Novell BorderManager®

3.9

www.novell.com

TROUBLESHOOTING GUIDE

April 05, 2007

Novell®

Legal Notices

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

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

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

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

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

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

Novell Trademarks

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

Third-Party Materials

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

About This Guide

Novell® BorderManager® 3.9 includes premier firewall and VPN technologies that safeguard your network and help you build a secure identity management solution. With the powerful directory-integrated feature in the Novell BorderManager, you can monitor users' Internet activities and control their remote access to corporate resources.

This documentation provides troubleshooting information for Novell BorderManager 3.9 components. It provides hints, bebuggging information, known issues, and procedures to help you install and configure Novell BorderManager 3.9 successfully.

This documentation includes the following sections:

Audience

This audience for this documentation are experienced network administrators. This document is also useful for end-users who have VPN client installed on their computers.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to Novell Feedback Web site (http://www.novell.com/documentation/feedback.html) and provide your comments.

Documentation Updates

For most recent version of the *Virtual Private Network FAQ*, visit the Novell Documentation Web site. (http://www.novell.com/documentation/nbm39/index.html)

Additional Documentation

It is recommended that you read this document as a supplement to the following other related documentation of Novell BorderManager 3.9:

- *Novell BorderManager 3.9 Administration Guide*
- *Novell BorderManager 3.9 Installation Guide*
- *Novell BorderManager 3.9 Proxy and Firewall Overview and Planning Guide*

- *Novell BorderManager 3.9 Virtual Private Network Client Installation Guide*
- *Novell BorderManager 3.9 Virtual Private Network Deployment Frequently Asked Questions*

Documentation Conventions

In Novell 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.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

Contents

Logs, Screens, Tools, and Parameters

1

This section provides information on the important logs and screens of Novell BorderManager. This section covers:

- Section 1.1, "Logs," on page 9
- Section 1.2, "Screens," on page 10
- Section 1.3, "VPN Debug Console Screen," on page 10
- Section 1.4, "Tools," on page 11
- Section 1.5, "VPN Configuration Dump Tool," on page 12
- Section 1.6, "Set Configuration Parameters," on page 15

1.1 Logs

***Table 1-1** Logs*

Component	Log File Location	Description	When to Look
Install	`sys:\ni\data\NBM_Instlog.csv`	Install summary.	After install.
Install (cache volume creation)	`sys:\ni\data\cachev.log`	Logs of cache volume creation on NetWare® 6.5.	When cache volume creation on NetWare fails.
Install	`sys:/ni/data/ni.log`	Contains milestone information on the stages of install.	After install or if the install fails.
Install	`sys:/ni/data/nierrors.log`	Information about fatal errors during installation.	If the install fails with a fatal error.
Install (VPN configuration migration)	`sys:/ini/data/vpnupgrade.log`	The log for VPN configuration migration.	If VPN configuration migration fails.
IKE VPN Server	`/etc/ike/ike.log`	Contains the IKE log messages.	When client-to-site or site-to-site connections are not established, or when the connections are dropped. (The level of informational or error messages printed depends on the IKE log level. This can be set through a configuration parameter.)

1.2 Screens

Table 1-2 Screens

Screen Name	Description	When to Look
Logger screen	Default screen for NetWare 6. Contains Novell BorderManager and non-Novell BorderManager logs	When VPN configuration is not saved. The configuration might show a status of the success, but you still cannot see the changes that you saved. Check the logger screen for Java* exceptions. To see if configuration changes made in iManager have taken effect on the server.
IKE screen	Shows IKE log messages	The output of this screen is the same as that logged into the IKE log file. See `/etc/ike/ike.log`.

1.3 VPN Debug Console Screen

The Virtual Private Network (VPN) debug console screen is available on each VPN server.

The VPN-NW console screen contains VPN specific logs and dumps of internal data structures. This shows the configuration information and the state of the server.

You look at this screen when you want to see the IPSec data structures and thereby trace the progress of a connection. It can dump information about established SAS, configuration, policies, and similar issues.

1.3.1 Options

Table 1-3 VPN Debug Console Screen Options

Number	Display Action
1	VPMaster/VPSlave miscellaneous information
2	IPSEC SA List
3	VPNINF miscellaneous information
4	Site-to-site member details
5	Client-to-site authentication rules
6	Client-to-site traffic rules
7	Site-to-site traffic rules
8	Site-to-site IPSEC policies

Number	Display Action
9	VPN address pool

1.4 Tools

Table 1-4 *Tools*

Tool Name	Description
`CASAUDIT`	`CASAUDIT` is a NetWare console tool to display the audit trail records that were logged using the CSLIB facility in NetWare. Novell BorderManager uses the CSLIB facility for its audit logs and these records can be displayed using this utility. Use this tool to detect any errors while establishing connection to the remote VPN server, as well as synchronization errors after establishing the connection logged to the `CSAUDIT` database. You can view this database by loading `CSAUDIT` at the server console.
`CALLMGR`	`CALLMGR` is a NetWare utility used to monitor the status of the wide area network (WAN) connections or to start and stop WAN calls manually. Use this tool to see the inbound or outbound connection from or to a remote VPN server. If you cannot see the function, there is an issue with the VPTUNNEL at the CSL layer. Suggest that customers verify that the vptunnel.lan driver is loaded, without any error messages. An example of an error could be: `A licensing issue caused the tunnel not to load`. `CALLMGR` is available at the root of the product CD in the `CALLMGR` directory.
`TCPCON`	`TCPCON` is a TCP/IP console NetWare NLM™ that enables a network administrator to monitor server or router activity in the TCP/IP segments of the network. This tool can be used when the tunnel is up and synchronized. At this time, point all routing table entries should be correct. That is, to get to a remote site through the tunnel, the next hop should be the local VPN tunnel address. For more details on troubleshooting this, refer to TID # 10011169 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=10011169&sliceId=&dialogID=31412574&stateId=1%200%201776526) on the Novell Support Web site.

Tool Name	Description
MONITOR	MONITOR is the NetWare Console monitor tool, which allows an administrator to monitor various server information including the open connections, information volumes, system resources, the server parameters, CPU utilization, etc. This is very useful for monitoring the performance and the runtime status of the NetWare system and also of the loaded modules. This tool is useful for confirming that packets are going through the VPTUNNEL interface, and not the local LAN interface. If the routing table is set up incorrectly, the packets going to the remote destination might end up going out on the LAN card, and not the VPN interface.
VPMON	VPMON is the monitoring frontend for Novell BorderManager 3.9 VPN services. This runs as a NetWare Loadable Module™ and interfaces with the Novell Remote Manager (NRM) framework to provide the monitoring functionality for the VPN services from the browser using the NetWare Remote Console. VPMON is available at the root of the product CD in the VPN directory.
VPN Upgrade Tool	Use this tool when you are upgrading to Novell BorderManager 3.9 from Novell BorderManager 3.8, and VPN Configuration Migration has failed during the installation process. You can also use this utility when you have not selected the VPN Configuration Migration option during the Novell BorderManager 3.9 installation and want to migrate your existing VPN configuration now.
Cache Volume Creation Tool	Use this utility to create traditional volumes on Netware 6.5. Proxy cache directories require traditional NetWare volumes.
VPN console options	This tool is useful for narrowing issues with the IKE/IPSEC SA negotiation, and determining that the VPN site-to-site and client-to-site profiles are setup correctly.

