Novell BorderManager®

3.8

www.novell.com

TROUBLESHOOTING GUIDE

November 07, 2003

Novell®

Legal Notices

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

www.novell.com

Novell BorderManager 3.8 Troubleshooting Guide
November 07, 2003

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

Novell Trademarks

Third-Party Materials

Contents

About This Guide

This documentation provides troubleshooting information for Novell® BorderManager® 3.8 components.

The document provides hints, debugging steps, known issues, and steps to be avoided in order to help the customers effectively install and configure Novell BorderManager 3.8. For the purpose of ease we shall refer to Novell BorderManager 3.8 as NBM in this document.

IMPORTANT: After installing the product review the install summary at sys:/ni/data/nbm_instlog.csv to verify if all steps in installation have been completed successfully. If not, refer to Chapter 2, “Installation,” on page 15 to troubleshoot.

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 Logs, Screens and Tools

This section provides the important logs and screens for Novell® BorderManager®. The section covers:

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® 6.5 fails.
Install	sys:/ni/data/ni.log	Contains milestone information on the stages of install.	After install or if install fails.
Install (vpn schema extension)	sys:/ni/data/vpn*.txt	Schema extension errors	If the VPN schema is not extended properly.
Install	sys:/ni/data/nierrors.log	Information about fatal errors during installation.	If install fails with a fatal error.
Install (NMAS)	sys:/etc/nmas/nmasinst.log	Information about NMAS installation	If NMAS schema extension or methods creation fails.
Install (VPN configuration migration)	sys:/ini/data/vpnupgrade.log	The log for VPN configuration migration	If VPN configuration migration fails

Component	Log File Location	Description	When to Look
IKE VPN Server	/etc/ike/ike.log	Schema extension errors	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 depend on the IKE log level. This can be set through a configuration parameter.)
CS Audit	Load csaudit and view the logs, or view them through NWAdmn	Contains the IKE log messages	To get information on setting up connections, restarting services after a configuration change, and for errors during establishing the connection.

Screens

Screen Name	Description	When and What to Look
Logger screen	Default screen for NetWare 6. Contains NBM and non-NBM 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.
VPN console screen	VPN-specific logs, dumps of internal data structures. This shows the configuration information and the state of the server.	When you want to see the internal IPSec data structures to help trace the progress of a connection. It has the provision to dump information about established SAS, configuration, policies and so on. This information will be logged in either in the console screen for NetWare 5.1 or in the logger for NetWare 6.
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.

VPN Debug Console Screen

This screen is available on each VPN server.

Options

Number	Display Action
1	VPMaster/VPSlave miscellaneous information
2	IPSEC SA List

Number	Display Action
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

Tools

Tool Name	Description	Usage
CSAUDIT	CSAUDIT is a NetWare Console tool to display the audit trail records that were logged using the CSLIB facility in NetWare. BorderManager uses the CSLIB facility for its audit logs, and these records can be displayed using this utility. This tool can be used to detect any errors establishing connection to remote VPN server, as well as synchronisation errors after establishing the connection logged to the CSAUDIT database. This database may be viewed by loading CSAUDIT at the server console.	--
CALLMGR	The NetWare utility used to monitor the status of the wide area network (WAN) connections or to start and stop WAN calls manually. This tool can be used to see the inbound/outbound connection from/to remote VPN server. If this is not the case, 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.	This is available at the root of the CD in the directory CALLMGR
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 synchonised. At such a 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. A useful troubleshooting TID for IP routing is TID #10011169	--

Tool Name	Description	Usage
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 setup incorrectly, the packets going to the remote destination may end up going out on the LAN card, and not the VPN interface.	--
VPMON	VPMON is the monitoring frontend for BorderManager 3.8 VPN services. This runs as a NetWare Loadable Module and interfaces with the NRM framework to provide the monitoring functionality for the VPN services from the browser using the NetWare Remote Console.	This is available at the root of the product CD in the directory VPN
Schema Extension Tool	If you have installed Novell BorderManager 3.8 and VPN Schema Extension has failed, you can use this tool to extend the schema without having to go through the entire installation process again.	Go to the unsupported\vpn schema extension removal utility\extension folder on the CD and follow the instructions provided in the readme.
Schema Removal Tool	To remove NBM 3.8 VPN Schema	Go to the unsupported\vpn schema extension removal utility\removal folder on the CD and follow the instructions provided in the readme.
VPN Upgrade Tool	If you are upgrading to Novell BorderManager 3.8 from NBM 3.6.2A or 3.7.2, and VPN Configuration Migration has failed due to some reason during during Install (check the reason in this guide). Or if you have not selected VPN Configuration Migration during the NBM3.8 Installation, you can also migrate your existing VPN Configuration using this utility.	Go to the Unsupported\vpnupgrade folder on the CD and follow the instructions provided in the readme.
Cache Volume Creation Tool	This a utility to create traditional volumes on NetWare 6.5. Proxy cache directories require traditional NetWare volumes.	Go to the Unsupported\CCRT folder on the CD and follow the instructions provided in the readme.
VPN console options	This tool is useful for narrowing down issues with the IKE/IPSEC SA negotiation, and determining that the VPN site-to-site and client-to-site profiles are setup correctly.	--

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.

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 and 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.

Viewing the Dump Information

The dump tool can be used on NetWare® as well as on Windows.

