Nortel VPN Gateway 5.1

Release Notes

part number: 216372-D, March 2005

4655 Great America Parkway
Santa Clara, CA 95054
Phone 1-800-4Nortel
http://www.nortel.com

Export

This product, software and related technology is subject to U.S. export control and may be subject to export or import regulations in other countries. Purchaser must strictly comply with all such laws and regulations. A license to export or reexport may be required by the U.S. Department of Commerce.

Licensing

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes a TAP-Win32 driver derived from the CIPE-Win32 kernel driver, Copyright © Damion K. Wilson, and is licensed under the GPL.

See Appendix D, “License Information”, in the *User's Guide* for more information

Release Notes

These Release Notes provide the latest information regarding your Nortel VPN Gateway (NVG) with version 5.1 software. This supplement lists the new features and modifies some information found in the complete documentation:

- *User's Guide*
  (part number 216368-C, March 2005)
- *Command Reference*
  (part number 216369-C, March 2005)
- *Application Guide for SSL Acceleration*
  (part number 216370-C, March 2005)
- *CLI Application Guide for VPN*
  (part number 216371-C, March 2005)
- *BBI Application Guide for VPN*
  (part number 217239-B, March 2005)
- *VPN Administrator's Guide*
  (part number 217238-B, March 2005)
- *VPN Gateway 3050/3070 Hardware Installation Guide*
  (part number 216213-B, March 2005)
- *Configuring Tunnel Guard Guide*
  (part number 317017-A, August 2003)

Documentation Download

These manuals are available for download from Nortel's Customer Support Web site:

1. **Point your browser to: http://www.nortel.com.**
2. **Under Support and Training, select Technical Documentation.**
3. **In the three-step Product Finder guide, select one of the following:**

   VPN Gateway ▸ VPN Gateway 3050/3070 ▸ Documentation

   Contivity ▸ VPN Tunnel Guard ▸ Documentation
4. **Select the desired document.**

New Features/Enhancements in Software Version 5.1

This section lists software features and enhancements added since version 5.0.3.

Hardware Support

Added support for the Nortel VPN Gateway 3070 hardware model.

General

- Added support for the VPN Gateway to automatically log in a remote user to the VPN if the user has a valid SMSESSION (SiteMinder session) cookie from another SiteMinder-enabled site.
  CLI path: `/cfg/vpn/aaa/auth/siteminder/sso` and `scope`
  BBI path: VPN Gateways>Authentication>Auth Servers (SiteMinder mechanism)>Allow Single Sign-On and Domain Cookie Scope
- Added command that can be used to force the Port Forwarder and HTTP Proxy applets to ignore any automatic proxy configuration script (PAC file) in Internet Explorer.
  CLI path: `/cfg/vpn/adv/usepac`

Fixes

This section lists fixes added since version 5.0.3.

General

- Added support for longer timeout when talking to more than one SiteMinder server. (CR Q01049925)
- Fixed problem with SMB/FTP directory link using Asian Character set (CR Q01083876).
- Fixed problem with hosts file update performed by the Outlook port forwarder when more than one Exchange server was specified. (CR Q01072952)
- Fixed problem with client certificates on smart cards. Previously, a user that logged in with a smart card would be able to login again even when the smart card was removed. (CR Q01068256)
  Also, it is now possible to configure the system to logout a user as soon as the card is removed from the card reader.
  CLI path: `/cfg/vpn #/server/http/certcard` command.
  BBI path: VPN Gateways>Gateway Setup>SSL>HTTP
- Macros in SMB and FTP link are now expanded in portal PDA mode.
- Macros in remote host settings are now expanded for the Port Forwarder applet.
- Fixed problem in terminal applets with Chinese characters in certificates. This problem has also been fixed in the other Portal applets (on the Portal's Advanced tab). (CR Q01066979)
- The Terminal/SSH applet on the Portal's Advanced tab failed to load when using certificate/key pairs containing the Chinese character set.
- Added support for expired passwords from Novell LDAP servers.
- Fixed problem with SSL to LDAP server which replies with large SSL records.
- Added support for disabling the SSL functionality (only) for a VPN. The `ena` and `dis` commands now only affect the SSL server, not IPsec.
  CLI path: `/cfg/vpn/server/ena` and `dis`
  (CR Q01091879)
- Fixed session cookie problem. Previously, if the cookie was stored in the cache of a remote NVG, the user received an internal error (bad xnet id) in the browser.
- Fixed problem with the vpnLicenseExhausted SNMP notification trap not being sent.

