DNS cache statistics:

- 1 Log in to the Novell Remote Manager.
- 2 Select *NBM Monitoring > Proxy Monitoring*.

- 3 Click *DNS Cache Statistics*. The *Proxy Monitoring - DNS Cache* page is displayed.

Proxy Monitoring - DNS Cache

Page Refresh Rate

[\[Back to Proxy Monitoring\]](#)

DNS Cache Statistics	
DNS Cache Lookup Requests:	4
DNS Cache Lookup Hits:	2
DNS Cache Lookup Misses:	2
DNS Negative Cache Hits:	0
DNS Errors:	0

The DNS Cache statistics are displayed on this page.

- 4 To update the statistics at a regular interval, select a value from the *Page Refresh Rate* drop-down list and click *Begin Refresh*.
- 5 To stop regular updating of statistics, click *Stop Refresh*.
- 6 To go back to the proxy monitoring page, click *Back to Proxy Monitoring*.

4.3.3 Monitoring Connection Cache Statistics

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

- 1 Log in to the Novell Remote Manager.
- 2 Select *NBM Monitoring > Proxy Monitoring*.
- 3 Click *Connection Cache Statistics*. The *Proxy Monitoring - Connection Cache* page is displayed.

Proxy Monitoring - Connection Cache

Page Refresh Rate

[\[Back to Proxy Monitoring\]](#)

Connection Cache Statistics	
Total Connection Blocks:	28
Active Connection Blocks:	1
Total Request Blocks:	2
Total Sent ECBs:	8
Total Sent Fragments:	129
Idle Persistent Client CBs:	0
Idle Persistent Server CBs:	0

The Connection Cache statistics is displayed on this page.

- 4 To update the statistics at a regular interval, select a value from the *Page Refresh Rate* drop-down list and click *Begin Refresh*.
- 5 To stop regular updating of statistics, click *Stop Refresh*.
- 6 To go back to the proxy monitoring page, click *Back to Proxy Monitoring*.

4.3.4 Monitoring Download Cache Statistics

To view download cache activity information:

- 1 Log in to the Novell Remote Manager.
- 2 Select *NBM Monitoring > Proxy Monitoring*.
- 3 Click *Download Cache Statistics*. The *Proxy Monitoring - Download Cache* page is displayed.

Proxy Monitoring - Download Cache

Page Refresh Rate

[\[Back to Proxy Monitoring\]](#)

Download Cache Statistics	
Active Sessions:	0
Objects Downloaded:	0
Sessions Completed:	0

The download cache statistics is displayed on this page.

- 4 To update the statistics at a regular interval, select a value from the *Page Refresh Rate* drop-down list and click *Begin Refresh*.
- 5 To stop regular updating of statistics, click *Stop Refresh*.
- 6 To go back to the proxy monitoring page, click *Back to Proxy Monitoring*.

4.4 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`.

4.5 Splash Screen Settings

The splash screen settings

```
[Extra Configuration]SplashScreenEnabled=1
```

Using Novell Audit for HTTP Proxy Logging

5

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

Novell Audit is an additional logging method apart from the other legacy logging methods such as Common, Extended and Indexed logging. However, Novell Audit has several key advantages, including:

- ♦ **Security:** Novell Audit events are signed and chained, which means that you have forensically viable evidence of all HTTP proxy activity. Novell Audit guarantees that no log data has been deleted or modified.
- ♦ **Log Data Aggregation:** The Novell Audit Secure Logging Server allows you to collect log data from multiple BorderManager proxy servers into one data store. Reports can then be generated that reflect Web activity for an entire organization, not just one server.
- ♦ **Performance:** Novell Audit is very fast and scalable. It allows you to do comprehensive logging with minimal impact on proxy performance.

This section has the following information:

- ♦ [Section 5.1, “Configuring Novell BorderManager for Novell Audit,” on page 75](#)
- ♦ [Section 5.2, “Understanding the Novell BorderManager Event Data,” on page 76](#)
- ♦ [Section 5.3, “Viewing Events in Novell Audit Report,” on page 77](#)
- ♦ [Section 5.4, “Configuring the Audit Server,” on page 78](#)

5.1 Configuring Novell BorderManager for Novell Audit

Novell BorderManager is not enabled for NovellAudit by default. You must configure it first:

- 1** Ensure that Novell Audit is properly installed and configured. This includes installing a Secure Logging Server and installing the NetWare Platform Agent on each BorderManager proxy server that will be reporting events to Novell Audit.
- 2** Ensure that the Platform Agents are correctly configured to communicate with the Secure Logging Server. On each BorderManager proxy server that will be reporting events to Novell 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** To simplify Secure Logging Server setup, an NCF file is provided that prepares Novell Audit to receive BorderManager 3.9 events. This file is located at `sys:\etc\proxy\naudit\runaud.ncf` on any server where BorderManager 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.

This only needs to be done once, no matter how many BorderManager proxy servers will be reporting events to Novell Audit.

4 Do one of the following:

- ♦ 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.
- ♦ If the 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.
- ♦ If the Secure Logging Server is 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.
- ♦ If the Secure Logging Server is on other platforms, see the Novell Audit product documentation for instructions on how to set up new applications on other platforms supported by the Secure Logging Server.

5 Restart the Secure Logging Server.

6 On each BorderManager proxy server that will be reporting events to Novell Audit, use a text editor to add the following in the `sys:\etc\proxy\proxy.cfg` file:

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

7 Restart the BorderManager servers.

5.2 Understanding the Novell BorderManager 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 HTTP proxy.

For the purposes of Novell Audit, each URL request through the BorderManager 3.9 HTTP proxy generates four events as indicated 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
00040004	Rule Hit Logging	Username or source IP address, URL or destination IP address, action (whether to allow or deny), rule sequence number, and type of ACL including time restriction.
00040005	Third Party Categorization	URL, username, URL-category, vendor-ID

For descriptions of the data fields in the Common and Extended Log Data events, refer to a 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)

Capturing the Third Party Categorization data is unique to BorderManager 3.9's support for Novell Audit. Descriptions of the Third Party Categorization data fields follow:

Data Field	Description
URL	The URL of the Web content being requested.
username	The name of the user requesting the URL.
URL-category	The categorization of the URL, based on the third-party categorization product being used on the proxy server that handled the request.
vendor-ID	The Vendor IDs for different third party categorization products are: <ul style="list-style-type: none">♦ 1: CyberPatrol* (This is not officially supported on BorderManager 3.9.)♦ 3: SurfControl Content Database♦ 4: N2H2 Category Server♦ 7: Connectotel LinkWALL*

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

5.3 Viewing Events in Novell Audit Report

Novell 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).

To generate a simple query:

- 1 In the Novell 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 the following SQL statements:

- ♦ To view all logs, enter the following command:

```
select * from log;
```
- ♦ To query for all common logs of Novell BorderManager, enter the following command:

```
select * from log where EventID=0x00040001;
```
- ♦ To query for all extended logs of Novell BorderManager, enter the following command:

```
select * from log where EventID=0x00040002;
```
- ♦ To query for all Rule Hit logs of Novell BorderManager, enter the following command:

```
select * from log where EventID=0x00040004;
```

5.4 Configuring the Audit Server

The Secure Logging Server manages the flow of information to and from the Novell auditing system. It receives incoming events and requests from the Platform Agents, logs information to the data store, monitors designated events, and provides filtering and notification services. It can also be configured to automatically reset critical system attributes according to a specified policy.

After you make configuration changes to any Novell Audit setting on an audit server, you must restart the audit server.

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Select *Novell Audit* in the *General* section.
- 5 Specify the IP address or DNS name of your auditing server:
 - Server:** The audit logging server you want to use. For failover protection, you can configure up to three servers. By default, the system uses the primary IP address. If you want to use a different server, specify that server's IP address here.
 - Port:** The port where the Platform Agents connect to the Secure Logging Server.
- 6 Click *OK*.
- 7 Click *Apply Changes* to save the changes.

Configuring Access Rules

6

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

When you enabled the Novell BorderManager 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) 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.

The default rule is set to deny any source to any destination. The default rule is created at the time of Novell BorderManager installation. Click the *Effective Rules* button in the proxy configuration page to view the default rule.

This section contains the following information:

- ◆ [Section 6.1, “Configuring a Rule to Allow Access through an Application Proxy,” on page 79](#)
- ◆ [Section 6.2, “Configuring URL-Based Access Rules,” on page 80](#)
- ◆ [Section 6.3, “Configuring Third-Party Filtering Solutions,” on page 81](#)
- ◆ [Section 6.4, “Configuring Time Restrictions for Access Rules,” on page 82](#)
- ◆ [Section 6.5, “Configuring Access Rule Ordering,” on page 82](#)
- ◆ [Section 6.6, “Viewing All Access Rules that Apply to an Object,” on page 83](#)

6.1 Configuring a Rule to Allow Access through an Application Proxy

If you want access rules to apply to users accessing services through an application proxy, you must set up access rules for the individual application proxies.

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Access Rules*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Click *New*, then select one of the options.
- 5 Specify a name for the rule in the *Name* field.
- 6 Specify a description of the rule in the *Description* field.
- 7 Click *New* in the *Condition Group* section, then select the conditions that you want to be added to the rule.

- 8 Select a value for the *Comparison* field
- 9 Specify a value for the *Value* field.
- 10 Select *Allow* at the *Action* field to allow access.
- 11 (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 enable this option to detect unauthorized activity.
- 12 Click *OK*.
- 13 Click *Apply Changes* to save the changes.

6.2 Configuring URL-Based Access Rules

URL-based access rules apply to users accessing Web content through the HTTP or FTP 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.

This section has the following information:

- ♦ [Section 6.2.1, “Configuring a URL-Based Access Rule for FTP or HTTP Proxy,” on page 80](#)
- ♦ [Section 6.2.2, “Modifying the Existing Access Rules as URL-based Access Rules,” on page 81](#)
- ♦ [Section 6.2.3, “Modifying the Existing URL-Based Access Rules,” on page 81](#)

6.2.1 Configuring a URL-Based Access Rule for FTP or HTTP Proxy

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Access Rules*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Click *New*, then select *HTTP* if you want to configure access rules for HTTP or select *FTP* if you want to configure access rules for FTP.
- 5 Specify a name for the rule in the *Name* field.
- 6 Specify a brief description of the rule in the *Description* field.
- 7 Click *New* in the *Condition Group* section, then select *URL* from the list.
- 8 Select a value for the *Comparison* field
- 9 Specify a value for the *Value* field.
- 10 Specify whether to set the action to *Allow* or *Deny*.
- 11 (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 enable this option so to detect unauthorized activity.
- 12 Click *OK*.
- 13 Click *Apply Changes* to save the changes.

6.2.2 Modifying the Existing Access Rules as URL-based Access Rules

You can modify the existing HTTP and FTP access rules into URL-based access rules as follows:

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Access Rules*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Select the HTTP or the FTP access-rule that you want to change into a URL-based rule.
- 5 Delete *Origin Server Port*, *Destination: Host IP addresses* and *Destination: DNS Hostname* from the *Condition Group* section.
- 6 Select Step 7 to Step 13 in [Section 6.2.1, “Configuring a URL-Based Access Rule for FTP or HTTP Proxy,”](#) on page 80.

6.2.3 Modifying the Existing URL-Based Access Rules

To change the existing URL-based access rules into FTP or HTTP access rules, follow the steps given below:

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Access Rules*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Select the URL-based access rule that you want to modify.
- 5 Delete *URL* from the *Condition Group* section.
- 6 Select Step 5 to Step 13 in [Section 6.1, “Configuring a Rule to Allow Access through an Application Proxy,”](#) on page 79.

6.3 Configuring Third-Party Filtering Solutions

You can configure third-party filtering solutions with the URL-based access rules.

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Access Rules*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Click *New*, then select any of the options.
- 5 Click *New*, then select HTTP.
- 6 Specify a name for the rule in the *Name* field.
- 7 Specify a description of the rule in the *Description* field.
- 8 Click *New* in the *Condition Group*, then select URL.
- 9 Select a type for the *Type* field
- 10 Specify a value for the *Select Category* field.

- 11 Specify whether to set the action to *Allow* or *Deny*.
- 12 (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 enable this option to detect unauthorized activity.
- 13 Click *OK*.
- 14 Click *Apply Changes* to save the changes.

6.4 Configuring 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.

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Access Rules*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Click *New*, then select any of the proxy services.
- 5 Specify a name for the rule in the *Name* field.
- 6 Specify a brief description of the rule in the *Description* field.
- 7 Click *New* in the Condition Group, then select *Time*.
- 8 Select a type for the *Type* field.
- 9 Specify a value for the *Select Category* field.
- 10 Specify whether to set the action to *Allow* or *Deny*.
- 11 (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 enable this option to detect unauthorized activity.
- 12 Click *OK*.
- 13 Click *Apply Changes* to save the changes.

6.5 Configuring Access Rule Ordering

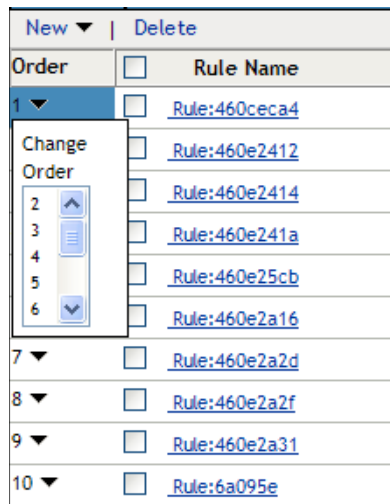
The first rule in the access rule is always checked first. If the first rule matches the criteria, then no other rules are checked. Therefore, it is very important to order the Access Rules, so that the most

important rule is never missed. By default, any new rule that you create takes the last position. But you can change the order of the rules as per your requirement.

- 1 Create access rules. For more information on creating access rules, see [Section 6.1](#), “Configuring a Rule to Allow Access through an Application Proxy,” on page 79.

Proxy Configuration		Access Rules							
Rules:		NWSERVER-37.novell							
New		Delete							
Order	<input type="checkbox"/>	Rule Name	Action	Source	Access	Destination	Time	Log	Description
1	▼	<input type="checkbox"/> Rule:460ceca4	Allow	Any	HTTP	[IPAddress].....	No	No	
2	▼	<input type="checkbox"/> Rule:460e2412	Allow	[NDSObject].....	HTTP	[URL List].....	No	No	
3	▼	<input type="checkbox"/> Rule:460e2414	Allow	[IPAddrss].....	HTTP	[URL List].....	No	No	
4	▼	<input type="checkbox"/> Rule:460e241a	Allow	Any	Port	[IPAddress].....	No	No	
5	▼	<input type="checkbox"/> Rule:460e25cb	Allow	Any	HTTP	[URL List].....	No	No	
6	▼	<input type="checkbox"/> Rule:460e2a16	Allow	Any	HTTP	[URL List].....	No	No	
7	▼	<input type="checkbox"/> Rule:460e2a2d	Allow	Any	HTTP	[URL List].....	No	No	
8	▼	<input type="checkbox"/> Rule:460e2a2f	Allow	Any	HTTP	[URL List].....	No	No	
9	▼	<input type="checkbox"/> Rule:460e2a31	Allow	Any	HTTP	[URL List].....	No	No	
10	▼	<input type="checkbox"/> Rule:6a095e	Allow	Any	HTTP	[URL List].....	No	No	

- 2 To change the order of any of the access rules, click the arrow in the *Order* section.



- 3 Select the order that you want to move the access rule to. For example, if you want to move the access rule that is currently in the first position to the eighth position, click the arrow in the Order section of the first access rule, then select 8. The access rule shifts to the eighth position.

6.6 Viewing All Access Rules that Apply to an Object

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

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Access Rules*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.

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.

Configuring Alert Notification

7

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

- ♦ Server performance
- ♦ License acquisition, excluding Novell BorderManager Authentication Services licenses
- ♦ Security
- ♦ Proxy server connections

Novell BorderManager 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 server, the default notification includes the following:

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

NOTE: Novell BorderManager 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.

7.1 Configuring E-Mail Alert Notification

- 1 Log in to iManager.
- 2 Select *Novell BorderManager > Proxy Services*.
- 3 Browse to and select the BorderManager server or container that you want to configure, then click *OK*.
- 4 Select *Alerts* from the *General* section.
- 5 Select one of the following notification schemes:
 - Inherited:** 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.
 - 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 6.
 - None:** Disables the alert service. No event or error notification will occur. However, selecting None preserves your configuration; recipients and servers are only inactive.
- 6 (Optional) If you selected *Send Alert*, specify the alert conditions for which you want notification as given in the following steps:
 - 6a Click *Alert Conditions*.

6b Select *All* to select all alert conditions. The default option is all. Otherwise, to select specific conditions, click *Specific*.

6c Select the alert conditions, then click *OK*.

7 Specify E-mail Alert Recipients and E-mail Servers.

The Novell BorderManager server must be configured with at least one e-mail server. Otherwise, alert notification fails.

7a Click *New* to add a new *E-mail Alert Recipient* and specify the e-mail address of the person to be notified by Novell BorderManager Alert.

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

7b (Optional) To remove a recipient from the list, select the recipient's e-mail address, then click *Delete*.

7c Click *New* to add a new E-mail Server and specify the e-mail server name or IP address for the recipients added in Step 7a.

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 Alert sends alerts to only one e-mail server on the list.

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

7d (Optional) To remove an e-mail server or servers from the list, select the e-mail server name or IP address, then click *Delete*.

7e (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.

8 Click *OK* to save the configuration.

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 servers to be notified of the configuration change in NDS or eDirectory.

9 (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:

9a Double-click the Server object representing the Novell BorderManager server you want to begin using the alert configuration immediately.

9b From the Server object's Details page, click *Novell BorderManager Alert* to view the Novell BorderManager Alert page for the server.

9c Click *Refresh Server*.

IMPORTANT: When you first open the Novell BorderManager 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.

Managing Alert Messages

8

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

- ♦ [Section 8.1, “Viewing Alerts Sent as E-Mail Messages,” on page 89](#)
- ♦ [Section 8.2, “Viewing Alerts in Audit Trail Log File,” on page 90](#)
- ♦ [Section 8.3, “Viewing Alerts in the Control Log,” on page 91](#)
- ♦ [Section 8.4, “Responding to Alerts,” on page 91](#)

See [Chapter 7, “Configuring Alert Notification,” on page 85](#) for information on how to set up alerts.

8.1 Viewing Alerts Sent as E-Mail Messages

All e-mail notifications triggered by Novell BorderManager 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 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.
- ♦ All e-mail addresses configured for the Novell BorderManager 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 server and inspect the trace on the route.
- ♦ There are no filters on routers between the Novell BorderManager server and the mail server that deny Simple Mail Transfer Protocol (SMTP) traffic.

8.2 Viewing Alerts in Audit Trail Log File

Novell BorderManager 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 90](#)
- ♦ [“Archiving the Audit Trail Log File” on page 91](#)

8.2.1 Displaying Audit Trail Log Records with the Audit Trail Utility

To run the CSLIB audit trail utility:

- 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.

8.2.2 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.

8.3 Viewing Alerts in the Control Log

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

To view the console log at the server console, use the following command:

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

8.4 Responding to Alerts

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

For information on specific alerts:

- ♦ “[Server Performance Alerts](#)” on page 92
- ♦ “[License Acquisition Alerts](#)” on page 93
- ♦ “[Security Alerts](#)” on page 93
- ♦ “[Proxy Alerts](#)” on page 95

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

Alert	Recommended Actions
Disk space shortage	Reduce the size and number of log files. Add more disk space, if necessary.

Alert	Recommended Actions
Memory shortage	<p>Check server resources using monitor.nlm 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 startup.ncf 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>
ECB shortage	<p>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.</p>
License error	<p>Verify the current licenses installed for the server and check for license conflicts or expired trial licenses. Install additional licenses, if necessary.</p>
Loading or unloading a security-sensitive NLM	<p>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.</p>
Oversized ping packet	<p>Use a packet sniffer to capture packets and determine the source IP address.</p> <p>Configure a TCP/IP packet forwarding filter to block pings originating from that source.</p>
SYN packet flooding	<p>Use a packet sniffer to capture packets and determine the source IP address.</p> <p>Configure a TCP/IP packet forwarding filter to block TCP packets originating from that source.</p>
Oversized UDP packet	<p>Use a packet sniffer to capture packets and determine the source IP address.</p> <p>Configure a TCP/IP packet forwarding filter to block UDP packets originating from that source.</p>
Cache hierarchy parent (ICP parent) down	<p>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.</p> <p>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.</p>
SOCKS server down	<p>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.</p>
POP3 or SMTP server down	<p>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.</p>

8.4.1 Server Performance Alerts

Server performance alerts notify you of potential problems with server parameters or operations that can cause Novell BorderManager 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.

8.4.2 License Acquisition Alerts

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

Novell BorderManager Alert monitors license acquisition for the following:

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

8.4.3 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 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 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 Alert, although attacks are not identified by name.

