Novell BorderManager®

3.7

www.novell.com

INSTALLATION

Novell®

Legal Notices

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

Installation
April 2002
103-000238-001

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

Novell Trademarks

BorderManager is a registered trademark of Novell, Inc,. in the United States and other countries
eDirectory is a trademark of Novell, Inc.
Internetwork Packet Exchange is a trademark of Novell, Inc.
IPX is a trademark of Novell, Inc.
NDS is a registered trademark of Novell, Inc., in the United States and other countries.
NetWare is a registered trademark of Novell, Inc., in the United States and other countries.
NetWare Loadable Module is a trademark of Novell, Inc.
NLM is a trademark of Novell, Inc.
Novell is a registered trademark of Novell, Inc., in the United States and other countries.
Novell Technical Support is a service mark of Novell, Inc.

Third-Party Trademarks

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

Contents

About This Guide

Introduction

The purpose of this documentation is to describe how to install the components of Novell® BorderManager® 3.7, and how to perform basic software setup and configuration. In addition, this documentation refers you to specific online documents for more information.

The audience for this documentation is experienced network administrators.

Documentation Conventions

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

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

1 Installing Novell BorderManager 3.7

This section provides instructions for installing the Novell® BorderManager® 3.7 software and contains:

NOTE: This chapter describes the tasks required to install an initial implementation of Novell BorderManager 3.7 software. For planning and conceptual information about the services that comprise the Novell BorderManager 3.7 software suite, refer to the Novell BorderManager 3.7 Overview and Planning Guide, available in the online documentation. Make sure you understand this information before setting up and configuring the various services included in the Novell BorderManager 3.7 suite.

System Requirements

Novell BorderManager 3.7 (NBM 3.7) is installed on a NetWare® server and is administered using NetWare Administrator from a client Windows* 98, Windows 2000, Windows NT* or Windows XP workstation.

Server Requirements

For Installing on NetWare 5.1 SP4

Server Hardware	Server Software
PC with a Pentium* II or later processor	NetWare 5.1 Support Pack 4 or later
Minimum of 256 MB of RAM for NBM 3.7	Note: For NetWare 5.1 MLA servers, you must have a server-based license on the target server.
Additional 512 MB RAM for SurfControl*	
Minimum of 160 MB of disk space, with an additional 40 MB available during installation	NDS® 8 NetWare Update read/write replica on the Novell BorderManager server
4 GB disk space to support caching services	Novell Licensing Service (NLS) Kit (installed automatically with NetWare 5.1)
CD drive that can read ISO 9660 formatted disks	TCP/IP network interface bound and configured
	Run INETCFG once and transfer the commands from AUTOEXEC.NCF

For Installing on NetWare 6.0 Support Pack 1

Server Hardware	Server Software
PC with a Pentium II or higher processor Minimum of 256 MB of RAM for NBM 3.7 Additional 512 MB RAM for SurfControl Minimum of 160 MB of disk space, with an additional 40 MB available during installation 4 GB disk space to support caching services CD drive that can read ISO 9660 formatted disks	NetWare 6.0 SP 1 or later Novell eDirectory™ 8.6.2 read/write replica on the Novell BorderManager server Novell Licensing Service (NLS) Kit TCP/IP network interface bound and configured Run INETCFG once and transfer the commands from AUTOEXEC.NCF

NOTE: Because Novell BorderManager 3.7 is enabled for Novell Licensing Services (NLS), the first Novell BorderManager 3.7 server installed into a tree or partition must be installed on a NetWare server that holds an NDS or eDirectory read/write replica of that partition. All Novell BorderManager 3.7 servers installed into the same partition at a later time are not required to have a read/write replica.

Client Requirements

Client Hardware	Client Software
Windows 98, 2000, NT, XP or Me	Windows 98, 2000, NT, XP or Me
Minimum of 28 MB of free disk space	Netscape* Navigator* 4.7 or later
Minimum of 32 MB of RAM	Microsoft* Internet Explorer 5.5 or later.

End User License Agreement

Before installing Novell BorderManager 3.7, you need to go through the End User License Agreement (EULA). The EULA in English, Portugese, French, Italian, German, Spanish, Japanese, Czech, Polish, and Dutch is in the relevant language folder under root of the CD in the \LICENSE directory.

Upgrading

Novell BorderManager 3.7 can be installed as an upgrade to BorderManager Enterprise Edition 3.6. The installation will preserve the existing server configuration, with the exception of the Virtual Private Network (VPN). The upgrade will do a file copy of the basic configuration and extend the schemas. Migrate the filters manually after you finish installation. See Step 18 on page 17 for further information.

Preparing for Installation

Review the following list of items and record the information:

- ❑ Location of the license diskettes or the path to the license file
- ❑ Server IP address and default gateway
- ❑ Public and private interfaces and their IP address bindings
- ❑ Domain Name System (DNS) domain name
- ❑ IP addresses for up to three DNS name servers on the network

Installing Novell BorderManager 3.7 on a NetWare 5.1 SP 4 or NetWare 6.0 SP 1 Server

To install Novell BorderManager 3.7 from a CD on the server:

1. Verify that you have NetWare 5.1 Support Pack 4 or NetWare 6.0 Support Pack 1 or later software on your server.
2. Mount the NBM 3.7 CD from server by typing **CDROM** on the server console.
3. On the server side, go to the X-Server graphical console. If X-Server graphical console is not loaded, type **STARTX** on server console.

   If STARTX was already loaded, press Ctrl+Esc and select the X-Server Graphical Console.

   Installation of Novell BorderManager 3.7 from NWCONFIG is disabled. The installation can be done only from the X-Server graphical console.
4. Click the Novell logo > select Install to display the currently installed products.

5 Click Add > browse to the root of the CD > click OK.

6 Select the Welcome page > click Next.

7 Read the license agreement. If you accept the terms of the agreement, click I Accept.

Refer to "End User License Agreement" on page 13 for more details.

8 Check the check box for each Novell BorderManager 3.7 service you want to install.

NOTE: Regardless of what Novell BorderManager 3.7 services you select, licenses for all the services will be installed.

9 To install the licenses now, insert the Novell BorderManager 3.7 License diskette and enter the path to the license directory (for example A:\LICENSE) > click Next. Otherwise, check the Skip License Install check box > click Next so that it can be installed later.

You can install the system files without installing the license; however, Novell BorderManager 3.7 will not load until a valid or trial license is installed.

You can choose the trial licenses from the drop-down menu on this page.

10 At the login dialog box, log into the NDS or eDirectory tree with a fully distinguished name (with administrative rights).

You must have administrative rights to the root of the NDS or eDirectory tree. This requirement applies to any user who is a trustee with Supervisor rights at a container at the same level as the server. Administrative rights are required to extend the eDirectory schema to the tree, install product licenses, and configure Novell BorderManager 3.7 for the first time.

If you are installing BorderManager firewall/caching services or BorderManager VPN services, review the list of network interfaces and their IP bindings. Specify each interface as public, private, or both.

If you are upgrading, go to Step 16.

11 For both firewall/caching and VPN services, you must specify a public IP address to use with Novell BorderManager 3.7 to secure your network border. Public IP addresses specify server interfaces to a public network, typically the Internet. Private IP addresses specify server interfaces to a private network or intranet.

11a Specify a public IP address.

Specifying an interface as public makes the Set Filters to Secure All Public Interfaces check box available. Check this check box to deny all traffic into and out of the public interfaces. If this is an upgrade, existing filters are preserved and the option Deny All Filters is not set on public interfaces.

11b Specify a private IP address.

11c Select the check box Set Filters to Secure All Public Interfaces to set the default IP and IPX filters for the checked public interfaces. If this is an upgrade, the existing filters will be preserved.

11d Specify a gateway. If the Gateway IP field is empty, type the default gateway name.

11e Click Next.

If you have not specified a private IP Address go to Step 14; otherwise, go to Step 12.

12 Check the check boxes for the services that you want to enable. Filter exceptions for these services will be created on the public interface > click Next.

After installation, configure the Mail and News Services manually with NetWare Administrator.

NOTE: If there is only one interface and has a public filter, exceptions will not be created.

13 The check box for Access Control is enabled by default. We recommend that you accept the default. Access control enforces additional security by denying all traffic. Access control rules can be set by using the NetWare Administrator utility. Access rules are used to allow or deny access from any source or to any destination. This option comes up only if you select one or more services on the previous screen.

14 Enter a unique DNS domain name for your network > click Next.

15 Click Add to enter at least one or up to three DNS server IP addresses.

By default, the existing DNS entry will be listed.

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

17 Do one of the following:

- Click Readme to view the Readme file.
- Click Reboot for Novell BorderManager 3.7 services to come up.
- Click Close to complete the installation and return to the GUI screen.

18 After rebooting, verify that FILTSRV.NLM is not loaded. If it is loaded, unload it. If it fails to unload, unload all FILTSRV.NLM dependent NLM files > unload FILTSRV.NLM.

19 Enter **`FILTSRV MIGRATE`** on the console prompt to migrate the existing filters to eDirectory.

20 Unload FILTSRV and load it in normal mode (Enter **`FILTSRV`** on the console prompt).

Installing the Novell Client Software

The Novell Client™ software provides access to Novell BorderManager 3.7 from Windows 98, 2000, NT and XP workstations. To install the Novell Client, refer to the documentation on the Novell Documentation Web site (http://www.novell.com/documentation/lg/noclienu/index.html).

The Novell Client version 4.8 or later is required for Windows NT, 2000, and XP. The Novell Client version 3.3 or later is required for Windows 98. Also, to support the Novell IP Gateway, you must install the Novell IP Gateway client component on all client workstations.

Installing NetWare Administrator Snap-In Modules

NetWare Administrator snap-in modules allow you to enable, configure, and manage Novell BorderManager 3.7 components, such as Proxy Services, the Novell IP Gateway, VPN, BorderManager Authentication Services, and access control.

The Novell BorderManager 3.7 installation utility installs the 32-bit client NetWare Administrator snap-in modules on the server. You can administer your BorderManager servers by running NWADMN32.EXE from the server's SYS:\PUBLIC\WIN32 directory.

To install the snap-in modules:

1 Launch the version of NetWare Administrator to which you want to install the snap-in modules > verify that it is working properly > exit the utility.

2 From your administrator workstation, map a drive to the SYS: volume of the Novell BorderManager 3.7 server > launch the Novell BorderManager 3.7 Setup program (SETUP.EXE).

The Novell BorderManager 3.7 SETUP.EXE program is located on the server in SYS:\PUBLIC\BRDRMGR\SNAPINS.

3 Follow the instructions provided by the installation wizard.

   During the snap-in module installation, you are prompted for the location of your administrator files. Usually, administrator files are located on SYS: volume of the server in the \PUBLIC\WIN32 directory. If you want to install the Novell BorderManager 3.7 snap-in modules into a centralized NetWare Administrator 32 location, specify the directory where your centralized NWADMN32.EXE resides (for example, SYS:\PUBLIC\WIN32).

4 After the snap-in modules are installed, exit the installation wizard.

5 To bring up the snap-ins after installation, go to SYS:/PUBLIC/WIN 32 > double-click the NWADMIN32 icon.

Installing the Virtual Private Network Client

To access Virtual Private Network (VPN) services from Windows client workstations, you need to install the VPN Client. Installing the Novell Client along with the VPN client is optional but not essential for VPN services. To install the VPN client from the CD, click SETUPEX.EXE under /CL_INST/VPN/EXES or from the server under SYS:/PUBLIC/BRDRMGR/VPN/EXES.

Accessing Novell iManager for Filter Configuration

You can use Novell iManager for filter configuration on NetWare 6 SP 1 only. The Novell BorderManager (NBM) Access Management Role and Packet Filtering Configuration Task is automatically plugged in to Novell iManager during Novell BorderManager 3.7 installation. By default, this role is assigned to the administrator only.

To log in to Novell iManager:

1 In Internet Explorer > go to https://*ipaddress:2200* or use https://*DNS:2200* of the server.

2 Log in to Novell iManager to use the Packet Filtering Configuration Task.

3 When you log in to the Novell iManager you can see the role of NBM Access Management on the left panel. Click NBM Access Management to see the Filter Configuration task.

4 Click the Filter Configuration task to see the NBM Server Selection option.

Setting Up Login Policies

All users logging in to services through Novell BorderManager 3.7 must be authenticated. The type of authentication required for a user to log in and access network services through Novell BorderManager 3.7 is stored in NDS or eDirectory in a Login Policy object. Because of this, you must set up a generic login policy to enable users to access Novell BorderManager 3.7 services. Until a policy is set up, no user access will be allowed. There can be only one Login Policy object in an NDS or eDirectory tree. This object holds the login policies for all Novell BorderManager 3.7 servers and services in the tree.

NOTE: The policies stored in the Login Policy object apply only to Novell BorderManager 3.7 services. Previous versions of Novell BorderManager 3.7 use hardcoded default policies.To manage login polices for all Novell BorderManager 3.7 services using the Login Policy object, you must upgrade previous versions of BorderManager to Novell BorderManager 3.7.

To create a Login Policy object and set up generic policy rules that allow users to access network services through each of the various Novell BorderManager 3.7 services with an eDirectory password, complete the following steps:

1. In NetWare Administrator, select the Security container object in your eDirectory tree.

   The Login Policy object can only be created in the Security container object.

2. From the Object menu, click Create > Login Policy > OK.

3. To configure a login policy rule, click Rules > Add.

4. To configure a rule for Novell BorderManager 3.7 Authentication Services, select the Object name radio button from the Service Type dialog box > browse to select the Dial Access System object associated with that service > check the Enabled check box.

   If this is a new installation of Novell BorderManager 3.7 Authentication Services, you will need to create a Dial Access System object. Refer to “Creating a Dial Access System Object” on page 123 for more information.

5. Select the Users tab > click Add > browse to select the user, group, or container objects to enable access.

6. Select the Methods tab > click Add > check the Login Method enabled check box.

7. In the Method Types dialog box, check NDS or eDirectory Passwords.
8. In the Method Enforcement dialog box, check Mandatory > click OK > Add.
9. To configure a rule for Proxy Services, select the Predefined radio button from the Service Type dialog box > select Proxy > check the Enabled check box.
10. To configure a rule for SOCKS, select the Predefined radio button from the Service Type dialog box > select SOCKS > check the Enabled check box.
11. To configure a rule for VPN, select the Predefined radio button from the Service Type dialog box > select VPN > check the Enabled check box.

    As NDS or eDirectory passwords are a prerequisite for VPN authentication, you only need to define additional method types and enforcement policies if you would like users to be authenticated by additional means such as token devices. (VPN users are always required to enter their NDS or eDirectory passwords.)
12. Exit the utility.

Installing SurfControl

SurfControl* is delivered with Novell BorderManager 3.7 with a 45-day trial subscription. If you plan to create access rules that use SurfControl URL categories, you must install the SurfControl NetWare Loadable Module™ (NLM™) on the BorderManager server. SurfControl includes the list of Internet sites containing content that is inappropriate or counterproductive in the workplace, such as sexually explicit or drug-related material. SurfControl for BorderManager also includes the list of educational sites and the Sports and Entertainment list. SurfControl lists are updated daily.

You can use the SurfControl lists free of charge during the 45-day trial period. At the end of the trial period, you can choose to subscribe to SurfControl and receive updated lists on an ongoing basis. For more information, see the SurfControl Web site at (www.surfcontrol.com).

Novell BorderManager 3.7 Documentation

In addition to this document, further documentation for the Novell BorderManager 3.7 product is available in the online documentation at

www.novell.com/documentation

Web delivery of the online documentation provides convenient access to the most up-to-date documentation available. The online documentation includes the following:

- Overview and planning—Provides an overview of the Novell BorderManager 3.7 services that you use to successfully manage your network borders, discusses the requirements for managing and controlling access to a network border, and includes detailed descriptions of each BorderManager service.
- Administraion—Provides information on Packet Filtering, Network Address Translation, Novell IP Gateway, Proxy Services, Virtual Private Networks, Access Control, and Authentication Services.

Where to Go from Here

The following table lists the default settings for each component service provided by Novell BorderManager 3.7, and provides references to the Novell BorderManager 3.7 documentation for more information.

NOTE: If you upgraded your server, your existing server configuration, with the exception of your VPN configuration, was preserved.

Table 1 Default Configuration for NetWare 5.1 and NetWare 6

Service	Default Setting	Configuration Information
Packet filters	If you selected Yes to secure access to the public network with the packet filtering option during the installation, the public interface is set to deny access by filtering all packets. You must configure exception lists with the FILTCFG utility to allow specific packet types. If you selected No, the public interface is set to permit all access and does not filter any packets. You must configure exception lists with the FILTCFG utility to filter specific packet types.	Refer to Chapter 2, "Setting Up Packet Filters," on page 25. For a detailed list of the default filters, refer to Novell BorderManager 3.7 Overview and Planning Guide in the online documentation.
Network Address Translation (NAT)	Disabled. All incoming and outgoing packets are passed without any translation or modification to the address or port.	Refer to Chapter 3, "Setting Up NAT," on page 41.
Novell IP Gateway	Disabled. The IPX/IP gateway, IP/IP gateway, and SOCKS gateway services are disabled.	Refer to Chapter 4, "Setting Up the Novell IP Gateway," on page 47.

Service	Default Setting	Configuration Information
Proxy Services	Disabled. All Proxy Services are disabled, including Web client acceleration (standard proxy cache), Web server acceleration (HTTP acceleration), network acceleration (ICP hierarchical caching), and all application proxies (HTTP, FTP, FTP Reverse, Mail, News, RealAudio*, DNS, HTTPS, SOCKS, Generic, and Transparent).	Refer to Chapter 5, "Setting Up Proxy Services," on page 61.
Virtual Private Network (VPN)	Disabled. No default VPN connections are set. The previous configuration must be manually preserved. Refer to "Upgrading VPN from a Previous Version" on page 105 for details.	Refer to Chapter 6, "Setting Up Virtual Private Networks," on page 87.
Access control	Disabled. If you enable this feature using NetWare Administrator, the access control list contains one default rule, which denies access from any source to any destination.	Refer to Chapter 7, "Setting Up Access Control," on page 111.
Novell BorderManager 3.7 Authentication Services	No default. You must set up an initial configuration using NetWare Administrator.	Refer to Chapter 8, "Setting Up Authentication Services," on page 121.
Novell BorderManager 3.7 Alert	Default setting is inherited. The alert configuration is inherited from a container higher in the NDS or eDirectory tree.	Refer to Chapter 9, "Setting Up Alert Notification," on page 133.