1.5 VPN Configuration Dump Tool

The VPN configuration dump tool is a command line utility that dumps the required VPN configuration information to a file. The VPN configuration is read from Novell eDirectory™ and written to a text file on the server.

The user is provided with menus indicating which specific type of dump can be chosen.

- Section 1.5.1, "Information That Can Be Dumped," on page 13
- Section 1.5.2, "Viewing the Dump Information," on page 13
- "Example on Windows" on page 14

1.5.1 Information That Can Be Dumped

- The following VPN configuration information can be dumped into a file: ◆**VPN Server Information:** This includes information about services being hosted on the server.
- **VPN Client-to-Site Configuration:** This includes general configuration, traffic, and authentication rules. The general parameters include remote LDAP server information and DNS/SLP configuration.
- **VPN Site-to-Site Configuration:** This includes general configuration, member details and traffic and third-party rules.

1.5.2 Viewing the Dump Information

The dump tool can be used on Netware as well as Windows*.

- "On NetWare" on page 13
- "On Windows" on page 14

On NetWare

To download the dump tool files:

1. Locate the `vpndump.ncf` and `vpnDump.jar` files.

   These two files are available as a zip file named `vpndump_NW.zip` in the `unsupported` directory under VPN on the product CD.
2. Unzip the `vpndump_NW.zip` file on the `sys:` volume of the NetWare server.

   The `vpndump_NW.zip` file must be unzipped on the `sys:` volume of the NetWare server. The following files are copied in the specified folders:
   - `vpnDump.jar` in `sys:\tomcat\4\webapps\nps\web-inf\lib`
   - `vpndump.ncf` in `sys:\system`
3. Run Tomcat 4 and restart Tomcat.

To use the tool:

1. Execute `vpndump.ncf` by providing the following command line arguments:

   ```
   vpndump <user> <context>
   ```

   For example: `vpndump admin novell`
2. When prompted, specify the password and choose the type of dump.
3. The configuration is dumped to a text file and the name of the text file is displayed.

On Windows

1. Locate the dump tool files and extract them to any folder on a Windows machine.

   The files for the dump tool on Windows are

   - `vpndump.bat`
   - `vpnDump.jar`
   - `vpndump_win_readme.txt`

   These three files are available as a zip file named `vpndump_win.zip` in the `unsupported` directory under VPN on the product CD.

2. Edit the `vpndump.bat` file. To do so, change the `SET UDR=C: \ imgrsdk\tomcat` line to provide the tomcat_home path.

   The tomcat home path is the folder where tomcat has been installed such as `SET UDR= tomcat_home absolute path >`

3. Save the `vpndump.bat` file.

4. Run the `vpndump.bat` file by providing two arguments, user and context. `vpndump` *<user> <context>*

   For example, `vpndump admin novell`

5. When you are prompted, provide the Tree IP, Novell BorderManager server name, and the password.

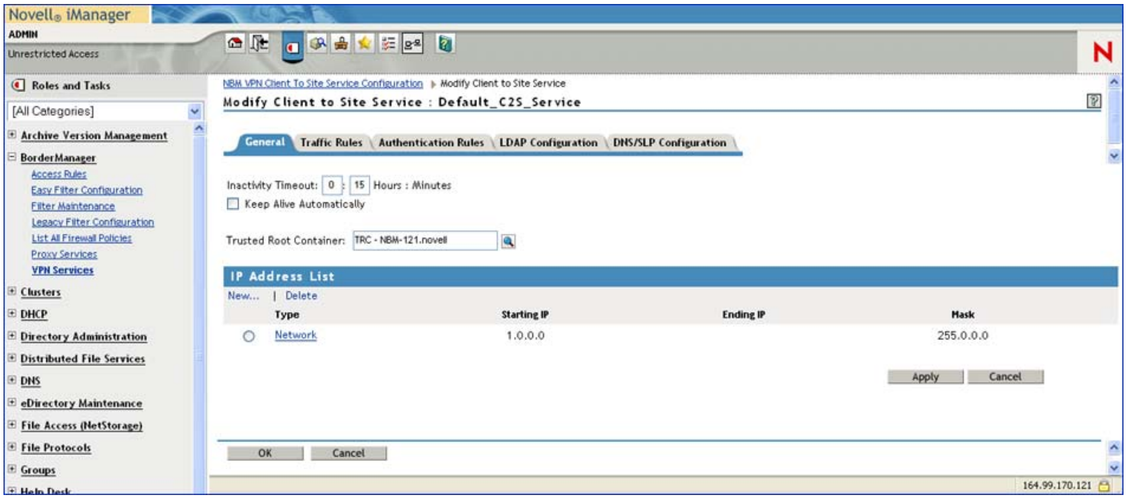
   After successful authentication to the server, you can choose the type of dump.

   The configuration is dumped to a text file and the name of the text file is displayed.

Example on Windows

The following screen shot displays how the configuration dump tool information is available on a Windows machine.

Figure 1-1 *VPN Configuration Dump Tool on Windows*



Modify Client to Site Service : Default_C2S_Service

Inactivity Timeout: 0 : 15 Hours : Minutes

☐ Keep Alive Automatically

Trusted Root Container: TRC - NBM-121.novell

IP Address List

	Type	Starting IP	Ending IP	Mask
○	Network	1.0.0.0		255.0.0.0

1.6 Set Configuration Parameters

This section explains the following configuration parameters.

- "set ike debugmask" on page 15
- "set ike dumpsa" on page 15
- "set ipsec sadump" on page 15

set ike debugmask

Explanation: 2 = Only message headers (default)

4 = Message body (Use this only if you are trying to look at the IKE protocol messages)

8 = Attributes (this is useful if there is an error in IKE logs saying that the quick mode proposal is not chosen; in that case, set the debug mask to 8 | 2 = 10)

set ike dumpsa

Explanation: This dumps the existing IKE SA (waiting list, up list, working list).

Action: Toggle the numbers on the `ike.log` to get the SA information dumped on the IKE screen. The numbers are 1 and 2.

set ipsec sadump

Explanation: This dumps IPSEC SAs to the console.

This is similar to VPN debug console option 2, but prints on screen 1, where you cannot scroll up or down.

Action: Toggle the numbers on the `ike.log` to get the SA information dumped on the IKE screen. The numbers are 1 and 2.

Troubleshooting Installation 2

This section provides some of the important error messages that might appear while installing Novell BorderManager 3.9. It also covers some of the common install problems.

This section contains information on the following:

- Section 2.1, "Minimum Requirements Check Messages," on page 17
- Section 2.2, "License Selection Problems," on page 19
- Section 2.3, "Installation Messages," on page 19
- Section 2.4, "VPN Configuration Migration Messages," on page 23
- Section 2.5, "Common Install Scenarios," on page 24

2.1 Minimum Requirements Check Messages

- "Improper Version of Netware" on page 17
- "No Version, or Improper Version of NICI" on page 17
- "No Version, or Improper Version of eDirectory" on page 17
- "No Version, or Improper Version of LDAP" on page 18
- "Improper Version of Novell BorderManager" on page 18
- "No Version, or Improper Version of PKI" on page 18
- "No Version, or Improper Version of SAS" on page 18
- "No Version, or Improper Version of NetNLM32.NLM" on page 18
- "Improper Version of tcp.nlm or tcpip.nlm or bsdsock.nlm" on page 18
- "No Version, or Improper Version of iManager" on page 19

Improper Version of Netware

Explanation: The install discontinues if the required version of Netware® is not present.