8.4.4 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 server cannot forward outgoing mail to the POP3 server or deliver incoming mail to the SMTP server.

Filters



Novell® BorderManager® delivers filter configuration based on Novell iManager. FILTCFG can still be used to configure filters.

Novell BorderManager 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 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, 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 extends the functionality. See the following sections for more information:

- ◆ [Chapter 9, “Setting Up Packet Filters,” on page 99](#)
- ◆ [Chapter 10, “Using Novell iManager for Filter Configuration,” on page 109](#)
- ◆ [Chapter 11, “Managing IP Packet Filters,” on page 145](#)
- ◆ [Chapter 12, “Backing Up and Restoring Filters,” on page 149](#)
- ◆ [Chapter 13, “Advanced Configuration of IP Packet Filters Using FILTCFG,” on page 151](#)

Setting Up Packet Filters

9

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, 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 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 service. Novell BorderManager 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 server. 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 packet filtering. For planning and conceptual information about packet filtering, see *Novell BorderManager 3.9 Proxy and Firewall Overview and Planning Guide*. Make sure you understand this information before setting up and configuring packet filtering.

The following sections are discussed here:

- ◆ [Section 9.1, “Packet Filter Prerequisites,” on page 99](#)
- ◆ [Section 9.2, “Setting Up the Default Filters,” on page 100](#)
- ◆ [Section 9.3, “Using FILTCFG for Filter Configuration,” on page 100](#)
- ◆ [Section 9.4, “Saving Filters to a Text File,” on page 106](#)
- ◆ [Section 9.5, “Enabling Global IP Packet Logging,” on page 106](#)
- ◆ [Section 9.6, “Completing Advanced Setup, Configuration, and Management Tasks,” on page 107](#)

9.1 Packet Filter Prerequisites

Before you begin to configure packet filters for your Novell BorderManager 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.

9.2 Setting Up the Default Filters

If you did not choose to secure the public interfaces of Novell BorderManager 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 the following command:

```
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 the following command:

```
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.

9.3 Using FILTCFG for Filter Configuration

These sections tell you how to use FILTCFG on a Novell BorderManager server:

- ♦ [“Setting Up Outbound Packet Filter Exceptions” on page 101](#)
- ♦ [“Setting Up Inbound Packet Filter Exceptions” on page 105](#)
- ♦ [“Defining Custom Stateful Packet Types” on page 105](#)
- ♦ [Section 9.4, “Saving Filters to a Text File,” on page 106](#)
- ♦ [Section 9.5, “Enabling Global IP Packet Logging,” on page 106](#)
- ♦ [Section 9.6, “Completing Advanced Setup, Configuration, and Management Tasks,” on page 107](#)

9.3.1 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 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 server:

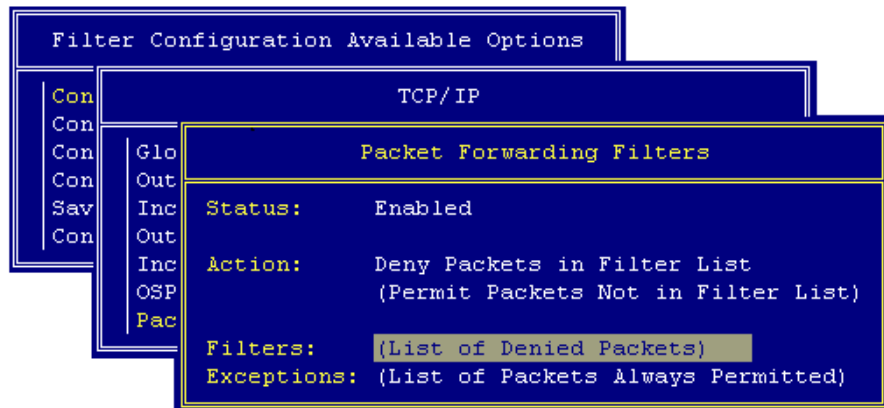
- 1** At the server console prompt, enter the following command:

```
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 9-1 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 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:

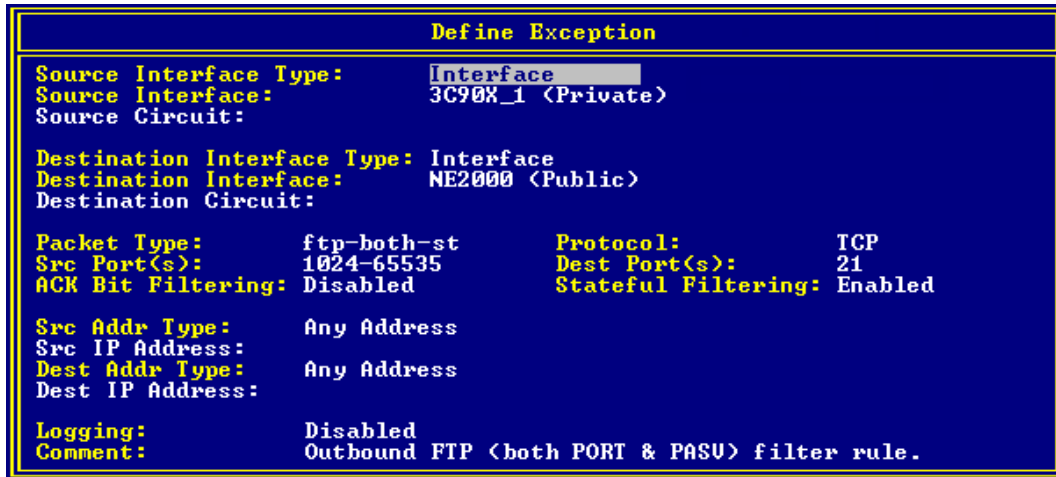
- ◆ Secure Sockets Layer (SSL) authentication: TCP port 443.
- ◆ Dynamic TCP: TCP ports 1024 to 65535.
- ◆ Dynamic UDP: UDP ports 1024 to 65535.
- ◆ VPN master or slave (IPX/TCP): TCP port 213.
- ◆ VPN client authentication: TCP port 353.
- ◆ VPN keep-alive: UDP port 353.
- ◆ VPN Simple Key Management for Internet Protocol (SKIP)[Inbrk]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 [Section 9.6, "Completing Advanced Setup, Configuration, and Management Tasks," on page 107](#), 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 9-2 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 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 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, 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.

9.3.2 Setting Up Inbound Packet Filter Exceptions

If you elected to secure the public interface Novell BorderManager 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 server's public interface:

- 1 At the server console prompt, enter the following command:

```
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.

9.3.3 Defining Custom Stateful Packet Types

The Novell BorderManager firewall has many static packet types defined in addition to the stateful packet types listed in [“Setting Up Outbound Packet Filter Exceptions” on page 101](#).

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 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.

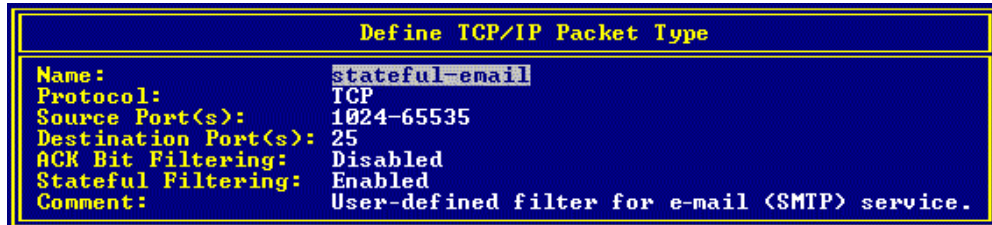
- 6 Enable stateful filtering by selecting one of the following stateful filtering modes:
 - ♦ Enabled
 - ♦ Enabled for Active FTP only (PORT)
 - ♦ Enabled for Passive FTP only (PASV)

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 9-3 Define TCP/IP Packet Type



- 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.

9.4 Saving Filters to a Text File

To document the filters and exceptions you enabled for your server:

- 1 At the server console prompt, enter the following command:

```
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.

9.5 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 the following command:

```
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.

9.6 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. For more information, see [Section 13.2, “Setting Up an HTTP Filter,” on page 151](#).
- ♦ Setting up an FTP filter. For more information, see [Section 13.3, “Setting Up an FTP Filter,” on page 153](#).
- ♦ Setting up a Telnet filter. For more information, see [Section 13.4, “Setting Up a Telnet Filter,” on page 154](#).
- ♦ Setting up an SMTP filter. For more information, see [Section 13.5, “Setting Up an SMTP Filter,” on page 156](#).
- ♦ Setting up a POP3 filter. For more information, see [Section 13.6, “Setting Up a POP3 Filter,” on page 157](#).
- ♦ Modifying default IP packet logging parameters. For more information, see [Section 11.1, “Modifying Default IP Logging Parameters,” on page 145](#).
- ♦ Viewing IP packet log information. For more information, see [Section 11.2, “Viewing IP Packet Log Information,” on page 146](#).

Using Novell iManager for Filter Configuration

10

The Novell BorderManager Access Management role and Packet Filtering configuration tasks are automatically plugged into Novell iManager during Novell BorderManager installation. By default, this role is assigned to the administrator only.

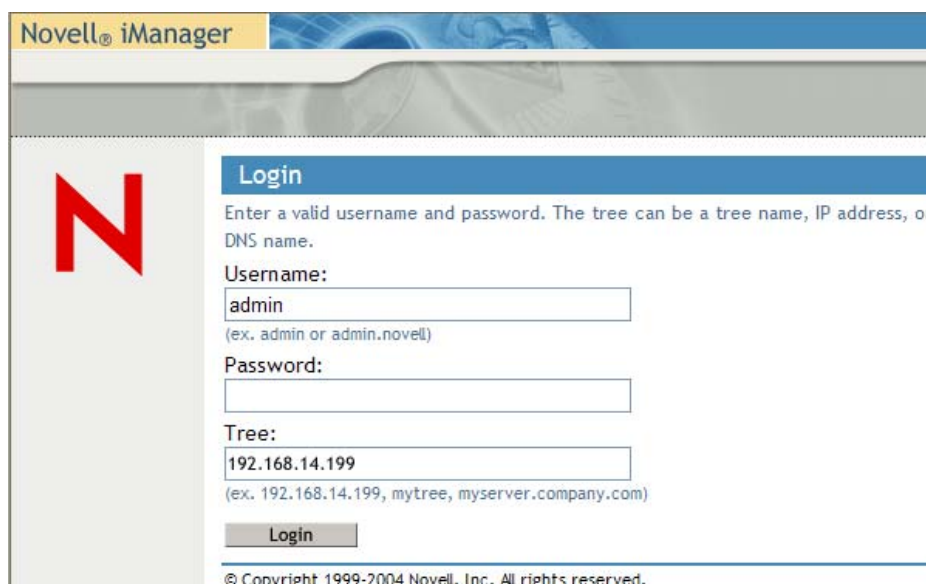
In NBM Filter Management, the Easy Filter Configuration task lets you easily configure filters and exceptions without having an extensive knowledge of services and protocols. The Filter Maintenance task allows you to restore default filters and clear filter configuration, List All Firewall Policies lists all policies in one page and Legacy Filter Configuration allows you to configure legacy filters. This section has the following information:

- ◆ Section 10.1, “Before you Begin,” on page 109
- ◆ Section 10.2, “Setting Up Public Interface,” on page 110
- ◆ Section 10.3, “Easy Filter Configuration,” on page 110
- ◆ Section 10.4, “Filter Maintenance,” on page 116
- ◆ “Legacy Filter Configuration” on page 116
- ◆ Section 10.6, “List All Firewall Policies,” on page 141
- ◆ Section 10.7, “Troubleshooting: Possible Installation Scenarios,” on page 142

10.1 Before you Begin

Make sure that Novell iManager is up and working on the NetWare® or Windows machine.

- 1 Open a Web browser and type `https://<ipaddress>/nps/iManager.html` or `https://<DNS>/nps/iManager.html` to log in to Novell iManager.



Novell® iManager

Login

Enter a valid username and password. The tree can be a tree name, IP address, or DNS name.

Username:

(ex. admin or admin.novell)

Password:

Tree:

(ex. 192.168.14.199, mytree, myserver.company.com)

© Copyright 1999-2004 Novell, Inc. All rights reserved.

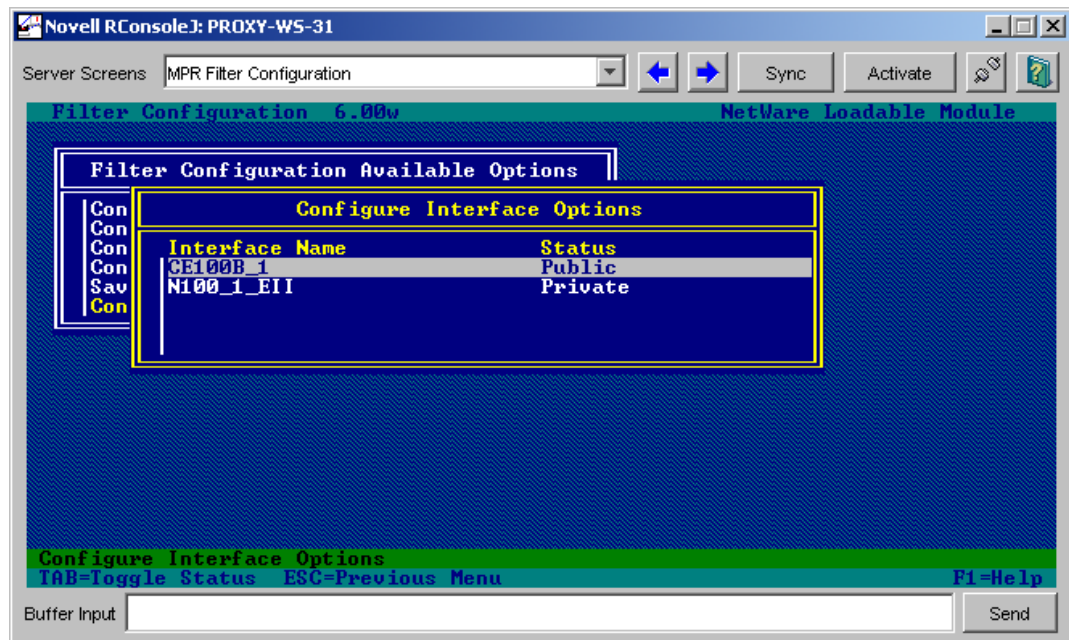
2 Expand BorderManager role in the left pane.

You will see the following links related to Filter management:

- ♦ **Easy Filter Configuration:** All NBM, On Server and Off Server services are grouped under this section for easy configuration and maintenance. For more information, see
- ♦ **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.
- ♦ **Legacy Filter Configuration:** Use this to configure packet forwarding filters, service type, incoming and outgoing RIP filters, incoming and outgoing EGP filters and OSPF filters.
- ♦ **Listall Firewall Policies:** This page lists all Firewall policies. You can modify or delete each filter/exception. New filters can also be defined and added.

10.2 Setting Up Public Interface

1 Load filtercfg.nlm, then select Configure Interface.



2 Press Tab to select the configuration as Public or Private.

3 Enter `Reinitialize system` at the server console and refresh iManager.

10.3 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

The following sections describe steps to configure filters and exceptions using Easy Filter Configuration to allow specific IP services through the Novell® BorderManager® 3.9 firewall.

- ◆ Section 10.3.1, “Configuring Filters for Novell BorderManager services,” on page 111
- ◆ Section 10.3.2, “Configuring On-Server Service Exceptions,” on page 112
- ◆ Section 10.3.3, “Configuring Off-Server Service Exceptions,” on page 114

10.3.1 Configuring Filters for Novell BorderManager services

To configure filters for Novell BorderManager Services do the following:

- 1 Log in to iManager, then select *BorderManager > Easy Filter Configuration*.
- 2 From the list, select the server where the filters are to be configured by clicking the icon and then click *OK*.

Novell BorderManager Service	Enable Filter	Enable Log	Stateful
HTTP and Secure HTTP Proxy	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FTP Proxy	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
DNS Proxy	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Mail Proxy	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
News Proxy	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Real Audio Proxy	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
RTSP Proxy	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Transparent Telnet Proxy	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
VPN Service <input type="checkbox"/> SKIP Mode <input type="checkbox"/> IKE Mode			
VPN Client-to-Site	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
VPN Site-to-Site	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

- 3 From the *Public Interface* 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*.

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

NOTE: 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\ippktlog`. 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 therefore 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*. A page listing the filters that were added is displayed.

NOTE: Use the List All Firewall Policies option to delete any filter. For more information, see [“List All Firewall Policies” on page 141](#).

10.3.2 Configuring 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.

To configure filters and exceptions for On-Server Services, complete the following steps:

- 1 Log in to iManager, then select *BorderManager > Easy Filter Configuration*.
- 2 From the list, select the server where the filters are to be configured by clicking the icon and then click *OK*.

3 Select the *On-Server Service Exceptions* tab.

Easy Filter Configuration

Public Interface IP Address

NBM Service Exceptions | **On-Server Service Exceptions** | **Off-Server Service Exceptions**

GroupWise Web Access	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GroupWise Post Office Agent	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GroupWise Mail Transfer Agent	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
File Services			
iFolder	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Apple Filing Protocol	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Common Internet File System	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Network File System	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Network Attached Storage Device	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Print Services			
iPrint	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Line Printer Daemon	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Novell Distributed Print Services	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Network Management			
ZENworks for Desktop 3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ZENworks For Server 2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ZENworks For Server 3.2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Miscellaneous			
iManager	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Web Server	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Remote Debugger	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

4 To enable the filter for a service, select the corresponding check box under *Enable Filter..*

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

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.

- 5 To enable the log for a service, select the corresponding check box, under *Enable Log*.
- 6 Select the check box under *Stateful* to enable a stateful filter.
- 7 Click *Add*.

The results page is displayed.

10.3.3 Configuring Off-Server Service Exceptions

To configure Off-Server service exceptions, complete the following steps:

- 1 Log in to iManager, then select *NBM Filter Management > Easy Filter Configuration*.
- 2 From the list, select the server where the filters are to be configured by clicking the icon and then click *OK*.

3 Select the *Off-Server Services Exceptions* tab.

Easy Filter Configuration

Public Interface IP Address

NBM Service Exceptions | **On-Server Service Exceptions** | **Off-Server Service Exceptions**

This page allows you to create Firewall exceptions for Off-Server services. Use "List All Firewall Policies" task to delete exceptions.

Off Server Services	Enable Filter	Enable Log	Stateful	Behind Firewall	Outside Firewall	Server IP Address
Proxy Services						
HTTP and Secure HTTP Proxy	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
FTP Proxy	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
Mail Proxy	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
News Proxy	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
Real Audio Proxy	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
RTSP Proxy	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
DNS Proxy	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
Transparent Telnet Proxy	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
Other Services						
Mail Server	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>			<input type="text"/>
Web Server	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>			<input type="text"/>
FTP Server	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>			<input type="text"/>
DNS Server	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>			<input type="text"/>
VPN Service <input type="checkbox"/> SKIP Mode <input checked="" type="checkbox"/> IKE Mode						
VPN Client-to-Site	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>			<input type="text"/>
VPN Site-to-Site	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>			<input type="text"/>

4 From the *Public Interface* drop-down list 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.

5

6 To enable the filter for a service, select the corresponding check box under *Enable Filter*.

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

7 To enable the log for a service, select the corresponding check box, under *Enable Log*.

8 Select the check box under *Stateful* to enable a stateful filter.

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.

9 Indicate whether the proxy server is behind or outside the firewall by selecting the respective radio buttons.

9a Select *Behind Firewall* if the service is behind the firewall and the traffic to the Internet has to pass through the firewall.

9b 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*.

10 Specify the server IP address of the proxy where the services are running in the Server IP Address field, then click *Add*.

10.4 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 Log in to iManager, then select *BorderManager > Filter Maintenance*.

2 From the list, select the server where the filters are to be configured by clicking the icon and then click *OK*.

BorderManager Filter Maintenance

Select the operation you would like to perform:

Restore Default Filters
Clear Filter Configuration

<input type="button" value="Next >>"/>	<input type="button" value="Cancel"/>
--	---------------------------------------

3 To restore default filters do the following:

3a select the *Restore Default Filters* option, then click *Next*.

3b Select a public interface from the *Public Interface* drop-down list, then click *OK*.

4 To clear filter configuration and remove all filters and exceptions from the server, select *Clear Filter Configuration*, then click *OK*. Click *OK*, to reconfirm.

10.5 Legacy Filter Configuration

1 Log in to iManager, then select *BorderManager > Legacy Filter Configuration*.

- From the list, select the server where the filters are to be configured by clicking the icon, then click *OK*.



Global IP Logging

Select the operation you would like to perform:

- Configure Packet Forwarding Filters
- Configure Service Type
- Configure Incoming RIP Filters
- Configure Outgoing RIP Filters
- Configure Incoming EGP Filters
- Configure Outgoing EGP Filters
- Configure OSPF Filters

Next >> Done Cancel Help

To set up the Packet Filtering Configuration Task, refer to [Section 10.5.1, “Configuring the Packet Forwarding Filter,”](#) on page 118.