2 Setting Up Packet Filters

Packet filters provide network-layer security to control the types of information sent between networks and hosts. Novell® BorderManager® supports Routing Information Protocol (RIP) filters, External Gateway Protocol (EGP) and packet forwarding filters to control the service and route information for the common protocol suites, including Internetwork Packet Exchange™ (IPX™) software and TCP/IP.

If you chose to secure the public interfaces of your Novell BorderManager 3.7 server during installation, a set of default filters was configured at that time. If you performed an upgrade, the existing filters were retained and the default filters were added to the filter list.

The default filters block all traffic through the public interfaces except for the traffic being forwarded to and from an enabled Novell BorderManager 3.7 service. Novell BorderManager 3.7 creates exceptions to allow some selected services during installation. This chapter explains the tasks you must complete to configure packet filtering to allow additional services to be routed through the Novell BorderManager 3.7 server.

With Novell BorderManager 3.7 on NetWare® 6 the TCP/IP filters can also be configured through Novell iManager.

The following sections are discussed here:

Packet Filter Prerequisites

Before you begin to configure packet filters for your Novell BorderManager 3,7 server, you should have the following information at hand:

- Your company security policy

  The security policy should define the communication allowed with external sources and between various segments of the corporate intranet.

- Your current network topology

  You need to know the physical layout of the network components.

- Information about other firewall components

  You need to know what other security measures are in place (or will be in place) so that you do not inadvertently circumvent or disable those measures.

Setting Up the Default Filters

If you did not choose to secure the public interfaces of Novell BorderManager 3.7 during installation, you can do so at any time. To set up default filters:

1. At the server console prompt, enter

   LOAD BRDCFG

2. When prompted, select Yes to configure the set of default filters and press Enter.
3. When prompted to launch INETCFG, select No > press Enter.
4. From the Filter Configuration Options menu, select Setup filters on the Public interface > press Enter.
5. Select the Public interface from the list > 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 Novell IP Gateway, Proxy Services, and Virtual Private Networks (VPNs). Filter support for both IPX and TCP/IP is automatically enabled when the default filters are enabled.

To manually enable or disable the Filter Support option for the TCP/IP protocol:

1. At the server console prompt, enter

   ```
   LOAD INETCFG
   ```

2. Select Protocols > TCP/IP > Filter Support > Status.

3. Select Enabled or Disabled > 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 your having to reinitialize the server.

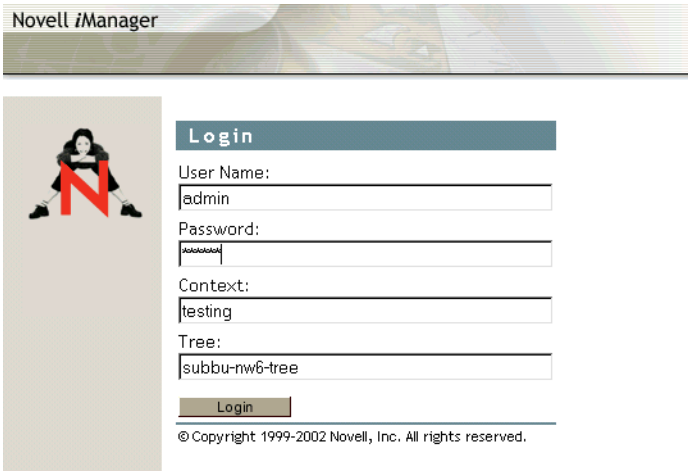
NOTE: This chapter describes the tasks required to set up an initial implementation of Novell BorderManager 3.7 packet filtering. For planning and conceptual information about packet filtering, refer to Novell BorderManager 3.7 Overview and Planning GuideNovell BorderManager 3.7 Overview and Planning Guide, available in the online documentation. Make sure you understand this information before setting up and configuring packet filtering.

Using Novell iManager for Filter Configuration

These sections tell you how to use Novell iManager for filter configuration on NetWare 6. The Novell BorderManager (NBM) Access Management Role and Packet Filtering Configuration Task gets plugged in automatically into Novell iManager during Novell BorderManager 3.7 install. By default this role is assigned to the administrator only.

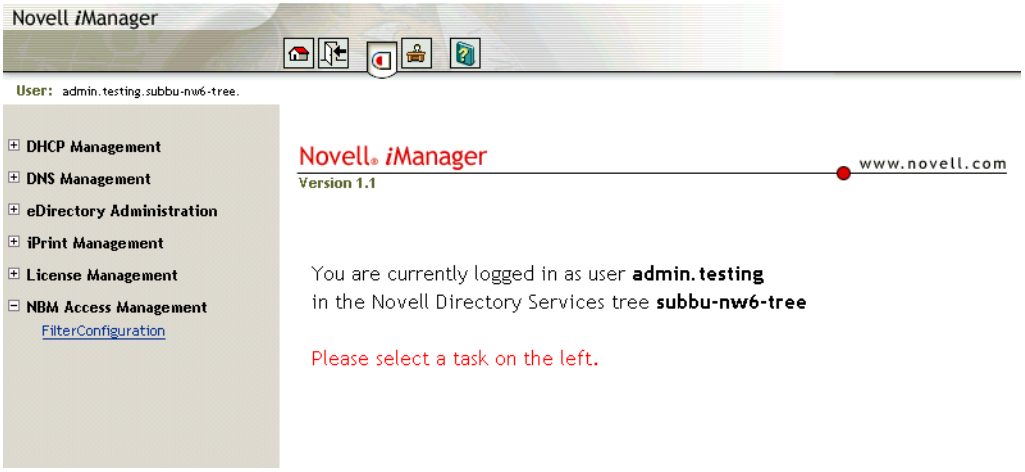
Log in to Novell iManager to use the Packet Filtering Configuration Task.

Figure 1 Novell iManager login screen



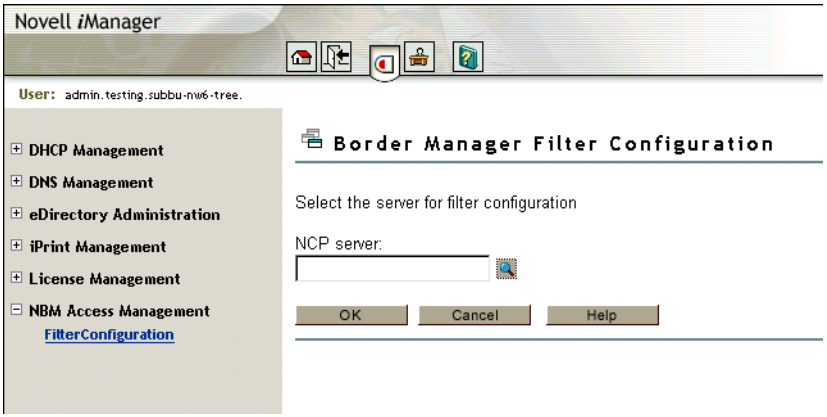
When you log in to the Novell iManager you can see the role of NBM Access Management on the left panel. Click NBM Access Management to see the Filter Configuration task.

Figure 2 NBM Access Management panel



Click the Filter Configuration task to see the NBM Server Selection option.

Figure 3 Server Selection Option screen

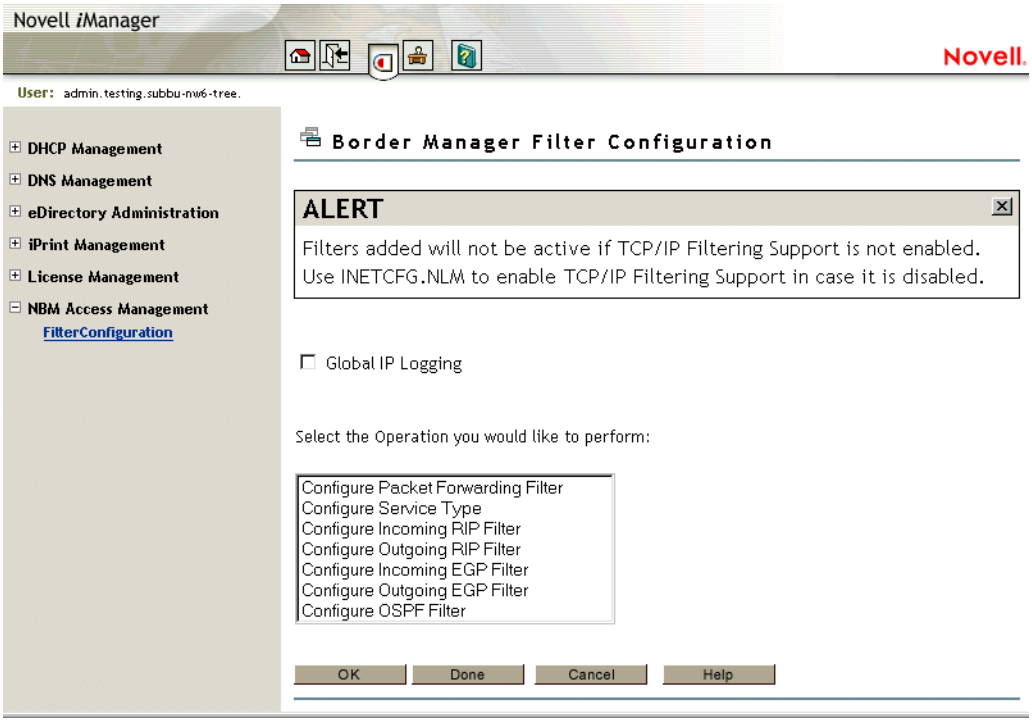


Click object selector icon to find the server you want to select.

Click the server icon.

The selected server will be reflected in the main page. Click OK.

Figure 4 Task list box



Select the task you want to perform from the list box > click OK.

Using FILTCFG for Filter Configuration

These sections tell you how to use FILTCFG on Novell BorderManager 3.7 server:

- “Setting Up Outbound Packet Filter Exceptions” on page 31
- “Setting Up Inbound Packet Filter Exceptions” on page 36
- “Defining Custom Stateful Packet Types” on page 37
- “Saving Filters to a Text File” on page 39
- “Enabling Global IP Packet Logging” on page 39
- “Completing Advanced Setup, Configuration, and Management Tasks” on page 40

Setting Up Outbound Packet Filter Exceptions

Because the default filters don't automatically allow certain packet types to cross the firewall, you may also need to enable filter exceptions to enable other services.

The system-defined packet types enable you to configure stateful packet filter exceptions for the following services:

- DNS over UDP
- DNS over TCP
- FTP
- Ping
- POP3
- Simple Mail Transfer Protocol (SMTP)
- Telnet
- HTTP
- HTTPS

With stateful (dynamic) packet filtering, you only need to define the exceptions that allow specific types of outbound traffic going to specific destinations to be forwarded by the Novell BorderManager 3.7 server. Stateful packet filtering monitors each connection and creates a temporary (time-limited) filter exception for the inbound connection. This allows you to block incoming traffic originating from a particular port number and address, while still allowing return traffic from that same port number and address.

Stateful packet filters track the outgoing packets allowed to pass and allows only the corresponding response packets to return. When the first packet is transmitted to the public network (Internet), a reverse filter is dynamically created. To be counted as a response, the incoming packet must be from the same host and port to which the outbound packet was originally sent.

To configure stateful packet forwarding exceptions to forward outbound traffic through the Novell BorderManager 3.7 server:

1. At the server console prompt, enter

   LOAD FILTCFG

2. From the Filter Configuration Available Options menu, select Configure Interface Options > press Enter.

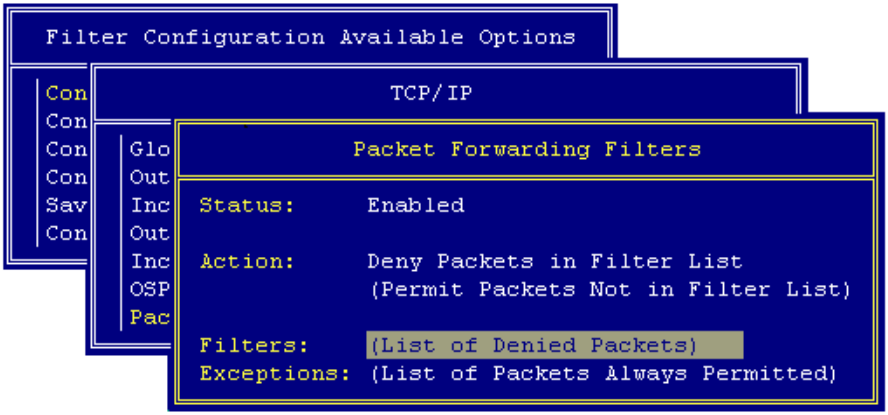
3 Select an interface from the list press Tab to switch between Public and Private.

Any interface listed can be designated as either a public (external) interface or a private (internal) interface.

4 Press Esc > select Configure TCP/IP Filters > Packet Forwarding Filters.

The screen displayed should appear similar to the following.

Figure 5 Packet forwarding filters screen



5 Do the following:

- If the status is Disabled press Enter > select Enabled > 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 > press Enter again. Packets matching the types listed in the filter list will not be forwarded by the Novell BorderManager 3.7 server.

6 Select Filters and 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 > 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:

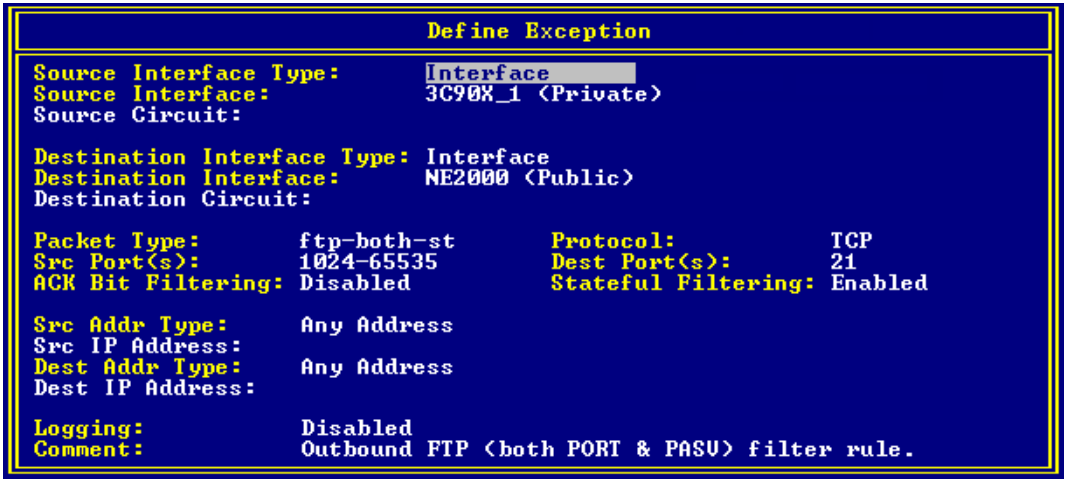
- Secure Sockets Layer (SSL) authentication—TCP port 443.
- Dynamic TCP—TCP ports 1024 to 65535.
- Dynamic UDP—UDP ports 1024 to 65535.
- VPN master/slave (IPX/TCP)—TCP port 213.
- VPN client authentication—TCP port 353.
- VPN keep-alive—UDP port 353.
- VPN Simple Key Management for Internet Protocol (SKIP) Protocol 57.
- Web proxy cache (WWW-HTTP)—TCP port 80.

NOTE: Although the default filter exceptions allow certain VPN-related packets to be forwarded, the default VPN exceptions do not allow encrypted packets to be routed from one VPN member to another. The filters for the VPN tunnels must be updated each time you configure a VPN server. For more information, refer to "Completing Advanced Setup, Configuration, and Management Tasks" on page 40, and Virtual Private Network 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.

Figure 6 Define Exception screen



10 Select Source Interface Type > press Enter.

11 Select Interface or Interface Group > press Enter.

12 Select Source Interface > press Enter.

13 Select the Novell BorderManager 3.7 server's private interface or interface group > press Enter.

14 If you selected a WAN interface, select Source Circuit and 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 > press Enter.

16 Select Interface or Interface Group > press Enter.

17 Select Destination Interface > press Enter.

18 Select the Novell BorderManager 3.7 server's public interface or interface group > press Enter.

19 If you selected a WAN interface, select Destination Circuit > 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 > 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 > enter 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 > enter the host or network address.

25 (Optional) For Logging, press Enter and change the status from Disabled to Enabled.

26 (Optional) Enter a comment in the Comment field describing the purpose of the filter. Press Esc > select Yes to save the filter. Press Esc until you are prompted to exit FILTCFG.

IMPORTANT: If you enabled logging for a filter exception, you must also enable global logging for TCP/IP. Both global logging and logging for the specific filter exception must be enabled for logging to occur.

Setting Up Inbound Packet Filter Exceptions

If you elected to secure the Novell BorderManager 3.7 server's public interface and support Novell IP Gateway or SOCKS clients, you may be required to enable inbound packet filter exceptions to allow them to connect through the public interface. Novell IP Gateway clients connect through TCP port 8224 and port 8225, and SOCKS clients connect through TCP port 1080.

To configure packet forwarding exceptions to forward inbound Novell IP Gateway and SOCKS traffic go through the Novell BorderManager 3.7 server's public interface:

1 At the server console prompt, enter

```
LOAD FILTCFG
```

2 Select Configure TCP/IP Filters > Packet Forwarding Filters.

3 Select Exceptions > press Enter to display the exceptions list.

4 Press Ins to define a new inbound packet forwarding filter exception.

5 Configure the exception for Novell IP Gateway clients as follows:

5a Select Source Interface Type and press Enter.

5b Select Interface or Interface Group and press Enter.

5c Select Source Interface and press Enter.

5d Select the Novell BorderManager 3.7 server's public interface or interface group and press Enter.

5e Select Packet Type > press Enter.

5f Press Insert to define a new TCP/IP packet type.

5g Select Name and enter a name for the packet type.

5h Select Protocol and press Insert.

5i Select TCP from the list of commonly used Internet protocols.

5j Accept <All> for the Source Port(s).

5k Select Destination Port(s) and enter 8224-8225.

5l Select Comment and enter a description of the packet type, such as Novell IP Gateway Client or SOCKS client.

5m Press Esc to add the packet type to the top of the packet list.

5n Select the packet type you added.

5o Select Dest Addr Type and change the setting from Any Address to Host.

5p Select Dest IP Address and enter the IP address assigned to the Novell BorderManager 3.7's public interface.

5q (Optional) Select Comment and enter a description of the filter.

5r Press Esc to add the exception.

6 Configure the exception for SOCKS clients.

7 Press Esc until you are prompted to exit FILTCFG.

Defining Custom Stateful Packet Types

The Novell BorderManager 3.7 firewall has many static packet types defined in addition to the stateful packet types listed in "Setting Up Outbound Packet Filter Exceptions" on page 31. Static packet types are those without -st in their names. A static packet type is used to define a filter operating on traffic in one direction only. For example, instead of creating a stateful packet filter in one direction and relying on the system to enable the time-limited filter in the reverse direction, you can create two static packet filters, one for packets flowing in each direction. However, stateful packet filters provide more security than static packet filters.