- Fixed problem with port forwarders disappearing. Previously, this could have the effect that the wrong user was logged out.
- Fixed problem with generic error when polling specific IDs via SNMP. Previously, SNMP GET requests did not work properly for all instrumentation functions.
(CR Q01095078)
- Fixed RADIUS authentication problems. A Vendor-Specific attribute containing the VPN ID has been added and is now always sent in the RADIUS authentication request.
- Fixed memory leak on IPsec session rekey/delete. Previously, a memory leak caused loss of approximately 1 kByte of memory on each IPsec session rekey and when an IPsec session was terminated. This could eventually lead to a restart or reboot of the system.
- Fixed problem with client certificate authentication displaying an error page.
(Q001104375) (Q01108295)
- Fixed problem with Tunnel Guard not working with Sun's JRE 1.5.
(Q01067435)

Browser-Based Management Interface (BBI)

- The maximum range for IKE and User tunnel profiles has been changed from 1023 to 64.
- Added missing option (`require`) for certificate verification level under SSL Offload>SSL>Verify Level. Previously, only the `none` and `optional` options were available. (CR Q01086752)

Software Installation and Upgrade Notice

SSL VPN Server Software

The SSL VPN server software is delivered in two different forms, as described below.

- `SSL-5.1.1-upgrade_complete.pkg`

  Using this package is the preferred method for upgrading an existing SSL VPN cluster, as the upgrade is propagated across the cluster and all current configuration is preserved.

  The upgrade procedure is described in "Performing Minor/Major Release Upgrades" in Chapter 4 in the *VPN Gateway User's Guide*.

- `SSL-5.1.1-boot.img`

  Using this image will reset the VPN Gateway to its factory default configuration. It must be used when an VPN Gateway with a different software installed is to be added to a cluster, to bring the additional device to the same software version as in the cluster before joining it to the cluster.

  The software reinstall procedure is described in "Reinstalling the Software" in Chapter 3 in the *VPN Gateway User's Guide*.

Server Software Download

The server software is available for download from Nortel's Customer Support Web site. To access the site, proceed as follows:

1. **Point your browser to: http://www.nortel.com.**

2. **Under Support and Training, select Software Downloads.**

3. **In the three-step Product Finder guide, select one of the following options:**

   VPN Gateway ▸ VPN Gateway 3050/3070 ▸ Software

   Alteon ▸ SSL Accelerator/SSL VPN ▸ Software

4. **Select the desired software release.**

5. **Downloading software requires that you enter the registered user name and password previously assigned to you by Nortel Customer Support.**

   If you are not a registered user at Nortel, click on **Register** on the left-hand column of the Nortel's Customer Support Web site, and follow the 5-step registration process.

Nortel SSL VPN Client Software

New versions of the manually installable SSL VPN transparent client software can be downloaded from Nortel’s Customer Support Web site. In the three-step Product Finder guide, select **VPN Gateway ▸ VPN Gateway 3050/3070 ▸ Software.**

The installable SSL VPN client comes in two versions (for limitations, see page 13):

- Version 1.1.0.4: Compatible with Windows 98, ME, NT (with IE 5 or later) 2000 and XP.
- Version 1.5.0.9: Compatible with Windows 2000 and XP.

Nortel IPsec VPN Client Software (formerly Contivity)

The IPsec VPN client software can be downloaded from Nortel’s Customer Support Web site. In the three-step Product Finder guide, select **Contivity ▸ VPN Client ▸ Software.**

Disk Repartitioning Required for Version 5.x on Some Systems

This applies to the following systems:

- ASA 310, ASA 310 FIPS, ASA 410, delivered with a software version prior to 4.0 pre-installed
- AAS 2424-SSL delivered with a software version prior to 5.0 pre-installed.

On these systems, the existing disk partitioning does not allow for a 5.x version to be installed simultaneously with version 4.2 or later. I.e. it isn't possible to do a standard upgrade from 4.2 to 5.x, or from one version of 5.x to another. Upgrade from versions earlier than 4.2 to 5.x, and software reinstall using a 5.x version, is still possible.

Hence, the following applies regarding standard upgrade to version 5.x from versions prior to 5.0 for clusters that include systems of the above type:

Current version	Procedure
4.1.x or earlier	Upgrade to 5.x, and repartition before subsequent upgrade
4.2.x before 4.2.1.11	Upgrade to 4.2.1.11 or later 4.x, repartition, and then upgrade to 5.x.
4.2.1.11 or later 4.x	Repartition before upgrade to 5.x.