To ensure that the configured filters are active, check to see that you have enabled filter support using INETCFG.

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.

- 4 Select the Global IP Logging check box if you want to enable global IP logging. The global logging status for all filter types can be enabled or disabled from the configuration menu.
- 5 Click *Done* if you want to save changes to IP logging and exit Filter Configuration.
- 6 Click *Cancel* to exit Filter Configuration.

The following sections contain information about configuring filter types:

- ♦ [Section 10.5.1, “Configuring the Packet Forwarding Filter,” on page 118](#)
- ♦ [Section 10.5.2, “Configuring the Service Type,” on page 123](#)
- ♦ [Section 10.5.3, “Configuring an Incoming RIP Filter,” on page 125](#)
- ♦ [Section 10.5.4, “Configuring an Outgoing RIP Filter,” on page 128](#)
- ♦ [Section 10.5.5, “Configuring an Incoming EGP Filter,” on page 132](#)
- ♦ [Section 10.5.6, “Configuring an Outgoing EGP Filter,” on page 135](#)
- ♦ [Section 10.5.7, “Configuring an OSPF Filter,” on page 138](#)

10.5.1 Configuring the Packet Forwarding Filter

- 1 Log in to iManager, then select *BorderManager > Legacy Filter Configuration*.
- 2 From the list, select the server where the filters are to be configured by clicking the icon, then click *OK*.

Packet Forwarding Filter Configuration

Status
 Disabled

Action
 Deny Packets in Filter list

Select a list of filters to be configured:
 Filter List
 Exception List

Next >> Done Cancel

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.

- 3 Select *Filter List* or *Exception List* and click *Next* to configure filters in that list. The Packet Forwarding Filter Configuration page is displayed.

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	-

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.

- 4 To change properties for the filters, select the filter that you want to modify and click *Modify*.


- 5 Click *Add* to add a new filter.

 **Packet Forwarding Filter Configuration**

Filter Name:

Service Type:
ANY 

Comment:

Logging:
Disabled 

This page helps you to add or modify your filter properties.

Filter Name: Specify the name of the packet filter. This is the name of the filter object that would be created in Novell eDirectory.

Service Type: Specify 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.

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*.

- 6 You can add or modify the following 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.

Comment: Specify a short comment in this field, to save in the database along with the other entries in the form.is

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.

7 Click *Next* to add or alter the source information for the filter.

Packet Forwarding Filter Configuration

Source Interface Type:

Source Interface:

Source Circuit:

Source Address Type:

Source IP Address:

Source Subnet Mask:

8 You can to add or modify the following 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.

- 9 Click *Next* to configure the destination information for filters.

Packet Forwarding Filter Configuration

Destination Interface Type:

Destination Interface:

Destination Circuit:

Destination Address Type:

Destination IP Address:



Destination Subnet Mask:

- 10 You can add or modify the following 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.
- 11 Click *Done* to save changes to the status or action of this filter type and return to the filter configuration menu.
- 12 Click *Cancel* to discard changes to the status or action and return to the filter configuration menu.

10.5.2 Configuring the Service Type

This page allows you to configure new TCP/IP service types and modify the property of existing ones.

- 1 Log in to iManager, then select *BorderManager > Legacy Filter Configuration*.
- 2 From the list, select the server where the filters are to be configured by clicking the icon, then click *OK*.
- 3 Select *Configuring Service Type*, then click *Next*.

 Service Type Configuration 

Defined TCP/IP Service Types

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"/>	AH-st	51	-	-	Stateful Authentication Header Protocol
<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"/>	chargen	TCP	All	19	Character Generator
<input type="checkbox"/>	chargen/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
<input type="checkbox"/>	dynamic/tcp	TCP	All	1024-65535	Dynamic Destination Ports Over TCP
<input type="checkbox"/>	dynamic/udp	UDP	All	1024-65535	Dynamic Destination Ports Over UDP
<input type="checkbox"/>	echo	TCP	All	7	
<input type="checkbox"/>	echo/udp	UDP	All	7	Echo Over User Datagram Protocol
<input type="checkbox"/>	ESP-st	50	-	-	Stateful Encapsulating Security Payload Protocol
<input type="checkbox"/>	exec	TCP	All	512	Remote Command Execution
<input type="checkbox"/>	finger	TCP	All	79	
<input type="checkbox"/>	ftp	TCP	All	21	File Transfer Control

This page gives you a summary of defined TCP/IP service types.

- 4 You can add new service types, or delete or modify only User Service types.

Service Type Configuration

Add New Service Type:

Name:

Protocol:

Select from list

IP(0) 

Specify protocol id

Source Port:

Destination Port:

ACK Bit Filtering:

Disabled

Enabled

Stateful Filtering:

Disabled 

Comment:

OK

Cancel

Fill in the following fields:

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 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.

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 rule, 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.

- 5 Click *OK* to add the Service Type.

10.5.3 Configuring an Incoming RIP Filter

You can configure the incoming RIP filters as follows:

- 1 Log in to iManager, then select *BorderManager > Legacy Filter Configuration*.
- 2 From the list, select the server where the filters are to be configured by clicking the icon, then click *OK*.
- 3 Select *Configuring Incoming RIP Filters*, then click *Next*.

Incoming RIP Filter Configuration

Status
Disabled

Action
Deny Packets in Filter list

Select a list of filters to be configured:
Filter List
Exception List

Next >> Done Cancel

This page helps you to set the properties of the selected filter type.

Status: You can either enable or disable 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: You can either deny or permit 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: You can 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.
- 4 Select Filter List or Exception List and click *Next* to configure filters in that list. The next page displays the list of routes denied or always permitted depending on whether you have selected the Filter List or Exception list respectively.

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.

- 5 Click Add to add new filters or select the filter you want to modify and click modify.

Incoming RIP Filter Configuration

Incoming RIP Filter Name:

Filtered Route:
Route to Network or Host:

Accept Route From:
Source Type:

Comment:

Logging:

Fill in the following fields:

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.

6 Click *Next* to configure the filter information:

Incoming RIP Filter Configuration

Filtered Route:

Route to Network or Host: All Routes

Accept Route From:

Source Type: Interface

Source Interface:

All Interfaces

Source Circuit:

-NA-

<< Previous

Done

Cancel

Fill in the following information:

Filtered Route: This section has the following fields:

- ♦ **Route to 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: This section has the following fields:

- ♦ **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.
 - ♦ **IP Address of Network:** If your Source Type is Network or Host, specify the IP address.
 - ♦ **Subnetwork Mask:** If your Source Type is Network, specify the subnetwork mask.
- 7 Click *Done* to save changes to Status and/or Action of this filter type and return to the filter configuration menu.

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.

- 8 Click *Cancel* to discard changes to Status and/or Action and return to the filter configuration menu.

10.5.4 Configuring an Outgoing RIP Filter

You can configure the outgoing RIP filters as follows:

- 1 Log in to iManager, then select *BorderManager > Legacy Filter Configuration*.
- 2 From the list, select the server where the filters are to be configured by clicking the icon, then click *OK*.

- 3 Select *Configuring Outgoing RIP Filters*, then click *Next*.

Outgoing RIP Filter Configuration

Status

Action

Select a list of filters to be configured:

This page helps you to set the properties of the selected filter type.

Status: You can either enable or disable 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: You can either deny or permit 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: You can 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.
- 4 Select Filter List or Exception List and click *Next* to configure filters in that list. The next page displays the list of routes denied or always permitted depending on whether you have selected the Filter List or Exception list respectively.

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.

- 5 Click Add to add new filters or select the filter you want to modify and click modify.

Outgoing RIP Filter Configuration

Outgoing RIP Filter Name:

Filtered Route:
Route to Network or Host:

Do Not Advertise Route To:
Destination Type:

Comment:

Logging:

Fill in the following fields:

Outgoing 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.

Destination Type: Specify the destination 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.

6 Click *Next* to configure the filter information:

Outgoing RIP Filter Configuration

Filtered Route:
Route to Network or Host: All Routes

Do Not Advertise Route To:
Destination Type: Interface
Destination Interface: All Interfaces 
Destination Circuit: -NA-

Fill in the following information:

Filtered Route: This section has the following fields:

- ♦ **Route to 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.

Do Not Advertise Route To: This section has the following fields:

- ♦ **Destination Type:** Specifies whether the destination is a Host, Interface, Interface Group, or Network.
- ♦ **Destination Interface:** If your Source Type is Interface or Interface Group, select a source location from the list of network interfaces.
- ♦ **Destination Circuit:** If the current source is of type Interface or Interface Group and is of WAN Media Type, specify the destination circuit parameters.
- ♦ **IP Address of Network:** If your destination Type is Network or Host, specify the IP address.
- ♦ **Subnetwork Mask:** If your destinationType is Network, specify the subnetwork mask.

- 7 Click *Done* to save changes to Status and/or Action of this filter type and return to the filter configuration menu.

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.

- 8 Click *Cancel* to discard changes to Status and/or Action and return to the filter configuration menu.

10.5.5 Configuring an Incoming EGP Filter

You can configure incoming RIP filters as follows:

- 1 Log in to iManager, then select *BorderManager > Legacy Filter Configuration*.
- 2 From the list, select the server where the filters are to be configured by clicking the icon, then click *OK*.
- 3 Select *Configuring Incoming EGP Filters*, then click *Next*.

The screenshot shows a dialog box titled "Incoming EGP Filter Configuration". It has three main sections: "Status" with a dropdown menu set to "Disabled"; "Action" with a dropdown menu set to "Deny Packets in Filter list"; and "Select a list of filters to be configured:" with a list box containing "Filter List" and "Exception List". At the bottom, there are three buttons: "Next >>", "Done", and "Cancel".

This page helps you to set the properties of the selected filter type.

Status: You can either enable or disable 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: You can either deny or permit 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: You can 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.
- 4 Select Filter List or Exception List and click *Next* to configure filters in that list. The next page displays the list of routes denied or always permitted depending on whether you have selected the Filter List or Exception list respectively.

If the Action is deny, then the EGP routes that match the criteria of a filter in the Filter List are not accepted by the router. All other EGP 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.
 - 5 Click Add to add new filters or select the filter you want to modify and click modify.

Incoming RIP Filter Configuration

Incoming RIP Filter Name:

Filtered Route:
 Route to Network or Host:

Accept Route From:
 Source Type:

Comment:

Logging:

Fill in the following fields:

Incoming EGP Filter Name: Specify the name of the EGP 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.

6 Click *Next* to configure the filter information:

Incoming RIP Filter Configuration

Filtered Route:

Route to Network or Host: All Routes

Accept Route From:

Source Type: Interface

Source Interface:

All Interfaces 

Source Circuit:

-NA-

<< Previous

Done

Cancel

Fill in the following information:

Filtered Route: This section has the following fields:

- ◆ **Route to 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: This section has the following fields:

- ◆ **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.
 - ♦ **IP Address of Network:** If your Source Type is Network or Host, specify the IP address.
 - ♦ **Subnetwork Mask:** If your Source Type is Network, specify the subnetwork mask.
- 7 Click *Done* to save changes to Status and/or Action of this filter type and return to the filter configuration menu.

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.

- 8 Click *Cancel* to discard changes to Status and/or Action and return to the filter configuration menu.

10.5.6 Configuring an Outgoing EGP Filter

You can configure configure incoming RIP filters as follows:

- 1 Log in to iManager, then select *BorderManager > Legacy Filter Configuration*.
- 2 From the list, select the server where the filters are to be configured by clicking the icon, then click *OK*.
- 3 Select *Configuring Outgoing EGP Filters*, then click *Next*.

Outgoing EGP Filter Configuration

Status
Disabled

Action
Deny Packets in Filter list

Select a list of filters to be configured:

Filter List
Exception List

Next >> Done Cancel

This page helps you to set the properties of the selected filter type.

Status: You can either enable or disable 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: You can either deny or permit 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: You can 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.
- 4 Select Filter List or Exception List and click *Next* to configure filters in that list. The next page displays the list of routes denied or always permitted depending on whether you have selected the Filter List or Exception list respectively.

If the Action is deny, then the EGP routes that match the criteria of a filter in the Filter List are not accepted by the router. All other EGP 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.

- 5 Click Add to add new filters or select the filter you want to modify and click modify.

Outgoing EGP Filter Configuration

Outgoing EGP Filter Name:

Filtered Route:
Route to Network or Host:

Do Not Advertise Route To:
Destination Type:

Comment:

Logging:

Fill in the following fields:

Outgoing EGP Filter Name: Specify the name of the EGP 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.

Destination 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.

6 Click *Next* to configure the filter information:

Outgoing EGP Filter Configuration

Filtered Route:

Route to Network or Host:

Do Not Advertise Route To:

Destination Type:

Destination Interface:

Destination Circuit:

Fill in the following information:

Filtered Route: This section has the following fields:

- ◆ **Route to Network/Host:** Specify a four-byte IP address in dotted decimal notation. For example: 130.57.172.0.

NOTE: When configuring EGP filters for IP networks you should be aware of the fact that depending on the network topology, EGP 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 EGP 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: This section has the following fields:

- ♦ **Destination Type:** Specifies whether the destination is a Host, Interface, Interface Group, or Network.
- ♦ **Destination Interface:** If your Destination Type is Interface or Interface Group, select a source location from the list of network interfaces.
- ♦ **Destination Circuit:** If the current source is of type Interface or Interface Group and is of WAN Media Type, specify the destination circuit parameters.
- ♦ **IP Address of Network:** If your Destination Type is Network or Host, specify the IP address.
- ♦ **Subnetwork Mask:** If your Destination Type is Network, specify the subnetwork mask.

7 Click *Done* to save changes to Status and/or Action of this filter type and return to the filter configuration menu.

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.

8 Click *Cancel* to discard changes to Status and/or Action and return to the filter configuration menu.

10.5.7 Configuring an OSPF Filter

You can configure configure incoming RIP filters as follows:

- 1 Log in to iManager, then select *BorderManager > Legacy Filter Configuration*.
- 2 From the list, select the server where the filters are to be configured by clicking the icon, then click *OK*.
- 3 Select *Configuring OSPF Filters*, then click *Next*.

Incoming RIP Filter Configuration

Status
Disabled

Action
Deny Packets in Filter list

Select a list of filters to be configured:

Filter List
Exception List

This page helps you to set the properties of the selected filter type.

Status: You can either enable or disable 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: You can either deny or permit 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: You can 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.
- 4 Select Filter List or Exception List and click *Next* to configure filters in that list. The next page displays the list of routes denied or always permitted depending on whether you have selected the Filter List or Exception list respectively.

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.

- 5 Click Add to add new filters or select the filter you want to modify and click modify.

Incoming RIP Filter Configuration

Incoming RIP Filter Name:

Filtered Route:

Route to Network or Host:

Accept Route From:

Source Type:

Comment:

Logging:

Next >>

Cancel

Fill in the following fields:

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.

6 Click *Next* to configure the filter information:

Incoming RIP Filter Configuration


Filtered Route:

Route to Network or Host: All Routes

Accept Route From:

Source Type: Interface

Source Interface:

All Interfaces 

Source Circuit:

-NA-

<< Previous

Done

Cancel

Fill in the following information:

Filtered Route: This section has the following fields:

- ◆ **Route to 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: This section has the following fields:

- ♦ **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.
- 7 Click *Done* to save changes to Status and/or Action of this filter type and return to the filter configuration menu.

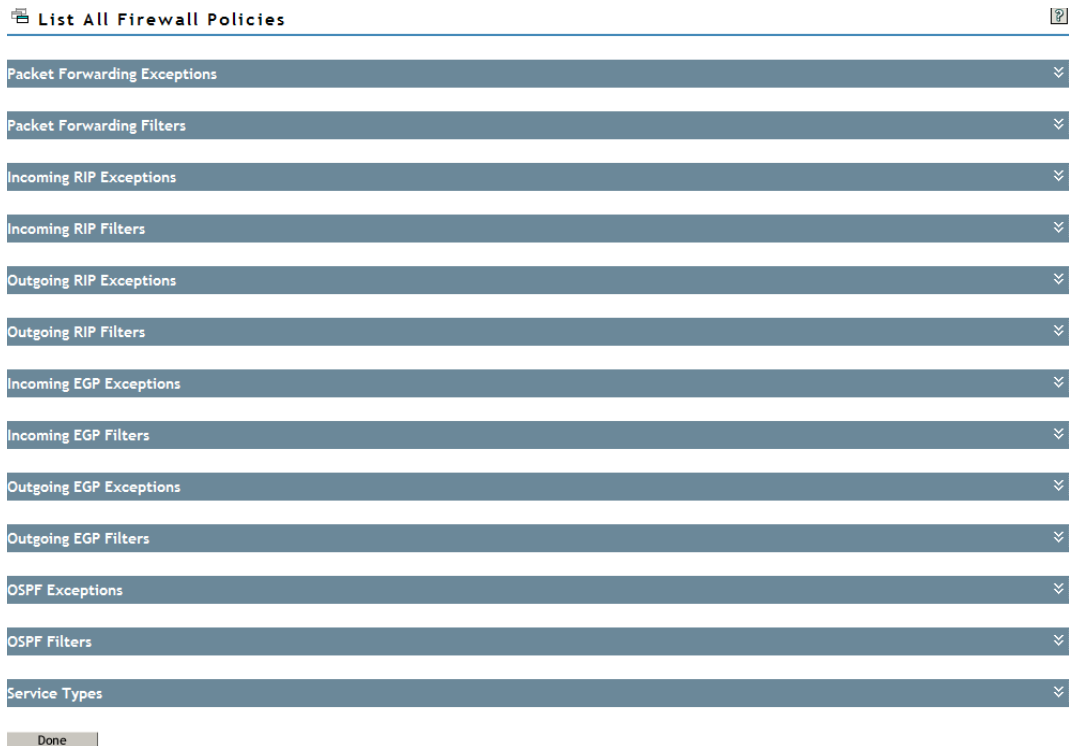
After you save the changes, TCP/IP dynamically updates to the new configuration. The action taken on routes matching filters in this list is described in the Action field. You can select the Route and Source parameters from the list of defined values.

- 8 Click *Cancel* to discard changes to Status and/or Action and return to the filter configuration menu.

10.6 List All Firewall Policies

- 1 Log in to iManager, then select *BorderManager > List All Firewall Policies*.
- 2 From the list, select the server where the filters are to be configured by clicking the icon and then click *OK*.

The following page is displayed listing all the firewall policies:



- 3 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 123](#).