On NetWare

The files for the dump tool on Netware are vpndump.ncf and vpnDump.jar. These two files are available as a zip file named vpndump_NW.zip in the unsupported directory under VPN on the product CD.

The vpndump_NW.zip file must be unzipped on the sys: volume of the NetWare server. The following files will be copied in the specified folders:

1. vpnDump.jar in sys:\tomcat\4\webapps\nps\web-inf\lib
2. vpndump.ncf in sys:\system

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

The files for the dump tool on Windows are vpndump.bat, vpnDump.jar and 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.

The vpndump_win.zip file must be unzipped under any folder in a Windows machine.

After extracting the three files into a folder:

1. 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. SET UDR= < tomcat_home absolute path >

2. Save the vpndump.bat file. Run the vpndump.bat file by providing two arguments, user and context.

   vpndump <user> <context>

   For example, vpndump admin novell

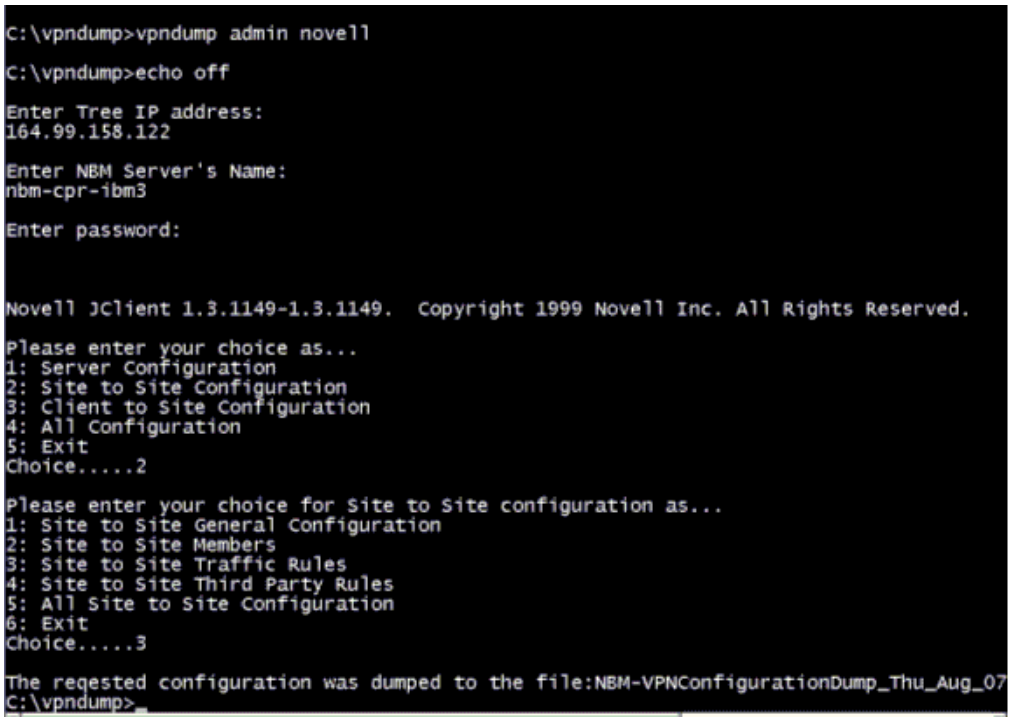
3. You will be prompted for the Tree IP, Novell BorderManager server name, and the password. After successful authentication to the server, you can choose the type of dump.

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

Example on Windows

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

Figure 1 VPN Configuration Dump Tool on Windows



2 Installation

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

IMPORTANT: After installing the product, review the install summary at sys:/ni/data/nbm_instlog.csv to verify if all steps in installation have been completed successfully. If not, refer to the following sections to troubleshoot:

Minimum Requirements Check

The following section lists out the error messages for minimum requirements.

Improper version of NetWare

Action: Install NetWare 5.1 SP6, NetWare 6.0 SP3 or NetWare 6.5

Explanation: The install will discontinue if any of these requirements is not met. Install the minimum required version of the product or software before proceeding with NBM installation.

No version or improper version of NICI

Action: Install NICI from the Companion CD (The minimum required version is 2.6.0). The recommended version is 87.1.0.

Explanation: The install will discontinue if any of these requirements is not met. Install the minimum required version of the product or software before proceeding with NBM installation.

No version or improper version of eDirectory

Action: Install eDirectory from the Companion CD (The minimum required version is 86.0.2). The recommended version is 87.1.0

Explanation: The install will discontinue if any of these requirements is not met. Install the minimum required version of the product or software before proceeding with NBM installation.

No version or improper version of LDAP

Action: Install eDirectory from the Companion CD (The minimum required version is 86.0.2). The recommended version is 87.1.0

Explanation: The install will discontinue if any of these requirements is not met. Install the minimum required version of the product or software before proceeding with NBM installation.

Improper version of NBM

Action: Upgrade allowed only from 3.6SP2A and 3.7SP2

Explanation: The install will discontinue if any of these requirements is not met. Install the minimum required version of the product or software before proceeding with NBM installation.

No version or improper version of PKI

Action: Install eDirectory from Companion CD (The minimum required version is 86.0.2). The recommended version is 87.1.0

Explanation: The install will discontinue if any of these requirements is not met. Install the minimum required version of the product or software before proceeding with NBM installation.

No version or improper version of SAS

Action: Install eDirectory from Companion CD (The minimum required version is 86.0.2). The recommended version is 87.1.0

Explanation: The install will discontinue if any of these requirements is not met. Install the minimum required version of the product or software before proceeding with NBM installation.

