Version 8.0

Part No. NN46110-501 02.01
318451-C Rev 01
13 October 2008
Document status: Standard

600 Technology Park Drive
Billerica, MA  01821-4130

# Nortel VPN Router Configuration — SSL VPN Services

NORTEL

## Nortel Networks Inc. software license agreement

This Software License Agreement (“License Agreement”) is between you, the end-user (“Customer”) and Nortel Networks Corporation and its subsidiaries and affiliates (“Nortel Networks”). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

“Software” is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

**1. Licensed Use of Software.** Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment (“CFE”), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer’s Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

**2. Warranty.** Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided “AS IS” without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

**3. Limitation of Remedies.** IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER’S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

**4. General**

a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States

Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

# Contents

# Preface

This guide introduces the Nortel VPN Router Secure Sockets Layer (SSL) Virtual Private Network (VPN) service. It also provides overview and basic configuration information to help you initially set up SSL VPN services.

## Before you begin

This guide is for network managers who are responsible for the set up and configuration of the Nortel VPN Router. This guide is based on the assumption that you have experience with windowing systems or graphical user interfaces (GUIs) and are familiar with network management.

## Text conventions

This guide uses the following text conventions:

| | |
|---|---|
| angle brackets (< >) | Indicates that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command.<br>Example: If the command syntax is **`ping`** <*`ip_address`*>, you enter **`ping 192.32.10.12`** |
| **`bold Courier text`** | Indicates command names and options and text that you need to enter.<br>Example: Use the **`show health`** command.<br>Example: Enter **`terminal paging`** {**`off`** \| **`on`**}. |

| | |
|---|---|
| braces ({}) | Indicates required elements in syntax descriptions where more than one option exists. You must choose only one option. Do not type the braces when you enter the command.<br>Example: If the command syntax is **`ldap-server source {external \| internal}`**, you must enter either **`ldap-server source external`** or **`ldap-server source internal`**, but not both. |
| brackets ([ ]) | Indicates optional elements in syntax descriptions. Do not type the brackets when you enter the command.<br>Example: If the command syntax is **`show ntp [associations]`**, you can enter either **`show ntp`** or **`show ntp associations`**.<br>Example: If the command syntax is **`default rsvp`** [**`token-bucket`** {**`depth \| rate`**}], you can enter **`default rsvp`**, **`default rsvp token-bucket depth`**, or **`default rsvp token-bucket rate`**. |
| ellipsis points (. . .) | Indicates that you repeat the last element of the command as needed.<br>Example: If the command syntax is **`more disk`***`n`*`:<`*`directory`*`>/...<`*`file_name`*`>`, you enter **`more`** and the fully qualified name of the file. |
| *italic text* | Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, an underscore connects the words.<br>Example: If the command syntax is **`ping`** <*`ip_address`*>, *`ip_address`* is one variable and you substitute one value for it. |
| `plain Courier text` | Indicates system output, for example, prompts and system messages.<br>Example: `File not found.` |

| | |
|---|---|
| separator ( > ) | Shows menu paths.<br>Example: Choose Status > Health Check. |
| vertical line ( \| ) | Separates choices for command keywords and arguments. Enter only one choice. Do not type the vertical line when you enter the command.<br>Example: If the command syntax is **`terminal paging {off \| on}`**, you enter either **`terminal paging off`** or **`terminal paging on`**, but not both. |

# Related publications

For more information about the Nortel VPN Router, see the following publications:

- Release notes provide the most recent information, including brief descriptions of the new features, problems fixed in this release, and known problems and workarounds.
- *Nortel VPN Router Configuration—Client* (NN46110-306) provides information to install and configure client software for the SSL VPN Module 1000.
- *Nortel VPN Router Configuration—TunnelGuard* (NN46110-307) provides information to configure and use the TunnelGuard feature.
- *Nortel VPN Router Upgrades—Server Software Release 8.0* (NN46110-407) provides information to upgrade the server software to the most recent release.
- *Nortel VPN Router Installation and Upgrade—Client Software Release 8.01* (NN46110-409) provides information to upgrade the Nortel VPN Client to the most recent release.
- *Nortel VPN Router Configuration—Basic Features* (NN46110-500) introduces the product and provides information about initial setup and configuration.
- *Nortel VPN Router Configuration—Advanced Features* (NN46110-502) provides configuration information for advanced features such as the Point-to-Point Protocol (PPP), Frame Relay, and interoperability with other vendors.
- *Nortel VPN Router Configuration—Tunneling Protocols* (NN46110-503) provides configuration information for the tunneling protocols IPsec, Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), and Layer 2 Forwarding (L2F).
- *Nortel VPN Router Configuration—Routing* (NN46110-504) provides instructions to configure the Border Gateway Protocol (BGP), Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Virtual Router Redundancy Protocol (VRRP), Equal Cost Multipath (ECMP), routing policy services, and client address redistribution (CAR).
- *Nortel VPN Router Using the Command Line Interface* (NN46110-507) provides syntax, descriptions, and examples for the commands that you can use from the command line interface (CLI).

- *Nortel VPN Router Configuration—Firewalls, Filters, NAT, and QoS* (NN46110-508) provides instructions to configure the Stateful Firewall and SSL VPN Module 1000 interface and tunnel filters.
- *Nortel VPN Router Security—Servers, Authentication, and Certificates* (NN46110-600) provides instructions to configure authentication services and digital certificates.
- *Nortel VPN Router Troubleshooting—Server* (NN46110-602) provides information about system administrator tasks such as recovery and instructions to monitor VPN Router status and performance. This document provides troubleshooting information and event log messages.
- *Nortel VPN Router Administration* (NN46110-603) provides information about system administrator tasks such as backups, file management, serial connections, initial passwords, and general network management functions.
- *Nortel VPN Router Troubleshooting—Client* (NN46110-700) provides information to troubleshoot installation and connectivity problems with the Nortel VPN Client.

## Printed technical manuals

To print selected technical manuals and release notes free, directly from the Internet, navigate to www.nortel.com/products. Find the product for which you need documentation, then locate the specific category and model or version for your hardware or software product. Use Adobe Acrobat Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems website at www.adobe.com to download a free copy of the Adobe Acrobat Reader.

# How to get Help

This section explains how to get help for Nortel  products and services.

## Finding the latest updates on the Nortel Web site

The content of this documentation was current at the time the product was released. To check for updates to the latest documentation and software for **SSL VPN Module 1000**, click one of the following links:

| Link | Website |
|---|---|
| **Most recent software** | Nortel page for **SSL VPN Module 1000** software located at<br>support.nortel.com/go/main.jsp?cscat=SOFTWARE&poid=13922. |
| **Most recent documentation** | Nortel page for **SSL VPN Module 1000** documentation located at<br>support.nortel.com/go/main.jsp?cscat=documentation&tranProduct=13922 |

## Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

**www.nortel.com/support**

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

## Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the phone number for your region:

**www.nortel.com/callus**

## Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

**www.nortel.com/erc**

## Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

# New in this release

There are no new features in *Nortel VPN Router Configuration —SSL VPN Services* for Release 8.0.

# Chapter 1
# SSL VPN Overview

SSL VPN enables remote access to intranet resources, such as applications, mail, files, intranet Web pages, through a secure connection. Secure Sockets Layer (SSL) is the underlying protocol used for these sessions.

With SSL VPN activated, mobile workers, telecommuters, and partners can access information and applications on the intranet. Access rules from the access control list (ACL) determines what information is accessible to a user group and thus to the user who belongs to that group.

SSL VPN services are available to the remote user on Nortel VPN Router gateway IP addresses—physical and Circuitless IP(CLIP). The Nortel VPN Router distinguishes between services that it provides and the services the SSL VPN provides and immediately forwards the appropriate traffic to the SSL VPN module.

Traffic between users and SSL VPN virtual servers has either a destination IP address equal to the Nortel VPN Router physical IP or a CLIP address. You must use CLIP addresses when you use SSL VPN if you want access from a user tunnel or branch office tunnel. A unique destination IP and port combination identifies virtual server traffic.

SSL VPN is an SSL acceleration features, which makes it possible to combine SSL acceleration and VPN.

# Hardware platforms

The SSL VPN Module 1000 card is supported on Nortel VPN Router 1740, 1750, 2700, 2750 and 5000 platforms since Version 5.00 software. The software enforces the requirement of installation in slot 1. If you install the SSL card in a different slot, the software holds the card in reset mode and logs a persistent warning asking you to reinstall it in slot 1.