10.7 Troubleshooting: Possible Installation Scenarios

This section contains the following troubleshooting information:

- ♦ [Section 10.7.1, “The Off Server Service Fields Appear Disabled,” on page 142](#)
- ♦ [Section 10.7.2, “Roles and Tasks Do Not Appear on the Left Pane,” on page 143](#)

10.7.1 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
```

10.7.2 Roles and Tasks Do Not Appear on the Left Pane

Refresh the page or log in again.

Managing IP Packet Filters

11

The following sections describe how to manage Novell® BorderManager® 3.9 IP packet filters used as part of your firewall. Refer to [Table 11-1 on page 145](#) for the logging configuration parameters in `ippktlog.cfg`.

- ♦ [Section 11.1, “Modifying Default IP Logging Parameters,” on page 145](#)
- ♦ [Section 11.2, “Viewing IP Packet Log Information,” on page 146](#)

11.1 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 11-1 *ippktlog.cfg* Configuration Parameters

Parameter	Default Value	Available Settings
<code>LOG_FILE_TYPE</code>	1	1 = Sequential log file.
<code>LOG_FILE_LOCATION</code>	<code>sys:\etc\logs\ippktlog</code>	Any directory.
<code>LOG_FILE_ROLL_METHOD</code>	3	1 = Roll log file every <i>n</i> hours, where <i>n</i> is the value assigned to <code>LOG_FILE_ROLL_METHOD_VALUE</code> . 2 = Roll log file every <i>n</i> days, where <i>n</i> is the value assigned to <code>LOG_FILE_ROLL_METHOD_VALUE</code> . 3 = Roll log file when the log file size exceeds <i>n</i> KB, where <i>n</i> is the value assigned to <code>LOG_FILE_ROLL_METHOD_VALUE</code> .
<code>LOG_FILE_ROLL_METHOD_VALUE</code>	100	Any value representing hours when <code>LOG_FILE_ROLL_METHOD</code> is 1. Any value representing days when <code>LOG_FILE_ROLL_METHOD</code> is 2. Any value representing KB when <code>LOG_FILE_ROLL_METHOD</code> 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 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 the following command:

```
SET SHUTDOWN PUBLIC INTERFACE ON LOG FAILURE = OFF
```

To re-enable the automatic shutdown of the public interface, enter the following command:

```
SET SHUTDOWN PUBLIC INTERFACE ON LOG FAILURE = ON
```

11.2 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.

Backing Up and Restoring Filters

12

Novell® BorderManager® 3.9 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 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.

- ♦ [Section 12.1, “Backing Up eDirectory Filters to LDIF,” on page 149](#)
- ♦ [Section 12.2, “Restoring Filters to eDirectory from LDIF,” on page 149](#)
- ♦ [Section 12.3, “Backing Up eDirectory Filters to Text Files,” on page 150](#)
- ♦ [Section 12.4, “Restoring Filters to eDirectory from Text Files,” on page 150](#)

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.

12.1 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*.

12.2 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`.

12.3 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`.

12.4 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`.

Advanced Configuration of IP Packet Filters Using FILTCFG

13

The following sections describe how to configure exceptions using FILTCFG to allow specific IP services through the Novell® BorderManager® 3.9 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.

- ◆ [Section 13.1, “Choosing between Stateful or Static Packet Filters,” on page 151](#)
- ◆ [Section 13.2, “Setting Up an HTTP Filter,” on page 151](#)
- ◆ [Section 13.3, “Setting Up an FTP Filter,” on page 153](#)
- ◆ [Section 13.4, “Setting Up a Telnet Filter,” on page 154](#)
- ◆ [Section 13.5, “Setting Up an SMTP Filter,” on page 156](#)
- ◆ [Section 13.6, “Setting Up a POP3 Filter,” on page 157](#)
- ◆ [Section 13.7, “Setting Up a DNS Filter,” on page 157](#)
- ◆ [Section 13.8, “Setting Up VPN Filters,” on page 158](#)
- ◆ [Section 13.9, “Filtering IP Packets that Use the IP Header Options Field,” on page 158](#)

13.1 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.

13.2 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 151](#)
- ◆ [“Setting Up Static Filters for HTTP” on page 152](#)

13.2.1 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.

13.2.2 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.

13.3 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 153](#)
- ♦ [“Setting Up Static Filters for FTP” on page 154](#)

13.3.1 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.

13.3.2 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.

13.4 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 155](#)
- ♦ [“Setting Up Static Filters for Telnet” on page 155](#)

13.4.1 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.

13.4.2 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.

13.5 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 firewall.

This section contains the following topics:

- ♦ “Setting Up a Stateful SMTP Filter” on page 156
- ♦ “Setting Up Static Filters for SMTP” on page 156

13.5.1 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.

13.5.2 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.

13.6 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 157](#)
- ♦ [“Setting Up a Static POP3 Filter” on page 157](#)

IMPORTANT: These filters do not forward requests for domain name resolution by a DNS server in your private network. A DNS filter is required.

13.6.1 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.

13.6.2 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.

13.7 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 158](#)
- ♦ [“Setting Up Static Filters for DNS” on page 158](#)

13.7.1 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 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.

13.7.2 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*

13.8 Setting Up VPN Filters

To set filter exceptions to allow VPN traffic refer to [“Setting Up VPN Filters” on page 192](#).

13.9 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 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.

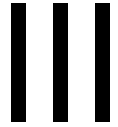
To disable the filtering of packets that use IP header options from the server console, enter