No version or improper version of NETNLM32.NLM

Action: Copy netnlm32.nlm from the NETNLM32 folder on the companion CD to sys:system of the server. (The minimum required version is 5.5.8 June 4, 2003.)

The latest version of the nlm can be found at:

Novell Support (http://support.novell.com/cgi-bin/search/searchtid.cgi?/2966367.htm)

Explanation: Required during NMAS start, else server will abend

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

Action: Run the PERL* script from the Companion CD as mentioned in the NBM Quick Start Card.

Explanation: These are optional requirements and the install will continue without them. However, the product might not function correctly after installation if the proper file version is not available.

No version or improper version of iManager

Action: The reccomended version for NetWare 6.5 is iManager 2.0 and for NetWare 6 is iManager 2.0.1.

Explanation: These are optional requirements and the install will continue without them. However, it would be difficult to administer the product if the proper iManager version is not available.

License Selection

This section lists some of the common problems with licenses:

- "User selected Skip Licenses during installation" on page 17
- "Error validating licenses or invalid license Location" on page 17

User selected Skip Licenses during installation

Action: Install the licenses later using NWAdmn or iManager.

Explanation: NBM services will not function if licenses are not installed

Error validating licenses or invalid license Location

Action: Check the license location path. Paths other than the local file system, such as NBM source path or floppy drives are not valid. Also, make sure that the path contains the licenses for the selected NBM services.

Explanation: NBM services will not function if licenses are not installed

Install Messages

- "File Copy" on page 18
- "Firewall Schema Extension" on page 18
- "Filters Migration to Novell eDirectory" on page 18
- "NMAS Objects Creation in Novell eDirectory" on page 18
- "NMAS Methods Installation" on page 18
- "BMAS Login Policy Object (LPO)" on page 19
- "RADIUS Components Migration" on page 19
- "Cache Volume Creation (only on NetWare 6.5)" on page 20
- "VPN Schema Extension" on page 20
- "iManager snap-in Install for Firewall/VPN" on page 20
- "Filter Configuration" on page 20

- "Updating Firewall/Proxy/Filter configuration to Novell eDirectory (eDirectory schema extension)" on page 21
- "VPN Configuration Migration (in case of upgrade from NBM 3.7 or BMEE 3.6)" on page 22
- "License Installation" on page 22

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 may be in use by another process.

Explanation: Close any other process that may 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 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 Schext. If it cannot be unloaded, restart server and run Schext.

Filters Migration to Novell eDirectory

Possible Cause: FILTSRV/BRDCFG already loaded

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

Explanation: Server was not restarted after a previous installation

NMAS Objects Creation in Novell eDirectory

Possible Cause: See sys:\etc\nmas\nmasinst.log for more information and error messages

Action: Run NMASInst.nlm manually after the install.:NMASInst -m ***<user DN> <admin password>*** . For example: NMASInst -m admin.org mypassword

Explanation: NMASInst.nlm writes trace information to sys:\etc\nmas\nmasinst.log. If NMASInst is not working, this log file can help determine which object or attribute NMASInst is unable to create and why.

NMAS Methods Installation

Possible Cause: Failure to install one or more of the following NMAS methods:

- CertMutual
- DIGEST-MD5
- NDS
- Simple Password
- X509 Certificate

- X509 Advanced Certificate
- Enhanced Password
- Entrust
- NBM LDAP
- NDS Change Password
- NMAS Proximity Card
- Secure Workstation
- Universal Smart Card

Action: Option 1 : Run MethodInstaller.exe from the NBM CD\Nmas_EE\NmasMethods.

Option 2: 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 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: As above, you may view sys:\etc\nmas\nmasinst.log for status/details of what happened.

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 the NMAS documentation see NMAS Documentation (http://www.novell.com/documentation/lg/nmas22/index.html)

BMAS Login Policy Object (LPO)

Possible Cause: Login policies were detected in the existing BMAS. Ignore the step if BMAS LPO objects were not detected (this information is not available in the install Summary).

Action: Migrate the BMAS login policies for VPN and proxy services to the NMAS login sequences. You need to do this manually by looking at the old login rules using NWAdmn and creating equivalent rules using ConsoleOne®.

Explanation: For details on configuring LPO rules, refer the section on Setting up Login Policies in Chapter 3 of Novell RADIUS Services Administration Guide

RADIUS Components Migration

Possible Cause: Failure in migrating the Dial Access System (DAS) Object of BMAS to NMAS.

Action: Use radmig.nlm as described in Novell RADIUS Services Administration Guide, Chapter 2, Section Upgrading From BorderManager Authentication Service 3.5 or BorderManager Authentication Service 3.6 to Novell RADIUS Services.

Once the BMAS - NMAS DAS object migration is over, the BMAS server will no longer be useful.

Explanation: If RADMIG fails, you should call Technical Support and let them determine the reason for failure. You can also create a new DAS and manually configure it through ConsoleOne. However, if

RADMIG does not work in the your environment, RADIUS is also likely to have problems. Possible reasons why RADMIG might fail:

1) The user's tree has eDirectory problems that must be addressed (run DSRepair)

2) The tree key is invalid, or does not exist on the server. If you have tree key problems, RADMIG will return a -1460 or -1418 error.

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 less 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 (see next para.).