Action: Install Netware 6.5 SP6 before proceeding with Novell BorderManager 3.9 installation.

No Version, or Improper Version of NICI

Explanation: The install discontinues if the required version of NICI is not present.

Action: The minimum required version of NICI is 2.6.

No Version, or Improper Version of eDirectory

Explanation: The install discontinues if the required version of eDirectory™ is not present.

Action: The required version of eDirectory is 873.9.

No Version, or Improper Version of LDAP

Explanation: The install discontinues if the required version of LDAP is not present.

Action: The required version of LDAP is 87.3.0.

Improper Version of Novell BorderManager

Explanation: Upgrading from versions of Novell BorderManager earlier than Novell BorderManager 3.8 is not possible.

Action: Upgrading from Novell.BorderManager 3.8 to Novell BorderManager 3.9 is allowed. If your version is earlier than 3.8, upgrade to 3.8 before upgrading to 3.9.

No Version, or Improper Version of PKI

Explanation: The install discontinues if the required version of Public Key Infrastructure (PKI) is not present.

Action: The required version of PKI is 3.2.0.

No Version, or Improper Version of SAS

Explanation: The install discontinues if the required version of Secure Authentication Services is not present.

Action: The required version of SAS is 1.7.0.

No Version, or Improper Version of NetNLM32.NLM

Explanation: The install discontinues if the required version of `NetNLM32.NLM` is not present.

Action: The required version of `NetNLM32.NLM` is 6.00.06, dated September 25, 2006.

The latest version of the NLM™ can be found at the Novell Support Web site. (http://www.novell.com/support/)

Improper Version of tcp.nlm or tcpip.nlm or bsdsock.nlm

Explanation: These NLM programs are optional requirements, and the installation continues without them.

However, Novell BorderManager 3.9 might not function as desired if the proper file version is not available.

Action: The following table give a list of the required versions:

NLM Name	NLM Version	
	Null Encryption	**Domestic Encryption**
`tcp.nlm`	6.80.01	6.90.01
`tcpip.nlm`	6.80.02	6.90.02
`bsdsock.nlm`	6.80.02	6.90.02

No Version, or Improper Version of iManager

Explanation: You might encounter problems in administering Novell BorderManager 3.9 if you have an incorrect version of iManager.

Action: The required version of iManager is 2.6.

2.2 License Selection Problems

- "User selected Skip License during installation" on page 19
- "Error Validating Licenses, or Invalid License Location" on page 19

User selected Skip License during installation

Explanation: Novell BorderManager 3.9 does not function if the license is not installed.

Action: Use iManager 2.6 to install the license separately later.

Error Validating Licenses, or Invalid License Location

Explanation: Novell BorderManager 3.9 services do not function if the licenses are installed in the wrong location.

Action: Check the license location path. Paths other than the local system, such as the Novell BorderManager 3.9 source path or a floppy drive, are not valid. Also, ensure that the path contains licenses for the selected Novell BorderManager 3.9 services.

2.3 Installation Messages

- "File Copy" on page 19
- "Firewall Schema Extension" on page 20
- "Filters Migration to Novell eDirectory" on page 20
- "NMAS Methods Installation" on page 20
- "Cache Volume Creation (only on NetWare 6.5)" on page 21
- "iManager snap-in Install for Proxy/Firewall/VPN" on page 21
- "Filter Configuration" on page 22
- "Updating Firewall/Proxy/Filter configuration to Novell eDirectory (eDirectory schema extension)" on page 22
- "License Installation" on page 23

File Copy

Possible Cause: A newer version of the file already exists on the server.

Action: Select *Never Overwrite Newer Files*.

Possible Cause: Error opening destination file. The file might be in use by another process.

Explanation: Close any other process that might be using the file and retry. If you still get the error, note the name of the file along with the complete path, and skip copying the file.

After installation, search for the file on the product CD and copy it to the destination location.

Firewall Schema Extension

Possible Cause: Firewall schema extension failed.

Action: Run `schext.nlm` at server prompt:schext *`FDN_of_user password`*. For example, `schext.cn=admin.o=novell border12`.

Explanation: User should have admin or admin equivalent rights. If `Schext` shows as already loaded, unload it and run the `Schext` again. If it cannot be unloaded, restart server and run `Schext`.

Filters Migration to Novell eDirectory

Possible Cause: `FILTSRV/BRDCFG` is already loaded

Action: Restart the server and run load `FILTSRV` migrate. (If `filtsrv` is already loaded, unload `filtsrv`. After migrating `filtsrv`, unload `filtsrv` and, load `filtsrv` again.)

Explanation: The server was not restarted after a previous installation.

NMAS Methods Installation

Possible Cause: Unavailability of one or more of the following NMAS™ methods:

- CertMutual
- DIGEST-MD5
- NDS
- Simple Password
- X509 Certificate
- X509 Advanced Certificate
- Enhanced Password
- Entrust
- Novell BorderManager LDAP
- NDS Change Password
- NMAS Proximity Card
- Secure Workstation
- Universal Smart Card

Action: Run `NMASInst.nlm` manually after the install.:`NMASInst -addmethod` *`user_DN admin_password config_file_path`*.

Here the configFilePath is the full path of the file `config.txt` present in the corresponding NMAS method folder.

These files are copied to the `sys:\SYSTEM\nds8temp\products\nmasmthd` folder. For example, if you want to install the CertMutual method, your command will look like: `NMASInst -addmethod admin.org`

```
mypassword sys:\SYSTEM\nds8temp\
products\nmasmthd\CertMutual\config.txt
```

Explanation: View the `sys:\etc\nmas\nmasinst.log` for status and details.

If you find that the files or directories in `sys:\SYSTEM\nds8temp\products\nmasmthd\NMAS_Method` are empty, copy them from the product CD from the location `Nmas_EE\NmasMethods\Novell\NMAS Method`

For more details on NMAS documentation see the NMAS Documentation (http://www.novell.com/documentation/nmas311/index.html)

Cache Volume Creation (only on NetWare 6.5)

Possible Cause: Could be any one of the following:

- Partition Creation failed.
- Volume Creation failed: No volumes could be created.
- Volume Creation failed: Number of volumes actually created are fewer than those chosen by user. Failed to write cache volume information to eDirectory

Action: Run the standalone Cache Volume Creation Utility provided in the `Unsupported` folder of the product CD, and then write the information to eDirectory.

If writing the Cache Volume Information to eDirectory fails, do the following:

1. Launch NWAdmin.
2. Double-click the *NCP Server Object*.
3. Select *BorderManager Setup* > *Caching* > *Cache Location* tab, then update cache volume and directory information.

Explanation: If volume creation failed but partition was created, delete the partition using the NSS Management Utility before running the tool. To do this, run `nssmu` on the server console, select the traditional partition created, then delete it.

iManager snap-in Install for Proxy/Firewall/VPN

Possible Cause: This is skipped if iManager 2.6 is not installed, or if the option is deselected by the user.

For the cause of the failure, see sys:`\ni\data\ nioutput.txt` under the heading Exception at VPN Plugin Install.

Action: Install the `bmacl.npm, bmpxy.npm`, `bm.npm` (for firewall), and `vpn.npm` (for VPN) modules from iManager. To do this,

1. Open iManager on the server.
2. Click the *Configure* tab.
3. Click *Module Configuration* on the left panel.
4. Install the Module Package. Specify the path\names of the `npm` files.