```
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
```


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 3.9 integrates with Novell eDirectory™ and gives remote and mobile employees a secure access to the required resources. This means that users can enjoy direct and secure access to all the services such as file, print, and email applications from wherever they are working.

Novell BorderManager 3.9 supports open standards and authenticates the users with any fully compliant Lightweight Directory Access Protocol (LDAP) directory or Novell eDirectory. Novell BorderManager 3.9 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.

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 3.9 can interoperate with third-party servers using standard based protocols such as IKE and IPsec.

The following sections provide information on how to set up and use VPN. This is an iManager-based configuration.

- ◆ [Chapter 15, “Certificate-Based Authentication,” on page 171](#) provides information on the prerequisites for setting up the new VPN services.
- ◆ [Chapter 16, “Configuring VPN Services,” on page 185](#) describes how to set up the VPN services and use Novell iManager to configure and use policies on the VPN Server.
- ◆ [Chapter 17, “Upgrading Virtual Private Networks,” on page 215](#) provides basic information on how to upgrade to the new VPN.
- ◆ [Chapter 18, “Monitoring Virtual Private Networks,” on page 219](#) describes how to monitor the VPN services through the NetWare Remote Manager framework.
- ◆ [Chapter 19, “Virtual Private Network Client,” on page 229](#) describes the basic functionality of the VPN client and the procedure to install it. The VPN client is released along with Novell BorderManager 3.9.

Pre-Shared Key Support

14

This release of Novell BorderManager introduces a mode of configuring a VPN tunnel between two Site-to-Site members with ease. This is the Pre-Shared Key mode of authentication.

The Pre-Shared Key (PSK) establishes a VPN tunnel between two Site-to-Site (S2S) members. In the PSK authentication method, a common secret or a pre-shared key is configured on both the servers. The VPN server uses this key secret to establish the tunnel. This method is the simplest way of configuring a Site-to-Site connection.

For explanation on configuring and modifying the pre-shared key mode of authentication on master and slave, refer to [Chapter 16, “Configuring VPN Services,” on page 185](#).

14.1 PSK Use Cases and Error Messages

Following is a list of PSK use cases and error messages in a site-to-site pre-shared key mode of authentication setup.

Table 14-1 PSK Use Cases and Error Messages

<input checked="" type="checkbox"/> PSK	<input checked="" type="checkbox"/> PSK
Auth method – PSK	Auth method – PSK
Master	Slave
Message : In ike logs	Message : In ike logs
Initiator : Pre-shared key is not configured.	Initiator : Pre-shared key is not configured.
Responder : NA	Responder : NA
<input checked="" type="checkbox"/> PSK	<input checked="" type="checkbox"/> PSK
Auth method – PSK	Auth method – PSK
Master	Slave
Message : In ike logs	Message : In ike logs
Initiator : Pre-shared key is not configured.	Initiator : Pre-shared key is not configured in peer x.x.x.x.
Responder : NA	Responder : NA

<input checked="" type="checkbox"/> PSK	<input checked="" type="checkbox"/> PSK
psk = secret	psk = different-secret
Auth method – PSK	Auth method – PSK
Master	Slave
Message : In csaudit logs	Message : In csaudit logs
Initiator : Pre-shared key mismatch for peer x.x.x.x	Initiator : Pre-shared key mismatch for peer x.x.x.x
Responder : Pre-shared key mismatch for peer x.x.x.x	Responder : Pre-shared key mismatch for peer x.x.x.x
<input checked="" type="checkbox"/> PSK	<input checked="" type="checkbox"/> PSK
psk = secret1	psk = secret1
Pre-shared keys are matching.	Auth method – PSK
Auth method – PSK	Slave
Master	Message : In csaudit logs
Message : In csaudit logs	Initiator : IKE SA established to x.x.x.x
Initiator : IKE SA established to x.x.x.x	Responder : IKE SA established to x.x.x.x
Responder :IKE SA established to x.x.x.x	
<input checked="" type="checkbox"/> PSK	<input checked="" type="checkbox"/> PSK
psk = secret1	psk = secret1
Auth method – Certificate	Auth method – Certificate
Certificate configuration is proper	Slave
Master	Message : In csaudit logs
Message : In csaudit logs	Initiator : IKE SA established to x.x.x.x
Initiator : IKE SA established to x.x.x.x	Responder : IKE SA established to x.x.x.x
Responder :IKE SA established to x.x.x.x	

14.2 Use Case Scenarios of Novell BorderManager 3.8 Master and Slaves

The following list considers scenarios of Novell BorderManager 3.8 master with two Novell BorderManager 3.8 slaves.

In the following scenario, alphabet M denotes master and S1 and S2 denote slaves.

Table 14-2 *Upgrading Only The Master From Novell BorderManager 3.8 To Novell BorderManager 3.9*

<input checked="" type="checkbox"/> Certificate	<input checked="" type="checkbox"/> Certificate
Auth method – Certificate	Auth method – Certificate
Master(3.9)	Slave S1(3.8)
Message : In csaudit logs	Message : In csaudit logs
Initiator : IKE SA established to x.x.x.x	Initiator : IKE SA established to x.x.x.x
Responder :IKE SA established to x.x.x.x	Responder : IKE SA established to x.x.x.x
<input checked="" type="checkbox"/> Certificate	<input checked="" type="checkbox"/> Certificate
Auth method – Certificate	Auth method – Certificate
Master(3.9)	Slave S2(3.8)
Message : In csaudit logs	Message : In csaudit logs
Initiator : IKE SA established to x.x.x.x	Initiator : IKE SA established to x.x.x.x
Responder :IKE SA established to x.x.x.x	Responder : IKE SA established to x.x.x.x
<input checked="" type="checkbox"/> Certificate	<input checked="" type="checkbox"/> Certificate
Auth method – PSK	Auth method – Certificate
Certificate Not configured properly	Slave S1/Slave S2(3.8)
Master(3.9)	Message : In csaudit logs
Message : In csaudit logs	Not supported
Not supported	
<input checked="" type="checkbox"/> Certificate	<input checked="" type="checkbox"/> Certificate
Auth method – Certificate	Auth method – Certificate
Slave S1(3.8)	Slave S2(3.8)
Message : In csaudit logs	Message : In csaudit logs
Initiator : IKE SA established to x.x.x.x	Initiator : IKE SA established to x.x.x.x
Responder :IKE SA established to x.x.x.x	Responder : IKE SA established to x.x.x.x

14.3 Use Case Scenarios in Mixed Environment

This section lists the scenarios of a mixed environment with a Novell BorderManager 3.9 master and slave (S1) and another slave (S2) in Novell BorderManager 3.8 environment.

Table 14-3 *Mixed Environment*

<p><input checked="" type="checkbox"/>Certificate</p> <p>Auth method – CertificateMaster(3.9)</p> <p>Message : In csaudit logs</p> <p>Initiator : IKE SA established to x.x.x.x</p> <p>Responder :IKE SA established to x.x.x.x</p>	<p><input checked="" type="checkbox"/>Certificate</p> <p>Auth method – Certificate</p> <p>Slave S1(3.9)</p> <p>Message : In csaudit logs</p> <p>Initiator : IKE SA established to x.x.x.x</p> <p>Responder : IKE SA established to x.x.x.x</p>
<p><input checked="" type="checkbox"/>PSK</p> <p>Auth method – PSK</p> <p>Master(3.9)</p> <p>Message : In csaudit logs</p> <p>Initiator : “Pre-shared key not configured for the peer x.x.x.X”</p> <p>Responder: NA</p>	<p><input checked="" type="checkbox"/>Certificate</p> <p>Auth method – Certificate</p> <p>PSK is not configured</p> <p>Slave S1(3.9)</p> <p>Message : In csaudit logs</p> <p>Initiator : “Pre-shared key is not configured”</p> <p>Responder :NA</p>
<p><input checked="" type="checkbox"/>Certificate</p> <p>Auth method – Certificate</p> <p>PSK is also configured</p> <p>Master(3.9)</p> <p>Message : In csaudit logs</p> <p>Initiator : IKE SA established to x.x.x.x</p> <p>Responder : IKE SA established to x.x.x.x</p>	<p><input checked="" type="checkbox"/>PSK</p> <p>Auth method – PSK</p> <p>Slave S1(3.9)</p> <p>Message : In csaudit logs</p> <p>Initiator : IKE SA established to x.x.x.x</p> <p>Responder : IKE SA established to x.x.x.x</p>
<p><input checked="" type="checkbox"/>PSK</p> <p>psk = secret</p> <p>Auth method – PSK</p> <p>Master(3.9)</p> <p>Message : In csaudit logs</p> <p>Initiator : Pre-shared key mismatch in peer</p> <p>Responder : Pre-shared key mismatch for peer x.x.x.X</p>	<p><input checked="" type="checkbox"/>PSK</p> <p>psk = secret1</p> <p>Auth method – PSK</p> <p>Slave S1(3.9)</p> <p>Preshared key configured is incorrect</p> <p>Message : In csaudit logs</p> <p>Initiator : Pre-shared key mismatch in peer</p> <p>Responder : Pre-shared key mismatch for peer x.x.x.X</p>

<input checked="" type="checkbox"/> Certificate	<input checked="" type="checkbox"/> Certificate
Auth method – Certificate	Auth method – Certificate
PSK is also configured	Slave S2(3.8)
Slave S1(3.9)	Message : In csaudit logs
Message : In csaudit logs	Initiator : IKE SA established to x.x.x.x
Initiator : IKE SA established to x.x.x.x	Responder : IKE SA established to x.x.x.x
Responder : IKE SA established to x.x.x.x	
<input checked="" type="checkbox"/> Certificate	<input checked="" type="checkbox"/> Certificate
Auth method – Certificate	Auth method – Certificate
PSK is not configured	Slave S2(3.8)
Slave S1(3.9)	Message : In csaudit logs
Message : In csaudit logs	Initiator : IKE SA established to x.x.x.x
Initiator : IKE SA established to x.x.x.x	Responder : IKE SA established to x.x.x.x
Responder : IKE SA established to x.x.x.x	

14.4 Communication Between Two Novell BorderManager 3.9 Slaves

PSK always takes precedence over certificate mode of authentication when two slaves are initiating connection between themselves.

This section gives the scenarios where Slave S1 and Slave S2 are communicating with each other:

Table 14-4 *Communication Between Two Novell BorderManager 3.9 Slaves*

<input checked="" type="checkbox"/> Certificate	<input checked="" type="checkbox"/> Certificate
Auth method – Certificate	Auth method – Certificate
Slave S1(3.9)	Slave S2(3.9)
Message : In csaudit logs	Message : In csaudit logs
Initiator : IKE SA established to x.x.x.x	Initiator : IKE SA established to x.x.x.x
Responder :IKE SA established to x.x.x.x	Responder : IKE SA established to x.x.x.x

<input checked="" type="checkbox"/> PSK Auth method – PSK Certificate is also configured Slave S1(3.9) Message : In csaudit logs Initiator : IKE SA established to x.x.x.x Responder :IKE SA established to x.x.x.x	<input checked="" type="checkbox"/> Certificate Auth method – Certificate Slave S2(3.9) Message : In csaudit logs Initiator : IKE SA established to x.x.x.x Responder :IKE SA established to x.x.x.x
<input checked="" type="checkbox"/> PSK Auth method – PSK psk = secret Certificate is also configured. Slave S1(3.9) Message : In csaudit logs Initiator : IKE SA established to x.x.x.x Responder : IKE SA established to x.x.x.x	<input checked="" type="checkbox"/> PSK Auth method – PSK psk = secret Slave S2(3.9) Message : In csaudit logs Initiator : IKE SA established to x.x.x.x Responder : IKE SA established to x.x.x.x
<input checked="" type="checkbox"/> Certificate Auth method – Certificate psk = secret PSK is also configured Slave S1(3.9) Message : In csaudit logs Initiator : IKE SA established to x.x.x.x Responder : IKE SA established to x.x.x.x	<input checked="" type="checkbox"/> PSK Auth method – PSK psk = secret Slave S2(3.9) Message : In csaudit logs Initiator : IKE SA established to x.x.x.x Responder : IKE SA established to x.x.x.x
<input checked="" type="checkbox"/> Certificate Auth method – Certificate psk = secret PSK is also configured Slave S1(3.9) Message : In csaudit logs Initiator : Pre-shared key mismatch in peer Responder : Pre-shared key mismatch for peer x.x.x.x	<input checked="" type="checkbox"/> PSK Auth method – PSK psk = secret1 Slave S2(3.9) Message : In csaudit logs Initiator : Pre-shared key mismatch in peer Responder : Pre-shared key mismatch for peer x.x.x.x

<input checked="" type="checkbox"/> Certificate Auth method – Certificate PSK is not configured Slave S1(3.9) Message : In csaudit logs Initiator : Preshared key not configured Responder : NA	<input checked="" type="checkbox"/> PSK Auth method – PSK Slave S2(3.9) Message : In csaudit logs Initiator : Preshared key not configured in peer Responder : NA
<input checked="" type="checkbox"/> PSK Auth method – PSK Certificate is also configured. Slave S1(3.9) Message : In csaudit logs Initiator : Preshared key not configured in peer Responder : NA	<input checked="" type="checkbox"/> Certificate Auth method – Certificate PSK is not configured Slave S2(3.9) Message : In csaudit logs Initiator : Preshared key not configured Responder : NA
<input checked="" type="checkbox"/> PSK Auth method – PSK psk = secret Certificate is also configured Slave S1(3.9) Message : In csaudit logs Initiator : Preshared key not configured in peer Responder : Pre-shared key mismatch for peer x.x.x.x	<input checked="" type="checkbox"/> Certificate Auth method – Certificate psk = secret1 PSK is configured with wrong secret Slave S2(3.9) Message : In csaudit logs Initiator : Preshared key not configured in peer Responder : Pre-shared key mismatch for peer x.x.x.x

Novell BorderManager 3.9 VPN services are significantly different from the VPN services of all earlier versions of the software. The VPN services are enabled for iManager 2.6. 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 in to 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 [Section 15.1, “Automated Creation of eDirectory Certificates or Objects,” on page 172](#) 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

- ◆ [Section 15.1, “Automated Creation of eDirectory Certificates or Objects,” on page 172](#)
- ◆ [Section 15.2, “Creating Server Certificates,” on page 172](#)
- ◆ [Section 15.3, “Exporting Root Certificates from the Server Certificate,” on page 178](#)
- ◆ [Section 15.4, “Creating Trusted Root Containers,” on page 179](#)
- ◆ [Section 15.5, “Creating the Trusted Root Object,” on page 180](#)
- ◆ [Section 15.6, “Creating a User Certificate,” on page 180](#)
- ◆ [Section 15.7, “Exporting User Certificates,” on page 182](#)
- ◆ [Section 15.8, “Third-Party Certificate Server,” on page 183](#)

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: It is recommended that you use iManager on a different server that on which the site-to-site VPN services are running.

15.1 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 [Section 15.2, “Creating Server Certificates,” on page 172](#) and [Section 15.4, “Creating Trusted Root Containers,” on page 179](#). After creating the Server Certificate and the Trusted Root Container, export the Trusted Root from the server certificate using steps in [Section 15.3, “Exporting Root Certificates from the Server Certificate,” on page 178](#), and create a Trusted Root object in the Trusted Root container using the steps in [Section 15.5, “Creating the Trusted Root Object,” on page 180](#).

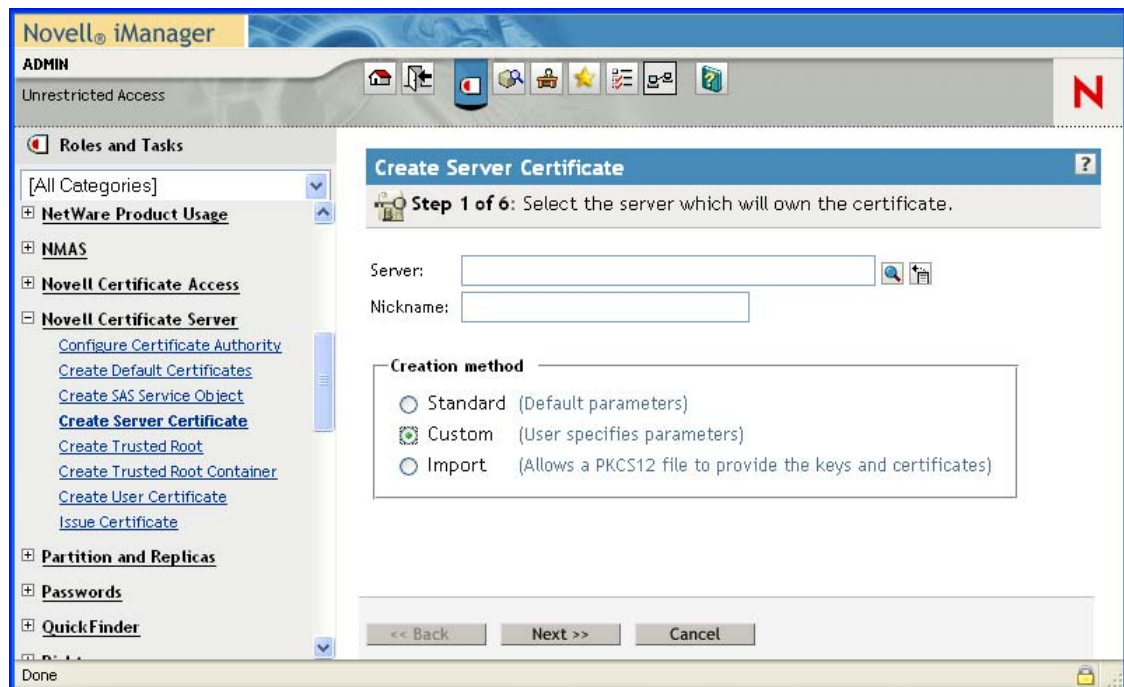
15.2 Creating Server Certificates


- 1 Log in to iManager. On a Windows XP or 2000 machine connected to a NetWare® 6.5 server, open either the Internet Explorer or Mozilla Firefox browser and go to (<https://ipaddress/nps/iManager.html>), where *ip address* is the IP address of a NetWare 6.5 server running Novell BorderManager 3.9.

NOTE: You can run iManager from a NetWare server to configure other Novell BorderManager 3.9 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 15-1 Server Certification Creation



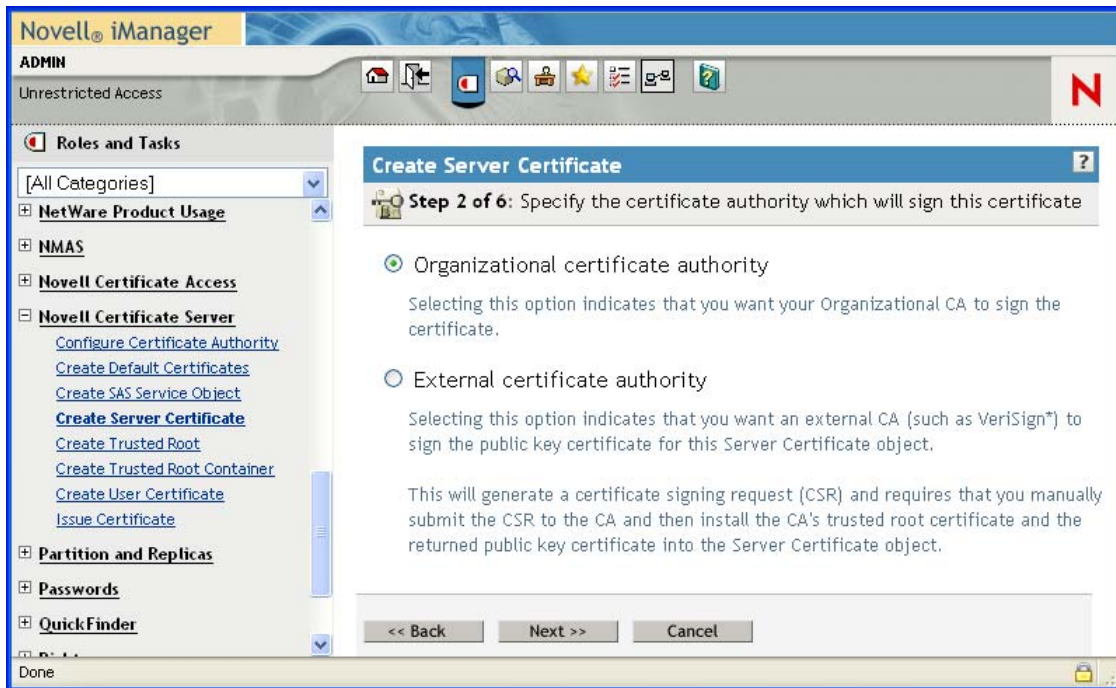
- 4 Specify the *Server* and the *Nickname* for the certificate, or click  to select the server object. Select the *Custom* check box and specify the details of the certificate, then click *Next*.

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.

It is recommended that you use the *Custom* option. If you use the *Standard* option, although client-to-site services will work, there might be some problems with site-to-site services.

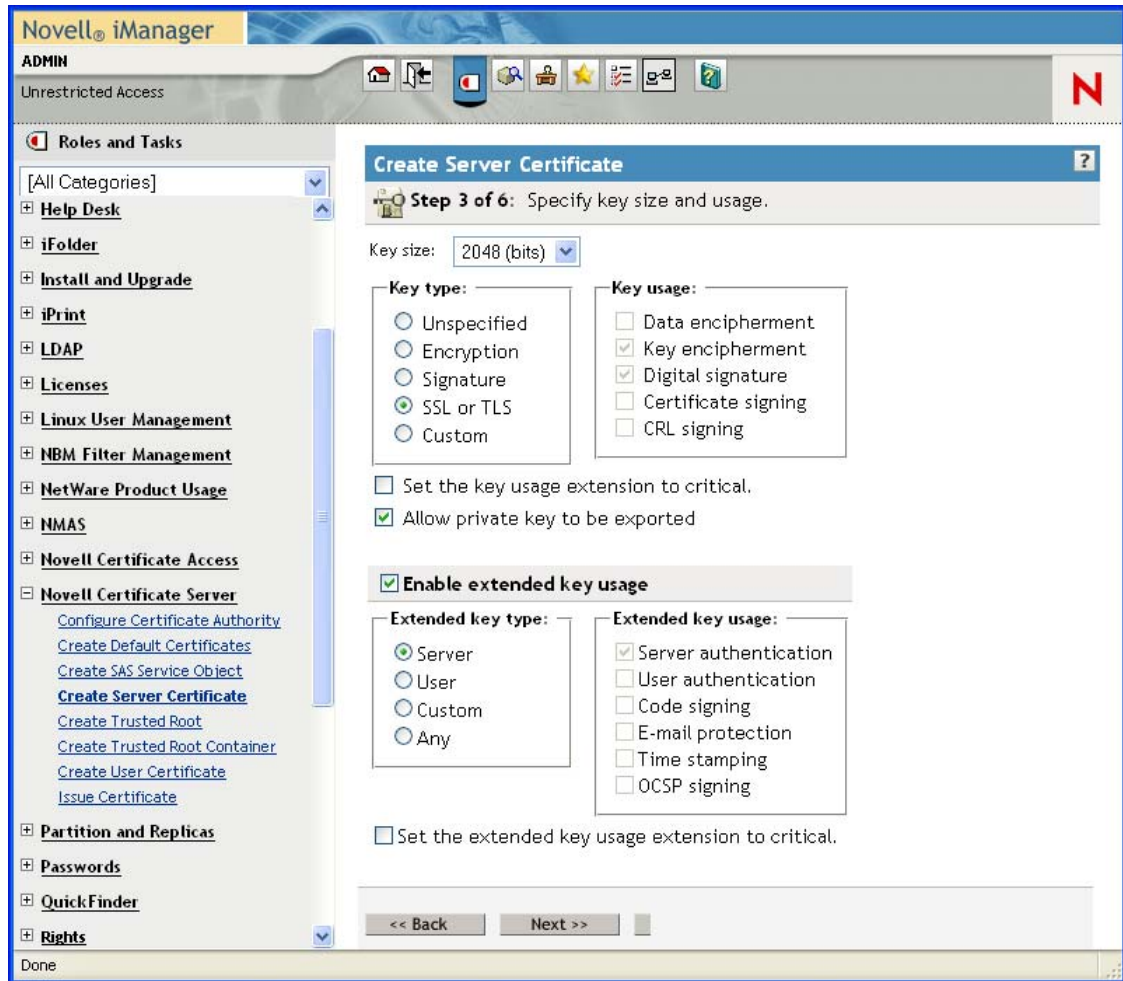
- 5 Select *Organizational Certificate Authority*, then click *Next*.

Figure 15-2 Certificate Authority



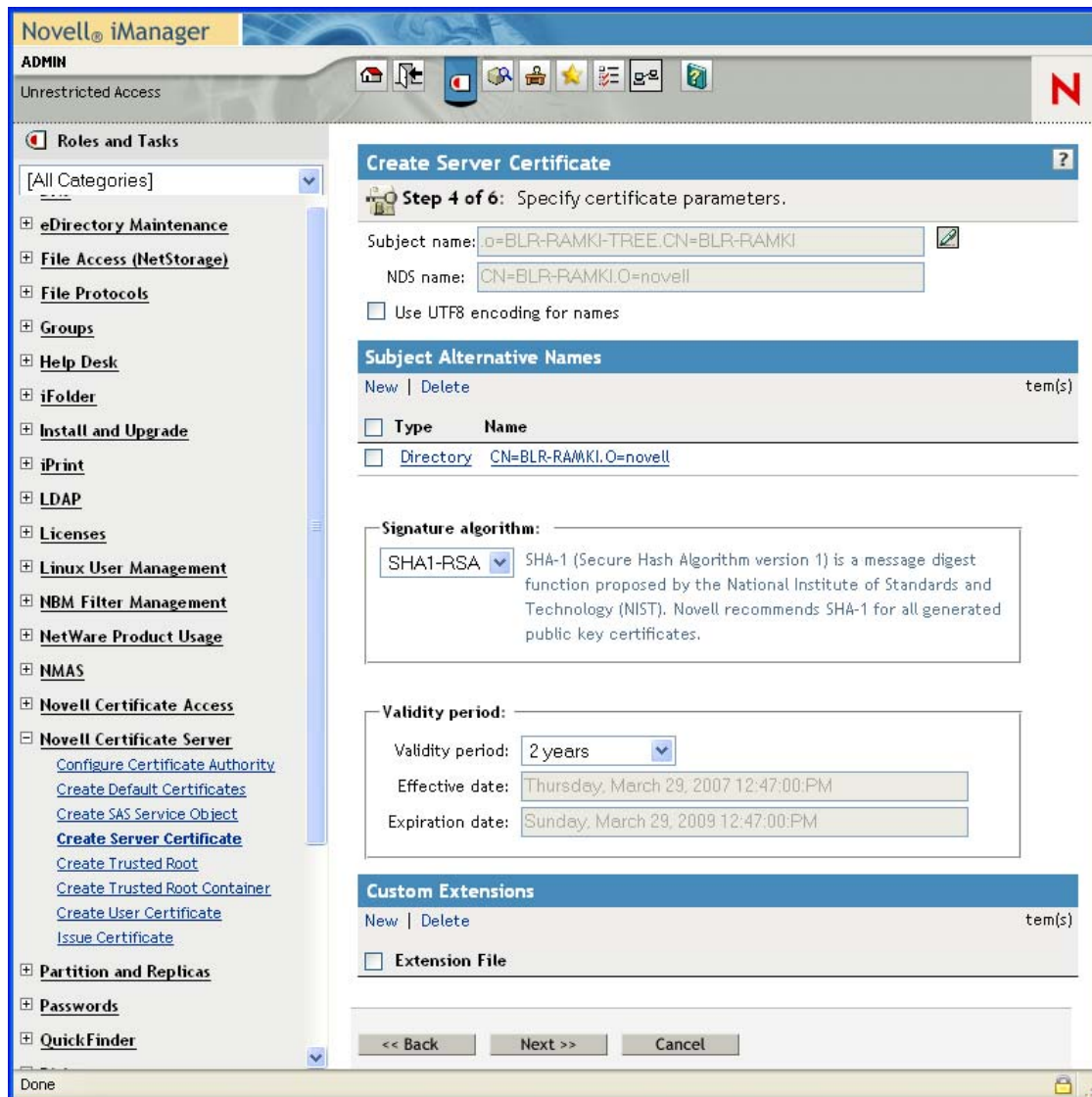
6 Specify the *Key size* and *usage*, then click *Next*.

Figure 15-3 Key Size and Usage



7 Specify the parameters of the certificate, then click *Next*.

Figure 15-4 Certificate Parameters

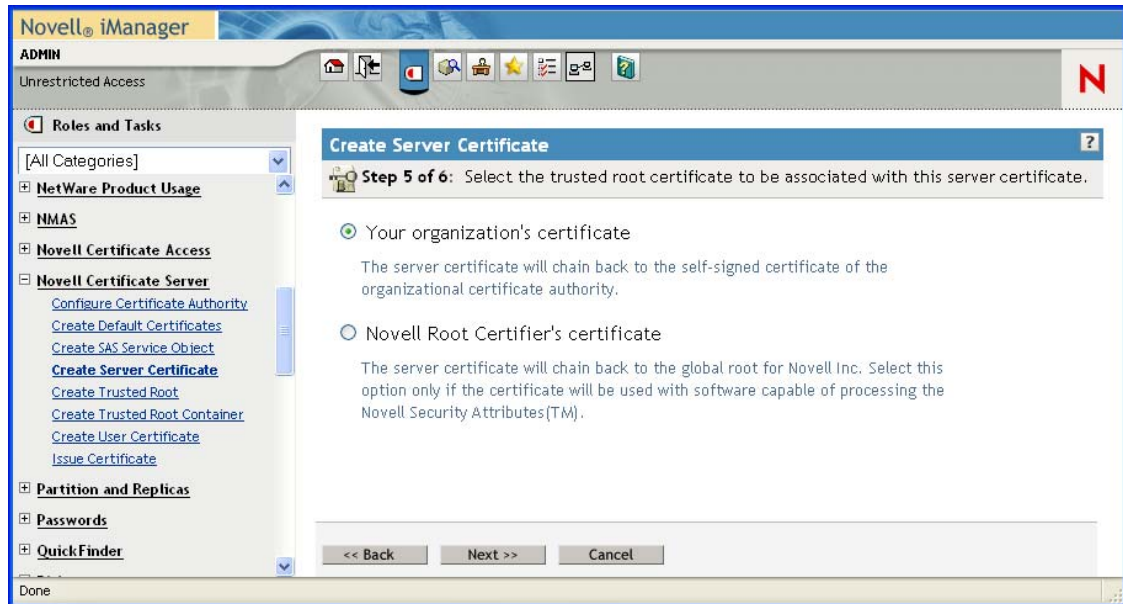


NOTE: The advantage of providing the exact time for the validity of the certificate is that, if there is a timing issue with the server the entry will not be invalid.

Entering the exact time for validity has the advantage that if there is a timing issue with the server the entry will not be invalid.

- 8 Select the relevant text box to specify the trusted root for the certificate, then click *Next*.

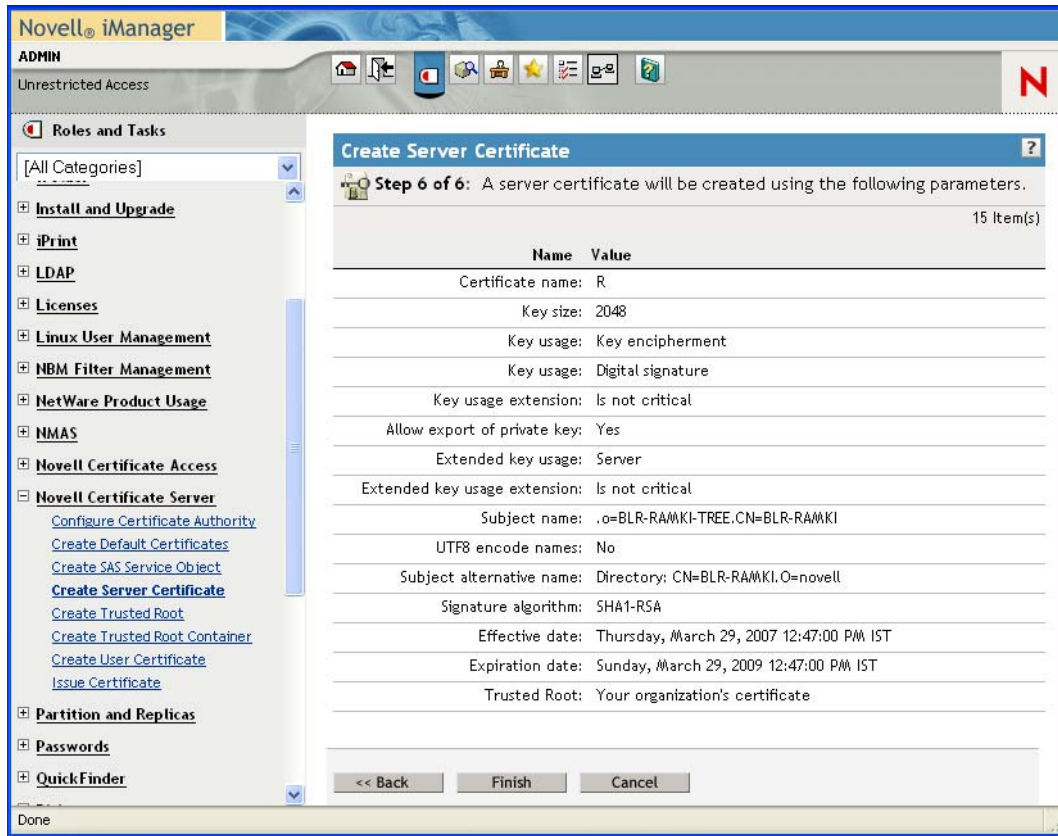
Figure 15-5 *Trusted Root*



- 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 the required changes.

After the certificate is successfully created, you get a Success message.

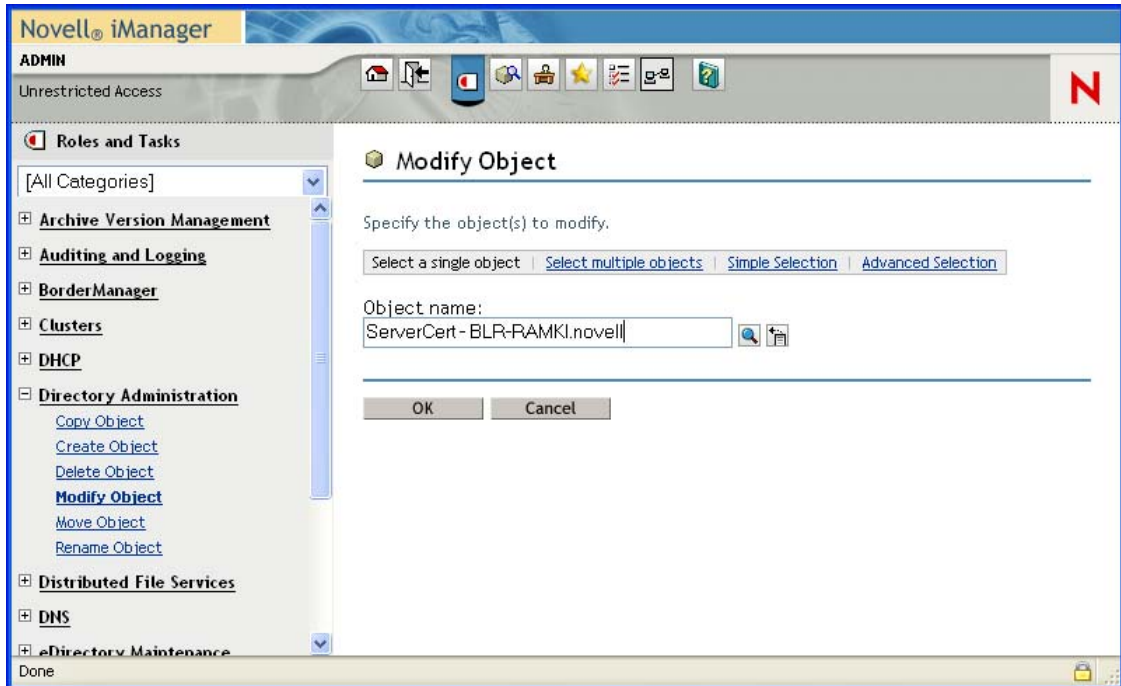
Figure 15-6 Sever Certificate Completion



15.3 Exporting Root Certificates from the Server Certificate

- 1 Under *Directory Administration*, Click *Modify Object*.

Figure 15-7 *Modify Object*



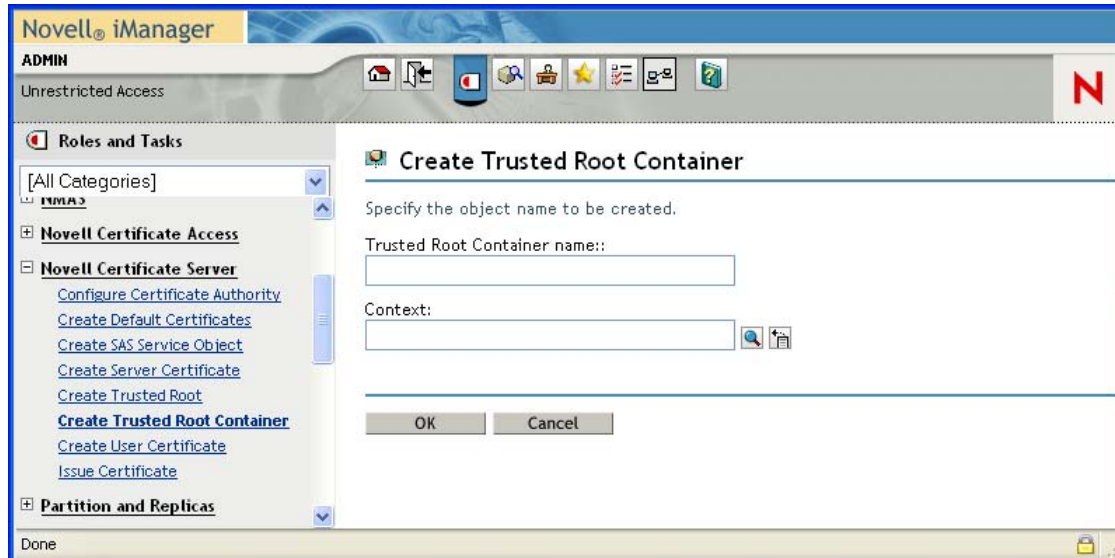
- 2 Select *Select a single object*, then specify the name of the object. This object is the server certificate itself.
- 3 Click *OK*.
- 4 Click *Certificates*, then click the link of the certificate to view the details of the certificate. Click *Close* to close this screen and return to the previous page.
- 5 To export the certificate, select the certificate and click *Export*.
- 6 Click *Next*. This page displays a message indicating that the export was successful. You are then prompted to save the certificate.


If you choose to save the certificate, you are prompted to save it on the local machine.

15.4 Creating Trusted Root Containers

- 1 Click *Create Trusted Root Containers* under *Novell Certificate Server*.

Figure 15-8 Create Trusted Root Container

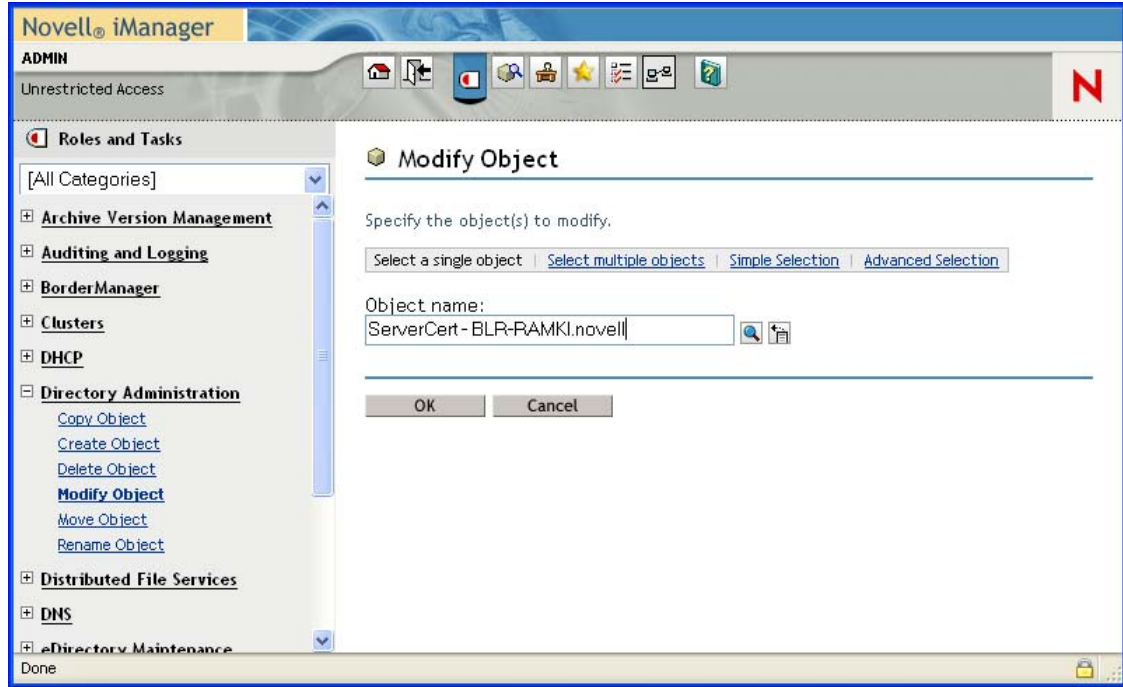


- 2 Specify the *Trusted Root Container* name and *Context*, then click *OK*. Alternatively, click  icon to set the context. In the next page, you can create new containers or modify the existing containers.