When 5.x is installed, the `/boot/software/download` command will give an error if one or more systems of the above type are running in the cluster, listing the hosts that need disk repartitioning.

To support the repartitioning procedure, the following commands are present as of version 4.2.1.11:

- `/boot/software/repartcheck`
  Checks for and reports hosts in the cluster that need repartitioning.
- `/boot/repartition`
  Initiates repartitioning for the local host.
- `/cfg/sys/cluster/host #/repartition` (in version 4.2)
  `/cfg/sys/host #/repartition` (in version 5.x)
  Initiates repartitioning for the given host (which must be running).

These commands are “hidden”, i.e. not shown in the menu or considered for auto-completion via <TAB>, since they shouldn't be used in normal operation. During the repartition, which includes two automatic reboots, the host will effectively be out of service.

The time required for the repartition is approximately:

- 4-5 minutes for ASA
- 7-10 minutes for AAS 2424-SSL

NOTE – It is vitally important to avoid power cycle, reset, or any other manually initiated reboot of the host while the repartition procedure is running - this may lead to a totally non-functional system.

NOTE – On the AAS 2424-SSL, after repartition is completed, it will not be possible to downgrade to software versions prior to 4.2.1.8, even via software reinstall.

Upgrading from Versions Earlier than 2.0.11.15

If you are currently running a software version earlier than 2.0.11.15, upgrade to version 2.0.11.15 (or a later 2.0.11.x version) prior to upgrading to version 3.x or later. The “intermediate” upgrade to version 2.0.11.15 is necessary in order to maintain your current configuration, and to provide reliable fallback in case the upgrade should fail.

Downgrading to Versions Prior to 5.0

SSL VPN clusters running software version 5.x or later cannot be downgraded to software version 4.x or earlier and still retain the configuration. To downgrade such a cluster to a version lower than 5.0, a complete software reinstall using the boot.img must be performed, followed by manual reconfiguration of the cluster. This is due to changes in the internal database format.

Supported Hardware Platforms

The SSL VPN 5.1 server software version is currently supported on the following hardware platforms:

- Nortel VPN Gateway 3050
- Nortel VPN Gateway 3070
- Alteon SSL Accelerator 310 (IPsec not supported)
- Alteon SSL Accelerator 410 (IPsec not supported)
- Alteon SSL Accelerator 310-FIPS (IPsec not supported)

TFTP Server Support

- The following TFTP server (for Microsoft Windows 95/NT) has been tested and verified to handle the upgrade process correctly:
    - TFTPd32 software (use any search engine to search for "`tftpd32`")
- The following TFTP server software are *not* supported when upgrading the SSL VPN software:
    - Cisco TFTP server software (for Microsoft Windows 95/98/NT)
    - 3Com TFTP server software (for MS-DOS 5.x or higher)

Known Limitations

Browser Requirements

Basic Portal Access (no applets)

When using the NVG software for basic portal access, i.e. when not using the applets (see below), the following browsers are recommended:

- Internet Explorer 5 or later
- Mozilla 1.1 or later
- Netscape 4 or later
- Firefox

Applet Support

To support the Telnet/SSH Access, HTTP Proxy, Port forwarder and Citrix applets, the following browser and Java combinations are recommended:

- Windows:
  Internet Explorer 5 or later with Microsoft’s JVM 4 or later Sun’s JRE 1.4.2 or later
  Mozilla 1.5 or later with Sun’s JRE 1.4.2 or later
  Firefox with Microsoft’s JVM 4 or later or Sun’s JRE 1.4.2 or later
- Unix/Linux:
  Mozilla 1.5 or later with Sun’s JRE 1.4.2 or later
  Firefox with Sun’s JRE 1.4.2 or later

Tunnel Guard Applet Support

To support the Tunnel Guard SSL applet (used for checking the client machine), Internet Explorer 5.5 or later is recommended.

The following browsers support the Tunnel Guard management applet (used for configuring SRS rules):

Windows:
Internet Explorer 5.5 or later
Netscape Navigator 7.1 or later
Mozilla 1.5 or later
Firefox 1.0
Java 1.4.2 or later is required

BBI Support

Configuration via the Browser-Based Management Interface (BBI) is supported when the following browsers are used:

- Windows:
  Internet Explorer 5.5 or later
  Netscape Navigator 7.1 or later
  Mozilla 1.5 or later
  Firefox 1.0
- Unix/Linux:
  Netscape Navigator 7.1 or later
  Mozilla 1.5 or later

Net Direct Agent

- The Net Direct agent is only supported on Internet Explorer running on Windows 2000 and Windows XP.
- To be able to install and run the Net Direct agent, the remote user should have administrative rights on the client PC.
- Net Direct only works with port 443.