# Features

The following features are supported on the software:

- management
  - — configuration through the SSL VPN GUI, which is launched from the Services > SSL VPN window
  - — ability to control remote access through Telnet and Secure Shell to specific Nortel VPN Router device
- performance

  Depending on the model, supports up to 600 SSL transactions per second for each Nortel VPN Router device. It scales up to 1000 users simultaneously logged in.
- scalability and redundancy

  supports 256 virtual SSL servers and up to 1500 certificates
- certificate and key management
  - — supports import of private keys generated in Apache, OpenSSL, Stronghold, WebLogic, and Microsoft IIS 4.0
  - — supports client authentication, generation of client certificates, revocation of client certificates, and automatic retrieval of Certificate Revocation Lists (CRL)
  - — supports Entrust
  - — supports validation of private keys and certificates
  - — supports generation of certificate signing requests (CSR)
  - — Supports creation of self-signed test certificates

— supports automatic retrieval of CRLs through Hypertext Transfer Protocol (HTTP), Trivial File Transfer Protocol (TFTP), or Lightweight Directory Access Protocol (LDAP) Version 3

— supports Public Key Cryptography Standards (PKCS7) certificates, where the user is prompted to select a certificate when the certificate file contains multiple certificates

— supports adding an X-Client-Cert multiline HTTP header to a client request

Use of this feature makes the Nortel VPN Router insert the entire client certificate as a multiline HTTP header in Privacy Enhanced Mail (PEM) format. The back end Web servers can then perform additional user authentication, based on the information in the client certificate. The back end servers can also make use of any auxiliary fields in the client certificate.

- advanced processing

— supports rewriting of client requests

Customized error messages transmit to the client Web browser if the browser is unable to perform the required cipher strength. Without this feature, the client request would be rejected during the SSL handshake.

— ability to transmit extra SSL information to the back end servers, such as the negotiated cipher suite and client certificate information, in case the virtual SSL server requires client certificates

To ensure the information transmits correctly, you can configure the virtual SSL server to add an extra SSL header to the client request.

- logging capabilities

— support for traffic logging through UDP syslog messages.

An SSSL server can send all User Datagram Protocol (UDP) syslog messages for all HTTP requests to a configured syslog server. You can use this feature as an alternative to traffic logging on the back end Web servers in environments where you must perform traffic logging on the SSL terminating device itself, due to laws or regulations.

— support for Remote Authentication Dial In User Service (RADIUS) accounting and auditing

- supported standards

- supports SSL version 2.0 and 3.0, plus Transport Layer Security (TLS) version 1.0
- supports Secured Simple Mail Transfer Protocol (SMTPs), Secure Post Office Protocol (POP3s), and Secure Internet Message Access Protocol (IMAPs) in addition to the standard Secure HTTP (HTTPS)
- supports Simple Network Management Protocol (SNMP) version 1 and SNMP version 2c

# Chapter 2
# Configuring the SSL VPN Module

This chapter provides information about SSL VPN Module initialization and initial configuration.

To configure the SSL VPN module, perform the following procedures:

1. Initialize the SSL VPN module.
2. Enable DNS proxy and RADIUS service.
3. Enable Nortel VPN Router Stateful Firewall.
4. Generate certificates.
5. Create a VPN portal with the VPN Quick Wizard.
6. Update DNS servers.
7. If required, configure the NetDirect Agent.

## SSL VPN configuration considerations

Note the following considerations:

- The Nortel VPN Router provides most services for SSL access and acts as a Remote Authentication Dial In User Service (RADIUS) server and Domain Name Service (DNS) proxy service for the SSL device. PassGo Defender is not supported at this time.
- Groups on the SSL card can mirror those on the Nortel VPN Router by using the SSL VPN GUI. Groups that mirror the Nortel VPN Router groups are given SSL VPN access.
- You cannot use the Transmission Control Protocol (TCP) port on any Nortel VPN Router interface for both a Nortel VPN Router service and an SSL service.

For example, if you use SSL to manage the Nortel VPN Router on the public interface on TCP port 443, you cannot set up an SSL portal on this same interface on TCP Port 443. The SSL device always takes priority; therefore you can no longer manage the Nortel VPN Router using SSL from the public interface. Nortel recommends that you change the Nortel VPN Router SSL port to a nonstandard port from the Nortel VPN Router Services > SSLTLS window.

- If you require access over a tunnel, you must use a Circuitless IP (CLIP) address.
- When configured, the physical private interface of the Nortel VPN Router has the following four IP addresses assigned to it:
  - Nortel VPN Router management IP address
  - Nortel VPN Router interface IP address
  - SSL management IP address
  - SSL interface IP address
- If the SSL VPN applet time zone and the Nortel VPN Router time zone do not match and you see errors, configure the time zone to the correct one by using the following command:

  ```
  tzone "Etc/GMT-5".
  ```

# Initializing the SSL VPN module

Before you configure the SSL VPN Module, you must initialize it to ensure that the Nortel VPN Router can communicate with it.

**Note:** The SSL VPN card takes time rebooting before it reaches operational status.

To initialize the SSL VPN Module, perform the following steps:

1. Log in to the Nortel VPN Router.
2. Choose **Services, SSL VPN**.
3. In the **Configuration Status** section, click **Initialize**.

A message appears to advise you that it can take several minutes to initialize the SSL VPN hardware.

4 Click **OK** to confirm that you want to continue.

The SSL VPN Initialization window appears.

5 Enter an IP address in the **SSL VPN management address** box.

The IP address must be within the management subnet as defined on the Nortel VPN Router.

6 Enter an IP address in the **SSL VPN interface address** box.

This IP address is the source IP address for all proxy requests that the SSL VPN makes to private-side back end servers. The IP address must be within the management subnet as defined on the Nortel VPN Router.

7 Enter a password in the **SSL VPN admin password** box to configure the password for the Admin account on the SSL VPN module.

The Nortel VPN Router needs this password to support the card initialization and subsequent configuration and management that occurs over a private control channel.

8 Reenter the password in the **Confirm** box.

9 Click **OK.**

It takes approximately one minute to complete the initialization.

The Services > SSL VPN window refreshes. Because there are no SSL VPN servers configured, the Virtual Server Ports section is empty.

# Configuring Web interface parameters

To use the Nortel VPN Router for RADIUS authentication service or DNS proxy, you must enable them. When you enable DNS proxy, define a primary DNS server and configure the Nortel VPN Router Stateful Firewall or interface filters to support the SSL VPN.

To define a DNS server, perform the following steps:

1. Choose **System, Identity.**
2. Ensure that:
   a. the Nortel VPN Router has a functional Primary DNS server configured.
   b. the Nortel VPN Router has DNS Proxy enabled in the DNS Server Configuration section of the window.
3. Choose **Services, RADIUS**.
4. Select the **Enable RADIUS Service** check box.
5. In the **Clients** section, click the **Enable** check box to enable the default client.
6. In the **Secret** box, enter a shared secret.
7. In the **Confirm** box, reenter the shared secret.
8. Click **OK**.
9. Configure the Authentication order to match how you are authenticating Nortel VPN Router users.
10. Choose **Services, Firewall/NAT**.
11. Enable either the **VPN Router Stateful Firewall** or the **VPN Router Interface Filters** to support SSL VPN access.

    If you are unfamiliar with interface filters, go to the System > LAN window and configure the private interface for Permit All. If you use the Stateful Firewall, ensure that Allow SSL-VPN traffic through Stateful FW is checked on the Services > SSL VPN window. If Stateful FW is checked, implied rules are automatically added, giving the SSL VPN the access it needs. When you enable either type of firewall for the first time, you must reboot. If you reboot, continue with the next step after restart.
12. Choose **Services, SSL VPN**.

**13** Ensure that the **Current Status** is Operational.

# SSL VPN and Nortel VPN Router Stateful Firewall

The SSL VPN fully integrates with the Nortel VPN Router Stateful Firewall, and you can permit or deny access through Firewall settings.

Nortel VPN Router Stateful Firewall has two ways to configure SSL VPN access:

- with implied firewall rules
- without implied firewall rules

## Configuring SSL VPN access with implied firewall rules

To configure SSL VPN access with implied firewall rules, perform the following steps:

1. Choose **Services, SSL VPN**.
2. Select the **Allow SSL-VPN traffic through Stateful FW** check box.
3. Click **OK**.

When you select the Allow SSL-VPN traffic through Stateful FW check box, all traffic from the public side of the Nortel VPN Router can access the SSL device. This setting inserts an implied rule into the firewall.

## Configuring SSL VPN without implied firewall rules

To configure SSL VPN access without implied firewall rules, perform the following steps:

1. Choose **Services**, **SSL VPN**.
2. Clear the **Allow SSL-VPN traffic through Stateful FW** check box.

If you clear the Allow SSL-VPN traffic through Stateful FW check box, the setting clears implied rules except those required to manage the SSL device and for the SSL device to send to the public.

### Access control with the firewall

You can control access to the SSL VPN within the firewall. For example, if you use the system default policy (Deny All), the first configuration allows SSL through because the implied rules override all other rules.

To allow SSL traffic through, you need to create a new policy with a rule that makes SSL VPN accessible. You can configure the policy to drop connections on a public interface from My Disallowed Network and allow all other traffic.