15.5 Creating the Trusted Root Object

- 1 Click *Modify Object* under *Directory Administration*. Select the Server Certificate.

Figure 15-9 *Modify Object*



- 2 Specify the certificate name, the container, and the complete location of the file you exported in [Section 15.3, “Exporting Root Certificates from the Server Certificate,”](#) on page 178 then, click *OK*.

The next page shows the successful creation of the certificate.

15.6 Creating a User Certificate

IMPORTANT: Before you commence, ensure that you have administrative or equivalent rights for creating user certificates.

- 1 Click *Create User Certificate* under *Novell Certificate Server*.


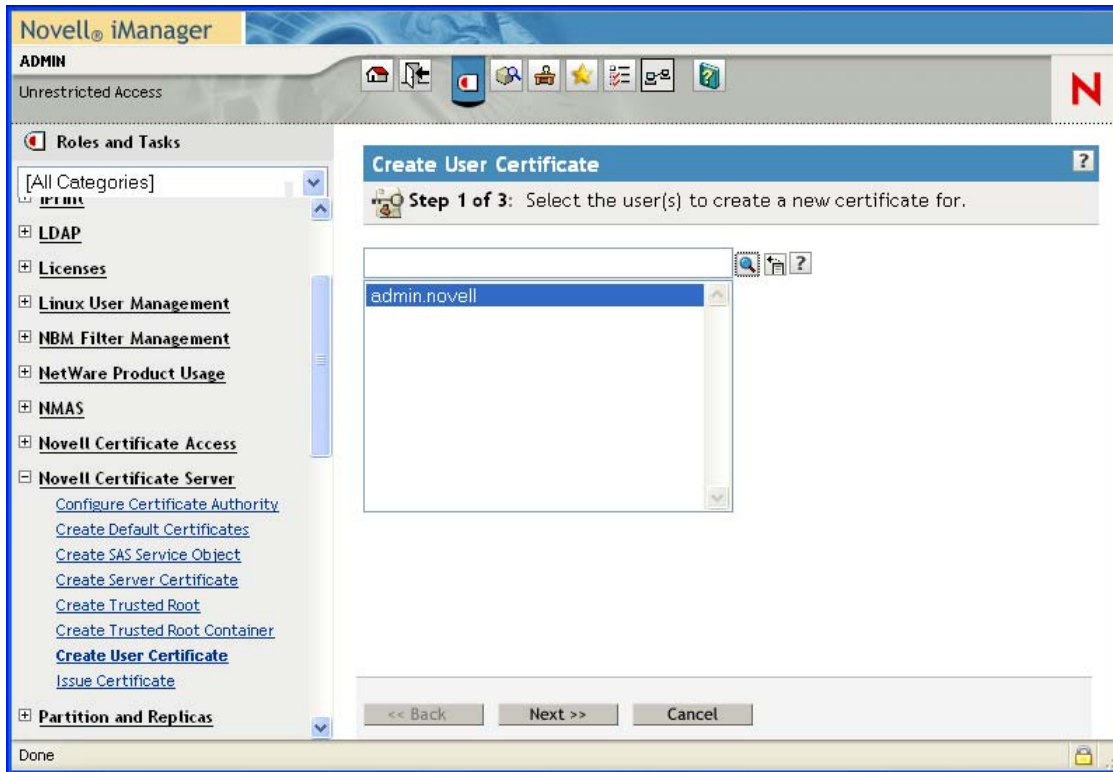
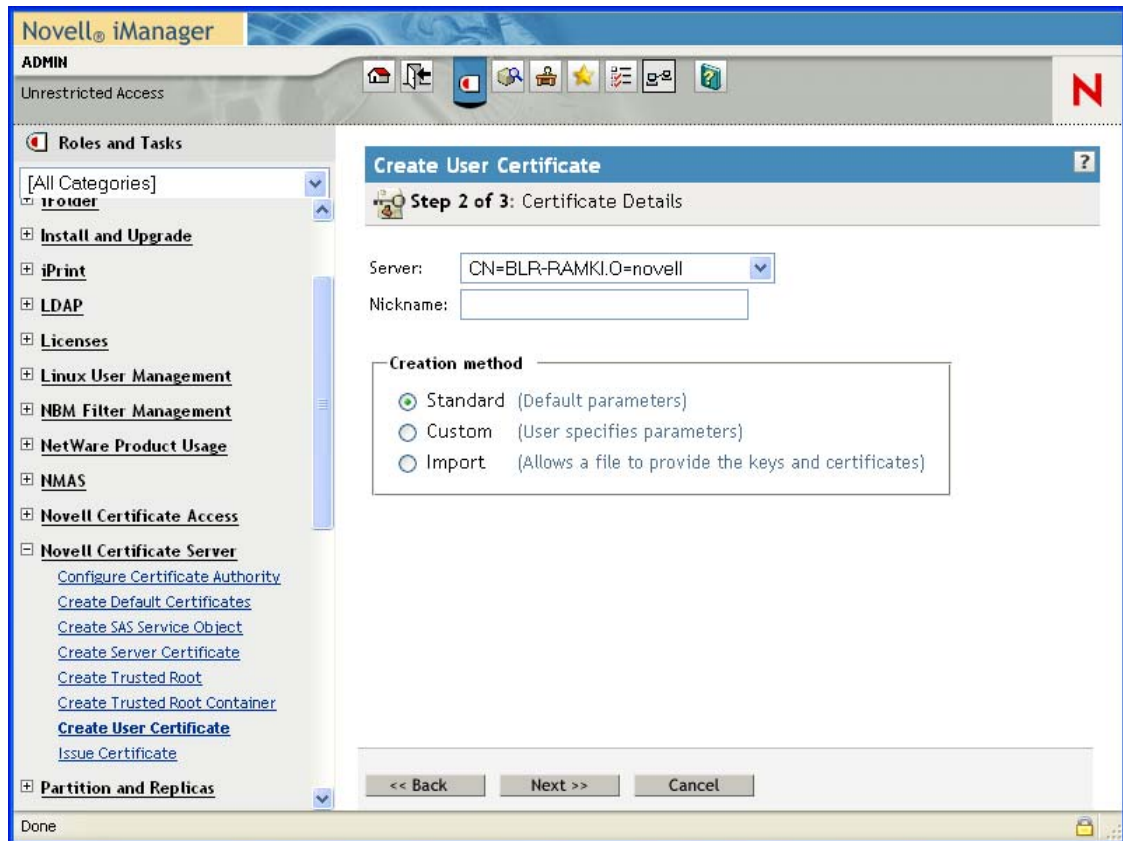
2 Click  icon to locate the user for whom you are creating the certificate. Click *Next*.

Figure 15-10 Create User Certificate Wizard



- 3 Specify the name of the *Server* and the *Nickname* for the certificate. Select the relevant *Creation method*.

Figure 15-11 Certificate Details



- 4 Click *Next*.
- 5 The summary page shows you the parameters of the certificate you are about to create. To modify the information displayed here, click *Back* and modify the details as necessary. Click *Finish* to create the certificate.

The user certificate will be created and you see a Success message.

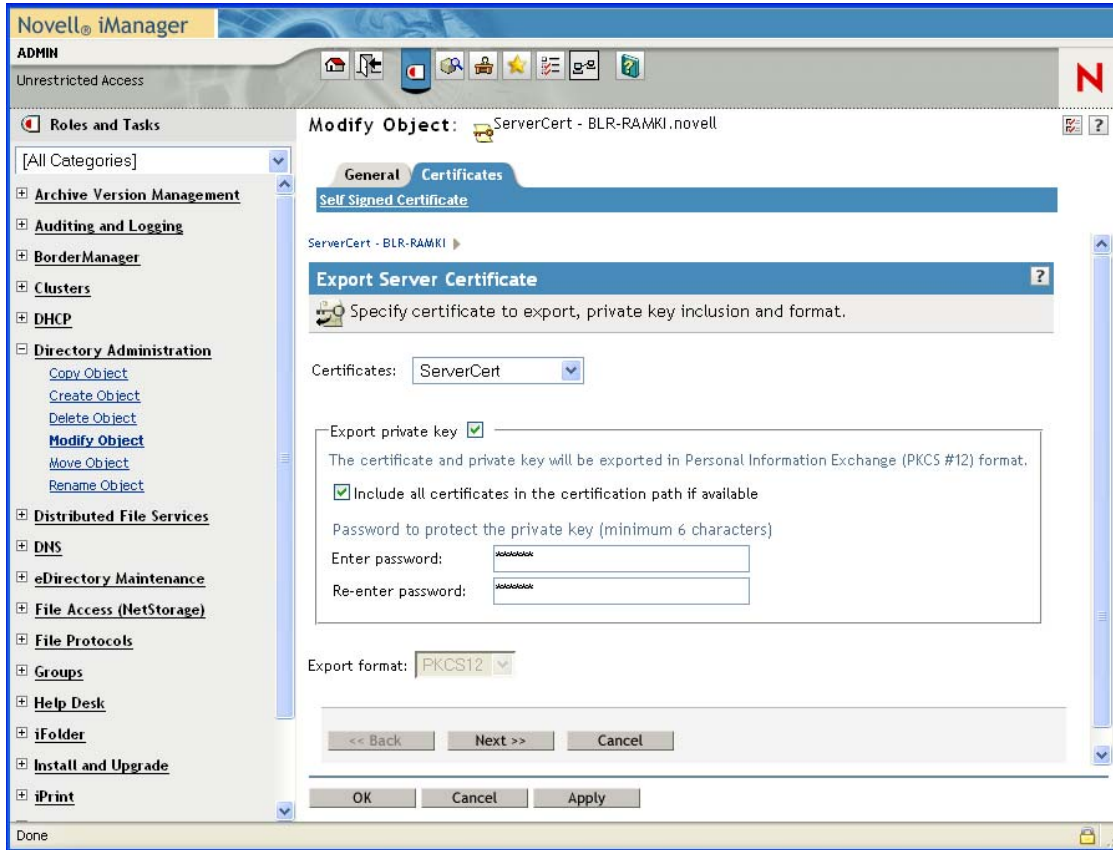
15.7 Exporting User Certificates

- 1 Click *Modify Object* under *Directory Administration*, then select *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 15-12 Modify Object: Certificates



- 3 To export the certificate, select the certificate and click *Export*. If you choose to export the key, select *Export private key*. You are then required to provide the password to protect the private key.
- 4 Click *Next*.
- 5 The next page displays a message indicating the export was successful, and prompts you to save the certificate.
- 6 If you choose to save the certificate, you are prompted to save it on the local machine.

15.8 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.

Configuring VPN Services

16

The VPN configuration software for Novell BorderManager 3.9 is based on Novell iManager 2.6.x. The VPN services provide extensive facilities to set up and configure site-to-site and client-to-site services.

NOTE: Configure the VPN server before configuring the client-to-client or site-to-site services.

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.

This section consists of the following information:

- ♦ Section 16.1, “Setting Up VPN Services,” on page 185
- ♦ Section 16.2, “VPN Server Configuration,” on page 186
- ♦ Section 16.3, “Virtual Private Network Prerequisites,” on page 189
- ♦ Section 16.4, “Client-to-Site Configuration,” on page 196
- ♦ Section 16.5, “Attaching a Client-to-Site Service to the VPN Server,” on page 204
- ♦ Section 16.6, “Site-to-Site Configuration,” on page 204
- ♦ Section 16.7, “VPN Policy,” on page 213

16.1 Setting Up VPN Services

- 1 Log in to iManager-based VPN Services. On a Windows XP or 2000 machine connected to a NetWare® server, open Internet Explorer or Mozilla Firefox browser and 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 3.9.

NOTE: You can run iManager from a NetWare server to configure other Novell BorderManager 3.9 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 *BorderManager>VPN Services* role to see the three kinds of configuration options available.
 - ♦ *Server Configuration*: Click this to set up the server as a VPN server.
 - ♦ *Client-to-Site Configuration*: Click this to configure client-to-site services. You can also configure a new client-to-site service.
 - ♦ *Site-to-Site Configuration*: Click this to modify or delete site-to-site services. You can also configure a new site-to-site service.

16.2 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:

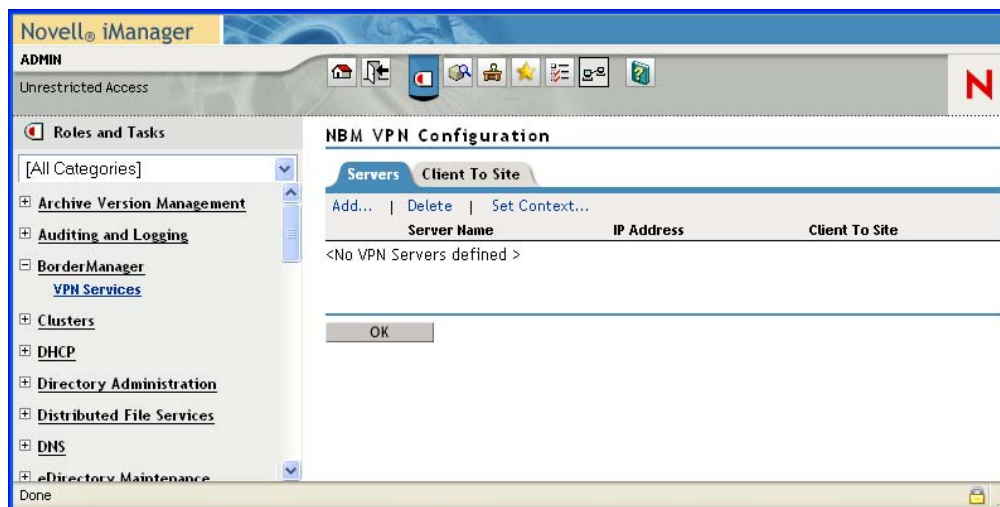
- Trusted Root Container (TRC, referred to as Trusted Root in the iManager and in Novell eDirectory). If you want to create the Container see [Section 15.4, “Creating Trusted Root Containers,” on page 179](#). If you want the VPN configuration utility to create the Container automatically, skip the Creating Trusted Root Containers section.
- Key Material Object (KMO) for the server. If you want to create the KMO manually, see [Section 15.2, “Creating Server Certificates,” on page 172](#), and export the KMO using the steps in [Section 15.3, “Exporting Root Certificates from the Server Certificate,” on page 178](#). 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 [Section 15.3, “Exporting Root Certificates from the Server Certificate,” on page 178](#).
- Trusted Root Object (TRO) under the Trusted Root Container see [Section 15.5, “Creating the Trusted Root Object,” on page 180](#).


16.2.1 Adding a New VPN Server

- 1 Log in to iManager. On a Windows XP or 2000 machine connected to a NetWare® 6.5 server, open either the Internet Explorer or Mozilla Firefox browser and, go to (<https://ipaddress/nps/iManager.html>), where *ip address* is the IP address of a NetWare 6.5 server running Novell BorderManager 3.9.
- 2 On the left pane, select *BorderManager > VPN Services*.

Initially, the page is 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.

Figure 16-1 NBM VPN Server Configuration

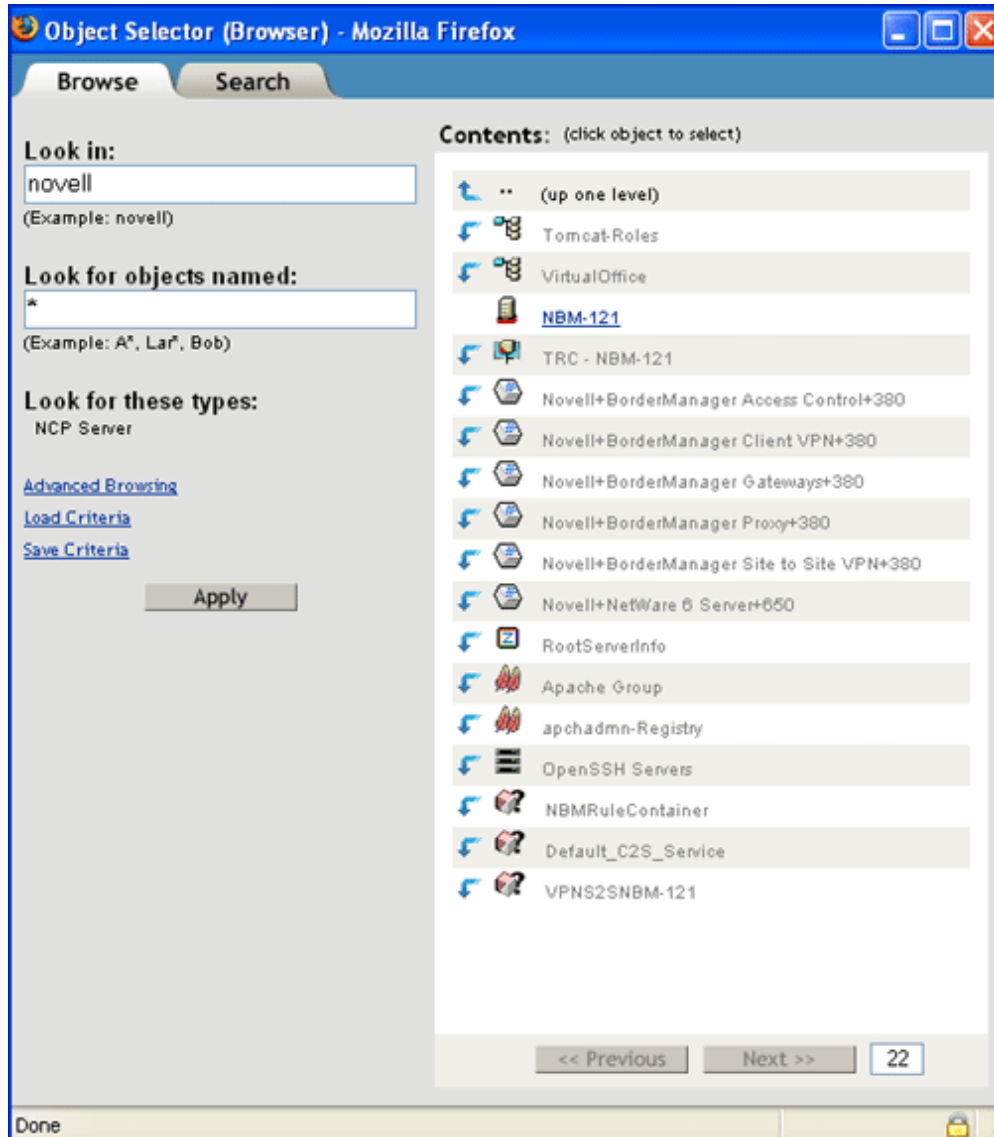


- 3 To add a new VPN server, under *Role* click *Add*.
- 4 Provide the Server Name or, click the  icon and select the Novell eDirectory context in which you would want to view the already configured VPN servers. Select *Subtree Level* for a

detailed context check. The *Subtree Level* search shows all VPN servers residing in Configuring VPN Services all subcontexts.

- 5 Click the  icon next to the field and choose a server in the tree.

Figure 16-2 Server Selection



- 6 Select a server from the list (it should be one of the underlined objects). After you have selected the server, you return to the previous page.
- 7 Click *Next*.
- 8 Select *Site To Site > Master* and click *Create*.
- 9 Select the *Member Version*.

NOTE: 3.9 is the only member version option. This is selected by default.

- 10 Select the *Preferred Authentication Method*.

If you select the *Certificate* method of authentication, specify the following:

- ◆ **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.
- ◆ **Subject Name:** The subject name of the X.509 server certificate used for the master member.
- ◆ **Alternative Subject Name:** One of the following three types:
 - ◆ DNS
 - ◆ Mail
 - ◆ IPv4

NOTE: If you choose one of these, you must provide the alternative subject name.

You can also add the following:

- ◆ **Protected IP Network and Hosts:** The list of networks or hosts to be protected by this site-to-site master member.
- ◆ **Enable IP RIP:** Adds RIP filters to IPFLT.

If you select the Pre-Shared Key method of authentication, you must provide the shared key. You can provide the shared key on the previous page.

NOTE: You can configure other parameters too. However, this depends on the peer's capability. We recommend that you configure both the methods of authentication in a mixed mode deployment.


When two slaves are initiating connection between two slaves, the PSK authentication method always takes precedence over certificate method of authentication.

- 11** After you have provided all the relevant information, click *Apply*. You return to the previous page. Here, specify the following:

On the page that appears, specify the following:

- ◆ **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 3.9 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.
- ◆ **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 [Section 15.2, "Creating Server Certificates," on page 172](#), select the Key Material Object from Novell eDirectory by using the Browse button.
- ◆ **Trusted Root Container:** 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 [Section 15.4, “Creating Trusted Root Containers,” on page 179](#), select the Trusted Root Container for eDirectory using the Browse button (trusted root is one of the underlined items).

- ♦ **S2S Pre-Shared Key:** The Pre-Shared Key (PSK) establishes a VPN tunnel between two Site-to-Site (S2S) members. In the PSK authentication method, a common secret or a pre-shared key is configured on both the servers. The VPN server uses this key secret to establish the tunnel. This method is the simplest way of configuring a Site-to-Site connection. To set a S2S Pre-Shared Key, click the  icon. Provide the Pre-Shared Key.
- ♦ **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.
- ♦ **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 is visible.

12 Click *OK*. You have now successfully configured a site-to-site master server.

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.

16.2.2 Deleting a VPN Server Configuration

To delete a VPN server configuration from a particular Novell BorderManager 3.9 server,

- 1** Select the VPN server configuration and click *Delete*.
- 2** 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.

VPN Server Behind NAT

The VPN server can also be configured behind NAT. To do so, use the `nat.nlm` shipped with Novell BorderManager 3.9. The `nat.nlm` is available in `filtersrv\system` directory on the product CD. For more details on NAT, see [Chapter 20, “Setting Up NAT,” on page 235](#).

16.3 Virtual Private Network Prerequisites

Before you start to set up the VPN component of the Novell BorderManager 3.9 software, you must meet the prerequisites described in this section.

This section contains the following topics:

- ♦ [“Site-to-Site VPN Prerequisites” on page 190](#)
- ♦ [“Client-to-Site VPN Prerequisites” on page 191](#)
- ♦ [“Setting Up VPN Filters” on page 192](#)

- ◆ [Section 16.3.4, “On VPN Master Site,” on page 193](#)
- ◆ [Section 16.3.5, “On VPN Slave Site,” on page 194](#)
- ◆ [Section 16.3.6, “Exceptions required to keep a Client-toSite and a Site-to-Site Connection Up,” on page 195](#)

16.3.1 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 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 3.9 for Secure Access to the Public Interface option during the initial Novell BorderManager 3.9 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 3.9 software, select the Setup Novell BorderManager 3.9 for Secure Access to the Public Interface option during the initial Novell BorderManager 3.9 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 192](#).

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 3.9 services.

The firewall filters can also be configured after installation by loading `BDRCFG`. If the firewall is not running the Novell BorderManager 3.9 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.

16.3.2 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 2000 or Windows XP.
- ◆ 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 on the [Novell Documentation Web site](http://www.novell.com/documentation). (<http://www.novell.com/documentation>).
- ◆ If you are using the VPN client with the Novell Client™ software, Novell Client version 4.9.1 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 3.9 software, select the Setup Novell BorderManager 3.9 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 3.9 services.

The firewall filters can also be configured after installation by loading `BDRCFG`. If the firewall is not running the Novell BorderManager 3.9 software, you must configure these filters manually as described in the documentation provided with the third-party firewall product.

16.3.3 Setting Up VPN Filters

These tables provide details on exceptions required for a Novell BorderManager 3.9 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	(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	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	Public IP Address	Any	Any	4500 (IKE-NAT-st)	IKE-NAT-ST
2	Any	Any	Public IP Address	4500 (IKE-NAT-st)	IKE-NAT-ST

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.

16.3.4 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.
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.
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.

16.3.5 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.
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.
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.

16.3.6 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	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)	

Source Address	Source Port(Service Type)	Destination Address	Destination Port (Service Type)	Protocol	Description
Public IP Address	Any	Any	Any	ESP (50)	
Any	Any	Public IP Address	500	IKE (UDP)	
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	

16.4 Client-to-Site Configuration

This utility helps you configure VPN client-to-site services on your network.

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.

16.4.1 Creating a New Client-to-Site Configuration

You can modify or delete the existing client-to-site services. You can also configure a new client-to-site service. To create a new client-to-site configuration, do the following:

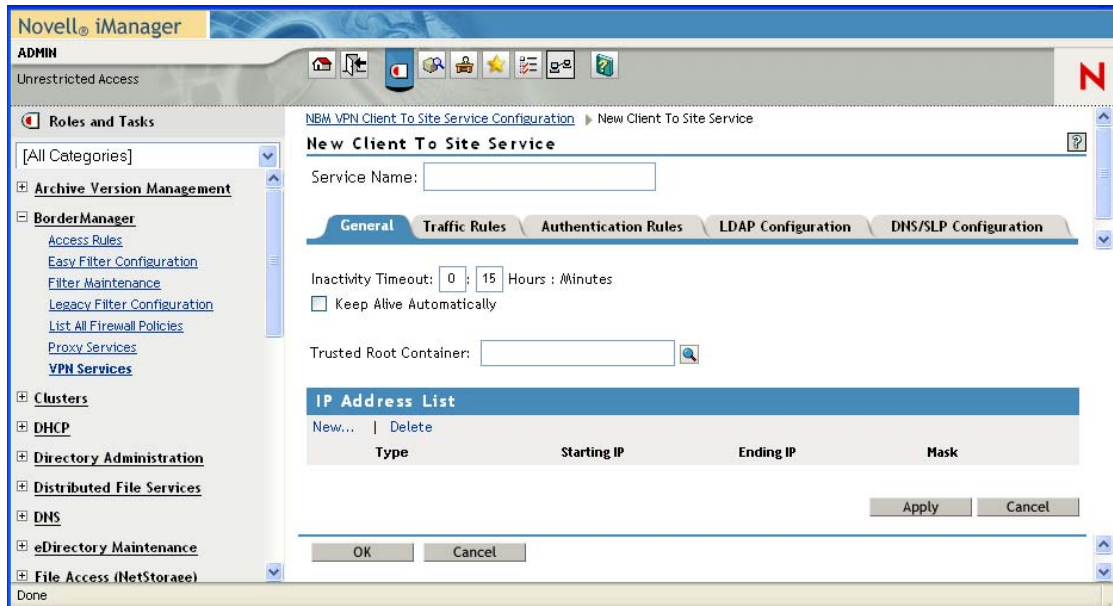
- 1 Click *Client To Site > Add*.
- 2 Provide a *Service Name*. With this, you have begun configuring a new client-to-site configuration. You can configure the client-to-site connection with the following parameters:
 - ♦ “General” on page 197
 - ♦ “Traffic Rules” on page 197
 - ♦ “Authentication Rules” on page 201
 - ♦ “Remote LDAP Configuration” on page 203
 - ♦ “DNS/SLP Configuration” on page 204
 - ♦ “Final Client-to-Site Page” on page 204

16.4.2 General

These are the general properties of the client-to-site service. Make sure to click *Apply* button if you have made any modifications to the general parameters.

- 1 Provide the *Service Name* for your client-to-site configuration..
- 2 By default, the *General* tab is selected. 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.
 - ♦ **IP Address List:** 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.

Figure 16-3 Default Values for a New Client-to-Site Service.



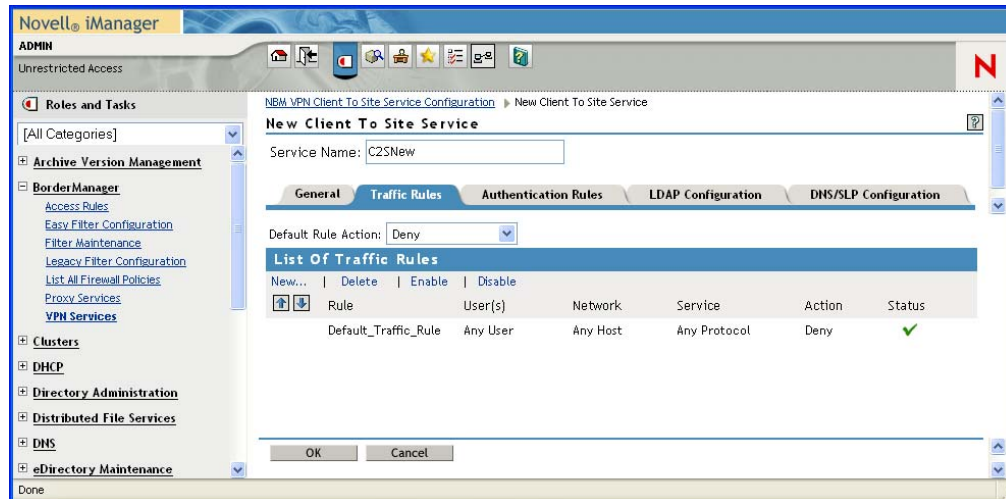
16.4.3 Traffic Rules


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.

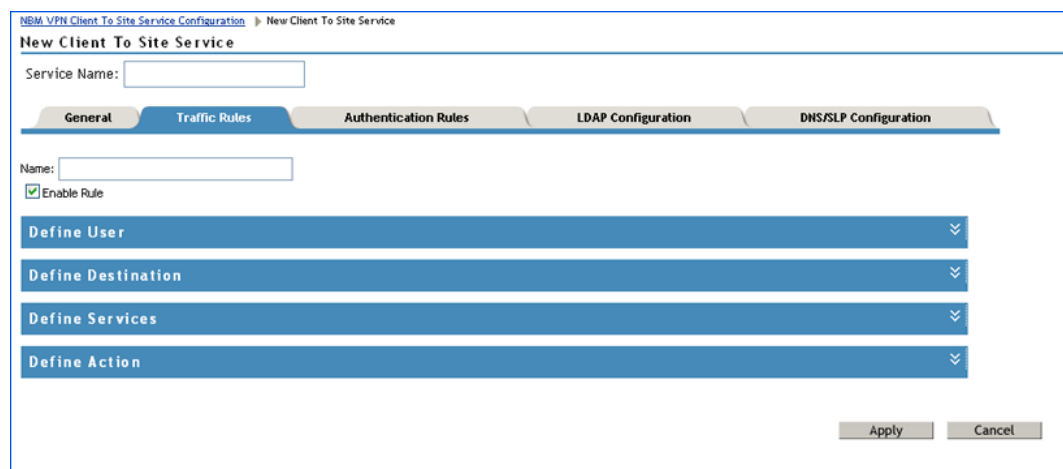
Figure 16-4 Traffic Rule



- 1 Click *New* to add a new traffic rule.
- 2 You can configure any one if the following in a traffic rule.
 - Use the  icon to view the traffic rule parameters. On expanding each of the rules, the following can be configured.
 - ◆ “Define User” on page 199
 - ◆ “Define Destination” on page 200
 - ◆ “Define Services” on page 201
 - ◆ “Define Action” on page 201

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.

Figure 16-5 Expanded View of The Traffic Rules



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:

- ◆ “All Users” on page 199
- ◆ “Only User List” on page 199

All Users

- 1 Click *Add* and select the user from the page.
- 2 Click  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.

Only User List

- 1 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 Remote User or Group name list

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 NMASTM 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.

- ◆ 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. 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.

- 1 Click *Define Service* to see this page. The values shown on the page are the default values. You can modify them.

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.

- ◆ 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.

16.4.4 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.

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 202
- ◆ “Authentication Condition” on page 202
- ◆ “Allow/Deny Action” on page 202
- ◆ “Example of a Default NMAS Configuration” on page 203

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 [Section 16.4.3, “Traffic Rules,” on page 197](#) Traffic Rules > Define User for details on this page.

Authentication 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 in to the iManager.
- 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 select *All User*.
- 7 Select *Authentication Condition*, the following screen will be displayed.
- 8 Select *Allow NMAS Authentication* as shown in the figure.
- 9 Under *Allow/Deny Users*, select *Allow*.
- 10 Click *Apply* > *OK*.

16.4.5 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.

- ♦ **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`.

16.4.6 DNS/SLP Configuration

Use this page to configure DNS/SLP to be applied on Windows workstation during a VPN session.

- ♦ **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.

16.4.7 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.

- 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.

16.5 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 *BorderManager > VPN Services* in the left pane of iManager.

- 1 Click the *VPN Server* link to modify the VPN configuration. On the new page that appears, select *client-to-site* and click *Details*. Click *OK* in the message box.

In case the service is already attached, click *client-to-site*. This detaches the service.

- 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.

16.6 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 [Section 16.2, “VPN Server Configuration,” on page 186](#).

- ◆ 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 [Section 15.3, “Exporting Root Certificates from the Server Certificate,” on page 178](#) and create the TROs in the Trusted Root container using the steps in [Section 15.5, “Creating the Trusted Root Object,” on page 180](#).

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 [Section 16.2, “VPN Server Configuration,” on page 186](#)
- ◆ 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 [Section 15.3, “Exporting Root Certificates from the Server Certificate,” on page 178](#) and create the TROs in the Trusted Root container using the steps in [Section 15.5, “Creating the Trusted Root Object,” on page 180](#).

The following topics are discussed here:

- ◆ [“Configuring a VPN Server As a Master Server” on page 205](#)