If writing the Cache Volume Information to eDirectory failed, launch NWAdmn to do the configuration. Double-click the NCP Server Object > 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 NSS Management Utility before running the tool. To do this, run nssmu on the server console > Partitions > select the traditional partition created and delete.

VPN Schema Extension

Possible Cause: See sys:\ni\data\vpnlog.txt and vpnerr<0-7>.txt for cause of failure

Action: Use the VPN Schema Extension Removal Tool in the unsupported directory at the root of the CD. Also see section “VPN Schema Extension” on page 22.

iManager snap-in Install for Firewall/VPN

Possible Cause: This will be skipped for NetWare 5.1 or if iManager 2.0 or 2.0.1 is not installed or if the option is deselected by user.

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

PortalServlet.properties under sys:\ tomcat\4\webapps\nps\WEB-INF might contain incorrect data.

Action: Install the modules bm.npm (for Firewall) and vpn.npm (for VPN) from iManager.

Open iManager on the server. Click the configure tab. Click Module Confuguration on the left panel > Install Module Package. Specify the path\names of the npm files.

Explanation: The bm.npm and vpn.npm modules can be found in the NBM CD under the directories border and VPN.

Filter Configuration

Possible Cause: Making Interface public

Action: On server console, type filtcfg > Select Configure Interface Options > Make the interface(s) public/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 > Enable TCP/IP filtering support > Reinitialize System. You can configure filters using FILTCFG.

Possible Cause: Adding Filter Exceptions for VPN Services in case of upgrade failed. This could happen because Install could not read the following information from eDirectory or due the following conditions:

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

Action: Run brdcfg.nlm after Install is over and follow the instructions that appear.

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

Possible Cause: Could be any one of the following

- Adding BRDSRVS attributes to eDirectory/NDS Schema
- Adding IPX/IP Gateway Class and attributes to NDS Schema
- Writing 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 NWAdmn to do the configuration.

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

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

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

VPN Configuration Migration (in case of upgrade from NBM 3.7 or BMEE 3.6)

Possible Cause: Error in getting Object Entry, Context, tree, Namespace, NsObject, Component Enable Flag;NBM3.6/3.7 VPN not configured; Error in adding vpnAuxClass,IP address, Tunnel IP address and mask; error in creating Trusted Root Container, Certificate or Trusted Root Object.

Action: See sys:\ni\data\vpnUpgrade.log for details of events/errors and troubleshoot using the VPN Configuration Migration Troubleshooting guide (below).

Explanation: In VPN configuration migration fails, use the VPN Configuration Migration Script and its Readme provided in the VPN upgrade folder under the unsupported directory of the CD.

License Installation

Action: Install Licenses using NWAdmn or iManager. To install from NWAdmn, select the NCP Server Object, select Tools > Novell Licensing Services > Add Licenses > License File > Select license file to install.

Explanation: Novell BorderManager services will not work if Licenses are not installed. Trial Licenses are obtained at the root of the CD under licenses\trial and Regular (Production) Licenses under licenses\regular.

VPN Schema Extension

Most of these errors can occur if you are running Schema Extension from the standalone utility and have provided wrong/inconsistent inputs.

For a comprehensive list of LDAP return values see LDAP Return Values (http://developer.novell.com/ndk/doc/ldapover/index.html?page=/ndk/doc/ldapover/ldap_enu/data/a3zxc1a.html).

ldapssl_client_init failed: -1 der file:

Possible Cause: Invalid or non-existent Trusted Root Certificate

Action: - Check if Trusted Root Certificate with given name exists

- Check if the certificate is valid and if not, create it using the steps mentioned

sys:\system\Svc.ldf cannot be opened

Possible Cause: LDIF files used for schema extension not present in proper location

Action: Copy files from vpn\system\schema on the CD to sys:\system and try again.

ldap_simple_bind failed: 49 (Invalid credentials)

Possible Cause: Invalid password

Action: Run the schema extension tool with valid password

ldap_simple_bind failed: 32 (No such object)

Possible Cause: Invalid Admin name

Action: Run the schema extension tool with valid Admin name in LDAP format

Schema Validation failed

Possible Cause: Faulty ICE (NetWare 6 SP 3 ICE has issues with using SSL). DS on the machine is corrupt or timesync is not proper.

Explanation: Use the ICE PATCH provided in the Companion CD.

Try running dsrepair on the machine (unattended full repair), and retry the schema extension using the tool provided.

ldap_modify failed: 65 (Object class violation)

Possible Cause: Usually not a problem, but if an object class is already present with a different definition, this may cause problems.

Action: In case this is not a new install try removing schema (using files in the unsupported directory) and then extending it again.

ldap_modify failed: 20 (Type or value exists)

Possible Cause: Schema already extended

ldap_modify failed: 81 (Can't contact LDAP server)

Possible Cause: LDAP server is down or unreachable. This may happen when nldap is not loaded or ldap is not properly configured.

This may also happen if SSL option is selected and schema is already extended.

Action: Check if LDAP is installed and nldap is loaded and try again.

If the above check is OK, then most probably this is not a problem; check if schema is already extended. If not try again with cleartext password.

To check if LDAP is actually loaded: Type tcpcon at server console > Select Protocol Information > TCP > TCP Connections. Check if LDAP is listening in port 389 (for Clear Text) or 669 (using SSL). If not, go to ConsoleOne > LDAP Server and check the values therein. Press Refresh NLDAP server now and try again.

ldap_simple_bind failed: 13 (Confidentiality required)

Possible Cause: You chose the Clear Text Password option but did not enable it in ConsoleOne.