Alternatively, you can configure the policy to allow connections on a public interface from “My Allowed Network” and drop all other traffic Interface filters do not provide this functionality.

## Launching the SSL VPN BBI

To launch the SSL VPN BBI, perform the following steps:

1. To enable management, select the **SSL VPN HTTP Management Enabled** check box.
2. Click **OK**.

   The Welcome to the Nortel VPN Gateway window appears.
3. Enter the username and password.
4. Click **Login**.

The Nortel VPN Gateway GUI appears with the Expert tab displayed. From this tab, you can manage the SSL-VPN module.

For more information about the SSL VPN BBI, see *Nortel VPN Gateway—BBI Application Guide for VPN* (NN46120-102).

# Upgrading the software

The SSL VPN software image is the executable code running on the SSL VPN Module. A version of the image ships with the card. As new versions of the image are released, you can have two types of upgrades:

## Minor release upgrade

This is typically a bug fix release. Usually, you can perform this type of upgrade without the need to reboot the SSL VPN Module 1000. Therefore, the SSL VPN module maintains normal operation and traffic flow, and retains all configuration data.

## Major release upgrade

This type of release con contain bug fixes and feature enhancements. If the new features enhance the operating system, the SSL VPN Module 1000 automatically reboots after a major upgrade. The SSL VPN retains all configuration data.

## Activating SSL VPN upgrade packages

When you download a new version of the software to the Nortel VPN Router, the software package is automatically decompresses and is marked as unpacked. After you activate the unpacked software version, which can cause the Nortel VPN Router to reboot, the software version is marked as permanent. The software version previously marked as permanent is then marked as old.

The four possible status values are described as follows:

- unpacked—the software upgrade package is downloaded and automatically decompressed.
- permanent—the software is operational and survives reboots of the system.
- old—the software version is no longer permanent and is not currently operational. If a software version marked old is available, it is possible to switch back to this version if you activate it again.
- current—a software version marked as old or unpacked is activated. As soon as the system performs the necessary health checks, the current status changes to permanent.

# Generating and adding certificates

To use encryption capabilities you must add a key and certificate that conforms to the X.509 standard to the Nortel VPN Router.

The Nortel VPN Router supports up to 1500 certificates. The Nortel VPN Router supports importing certificates and keys in these formats:

- Privacy Enhanced Mail (PEM)
- NET
- DER
- Public Key Cryptography Standards (PKCS7) (certificate only)
- PKCS8 (keys only, used in WebLogic)
- PKCS12 (also known as PFX)

Besides these formats, the Nortel VPN Router can import keys in the proprietary format used in MS IIS 4 and keys from Netscape Enterprise Server or iPlanet Server. To import keys from Netscape Enterprise Server or iPlanet Server however, you must first use a conversion tool. For more information about the conversion tool, contact Nortel Technical Support.

When you export certificates and keys from the Nortel VPN Router, you can specify to save in the PEM, NET, DER, or PKCS12 format using the Export command. If you choose to use the Display command, which requires a copy-and-paste operation, you are restricted to saving certificates and keys in the PEM format only.

**Note:** When performing a copy-and-paste operation to add a certificate or key, you must always use the PEM format.

To generate and add a new certificate, perform the following steps:

1. Generate a Certificate Signing Request (CSR)
2. Send it to a Certificate Authority (CA), such as Entrust or VeriSign, for certification.

**3** Add the signed certificate to the Nortel VPN Router.

**Note:** Even though the Nortel VPN Router supports Apache-SSL, OpenSSL, or Stronghold SSL keys and certificates, the preferred method from a security point of view is to create keys and generate certificate signing requests from within the Nortel VPN Router. The encrypted private key never leaves the Nortel VPN Router and is invisible to the user.

For more information about certificates, see *Nortel VPN Router Security—Servers, Authentication, and Certificates* (NN46110-600).

### Updating existing certificates

To substitute an existing certificate with a new certificate, keep the existing certificate until you verify that the new certificate works as designed.

## Updating DNS servers

Update the local DNS server with the VPN name, and configure the server to perform reverse DNS lookups.

For more information about VPNs, see *Nortel VPN Gateway—BBI Application Guide for VPN* (NN46120-102).

For more information about DNS server configuration, see *Nortel VPN Router Security—Servers, Authentication, and Certificates* (NN46110-600).

## NetDirect Agent

The NetDirect agent is an SSL VPN client you can download from the Portal for each user session. Once downloaded, the remote user can access intranet resources through native applications without the need to manually install VPN client software. When the user exits the NetDirect agent or the Portal, the agent uninstalls.

Compared to the full version of the SSL VPN client installed permanently on a remote machine, the NetDirect agent does not have a user interface. The NetDirect agent is packet-based, while the installed client uses system calls.

To configure NetDirect refer to *Nortel VPN Gateway—BBI Application Guide for VPN* (NN46120-102).

## Configuring VPNs

Virtual servers configured as type HTTP or Sockets (SOCKS) needs a VPN associated with it. VPNs provide the authorization, authentication, and accounting infrastructure that is used to determine whether users are valid, what they are allowed to access, and to track their activities.

For more information about VPNs, see *Nortel VPN Gateway—BBI Application Guide for VPN* (NN46120-102).

# Appendix A
# Supported ciphers

The Nortel VPN Router supports SSL version 2.0, SSL version 3.0, and Transport Layer Security (TLS) version 1.0. All ciphers covered in these versions of SSL are supported, except the IDEA and FORTEZZA ciphers and ciphers using Diffie-Helman (DH) or digital signature standard (DSS) authentication.

**Table 1** Supported Ciphers

| Cipher Name | SSL Protocol | Key Exchange Algorithm, Authentication | Encryption Algorithm | MAC Digest Algorithm |
|---|---|---|---|---|
| DHE-RSA-AES256-SHA | SSLv3 | DH, RSA | AES (256) | SHA1 |
| AES256-SHA | SSLv3 | RSA, RSA | AES (256) | SHA1 |
| EDH-RSA-DES-CBC3-SHA | SSLv3 | DH, RSA | 3DES (168) | SHA1 |
| DES-CBC3-SHA | SSLv3 | RSA, RSA | 3DES (168) | SHA1 |
| DES-CBC3-MD5 | SSLv2 | RSA, RSA | 3DES (168) | MD5 |
| DHE-RSA-AES128-SHA | SSLv3 | DH, RSA | AES (128) | SHA1 |
| AES128-SHA | SSLv3 | RSA, RSA | AES (128) | SHA1 |
| RC4-SHA | SSLv3 | RSA, RSA | RC4 (128) | SHA1 |
| RC4-MD5 | SSLv3 | RSA, RSA | RC4 (128) | MD5 |
| RC2-CBC-MD5 | SSLv2 | RSA, RSA | RC2 (128) | MD5 |
| RC4-MD5 | SSLv2 | RSA, RSA | RC4 (128) | MD5 |
| RC4-64-MD5 | SSLv2 | RSA, RSA | RC4 (64) | MD5 |
| EXP1024-RC4-SHA | SSLv3 | RSA(1024), RSA | RC4 (56) | SHA1 EXPORT |

**Table 1** Supported Ciphers

| Cipher Name | SSL Protocol | Key Exchange Algorithm, Authentication | Encryption Algorithm | MAC Digest Algorithm |
|---|---|---|---|---|
| EXP1024-DES-CBC-SHA | SSLv3 | RSA (1024), RSA | DES (56) | SHA1 EXPORT |
| EXP1024-RC2-CBC-MD5 | SSLv3 | RSA (1024), RSA | RC2 (56) | MD5 EXPORT |
| EXP1024-RC4-MD5 | SSLv3 | RSA (1024), RSA | RC4 (56) | MD5 EXPORT |
| EDH-RSA-DES-CBC-SHA | SSLv3 | DH, RSA | DES (56) | SHA1 |
| DES-CBC-SHA | SSLv3 | RSA, RSA | DES (56) | SHA1 |
| DES-CBC-MD5 | SSLv2 | RSA, RSA | DES (56) | MD5 |
| EXP-EDH-RSA-DES-CBC-SHA | SSLv3 | DH (512), RSA | DES (40) | SHA1 EXPORT |
| EXP-DES-CBC-SHA | SSLv3 | RSA (512), RSA | DES (40) | SHA1 EXPORT |
| EXP-RC2-CBC-MD5 | SSLv3 | RSA (512), RSA | RC2 (40) | MD5 EXPORT |
| EXP-RC4-MD5 | SSLv3 | RSA (512), RSA | RC4 (40) | MD5 EXPORT |
| EXP-RC2-CBC-MD5 | SSLv2 | RSA (512), RSA | RC2 (40) | MD5 EXPORT |
| EXP-RC4-MD5 | SSLv2 | RSA (512), RSA | RC4 (40) | MD5 EXPORT |
| ADH-AES256-SHA | SSLv3 | DH, NONE | AES (256) | SHA1 |
| ADH-DES-CBC3-SHA | SSLv3 | DH, NONE | 3DES (168) | SHA1 |
| ADH-AES128-SHA | SSLv3 | DH, NONE | AES (128) | SHA1 |
| ADH-RC4-MD5 | SSLv3 | DH, None | RC4 (128) | MD5 |
| ADH-DES-CBC-SHA | SSLv3 | DH, NONE | DES (56) | SHA1 |
| EXP-ADH-DES-CBC-SHA | SSLv3 | DH (512), None | DES (40) | SHA1 EXPORT |
| EXP-ADH-RC4-MD5 | SSLv3 | DH (512), None | RC4 (40) | MD5 EXPORT |

# Cipher list formats

The cipher list you specify for a virtual SSL server consists of one or more cipher strings separated by colons (for example, RC4:+RSA:+ALL:!NULL:!DH:!EXPORT@STRENGTH). You can combine lists of ciphers using a logical **and** operation (+) For example, SHA1+DES represents all cipher suites containing the SHA1 and the DES algorithms.