Explanation: The `bmacl.npm, bmpxy.npm`, `bm.npm`, and `vpn.npm` modules can be found on the product CD.

Filter Configuration

Possible Cause: Making the interface public

Action: At the server console, type `filtcfg` > Select *Configure Interface Options* > Make the interfaces public or private as you want.

Possible Cause: Setting default filters

Action: Run `brdcfg.nlm`

Possible Cause: Enabling Packet Filtering

Action: Run `INETCFG` from the server console, then select *Enable TCP/IP filtering support* > *Reinitialize System*. You can configure filters using `FILTCFG`.

Possible Cause: Adding Filter Exceptions for VPN Services failed during an upgrade. This could happen because of the following conditions:

- Absence of an interface that is only public
- Packet filtering is disabled

Action: Run `brdcfg.nlm` after the install is over and follow the on-screen instructions.

Updating Firewall/Proxy/Filter configuration to Novell eDirectory (eDirectory schema extension)

Possible Cause: Any one of the following

- Adding BRDSRVS attributes to the eDirectory/NDS schema
- Writing the public and private address list to NCP Server Attributes.
- Writing the event logging values.
- Writing the time stamp values.
- Writing the access control flag value
- Writing gateway port value
- Writing the proxy parameters value.

Action: Launch NWAdmin to do the configuration.

Double-click the *NCP Server Object* > Select *BorderManager Setup*, then configure the parameters.

If NWAdmin crashes on launch, delete the BRDSRVS:xxx attributes on the NCP server object representing the server.

Explanation: The following are some of the attributes of the NCP Server Object added by the Install:

BRDSRVS: Access Control Flag

BRDSRVS: Component Enable Flag

BRDSRVS: Event Logging

BRDSRVS: Gateway Port Number

BRDSRVS: Timestamp

BRDSRVS: private addr list

BRDSRVS: proxy parameters

BRDSRVS: public addr list,fwsAction,fwsExceptionList, FwsFilterList, fwsInterfaceList, fwsStatus.Objects added to eDirectory: NBMRuleContainer, `<NCP Server Object>` -GW.

License Installation

Action: Use iManager to install licenses.

Explanation: Novell BorderManager 3.9 services do not work if licenses are not installed. Trial Licenses are obtained at the root of the product CD under `licenses\trial` and regular (production) licenses are `licenses\regular`.

2.4 VPN Configuration Migration Messages

- "Server Object, Context Object, Server NsObject, Context NsObject, Tree Object" on page 23
- "Attribute-Component Enable Flag, or Did Not Migrate" on page 23

Server Object, Context Object, Server NsObject, Context NsObject, Tree Object

Explanation: Failed to get the Server Object

Failed to get the Context Object

Failed to get the Namespace

Failed to get the Server's NsObject

Failed to get the Context's NsObject

Failed to get the Tree Object

Possible Cause: Authentication to the server failed.

Action: Copy the `VPNMigration.ncf` file from the `vpnupgrade` folder under the `unsupported` directory and place it in the `sys` volume. Make the changes in the `NCF` file according to the instruction in the Readme provided in the same directory, then run the configuration file from the server console and restart the server.

Attribute-Component Enable Flag, or Did Not Migrate

Explanation: Failed to get the Attribute-Component Enable flag.

Possible Cause: The Novell BorderManager 3.9 VPN was not configured on this server.

Action: Check for the `sys:\_netware\vpn\svtun.cfg` file. If it is not present, it means that you have not configured Novell BorderManager 3.8 earlier, so VPN migration did not occur.

2.5 Common Install Scenarios

Proxy, Access Rules, Filters Configuration Failed to Migrate

Explanation: Proxy, Access Rules and Filters configuration migration might fail after upgrading from Novell BorderManager 3.8 SP5 to Novell BorderManager 3.9.

Action: If this happens, enter the following command:

```
fillattr <host ip> <login dn> <password> <server dn>
<search base dn>
```

For example, `fillattr 192.10.10.10 cn=admin,o=novell novell cn=nwserver-38,o=novell o=novell`

Does selective installation of the VPN also install other components?

Explanation: When the VPN is installed, the firewall is installed by default.

Action: If this is not the desired option, unload the firewall after VPN installation.

How can I make sure that the schema is correctly extended?

Action: Access iManager and verify whether the following object classes exist:

- vpnMemberEntry
- vpnRule
- inetPolicyVpnAuthCondition

What if the install aborts before completion?

Action: If the Novell BorderManager 3.9 install aborts before completion and you want to repeat the install, restart the install. After you are authenticated, choose the *Fresh Install* option.

Can only one license be installed per tree?

Explanation: Only one trial license can be installed in a tree containing multiple servers with Novell BorderManager 3.9. If you install trial licenses on a server in a tree when a trial license is already installed on another server in the same tree, you get an error stating that the license already exists.

What if products other than eDirectory are not installed properly?

Explanation: While upgrading from an older version to eDirectory 87.39, some products like SAS, PKI, and LDAP might not get updated properly in the products database, so the minimum requirements check for Novell BorderManager 3.9 fails.

Action: If you are sure that eDirectory 87.39 is installed on the server, modify the products database to write the correct version of the corresponding products. For information on this, see the Novell Support Web site (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10086525.htm).

Does the uninstall remove all the components completely?

Explanation: Uninstalling the product removes only the BorderManager files and does not revert to the original configuration.

Action: To remove all the files, remove Novell BorderManager 3.9 from the server and run `uninst.bat`, available in `sys:\ni\update\bin,` from a Windows client. To remove the configuration manually, remove the eDirectory objects added by Novell BorderManager 3.9.

How do I create a new cache volume on the NetWare 6.5 server if it shows free space as zero?

Explanation: If any partition label has non-ASCII characters in it, the Cache Volume Creation tool or CCRT utility does not work. Free space is shown as zero even if there is free space on the server. Labels can have non-ASCII characters if in some cases if a disk imager is used to restore disk images.

Action: Modify the partition label.

Viewing the Partition Label

The partition label can be viewed through NSSMU on the server as follows:

1. Load `NSSMU.NLM`.
2. Select *Partitions* > *Partition Information - Label*.

Modifying the Partition Label

To modify the partition label:

1. Type the following URL in the browser to access Novell Remote Manager:

   ```
   https://<IPAddress>:8009
   ```
2. Select *Manage server* > *Partition Disks*.

All the partitions and volumes are displayed. Partition labels are shown next to the partition labels.

3. Click the existing label and specify a new label.
4. Click *Apply*.

How do I create traditional NetWare volumes for the proxy cache?

Explanation: The Cache Volume Creation tool or CCRT is a utility to create traditional NetWare volumes. You can create the traditional NetWare volumes for the proxy cache.

The CCRT utility provides the following two options to create traditional Netware volumes:

- **Custom Method:** In this method, you can choose a free partition from the list displayed, to create the cache volume.
- **Default Method:** In this method, the utility automatically chooses the suitable partition to create the cache volume, depending on the volume size entered.

To create a traditional NetWare cache volume:

1. Type the following command in the console prompt to run the CCRT utility:

   ```
   sys:\CCRT\ccrt
   ```

   The utility displays a list of existing volumes, available free space, and the maximum volume size available in the server.
2. Press *Y* to confirm that you want to create a new volume.
3. Specify if you want to choose the custom method or the default method to create cache volumes.