- ◆ [“Configuring a VPN Server As a Slave Server” on page 207](#)
- ◆ [“Modifying a Site-to-Site Service” on page 208](#)
- ◆ [“Removing Site-to-Site Members” on page 211](#)

16.6.1 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.

- 1 To create and attach a site-to-site service to a VPN server, select *site-to-site*; select the *Master* option, and then click *Create*.
- 2 In the next page, select the *Member Version* and the *Authentication Method*. You will also have to specify the certificate 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 [Section 15.5, “Creating the Trusted Root Object,” on page 180](#), 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=nbm39.o=novell` or `o=novell.cn=nbm39`. 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.

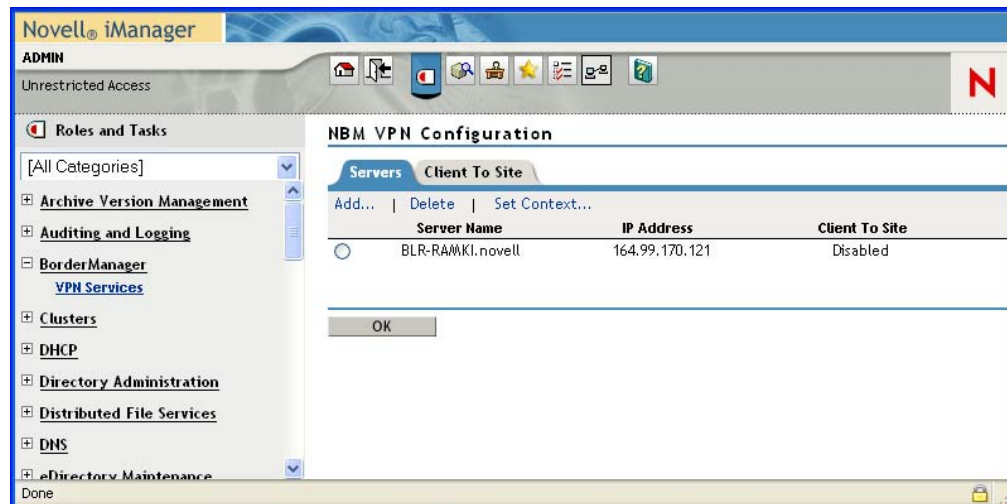
NOTE: To view the certificate subject name, go to *iManager > eDirectory Administration > Modify Object > select the Key Material Object* (server certificate that you have created). Select the certificate from the list and click *Details*.

- ♦ **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.
 - ♦ **S2S Pre-Shared Key:** If you chosen the Pre-Shared Key (PSK) mode of authentication. You will have to provide a secret key.
- 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 16-6 Server Attached to a Site-to-Site Service



This example shows a server *BLR.RAMKI.novell* with public IP address 164.99.171.77 configured as a VPN server with client-to-site services enabled and site-to-site services enabled. This VPN server is a master of the site-to-site service to which it belongs.

16.6.2 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 [Section 16.2, “VPN Server Configuration,” on page 186](#). In the left pane, click *VPN Services*, then click the configured server. Select the site-to-site service and click the Slave option button.

- 1 Select the configured server. Click *Slave*. 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` Configuring VPN Services 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.

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.

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 209](#).

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.

- ◆ 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.
- ◆ 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 18, “Monitoring Virtual Private Networks,” on page 219](#).

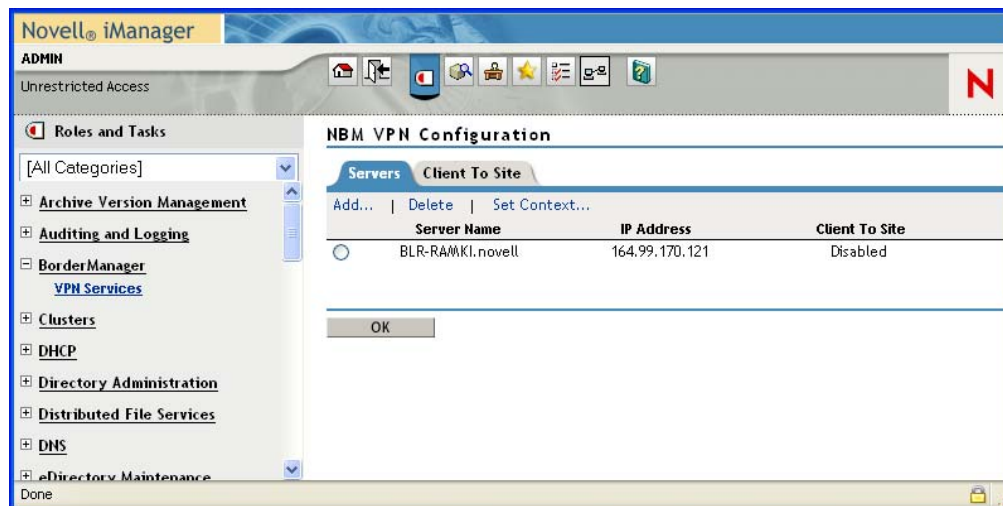
You will see the list of members.

- 2 Click `Synchronize All`.

16.6.3 Modifying a Site-to-Site Service

Click *VPN Services* 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.

Figure 16-7 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 209
- ◆ “[Traffic Rules](#)” on page 210


- ◆ “Third-Party Traffic Rules” on page 211
- ◆ “Final Site-to-Site Page” on page 211

Member List

The member list shows the master server that was configured during the creation of the site-to-site service.

- 1 To modify master server details, select the server and click *Edit*.
- 2 To add a slave server to this site-to-site service, click *New*.
- 3 Fill the details in the next page.

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 207

- ◆ **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  icon if the server that you are 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 Click *OK* to exit after saving the member list changes to Novell eDirectory, or you can configure *General Parameters* and *Traffic Rules* for the site-to-site service.

General Parameters

The General Parameters page has the following fields:

- ♦ **Connection Initiation:** Two types of connection initiations are supported:
 - One Side:** The connection is only from one side.
 - Both Sides:** The connection is both ways: master to slave and slave to master.
- ♦ **VPN Network Topology:** 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.
 - Ping:** 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.

16.6.4 Removing Site-to-Site Members

The following scenarios are possible while removing site-to-site members:

- ♦ “Removing Slave” on page 212
- ♦ “Forcefully Removing the Slave” on page 212
- ♦ “Removing a Master” on page 212
- ♦ “Forcefully Removing a Master” on page 212

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, 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. Remove all the slaves using the steps mentioned in **“Removing Slave” on page 212**, and verify that the changes are synchronized.
- 2 Using iManager remove the VPN site-to-site configuration.

Forcefully Removing a Master

Ocasionalmente, 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.

16.7 VPN Policy

Novell BorderManager 3.9 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 213](#)
- ◆ [“Default Values for Client-to-Site Traffic Rules” on page 214](#)
- ◆ [“Default Values for Site-to-Site Traffic Rules” on page 214](#)

16.7.1 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.

16.7.2 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.

16.7.3 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.

Upgrading Virtual Private Networks

17

This section explains the tasks you must complete to set up the VPN component of the Novell® BorderManager® 3.9 software for an upgrade from an Novell BorderManager 3.8.

For configuration information, see [Chapter 16, “Configuring VPN Services,” on page 185](#). Refer to [Chapter 15, “Certificate-Based Authentication,” on page 171](#) for details on how to configure certificates before you launch VPN services.

This section also describes the preparatory steps required for some tasks.

- ◆ [Section 17.1, “Upgrading a VPN from a Previous Version,” on page 215](#)

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 3.9 Overview and Planning Guide*, available in the online documentation. Make sure you understand this information before setting up and configuring your VPN.

17.1 Upgrading a VPN from a Previous Version

Novell BorderManager 3.9 supports industry-standard IKE for key management. This section discusses ways of upgrading a Novell BorderManager 3.8 VPN network to a Novell BorderManager 3.9 VPN network without affecting the connectivity between these networks. If you want to migrate the VPN configuration before upgrading to Novell BorderManager 3.9, make sure that the VPN is configured.

NOTE: After initial configuration through VPBNCFG, reload vpmaster and vpslave if they are not already loaded.

17.1.1 General Guidelines for Upgrading

First, upgrade the master Novell BorderManager 3.9 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 3.9 configuration. The actual upgrade consists of three steps:

1. Installing Novell BorderManager 3.9 over earlier versions of BorderManager.
2. During installation, selecting the Automatic Migration check box, which will automatically migrate the existing configuration.

After the preceding steps are complete, an earlier version of a BorderManager server can be considered fully migrated to a Novell BorderManager 3.9 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 IKE mode.

The IKE configuration can be done using the iManager plug-ins. The Novell BorderManager 3.9 slaves and master can be monitored through the new Netware Remote Manager monitoring interface. For information see [Chapter 18, “Monitoring Virtual Private Networks,” on page 219](#).

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.

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 3.9 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 3.9 slave to the VPN site-to-site network. This will be a fresh, newly configured Novell BorderManager 3.9 slave.

17.1.2 Upgrade Procedure

The following upgrade scenarios are discussed here:

- ♦ [“Upgrading an Earlier BorderManager Master to Novell BorderManager 3.9” on page 216](#)
- ♦ [“Upgrading an Earlier BorderManager Slave to Novell BorderManager 3.9” on page 216](#)
- ♦ [“Adding a New Novell BorderManager 3.9 Slave to a Partially or Fully Upgraded Setup” on page 216](#)

Upgrading an Earlier BorderManager Master to Novell BorderManager 3.9

- 1 Run the Novell BorderManager 3.9 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 3.9

- 1 Run the Novell BorderManager 3.9 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.

Adding a New Novell BorderManager 3.9 Slave to a Partially or Fully Upgraded Setup

- 1 Run the Novell BorderManager 3.9 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 207](#).
- 2b** Go to the master and add this slave as a Novell BorderManager 3.9 slave. For information, refer to [“Configuring a VPN Server As a Slave Server” on page 207](#).

At this point, the new slave is able to receive the configuration from the master, and also communicate with the other Novell BorderManager 3.9 slaves.

Monitoring Virtual Private Networks

18

The following sections describe the statistics used to monitor the operation of Novell BorderManager 3.9 Virtual Private Network. 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:

- ◆ [Section 18.1, “Logging into NetWare Remote Manager,” on page 219](#)
- ◆ [Section 18.2, “Checking the VPN Real-Time Monitor,” on page 221](#)
- ◆ [Section 18.3, “Checking the Audit Log on a VPN Server,” on page 224](#)
- ◆ [Section 18.4, “Checking the Activity of a VPN Server,” on page 227](#)

NOTE: VPN Monitoring through NRM is available only for Novell BorderManager 3.9 servers. If your site-to-site setup has both Novell BorderManager 3.9 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 3.9 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 3.9 members. For synchronizing the BMEE 3.6/NBM 3.7 members, you still need to use the Synchronize option available in NWAdmn.

18.1 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 18-1 VPN Monitoring



4 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 18-2 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	
<input type="button" value="Synchronize Selected Servers"/>		<input type="button" value="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.

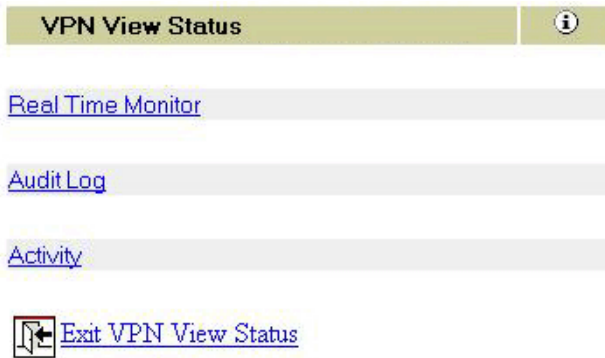
Synchronization: This is an important feature used to distribute configuration information from a master server to slaves. This feature is available only in NRM-based VPN Monitoring

and is applicable only to Novell BorderManager 3.9 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 18-3 VPN View Status



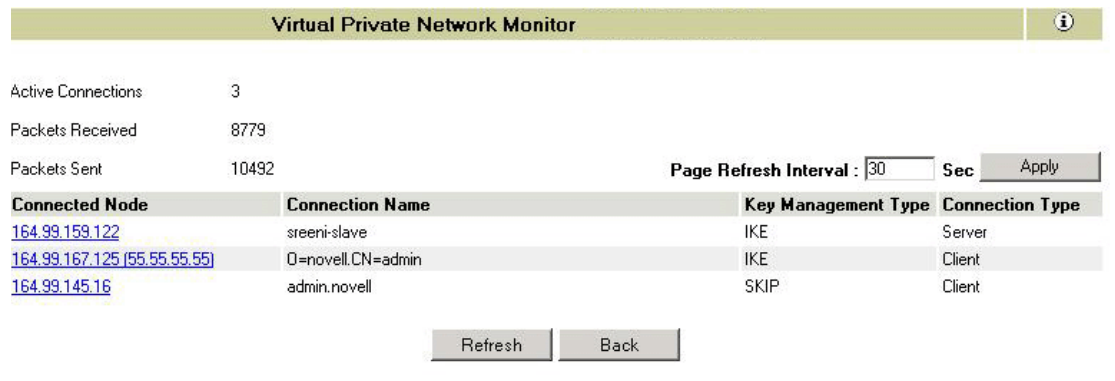
TIP: For a full screen view, specify the port and /VPN (https://ip address:8009/VPN). The right pane occupies the full screen and the left pane is suppressed.

18.2 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 18-3 on page 221](#)) click the Real Time Monitor link for a selected member to display a page with the following information:

Figure 18-4 Connection Information for the Selected Member



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 3.9 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 3.9 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. If the connections are behind NAT, the key management type is NATed IKE. 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 18-5 Detailed Information for an IKE Connection

Virtual Private Network Monitor		i		
Connection Name	0=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 18-6 Policy Statistics for an Active Traffic Rule

The screenshot shows the 'Virtual Private Network Monitor' interface. The main window displays connection details for 'sreeni-slave'. A pop-up window titled 'Policy Statistics' is overlaid, showing the following data:

Metric	Value
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

Below the pop-up window, the 'Active Policies' section contains a table with the following data:

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

Buttons for 'Refresh' and 'Back' are located at the bottom of the interface.

18.3 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 18-3 on page 221](#)), click the *Audit Log* link for a selected member to display a page with the following information.

Figure 18-7 Audit Log Page

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.

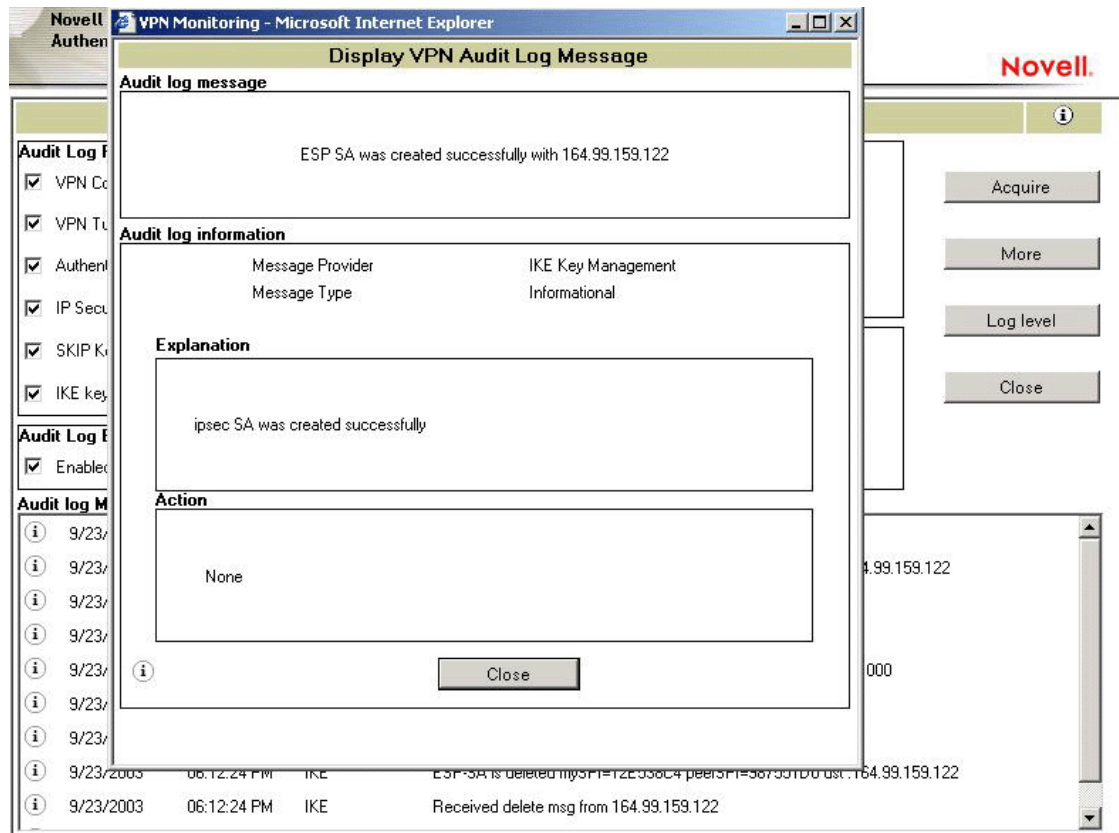
Audit Log Messages

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 18-8 Audit Log Message Details



Log Level

Pressing Log Level displays the dialog box shown below. This dialog box helps you set the log levels for a selected server.

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.
- ◆ **IKE Key Management:** Provides key management messages for Novell BorderManager 3.9 clients.

18.4 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 18-3 on page 221](#)), click the Activity link for a selected member.

Figure 18-9 Activities of a VPN server

The screenshot displays the 'VPN Member Activity' page. It is divided into several sections:

- Associated Connections: 1**: A table with columns for IPX, IP, and Connection. It shows one connection named 'sreeni-slave' with a status icon.
- Global details**: A table listing various statistics such as Tunnel status (Loaded), Tunnel time active (3:05:46:01), and various packet and byte counts.
- Associated connection details**: A table providing details for the 'sreeni-slave' connection, including associated address (164.99.159.122) and byte counts.
- IPX associated connection details**: A table showing connection state (Unattached) and call direction (None).
- IP associated connection details**: A table showing connection state (Established), call direction (Outgoing), and time active (3:05:46:01).

On the right side of the page, there are several buttons: 'Update', 'Clients', 'Reset', and 'Close'. A small icon at the bottom right indicates the current view (Server or Client).

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.

The Novell BorderManager VPN client software allows a workstation to communicate securely over the Internet to a network protected by a Novell VPN server.

With this release, Novell BorderManager introduces VPN client on Linux.

This section discusses the following:

- ◆ [Section 19.1, “VPN Client Features,” on page 229](#)

19.1 VPN Client Features

The following features are available in the VPN client software:

- ◆ [“X.509 Certificate Authentication Mode” on page 229](#)
- ◆ [“NMAP Authentication Mode” on page 230](#)
- ◆ [“NMAP LDAP Authentication Mode” on page 230](#)
- ◆ [“Pre-Shared Key Authentication Mode” on page 230](#)
- ◆ [“VPN Client Integration with the Novell Client” on page 230](#)
- ◆ [“Use NICE for Encryption” on page 231](#)
- ◆ [“Selecting Dial-Up Entries” on page 231](#)
- ◆ [“Automatic Creation of a Novell VPN Dial-Up Entry” on page 231](#)
- ◆ [“Password Expiry Notice” on page 231](#)
- ◆ [“VPN Server Hosts List” on page 232](#)
- ◆ [“Policy” on page 232](#)
- ◆ [“VPN Connections through NAT” on page 232](#)

19.1.1 X.509 Certificate Authentication Mode

The Novell BorderManager 3.9 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, tree 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 3.9 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.

19.1.2 NMAS Authentication Mode

Novell VPN client is integrated with Novell Modular Authentication Services (NMASTM). NMAS works with the Novell Client, so you must install the Novell Client to benefit from the NMAS 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.

19.1.3 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.

19.1.4 Pre-Shared Key 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 (PSK) 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 PSK.

19.1.5 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.

19.1.6 Use NICI for Encryption

Novell Client 4.91 is recommended for Windows NT, 2000, XP, and XP Home edition.

19.1.7 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.

19.1.8 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.

19.1.9 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.

19.1.10 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.

19.1.11 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.

19.1.12 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 `filtsrv\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.

Network Address Translation

IV

The following sections provide the basic information you need to set up Network Address Translation (NAT).

- ♦ [Chapter 20, “Setting Up NAT,” on page 235](#) provides information on how to set up Network Address Translation.
- ♦ [Chapter 21, “Advanced Configuration of NAT,” on page 239](#) gives the procedures you need to set up and configure various NAT features and parameters.
- ♦ [Chapter 22, “Managing Network Address Translation,” on page 243](#) gives tips and guidelines for monitoring NAT functionality.

Setting Up NAT

20

Novell BorderManager 3.9 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:

- ♦ [Section 20.1, “NAT Prerequisites,” on page 235](#)
- ♦ [Section 20.2, “Setting Up NAT on a Single Interface,” on page 236](#)
- ♦ [Section 20.3, “Setting Up NAT with Multihoming,” on page 237](#)
- ♦ [Section 20.4, “Completing Advanced Setup, Configuration, and Management Tasks,” on page 238](#)

NOTE: This section describes the tasks required to set up an initial implementation of Novell BorderManager 3.9 NAT. For planning and conceptual information about NAT, refer the *Novell BorderManager 3.9 Overview and Planning Guide*, available in the online documentation.

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

20.1 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 3.9 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 3.9 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 3.9 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.

20.2 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 [Section 20.3, “Setting Up NAT with Multihoming,” on page 237](#), 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 [Section 20.3, “Setting Up NAT with Multihoming,” on page 237](#) 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.

20.3 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, “Configuring Proxy Services,” on page 19](#) or [Chapter 17, “Upgrading Virtual Private Networks,” on page 215](#).

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
```