In the colon-separated list, the characters !, -, or + can precede any cipher string. These characters serve as modifiers, with the following meanings:

- `!` permanently deletes the ciphers from the list (for example: !RSA).
- `-` deletes the ciphers from the list, but you can add the ciphers again.
- `+` moves the ciphers to the end of the list. This option does not add any new ciphers; it just moves matching existing ones.
- `@STRENGTH` is placed at the end of the cipher list, and sorts the list in order of encryption algorithm key length.

`ALL@STRENGTH is` The default cipher list used for all virtual SSL servers on the Nortel VPN Router

A cipher list consisting of the string `RC4:ALL:!DH` translates into a preferred list of ciphers that begins with all ciphers using RC4 as the encryption algorithm, followed by all cipher suites except the eNULL ciphers (ALL). The final `!DH` string means that all cipher suites containing the DH (Diffie-Hellman) cipher are removed from the list. (Few of the major Web browsers support these ciphers.)

# Modifying a cipher list

An example of a slightly modified cipher list is: `RC4:ALL:!EXPORT:!DH`

This example removes all EXPORT ciphers and the DH-related cipher suites. Removing the EXPORT ciphers also remove ciphers using either 40- or 56-bit symmetric ciphers from the list. This means that browsers running export-controlled crypto software cannot access the server.

Use the OpenSSL command line tool (on a UNIX machine) to check which cipher suites a particular cipher list corresponds to. The preceding example yields the following output:

```
# openssl ciphers -v 'RC4:ALL:!EXPORT:!DH
RC4-SHA          SSLv3 Kx=RSA    Au=RSA   Enc=RC4(128)    Mac=SHA1
RC4-MD5          SSLv3 Kx=RSA    Au=RSA   Enc=RC4(128)    Mac=MD5
RC4-64-MD5       SSLv2 Kx=RSA    Au=RSA   Enc=RC4(64)     Mac=MD5
RC4-MD5          SSLv2 Kx=RSA    Au=RSA   Enc=RC4(128)    Mac=MD5
DES-CBC3-SHA     SSLv3 Kx=RSA    Au=RSA   Enc=3DES(168)   Mac=SHA1
DES-CBC-SHA      SSLv3 Kx=RSA    Au=RSA   Enc=DES(56)     Mac=SHA1
DES-CBC3-MD5     SSLv2 Kx=RSA    Au=RSA   Enc=3DES(168)   Mac=MD5
DES-CBC-MD5      SSLv2 Kx=RSA    Au=RSA   Enc=DES(56)     Mac=MD5
RC2-CBC-MD5      SSLv2 Kx=RSA    Au=RSA   Enc=RC2(128)    Mac=MD5
```

# Supported cipher strings and meanings

The following table lists each supported cipher string alias and its significance.

**Table 2** Cipher Strings and Meanings

| Cipher String Aliases | Meaning |
|---|---|
| DEFAULT | The default cipher list, which corresponds to `ALL@STRENGTH`. |
| ALL | All cipher suites except the eNULL ciphers, which you must explicitly enable. |
| HIGH | Cipher suites with key lengths larger than 128 bits. |
| MEDIUM | Cipher suites using 128-bit encryption. |
| LOW | Includes cipher suites using 64- or 56-bit encryption, but excludes export cipher suites. |
| EXPORT | Cipher suites using 40- and 56-bit encryption. |
| EXPORT40 | Cipher suites using 40-bit export encryption only. |
| EXPORT56 | Cipher suites using 56-bit export encryption only. |
| Cipher String Aliases | Meaning |

**Table 2** Cipher Strings and Meanings

| | |
|---|---|
| eNULL, NULL | Cipher suites that do not offer any encryption at all because they pose a security threat; they are disabled unless explicitly included. |
| aNULL | Cipher suites that do not offer authentication, like anonymous DH algorithms. The use of such cipher suites is not recommended, because they facilitate man-in-the-middle attacks. |
| kRSA, RSA | Cipher suites using RSA key exchange. |
| kEDH | Cipher suites using ephemeral Diffie-Hellman key agreement. |
| aRSA | Cipher suites using RSA authentication, which implies that the certificates carry RSA keys. |
| SSLv3, SSLv2 | SSL version 3.0 and SSL version 2.0 cipher suites, respectively. |
| DH | Cipher suites using DH encryption algorithms, including anonymous DH. |
| ADH | Cipher suites using anonymous DH encryption algorithms. |
| AES | Cipher suites using AES encryption algorithms. |
| 3DES | Cipher suites using triple DES encryption algorithms. |
| Cipher String Aliases | Meaning |
| DES | Cipher suites using DES encryption algorithms, but not triple DES. |
| RC4 | Cipher suites using RC4 encryption algorithms. |
| RC2 | Cipher suites using RC2 encryption algorithms. |
| MD5 | Cipher suites using MD5 encryption algorithms. |
| SHA1, SHA | Cipher suites using SHA1 encryption algorithms. |

# Appendix B
# SNMP agent

A Simple Network Management Protocol (SNMP) agent resides on the Nortel VPN Router. The agent listens to the IP address and Management IP (MIP).

The SNMP agent supports SNMP version 1 and version 2c. You can configure notification targets, which are the SNMP managers receiving trap messages from the agent, to use either SNMP v1 or SNMP v2c. The default is SNMP v2c. You can specify any number of notification targets on the Nortel VPN Router.

## Supported MIBs

The Nortel VPN Router supports the following MIBs:

- SNMPv2-MIB (host-specific)
- IP-MIB (host-specific)
- IP-FORWARD-MIB (host-specific)
- IF-MIB (host-specific)
- ALTEON-ISD-PLATFORM-MIB (cluster-specific)
- ALTEON-ISD-SSL-MIB (cluster-specific)
- SNMP-TARGET-MIB (cluster-specific)

The MIB is either host-specific or cluster-specific. The SNMP agent supports host-specific MIBs on every Nortel VPN Router and contains host-specific information. Only the MIB agent, which is the agent on the Nortel VPN Router that currently holds the MIB, supports cluster-specific MIBs and contains cluster-specific information.

## SNMPv2 MIB

The SNMPv2-MIB is a standard MIB that all agents implement and it contains the following groups and objects:

- System group, which is a collection of objects common to all managed systems.
- SNMP group, which is a collection of objects providing basic instrumentation and control of an SNMP entity.

## IP-MIB

The agent implements the following groups:

- ipGroup
- icmpGroup

## IP-FORWARD-MIB

The agent implements the following group:

- ipCidrRouteGroup

## IF-MIB

The agent implements the following groups:

- ifPacketGroup
- ifStackGroup

### Limitations

The agent does not implement the following objects:

- ifType
- ifSpeed
- ifLastChange

- ifInUnknownProtos
- ifOutNUnicast

The agent does not implement the following traps:

- linkUp
- linkDown

## Alteon iSD platform MIB

The ALTEON-ISD-PLATFORM-MIB contains the following groups and objects:

- Cluster group, whose objects provide information about the operational status of each Nortel VPN Router, IP address assignment, master/slave assignment, and the iSD host number.
- Performance group, whose objects provide information about CPU and memory utilization.
- Current Alarm group, whose objects provide information about the number of active alarms, alarm IDs, alarm severity levels, alarm cause, and the time when the alarm was triggered.
- Event group, whose objects provide information about the time when the event was generated, as well as a description of the event.

## Alteon iSD-SSL MIB

The ALTEON-ISD-SSL-MIB contains objects for monitoring the SSL gateways. The objects provide information about the following:

- Number of SSL transactions per second.
- Number of initiated client SSL connections.
- Number of renegotiated client SSL connections.
- Number of successfully completed SSL handshakes.
- Number of client requests for a session ID found in the SSL cache.
- Number of client requests for a session ID not found in the SSL cache.
- Number of times a session ID could not be cached because the SSL cache was full.