If the stateful packet types already defined by the Novell BorderManager 3.7 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, complete the following steps:

1 From the Defined TCP/IP Packet Types window, press Insert.

2 Enter 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, enter the source and destination port number or range of port numbers.

5 Do not change the default setting of Disable for ACK Bit Filtering.

Because ACK bit filtering automatically occurs when stateful packet filtering is enabled, you don't need to enable ACK bit filtering separately. The software will 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:

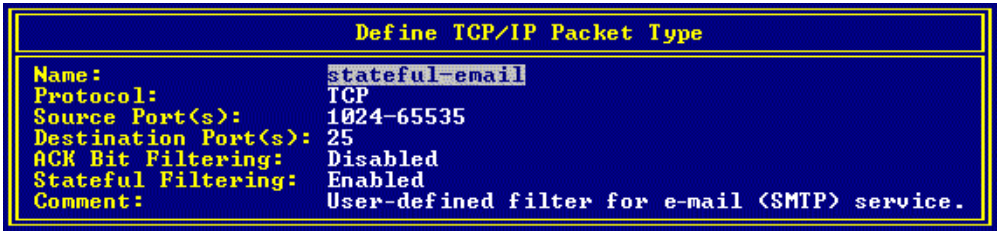
- Enabled
- Enabled for Active FTP only (PORT)
- Enabled for Passive FTP only (PASV)

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) Enter a comment to describe the packet type.

The TCP/IP packet type definition will look similar to the following.

Figure 7 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.

Saving Filters to a Text File

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

1. At the server console prompt, enter

   LOAD FILTCFG

2. Select Save Filters to a Text File.
3. Enter the filename to which the filters will be saved.
4. Pres Esc to exit FILTCFG.

Enabling Global IP Packet Logging

The Global Logging flag allows you to turn logging on and off for all filters within a specific protocol, such as TCP/IP. If this flag is not enabled, no logging will occur, even if the log flag has been enabled for a specific filter or exception. Packet logging records the activity of the individual filters specified in the filter lists or the exception lists.

NOTE: Logging options can slow server performance. Consider disabling logging after you have tested your filters and exceptions.

To enable global IP logging:

1. At the server console prompt, enter

   LOAD FILTCFG

2. Select Filter Configuration Available Options > Configure TCP/IP Filters > Global IP Logging > Status.
3. Select Enabled > press Enter.

   NOTE: When Global IP Logging is enabled, logging activity will start. If you want to log the activity of a particular filter, you must enable both Global IP Logging and the packet logging option for that filter.

4. Press Esc until you are prompted to exit FILTCFG.

Completing Advanced Setup, Configuration, and Management Tasks

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

- Setting up an HTTP filter
- Setting up an FTP filter
- Setting up a Telnet filter
- Setting up an SMTP filter
- Setting up a POP3 filter
- Modifying default IP packet logging parameters
- Viewing IP packet log information

3 Setting Up NAT

Novell® BorderManager® 3.7 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 three modes: dynamic only, static only, or a combination of static and dynamic.

Dynamic-only mode is used to allow clients on your private network to access a public network, such as the Internet.

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.

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 chapter contains the following sections:

NOTE: This section describes the tasks required to set up an initial implementation of Novell BorderManager 3.7 NAT. For planning and conceptual information about

NAT, refer to the Novell BorderManager 3.7 Overview and Planning Guide , available in the online documentation. Make sure you understand this information before setting up and configuring NAT.

NAT Prerequisites

Before configuring NAT, verify that the following prerequisites have been met:

- A registered IP address has been obtained for each public interface on the server.
- TCP/IP has been enabled for and bound to two interface boards (the public and private interfaces).

  If your Novell BorderManager 3.7 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 3.7 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 3.7 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.

Settting Up NAT on a Single Interface

To enable and set up NAT on a LAN or WAN interface:

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, enter the public IP address to which a private address is mapped.

   7d. In the Private Address field, enter the IP address of the private host that you want public hosts to access using the public IP address.

   7e. Press Esc to add the entry to the NAT table.

   7f. For address translation of inbound requests, repeat the steps for each private host to be accessed by public hosts.

   7g. (Optional) If you selected Static Only, for address translation of outbound requests, repeat the steps for each private host that you want to have access to the Internet through the NAT-enabled interface using a public address.

   The public addresses can be on the same network or subnetwork as the primary IP address, or they can be on a different network or subnetwork. If the public addresses are on the same network or subnetwork, use multihoming, as described in “Setting Up NAT with Multihoming” on page 44, to add secondary addresses to the NAT-enabled interface.

Each private host address can be mapped to only one public host address. To access IP hosts using the public address within the private network, ensure that the static address pair specifies the same address for both the public and private addresses.

If NAT is connected to the Internet using multi-access WAN links, you must add static routes on your external router so that packets that are destined to one of the public addresses can be routed to the NAT interface.

8. If you set Status to Static Only or Static and Dynamic, configure a secondary address for each public address you configured in the network address translation table.

   Refer to "Setting Up NAT with Multihoming" on page 44 for instructions on how to configure a secondary address.

9. Press Esc until you are prompted to update your changes, then select Yes.
10. Press Esc until you are prompted to exit INETCFG, then select Yes.
11. If you want the NAT configuration to take effect immediately, bring down and restart the server.

Setting Up NAT with Multihoming

Multihoming enables a server to have multiple IP addresses. Multihoming can be achieved by adding a secondary IP address to an existing interface or by physically adding another interface to the server and binding another IP address to it.

A secondary IP address added to an existing interface must be on the same network as the IP address already bound to that interface. If there are multiple interfaces and the secondary IP address being added is not valid on any of the existing networks, the address is rejected and an error message appears on the server console. For example, if the IP addresses 130.57.0.1 and 10.0.0.1 are bound to two interfaces and you attempt to add 172.16.1.1 as a secondary IP address, it will be rejected because it does not belong to the same network as 130.57.0.1 or 10.0.0.1.

Multihoming is required for NAT when static mode is used. For an example of using multihoming with NAT, refer to the NAT online documentation. For information about how to set up NAT for a particular implementation with Proxy Services or the Virtual Private Network (VPN), refer to the Chapter 5, "Setting Up Proxy Services," on page 61 or Chapter 6, "Setting Up Virtual Private Networks," on page 87.

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:

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 > bind one IP address to the public interface under Bindings.
4. Press Esc until you are prompted to save your changes > select Yes.
5. Select Manage Configuration > 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 it at the server console.

7. To delete or display secondary IP addresses, press Alt+Esc until the server console prompt is displayed.

   You can delete secondary IP addresses by entering the following command:

   DELETE SECONDARY IP ADDRESS *n.n.n.n*

   where *n.n.n.n* is your server's secondary IP address.

   Ensure that when you delete secondary IP addresses, the corresponding commands are also removed from AUTOEXEC.NCF.

   You can display secondary IP addresses by entering the following command:

   DISPLAY SECONDARY IP ADDRESS

Completing Advanced Setup, Configuration, and Management Tasks

In addition to the basic setup procedures described in this chapter, there are several advanced setup, configuration, or management procedures you might need to complete, depending on your specific configuration. Advanced tasks are available in the NAT online documentation and include the following:

- Using NAT within a private network
- Managing NAT

4 Setting Up the Novell IP Gateway

The Novell® IP Gateway enables Internetwork Packet Exchange™ (IPX™) and IP clients on your local network to access the Internet without requiring you to assign globally unique IP addresses to each local system. The Novell IP Gateway also supports SOCKS clients. In addition, the Novell IP Gateway enables you to hide the IP addresses of your local network from the Internet and implement access control for local clients.

This section explains the tasks you complete to set up the Novell IP Gateway of Novell BorderManager® 3.7.

NOTE: This chapter describes the tasks required to set up an initial implementation of the Novell IP Gateway. For planning and conceptual information about the Novell IP Gateway, refer to the Novell BorderManager 3.7 Overview and Planning Guide, available in the online documentation. Make sure you understand this information before setting up and configuring the Novell IP Gateway.

Novell IP Gateway Prerequisites

Before you set up the Novell IP Gateway, you must meet the following prerequisites:

Server Prerequisites

Before setting up the Novell IP Gateway, verify that the following prerequisites have been met for the gateway server:

- A registered IP address has been obtained for each public interface.
- TCP/IP has been enabled for one or more interface boards (accomplished by successful Novell BorderManager 3.7 installation).
- For interfaces that have TCP/IP enabled, IP packet forwarding 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 set up static routing from the server console, load INETCFG, select Protocols > TCP/IP enable LAN Static Routing > select LAN Static Routing Table to enter static routes.
- (For IPX™/IP gateway service only) The IPX protocol has been set up and bound to at least one interface.

  To set up IPX from the server console, load INETCFG > select Protocols > IPX. To bind IPX to an interface on the server, load INETCFG and select Bindings.
- An Internet Service Provider (ISP) connection has been set up with enough bandwidth for the number of users on your network.

  If the Novell BorderManager 3.7 server does not provide the connection to the ISP, ensure that the server has a static route set up or that the router to the ISP is in the Novell BorderManager 3.7 server's routing path.
- Novell Public Key Infrastructure (PKI) Services and Secure Authentication Service (SAS) have been installed on the server to support Secure Sockets Layer (SSL) authentication of SOCKS 5 clients.

  PKI and SAS are installed automatically during Novell BorderManager 3.7 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 task:

  - 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

More information about Novell PKI Services and certificate authorities is located in the NetWare online documentation.

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

- Domain Name System (DNS) Resolver setup has been performed to provide a valid domain name for the DNS and an IP address of at least one DNS name server to resolve IP hostnames. This should have been done by you during the BorderManager product installation. If the DNS Resolver has not been set up, refer to "Novell IP Gateway Prerequisites" on page 47.
- Packet filtering has been set up to allow DNS query and response packets.

  Default installation sets packet filtering to block all incoming and outgoing traffic. To modify the packet filtering setup, refer to Chapter 2, "Setting Up Packet Filters," on page 25.

Setting Up the DNS Resolver

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

1. Enter **`LOAD NIASCFG`**, then select Configure NIAS > Protocols and Routing > Protocols > TCP/IP > DNS Resolver Configuration.
2. Enter the DNS domain name for your corporation or organization.

   Your ISP typically supplies this name. Domain names usually take the form company_name.com or organization.org. For example, novell.com or acme.org.
3. Enter 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. Pres Esc until you return to the Internetworking Configuration menu > select Reinitialize System and exit NIASCFG.

Client Prerequisites

Client prerequisites are provided in the following sections:

- “Novell IP Gateway Prerequisites” on page 47

Novell IP Gateway Administration Prerequisites

The client used by an administrator to set up Novell IP Gateway services must have the following installed:

- Windows 98, Windows* 2000, Windows* XP, Windows* Me or Windows* NT.
- The Novell Client™ for Windows software
- The Novell BorderManager 3.7 snap-in modules to NetWare Administrator
- If the Novell IP Gateway's SOCKS service will be set up to use SSL, a Novell PKI Services snap-in module to NetWare Administrator

NOTE: The Novell BorderManager 3.7 and PKI snap-in modules can be installed on the server instead of the client. This is preferable if an administrator uses multiple client machines but has a login script to consistently map a drive to the directory from which NetWare Administrator is run (the same directory where the snap-in modules are installed).

IPX/IP Gateway Client Prerequisites

A client accessing the Internet using the IPX/IP gateway service must have the following installed:

- Windows 98, Windows 2000, Windows XP, Windows Me or Windows NT
- The Novell Client for Windows software
- The Novell IP Gateway component of the Novell Client software

IP/IP Gateway Client Prerequisites

A client accessing the Internet using the IP/IP gateway service must have the following installed:

- Windows 98, Windows 2000, Windows XP, Windows Me or Windows NT

- The Novell TCP/IP stack (for Windows 3.1 clients) or the Microsoft* TCP/IP stack (for all other Windows clients)
- The Novell Client for Windows software
- The Novell IP Gateway component of the Novell Client software

SOCKS Client Prerequisites

A SOCKS client accessing the Internet using the Novell IP Gateway SOCKS service does not need special configuration. However, to enable the Novell IP Gateway to verify or authenticate SOCKS users, the following is required:

- An administrator must create a User object in NDS or eDirectory for each SOCKS user.

  A SOCKS user who also uses Novell Client software already has a User object. However, SOCKS users whose client machines are UNIX*, Macintosh*, or OS/2*, most likely require a new User object.
- The usernames and passwords created in NDS or eDirectory should match the usernames and passwords SOCKS 5 clients already use to avoid confusion. This prerequisite does not apply to SOCKS 4 users because they do not have to use passwords for authentication.

Setting Up the Novell IP Gateway

The Novell IP Gateway is comprised of two circuit-level gateways:

- The IPX/IP gateway, which provides IPX clients with secure, controlled access to the Internet.
- The IP/IP gateway, which provides Windows-based IP clients with secure, controlled access to the Internet.

When the Novell IP Gateway is set up to act as a SOCKS server, it can also be used to authenticate SOCKS clients and determine their access to network resources using access control rules stored in the NDS or eDirectory database.

NOTE: The IPX/IP gateway, IP/IP gateway, and SOCKS services can be enabled to run simultaneously on the same server. This permits Windows clients, as well as SOCKS clients, to access the Internet through the same Novell BorderManager 3.7 server.

All three gateway services are set up using NetWare Administrator. For detailed instructions, refer to the following procedure:

- “Setting Up the Novell IP Gateway” on page 51

Setting Up the IPX/IP or IP/IP Gateway Service

You can set up the IPX/IP gateway service to support the use of TCP/IP applications by Windows clients that do not have an assigned IP address. You can set up the IP/IP gateway service to support NDS or eDirectory access control for networks whose clients use TCP/IP.

To set up the IPX/IP or IP/IP gateway service:

1. In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. Click the Gateway tab.
3. Under Enable Service, check the IPX/IP Gateway or IP/IP Gateway check box.
4. (Optional) If you want to assign a different port number for gateway traffic, complete the following substeps to change the gateway service port:

   4a. Under Enable Service, double-click the gateway whose service port is to be changed, or highlight the gateway and click Details.

   4b. Under Service Attributes, enter a different port number in the Service Port field.

   By default, both gateways use port 8225 (decimal). Although changing the service port is not recommended, if another service is using this port, you can assign a different port number for gateway traffic.

5. (Optional) If you want to enable single sign-on authentication for the IPX/IP gateway service, check the Single Sign On Authentication check box under Service Attributes.

   Single sign-on authentication enables the IPX/IP gateway to perform a background user authentication if the user has already logged in to NDS or eDirectory. With single sign-on, users are not required to provide a username and password to access resources through the gateway. If single sign-on is not enabled, the Novell IP Gateway software performs a secondary authentication when a user attempts to access resources using the IPX/IP gateway service, regardless of whether the user has already logged in.

   NOTE: Single sign-on applies to the IPX/IP gateway service only. Single sign-on is ignored when the IP/IP gateway service is used.

6 Click OK twice to close the Configure Gateway Services window and the Novell BorderManager 3.7 Setup page.

When you close the Novell BorderManager 3.7 Setup page, the server loads IPXIPGW.NLM, the gateway NLM file, and creates a Gateway Server object in the NDS or eDirectory tree.

Refer to Chapter 7, "Setting Up Access Control," on page 111 for information about setting up and using access control with the Novell IP Gateway.

IMPORTANT: Access control rules set up for the Server object using IPX/IP gateway software released before Novell BorderManager 3.7 will no longer operate after you upgrade your server to Novell BorderManager 3.7 and enable the Novell IP Gateway. To take effect, these rules must be set up again for the Server object.

Setting Up the SOCKS 4 or SOCKS 5 Service

If you have SOCKS 4 or SOCKS 5 clients on your network and want to control their access to the Internet through the Novell IP Gateway, you must set up the SOCKS service.

As part of the configuration procedure, you must either specify SOCKS 5 authentication parameters or enable SOCKS 4 user verification, or do both, if your network has a combination of SOCKS 4 and SOCKS 5 clients.

To set up the SOCKS service on the Novell IP Gateway:

1 In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.

2 Select the Gateway tab.

3 Under Enable Service, check the SOCKS V4 and V5 check box.

4 (Optional) If you want to assign a different port number for SOCKS traffic, complete the following substeps to change the gateway service port:

4a Under Enable Service, double-click SOCKS V4 and V5, or highlight SOCKS V4 and V5 and click Details.

4b In the Service Port field, enter a different port number.

By default, the SOCKS service uses port 1080 (decimal). Although changing the service port number is not recommended, if another service is using this port, you can assign a different port number for SOCKS traffic.

IMPORTANT: If you change the service port number, you must modify the setup of all SOCKS clients to use the new port number.

4c Click OK to close the Configure SOCKS V4 and V5 window.

5 Set SOCKS 5 authentication parameters by completing the following substeps:

5a Under Enable Service, double-click SOCKS V4 and V5, or highlight SOCKS V4 and V5 > click Details.

5b Under SOCKS V5 Authentication, select any or all of the following authentication schemes (listed in order of lowest to highest priority):

An additional method of authentication is available for SOCKS 5 client users. SOCKS 5 client users can use security devices such as hardware tokens in addition to using their 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. See the Authentication Services online documentation for more information.

IMPORTANT: If multiple authentication schemes are selected, the Novell IP Gateway uses the highest priority scheme that the client is capable of performing.

- None—This option is equivalent to the null authentication option for SOCKS 5 clients. No authentication is required by the Novell IP Gateway.
- Clear Text User/Password—When the Novell IP Gateway authenticates a user, the user's password is transmitted across the wire in clear text without any encryption. The password is checked against the user's password stored in NDS or eDirectory, but this is not the same as NDS or eDirectory authentication. Because a password that is transmitted in clear text is insecure, this option should be used only if SSL is also selected to encrypt the password before it is transmitted.
- NDS or eDirectory User/Password—When the Novell IP Gateway authenticates a user, the user's password is never transmitted across the wire. Instead, similar to the authentication of a Novell client, the password is used to generate a secure key pair. Successive challenge handshakes between the client and the server complete the authentication. An NDS or eDirectory authentication option must be available in the SOCKS client for this authentication scheme to work.
- SSL—This option requires that an SSL connection between the client and the server must be established before the Novell IP

Gateway can authenticate a user with any of the other authentication schemes. SSL uses a public key/private key encryption system. Enabling this option also ensures the encryption of all data transmitted between the client and the server.

IMPORTANT: If SSL and access control are both enabled for the Novell IP Gateway, you must also select NDS or eDirectory User/Password or Clear Text User/Password because the SSL protocol does not perform user authentication for NDS or eDirectory access control.