   If you choose the custom method, a list of free partitions is displayed along with the freepartition ID and the free partition size. You can select a free partition from the list, to create volume.
4. Specify the volume size and the number of volumes to be created.

NOTE: ◆The actual size of the volume created is the quotient of volume size specified divided by the number of volumes.

◆The actual size of the volume should be at least 10MB and the number of volumes should be in the range (1-4).

◆Make sure that the volume size specified by you does not exceed the maximum volume size displayed (the maximum volume size displayed is the size of the largest free partition available).

How do I delete partitions and volumes?

Explanation: There is no free space available in the system.

Action: Delete volumes and partitions to recover space.

1. Access the Novell Remote Manager through the following URL:

https://<IPAddress>:8009

2 Select *Manage Server* > *Partition Disks*.

3 Delete the partitions and volumes that are not required.

3a Dismount the volumes in the partition.

3b Delete the volumes in the partition.

3c Delete the partition.

4 Restart the server before running the utility.

Why do I need domestic TCP/IP patches for NetWare 6.5?

Explanation: The shipping version of NetWare 6.5 does not work on a Novell BorderManager 3.9 VPN if it is not patched with the domestic stack TCP/IP patch. The domestic stack available at `sys:/system/tcp/tcpl` resolves this issue.

What if eDirectory services are down?

Explanation: If you get a message during install indicating `Due to a DS error, install cannot bring up the Login Dialog`, cancel the installation. Verify if the eDirectory services are up, then restart the installation.

Troubleshooting Configuration 3

This section covers some of the important configuration parameters for Novell BorderManager 3.9. It also covers some of the common configuration scenarios for VPN.

3.1 VPN Configuration Questions

This section contains information on the following:

- "What should I do if I am unable to navigate through iManager 2.6 screens?" on page 29
- "Is it wrong if I get the same screen on two frames in either the site-to-site, or the client-to-site configuration?" on page 29
- "What if navigation fails with a browser warning when I click OK on a VPN configuration screen?" on page 30
- "What if I can't save changes in VPN configuration?" on page 30
- "What if the install fails to automatically configure iManager snap-ins?" on page 30
- "I have some problems in certificate management" on page 31
- "Should site-to-site service stop on deletion of a VPN Trusted Root Object from the TRC?" on page 31
- "What if the server being configured is behind NAT?" on page 32
- "What happens if VPN is configured on a non-certificate authority server?" on page 32
- "What if PKI snap-ins are not installed on iManager?" on page 32
- "How do I reload the VPN configuration from eDirectory to the VPN server?" on page 32
- "I keep seeing error message on the IKE screen stating "Certificate subject-names do not match". What do I do?" on page 32

NOTE: This section lists some of the issues commonly observed in VPN configuration.

For information on pre-shared key use case scenarios, see the PSK Use Cases and Error Messages in the *Novell BorderManager 3.9 Administration Guide.*

What should I do if I am unable to navigate through iManager 2.6 screens?

Explanation: This could be because of a JavaScript* error on the browser.

Action: Check the browser version. The browser you are using should be either Internet Explorer 6.0 or Firefox* 1.5.

Is it wrong if I get the same screen on two frames in either the site-to-site, or the client-to-site configuration?

Explanation: This could be a JavaScript error on the browser.

Action: Click on the first tab on the screen (*General* in Client-to-Site and *Members* in Site-to-Site) and continue configuration.

What if navigation fails with a browser warning when I click OK on a VPN configuration screen?

Explanation: The warning for this condition is `This page contains both secure and non-secure items.`

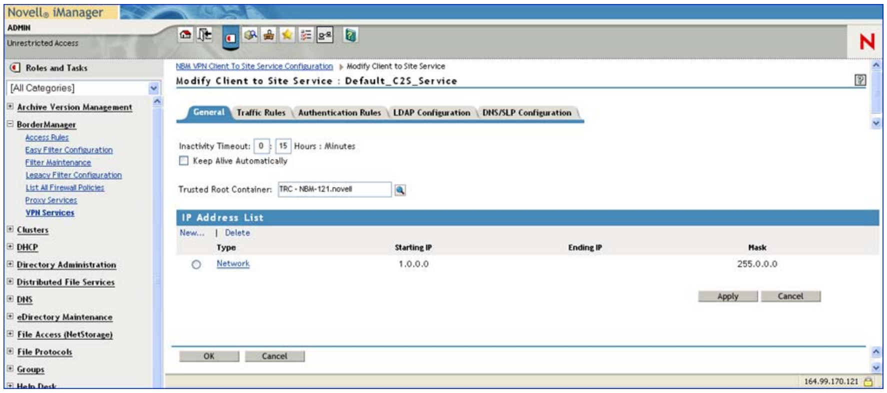
Action: Refresh the screen and repeat the operation. If the problem persists, change your browser settings.

What if I can’t save changes in VPN configuration?

Explanation: You might not be able to see the changes, or the same configuration page might appear when you repeat the operation.

Action: In the Site-to-Site or Client-to-Site > *General Parameters*, ensure that you click *Apply* before clicking *OK* at the bottom of the page. Similarly, for Traffic Rules and Authentication Rules, click *Apply* before you click *OK* at the bottom of the page.

Figure 3-1 *Saving Changes for VPN Configuration*



Modify Client to Site Service : Default_C2S_Service

Inactivity Timeout: 0 : 15 Hours : Minutes

□ Keep Alive Automatically

Trusted Root Container: TRC - NBM-121.novell

IP Address List

	Type	Starting IP	Ending IP	Mask
○	Network	1.0.0.0		255.0.0.0

What if the install fails to automatically configure iManager snap-ins?

Action: To manually configure iManager snap-ins:

1 Log in to iManager.

2 Click *Configure* on the top-most panel of the iManager page.

3 On the left panel, go to *Module Configuration* > *Install Module Package*. Select the appropriate module file (it could be `vpn.npm` for VPN or `bm.npm` for Filter configuration). If the VPN or Filter file is not available, copy them from the product CD under either the `VPN` or `Border` directory.

4 Click *Install*. This installs the module on your system.

5 If you have configured Role-Based Services in your iManager, you now need to upgrade the collection.

5a Click *RBS Configuration* > *Configure iManager* and select the *Upgrade Collections* option.

5b Select the collection that you want to upgrade, then click *Next*.

- **5c** The next page displays the list of modules that need to be updated into the collection. You should see *vpn* in this list. Select the modules that you want to update the collection with, specify a scope for this role, and click *Start* to update the collection.
- **5d** If you need users other than admin to have access rights to VPN configuration tasks, modify them by selecting *Role Configuration* > *Modify iManager Roles* and *NBM VPN Configuration* role.

6 Restart Tomcat and log in to iManager again.

You should see now *VPN Services* as one of the roles in the left panel for admin and other assigned users.

I have some problems in certificate management

Problem: The problems could be the following:

- Why is it not clear how to create the DER files required for trusted root object creation?
- Why is it not clear how to export the server certificates?
- Why is it not clear how to import certificates created by third-party certificate products?

Explanation: The Novell PKI documentation provides detailed help on various certificate management operations such as importing, exporting, creating, deleting, and updating of certificates.