- Number of client requests for a session ID that was found in the SSL cache, but inaccessible due to the fact that the Time To Live value for the session was exceeded.

### SNMP-TARGET-MIB

The SNMP-TARGET-MIB contains information about where to send traps.

## Supported traps

The following SNMP traps are supported by the Nortel VPN Router:

**Table 3** Traps supported by the Nortel VPN Router

| Trap Name | Description |
|---|---|
| alteonISDSSLHwFail | Signifies that the SSL accelerator hardware failed. The Nortel VPN Router will continue to handle traffic, but with severely degraded performance. |
| alteonISDDown | Signifies that the Nortel VPN Router is down and out of service. |

# Appendix C
# Syslog messages

This appendix contains a list of the syslog messages sent from the Nortel VPN Router to a syslog server if a syslog server resides on the system. Syslog servers are added to the system configuration by using the menu options in the Syslog Servers menu.

The messages are divided into the following message types:

- Operating system (OS)
- system control
- traffic processing
- startup
- configuration reload

To view a list of syslog messages in alphabetical order, see section "Syslog messages in alphabetical order" on page 57.

## Operating system messages

The operating system (OS) messages are divided into three categories:

- EMERG
- CRITICAL
- ERROR

### EMERG

The following lists the EMERG messages:

- Root filesystem corrupt.
- The system cannot boot, but stops with a single-user prompt. fsck failed. Reinstall in order to recover.
- Config filesystem corrupt beyond repair.
- The system cannot boot, but stops with a single-user prompt. Reinstall in order to recover.
- Failed to write to config filesystem.
- Probable hardware error. Reinstall.

## CRITICAL

The following lists the CRITICAL messages:

- Config filesystem re-initialized - reinstall required.
- Reinstall.
- Application filesystem corrupt - reinstall required.
- Reinstall.

## ERROR

The following lists the ERROR messages:

- Config filesystem corrupt.

  Possible loss of configuration. Followed by the message Config filesystem re-initialized - reinstall required or Config filesystem restored from backup.

- Missing files in config filesystem.

  Possible loss of configuration. Followed by the message Config filesystem re-initialized - reinstall required or Config filesystem restored from backup.

- Logs filesystem re-initialized.

  Loss of logs.

- Root filesystem repaired - rebooting.

  fsck found and fixed errors. Probably OK.

- Config filesystem restored from backup.

Loss of recent configuration changes.

- Rebooting to revert to permanent OS version.

  Happens after Config filesystem re-initialized - reinstall required or Config filesystem restored from backup if software upgrade is in progress (if failure at first boot on new OS version).

# System control messages

The system control process messages are divided into three categories:

- INFO
- ALARM
- EVENT

Both events and alarms are stored in the event log file.

## INFO

System started [isdssl-<version>]

Sent whenever the system control process is started or restarted.

## ALARM

Alarms are sent at a syslog level corresponding to the alarm severity as shown in the following table:

**Table 4** Alarm severity

| Alarm Severity | Syslog Level |
|---|---|
| CRITICAL | ALERT |
| MAJOR | CRITICAL |
| MINOR | ERROR |
| WARNING | WARNING |
| * | ERROR |

Alarms are formatted according to the following pattern:

Id: <alarm sequence number>
Severity: <severity>
Name: <name of alarm>
Time. <date and time of the alarm>
Sender: <sender, for example, system or the Nortel VPN Router IP address>
Cause: <cause of the alarm>
Extra: <additional information about the alarm>

To simplify finding the desired alarm messages, this section lists alarms with the **name** parameter on top.

- Name: **isd_down**
  Sender: <IP>
  Cause: down
  Extra:
  Severity: critical

  A member of the SSL VPN Module 1000 cluster is down. This alarm is only sent if the cluster contains more than one Nortel VPN Router.

- Name: **single_master**
  Sender: system
  Cause: down
  Extra:
  Severity: warning

  Only one master Nortel VPN Router in the cluster is up and running.

- Name: **log_open_failed**
  Sender: <IP>, event
  Cause and Extra are explanations of the fault.
  Severity: major

  The event log (where all events and alarms are stored) could not open.

- Name: **make_software_release_permanent_failed**
  Sender: <IP>
  Cause: file_error | not_installed
  Extra: “Detailed info”
  Severity: critical

Failed to make a new software release permanent after activation. The system automatically reverts to the previous version.

- Name: **copy_software_release_failed**
  Sender: <IP>
  Cause: copy_failed | bad_release_package | no_release_package | unpack_failed
  Extra: “Detailed info”
  Severity: critical

  A Nortel VPN Router failed to install a software release while trying to install the same version as all other Nortel VPN Routers in the cluster. The failing Nortel VPN Router tries to catch up with the other cluster members as it was not up and running when the new software version was installed.

- Name: **license**
  Sender: license_server
  Cause: license_not_loaded
  Extra: “All iSDs do not have the same license loaded”
  Severity: warning

  One or several Nortel VPN Routers in the cluster do not have the same SSL VPN license (with reference to number of concurrent users).

- Name: **ssl_hw_fail**
  Sender: <IP>
  Cause: find_error |init_error
  Extra:
  Severity: major

  The SSL hardware acceleration card cannot be found or initiated. This causes the Nortel VPN Router to run with degraded performance.

- Name: **hsm_not_logged_in**
  Sender: <IP>, <Token>
  Cause: reboot
  Extra: “Card<Token>”
  Severity: critical

  After a reboot, login to the HSM card is required.

- Name: **hsm_tampered_with**
  Sender: <IP>, <Token>
  Cause: hsm_detected
  Extra: “Card<Token>”
  Severity: critical
- Name: **slave_not_starting**
  Sender: <IP>, <SlaveNo>
  Cause: start_error | connect_timeout | fdsend | nothidden | name_resolv | nodename_occupied
  Extra:”
  Severity: warning

  The portal handling subsystem cannot be started.

## EVENT

Events are sent at the NOTICE syslog level. They are formatted according to the following pattern:

Name: <Name>
Sender: <Sender>
Extra: <Extra>

- Name: **clear_alarm**
  Sender: <ID>
  Extra:

  The alarm with <ID> is cleared.
- Name: **partitioned_network**
  Sender and Extra is lower level information.

  Sent to indicate that an Nortel VPN Router is recovering from a partitioned network situation.
- Name: **software_configuration_changed**
  Sender: system
  Extra: software release version <VSN> <Status>

  Indicates that release <VSN> (version) is <Status> (unpacked/installed/permanent).

- Name: **software_release_copying**
  Sender: <IP>
  Extra: copy software release <VSN> from other cluster member

  Indicates that <IP> is copying the release <VSN> from another cluster member.

- Name: **software_release_rebooting**
  Sender: <IP>
  Extra: reboot with release version <VSN>

  Indicates that a Nortel VPN Router (<IP>) is rebooting on a new release (Nortel VPN Router that was not up and running during the normal installation is now catching up).

# Traffic processing messages

The traffic processing subsystem messages are divided into these categories:

- CRITICAL
- ERROR
- WARNING
- INFO

## CRITICAL

DNS alarm: all dns servers are DOWN

All DNS servers are down. The Nortel VPN Router cannot perform DNS lookups.

## ERROR

The following lists the ERROR messages:

- internal error: <no>

  An internal error occurred. Please contact support with as much information as possible to reproduce this message.

- javascript error: <reason> for: <host><path>

JavaScript parsing error encountered when parsing content from <host><path>. This can be a problem in the SSL VPN Module 1000 JavaScript parser, but most likely a syntactical error in the JavaScript on that page.

- vbscript error: <reason> for: <host><path>

  VBScript parsing error encountered when parsing content from <host><path>. This can be a problem in the SSL VPN Module 1000 VBScript parser, but most likely a syntactical error in the VBScript on that page.

- jscript.encode error: <reason>

  Problem encountered when parsing an encoded JavaScript. It can be a problem with the JavaScript parser in the SSL VPN Module 1000 or it can be a problem on the processed page.

- css error: <reason>

  Problem encountered when parsing a style sheet. It can be a problem with the css parser in the SSL VPN Module 1000 or it can be a problem on the processed page.

- Failed to syslog traffic:<reason> -- disabling traf log

  Problem occurred when the SSL VPN Module 1000 tried to send traffic logging syslog messages. Traffic system logging was disabled as a result.

- www_authenticate: bad credentials

  The browser sent a malformed WWW-Authenticate: credentials header. Most likely a broken client.

- http error: <reason>, Request="<method> <host><path>"

  A problem was encountered when parsing the HTTP traffic. This message indicates that a nonstandard client or server or the SSL VPN Module 1000 HTTP parser is out of sync due to an earlier non-standard transaction from the client or server on this TCP stream.