5c (Optional) If you selected Clear Text User/Password as an authentication scheme, click Authentication Context > Context > Add > enter the user's default NDS or eDirectory context and tree > click OK.

Enter 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.

5d (Optional) If you selected SSL as an authentication scheme, use the Key ID pull-down menu to select from a list of available files.

NOTE: A key ID file is available only after you create a KMO in NDS or eDirectory for the server using NetWare Administrator. For more information about how to create a KMO, refer to the PKI online help in NetWare Administrator or the PKI information located in the NetWare online documentation.

5e (Optional) Enable single sign-on for SOCKS 5 clients by checking the Single Sign On check box under SOCKS V5 Authentication.

This option is provided for clients that use both the Novell Client for Windows and a third-party SOCKS 5 client on the same workstation. If a user has already authenticated to NDS or eDirectory by logging in from a Novell client and attempts to use a SOCKS 5 client to access the Internet through the Novell IP Gateway, the gateway does not authenticate the user again.

For single sign-on to occur, the client machine must be running CLNTRUST.EXE and DWNTRUST.EXE. For more information about these files, refer to "Setting Up Gateway Clients" on page 56.

NOTE: If single sign-on is enabled but the user has not logged in to NDS or eDirectory or is limited to the use of a SOCKS 5 client, the gateway will authenticate the user with one of the authentication schemes. If single sign-on fails and no authentication scheme has been selected, the user's connection is dropped.

5f Click OK to close the Configure SOCKS V4 and V5 window.

6 Enable SOCKS 4 user verification by completing the following substeps:

6a Under Enable Service, double-click SOCKS V4 and V5, or highlight SOCKS V4 and V5 > click Details.

6b Check the check box for SOCKS V4 User Verification.

SOCKS 4 user verification requires the Novell IP Gateway to verify that the user exists in NDS or eDirectory, but the gateway does not authenticate the user. The user does not need to provide a password to gain access to the Internet through the gateway.

6c Click OK to close the Configure SOCKS V4 and V5 window.

7 Click OK to close the Novell BorderManager 3.7 Setup page.

Refer to Chapter 7, "Setting Up Access Control," on page 111 for information about setting up and using access control with the Novell IP Gateway.

NOTE: NDS or eDirectory-based access rules for SOCKS clients can restrict access sites only and not to specific URLs. For content filtering, use SurfControl* installed on the Novell BorderManager 3.7 server.

Setting Up Gateway Clients

The Novell IP Gateway client software must be set up on each Windows workstation that accesses the Internet through the gateway server. This task is typically the responsibility of the network administrator or the person responsible for desktop administration and support. In some cases, users set up their own gateway client software.

All gateway clients must have the gateway component of the Novell Client software installed and set up. The gateway component is installed by selecting a custom client installation and selecting Novell IP Gateway from the list of additional components to install.

All clients using the IP/IP gateway must have a TCP/IP stack installed and set up.

Refer to the following procedures for setting up Novell IP Gateway clients:

- "Setting Up Gateway Clients" on page 56

Setting Up Windows NT or Windows 98 Clients

To enable the gateway client software on Windows NT or Windows 98 clients and set up a preferred gateway server:

1. Right-click Network Neighborhood > select Properties.
2. To set up a Windows 98 client, select the Configuration tab and click Novell IP Gateway.

   or

   To set up a Windows NT client, select the Protocols tab > click Novell IP Gateway in the Network Protocols list.

   If you do not see Novell IP Gateway in the list, you probably do not have the gateway client component installed on your workstation. Do not continue with this procedure until you have installed the Novell Client software provided with the Novell BorderManager 3.7 product. For more information, refer to "Installing the Novell Client Software" on page 17.
3. Click Properties > check the Enable Gateway check box.
4. In the Preferred Server field > the preferred gateway server.

   The correct syntax for the gateway server is the server name with -GW appended to it. You must also include the server's context with a leading period. For example, if the Novell IP Gateway is enabled on the server SJ-NW5 whose context is docs.novell, specify the preferred gateway server as .SJ-NW5-GW.docs.novell.
5. In the Preferred Tree field, enter the NDS or eDirectory tree where the server is located > click OK.
6. Restart the workstation.

Setting Up SOCKS Clients

A workstation running the Novell Client software and a SOCKS application is considered a SOCKS client.

To enable a SOCKS client to use the Novell IP Gateway SOCKS service, the IP address or hostname of the Novell BorderManager 3.7 server is typically set up in the SOCKS application to identify the Novell BorderManager 3.7 server as the SOCKS server.

SOCKS applications might also require the following to be set up:

- Destinations
- Redirection rules
- DNS hostname resolution
- Authentication schemes

For more specific information, refer to the documentation provided with your SOCKS applications.

Setting Up Clients to Use Single Sign-On Enabled on the Gateway Server

When single sign-on is enabled, the Novell IP Gateway software can perform background NDS or eDirectory authentication for Windows 98, Windows NT clients, and SOCKS 5 clients that have the NDS or eDirectory authentication capability. With single sign-on enabled on the server, a user who is already logged in is not presented with a login dialog box to use the Novell IP Gateway's IPX/IP gateway or SOCKS services.

Before single sign-on can occur, the client workstations must be running CLNTRUST.EXE and DWNTRUST.EXE. CLNTRUST.EXE enables the client to be authenticated in the background, and DWNTRUST.EXE stays resident on the client to terminate CLNTRUST.EXE after a user logs out.

These files are located in the SYS:PUBLIC directory on the server. The gateway component of the Novell Client does not run these files automatically, nor does the SOCKS 5 client software. Although these files can be copied to client machines and run by batch files before users log in to NDS or eDirectory, it is more effective to create a login script for each user you want to be authenticated using the single sign-on feature. By implementing a login script, when a user logs in to NDS or eDirectory from any workstation, that workstation automatically runs DWNTRUST.EXE and CLNTRUST.EXE.

To create a login script:

1. In NetWare Administrator, right-click the container object where you want to create a login script and select Details.
2. Select Login Script.
3. In the login script field, enter the following lines that apply to the operating systems on users' workstations, where Server_Name is the name of your server:

```
If OS= WINNT THEN

# Server_Name\SYS\PUBLIC\DWNTRUST.EXE

# Server_Name\SYS\PUBLIC\CLNTRUST.EXE

END

IF OS = "WIN95" THEN

#  Server_Name\SYS\PUBLIC\DWNTRUST.EXE

#  Server_Name\SYS\PUBLIC\DWNTRUST.EXE

END

IF OS = "WIN98" THEN

#  Server_Name\SYS\PUBLIC\DWNTRUST.EXE

#  Server_Name\SYS\PUBLIC\CLNTRUST.EXE

END
```

4. Click OK to close the Login Script page, the Details page, and exit NetWare Administrator.

Setting Up Clients to Use the Gateway Client Transparent Proxy

Because the Gateway Client Transparent proxy feature is enabled by default, no configuration is required. When a user logs in to NDS or eDirectory, the gateway component of the Novell Client software locates all the proxy servers that the user has permission to access. If the user starts a browser session, the Novell IP Gateway client connects to the first proxy server it finds during its search of the NDS or eDirectory database and does not make a connection through the Novell IP Gateway.

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 Novell IP Gateway online documentation and include the following:

- Setting up logging for all gateway services
- Decoding gateway packet traces

- Checking gateway real-time activity
- Checking the access control log
- Viewing user statistics
- Viewing host statistics
- Exporting data
- Checking the information log

5 Setting Up Proxy Services

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.

You can use the service as an application proxy for such services as HTTP, Gopher, FTP, Simple Mail Transfer Protocol (SMTP), Domain Name System (DNS), RealAudio*, and Real Time Streaming Protocol (RTSP). You can also use the service as a protocol filter to prevent certain kinds of user connections or as a gateway to hide the names and addresses of internal systems so that the gateway is the only hostname known outside the system.

This section explains the tasks you complete to set up Novell® BorderManager® 3.7 Proxy Services.

- "Setting Up the SOCKS Client (Upstream)" on page 78
- "Setting Up HTTP Transparent Proxy" on page 80
- "Setting Up Telnet Transparent Proxy" on page 81
- "Setting Up Proxy Authentication" on page 81
- "Completing Advanced Setup, Configuration, and Management Tasks" on page 84

NOTE: This section describes the tasks required to set up an initial implementation of the Proxy Services. For planning and conceptual information about Proxy Services, refer to the Novell BorderManager 3.7 Overview and Planning Guide, available in the online documentation. Make sure you understand this information before setting up and configuring Proxy Services.

Proxy Services Prerequisites

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

- IP addresses of your server's IP interfaces, and which are considered private or public access
- Port number (8080 by default) and the hostname or IP address of the Novell BorderManager 3.7 proxy server

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

- DNS Resolver setup has been performed to provide a valid domain name for the DNS and an IP address of at least one DNS name server to resolve IP hostnames. This should have been done by you during the Novell BorderManager 3.7 product installation. If the DNS Resolver has not been set up, refer to "Novell IP Gateway Prerequisites" on page 47.
- Packet filtering has been set up to allow DNS query and response packets.

  Default installation sets packet filtering to block all incoming and outgoing traffic. To modify the packet filtering setup, refer to Chapter 2, "Setting Up Packet Filters," on page 25.
- Corporate users who will use Proxy Services to access Internet Web sites have set up their Web browsers to use the Novell BorderManager 3.7 proxy server, as described in the following sections:
  - "Proxy Services Prerequisites" on page 62

You can also use the Novell BorderManager 3.7 HTTP Transparent proxy feature to set up background, automatic proxy services. With HTTP Transparent proxy, users are not required to configure their browsers to use a proxy; it is done invisibly for them. For more information about using HTTP Transparent proxy, refer to "Setting Up HTTP Transparent Proxy" on page 80.

- The Novell IP Gateway client software should be set up on each Windows* client that will need to access Internet services and destinations through the Novell IP Gateway. For more information, refer to Chapter 4, "Setting Up the Novell IP Gateway," on page 47.
- Novell Public Key Infrastructure (PKI) Services and Secure Authentication Service (SAS) should be installed on the server to support Secure Sockets Layer (SSL) authentication of SOCKS 5 clients.

  PKI and SAS are installed automatically during Novell BorderManager 3.7 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 task:

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

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

Setting Up the DNS Resolver

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

1. Enter **`LOAD NIASCFG`**, then select Configure NIAS > Protocols and Routing > Protocols > TCP/IP > DNS Resolver Configuration.
2. Enter the DNS domain name for your corporation or organization.

Your Internet Service Provider (ISP) typically supplies this name. Domain names usually take the form company_name.com or organization.org, for example, novell.com or acme.org.

3. Enter 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 NIASCFG.

Setting Up Microsoft Internet Explorer to Use a Web Proxy

To specify the Novell BorderManager 3.7 proxy server on a Microsoft* Internet Explorer Web browser:

1. Launch Internet Explorer, then select one of the following menu paths, based on the software version.

   - For Internet Explorer 5.5, select Tools > Internet Options > Connections > LAN Settings > Use a Proxy Server

2. Enter the port number (8080 by default) and hostname—or IP address—of the Novell BorderManager 3.7 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 one of the following menu paths, based on the software version.

   - For Internet Explorer 5.5, select Tools > Internet Options > Connections > LAN Settings > Use a Proxy Server > click Advanced > check the check box Use the Same Proxy for All Protocols.

2. Enter the port number (8080 by default) and hostname—or IP address—of the Novell BorderManager 3.7 proxy server in the proxy field.

3. Click Apply.

Setting Up Netscape Navigator to Use a Web Proxy

To specify the Novell BorderManager 3.7 proxy server on a Netscape Navigator* 3.*x* Web browser, complete the following steps:

1. Launch Netscape Navigator, then select Options > Network Preferences > Proxies > Manual Proxy Configuration.
2. Click View.
3. Enter the hostname—or IP address—and port number (8080) of the Novell BorderManager 3.7 proxy server in the proxy field.
4. Click OK.

To specify the Novell BorderManager 3.7 proxy server on a Netscape Navigator 4.*x* Web browser, complete the following steps:

1. Launch Netscape Navigator, then select Edit > Preferences > Advanced > Proxies > Manual Proxy Configuration > View.
2. Enter the URL of the Novell BorderManager 3.7 proxy server in the URL field.
3. Click OK.

Setting Up an HTTP Proxy Server

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

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

To set up an HTTP proxy server:

1. In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. From the Application Proxy tab, check the HTTP Proxy check box.
3. Click Details or double-click the HTTP Proxy service.
4. Click the HTTP tab > enter the number of the HTTP listening port.

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

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

5. Specify whether to do the following:

   - Ignore refresh requests from the browser.

     If you select this option, the proxy will not access the Web server to refetch a URL when a user specifies to reload or refresh from the browser. All user requests will be filled from the cache.

   - Filter cookies.

     If you select this option, the cookie header is not forwarded to the origin server, and pages with the Set-Cookie header are not cached. Enable this option to increase security.

   - Enable persistent connections to browsers.

     If you select this option, the connection between a browser and a proxy server remains active even if there is no data flow.

   - Enable persistent connections to origin servers.

     If you select this option, the connection between the origin server and the proxy remains active even if there is no data flow.

   - Enable or disable Java* applet stripping from HTML files.

     When enabled, Java applets are stripped from the HTML file before the file is displayed in the browser window.

6. Click OK, then click OK again from the Novell BorderManager 3.7 Setup page.

To set up authentication for an HTTP proxy server, refer to "Setting Up Proxy Authentication" on page 81.

Setting Up an HTTP Accelerator Server

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

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

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

To set up an HTTP accelerator server:

1. In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. From the Acceleration tab, check the HTTP Acceleration check box.
3. Click Details or double-click the HTTP Acceleration service.
4. Click Add to add a new acceleration server to the HTTP Accelerator list, then do the following:

   4a Specify whether to enable this HTTP accelerator server after you have set it up.

   The default is Disabled. Specify to disable the server if you are setting up for multiple accelerations. You can disable one or more servers without affecting the other accelerated sites.

   4b Specify whether to enable authentication for this accelerator.

   4c Enter the accelerator server name.

   If reverse proxy authentication is enabled the accelerator server name must be the DNS domain name of the Web site that is being accelerated. The DNS domain name entry should be the same for both inbound and outbound configurations.

   4d Enter the port number the origin Web server is listening on for incoming connections.

   The default is 80 for HTTP.

   4e Click Add and enter a Web server name or IP address.

   4f Click Add and select one or more public proxy IP addresses.

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

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

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

As another example, you have multiple Web servers and several proxy IP addresses. You can configure two entries: one for www1.myco.com with port 80 and IP address 1.2.3.4, and another for www2.myco.com with port 80 and IP address 1.2.3.5.

4g Specify whether to accelerate on a different port, and enter an accelerator port number.

All internal Web server links must be relative URLs.

5 Click OK > click OK again from the Novell BorderManager 3.7 Setup page.

To set up authentication for an HTTP accelerator server, refer to "Setting Up Proxy Authentication" on page 81.

Blocking Virus Requests in HTTP Accelerator

For Web servers that are being accelerated by Novell BorderManager 3.7's reverse proxy capability, Novell has added a new Virus Pattern Recognition feature to Novell BorderManager 3.7 that can help protect against such attacks. This enhancement includes features to facilitate its configuration and monitoring.

To enable this feature, you must have the latest version of PROXY.NLM. You also need the following lines in the SYS:\ETC\PROXY\ PROXY.CFG file, which is used to initialize the NBM Proxy Server at startup:

```
[Extra Configuration]

ScanVirusPatterns=1

[Virus Pattern Configuration]

NoOfVirusPatterns=0

PatternSize=16

PatternStartOffset=1

EnablePatternAutoUpdate=1
```

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

Command Line Configuration

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

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

Adding and Deleting Virus Request Patterns

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

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

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

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

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

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

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

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

Updating the Database via a Script (NCF File)

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

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

virus dump

The name of the dump file is SYS:\ETC\PROXY\VIRPAT.NCF. This NCF file can be run as part of the Proxy Server restart process, or you can run it manually after the Proxy Server has been loaded.

Enabling and Configuring Auto Update

Novell BorderManager 3.7 provides an Auto Update feature that automatically detects virus requests and adds their patterns to the database. This feature's heuristic (self- learning) request examination method is especially useful in detecting frequently changing virus request patterns.

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

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

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

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

The Virus Pattern Configuration screen provides information that can help you adjust these parameters for your particular system. See "Choosing a Proper Threshold" for details.

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

virus -e 1

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

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

```
[Virus Pattern Configuration]
EnablePatternAutoUpdate=1
```

Adding New Virus Keywords

Virus request patterns of the same virus type contain keywords or character strings that can be used to identify the request. For example, all URLs with Code Red virus requests contain the string CMD.EXE. Since the presence of this string identifies the URL as a virus request, "cmd.exe" is a keyword.

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

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

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

virus add -k *keyword*

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

Monitoring the Virus Pattern Recognition Feature

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

Effect on Performance

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

Setting Up an FTP Proxy Server

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

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

To set up an FTP proxy server:

1. In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. From the Application Proxy tab, check the FTP Proxy check box.
3. Click Details or double-click the FTP Proxy service.
4. Enter a username/password separator.

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

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

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

   where john_smith.novell is the NDS or eDirectory username, anonymous is the FTP username, ftp.novell.com is the FTP host, *xxxxx* is the NDS or eDirectory password for john_smith, and *yyyyy* is the FTP password for anonymous users at ftp.novell.com.
5. Enter an anonymous FTP e-mail address or keep the default.

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

6. Select a method of user authentication: none, clear text username/password, or single sign-on.
   - None-The user will not be required to enter the FTP proxy username and password when accessing the FTP server, and will need to supply only the FTP hostname and password.
   - Clear text username/password—The user must enter a fully distinguished NDS or eDirectory username, FTP username, and FTP hostname at the user prompt; and an NDS or eDirectory password and FTP password at the pass prompt.
   - Single sign-on—If a user is logged in to NetWare through the latest Novell Client™, the user is not prompted to authenticate to the proxy.
7. Click OK, then click OK again from the Novell BorderManager 3.7 Setup page.

To set up the server as an FTP accelerator as well, refer to "Setting Up an FTP Accelerator Server" on page 73.

Setting Up an FTP Accelerator Server

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

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

To set up an FTP accelerator server:

1. In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. From the Acceleration tab, check the FTP Acceleration check box.
3. Click Details or double-click an FTP Acceleration service.
4. Click Add, then do the following:

4a Specify whether to enable the FTP accelerator server after you have set it up.

4b Enter the hostname of the origin FTP server.

4c Select one or more public proxy IP addresses from the list.