See the following:

- The Novell Certificate Server Documentation. (http://www.novell.com/documentation/crt311/index.html)
- The Novell Support Web site. (http://www.novell.com/support/browse.do?WidgetName=BROWSE_PRODUCT&IsRootNode=true&TaxoName=SG_SupportGoals&BROWSE_PRODUCT.isProductTaxonomy=true&BROWSE_PRODUCT.NodeId=SG_PKIS_NOVELLCERTIFICATESERVER__1_1&BROWSE_PRODUCT.thisPageUrl=%2Fproduct%2Fproducts.do)

Should site-to-site service stop on deletion of a VPN Trusted Root Object from the TRC?

Explanation: When the trusted root object, which is used by the VPN member configuration, is deleted the VPN member configuration is not consistent anymore, so the setup stops working. Before deleting a trusted root objective, ensure that the trusted root objective is not referenced by any member entry in the VPN site-to-site configuration.

Action: If you have already deleted a trusted root objective that was referenced, and the setup is not working anymore, do the following:

1. Delete the VPN site-to-site member entry that was previously using the trusted root objective.
2. Re-create the VPN site-to-site member entry.

What if the server being configured is behind NAT?

Explanation: If the server that is being configured is behind the NAT automatic server certificate creation during VPN, configuration might fail.

Action: Create a server certificate manually through iManager and attach it to the VPN server being configured.

What happens if VPN is configured on a non-certificate authority server?

Explanation: When VPN is configured on a Novell BorderManager 3.9 server that is not a non-certificate authority, the server certificate creation takes some time. If a certificate is not created within a few minutes, the VPN Configuration snap-in reports that it is unable to create trusted root objective.

Action: If this happens, wait for a few minutes, then save the changes for VPN Server again. By this time, the server certificate should be available.

What if PKI snap-ins are not installed on iManager?

Explanation: If PKI snap-ins are not installed in the iManager that is being used for configuration, server certificate creation and trusted root objective creation must be done manually. You can also download and install the PKI snap-ins from the Novell Support Web site. (http://download.novell.com) The snap-in file is `pki.npm`.

How do I reload the VPN configuration from eDirectory to the VPN server?

Explanation: The VPN configuration changes done in iManager are written to eDirectory and are reflected in the VPN server according to the configuration time interval set in the VPN server configuration page. By default it is 5 seconds and can be changed to a maximum of 300 seconds.

Action: To force the configuration to be loaded to a VPN server, click *Synchronize* on the server details page. This resets the configuration update interval to 5 seconds. If it is already 5 seconds, the interval changes to 6 seconds.

I keep seeing error message on the IKE screen stating "Certificate subject-names do not match". What do I do?

Explanation: This usually indicates a configuration problem with the certificates.

Action: Check the following:

- Verify that the certificate subject name specified in the peer matches the actual certificate subject name as viewed in the certificate snap-ins. A similar check needs to be done for alternate subject names if configured.
- Verify that the system time on the peer is within the range of the certificate validity period.

Troubleshooting the VPN Server

4

This section explains some of the common scenarios that you can encounter while using Novell BorderManager 3.9

Additional information can be found in Chapter 5, “Troubleshooting Client-to-Site Services,” on page 37 and Chapter 6, “Troubleshooting Site-to-Site Services,” on page 41.

4.1 VPN Server Questions

This section contains information on the following:

- “Why did my VPN services stop working after the IP address was changed?” on page 33
- “Why does CSAudit not show any VPN Audit logs?” on page 33
- “Why am I unable to find Callmgr to see or establish calls?” on page 34
- “Why are VPN services not working when default filters are enabled during install?” on page 34
- “Why do TCP/IP configuration vanish after an abend?” on page 34
- “Why is VPN not working after eDirectory is removed and reinstalled on server?” on page 34
- “Why does VPMASTER not load with AUTOFAIL message on startvpn?” on page 34
- “Where do I place the LDAP trusted root certificate?” on page 34
- “I can create certificates for users in my organization, but am unable to export their certificates into a pfx File. What do I do?” on page 35
- “Why do I see some old routing entries after I removed protected networks?” on page 35
- “Why can’t a VPN connection go through if the NMAS user is in another replica server?” on page 35

Why did my VPN services stop working after the IP address was changed?

Explanation: Changing of IP addresses is not supported.

Action:You need to reinstall the VPN services and reconfigure them i the IP address is changed.

Why does CSAudit not show any VPN Audit logs?

Explanation: Check if `CSAudit` logs (indexed logs) are enabled for VPN service in the Novell Remote Management monitoring tool.

Action:Use the set log level to set the required logging level. Also, enable VPN in the CSAudit configured services list, and then restart VPN services (`stopvpn/startvpn`).

Why am I unable to find Callmgr to see or establish calls?

Explanation:Callmgr is part of NIAS, and might not be present on your NetWare system. You need to install NIAS to get this NLM. Download and install NIAS from the Novell Support Web site (https://support.novell.com).

Why are VPN services not working when default filters are enabled during install?

Explanation: The default filters are not setting up the required exceptions for the VPN to work.

Action:Either disable the creation of default filters during install time, or unload `ipflt` after VPN services come up.

Why do TCP/IP configuration vanish after an abend?

Explanation: Immediately after you have configured VPN and the services are restarted, back up the `netinfo.cfg`, `tcpip.cfg`, `ipwan.cfg`, and `gateways` files in the `sys:\etc\ directory`.

Action:After an abend, if the networking configuration is not correct, restore the files from the backups and re initialize the system to get the configuration back.

Why is VPN not working after eDirectory is removed and reinstalled on server?

Explanation:Novell Certificate Server and iManager do not work if the directory is removed and reinstalled. In fact, Novell BorderManager 3.9 itself does not work.

Why does VPMASTER not load with AUTOFAIL message on startvpn?

Explanation: The domestic version of `TCP/IP NLM` file required for the Novell BorderManager 3.9 VPN might not be installed.

Action:Copy the `tcpip.nlm`, `tcp.nlm`, and `bsdsock.nlm` and restart the server.

Where do I place the LDAP trusted root certificate?

Explanation: Be cautious if you are using the same trusted root for LDAP as well as client-to-site and site-to-site. Some of the trusted root certificates that are valid for site-to-site and client-to-site might not be valid for LDAP, and if that happens then VPN LDAP authentication fails.

Action:Use a separate trusted root for VPN LDAP configuration, which contains only the trusted root certificates of the LDAP server configured.

I can create certificates for users in my organization, but am unable to export their certificates into a pfx File. What do I do?

Explanation:Although an administrator can create certificates for any user using iManager snap-ins, only the user can export those certificates into a file. Users need to be informed that they need to import the certificate.

Why do I see some old routing entries after I removed protected networks?

Action:Reinitialize the system on the server to refresh the routing information.

Why can't a VPN connection go through if the NMAS user is in another replica server?

Explanation: The error message in this scenario could be error: -1460 `CCS_GetPartitionKey: LTSSPerformX` in Nmasmon screen.

You can download this from the Novell Support Web site. (http://www.novell.com/support/)

For more information on using the SDIDIAG tool, refer the following:

- TID # 10088626 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10088626.htm)
- TID # 10086669 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10086669.htm)
- TID # 10081773 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10081773.htm)

Action: Synchronize the tree keys with the SDIDIAG tool.

Troubleshooting Client-to-Site Services 5

This chapter contains workarounds for some of the common issues in client-to-site services.

Additional information can be found in Chapter 4, “Troubleshooting the VPN Server,” on page 33 and Chapter 6, “Troubleshooting Site-to-Site Services,” on page 41.

5.1 Client-to-Site Services Questions

Why does the VPN client hang while establishing a client-to-site connection: authentication user?