- http header warning cli: <reason> (<header>)

  The client sent a bad HTTP header.

- http header warning srv: <reason> (<header>)

  The server sent a bad HTTP header.

- unknown WWW-Authenticate method, closing

Backend server sent unknown HTTP authentication method.

- failed to parse Set-Cookie <header>

  The SSL VPN Module 1000 got a malformed Set-Cookie header from the backend Web server.

- failed to locate corresponding portal for portal authenticated http server

  Portal authentication is configured for an HTTP server, but no portal using the same VPN can be found. Make sure that there is a portal running using the same VPN id.

- Bad IP:PORT data <line> in thc script

  Bad ip:port found in health check script. Please reconfigure the health script. The command line interface normally captures the bad ip:port.

- Bad regexp (<expr>) in health check

  Bad regular expression found in health check script. Please reconfigure.

- Bad script op found <script op>

  Bad script operation found in health check script. Please reconfigure.

- Unable to use the certificate for <server nr>

  Unsuitable certificate configured for server #.

- The private key and certificate don't match for <server nr>

  Key and certificate does not match for server #. You must change the certificate.

- Unable to use client private key for <server #>

  Key for doing sslconnect is not valid. Please reconfigure.

- Unable to find client private key for <server #>

  Key for doing sslconnect is not valid. Please reconfigure.

- Unable to use client certificate for <server #>

  Certificate for doing sslconnect is not valid. Please reconfigure.

- Failed to initialize SSL hardware

  Problem initializing SSL acceleration hardware. This causes the SSL VPN module firmware to run with degraded performance.

- Could not find SSL hardware.

Failed to detect SSL acceleration hardware.

- Connect failed: <reason>

  Connect to backend server failed with <reason>

- SSL connect failed: <reason>

  SSL connect to backend server failed with <reason>

- html error: <reason>

  Error encountered when parsing HTML. Probably non-standard HTML.

- socks error: <reason>

  Error encountered when parsing the socks traffic from the client. Probably a non-standard socks client.

- socks request: socks version <version> rejected

  SOCKS request of version <version> received and rejected. Most likely a non-standard SOCKS client.

- Cannot bind to local address: <ip>:<port>: <reason>

  Problem encountered when trying to set up virtual server on <ip>:<port>.

- Ignoring DNS packet was not from any of the defined namesserver <ip>:<port>

  SSL VPN Module 1000 received reply for non-configured DNS server.

## WARNING

TPS license limit (<limit>) exceeded

The transactions per second (TPS) limit is exceeded.

## INFO

The following lists the INFO messages:

- gzip error: <reason>

  Problem encountered when processing compressed content.

- gzip warning: <reason>

Problem encountered when processing compressed content.

- accept() turned off (<nr>) too many fds

  The Nortel VPN Router temporarily stopped accepting new connections. This happens when the Nortel VPN Router is overloaded. It starts accepting connections after it finishes processing current sessions.

- No cert supplied by backend server

  No certificate supplied by backend server when doing SSL connect. Session terminated to backend server.

- No CN supplied in server cert <subject>

  No CN found in the subject of the certificate supplied by the backend server.

- Bad CN supplied in server cert <subject>

  Malformed CN found in subject of the certificate supplied by the backend server.

- Shutting sslproxy down.

  Traffic subsystem is stopped.

- Restarting proxy due to <reason>

  Traffic subsystem restarted due to <reason>

- DNS alarm: dns server(s) are UP

  At least one DNS server is now up.

- HC: backend <ip>:<port> is down

  Backend health check detected backend <ip>:<port> to be down.

- HC: backend <ip>:<port> is up again

  Backend health check detected backend <ip>:<port> to be up.

## Startup messages

The traffic processing subsystem startup messages include the INFO category.

## INFO

The following lists the INFO messages:

- HSM mode: <mode>

  Hardware Security Mode <mode>.

- Disabling transparent proxy, non-compatible with pooling

  Transparent proxy mode is disabled due when pooling is enabled (startup message).

- Set CSWIFT as default

  Using CSWIFT SSL hardware acceleration. (startup message)

- Using <hwtype> hardware

  Using <hwtype> hardware for SSL acceleration. (startup message)

- Loaded <ip>:<port>

  Initializing virtual server <ip>:<port>.

- Because clicerts are used, force adjust totalcache size to: <size> per server that use clicerts

  Generated if the size of the SSL session cache is modified.

- No more than <nr> backend supported

  Generated when more than the maximum allowed backend servers is configured.

- TPS license limit: <limit>

  TPS limit set to <limit>

- No TPS license limit

  Unlimited TPS license used.

- Started ssl-proxy

  Traffic subsystem started.

- Found <size> meg of phys mem

  Amount of physical memory found on system.

# Configuration reload messages

The traffic subsystem configuration reload messages include the INFO category.

## INFO

The following lists the INFO messages:

- reload cert config start

  Starting reloading of certificates.
- reload cert config done

  Certificate reloading done.
- reload configuration start

  Virtual server configuration reloading start.
- reload configuration network down

# Syslog messages in alphabetical order

This section lists the syslog messages in alphabetical order.

**Table 5** Syslog Messages in Alphabetical Order

| Message | Severity | Type | Explanation |
|---|---|---|---|
| accept() turned off (<nr>) too many fds | INFO | Traffic Processing | The Nortel VPN Router temporarily stopped accepting new connections. This happens when the Nortel VPN Router is overloaded. It starts accepting connections after it finishes processing its current sessions. |
| Application filesystem corrupt - reinstall required | CRITICAL | OS | Reinstall. |
| Bad CN supplied in server cert <subject> | INFO | Traffic Processing | Malformed CN found in subject of the certificate supplied by the backend server. |

**Table 5** Syslog Messages in Alphabetical Order

| Message | Severity | Type | Explanation |
|---|---|---|---|
| Can't bind to local address: <ip>:<port>: <reason> | ERROR | Traffic Processing | Problem encountered when trying to set up virtual server on <*ip*>:<*port*>. |
| clear_alarm | EVENT | System Control | The alarm with <*ID*> is cleared. |
| Config filesystem corrupt | ERROR | OS | Possible loss of configuration. Followed by the message **Config filesystem re-initialized - reinstall required** or **Config filesystem restored from backup**. |
| Config filesystem corrupt beyond repair | EMERG | OS | The system cannot boot, but stops with a single-user prompt. Reinstall in order to recover. |
| Config filesystem re-initialized - reinstall required | CRITICAL | OS | Reinstall. |
| Config filesystem restored from backup | ERROR | OS | Loss of recent configuration changes. |
| Connect failed: <reason> | ERROR | Traffic Processing | Connect to backend server failed with <*reason*>. |
| copy_software_release_failed | ALARM (CRITICAL) | System Control | A Nortel VPN Router failed to install a software release while trying to install the same version as all other Nortel VPN Routers in the cluster. The failing Nortel VPN Router tries to catch up with the other cluster members as it was not up and running when the new software version was installed. |
| Could not find SSL hardware. | ERROR | Traffic Processing | Failed to detect SSL acceleration hardware. |
| css error: <reason> | ERROR | Traffic Processing | Problem encountered when parsing a style sheet. It can be a problem with the css parser in the SSL VPN Module 1000 or it can be a problem on the processed page. |
| Disabling transparent proxy, non-compatible with pooling | INFO | Startup | Transparent proxy mode is disabled due to pooling is enabled. |

**Table 5** Syslog Messages in Alphabetical Order

| Message | Severity | Type | Explanation |
|---|---|---|---|
| DNS alarm: all dns servers are DOWN | CRITICAL | Traffic Processing | All DNS servers are down. The Nortel VPN Router cannot perform DNS lookups. |
| DNS alarm: dns server(s) are UP | INFO | Traffic Processing | At least one DNS server is now up. |
| Failed to initialize SSL hardware | ERROR | Traffic Processing | Problem initializing SSL acceleration hardware. This causes the SSL VPN module firmware to run with degraded performance. |
| failed to locate corresponding portal for portal authenticated http server | ERROR | Traffic Processing | Portal authentication is configured for an http server, but no portal using the same VPN can be found. Make sure that there is a portal running using the same VPN id. |
| failed to parse Set-Cookie <header> | ERROR | Traffic Processing | The SSL VPN Module 1000 got a malformed Set-Cookie header from the backend Web server. |
| Failed to syslog traffic:<reason> -- disabling traf log | ERROR | Traffic Processing | Problem occurred when the SSL VPN Module 1000 tried to send traffic logging syslog messages. Traffic syslogging was disabled as a result. |
| Failed to write to config filesystem | EMERG | OS | Probable hardware error. Reinstall. |
| Found <size> meg of phys mem | INFO | Startup | Amount of physical memory found on system. |
| gzip error: <reason> | INFO | Traffic Processing | Problem encountered when processing compressed content. |
| gzip warning: <reason> | INFO | Traffic Processing | Problem encountered when processing compressed content. |
| HC: backend <ip>:<port> is down | INFO | Traffic Processing | Backend health check detected backend <ip>:<port> to be down. |
| HC: backend <ip>:<port> is up again | INFO | Traffic Processing | Backend health check detected backend <ip>:<port> to be up. |
| HSM mode: <mode> | INFO | Startup | Hardware Security Mode <mode>. |