Action: Enable Cleartext Passwords in ConsoleOne and try again.

ldap_simple_bind failed: 34 (Invalid DN syntax)

Possible Cause: Admin name was not given in LDAP format

Action: Try again using correct admin name in LDAP format (eg: cn=admin,o=novell)

VPN Configuration Migration Messages

This section lists some of the VPN configuration migration error messages.

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: Possible reason would be authentication to server failed.

Action: Take 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 as in the readme provided in the same directory and run it from the server console and restart the server.

vpnServerAuxClass

Explanation: Could not add the vpnServerAuxClass.

Possible Cause: The VPN schema might not be extended.

Action: Extend the VPN schema. Take 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 readme provided in the same directory and run it from the server console, and restart the server.

Attribute-Component Enable Flag or Did Not Migrate

Explanation: Failed to get Attribute-Component Enable Flag

Did not migrate VPN configuration as BMEE 3.6/NBM 3.7 VPN was not configured on this server

Possible Cause: BMEE 3.6/NBM 3.7 VPN was not configured on this server.

Action: If the BMEE 3.6/NBM 3.7 VPN was not configured in the server

VPN migration is not applicable.

IP Address or Mask

Explanation: Failed to get IP Address and Mask from configuration file.

Possible Cause: The configuration file does not exist..

Action: Check for the file sys:_netware\vpn\ snetaddr.cfg

If it is not there means you have not configured the NBM3.6/3.7 vpn before. VPN migration is not applicable.

Tunnel IP Address or Mask

Explanation: Failed to get Tunnel IP Address and Mask from configuration file

Possible Cause: The configuration file does not exist.

Action: Check for the file sys:_netware\vpn\ svptun.cfg.If it is not there means you have not configured the NBM3.6/3.7 VPN before. VPN migration is not applicable

Trusted Root Container or Server Certificate

Explanation: Failed to create Trusted Root Container/ Failed to create Server Certificate

Possible Cause: eDirectory login failed or npkiapi.nlm is not loaded. Login inputs from the install may not be same format as the van migration expects

Action: Take the VPNMigration.ncf file from the upgrade folder under the unsupported directory and place it in the sys volume. Make the changes in the NCF file as in the readme provided in the same directory and run it from the server console and restart the server.

PKI NLMs

Explanation: Error in loading the PKI NLM's. Please unload npkiapi.nlm and any dependent NLMs and then run the standalone Migration utility provided at the Unsupported folder of the CD after this Installation is complete.

Possible Cause: Might not have restarted the server after the NICI installation.

Action: Restart the server after installation is completed. Take the VPNMigration.ncf file from the upgrade folder under the unsupported directory and place it in the sys volume. Make the changes in the NCF file as in the readme provided in the same directory and run it from the server console and restart the server

Trusted Root Object

Explanation: Failed to create Trusted Root Object.

Possible Cause: Server Certificate creation in the case of a non-CA server takes time.In this case some times Server Certificate is actually may not available for Trusted Root object creation.

Install fails to create the trusted root object.

Action: Take the VPNMigration.ncf file from the upgrade folder under the unsupported directory and place it in the sys volume. Make the changes in the NCF file as in the readme provided in the same directory and run it from the server console and restart the server.

Could not execute (err=6)

Explanation: CreateProcess: load:Could not execute (err=6)

Possible Cause: The message appears once NPKIAPI nlm is already loaded and you try to load it again. The message appears on ConsoleOne when you run the VPNMigration tool.

Action: No need to do anything.

Common Install Scenarios

Does selective installation of the VPN also install other components?

Explanation: When VPN is installed the Firewall is installed by default.

Action: If this is not a desirable option, unload the Firewall after VPN installation.

How can I make sure that schema has been correctly extended?

Explanation: For a detailed check, you need to take a schema dump using ICE and compare the schema with the schema files provided in the vpn\system\schema directory.

See support.novell.com (http://support.novell.com) and search for schcmp* for a schema comparison tool or the TID 2931699.

Action: Open ConsoleOne Schema Manager, and verify that the following object classes exist:

- vpnMemberEntry
- vpnRule
- inetPolicyVpnAuthCondition

What if the install aborts before completion?

Action: If the NBM install aborts before completion and you want to repeat the install again, start install as usual. Just after you are authenticated, a dialog box will appear asking you whether you want to proceed as a Fresh Install or an Upgrade. 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 NBM. If you install Trial Licenses on a server in a tree when a Trial License is already installed on another server of the same tree you will get an error License Already Exists.

What if products other than eDirectory are not being installed properly?

Explanation: While upgrading from an older version to eDirectory 8.7, some products like SAS, PKI and LDAP may not get updated properly in the products database, because of which the Minimum Requirements Check for NBM will fail.

Action: If you are sure that eDirectory 8.6.2 or higher is installed on the server, you can modify the products database to write the correct version of the corresponding products using the Novell Support (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10086525.htm) given in the TID

What if vptunnel.lan is being deleted after upgrading the NetWare server to NetWare 6.5?

Action: If this happens copy vptunnel.lan from vpn\system from the root of the CD to the sys:\system and c:\nwserver\drivers directory on NetWare 6.5 and restart the server. The upgrade sequence is: NetWare 6/NetWare 5.1 > Novell BorderManager 3.7 > Novell BorderManager 3.7SP2 > Novell BorderManager 3. 8 > NetWare 6.5.