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

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

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

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

5 Click OK, then click OK again from the Novell BorderManager 3.7 Setup page.

Setting Up a Mail Proxy Server

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

To set up a Mail proxy server:

1 In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.

2 From the Application Proxy tab, check the Mail Proxy check box.

3 Click Details or double-click the Mail Proxy service.

4 Enter 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.

5. Click OK > click OK from the Novell BorderManager 3.7 Setup page.

Setting Up a News Proxy Server

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

To set up a News proxy server:

1. In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. From the Application Proxy tab, check the News Proxy check box.

3. Click Details or double-click the News Proxy service.
4. (Optional) Enter the primary news domain name.

   This is the domain name that is used to substitute the From address in posted news articles. This name replaces the internal originating hostnames in outbound news article header lines and hides the internal network architecture. If this parameter is unspecified, the News proxy uses the DNS domain name in the From address.
5. (Optional) Enter the server name or IP address of the private (internal) news servers to which the incoming news articles are forwarded.

   If you do not specify this information, the proxy server will not accept the connections from the public news servers to forward or retrieve articles from the private news servers.
6. Click Add and specify the DNS hostnames or IP addresses of the public (external) news servers from which news articles are retrieved.

   You must specify at least one server for the News proxy to work if a private news server is set up. The proxy connects to the first public news server on the list, and all queries from the private news server and readers are forwarded to that server. If the connection to the first server on the list fails, the News proxy will use the next server on the list, and so on.
7. Click OK > OK from the Novell BorderManager 3.7 Setup page.

Setting Up a Generic Proxy Server

Use a Generic proxy server to access multiple protocols if the application proxy you need (for example, Telnet and rlogin) is not already defined in Novell BorderManager 3.7. Generic proxy tunnels data without caching it.

To set up a Generic TCP or UDP proxy server:

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

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

4. Click Add to add a server to the Forward List, then complete the following substeps:

   4a. Specify whether to enable the Generic proxy server after you have set it up.

   4b. Enter the hostname of the origin server.

   4c. Enter the port number the origin server is listening on for incoming connections.

   The default is 0 for Generic proxy.

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

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

   4e. Enter the port number for the proxy server.

   The default is 0.

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

   4f. Click OK.

5. Click OK > OK from the Novell BorderManager 3.7 Setup page.

Setting Up DNS Proxy

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

NOTE: The intranet client must have the private IP address of the DNS proxy configured as the address of the DNS name server. For servers, you can set up the IP addresses of the DNS name servers and the domain name in the SYS:\ETC\RESOLV.CFG file.

To enable DNS proxy:

1. In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. From the Application Proxy tab, check the DNS proxy check box.
3. Click Details, or double-click the DNS proxy service.
4. Click OK > OK from the Novell BorderManager 3.7 Setup page.

Setting Up RealAudio and RTSP Proxies

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

To enable RealAudio and RTSP proxies:

1. In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. From the Application Proxy tab, check the RealAudio and RTSP Proxies check box.
3. Click Details, or double-click the RealAudio and RTSP Proxies service.
4. Click OK > OK from the Novell BorderManager 3.7 Setup page.

Setting Up the SOCKS Client (Upstream)

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

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

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

- Setting up the Proxy Services software to act as a SOCKS client
- Setting up the Novell IP Gateway to act as a SOCKS server
- Setting up the browser

The SOCKS client can also be used with a third-party SOCKS server instead of the Novell IP Gateway.

To set up the proxy server and the Novell IP Gateway to support SOCKS through HTTP proxy or FTP proxy:

1. In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. From the Application proxy tab, select HTTP or FTP proxy.
3. Click SOCKS Client, then check the Enable SOCKS check box.
4. Specify the IP address of the SOCKS server.
5. Enter the port number of the SOCKS server.

   The default is 1080.
6. Click Username/Password > enter a username and password that the proxy will use to authenticate with the SOCKS server.

   If you select No Authentication and do not specify a username and password, null authentication will be used. The username and password must match the username and password configured for the SOCKS server or at the third-party SOCKS server. If you configure null authentication, make sure that the SOCKS server is set up to allow null authentication.
7. Click OK to close the SOCKS Client page.
8. If you are not using a third-party SOCKS server:

   NOTE: The following steps apply only if the upstream SOCKS server is running Novell BorderManager 3.7.

   8a Click the Gateway tab.

   8b Check the SOCKS V4 and V5 check box > click Details.

   8c (Optional) Enter the port number of the SOCKS server.

   The default is 1080. This enables the Novell IP Gateway to act as a SOCKS server. Assign a different port number for SOCKS traffic if another service is already using this port.

   8d Select SOCKS V5 or SOCKS V4.

   Select V5 if the server must work with the Novell BorderManager 3.7 SOCKS client. If you select V5, select single sign-on and specify an authentication scheme. If you select SSL as an authentication scheme, select a key ID.

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

   8e Select an authentication method.

   8f Click OK.

8g Select the Users setup page and enter the username and password of the SOCKS client.

The username and password must match the username and password you configured for the SOCKS.

8h Click OK.

9 Click OK from the Novell BorderManager 3.7 Setup page.

10 To use a browser from a workstation, open the configuration window for the browser. In the field provided to specify the location of the HTTP proxy, enter the IP address or DNS hostname of the server running Novell BorderManager 3.7.

This allows requests from the browser to be sent to the SOCKS client operating with Novell BorderManager 3.7 Proxy Services, then forwarded to the SOCKS server if the requested information is not found in the proxy cache.

Setting Up HTTP Transparent Proxy

HTTP Transparent proxy enables you to use an HTTP proxy server without having to reconfigure each user's browser. Use HTTP Transparent proxy to require users to send requests through the proxy server.

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

To set up HTTP Transparent proxy:

1 In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.

2 From the Transparent Proxy tab, check the Transparent HTTP Proxy check box.

3 Click Details or double-click the Transparent Proxy service.

4 Click Add and enter a port for monitoring.

For example, specify 80 for HTTP traffic.

5 In the Exception IP Address List, click Add and enter a local IP address.

6 Click OK > click OK from the Novell BorderManager 3.7 Setup page.

NOTE: When HTTP Transparent proxy is enabled, it is also automatically enabled for the Novell® IP Gateway, if applicable.

To set up authentication for HTTP Transparent proxy, refer to “Setting Up Proxy Authentication” on page 81.

Setting Up Telnet Transparent Proxy

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

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

To set up Telnet Transparent proxy:

1. In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. From the Transparent Proxy tab, check the Transparent Telnet Proxy check box.
3. Click Details or double-click the Transparent Telnet service.
4. Click Add and enter a port for monitoring.

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

   NOTE: When Telnet Transparent proxy is enabled, it is also automatically enabled for the Novell IP Gateway, if applicable.

To set up authentication for Telnet Transparent proxy, refer to “Setting Up Proxy Authentication” on page 81.

Setting Up Proxy Authentication

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

The following sections provide information about setting up proxy authentication:

- “Setting Up Proxy Authentication” on page 81

Setting Up HTTP Proxy Authentication

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

- Single sign-on for Novell Client32 clients—If a user is logged in to NetWare through the latest Novell Client software and uses the browser, the user is not prompted to authenticate again to the proxy.
- SSL proxy authentication—The user is not prompted to authenticate to the proxy if already logged in to NDS or eDirectory.

You can enable HTTP proxy NDS or eDirectory authentication and require all users to authenticate with their browsers before they access the proxy server and the Internet. Proxy authentication consists of a username and a password. The proxy authentication password is the same as a user's NDS or eDirectory authentication password. Any type of browser client can be authenticated: Windows 98, Windows 2000, Windows XP, Windows Me, Windows NT, UNIX, OS/2, or Macintosh*.

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

Single sign-on is successful only when the client machine is running the Novell Client 32 software and has logged in to NDS or eDirectory. The client machine must also be running DWNTRUST.EXE and CLNTRUST.EXE. These files are located in the SYS:PUBLIC directory on the server. For more information about these files and creating login scripts for users to be authenticated using the single sign-on feature, refer to Chapter 4, “Setting Up the Novell IP Gateway,” on page 47.

To set up HTTP proxy authentication:

1. In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. Click Authentication Context.
3. From the Authentication tab, check the Enable HTTP Proxy Authentication check box.
4. Select an authentication scheme: single sign-on or SSL.
5. For single sign-on, enter the time to wait for a single sign-on reply.
6. For SSL, specify the following parameters:

- SSL Listening Port—Specify the port used for authentication. You might need to change the port number to prevent reverse proxy traffic from running into SSL traffic. Both reverse proxy and SSL traffic default to port 443.
- Key ID—Specify the key ID exchanged between the client and server for authentication.

  NOTE: Use the NetWare Administrator PKI Services to change and create key IDs in an NDS or eDirectory tree.
- Notification method—Specify whether to send authentication notification in HTML form or as a Java applet.
- Idle time—Specify the length of time a connection can remain idle before a new login is required.

7. Specify whether to authenticate only when the user attempts to access a restricted page.
8. Click the Context tab.
9. Click Add > enter the user's default NDS or eDirectory context and tree name.

   Enter a fully distinguished NDS or eDirectory container name (sales.my_org, for example). The NDS or eDirectory container name can have up to 256 characters. This entry is optional and makes logging in easier for users. Users in the specified container can log in by typing only their login names without the complete context string.
10. Click OK > click OK from the Novell BorderManager 3.7 Setup page.

Setting Up HTTP Transparent Proxy Authentication

To set up HTTP Transparent proxy authentication:

1. In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. Click Authentication Context.
3. From the Authentication tab, check the Enable HTTP Proxy Authentication check box.
4. Click the Context tab.
5. Click Add and enter the user's default NDS or eDirectory context and tree name.

Enter a fully distinguished NDS or eDirectory container name (sales.my_org, for example). The NDS or eDirectory container name can have up to 256 characters. This entry is optional and makes logging in easier for users. Users in the specified container can log in by typing only their login names without the complete context string.

6. Click OK > click OK from the Novell BorderManager 3.7 Setup page.

Setting Up Telnet Transparent Proxy Authentication

To enable Telnet Transparent proxy authentication:

1. In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. Click Authentication Context.
3. From the Authentication tab, check the Enable Transparent Telnet Proxy Authentication check box.
4. Click the Context tab.
5. Click Add > enter the user's default NDS context and tree name.

   Enter a fully distinguished NDS or eDirectory container name (sales.my_org, for example). The NDS or eDirectory container name can have up to 256 characters. This entry is optional and makes logging in easier for users. Users in the specified container can log in by typing only their login names without the complete context string.
6. Click OK > click OK from the Novell BorderManager 3.7 Setup page.

Completing Advanced Setup, Configuration, and Management Tasks

In addition to the basic setup procedures described in this chapter, there are several advanced setup, configuration, or management procedures you might need to complete, depending on your specific configuration. Advanced tasks are available in Advanced Configuration of Proxy Services and include the following:

- Configuring cache parameters
- Specifying batch downloading
- Configuring caching hierarchies

- Specifying transport timeout parameters
- Specifying DNS parameters
- Setting up HTTP proxy services logging
- Monitoring proxy cache real-time activity
- Viewing host statistics
- Displaying records
- Viewing host record entries
- Viewing user statistics
- Viewing user log entries
- Viewing usage trends
- Exporting data

6 Setting Up Virtual Private Networks

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.

This section explains the tasks you complete to set up the VPN component of the Novell® BorderManager® 3.7 software. This section also describes the preparatory steps required for some tasks.

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

Virtual Private Network Prerequisites

Before you start to set up the VPN component of the Novell BorderManager 3.7 software, you must meet the prerequisites described in this section. This section contains the following topics:

Site-to-Site VPN Prerequisites

Before you set up a site-to-site VPN, your network must meet the following requirements:

- The NetWare® routing software must be installed and configured on each VPN server. Configuring the routing software includes, but is not limited to, setting up the LAN or WAN links to the other VPN members, and configuring static or dynamic routing for Internet Packet Exchange™ (IPX™) and IP packets. Verify connectivity between your VPN servers as required by your selected VPN topology. Any associated firewall software should be configured and connectivity should be verified before the VPN software is installed and before each VPN server is attached to the private networks it will protect.
- If your VPN sites are not on the same intranet, each VPN server must have a connection to the Internet, either directly or indirectly. If your VPN server is connected directly to the Internet, obtain the public IP address provided by your Internet Service Provider (ISP) to use when connecting to the Internet. Each VPN server uses the public IP address to exchange encrypted information with other VPN servers. Obtain the public IP address before you set up the VPN. The ISP connection should also be tested before the VPN software is installed and before the VPN server is attached to any private networks. In the case of an intranet VPN, an ISP connection is not required.
- If your VPN server is connected directly to the Internet, you must obtain a permanent IP address for the ISP connection. The IP address cannot be dynamically assigned by the ISP.
- 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 3.7 for Secure Access to the Public Interface option during the initial Novell BorderManager 3.7 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 3.7 software, select the Setup Novell BorderManager 3.7 for Secure Access to the Public Interface option during the initial Novell BorderManager 3.7 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. 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 3.7 services.

  The firewall filters can also be configured after installation by loading BDRCFG. If the firewall is not running the Novell BorderManager 3.7 software, you must configure these filters manually as described in the documentation provided with the third-party firewall product.

Table 2 VPN Filters

Description of Filter	Protocol	Source Address	Source Port	Destination Address	Destination Port
Exception filters for the VPN master server to allow incoming traffic	TCP (ID=6)	Any	213	VPN public address	Any
	SKIP (ID=57)	Any	Any	Any	Any
	UDP (ID=17)	Any	2010	VPN public address	2010
Exception filters for the VPN master server to allow outgoing traffic	TCP (ID=6)	VPN public address	Any	Any	213
	SKIP (ID=57)	Any	Any	Any	Any
	UDP (ID=17)	VPN public address	2010	Any	2010

Exception filters for the VPN slave server to allow incoming traffic	TCP (ID=6)	Any	Any	VPN public address	213
	SKIP (ID=57)	Any	Any	Any	Any
	UDP (ID=17)	Any	2010	VPN public address	2010
Exception filters for the VPN slave server to allow outgoing traffic	TCP (ID=6)	VPN public address	213	Any	Any
	SKIP (ID=57)	Any	Any	Any	Any
	UDP (ID=17)	VPN public address	2010	Any	2010

- 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. Complete this process for both IPX and IP as described in the packet filtering online documentation.
- If your network uses Open Shortest Path First (OSPF) dynamic routing, your VPN server must be located on a pure OSPF backbone area.

Client-to-Site VPN Prerequisites

Before you install the VPN client software, verify that the following prerequisites have been met:

- The workstation must be running Windows 98*, Windows* 2000, Windows* XP, Windows* Me or Windows NT*.
- If the VPN client will be using a dial-up connection, Microsoft* Dial-Up Networking must be installed before installing the VPN client software.
- If you are using the VPN client with the Novell Client™ software, Novell Client version 3.3 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, the Windows NT Service Pack 3 (SP3) or later version must be installed before installing the VPN client software. Note that the SP3 must be reinstalled whenever you install a feature from the Windows NT CD-ROM, such as Networking or Remote Access Services, that was not already on the system when you installed SP3.
- 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 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 3.7 software, select the Setup Novell BorderManager 3.7 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 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 3.7 services.

  The firewall filters can also be configured after installation by loading BDRCFG. If the firewall is not running the Novell BorderManager 3.7 software, you must configure these filters manually as described in the documentation provided with the third-party firewall product.

Table 3 Filters Required for Client-to-Site VPNs

Description of Filter	Protocol	Source Address	Source Port	Destination Address	Destination Port
Exception filters for the VPN master or slave server to allow incoming traffic	TCP (ID=6)	Any	Any	VPN public address	353

	SKIP (ID=57)	Any	Any	Any	Any
	UDP (ID=17)	Any	353	Any	353
Exception filters for the VPN master or slave server to allow outgoing traffic	TCP (ID=6)	VPN public address	353	Any	Any
	SKIP (ID=57)	Any	Any	Any	Any
	UDP (ID=17)	Any	353	Any	353

Setting Up Your VPN

To set up any type of VPN, you must set up a master server. After you set up the master server, you will complete additional setup tasks based upon whether you want to set up a site-to-site VPN or a client-to-site VPN. This section contains the following procedure:

- "Setting Up Your VPN" on page 92

NOTE: You use the VPNCFG utility to set up the master server, set up the slave server, and generate the encryption information.

Setting Up the Master Server

A VPN can have only one master server. The master server is the central control point for the configuration and management of the VPN. In addition, a server (master or slave) can be a member of only one VPN.

To set up the master server for your VPN, complete the following steps:

1. At the server console prompt, enter

   ```
   LOAD VPNCFG
   ```

   If this server is the first in the NDS or eDirectory tree to be set up as a VPN server, you are prompted to log in to the tree. You must have administrative rights to the root directory to extend the NDS or eDirectory schema and define the VPN attributes.

2. Select Master Server Configuration.

3 Configure the IP addresses for the master server.

The VPN master server uses two IP addresses: a public address to communicate with the Internet, and a VPN tunnel address to exchange encrypted information with other VPN members.

3a Select Configure IP Addresses.

3b Enter the public IP address.

If the VPN server is connected directly to the Internet, the public IP address is the address that was assigned by your ISP.

3c Enter the subnet mask for the public IP address.

3d Enter the VPN tunnel IP address.

This address is associated with the VPN tunnel through which encrypted information passes. This address should be unregistered.

IMPORTANT: The VPN tunnel IP address for all VPN servers must be on the same subnet. The VPN tunnel IP address is an arbitrarily chosen private address. The scope of this address is limited to the VPN tunnel link. This address should not be used as the source or destination IP address for data packets. Use PING on this address to verify the direct connectivity through the VPN tunnel.

3e Enter the subnet mask for the VPN tunnel IP address.

3f Press Esc > select Yes when prompted to save your changes.

4 Generate the master server encryption information.

4a Select Generate Encryption Information.

4b Enter up to 255 characters for the random seed.

There is no need to record this value. The software uses this value to help randomize the master server Rivest Shamir Adleman (RSA) public and private keys, and the master server Diffie-Hellman public and private values that it generates.

5 Copy the master encryption information file (MINFO.VPN) to diskette or save it to a local hard disk.

5a Select Copy Encryption Information.

5b Enter the path where you want to save the master encryption information file.

6 Give the MINFO.VPN file to the network administrator of each slave server you want to add to the VPN.

You can either send the diskette containing the file by surface mail or send the file as an e-mail attachment. There is no danger of compromising security if the file is intercepted because it contains only public information. Any alteration of the file can be detected by verifying the message digest during the configuration of the slave server.