**Table 5** Syslog Messages in Alphabetical Order

| Message | Severity | Type | Explanation |
|---|---|---|---|
| hsm_not_logged_in | ALARM (CRITICAL) | System Control | After a reboot, login to the HSM card is required. |
| hsm_tampered_with | ALARM (CRITICAL) | System Control | |
| html error: <reason> | ERROR | Traffic Processing | Error encountered when parsing HTML. Probably non-standard HTML. |
| http error: <reason>, Request="<method> <host><path>" | ERROR | Traffic Processing | A problem was encountered when parsing the HTTP traffic. This message indicates a non-standard client or server or the SSL VPN Module 1000 HTTP parser is out of sync due to an earlier non-standard transaction from the client or server on this TCP stream. |
| http header warning cli: <reason> (<header>) | ERROR | Traffic Processing | The client sent a bad HTTP header. |
| http header warning srv: <reason> (<header>) | ERROR | Traffic Processing | The server sent a bad HTTP header. |
| HTTP NotLoggedIn, SrcIP="<ip>", Request="<request>" | INFO | AAA | |
| HTTP Rejected User="<user>", SrcIP="<ip>", Request="<request>" | INFO | AAA | The remote failed to access the specified Web server from the l Browse Intranet tab. on the portal |
| HTTP User="<user>", SrcIP="<ip>", Request="<request>" | INFO | AAA | The remote user successfully accessed the specified Web server from the Browse Intranet tab on the portal. |
| Ignoring DNS packet was not from any of the defined namesserver <ip>:<port> | ERROR | Traffic Processing | SSL VPN Module 1000 received reply for non-configured DNS server. |
| internal error: <no> | ERROR | Traffic Processing | An internal error occurred. Please contact support with as much information as possible to reproduce this message. |

**Table 5** Syslog Messages in Alphabetical Order

| Message | Severity | Type | Explanation |
|---|---|---|---|
| isd_down | ALARM (CRITICAL) | System Control | A member of the SSL VPN Module 1000 cluster is down. This alarm is only sent if the cluster contains more than one Nortel VPN Router. |
| javascript error: <reason> for: <host><path> | ERROR | Traffic Processing | JavaScript parsing error encountered when parsing content from <host><path>. This can be a problem in the SSL VPN Module 1000 JavaScript parser, but most likely a syntactical error in the JavaScript on that page. |
| jscript.encode error: <reason> | ERROR | Traffic Processing | Problem encountered when parsing an encoded JavaScript. It can be a problem with the JavaScript parser in the SSL VPN Module 1000 or it can be a problem on the processed page. |
| LDAP backend(s) unreachable VPNId=<id> AuthId=<authid> | ERROR | AAA | Shown if LDAP servers cannot be reached when a user tries to log in to the portal. |
| license | ALARM (WARNING) | System Control | One or several Nortel VPN Routers in the cluster do not have the same SSL VPN license (with reference to number of concurrent users). |
| Loaded <ip>:<port> | INFO | Startup | Initializing virtual server <ip>:<port>. |
| log_open_failed | ALARM (MAJOR) | System Control | The event log (where all events and alarms are stored) could not be opened. |
| Logs filesystem re-initialized | ERROR | OS | Loss of logs. |
| make_software_release_permanent_failed | ALARM (CRITICAL) | System Control | Failed to make a new software release permanent after activation. The system automatically reverts to the previous version. |
| Missing files in config filesystem | ERROR | OS | Possible loss of configuration. Followed by the message “Config filesystem re-initialized - reinstall required” or “Config filesystem restored from backup”. |

**Table 5** Syslog Messages in Alphabetical Order

| Message | Severity | Type | Explanation |
|---|---|---|---|
| No cert supplied by backend server | INFO | Traffic Processing | No certificate supplied by backend server when doing SSL connect. Session terminated to backend server. |
| No CN supplied in server cert <subject> | INFO | Traffic Processing | No CN found in the subject of the certificate supplied by the backend server. |
| No more than <nr> backend supported | INFO | Startup | Generated when more than the maximum allowed backend servers is configured. |
| No TPS license limit | INFO | Startup | Unlimited TPS license used. |
| partitioned_network | EVENT | System Control | Sent to indicate that a Nortel VPN Router is recovering from a partitioned network situation. |
| PORTAL reject User="<user>" Proto="<proto>" Host="<host>" Share="<share>" Path="<path>" | INFO | AAA | The remote user failed to access the specified folder/directory on the specified file server from the Files tab on the portal. |
| PORTAL User="<user>" Proto="<proto>" Host="<host>" Share="<share>" Path="<path>" | INFO | AAA | The remote user successfully accessed the specified folder/ directory on the specified file server from the Files tab on the portal. |
| Rebooting to revert to permanent OS version | ERROR | OS | Happens after “Config filesystem re-initialized - reinstall required” or “Config filesystem restored from backup” if software upgrade is in progress (if failure at first boot on new OS version). |
| reload cert config done | INFO | Config Reload | Certificate reloading done. |
| reload cert config start | INFO | Config Reload | Starting reloading of certificates. |
| reload configuration done | INFO | Config Reload | Virtual server configuration reloading done. |
| reload configuration network down | INFO | Config Reload | Accepting new sessions are temporarily put on hold. |
| reload configuration network up | INFO | Config Reload | Resuming accepting new sessions after loading new configuration. |

**Table 5** Syslog Messages in Alphabetical Order

| Message | Severity | Type | Explanation |
|---|---|---|---|
| reload configuration start | INFO | Config Reload | Virtual server configuration reloading start. |
| Restarting proxy due to <reason> | INFO | Traffic Processing | Traffic subsystem restarted due to <reason>. |
| Root filesystem corrupt | EMERG | OS | The system cannot boot, but stops with a single-user prompt. fsck failed. Reinstall in order to recover. |
| Root filesystem repaired - rebooting | ERROR | OS | fsck found and fixed errors. Probably OK. |
| Set CSWIFT as default | INFO | Startup | Using CSWIFT SSL hardware acceleration. |
| Shutting sslproxy down. | INFO | Traffic Processing | Traffic subsystem is stopped. |
| Because clicerts are used, force adjust totalcache size to: <size> per server that use clicerts | INFO | Startup | Generated if the size of the SSL session cache is modified. |
| single_master | ALARM (WARNING) | System Control | Only one master Nortel VPN Router in the cluster is up and running. |
| slave_not_starting | ALARM (WARNING) | System Control | The portal handling subsystem cannot be started. |
| socks error: <reason> | ERROR | Traffic Processing | Error encountered when parsing the SOCKS traffic from the client. Probably a non-standard socks client. |
| SOCKS Rejected User="<user>", SrcIP="<ip>", Request="<request>" | INFO | AAA | The remote user failed to perform an operation by using one of the features available under the Advanced tab. |
| socks request: socks version <version> rejected | ERROR | Traffic Processing | SOCKS request of version <version> received and rejected. Most likely a non-standard SOCKS client. |
| SOCKS User="<user>", SrcIP="<ip>", Request="<request>" | INFO | AAA | The remote user successfully performed an operation by using one of the features available under the Advanced tab. |

**Table 5** Syslog Messages in Alphabetical Order

| Message | Severity | Type | Explanation |
|---|---|---|---|
| software_configuration_changed | EVENT | System Control | Indicates that release <*VSN*> (version) is <*Status*> (unpacked/ installed/permanent). |
| software_release_copying | EVENT | System Control | Indicates that <*IP*> is copying the release <*VSN*> from another cluster member. |
| software_release_rebooting | EVENT | System Control | Indicates that a Nortel VPN Router (<*IP*>) is rebooting on a new release (Nortel VPN Router that was not up and running during the normal installation is now catching up). |
| SSL connect failed: <reason> | ERROR | Traffic Processing | SSL connect to backend server failed with <*reason*>. |
| ssl_hw_fail | ALARM (MAJOR) | System Control | The SSL hardware acceleration card could not be found or initiated. This causes the Nortel VPN Router to run with degraded performance. |
| Started ssl-proxy | INFO | Startup | Traffic subsystem started. |
| System started [isdssl-<version>] | INFO | System Control | Sent whenever the system control process is started or restarted. |
| The private key and certificate don't match for <server nr> | ERROR | Traffic Processing | Key and certificate do not match for server #. You must change the certificate. |
| TPS license limit (<limit>) exceeded | WARNING | Traffic Processing | The transactions per second (TPS) limit is exceeded. |
| TPS license limit: <limit> | INFO | Startup | TPS limit set to <*limit*>. |
| Unable to find client private key for <server #> | ERROR | Traffic Processing | Key for doing sslconnect is not valid. Please reconfigure. |
| Unable to use client certificate for <server #> | ERROR | Traffic Processing | Certificate for doing sslconnect is not valid. Please reconfigure. |
| Unable to use client private key for <server #> | ERROR | Traffic Processing | Key for doing sslconnect is not valid. Please reconfigure. |
| Unable to use the certificate for <server nr> | ERROR | Traffic Processing | Unsuitable certificate configured for server #. |