What if I get a fatal error during installation?

Explanation: In some cases you may get a fatal error at the beginning or during the installation and the install might abort. This may happen because all the required install files may not get properly extracted to the system, or because NIS files do not get properly upgraded to CSP9 or above.

Action: Try the following workaround.

- Copy uninst.bat provided in the unsupported folder on the CD to sys:\ni\update\bin folder of the server and double click the .bat file from a client Windows machine. Re-install NBM.
- (If the above does not work) You may get a fatal error saying file sp.db does not exist and you are on a NetWare 5.1 SP 6 machine, replace the ni\lib folder of the server by the NIS\lib folder provided in the Companion CD. Remember to backup the existing ni\lib folder before replacing it. Re-install NBM.

Does uninstall work completely?

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

Action: To remove all the files, remove NBM 3.8 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 NBM.

How to 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, this utility will not work. Free space will be shown as 0 even if there is free space on the server. Labels can have non-ascii characters if in some cases a disk imager is used to restore disk images. The partition label can be seen through NSSMU on the server. (Load NSSMU.NLM > Partitions > Partition Information - Label). Partition label can be viewed/modified using Novell Remote Manager.

Action: Open https://IpAddress:8009 from a browser. iManager server > Partition Disks. On the right panel all the partition and volumes will be shown. Partition labels are shown against the partition names. Click on an existing label to change it.

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

Explanation: Shipping version of NetWare 6.5 will not work properly if they are not patched with the latest TCP/IP patch. The domestic stack that is available in the Companion CD resolves this issue. If you want the null stack with bsdsock.nlm version 6.51o or later for NetWare 6.5 which solves the issue.

What if eDirectory services are down?

Explanation: If you get a message during install “Due to a DS error, install cannot bring up the Login Dialog” cancel the installation, check that the eDirectory services are up and restart installation.

3 Configuration

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

Set Configuration Parameters

set ike debugmask

Explanation: 2 = Only Message Headers (default)

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

8 = Attributes (this will be 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 will dump existing IKA 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 will dump IPSEC SAs to the console.

This is similar to VPN the debug console option 2, but will print on screen 1, where we 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.

VPN Configuration Scenarios

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

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

Action: Check the browser version. The browser you are using should be IE 5.5 or higher.

Is it wrong to 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 you 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 am not able to save changes in VPN configuration?

Explanation: You may not be able to see the changes. Or the same configuration page may appear when you repeat the operation.

Action: Ensure you click the Apply button for General Parameters of site-to-site or client-to-site and click OK in traffic rules/authentication rules before you click OK at the bottom of the site-to-site or client-to-site configuration page.

What if install automatically fails to configure iManager plug-ins?

Action: To manually configure the plug-in:

1. Click Configure on the top-most panel on the iManager screen.
2. 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 copied already, you can find a copy of the relevent file in the NBM CD under the VPN or Border directory. Click Install. This should install the module onto your system.

3. If you have configured Role Based Services in your iManager, now you need to upgrade the collection. To do this,
   - Click on RBS Configuration > Configure iManager and select the option Upgrade Collections. It would prompt you the collection that requires updation. Select the collection that you want to be updated and then click on Next. The next screen would display 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, also mention a scope for this role and click on Start. The collection will now be up to date.
   - If you would need users other than admin to have access rights to VPN configuration tasks, you can modify the same by selecting Role Configuration > Modify iManager Roles and NBM VPN Configuration role. Same for Filters, the tasks NBM Access Management.
4. Restart tomcat and log-in to iManager again.
5. You should see NBM VPN Configuration as one of the roles in the left panel for admin and other assigned users.

I have the following certificate management problems:

Problem: These could be the problems:

- 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 like importing, exporting, creation, deletion and updating of certificates.

- http://www.novell.com/documentation/lg/crt203ad/ - Novell Certificate Server Documentation
- http://developer.novell.com/research/appnotes/2000/january/05/index.htm - Novell Certificate Server Management AppNotes.

What if I am unable to create certificates using ConsoleOne?

Explanation: You will not be able to create certificates using ConsoleOne running on the NetWare server. You need ConsoleOne running on Windows to perform certificate management operations. User-space NICI 2.0.2 or later should be installed on the machine on which ConsoleOne is run.

Also, before you manage the certificates you need to see that the Novell Certificate Server and the ConsoleOne PKI snap-ins are installed.

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 gets deleted, the VPN member configuration is not consistent anymore, and hence the setup will stop working. Before deleting a TRO, please ensure that the TRO is not referenced by any member entry in the VPN site to site configuration.

Action: If you have already deleted a TRO which was referenced, and the setup is not working anymore, do the following:

1. Delete the corresponding VPN Site-to-Site member entry which was using the TRO previously.

2. Recreate 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: In that case create a server certificate manually through ConsoleOne 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 NBM 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 TRO.

Action: If this happens, wait for a few minutes, then save the changes for VPN Server again. By then 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 TRO creation would have to be done manually. If desired, the PKI snap-ins can be installed manually from the companion CD. The snap-in file is pki.npm.

How do I to reload the VPN configuration from eDirectory to 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 screen. 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 screen. This will reset the configuration update interval to 5 seconds. If it is already 5 seconds, the interval will change to 6 seconds.

I keep seeing error message on the IKE screen saying "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.

What could be the problem if IKE main mode went through, but quick mode is failing consistantly?

