Nortel VPN Gateway 5.1.3

Release Notes

part number: 216372-E, June 2005

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

Release Notes

These Release Notes provide the latest information regarding your Nortel VPN Gateway (NVG) with version 5.1.3 software. This supplement lists the new features and modifies some information found in the complete documentation:

- *VPN Gateway 5.1 User's Guide*
  (part number 216368-C, March 2005)
- *VPN Gateway 5.1 Command Reference*
  (part number 216369-C, March 2005)
- *VPN Gateway 5.1 Application Guide for SSL Acceleration*
  (part number 216370-C, March 2005)
- *VPN Gateway 5.1 CLI Application Guide for VPN*
  (part number 216371-C, March 2005)
- *VPN Gateway 5.1 BBI Application Guide for VPN*
  (part number 217239-B, March 2005)
- *VPN Gateway 5.1 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 5.1.3

This section lists software features and enhancements added since version 5.1.1. Note that these features are not documented in the 5.1 manuals listed on page 3.

General

Compression of HTTP Traffic

Added support for compressing HTTP traffic to clients. When compression is enabled for the portal server of a VPN, scripts and HTML are compressed to enable faster HTTP data transfer to the clients. When compression is enabled for a virtual SSL server, all HTTP data is compressed. Note that the encryption throughput on the NVG may be reduced, since the CPU will also be engaged in data compression.

CLI path: `/cfg/vpn #/server/http/compress` and `/cfg/ssl/server #/http/compress`
BBI path: VPN Gateways>Gateway Setup>SSL>HTTP>General (Compress HTTP Data) and SSL Offload>Servers>Types>HTTP>General (Compress HTTP Data)

Idle Users

Added support for listing SSL VPN users whose sessions have been idle longer than a specified time.

Examples of argument usage in the CLI:

`>> Information# idle 30`	Lists all SSL users who have been idle more than 30 seconds.
`>> Information# idle 5m 2`	Lists all SSL users currently logged in to VPN 2 who have been idle more than 5 minutes.
`>> Information# idle 1h 2 j*`	Lists all SSL users currently logged in to VPN 2, whose user name begins with the letter "`j`", who have been idle more than 1 hour.
`>> Information# idle 1h 2 joe`	Lists all SSL users currently logged in to VPN 2, whose user name is exactly "`joe`", who have been idle more than 1 hour.

The information includes VPN ID, user name, login time, last time active, source IP address and access method.

CLI path: `/info/idleusers`
BBI path: Administration>Monitor>Idle Users

Other General Enhancements

- Added question prompting for Subject Alternative Name (optional) when generating certificates and certificate signing requests.
  CLI path: `/cfg/cert #/request`, `/cfg/cert #/gensigned` and `/cfg/cert #/test`
  BBI path: Certificates>Generate>Request, Certificates>Generate>Signed Certificate and Certificates>Generate>Test Certificate

- Improved performance for connection pooling. A single connection to the backend server should now be able to service a large number of concurrent client connections. Now you can configure a short pool timeout (1 second) without forcing the client to reconnect frequently.
  CLI path: `/cfg/ssl/server #/adv/pool`
  BBI path: SSL Offload>Servers>Advanced>Pooling

- Added smb and ftp to the Trace feature. Logs information related to Portal SMB (Windows file share) and FTP sessions for troubleshooting purposes.
  CLI path: `/maint/starttrace`
  BBI path: Diagnostics>Maintenance>Trace

Portal

FTP Proxy

FTP Proxy is added as a new Portal link type and as a feature on the Portal's Advanced tab. The FTP Proxy feature lets the user run a native FTP client towards a remote FTP server via a secure SSL connection. The feature is similar to the existing port forwarder features.

To configure an FTP Proxy link, proceed as follows:

1. **When configuring a new Portal link (in the CLI or BBI), select FTP Proxy as the link type.**
2. **As the local host IP address, configure an IP address in the 127.x.y.z range, e.g. 127.0.0.1.**
3. **As the local port number, enter 21.**
4. **Specify the IP address or domain name of the remote FTP server.**
5. **Specify the remote FTP port number, i.e. 21.**

   An optional step is to specify the path to the remote user's native FTP client. This will start the FTP client when the user clicks the link. If an application argument is also specified, the FTP client can be told to automatically connect to the local host IP address (as specified in step 2). The default application path and argument starts an FTP session in the command window and lets it connect to 127.0.0.1. Note that each FTP client has its own sets of arguments.

   If no application path/argument is specified, the remote user should click the link on the Portal's Home tab to start the FTP Proxy, start his native FTP client and connect to the local host IP address specified in step 2.

   If no FTP Proxy link has been configured by the administrator, the remote user can set up an FTP Proxy session manually by selecting FTP Proxy on the Portal's Advanced tab.

   CLI path: `/cfg/vpn #/linkset #/link #/ftpproxy`
   BBI path: VPN Gateways>Portal Linksets>Links>FTP Proxy

Net Direct on Full Access Tab

Support has been added for the Net Direct client on the Portal's Full Access tab. If neither Nortel's IPsec VPN client nor Nortel's SSL VPN client is found on the remote user's machine, the NVG tries to launch the Net Direct client (if enabled). Read more about the Full Access tab in the "Transparent Mode" chapter in the *CLI/BBI Application Guides*.