7 Press Esc until you exit VPNCFG.

Setting Up Site-to-Site VPNs

This section explains the basic tasks you perform to set up a site-to-site VPN. This section contains the following procedures:

- "Setting Up Your VPN" on page 92

Setting Up a Slave Server

To set up a slave server for your VPN, complete the following steps. Make sure you have the MINFO.VPN file from the master server administrator.

1 At the server console prompt, enter

```
LOAD VPNCFG
```

2 Select Slave Server Configuration.

3 Configure the IP addresses for the slave server.

Like the master server, a VPN slave server uses two IP addresses: a public address to communicate with the Internet, and a VPN tunnel address to exchange encrypted information with other VPN members.

3a Select Configure IP Addresses.

3b Enter the public IP address.

If the VPN server is connected directly to the Internet, the public IP address is the address that was assigned by your ISP.

3c Enter the subnet mask for the public IP address.

3d Enter the VPN tunnel IP address.

This address is associated with the VPN tunnel through which encrypted information passes. This address should be unregistered.

IMPORTANT: The VPN tunnel IP address for all VPN servers must be on the same subnet.

3e Enter the subnet mask for the VPN tunnel IP address.

3f Press Esc and select Yes when prompted to save your changes.

4 Generate the slave server encryption information.

4a Select Generate Encryption Information.

4b Enter the location of the master encryption information file (MINFO.VPN).

4c Contact the master server administrator and verify that you have the same message digest values.

Having the same digest values ensures the authenticity of the MINFO.VPN file.

IMPORTANT: If the message digest values do not match, the encrypted tunnel between the slave and master servers cannot be created. In this case, the master server administrator must provide a new MINFO.VPN file.

4d Ask the master server administrator to select Authenticate Encryption Information to authenticate the MINFO.VPN file.

To authenticate this file, the administrator must load VPNCFG and select the following menu path:

Master Server Configuration > Authenticate Encryption Information

4e If the message digest values match, enter up to 255 characters for the random seed.

There is no need to record this value. The software uses this value to help randomize the Diffie-Hellman public and private values that it generates for the slave server.

5 Copy the slave encryption information file (SINFO.VPN) to diskette or save it to a local hard disk.

5a Select Copy Encryption Information.

5b Enter the path or name of the file in which you want to save the slave encryption information file. The default is A:\SINFO.VPN.

HINT: Rename your SINFO.VPN file to a name such as SINFO_S1.VPN. This enables the master server administrator to collect all slave encryption information files in a single directory without overwriting them. You can also use a server or location name when renaming the SINFO.VPN file.

6 Give your slave encryption information file to the master server administrator.

You can either send the diskette containing the file by surface mail or send the file as an e-mail attachment. There is no danger of compromising

security if the file is intercepted because it cannot be interpreted without the master server's RSA public and private keys and Diffie-Hellman public and private values.

7 Press Esc until you exit VPNCFG.

IMPORTANT: Before the slave server can communicate with other members of the VPN, you must perform the procedure described in "Setting Up Your VPN" on page 92.

Adding a Server to a VPN

Before you can add a server to a VPN, you must use the VPNCFG utility to do the following;

- Set up the master server
- Set up the slave server
- Generate encryption information files for the master and slave servers

After you complete the VPNCFG procedures, the master server is automatically added to the VPN. You use the NetWare Administrator utility to add a server to a VPN and synchronize VPN servers.

To add a slave server to the VPN, complete the following steps:

1 In NetWare Administrator, double-click the VPN master server and select the Novell BorderManager 3.7 Setup page.

2 Click the VPN tab.

3 Double-click Master Site-to-Site under Enable Service.

4 Click Add.

5 Locate the encryption information file for the server you want to add, then click Open.

The encryption information file is generated during the procedure described in "Setting Up Your VPN" on page 92. The default name for the file is SINFO.VPN. NetWare Administrator reads the file and displays a 16-byte message digest.

6 Contact the administrator of the VPN slave server and ask him to select Authenticate Encryption Information to authenticate the SINFO.VPN file.

To authenticate this file, the administrator must load VPNCFG and select the following menu path:

Slave Server Configuration > Authenticate Encryption Information

Compare the value of your message digest with the one generated at the slave server console.

7. If the digests are equal, click Yes; otherwise, click No.

   Unequal digest values indicate that the data has been tampered with or corrupted.

8. Click Status.

9. Click Synchronize All, then click OK.

Complete this procedure for each slave server that you want to add as a member of the VPN.

Synchronizing VPN Servers

When you synchronize servers on a VPN, the VPN master server updates all VPN slave servers with the current VPN topology and encryption keys. A server's synchronization status can assume one of the following states:

- Up-to-Date

  The server has been configured with the latest topology and encryption information. This does not indicate that the server's VPN tunnel connections are up. Use the Activity display to determine the status of the VPN tunnel connections.

- Being Configured

  The server still must receive the current topology and encryption information from the master server.

- Being Removed

  The server is being removed from the VPN.

NOTE: Any server state that remains at Being Configured or Being Removed for an extended period of time indicates a problem with the master server's ability to communicate with that VPN member. For more information, refer to the VPN online documentation.

To synchronize the members of a VPN:

1. In NetWare Administrator, double-click the VPN master server and select the Novell BorderManager 3.7 Setup page.

2. Click the VPN tab.

3. Under Enable Service, double-click Master Site-to-Site.

4 Click Status.

The Synchronization Status window displays each member of the VPN, its public IP address, and its update status.

5 To synchronize all servers on the VPN, click Synchronize All.

Or

To synchronize only one server on the VPN, select the server name and click Synchronize Selected.

Setting Up Specific Site-to-Site VPN Configurations

There are several different ways you can build your site-to-site VPN. Depending on the configuration you require, you will need to complete several different setup tasks. The following detailed examples are available in the VPN online documentation:

- Using the VPN server as a border server
- Using the VPN server behind a firewall
- Setting up a VPN within a private network

NOTE: To correctly set up a VPN for a particular configuration, it is vital that you refer to the examples in the VPN online documentation. The examples contain procedures that are required for a particular configuration but are not included in the basic procedures provided in this publication.

Setting Up Client-to-Site VPNs

This section explains the tasks required to set up a client-to-site VPN and make a client-to-site connection. This section contains the following procedure:

- “Setting Up Your VPN” on page 92

Setting Up a VPN Server to Support VPN Clients

To set up a VPN server to support VPN clients:

1 Set up a NetWare server with the VPN software.

- If you want the server to be a member of a site-to-site VPN network (master or slave), set up the VPN server to be part of the VPN network, as described in “Setting Up Your VPN” on page 92 or “Setting Up Your VPN” on page 92.

- If you want the server to support only remote clients and not be a member of a site-to-site VPN network, set up the VPN server as a VPN master, as described in "Setting Up Your VPN" on page 92.
- You must place the server in the path between your intranet and the Internet. If you have multiple access points to the Internet from your intranet, you must make sure the packets from the intranet can return to the VPN client through the VPN server. Packets will return to the client if you make the VPN server the default router on your network, or if you enable NAT on the private interface of your VPN server.

2. In NetWare Administrator, double-click the VPN server that you want to support the clients and select the Novell BorderManager 3.7 Setup page.
3. Click the VPN tab.
4. Double-click Client-to-Site under Enable Service.
5. (Optional) Configure the Inactivity Timeout parameter, if required.
6. To enable the encryption of IPX data for VPN clients, you must set WAN Client IPX Network Address to the IPX network address that VPN clients will use to access this server.

   This address must be unique and should not match the server's network address or the network address of any of the server's LAN adapters. If the client dials directly in to the VPN server using the remote access software, the IPX network address that you configured for remote access is automatically displayed. If you change the address in this field, the remote access software is updated with the new address.

   IMPORTANT: When IPX support is enabled for the VPN client on Windows 95 and Windows 98 workstations, the client's IPX LAN connection is disabled after the VPN IPX connection is established. This also occurs when the client is not a VPN client and you use Dial-Up Networking with IPX enabled.
7. (Optional) If you do not want the VPN clients to negotiate the data encryption and data authentication methods for the connection with the VPN server, select Restrict Clients to Use Server Preferred Security.

   To configure the server's preferred security, select Details under Master Site-to-Site or Slave Site-to-Site.
8. (Optional) If you want to specify a limited number of networks to which VPN clients can communicate securely using encryption, configure a list of protected networks.

   To add a network to the list, select Encrypt Only Networks Listed Below > click Add. Select the network address and subnet mask > click OK.

This step is optional because by default the client encrypts data to and from all networks. By specifying a list of protected networks, you enable the VPN client to send unencrypted IP traffic to the Internet and encrypt only intranet traffic.

If you have an IPX-only network and do not want to encrypt IP traffic, select Do Not Encrypt Any IP Packets.

9 (Optional) Click Digest to view the digest of the VPN server's configuration information.

This digest is used to authenticate the information sent to the VPN client during its attempt to log in to the VPN server.

10 Click OK > select Novell BorderManager 3.7 Access Rules.

11 To configure the NDS or eDirectory users, groups, or containers that are allowed to use this VPN server, complete the following substeps:

11a Click Add.

11b Select VPN Client for the access type.

11c Under Source, select Specified > click Browse.

11d Click Add.

11e Select a user, group, or container from the list of objects in the NDS or eDirectory tree, then click OK.

11f Repeat the steps for each additional object, as required.

12 Click OK until you return to the VPN page.

13 If needed, configure authentication rules and access methods.

VPN clients can use security devices such as hardware tokens in addition to using their NDS or eDirectory password to authenticate to the VPN server. If a Login Policy object exists in your NDS or eDirectory tree, it is associated with all VPN version 3.7 servers in the tree, and authenticates VPN users using authentication rules and access methods defined in the object.

If you have a Login Policy object in your tree, then only users that have a rule defined for their authentication method can connect to the VPN server.

14 If users are accessing the VPN server using the remote access software, set up the remote access accounts for the users as described in Chapter 6, “Setting Up Virtual Private Networks,” on page 87.

15 Provide VPN users with the following information by e-mail or telephone:

- The NDS or eDirectory username and password assigned to each user for the tree that contains the VPN server
- If users are accessing the VPN server through an ISP, the IP address of the VPN server
- If users are dialing directly in to the VPN server, the remote access information (phone number and remote access password)
- (Optional) The digest of the VPN server configuration information

Installing a VPN Dial-Up or LAN Client on a Windows 98, Windows 2000, Windows XP, Windows Me or Windows NT Workstation

To install a VPN client on a Windows 98, Windows 2000, Windows XP, Windows Me or Windows NT Workstation:

1 If you are using a dial-up client, verify that the workstation has a modem installed and set up.

2 Insert the VPN client CD-ROM and start the installation program.

3 Follow the online instructions in the installation program. Insert the Windows 98, Windows 2000, Windows XP, Windows Me or Windows NT CD containing the Novell Client software provided with Novell BorderManager 3.7 when prompted to do so.

4 Restart the workstation when prompted.

If the installation is successful, the Novell Virtual Private Network adapter will appear in the Windows 98, Windows 2000, Windows XP, Windows Me or Windows NT Network Control Panel. For Windows NT systems, the Novell BorderManager 3.7 VPN Client is listed under Services in the Network Control Panel.

Setting Up a VPN Dial-Up Client on a Windows 98, Windows 2000, Windows XP, Windows Me or Windows NT Workstation

A default dial-up entry named Novell VPN is automatically created for the VPN client during installation. This dial-up entry can be used to connect to your ISP by starting the VPN Login software. Use the VPN Login dialog box to configure various parameters before connecting to your ISP. These parameters include the dialing properties, the dialing location, the type of modem that is used, and the phone number, which can be entered manually or

selected from a phone book listing. If you do not want to use the default dial-up entry, you can create a new entry using Microsoft Dial-Up Networking.

To create and configure a new dial-up entry on a Windows 98, Windows 2000, Windows XP, Windows Me or Windows NT Workstation:

1. Create a new dial-up entry.
   - **1a** Double-click Make New Connection.
   - **1b** Enter the name of the dial-up entry and select the modem.
   - **1c** Click Next and enter the area code, phone number, and country code.
   - **1d** Click Next, then click Finish to complete the dial-up entry.
2. For Windows 98, Windows 2000, Windows XP, Windows Me clients, set the server type for the dial-up entry. For Windows NT clients, do not change the default setting.
   - **2a** Right-click the dial-up entry and select Properties, or select the dial-up entry and select Properties from the File menu.
   - **2b** Select Server Type.
   - **2c** Set Type of Dial-Up Server to Novell Virtual Private Network.
   - **2d** Click OK to save your changes.

Logging In from a VPN Client

Use the Dial-up VPN Login if you want to use a Microsoft Dial-Up Networking entry to connect to your ISP.

Use the LAN VPN Login if you are already connected to your ISP through a cable modem, an ADSL device, a LAN connection, or an established dial-up connection.

To log in from a VPN client, complete the following steps:

1. Start the VPN login in one of the following ways and wait for the Novell VPN Login dialog box to appear:
   - Double-click one of VPN Login icons that were automatically created during the client installation.
   - For Windows 98 and Windows Me clients, select Start > Programs > Novell > Novell BorderManager 3.7 VPN client > Dial-up VPN login or LAN VPN login.

- For Windows NT clients, select Start > Programs > NetWare > Novell BorderManager 3.7 VPN client > Dial-up VPN login or LAN VPN login.
- On Windows 98 and Widows Me workstations, double-click the VPN dial-up entry. The VPN Login program is launched when the specified dial-up connection is established.

2 Select the NetWare Login tab in the Novell VPN Login dialog box and provide the following information:

- NDS or eDirectory username
- NDS or eDirectory password
- NDS or eDirectory context
- VPN server's IP address

  The IP address can be followed by a space and a description.

- Token Password (Optional)

  This password is required only if you have configured the Login Policy object with rules requiring VPN clients to use a security device such as a hardware token in addition to using their NDS or eDirectory password. See the Authentication Services online documentation for more information on how to generate the token password and configure authentication rules.

After the client has been successfully authenticated, this information (except for the password) is saved by the VPN client in the workstation's registry and is presented to the user the next time the VPN client comes up. The most recently used entries for the name and IP address are saved and displayed.

3 For Dial-Up connections, select the Dial-Up tab and select a VPN dial-up entry name from the list of configured entries.

4 (Optional) Enter the dial-up username and password if you have not connected using this dial-up entry before or your password was not saved.

To configure the phone number and other dial properties, select Settings. You can override the dial-up password and phone number configured in the dial-up entry by selecting or entering new values.

5 (Optional) If your ISP is using the RADIUS proxy feature to authenticate users, click Use NetWare Name and set RADIUS Domain to the name

used by the ISP to identify the domain that contains the user when acting as an authentication request proxy.

The name used for the dial-up authentication is the NetWare username and context, followed by the RADIUS domain that you enter. For example, if the username is User1, the context is Engineering.ACME, and the RADIUS domain is acme.com, then the name used for the dial-up authentication is .User1.Engineering.ACME@acme.com.

6. Select the NetWare Options tab and select from the following options:

   - Enable IPX Encryption—Enables the VPN client to communicate with the VPN server using IPX.

     NOTE: If you configured your Novell Client software to use the compatibility mode driver (CMD), you can use the CMD to access IPX services through the VPN, instead of enabling IPX.

   - Login to NetWare—Automatically logs in to NetWare after the encrypted tunnel is established with the VPN server.
   - Clear Current Connection—Determines whether the connection replaces or augments your existing connections.
   - Run Scripts—Automatically executes your user login script.
   - Display Results Window—Automatically displays the result of login script processing.
   - Close Script Results Automatically—Automatically closes the script processing results page when the login is successful.

7. Click the Launcher tab to specify an application that is launched after the encrypted tunnel has been established with the VPN server.
8. Click OK to connect to the VPN server.
9. If you are prompted to compare the summary of the authentication information to the information that the administrator distributed, click OK if the values match.

   This prompt is displayed only if you are connecting to this VPN server from this workstation for the first time or the VPN server has regenerated its keys.

10. (Optional) Click the VPN Status tab to view the progress of the VPN connection.

    After the connection is established, a VPN Client icon appears in the task bar. Double-click the icon to display VPN client statistics for this session.

For more information about VPN client statistics, refer to the VPN online documentation.

11 To terminate your VPN connection, double-click the VPN statistics icon and click Disconnect.

On Windows NT systems, do not terminate your session by disconnecting your dial-up connection using the Dial-Up Monitor. You must terminate your VPN connection from the VPN Statistics screen.

Setting Up Specific Client-to-Site VPN Configurations

There are several different ways you can build your client-to-site VPN. Depending on the configuration you require, you will need to complete several different setup tasks. The following detailed examples are available in the VPN online documentation:

- Using the client to dial in to an ISP and connect to the VPN server over the Internet
- Using the client to dial directly in to the VPN server
- Using the client to connect to the VPN server through a LAN or cable modem

NOTE: To correctly set up a VPN for a particular configuration, it is vital that you refer to the examples in the VPN online documentation. The examples contain procedures that are required for a particular configuration but are not included in the basic procedures provided in this publication.

Upgrading VPN from a Previous Version

This section describes upgrading from the Novell VPN software contained in BorderManager version 3.5 or 3.6 to the current BorderManager version (version 3.7). This section contains the following procedure:

- "Upgrading VPN from a Previous Version" on page 105

Two approaches are available for upgrading from version 3.5 or 3.6 to version 3.7:

- All the VPN servers can be reconfigured at one time, overnight or during a weekend. This involves installing the new software and regenerating the encryption information for all VPN servers.

- A new VPN master server can be configured to operate in parallel with the existing version 3.5 or 3.6 master server, and the slave servers can be upgraded to the new network one at a time.

The advantage of the first approach is that no new equipment or ISP connections are required to run a master server in parallel with the existing version 3.5 or 3.6 master server. However, sufficient down time is required to convert all version 3.5 or 3.6 servers without interruption to service. The amount of time needed to transfer the encryption information to and from each slave server must be considered.

The second approach requires an additional machine that can be used as the new VPN master server to be run in parallel with the existing version 3.5 or 3.6 master server. The advantage of this approach is that the upgrade can take place over a period of time without causing complete loss of service. VPN slave servers that remain on the existing VPN can still communicate with each other, but they cannot communicate with any VPN members on the new VPN until the upgrade occurs.

Use the second approach if:

- The VPN master server is behind a router.

  This procedure is described in "Upgrading VPN from a Previous Version" on page 105. Use the same procedure if you want to replace the existing master server instead of adding a new master server in parallel.

- The VPN master server is connected directly to the ISP.

  There are two options in this case:

  - Add a new version master server on a LAN behind the machine that is acting as the existing version 3.5 or 3.6 master server.

    This option requires an additional machine to be used as the new version 3.7 master server. However, this scenario is preferable in terms of performance. This procedure is described in "Upgrading VPN from a Previous Version" on page 105.