Action: Verify that the "PFS enabled" flag is set to the same value on both the peers (enabled on both or disabled on both). Verify that the algorithms proposed by the client matches with the policies configured on the server.

4 VPN Server

The new VPN server is one of the major changes in Novell® BorderManager® 3.8. Some of the common scenarios that could cause problems to the users are listed here. Additional information can be found in Chapter 5, "Client-to-Site Services," on page 37 and Chapter 6, "Site-to-Site Services," on page 41.

VPN Server Scenarios

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

Explanation: Change of IP address is not supported.

Action: You will need to reinstall the VPN services and reconfigure after 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 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 may not be present on your NetWare system, but you can get it from the NBM Companion CD. Or you may have to get and install NIAS to get this NLM. Check https://support.novell.com for the same.

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 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: Just after VPN configuration is done, and the services are restarted, backup the following files in the sys:\etc\ directory: netinfo.cfg, tcpip.cfg, ipwan.cfg, gateways.

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

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

Explanation: Novell Certificate Server™ (PKI) and iManager will not work if the directory is removed and reinstalled. In fact, NBM itself won't work.

Why does VPMASTER does not load with AUTOFAIL message on startvpn?

Explanation: TCPIP NLM required for NBM 3.8 VPN may 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 roots certificates which are valid for site-to-site and client-to-site may not be valid for LDAP, and if that happens then VPN LDAP Authentication will fail.

Action: It is recommended to 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 the ConsoleOne® or the iManager snap-ins, only the user can export those certificates into a file. You need to tell users to import their certificates. An administrator can export a user certificate using the PKI Certificate Console.

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

Action: Run reinitialize system on the server to refresh the routing information.

Why VPN connection cannot go through, if NMAS user is in another replica server ?

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

Your tree keys must be synchronized with this tool. This tool ships with NW 6.5 sp1 and can also be downloaded at http://support.novell.com/cgi-bin/search/searchtid.cgi?/2966746.htm

Here are some TIDs that explain how to use the tool:

http://support.novell.com/cgi-bin/search/searchtid.cgi?/10088626.htm

http://support.novell.com/cgi-bin/search/searchtid.cgi?/10086669.htm

http://support.novell.com/cgi-bin/search/searchtid.cgi?/10081773.htm

Action: Use the above mentioned tool.

5 Client-to-Site Services

Client-to-site services on Novell® BorderManager® have changed completely from earlier versions of the software. For more information see Chapter 4, “VPN Server,” on page 33 and the next chapter Chapter 6, “Site-to-Site Services,” on page 41. Some of the common issues in client-to-site services are:

Client to Site Services

Why does the VPN client hang while establishing a client-to-site connection: Authentication User?

Problem: This message in this scenario could be Authenticating User.

Explanation: This can happen for the first time after configuring the NBM server.

Action: Retry and it should work.

Problem: The message in this scenario could be Connecting for Authentication

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

Action: Cancel the client operation. Retry after some time. If you have access to the server, load the tcpcon utility, and see if the server is listening on TCP port 353.

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

Explanation: The client-to-site connection may not take place because one of the two scenarios:

Possible Cause: NMAS™

Problem: Could be either of the two:

1. Server side NMAS not loaded

2. NMAS method not set for user8

Action: The solution could be to check the default login sequence for the user.

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

Problem: Certificate

1. Incorrect timestamp
2. Wrong certificate date
3. Alphanumeric names

Action: Check the validity of the certificate, get the certificate option and get the certificate from the client.

Delete and re-create the certificates involved. This may involve the user 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.

Possible Cause: The Error message thrown when NMAS is not set for the User is “Failed to get DH Parameters. Contact your Administrator".

One of the reasons can be that no rule might be established for the user.

Why does client-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, may indicate a problem with the Smart Card driver installed on the client machine.

Action: Reinstall the driver.

Why does NetWare login to 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 but when you try a login to VPN server through a client-to-site connection it tries to login to public interface (public ipaddress) which is denied.

Action: Define an exception in the Firewall to allow login to the server. The details of the exception are source interface = VPTunnel interface, source address = Any, destination interface = Public Interface, destination address = Public IP Address of the VPN server and service type = NCP Stateful (source port = Any, destination port = 524, protocol = TCP and stateful filtering enabled).

Can the client disconnect at random due to short IKE retransmit timeout?

Explanation: Yes, this could happen.

Action: Go to server set parameters and increase the IKE retransmit timeout to a higher value around 40 secs.

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 which is not supported by the BorderManager VPN gateway.

- For instance, BorderManager does not support 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 IKE screen.
- This can also happen when the client proposal an algorithm which is not supported by the server side policies in the phase 2 negotiations. In this case, the client algorithms should be changed to match the server side policies.
- The same error condition can also happen if the client is trying to authentication using PSS, whereas PSS is not configured on the BorderManager server. In this case, an additional error message, "PSS not configured", will appear on the IKE screen.

After establishing Client to Site VPN Connection, I am not able to ping from the client machine to the NBM Server or any other machine in the protected network behind the NBM Server. What could be the reason?

Explanation: The remote LAN Machine could receive the packet, but is unable to respond due to incorrect default gateway or no gateway being configured.

Action: Make sure that the Remote LAN Machine has a default gateway associated with it.

Explanation: VPN Client Address and Remote LAN Address should not be in the same subnet.