Tunnel Guard

Version TG_1.1.2.0_001 of the *installed* Tunnel Guard application is the minimum requirement for use with the Nortel IPsec VPN client (formerly the Contivity VPN client).

Nortel IPsec VPN Client (formerly Contivity)

- For IPsec termination on the VPN Gateway, the following Nortel IPsec VPN client versions have been tested: 4.15, 4.86, 4.91, 5.01 and 5.11.
- For use with the Portal’s Full Access feature, version 4.91 and later are supported.

SSL VPN Client

The installable SSL VPN client comes in two versions:

- Version 1.1.0.4: Compatible with Windows 98, NT (with IE 5 or later), ME and XP. This client does not support UDP.
- Version 1.5.0.9: Compatible with Windows 2000 and XP. This client supports UDP as well as TCP. Native Microsoft Outlook is not supported because not fully qualified domain names cannot be resolved.

License

The license is not part of the configuration and will not be included when exporting the configuration using the `/cfg/ptcfg` command. If a configuration is deleted, the license will be deleted as well.

Portal

- Sun's JRE earlier than 1.4 cannot download any applets from the VPN Gateway if the device has been setup to use a key length above 4096. This is supported in the native Microsoft JVM and may be supported in Sun's JRE 1.5 (yet unclear).
- Proxy chaining (option to specify an intermediate HTTP Proxy host and port, e.g. for the Portal's Telnet/SSH and Custom Port forwarder features) is only supported if SSL is enabled on the portal server.
- Proxy chaining is not supported for the Outlook Port forwarder feature.
- Microsoft Outlook 2003 is not supported when using the Outlook Port forwarder in combination with Exchange 2003.
- Running the Outlook Port forwarder on a Windows 2000 client requires installing the latest service pack for the operating system.
- Applications using *dynamic* UDP port number allocation (e.g. NetMeeting, FTP and all streaming media) are not supported by the Port forwarder feature. Applications using *static* port number allocation (e.g. DNS, SNMP) are supported.
- When specifying a URL without a path for an iauto (automatic login) link, e.g. http://www.example.com, enter the URL as `http://www.example.com/`. This will ensure that the root path is implied in the link. Iauto links are created using the `/cfg/vpn #/linkset #/link #/iauto` command.

- When an iauto link should be used for login to web servers using two-tier basic authentication with domain (i.e. one field for domain\user and one for password), the `/cfg /vpn #/linkset #/link #/iauto/mode` command must be set to `add_domain`.
- Creating a Port forwarder link for mapping a network drive is not supported on Windows 98 and XP clients.
- The features available on the Portal's Advanced tab (i.e. Telnet/SSH access, HTTP Proxy and Port forwarder) are supported only with SSL v3 and cipher type RC4-MD5.
- The features available on the Portal's Advanced tab are not supported for the TLS protocol.
- To create a Port forwarder link for mapping a network drive – and the link is to be used on a Windows 2003 server acting as client – port 445 has to be used instead of the suggested port 139. On the Windows 2003 server, port 445 should be disabled by following these steps:
    - Click Start, select Run and enter `regedit`. The registry editor is started.
    - Locate and select the following key: `HKLM\System\CurrentControlSet\Services\NetBT\Parameters`.
    - On the right panel, double-click the `TransportBindName` entry.
    - In the **Edit string** dialog, delete the displayed value. No value should be specified.
    - Click OK, exit the registry editor and restart the computer.
- Some SSH versions may not be supported when using the SSH feature on the Portal's Advanced tab, e.g. Alteon 184 SSH-1.5-1.2.27.
- Some of Microsoft's Telnet server versions may not be supported when using the Telnet feature on the Portal's Advanced tab.

Known Issues

This section lists known issues with software version 5.1.

Portal

The default.htm page presented by web-based WTS (Windows Terminal Server) is not supported through the NVG rewrite engine. This will be fixed in a coming patch release. (Q00867149)

SSL VPN Client

For the Full Access feature to work, the fully qualified domain name (FQDN) of the VPN *must* be specified as the server alias in the SSL VPN client (Servers tab>Add>Alias field). (Q01043664)