**Table 5** Syslog Messages in Alphabetical Order

| Message | Severity | Type | Explanation |
|---|---|---|---|
| unknown WWW-Authenticate method, closing | ERROR | Traffic Processing | Backend server sent unknown HTTP authentication method. |
| Using <hwtype> hardware | INFO | Startup | Using <*hwtype*> hardware for SSL acceleration. |
| vbscript error: <reason> for: <host><path> | ERROR | Traffic Processing | VBScript parsing error encountered when parsing content from <*host*><*path*>. This can be a problem in the SSL VPN Module 1000 VBScript parser, but most likely a syntactical error in the VBScript on that page. |
| www_authenticate: bad credentials | ERROR | Traffic Processing | The browser sent a malformed WWW-Authenticate: credentials header. Most likely a broken client. |
| VPN Login: failed - client ip: <ip> [user: <user>] error: <error> | INFO | AAA | Portal login failed. The remote user client IP address, user name is shown along with error cause. |
| VPN Login: succeeded - client ip: <ip> user: <user> groups: <groups> | INFO | AAA | Portal login succeeded. The remote user client IP address, user name and group membership is shown. |
| VPN Logout: user: <user> | INFO | AAA | The remote user logged out from the portal session. |

# Appendix D
# Key code definitions

When you use the Telnet applet available under the Advanced tab of the portal, you can specify a keymap URL that points to a key code definition file. If the application uses a different keyboard layout than the standard VT320, you can create and upload a key code definition file to the keymap URL. This appendix shows how to create the key code definition file.

## Syntax description

You can define most special keys according to the following syntax rule:

[**S**|**C**|**A**] *KEY***=***STRING*

The characters enclosed in square brackets (`[ ]`) are optional. Only one of the characters `S` (SHIFT), `C` (CTRL) or `A` (ALT) can appear before *KEY*, which is a textual representation of the key you want to redefine (F1, PGUP etc.).

The new *STRING* succeeds the equals character (**=**). Hash marks (#) in the file declare the line as a comment. The following examples explain the syntax in more detail:

On pressing the `F1` key, send the string *test*.

```
F1 = test
```

On pressing `Control + PGUP`, send the string *pgup pressed*:

```
CPGUP = pgup pressed
```

Redefine the key `Alt + F12` to send an escape character:

AF12 = \\e

The string can contain special characters which can be escaped using the backslash (\).

## Allowed special characters

The following table includes allowed special characters:

**Note:** For some escape codes, you need two backslashes, because these are specific Java SSH definitions the Java Property mechanism does not recognize.

**Table 6** Allowed special characters

| Special Character | Explanation |
|---|---|
| \\b | Backspace. This character is usually sent by the <- key (Backspace key). |
| \\e | Escape. This character is usually sent by the Esc key. |
| \n | Newline. This character will move the cursor to a new line. On UNIX systems, it is equivalent to carriage return + newline. Usually the Enter key sends this character. |
| \r | Carriage Return. This key moves the cursor to the beginning of the line. In conjunction with Newline, it moves the cursor to the beginning of a new line. |
| \t | Tabulator. The tab character is sent by the TAB key and moves the cursor to the next tab stop defined by the terminal. |
| \\v | Vertical Tabulator. Sends a vertical tabulator character. |
| \\a | Bell. Sends a terminal bell character which makes the terminal sound its bell. |
| \\number | Inserts the character that is defined by this *number* in the ISO Latin1 character set. The *number* must be an octal value. |

## Redefinable keys

The following table explains which keys can be redefined. You can prefix each key by a character to redefine the action that occurs when the key is pressed in with the SHIFT, CTRL or ALT keys.

**Table 7** Redefinable keys

| Key Representation | Remarks |
|---|---|
| F1-F20 | Function keys (F1, F2 etc. up to F20) |
| PGUP | Page Up key |
| PGDOWN | Page Down key |
| END | End key |
| HOME | Home (Pos 1) key |
| INSERT | Insert key |
| REMOVE | Remove key |
| UP | Cursor Up key |
| DOWN | Cursor Down key |
| LEFT | Cursor Left key |
| RIGHT | Cursor Right key |
| NUMPAD0-NUMPAD9 | Numbered Numeric keypad keys |
| ESCAPE | Escape key |
| BACKSPACE | Backspace key |
| TAB | Tab key |

# Example of key code definition file

The following output is an example of the `keyCodes.at386` key code definition file, created for an AT-386 Terminal.

```
#
F1=\\eOP
F2=\\eOQ
F3=\\eOR
F4=\\eOS
F5=\\eOT
F6=\\eOU
F7=\\eOV
F8=\\eOW
F9=\\eOX
F10=\\eOY
F11=\\eOZ
F12=\\eOA
#
# Shift F1 thru F10
#
SF1=\\eOp
SF2=\\eOq
SF3=\\eOr
SF4=\\eOs
SF5=\\eOt
SF6=\\eOu
SF7=\\eOv
SF8=\\eOw
SF9=\\eOx
SF10=\\eOy
SF11=\\eOz
SF12=\\eOa
#
# Other cursor movement keys
#
UP=\\e[A
DOWN=\\e[B
RIGHT=\\e[C
LEFT=\\e[D
#
INSERT=\\e[@
# REMOVE=\\177  #( hex 7F  /  Decimal 127  /  Octal  177  /
DEL Key)
#
HOME=\\e[H
PGDOWN=\\e[U
PGUP=\\e[V
END=\\e[Y
#
```

# Appendix E
# Troubleshooting

After you initialize the VPN and configure the SSL VPN, you are able to log in to the portal with the username and password of a user that is already defined on the Nortel VPN Router.

Listed below are a few scenarios that require troubleshooting.

**If you cannot get to the Portal Login Page:**

1. On the Nortel VPN Router, choose **Services, SSL VPN**.

   The Current Status section of the window should indicate that the status is Operational and the Virtual Server Ports list should include 443.

2. If it does not indicate the status as Operational, choose **Status, Event Log**.

   The eventlog tells you what the error is. If you can not find the error in the eventlog, go back to the Services > SSL VPN window. Each time you check this window (if there is an error), it will update the event log with another event.

3. Fix the condition indicated in the event log.

**If this does not fix your issue, try the following:**

1. Ensure that the user is using the following syntax on their browser:

   ```
   https://x.x.x.x/
   or
   https://<VPN_name>
   ```

   where *x.x.x.x* is the public interface of the Nortel VPN Router and <*VPN_name*> is the DNS entry for your Nortel VPN Router public interface.

2. You can also select the **Config Summary** button on the **Services, SSL VPN** page in the Nortel VPN Router web interface. This accesses the SSL VPN

Configuration Summary window that gives a big picture of all the important data configured on the SSL VPN. For example, a list of active servers and ports is at the very top.

**You can get to the Portal Page, but login fails.**

1. Choose **Status, Event log** and inspect it.

   After a user has attempted to log in, an event is written to the event log.If there are no event log entries pertaining to this issue, then it is likely that the dialog between the SSL card RADIUS client and the Nortel VPN Router RADIUS server is not working correctly.

2. Choose **Services, RADIUS**.

   Ensure that RADIUS is enabled and set up correctly. The easiest configuration is to enable the default client and enter the password.

**If there are entries in the event log:**

1. If the eventlog says that the user was accepted, check that the Groups on the SSL Card mirror the Groups on the Nortel VPN Router.
2. Check that the group on the SSL Card has the correct access permissions:
   a. In the GUI, choose **VPN Gateways and Group Settings, Access Lis**t.
   b. Check that the Access Lists have Actions. If not, add them.

**If the event log shows that the user was denied access or not found:**

The Nortel VPN Router must have configured users for internal LDAP, external LDAP, or RADIUS. The SSL Card uses these same users.

1. From the Nortel VPN Router, choose **Services, RADIUS** and check that the authentication order is set up correctly. If Nortel VPN Router users are held in RADIUS, be sure that RADIUS is at the top of the authentication list. The same applies for LDAP proxy.
2. If there are no users, choose **Profiles, Users** and add a user to the Nortel VPN Router. Make the authentication order LDAP internal.

# Index

## T



## U



## W