  - Replace the existing version 3.5 or 3.6 master server with a new VPN 3.7 master server and use the existing ISP connection with the new version 3.7 master server.

    This option does not require an additional machine for the new version 3.7 master server. The disadvantage is that after the version 3.5 or 3.6 master server is removed, the remaining version 3.5 or 3.6 slave servers cannot be managed using the master server until they are upgraded to the new VPN. This procedure is described in "Upgrading VPN from a Previous Version" on page 105.

Upgrading During a Complete VPN Shutdown

To upgrade version 3.5 or 3.6 sites to version 3.7 during a complete VPN shutdown, complete the following steps:

1. Install and configure the new VPN software on the master server.

   Refer to "Setting Up Your VPN" on page 92 for detailed instructions.

2. Configure the slave servers and regenerate the key for each new slave server using the master encryption information that was generated by the new master server.

   Refer to "Setting Up Your VPN" on page 92 for detailed instructions.

3. Add each slave server to the VPN.

   Refer to "Setting Up Your VPN" on page 92 for detailed instructions.

Upgrading with the Master Server behind a Router

To upgrade version 3.5 or 3.6 sites to version 3.7 with the master server behind a router, complete the following steps:

1. Designate a machine that will be used as the new VPN master server.

2. While keeping the original VPN master and slave servers running, install and configure the new master server on the same LAN.

   Refer to "Setting Up Your VPN" on page 92 for detailed instructions.

   IMPORTANT: Continue to run the original VPN master server until you are instructed later in this procedure to bring it down.

3. Select a slave server to upgrade to the new network, remove the slave server from the original network, and add it to the new network.

   Refer to the VPN online documentation and "Setting Up Your VPN" on page 92 for detailed instructions.

4. Regenerate the key for the new slave server using the master encryption information that was generated by the new master server.

   Refer to "Setting Up Your VPN" on page 92 for detailed instructions.

5. Repeat the steps for each slave server until all slave servers are removed from the original network and added to the new network.

6. After all slave servers have been upgraded to the new VPN, bring down and disconnect the original master server.

7. Complete the procedures described in "Setting Up Your VPN" on page 92, as required.

Upgrading with a Second Master Server behind a Router

To upgrade version 3.5 or 3.6 sites to version 3.7 with a second master server behind a router, complete the following steps:

1. Designate a machine that will be used as the new VPN master server.
2. While keeping the original VPN master and slave servers running, install and configure the new master server on the LAN behind the original VPN master.

   Refer to "Setting Up Your VPN" on page 92 for detailed instructions.

   IMPORTANT: Continue to run the original VPN master server until you are instructed later in this procedure to bring it down.
3. Select a slave server to upgrade to the new network, remove the slave server from the original network, and add it to the new network.

   Refer to the VPN online documentation and "Setting Up Your VPN" on page 92 for detailed instructions.
4. Regenerate the key for the new slave server using the master encryption information that was generated by the new master server.

   Refer to "Setting Up Your VPN" on page 92 for detailed instructions.
5. Repeat the steps for each slave server until all slave servers are removed from the original network and added to the new network.
6. After all slave servers have been upgraded to the new VPN, bring down and disconnect the original master server.
7. Complete the procedures described in "Setting Up Your VPN" on page 92, as required.

Upgrading Using a Replacement for an Existing Master Server

To upgrade version 3.5 or 3.6 sites to version 3.7 using a replacement for an existing master server, complete the following steps:

1. While keeping the version 3.5 or 3.6 slave servers running, install and configure the version 3.7 software on the original version 3.5 or 3.6 master server and use the same ISP connection.

   Refer to "Setting Up Your VPN" on page 92 for detailed instructions.
2. Select a slave server to upgrade to the new network, remove the slave server from the original network, and add it to the new network.

   Refer to the VPN online documentation and "Setting Up Your VPN" on page 92 for detailed instructions.

3 Regenerate the key for the new slave server using the master encryption information that was generated by the new master server.

   Refer to "Setting Up Your VPN" on page 92 for detailed instructions.

4 Repeat the steps for each slave server until all slave servers are removed from the original network and added to the new network.

5 Complete the procedures described in "Setting Up Your VPN" on page 92, as required.

Completing Advanced Setup, Configuration, and Management Tasks

In addition to the basic setup procedures described in this chapter, there are several advanced setup, configuration, and management procedures you might need to complete, depending on your specific configuration. Advanced tasks are available in Advanced Configuration of Virtual Private Networks and include the following:

- Selecting network protocols on your VPN
- Specifying the networks protected by a site-to-site VPN
- Setting up data encryption and data authentication methods
- Selecting whether the connection is initiated from one or both sides
- Adjusting the VPN server response timeout
- Tuning master-slave server synchronization
- Synchronizing VPN servers
- Removing a slave server from a VPN
- Selecting your VPN topology

7 Setting Up Access Control

Access control is the process by which user access to Internet and intranet services is regulated and monitored. Specifically, the Novell® BorderManager® 3.7 access control software allows or denies access requests made through the Novell IP Gateway, Proxy Services, or a Virtual Private Network (VPN) client.

When you enabled the Novell BorderManager 3.7 HTTP proxy for all private interfaces during the software installation, access control was enabled by default. All HTTP proxy traffic through the private interface is denied until you configure an access rule to specifically allow users to access the HTTP proxy.

When access control is enabled, the access control list (ACL)—comprising the access rules—also applies to the Novell IP Gateway, the application proxies, and VPN clients attempting to connect to a VPN server.

An access rule can be created for a Country (C), Organization (O), Organizational Unit (OU), or Server object. This chapter explains how to set up basic access control so users can use the Novell BorderManager 3.7 services you enabled.

This section contains the following sections:

- "Setting Up a Rule to Allow the Server to Resolve Hostnames" on page 118
- "Setting Up Time Restrictions for Access Rules" on page 119
- "Viewing All Rules That Apply to an Object" on page 119
- "Completing Advanced Setup, Configuration, and Management Tasks" on page 120

NOTE: This section describes the tasks required to set up an initial implementation of access control. For planning and conceptual information about access control, refer to the Novell BorderManager 3.7 Overview and Planning Guide, available in the online documentation. Make sure you understand this information before setting up and configuring access control.

Setting Up a URL-Based Rule

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

To create an access rule for a URL:

1. In NetWare® Administrator, right-click the object where the access rules are to be created and select Details.
2. Select the Novell BorderManager 3.7 Access Rules page and click Add.
3. In the Access Rule Definition page, specify Allow (the default) for Action.
4. For Access Type, select URL.
5. Under Source, specify Any to apply the rule to all NDS® or Novell eDirectory™ objects, Domain Name System (DNS) hostnames, IP addresses, and subnets. Otherwise, select users, groups, or hosts as follows:

   5a. Click Specified, then click Browse.

   5b. Specify an NDS or eDirectory object, a DNS hostname, an IP address or range of addresses, or a subnet, including its subnet mask, then click Add.

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

5c Add additional sources.

5d After you have added the sources you want, click OK.

6 Under Destination, specify Any to apply the rule to any URL, otherwise select Specified and do the following:

6a Click Browse > Add.

6b Enter the *unqualified* URL (www.novell.com, for example) and click OK.

6c Repeat this process to add additional URLs, if necessary.

NOTE: You can use wildcards in the URLs. However, be aware that the HTTP proxy and the Novell IP Gateway enforce rules with wildcards differently. The HTTP proxy enforces a rule with a wildcard in the hostname of a URL, while the Novell IP Gateway does not. For example, the HTTP proxy enforces rules for http://*.novell.*, http://*novell.*, and http://www.*.com, but the Novell IP Gateway ignores these rules. The Novell IP Gateway enforces rules containing wildcards only when the wildcard represents all the links from a home page, such as http://www.novell.com/*.

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

Logging access attempts can affect server performance; however, it is recommended that you do so to detect unathorized activity.

8 Click OK, as necessary, to return to the Novell BorderManager 3.7 Access Rules page > click OK to update the access rules.

Setting Up a Rule to Allow Access through the Novell IP Gateway

Access rules created for ports apply to users logged in from a Novell IP Gateway or SOCKS client. This section describes how to create an access rule for a port.

To allow users to access specific services through the Novell IP Gateway:

1 In NetWare Administrator, right-click the object where the access rules are to be created and select Details.

2 Select the Novell BorderManager 3.7 Access Rules page > click Add.

3 In the Access Rule Definition page, specify Allow (the default).

4 For Access Type, select Port.

5 Specify the following under Access Details:

- Select a service from the Service drop-down menu.
- Enter an origin server port or range of ports.
- Select a transport protocol from the Transport drop-down menu.

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

6a Click Specified, then click Browse.

6b Specify an NDS or eDirectory object, a DNS hostname, an IP address or range of addresses, or a subnet, including its subnet mask, and click Add.

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

6c Add additional sources.

6d After you have added the sources you want, click OK.

7 Under Destination, specify Any to apply the rule to any destination > click OK. Otherwise select destinations as follows:

7a Click Specified > Browse.

7b Specify a DNS hostname, an IP address or range of addresses, or a subnet, including its subnet mask, and click Add.

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

7c Add additional destinations.

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

IMPORTANT: If you create a rule that allows access to any destination whose hostname must be resolved by a DNS name server, you must create another rule that allows the Novell BorderManager 3.7 server to resolve the hostname. Refer to "Setting Up a Rule to Allow the Server to Resolve Hostnames" on page 118.

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

Logging access attempts can affect server performance; however, it is recommended that you do so to detect unathorized activity.

9 Click OK to close the Access Rule Definition page.

10 Repeat the steps for each service you want users to be able to access.

11 Click OK, as necessary, to return to the Novell BorderManager 3.7 Access Rules page > click OK to update the access rules.

Setting Up a Rule to Allow Access through an Application Proxy

If you set up port rules to allow HTTP (port 80), FTP (port 21), Telnet (port 23), Simple Mail Transport Protocol (SMTP) (port 25), Network News Transfer Protocol (NNTP) (port 119), or RealAudio* (port 7070), they apply only if users are accessing these services through the Novell IP Gateway. When a user is accessing an application proxy, these rules are ignored. If you want similar rules to apply to users accessing these services through an application proxy, you must set up access rules for the individual application proxies.

To create an access rule for an Proxy Services:

1. In NetWare Administrator, right-click the object where the access rules are to be created and select Details.
2. Select the Novell BorderManager 3.7 Access Rules page > click Add.
3. In the Access Rule Definition page, specify Allow (the default).
4. For Access Type, select Application Proxy.
5. For Access Details select a proxy from the Proxy drop-down menu.

   The port number information is automatically filled in for you. If you selected the News proxy, a drop-down menu is added that allows you to specify the direction: Posting or Reading.
6. Under Source, accept Any to apply the rule to all NDS or eDirectory objects, DNS hostnames, IP addresses, and subnets. Otherwise, select users, groups, or hosts as follows:

   6a Click Specified, then click Browse.

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

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

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

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

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

6e Add additional sources by repeating the steps.

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

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

7a Click Specified, then click Browse.

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

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

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

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

7e Add additional destinations by repeating the steps.

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

IMPORTANT: If you create a rule that allows access to any destination whose hostname must be resolved by a DNS name server, you must create another rule that allows the Novell BorderManager 3.7 server to resolve the hostname. Refer to "Setting Up a Rule to Allow the Server to Resolve Hostnames" on page 118.

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

Logging access attempts can affect server performance; however, it is recommended that you do so to detect unathorized activity.

9 Click OK, as necessary, to return to the Novell BorderManager 3.7 Access Rules page, then click OK to update the access rules.

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

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

To create an access rule for a VPN Client:

1. In NetWare Administrator, right-click the object where the access rules are to be created and select Details.
2. Select the Novell BorderManager 3.7 Access Rules page > click Add.
3. In the Access Rule Definition page, specify Allow (the default).
4. For Access Type, select VPN Client.
5. Under Source, accept Any to apply the rule to all NDS or eDirectory objects, DNS hostnames, IP addresses, and subnets. Otherwise, select users, groups, or hosts as follows:
   - **5a** Click Specified > click Browse.
   - **5b** Click Add, select from among the available objects in the NDS or eDirectory tree > click OK.
   - **5c** Add additional sources.
   - **5d** When you have added the sources you want, click OK.
6. Under Destination, accept Any to apply the rule to any VPN server in the NDS or eDirectory tree; otherwise select destinations as follows:
   - **6a** Click Specified > click Browse.
   - **6b** Click Add, select from among the available server objects in the NDS or eDirectory tree > click OK.
   - **6c** Add additional destinations.
   - **6d** After you have added all the destinations, click OK.
7. (Optional) If you want the server to record all access attempts that match the rule, click Enable Rule Hit Logging.

   Logging access attempts can affect server performance; however, it is recommended that you do so to detect unathorized activity.
8. Click OK, as necessary, to return to the Novell BorderManager 3.7 Access Rules page > click OK to update the access rules.

Setting Up a Rule to Allow the Server to Resolve Hostnames

If you create any rules that allow access to hostname destinations that must be resolved by a DNS name server, you must create another rule at the Organization (O) or Organizational Unit (OU) object that contains the Novell BorderManager 3.7 server to allow the server to resolve the hostname.

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

1. In NetWare Administrator, right-click the object where the access rules are to be created and select Details.
2. Select the Novell BorderManager 3.7 Access Rules page and click Add.
3. In the Access Rule Definition page, specify Allow (the default value).
4. For Access Type, select DNS.

   The port number 53 appears in the Port field. Allowing outbound access to port 53 enables the Novell BorderManager 3.7 server to issue a DNS query.
5. Under Source, accept Any.
6. Under Destination, accept Any to allow any DNS name server to resolve the hostname; otherwise select destinations as follows:

   6a Click Specified > click Browse.

   6b Specify a DNS hostname > click Add.

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

   6c Add additional destinations.
7. After you have added all the destinations > click OK.
8. (Optional) If you want the server to record all access attempts that match the rule, click Enable Rule Hit Logging.

   Logging access attempts can affect server performance; however, it is recommended that you do so to detect unathorized activity.
9. Click OK, as necessary, until you return to the Novell BorderManager 3.7 Access Rules page > click OK to update the access rules.

Setting Up Time Restrictions for Access Rules

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

To specify time restrictions for an access rule:

1. In NetWare Administrator, right-click the object where the access rule has been created and select Details.
2. Select the Novell BorderManager 3.7 Access Rules page.
3. In the access rules list, highlight the access rule for which you want to specify time restrictions. Click Time Restrictions, then click Specified.
4. In the grid, click and drag through the days and times that you want the access rule to be in effect.

   A highlighted area means the access rule applies to the source only during that time. To revert to enforcing the rule at all times, click None.
5. Click OK to return to the Novell BorderManager 3.7 Access Rules page, then click OK to update the access rules.

Viewing All Rules That Apply to an Object

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

To view the effective rules of an object:

1. From an administrator workstation, log in to the NDS or eDirectory tree where the Novell BorderManager 3.7 server is located and start the NetWare Administrator utility.
2. Locate the source object for which you want to view access rules in the NDS or eDirectory tree > right-click the object > select Details.

   The object must be a Server, Organization, Organizational Unit, or Country.
3. Select the Novell BorderManager 3.7 Access Rules page.
4. Click Effective Rules.

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

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

Completing Advanced Setup, Configuration, and Management Tasks

In addition to the basic setup procedures described in this 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 Managing Access Control and include the following:

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

8 Setting Up Authentication Services

Novell® BorderManager® 3.7 Authentication Services enable remote users to dial in to NetWare® networks and access network information and resources. It maintains security by requiring users to authenticate using the Remote Authentication Dial-In User Service (RADIUS) protocol. It is comprised of the following three components:

- RADIUS server (the NetWare server on which you install the Novell BorderManager 3.7 Authentication Services software)
- Network access server (the device remote users dial in to)
- Administration workstation (NetWare Administrator)

This section contains the following information:

NOTE: This chapter describes the tasks required to set up, start, and test an initial implementation of Novell BorderManager 3.7 Authentication Services. For

planning and conceptual information about Novell BorderManager 3.7 Authentication Services, refer to the Novell BorderManager 3.7 Overview and Planning Guide, available in the online documentation. Make sure you understand this information before setting up and configuring Novell BorderManager 3.7 Authentication Services.

Novell BorderManager 3.7 Authentication Services Prerequisites

Before you set up Novell BorderManager 3.7 Authentication Services, verify that the following prerequisites have been met:

- TCP/IP is configured and functioning on the RADIUS server and the network access server
- The network access server is RADIUS compliant (IETF RFC 2138 and RFC 2139 for accounting support)
- RADIUS authentication is enabled on the network access server
- The RADIUS server address on the network access server is set to either the NetWare server or the Windows* NT server on which the RADIUS server software will be installed
- The RADIUS secret is established and known by the network access server

Upgrading From A Previous Version

If you are upgrading Novell BorderManager 3.7 Authentication Services configuration information created with a previous version of the product to the current version, consider the following issues:

RADIUS Server	The current RADIUS server (RADIUS.NLM) can work with dial access configurations created with both previous and current versions of Novell BorderManager 3.7 Authentication Services.
NetWare Administrator	The current snap-in module to NetWare Administrator converts the dial access configuration created in a previous version to a new format that is incompatible with previous versions of NetWare Administrator.

Previous versions of the snap-in module to NetWare Administrator must only be used with a dial access configuration created using this snap-in module.

A previous version of the snap-in module to NetWare Administrator cannot be used with the current version of the RADIUS server.

Creating a Dial Access System Object

An NDS® or Novell eDirectory™ Dial Access System object stores configuration information for RADIUS servers and can manage a common configuration for a collection of RADIUS servers working together. You must create at least one Dial Access System object in the NDS or eDirectory tree where your RADIUS server resides. All participating RADIUS servers use the Dial Access System object for configuration. The information stored in the object includes the following:

- Client configuration—Allows you to define IP addresses for the network access servers and the shared secrets used among the RADIUS servers, network access servers, and proxy RADIUS servers from which requests will be received.
- Domains—Allow you to configure other RADIUS servers to which you want to forward RADIUS requests.
- Authentication policy—Allows you to define an authentication policy for the Dial Access System.
- Remote connections—Allow you to restrict the number of concurrent remote connections.
- Lookup context—Defines the search path for objects.

To create a Dial Access System object:

1. In NetWare Administrator, select the Organization or Organizational Unit object where you want to place the Dial Access System object.
2. From the Object menu, click Create > Dial Access System > OK.
3. Enter the name for the Dial Access System object > click Create.
4. Double-click the Dial Access System object you just created, then click Clients > Add.

4a Enter the IP address of the network access server in the Client Address field.

4b Select Client Type (the default is Generic RADIUS).

4c Enter the RADIUS secret. Reenter the secret.