20.4 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

Advanced Configuration of NAT

21

This section provides an example of using Novell BorderManager 3.9 Network Address Translation (NAT) in a private network when the network uses both registered and unregistered addresses.

See [Chapter 20, “Setting Up NAT,” on page 235](#) 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.

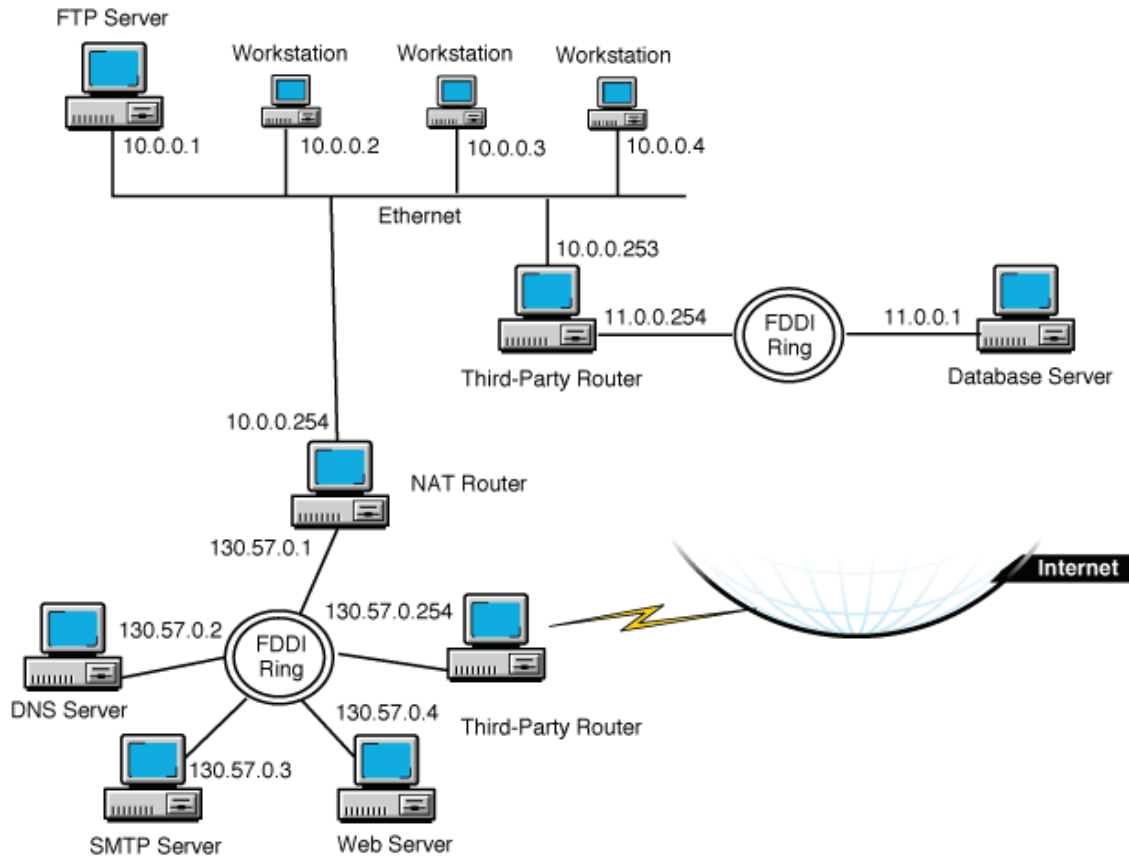
Workstations on network 10.0.0.0 should be able to access the rest of the private network and the Internet.

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 21-1 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[Inbrk]130.57.100.1 10.0.0.1[Inbrk]130.57.100.2
10.0.0.2[Inbrk]130.57.100.3 10.0.0.3[Inbrk]130.57.100.4 10.0.0.4[Inbrk]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.

Managing Network Address Translation

22

This section provides tips and guidelines for monitoring the functionality of Novell BorderManager 3.9 Network Address Translation 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.

SET Parameters

A

This section provides some of the common SET parameters for Novell BorderManager. Use these parameters to change your settings.

A.1 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.

A.1.1 IKE debugmask

Syntax:	IKE debugmask = n
Description:	2 = message header, 4 = message body, 8 = attribute
Range:	0 to 4294967295
Default:	8

A.1.2 IKE Certificate Request Payload

Syntax:	IKE cert request = OFF
Description:	Send certificate request payload ON=yes OFF=no
Range:	On Off
Default:	Off (disabled)

A.1.3 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

A.1.4 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

A.1.5 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

A.1.6 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

A.1.7 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

A.1.8 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 pre-shared key authentication.
Range:	1 to 11

Default:	1
----------	---

A.1.9 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

A.1.10 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

A.1.11 VPN Over NAT

Syntax:	VPN Over NAT = ON
Description:	Can be enabled or disabled over NAT
Range:	On Off
Default:	ON

A.1.12 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

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.