Problem: You see an *Authenticating User* message.

Explanation: This can happen the first time you access the Novell BorderManager 3.9 server after you configure it.

Action: Retry. It should work on second and subsequent tries.

Problem: You see a *Connecting for Authentication* message.

Explanation: The VPN server might be down or not responding.

Action:Cancel the client operation. Retry after waiting a few minutes. If you have access to the server, load the tcpcon utility, and see if the server is on TCP port 353.

Sometimes I am not able to establish client-to-site connection. Why?

Explanation: The client-to-site connection might not take place because one or both of the following reasons:

- Server side NMAS not loaded
- NMAS method not set for user

Action: Check the default login sequence for the user.

The first time the DH parameters are generated it takes some time. You can either wait for the operation to complete, or cancel and retry. After the initial parameters are generated, connection establishment goes through much faster.

Problem: The certificate is invalid because of one or all of the following reasons:

- Incorrect time stamp
- Wrong certificate date
- Alphanumeric names

Action: Check the validity of the certificate.

Delete and re-create the certificates involved. This may involve the user certificates as well as the server certificates for the `ikelog.txt` on the client. Check the validity of the certificate.

Avoid non-alphabetic and special characters in the certificate name.

Why does a rclient-to-site connection attempt fail in NMAS authentication?

Explanation: Error codes in the range of -1631 to -1695 are NMAS internal errors and, usually indicate some problem with the NMAS server or client methods or invalid credentials. Positive error code values, while using Universal Smart Card methods, might indicate a problem with the Smart Card driver installed on the client machine.

Action:Reinstall the driver.

Why does a NetWare login to the VPN server fail while making a client-to-site connection?

Explanation: This happens when the firewall on the VPN server is up. By default, the public interface of Firewall is blocked. However, when you try a log in to VPN server through a client-to-site connection, it tries to log in to the public interface (public IP address), which is denied.

Action:Define an exception in the firewall to allow login to the server as follows:
Source interface = VPTunnel interface
Source address = Any
Destination interface = Public interface
Destination address = Public IP address of the VPN server
Service type = NCP Stateful (source port = Any, destination port = 524)
Protocol = TCP and stateful filtering enabled

Can the client disconnect at random because of a short IKE retransmit time-out?

Action:Go to the server, set parameters, and increase the IKE retransmit time-out to a higher value such as 40 seconds.

Why do I keep getting a "No proposal chosen" message on the IKE screen when working with a third-party client?

Explanation: This could happen when a third-party peer (non-BorderManager peer) sends a proposal that is not supported by the BorderManager3.9 VPN gateway.

- For instance, BorderManager 3.9 does not support a rekey lifetime based on kilobytes. So, if a third-party peer contains a proposal for the rekey lifetime in kilobytes, you will see a `No proposal chosen` message on the BorderManager 3.9 IKE screen.

- This can also happen when the client proposes an algorithm that is not supported by the server-side policies in the Phase Two negotiations. In this case, change the client algorithms to match the server side policies.
- The same error condition can also happen if the client is trying to authenticate using a pre-shared key, but the pre-shared key is not configured on the BorderManager 3.9 server.

Troubleshooting Site-to-Site Services 6

This section contains workarounds for some of the commonly faced issues in site-to-site services.

For more information see, Chapter 4, "Troubleshooting the VPN Server," on page 33 and Chapter 5, "Troubleshooting Client-to-Site Services," on page 37.

6.1 Site-to-Site Services Questions

- "Can CSL failure be the cause for the failure of WAN call establishment to a particular destination address?" on page 41
- "Why is the site-to-site connection not established after the initial configuration?" on page 41
- "Why does the site-to-site connection not happen?" on page 42
- "Why does the site-to-site connection fail in IKE main mode?" on page 42
- "Why do logs on console show server is unreachable from VP Tunnel?" on page 42
- "Why do IKE logs show no user certificate available for signature authentication?" on page 42
- "What if one VPN slave is not able to ping another in a mesh network?" on page 42
- "Why can't I ping a server behind NAT?" on page 42
- "I am able to ping to the peer's tunnel address, but I am unable to access the Protected networks of the peer from a local protected network. Why?" on page 42

Can CSL failure be the cause for the failure of WAN call establishment to a particular destination address?

Explanation: If the address is a valid VPN slave or master, use `callmgr.nlm` to check if there is a WAN call to the specified destination. The `callmgr.nlm` is available in the product CD. If you find that there is no call established, it could be a transient error in CSL.

Action:Run `Reinitialize System` at the server console.

Why is the site-to-site connection not established after the initial configuration?

Explanation: The connection might also not happen after enabling site-to-site for the first time.

Action:Look in the logger screen to see if the server NLM programs were already up while the configuration was done; restart the VPN services (`stopvpn/startvpn`).

Why does the site-to-site connection not happen?

Action:Check whether the configuration is transferred to the slave. That is, verify if the `policy.dat` and `member.dat` files are created. Check the `csaudit` log for failure information.

Why does the site-to-site connection fail in IKE main mode?

Action:Check the value of the trusted root object field (issuer) and the subject name fields in the site-to-site general parameters. Also, ensure that pre-shared value is provided on both sides.

Why do logs on console show server is unreachable from VP Tunnel?

Action:Check the IP routing table and ensure that the VPN server is unreachable. Ensure that there are entries to reach the server through the VP Tunnel interface. Add filter exceptions in FILTCFG to deny advertisements to such destinations through the VP Tunnel interface.

Why do IKE logs show no user certificate available for signature authentication?

Explanation: This could happen if the certificate has been created with an alternate subject name.

Action:Delete the certificate and re-create it.

What if one VPN slave is not able to ping another in a mesh network?

Explanation: In a mesh network, one VPN slave is not able to ping to the tunnel address of another VPN slave. This problem happens when the public interface used while installing BorderManager 3.9 does not match with the VPN server address, and because of inconsistency in the automatic filter configuration.

Action:Set the public interface properly and run `brdcfg.nlm`.

Why can’t I ping a server behind NAT?

Explanation: This could happen if RIP is enabled and the NAT and the server behind NAT are causing a routing loop. If this is the case, disable RIP on the VPN server or NAT server.

Action: If you want to ping to the private address of the server behind NAT, add the private address as a protected network of the VPN server.

I am able to ping to the peer’s tunnel address, but I am unable to access the Protected networks of the peer from a local protected network. Why?

Action: Check if the protected networks for both the peers in the site-to-site network are correctly configured. Also, check the policies for the site-to-site network. There may be a lack of communication because of a Deny policy for the service that you are using. If the policies are correct, use `inetcfg` to verify that routes are added for the remote protected networks through the remote tunnel interface. If the routes are missing, click *Synchronize All* (for updating routes on the master), and click *Synchronize* for updating routes on a specific slave from the Novell Remote Manager Monitoring page.

NOTE: IPforwarding should also be enabled.

Troubleshooting the VPN Client

7

VPN client is an independent software bundled along with Novell BorderManager 3.9. The earlier versions of Novell BorderManager bundled VPN client for Windows* only. This version of Novell BorderManager provides VPN client for Linux* too.

This section provides information on some of the commonly faced troubles while installing or working with VPN client.