The RADIUS secret should be a random string of 20 to 30 alphanumeric characters. The secret is used to protect authentication information sent across the network.

4d Check Add Another Client if you want to add another network access server after you created this one. Leave this check box unchecked if this is the last (or only) RADIUS client that you will create.

4e Click OK.

5 Select Authentication Policy to configure an authentication policy.

5a Click Add.

5b Select one of the following under Policy Type:

- Authentication Method—Remote users are authenticated using an authentication policy that is not listed, such as token authentication. Browse and select the authentication policy.
- NetWare Password—Remote users are authenticated using the same passwords used for NetWare print and file services.
- Dial Access Password—Remote users are authenticated using separate passwords that are stored encrypted in the NDS or eDirectory database.
- Dial Access Password (CHAP)—Remote users are authenticated using Challenge Handshake Authentication Protocol (CHAP) passwords.
- Any User-Assigned Device—Remote users are authenticated using a token assigned to a user.

5c Select one of the following under Policy Rules:

- Must Authenticate By This Method—Remote users always authenticate using the selected policy type.
- Required If Assigned—Remote users always authenticate using the selected policy type (enabled only for Authentication Method and User-Assigned Device).
- Optional—Remote users will be able to choose the selected policy for authentication.

5d Select Decrement Grace Logins to set the counter used to limit grace logins.

5e Select Add Another Policy to specify another authentication policy.

6 Select Lookup Context if you want to use a common name login.

6a Click Add.

6b Browse and select the name context.

6c To add another search context, check Add Another Context.

6d Click OK.

7 Select Miscellaneous.

8 Select Change Dial Access System Password.

8a Enter the new password.

The Dial Access System password is used to generate encryption keys that protect passwords and secrets. Therefore, we recommend that the Dial Access System password be a random string of 20 to 30 alphanumeric characters. The password is required to start the service.

8b Reenter the new password > click OK.

9 Click OK twice.

You are now ready to create a Dial Access Profile object. Refer to the NetWare Administrator online help for information about specific configuration procedures for domains and remote connection restrictions.

Creating a Dial Access Profile Object

Each Dial Access Profile object defines the common attributes of a service used by one or more dial-in users. This simplifies administration by eliminating the need to configure the attributes of each user. You can define as many profiles as required to define different services. For example, you can create a Telnet profile that enables users to connect a terminal server to a host. You can also create a Telnet profile that enables users to connect to a host using a terminal or a terminal emulation program.

The Dial Access Profile object contains a list of RADIUS attributes that specify the configuration for creating a specific service.

Creating a Dial Access Profile Object for PPP Service

To create a Dial Access Profile object for the Point-to-Point Protocol (PPP) service:

1. In NetWare Administrator, select or create the Organizational Unit where you want to place the Dial Access Profile object.
2. From the Object menu, click Create > Dial Access Profile > OK.
3. Enter a name for the Dial Access Profile object (such as PPP) > click Create.
4. Double-click the Dial Access Profile object you just created > click Attributes > Add.
   - 4a. Double-click Generic.
   - 4b. Select Service-Type from the Attribute list and select Framed in the Value field.
   - 4c. Select Framed-Protocol from the Attribute list and select PPP in the Value field.
5. Select the appropriate attributes from the list > click OK.
6. When you have finished adding attributes, uncheck Add Another Attribute > click OK from the Edit Attribute dialog box.
7. Click OK.

You can now enable users for dial access services.

Creating a Dial Access Profile Object for Telnet Service

To create a Dial Access Profile object for Telnet service:

1. In NetWare Administrator, select or create the Organizational Unit where you want to place the Dial Access Profile object.
2. From the Object menu, click Create > Dial Access Profile > OK.
3. Enter a name for the Dial Access Profile object (such as Telnet) > click Create.
4. Double-click the Dial Access Profile object you just created > click Attributes > Add.
   - 4a. Double-click Generic.

4b Select Service-Type from the Attribute list and Select Login in the Value field.

4c Select Login-Service from the Attribute list and select Telnet in the Value field.

4d Select Login-IP-Host from the Attribute list and enter the host IP address in the Value field.

5 When you have finished adding attributes, uncheck Add Another Attribute > click OK from the Edit Attribute dialog box.

6 Click OK.

You can now enable users for dial access services.

Enabling a User for Dial Access Services

Dial access properties are added to the User object when the Novell BorderManager 3.7 Authentication Services software is installed. The User Dial Access Services property page allows you to

- Enable a user for dial access services
- Select the appropriate Dial Access System for the user
- Set the Dial Access System password for the user (if you use separate passwords for dial-in users)
- Configure or define dial-in services for the user
- Select a default service if a user is configured for more than one dial access service

In addition, the Organization and Organizational Unit Dial Access Services property pages let you define default dial access properties for all users in the selected container. You can also manage dial access services using a Group object. Refer to the NetWare Administrator online help for information about specific configuration procedures.

NOTE: You can specify dial access properties that are unique to a User object on a per-property basis. This means that a User object dial access setting can override the dial access setting of the parent container object, but other settings that are not overridden in the User object will always be inherited from the parent container object.

To enable a user for dial access services, complete the following steps:

1. In Netware Administrator, click the User object that you want to enable for dial access services and select Dial Access Services.
2. Select one of the following Dial Access Control settings:
   - Disable—Disables dial access services for this user.
   - Enable—Enables dial access services for this user.
   - Use Container Setting—Specifies that the Dial Access Control setting will be inherited from the parent container object.

   NOTE: You can still specify dial access properties that are unique to a User object on a per-property basis when Use Container Setting is selected. Settings that are not overridden are always inherited from the parent container object.
3. Browse the NDS or eDirectory tree and select a Dial Access System object.

   In most situations, all users select the same Dial Access System object.
4. If the password policy is set to Use Separate Dial Access Passwords, complete the following substeps:

   4a. Click Set Dial Access Password.

   4b. Enter the password. Reenter the password > click OK.

   The Set Dial Access Password button might be disabled for one of the following reasons:
   - Use NDS or eDirectory Password is selected in the Dial Access System object.
   - No Dial Access System object is specified for the User object or the parent container.
   - No password is set for the Dial Access System object.
5. If desired, select additional configured services and the appropriate attributes > click OK twice.

You can now start Novell BorderManager 3.7 Authentication Services.

Starting Novell BorderManager 3.7 Authentication Services

You should have performed the following tasks before you start Novell BorderManager 3.7 Authentication Services:

- Create a Dial Access System object
- Create a Dial Access Profile object
- Enable one or more User objects for dial access services

To start the Novell BorderManager 3.7 Authentication Services program on a NetWare server, complete the following steps:

1. Enter the following command at the server console for Novell BorderManager 3.7 Authentication Services:

   LOAD RADIUS

   TCP/IP should already be configured and running.

2. Enter the distinguished name of the Dial Access System object.

3. Enter the password of the Dial Access System object.

   The following message should be displayed:

   ```
   RADIUS services started.
   ```

You can now use Novell BorderManager 3.7 Authentication Services.

Refer to Testing Novell BorderManager 3.7 Authentication Services if you want to test whether your Novell BorderManager 3.7 Authentication Services configuration is working properly.

Testing Novell BorderManager 3.7 Authentication Services

To determine whether your Novell BorderManager 3.7 Authentication Services configuration is working properly:

1. In NetWare Administrator, check that you have a valid Dial Access System object.

2. Create a new Dial Access Profile object.

3. Enter PPP for the Dial Access Profile name and click OK.

4. Click the newly created PPP Dial Access Profile object > Attributes > Add.
5. In the Attribute field, select Service-Type from the list.
6. In the Value field, select Framed.
7. Uncheck Add Another Attribute > click OK twice.
8. Click the User object that you want to enable for PPP access > Dial Access Services.
9. Select the Dial Access System object that you already created.
10. Under Configured Services, select Add.
11. Select the PPP Dial Access Profile object that you already created and click OK twice.
12. From a dial-in client configured to use PPP, connect to the network access server.
13. When prompted for a username, enter the distinguished name of the newly enabled User object, for example, .eric.acme.
14. Enter the password for the user.
15. Check the dial-in client to see whether it has access to the network.

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 Managing Access Control and include the following:

- Changing RADIUS server options
- Setting up dial access services and dial access attributes
- Setting up user and groups for container and group administration
- Setting up remote connection restrictions
- Planning token authentication
- Managing token authentication
- Planning authentication policies

- Setting up authentication policies
- Planning RADIUS proxy services
- Managing RADIUS proxy services
- Displaying RADIUS status messages

9 Setting Up Alert Notification

Novell® BorderManager® 3.7 Alert monitors server performance and security, and reports potential or existing server problems that affect the performance of configured Novell BorderManager 3.7 services.

Novell BorderManager 3.7 Alert reports server events indicating a potential problem with any of the following:

- Server performance
- License acquisition, excluding Novell BorderManager 3.7 Authentication Services licenses; Novell BorderManager 3.7 Alert will not report a problem with a Novell BorderManager 3.7 Authentication Services license
- Security
- Proxy server connections

Novell BorderManager 3.7 Alert monitors a predefined set of server events. However, you can select the individual events for which you want to receive notification.

When an alert is triggered on a Novell BorderManager 3.7 server, the default notification includes the following:

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

NOTE: Novell BorderManager 3.7 Alert output supports automatic paging from your e-mail system. This requires additional configuration and the process varies depending on the e-mail software you use. Consult your e-mail software documentation to determine if this option is configurable for your system.

This chapter explains the tasks you need to complete to set up an initial implementation of Novell BorderManager 3.7 Alert e-mail notification. It contains the following sections:

- "Setting Up Alert E-Mail Notification" on page 134
- "Completing Advanced Setup, Configuration, and Management Tasks" on page 137

NOTE: This chapter describes the tasks required to set up an initial implementation of Novell BorderManager 3.7 Alert. For planning and conceptual information about Novell BorderManager 3.7 Alert, refer to Novell BorderManager 3.7 Overview and Planning Guide, available in the online documentation. Make sure you understand this information before setting up and configuring Novell BorderManager 3.7 Alert.

Setting Up Alert E-Mail Notification

To set up Novell BorderManager 3.7 e-mail notification:

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

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

2. Click the Novell BorderManager 3.7 Alert page.
3. Select one of the following notification schemes:

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

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

     To view the inherited information, click Effective Configuration. The Effective Configuration information is read-only. To change the alert information, identify the NDS or eDirectory container in the Location of Specification field and open the Novell BorderManager 3.7 Alert page from that container's Details page.

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

4 (Optional) If you selected Send Alert earlier, specify the alert conditions for which you want notification.

4a Click Alert Conditions.

4b Click Specific (the default is All).

4c Check the check boxes to select the alert conditions.

4d Click OK.

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

NOTE: The Novell BorderManager 3.7 server must be configured with at least one e-mail server. Otherwise, alert notification will fail.

5a Click Add for the E-mail Alert field and enter the e-mail address of the person to be notified by Novell BorderManager 3.7 Alert.

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

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

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

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

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

Add as many e-mail servers as necessary. Although there is no upper limit on the number of backup servers that can be added, Novell BorderManager 3.7 Alert sends alerts to only one e-mail server on the list.

HINT: To increase the performance of Novell BorderManager 3.7 Alert, enter the IP addresses of e-mail servers. When IP addresses are used, the Novell BorderManager 3.7 server is not required to process Domain Name System (DNS) lookups to resolve the DNS hostnames of e-mail servers.

5d (Optional) To remove an e-mail server's from the list, highlight the e-mail server name or IP address > click Delete for the E-mail Server field.

5e (Optional) To change an e-mail server's status as a primary or backup server, click the Up-arrow or Down-arrow to move the e-mail server's name or IP address up or down the list.

6 Click OK to save the configuration and exit the Details page.

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

If you enabled an alert configuration for an entire organization, it might take a while for all Novell BorderManager 3.7 servers to be notified of the configuration change in NDS or eDirectory.

7 (Optional) If you enabled an alert configuration for an entire organization and want a specific server to use the alert configuration immediately, rather than after NDS or eDirectory synchronization occurs, complete the following substeps:

7a Double-click the Server object representing the Novell BorderManager 3.7 server you want to begin using the alert configuration immediately.

7b From the Server object's Details page, click Novell BorderManager 3.7 Alert to view the Novell BorderManager 3.7 Alert page for the server.

7c Click Refresh Server.

IMPORTANT: When you first open the Novell BorderManager 3.7 Alert page, the Refresh Server button is available. Clicking Refresh Server causes BRDSRV.NLM to read the new alert configuration for this server only. It does not trigger a full NDS or eDirectory synchronization. If you modify the alert configuration for this Server object, the Refresh Server button is inactive and no longer an option.

Completing Advanced Setup, Configuration, and Management Tasks

In addition to the basic setup procedures described in this 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 Managing Alert Messages and include the following:

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

A Additional Information

This appendix provides instructions for licensing the Novell® BorderManager® 3.7 software on your NetWare® server using the License Install utility or NetWare Administrator. You can use these procedures to install an initial license, install an evaluation license, or install a new license over an expired license. If you do not have a valid or trial license installed, Novell BorderManager 3.7 will not load. This section contains the following information:

Master License Agreement (MLA), Corporate License Agreement (CLA), and Volume License Agreement (VLA) licenses are not assigned to a specific server. Therefore, they can be used by multiple servers in the same tree and need to be installed only once. Other license types, including trial licenses, must be installed and assigned to individual servers. If you use the License Install utility, the server license assignment is made automatically. If you use NetWare Administrator, you must make the server license assignments manually. Using the License Install utility is the preferred method.

Using the License Install Utility

When you use this utility to install licenses, the licenses are automatically assigned to the server from which you run the utility. This is the preferred method.

To install licenses at the server console using the License Install utility:

1. At the server console, enter

   LOAD LICINST

2. Log in to the Novell BorderManager 3.7 server with administrative rights.
3. Enter the path to the license envelope (for example, A:\ if your license is on a diskette).
4. Select the license envelope containing the licenses.
5. Press Enter.

   A summary window displays the licenses installed.

6. Press Esc twice > select Yes to exit the utility.

Using NetWare Administrator

When you use NetWare Administrator to install licenses, you must manually assign each license to the server.

To install licenses using NetWare Administrator:

1. From an administrator workstation, log in to the Novell BorderManager 3.7 server with administrative rights.
2. Map a drive to the SYS: volume of the Novell BorderManager 3.7 server > run NetWare Administrator.
3. Select the Novell BorderManager 3.7 server on which you want to install licenses.
4. From the Tools menu, select Install Licenses > Install Envelope.
5. Enter the path to the license envelope (for example, A:\ if your license is on a diskette), or click Browse to locate the license envelope.
6. Select the license envelope containing the licenses.
7. Select the license certificates to install.
8. Confirm the context field in which to install the licenses. Modify this field if necessary.
9. Review the envelope description and click OK.

   A summary report of successfully installed licenses is displayed.

10 Select Close, then exit and restart NetWare Administrator to refresh the license view.

11 To assign the license to an individual server, complete the following substeps if your license is not an MLA, CLA, or VLA:

11a Double-click the license container you installed.

The license certificate is displayed.

11b Double-click the license certificate > select Details > Assignments.

11c Click Browse to locate the Novell BorderManager 3.7 server on which to install the license certificate, select the server > click Add.

11d Select the context containing the Novell BorderManager 3.7 server, then click OK.

12 Exit NetWare Administrator.

Configuring TCP/IP

You must have TCP/IP bound and configured to install the Novell BorderManager 3.7 software. You can download the most recent version of TCPIP.NLM from the Novell Technical Support Web site. There are currently three versions of the TCPIP.NLM:

- A version for NetWare servers without Novell BorderManager 3.7 installed
- A version for NetWare servers with the 40-bit encryption version of Novell BorderManager 3.7 installed
- A version for NetWare servers with the 128-bit encryption version of Novell BorderManager 3.7 installed

Make sure you get the appropriate version required for the server on which you will be installing TCP/IP.

To verify that TCP/IP is configured on your server, complete the following steps:

1 At the server console prompt, enter

```
CONFIG
```

2 Review the list for TCP/IP protocol configuration.

If TCP/IP is not configured, continue with "Configuring TCP/IP" on page 141.

Loading TCP/IP

To load TCP/IP:

1. At the NetWare server console prompt, enter

   ```
   LOAD INETCFG
   ```

2. To transfer the LAN driver, protocol, and remote access commands, select Yes.
3. From the Internetworking Configuration menu, select Protocols > TCP/IP.
4. Highlight TCP/IP Status > press Enter.
5. Select Enabled > press Enter.
6. To return to the Internetworking Configuration menu, press Esc twice.
7. From the Internetworking Configuration menu, select Bindings.
8. Press Ins > select TCP/IP.
9. From the list of configured network interfaces, select the network board to which TCP/IP will bind.
10. Enter your local IP address and subnet mask.
11. To update the TCP/IP configuration, press Esc > select Yes.
12. To reinitialize the system, enter the following at the server console:

    ```
    REINITIALIZE SYSTEM
    ```

13. To verify that TCP/IP is configured successfully, enter the following at the server console:

    ```
    CONFIG
    ```

Adding an NDS or eDirectory Replica

Because Novell BorderManager 3.7 is a Novell Licensing Services (NLS) enabled application, the first Novell BorderManager 3.7 server installed into a tree or a particular partition must be installed on a NetWare server that holds a read/write replica of that partition. All Novell BorderManager 3.7 servers installed into the same partition at a later time are not required to have a read/write replica. You do not need to add a replica to install Novell BorderManager 3.7 on the first three servers in a tree because these servers already have NDS® or Novell eDirectory™ replicas by default. The first

server holds a master, and the second and third servers hold read/write replicas. Use the NDS or eDirectory Manager utility to add a read/write replica.

This utility is available to NetWare 5.1 users only.

To add a read/write replica to a server, complete the following steps:

1. From your administration workstation, run the NDS or eDirectory Manager utility (SYS:\PUBLIC\WIN95\NDSMGR32.EXE).
2. Select the partition you want to replicate.
3. From the object menu, select Add Replica.
4. Click Browse to select the server on which to place the replica.
5. Click the Server object representing the NetWare server to which you want to add the read/write replica > click OK.
6. Click the Read/Write radio button > click OK.
7. Select Yes to continue.

   After the utility adds the replica, the replica's status is displayed as New. After the status of the replica changes to On, you can continue with the Novell BorderManager 3.7 installation.
8. From the object menu, select Exit.

If you are a NetWare 6.0 user to add a read/write replica to a server, complete the following steps:

1. Go to ConsoleOne > log in > select the container/tree
2. Select View > Partition or Replica View
3. On the right panel select Replica List table > right click
4. Select Add Replica
5. Select the browser > select the server where you want to put replica
6. Select the replica type as read/write > click OK