For e.g., if we use a VPN gateway with a subnet 199.10.0.0/100.100.100.0, a value like 198.11.0.1 or 200.200.200.2 should be used in VPN Client address. If you choose an IP address in the subnet (which is not used) for the VPN client and send any TCP or UDP Packets to the target remote computer, the target machine will send inside its subnet an ARP request in order to get VPN Client MAC address.The request cannot receive any answer because the client is not physically residing inside the subnet. So, ping and all other network commands will obviously fail.

6 Site-to-Site Services

Site-to-site services on Novell® BorderManager® have changed completely from earlier versions of the software. For more information see Chapter 4, “VPN Server,” on page 33 and chapter next to that Chapter 5, “Client-to-Site Services,” on page 37. Some of the common issues in site-to-site services are:

Site-to-Site Services

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 to check that there is a WAN call to the specified destination. You can get callmgr.nlm from the NBM 3.8 Companion CD. If you find that there is no call established, this could be a transient error in CSL.

Action: Run Reinitialize System at the server console.

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

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

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

Why does site-to-site connection not happen?

Action: Check that the configuration is transferred to the slave (the policy.dat and member.dat files are created). Check the csaudit log for failure information.

Why does 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.

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

Action: Check the IP routing table and ensure 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 recreate it.

What if one VPN slave is not able to ping another is 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 does not match with the VPN server address, and is caused because inconsistency in the automatic filter configuration.

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

I am not able to ping a server behind NAT?

Explanation: This could happen if RIP is enabled and the NAT and the server behind NAT is causing a routing loop. In such an event disable RIP on the VPN server or NAT server.

Action: In case you want to ping to a 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 not able to access the protected networks of the peer, from a local protected network?

Action: Check if the protected networks for both the peers in the site-to-site network is 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, verify that routes are added for the remote protected networks through the remote tunnel interface, using inetcfg. If the routes are missing, please use the Synchronize All (for updating routes on master), and Synchronize selected (for updating routes on a specific slave) from the NRM based Monitoring page.

7 VPN Client

VPN client is an independent software bundled along with Novell BorderManager 3.8. This section covers some of the common troubleshooting issues with VPN client.

VPN Client Issues

The following section lists some of the common troubleshooting scenarios for the VPN client.

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.x VPN Client.
2. Remove the hklm\software\novell\novell BorderManager VPN Client key.
3. Restart the system and re-install

VPN Client Files

Explanation: The files are available at:

1. IKE file name: drive:/novell/vpnc/winnt/log/ikelog.txt for Windows NT, 2000 and XP. For Windows 98 and ME the location is drive:/novell/vpnc/win95/log/ikelog.txt.
2. Certificate location: drive:/novell/vpnc/certificates/users for user personal certificate (.pfx) and drive:/novell/certificates/trustedroots for server certificates (.der).

NOTE: The drive is only C.

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

Action: You need to manually remove the bindings if there is a failure:

1. On Windows 2000 and XP
   - Restart the system in safe mode
   - Go to My Computer > Properties > Hardware > Device Manager
   - Select View > Show Hidden Devices
   - Look for Novell Virtual Private Network bindings under Network adapters > Remove these bindings
   - Restart the system and re-install 3.8 VPN Client
2. On Windows 98, NT and ME
   - Restart and re-install

Does NMAS support VPN Client with Universal Smart Card?

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

Action: Refer to third party documentation for USC driver installation.

What are the minimum requirements for Universal Smart Card?

Explanation: Ensure 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. VPN client > Configuration tab > NMAS and USC buttons
2. VPN client > VPN tab > fill the details
3. Enter PIN number in the dialog box (this is the number of the smart card)

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

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

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

Why does 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 NBM 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 on the top of the login sequence.

Action: See TID#TID10088199 at the support website (http://support.novell.com/).

8 Reporting Issues

In order to help us improve the software please report back issues so that they can be fixed in time for the release of the product. Please report issues according to:

Reporting Issues

Install or Configuration Issues

While reporting install issues follow this procedure:

1. Send the files sys:/ni/data/nioutput.txt and sys:/ni/data/response.ni in addition to the Install Logs mentioned in Chapter 1, "Logs, Screens and Tools," on page 9.
2. For license addition errors send the file sys:system\nlstrace.old.
3. Also send any error message or error code displayed by Install.
4. Get the schema information on the server using ICE as follows: ice –S LDAP –s <hostname> -p <port> -d <admin's LDAP DN> -w <password> -b cn=schema –c base –F "objectclass=*" -D LDIF –f schema.ldf.

   Send the schema.ldf file.
5. Get the configuration information on the server using ICE as follows: ice –S LDAP –s <hostname> -p <port> -d <admin's LDAP DN> -w <password> -b "" –c sub –F "objectclass=*" –D LDIF –f objects.ldf

   Send us the objects.ldf file.
6. Contents of logger screen if any Java exceptions are seen.

VPN client-to-site or site-to-site Connection Establishment Issues

While reporting connection establishment issues provide the following information:

1. Output of VPN Console for options 7, 8, 9, 10 for client-to-site and site-to-site. For site-to-site please provide output of option 5 also.
2. Output of logger screen after configuration changes or after VPN service restart.
3. Output of IKE.LOG
4. CSAudit logs

VPN Server ABEND

While reporting abends provide the following information

1. Abend.log
2. Core image if possible.
3. Scenario when it happened
4. IKE.LOG and logger.txt files.
5. CSAudit logs.