- Section 7.1, “VPN Client Issues,” on page 45

7.1 VPN Client Issues

This section covers the following issues:

- “Installing VPN client on Linux breaks the existing Nortel VPN client plug-in functionality” on page 45
- “VPN connection through vpnlogin fails” on page 45
- “Error in accessing protected networks” on page 46
- “Registry settings (If VPN client install fails)” on page 46
- “VPN client files” on page 46
- “Why does installation of the latest VPN client or, uninstallation of the previous VPN client fail?” on page 46
- “Does NMAS support the VPN client with universal smart card?” on page 47
- “What are the minimum requirements for universal smart card?” on page 47
- “What are the steps for using NMAS universal smart card on client?” on page 47
- “Why does the VPN client not work in dial-up mode?” on page 47
- “Why does the VPN client not work with other IPSec VPN clients?” on page 47
- “Why does VPN client login fail with NMAS with a -1663 Error?” on page 47

Installing VPN client on Linux breaks the existing Nortel VPN client plug-in functionality

Action: Install the novell-nortelplugins.

Download the novell-nortelpulgins from the Novell Forge Web site. (http://forge.novell.com/)

VPN connection through vpnlogin fails

Explanation: VPN connection through vpnlogin is not supported. It can be used for profile creation only.

Error in accessing protected networks

Explanation: After you have set up a VPN connection and try to access protected networks, you might see an error message: `Resource temporarily not available`.

Possible Cause: The IPSec SAs are being created.

Action:Try accessing the protected networks after a few minutes.

Explanation: After you have set up a VPN connection and try to access protected networks, you might an see error message: `Operation not permitted`.

Possible Cause:The policies do not allow you to access the protected networks.

Registry settings (If VPN client install fails)

Action: Follow these steps:

1. In the registry, remove the key under `hklm\software\microsoft\windows\currentversion\uninstall`, which has its display name as Novell BorderManager 3.9 VPN Client.
2. Remove the `hklm\software\novell\novell BorderManager VPN Client` key.

Restart the system and re-install.

VPN client files

Explanation: The files are available at:

- IKE file name: `drive:/novell/vpnc/winnt/log/ikelog.txt` for Windows 2000 and XP.

Certificate location: `drive:/novell/vpnc/certificates/users` for user personal certificate (.pfx) and `drive:/novell/certificates/trustedroots` for server certificates (`.der`).

Why does installation of the latest VPN client or, uninstallation of the previous VPN client fail?

Action: If there is a failure, remove the bindings manually. To do this,

On Windows 2000 and XP:

1. Restart the system in safe mode.
2. Go to *My Computer* > *Properties* > *Hardware* > *Device Manager*.
3. Select *View* > *Show Hidden Devices*.
4. Under *Network adapters*, search for *Novell Virtual Private Network* bindings. Remove these bindings.

Restart the system and re-install the Novell BorderManager 3.9 VPN Client.

Does NMAS support the VPN client with universal smart card?

Explanation: The VPN client supports Universal Smart Card for NMAS. The supported drivers are provided by Universal Smart Card. These drivers need to be installed where the VPN client is installed.

Action:Refer to third party documentation for Universal Smart Card driver installation.

What are the minimum requirements for universal smart card?

Explanation: Ensure that the following are installed on both the client and the server:

- NICI
- NMAS
- NMAS method for USC
- NMAS method for LDAP

What are the steps for using NMAS universal smart card on client?

Action: Follow these steps:

1. Select *VPN client* > *Configuration* > *NMAS* and *USC*.
2. Click *VPN client* > *VPN* and fill the details.
3. Enter the PIN number. This is the number of the smart card.

Why does the VPN client not work in dial-up mode?

Explanation: Install dial-up settings before you install the VPN client.

Action: If you have already installed the VPN client, uninstall the VPN client. Install dial-up and reinstall the VPN client.

Why does the VPN client not work with other IPSec VPN clients?

Explanation: You need to uninstall any other VPN client that you may have on the workstation, before the Novell BorderManager 3.9 VPN client is installed.

Why does VPN client login fail with NMAS with a -1663 Error?

Explanation: This could happen if NDS® (eDirectory) is not first in the login sequence.

Action: See TID # 10088199 at the Novell Support Web site. (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=10088199&sliceId=&dialogID=31484574&stateId=1%200%201822003)

Troubleshooting Session Failover 8

This section contains the following information:

- Section 8.1, "Checking if the AuthAgent is Up and Running," on page 49
- Section 8.2, "The AuthAgent Hangs," on page 49
- Section 8.3, "List of Common Errors," on page 50

8.1 Checking if the AuthAgent is Up and Running

To check if the AughAgent is up and running:

1 Enter the following at the command prompt:

```
java -show
```

2 Check for the following entry:

```
com.novell.bordermanager.proxy.auth.AuthDB
```

This specifies that the AuthAgent is up and running.

8.2 The AuthAgent Hangs

If the AuthAgent hangs, kill it as follows:

Linux

1 Enter the following command to get the process ID of AuthAgent:

```
pgrep authdb
```

2 At the command prompt, enter the following command:

```
kill process ID
```

Alternatively, you can kill the AuthAgent by pressing Ctrl+C.

NetWare

1 Enter the following at the command prompt:

```
java -show
```

The class name and ID for all Java applications running on your system are displayed in the following format:

```
com.novell.bordermanager.proxy.auth.AuthDB......629
```

2 Run the following command to kill the AuthAgent:

```
java -kill classID
```

classID is the class ID of the application. For example,

```
java -kill629
```

Windows

1. Go to the Windows Task Manager.
2. Select the task corresponding to the AuthAgent. The task is an entry with:

   ```
   Command prompt - java-classpath ...
   ```

Alternatively, you can also kill the AuthAgent by pressing Ctrl+C.

8.3 List of Common Errors

Some of the common errors that can occur while configuring the ProxyAgent are:

- Specifying the IP address of the local server instead of typing the word `localhost`.
- Entering non-uniform serial numbers. For example, the same ProxyAgent was configured with one number on one machine and another number on another machine.

Giving Feedback on Issues

9

In order to help us improve the services and functionality of Novell BorderManager, please report issues so that they can be fixed in the future releases of the product.

Report issues according to:

- Section 9.1, "Reporting Installation or Configuration Issues," on page 51
- Section 9.2, "Reporting VPN Client-to-Site or Site-to-Site Connection Establishment Issues," on page 51
- Section 9.3, "Reporting a VPN Server Abend," on page 51

9.1 Reporting Installation or Configuration Issues

While reporting installation or configuration issues, obtain the following information:

- The files `sys:/ni/data/nioutput.txt` and `sys:/ni/data/response.ni` files. .
- The install logs mentioned in Chapter 1, "Logs, Screens, Tools, and Parameters," on page 9.
- For license addition errors, send the `sys:system\nlstrace.old` file.
- Any error message or error code displayed by the installation process.
- If any Java exceptions are seen, send the contents of logger screen.

9.2 Reporting VPN Client-to-Site or Site-to-Site Connection Establishment Issues

While reporting connection VPN Client-to-Site or Site-to-Site connection establishment issues, obtain the following:

- The output of the VPN Console for options 7, 8, 9, 10 for client-to-site and site-to-site. For site-to-site, also provide the output of option 5.
- The output of logger screen after configuration changes or after VPN service restart.
- The output of the `IKE.LOG`.
- `CSAudit` logs

9.3 Reporting a VPN Server Abend

While reporting VPN server abends, obtain the following information:

- The `abend.log` file
- A core image if possible
- A description of the scenario when it happened
- `IKE.LOG` and `logger.txt` files
- `CSAUDIT` logs