FTP and SMB

Backend Conversion

The Backend Conversion feature is used to handle conversion of character sets for specified FTP file servers or SMB (Windows file share) file servers without Unicode capability.

Example: An FTP file server uses the ISO-8859-1 character set. The remote user browses to the Portal, connects to the FTP server on the Files tab and tries to display the file list. The VPN's existing character set is SHIFT_JIS (used for Japanese). This mismatch between character sets may cause characters in file names to not display correctly. To solve this, configure the NVG to convert the ISO-8859-1 character set to the existing character set for the VPN (i.e. SHIFT_JIS) before sending the file list to the browser.

Proceed as follows:

1. **Specify whether to make the conversion for an FTP file server or an SMB (Windows file share) file server.**
2. **Specify the backend file server's host name or IP address.**
3. **Optionally, specify the desired shared network folder (only for SMB). Lets you limit conversion to a specific file share folder.**
4. **Specify the character set to be converted, e.g. ISO-8859-1.**

   Character set conversion is not required for SMB servers running on Windows 2000 or XP, since they support Unicode natively.

   CLI path: `/cfg/vpn #/portal/lang/beconv`
   BBI path: VPN Gateways>Portal Display>Language>Backend Conversion

Authentication

Common Authentication/Accounting

Added support for common authentication/accounting servers (shared by several VPNs) in Secure Service Partitioning configurations where the ISP wishes to use the same set of authentication/accounting servers for several end-customers. When the feature(s) are enabled, the default routing will be used for authentication/accounting services, i.e. requests will not be routed through the bound backend interface to authentication/accounting servers on the end-customer's private network.

The features are only available when a VPN is bound to an interface (configured with the `/cfg/vpn #/adv/interface` command in the CLI or under VPN Gateways>Gateway Setup>Interface (Interface) in the BBI).

CLI path: `/cfg/vpn #/adv/cauth` and `/cfg/vpn #/adv/cradacct`
BBI path: VPN Gateways>Gateway Setup>Interface (Use Common Authentication/Accounting Servers)

VPN ID Attribute

Added support for setting Vendor Id and Vendor Type for the VPN ID attribute in RADIUS access requests. When a user authenticates to a specific VPN (as configured on the NVG), the NVG sends the VPN ID to the RADIUS server. The RADIUS server in its turn can make use of the VPN ID to return user information (e.g. from a VPN-specific user database).

CLI path: `/cfg/vpn #/aaa/auth #/radius/vpnid` and `/cfg/vpn #/aaa/auth #/radius/vpntype`
BBI path: VPN Gateways>Authentication>Auth Servers (Vendor Id for VPN Id) and VPN Gateways>Authentication>Auth Servers (Vendor Type for VPN Id)

Net Direct

Split Tunneling Modes

Added support for four different split tunnel modes. Split tunneling allows network traffic to travel either through a tunnel to the VPN Gateway or directly to the Internet.

The following modes are supported:

- `disabled`. Tunnels all network traffic through the Net Direct client to the VPN Gateway.
- `enabled`. Tunnels traffic to *specified networks* to the VPN Gateway. All other network traffic goes through the computer's normal network interface.
- `enabled_inverse`. Does *not* tunnel traffic to specified networks, i.e. traffic goes through the computer's normal network interface. All other network traffic is tunneled through the Net Direct client to the VPN Gateway.
- `enabled_inverse_local`. Does *not* tunnel traffic to directly connected networks or to specified networks. This will e.g. allow the remote user to print locally, even while tunneled to the VPN Gateway. All other network traffic is tunneled through the Net Direct client to the VPN Gateway.

CLI path: `/cfg/vpn #/sslclient/splittun`
BBI path: VPN Gateways>VPN Client>Split Networks

Other Net Direct Enhancements

- Added support for MSS clamping which addresses the problem of packet fragmentation.
  CLI path: `/cfg/vpn #/sslclient/clampmss`
- Added support for reconnection. If the connection is lost, Net Direct reconnects with the same IP address if the Portal session is still active.

Fixes

This section lists fixes added since version 5.1.1.

General

- Fixed problem when configuring many VLAN-tagged interfaces. Previously, when more than approx. 140 VLAN-tagged interfaces were configured, deletion of interfaces did not work correctly.
  (CR Q01063883)
- Fixed problem with NTP queries. Previously, querying the NTP time-sync service over the network could reveal version details about the running operating system.
- Fixed supervision of NTP. Previously, setting the time manually while external NTP servers were in use, the NTP synchronization could stop working. A warning is now given when the time is set manually while NTP servers are configured.
  (CR Q01031542)
- For SNMP, sysName and sysLocation have been moved from cluster level to host level.
  CLI path: `/cfg/sys/host #`
  BBI path: Cluster>Host(s)>System
  (CR Q01040501)
- Fixed problem with incomplete SNMP responses.
  (CR Q01049920)
- Fixed problem with the private interface not being visible via SNMP ipAddrTable in two-armed configurations.
  (CR Q01109853)
- Fixed problem with Java script rewrite. The argument to document.createElement() was not properly rewritten.
- Fixed problem with allowing an invalid IP address of 127.0.0.1 as a real IP address. It is now validated that the backend server IP address (`/cfg/ssl/server #/rip`) is a valid IP address. Loop-back, multicast and reserved IP addresses are not allowed.
  (CR Q01081916)
- Fixed problem with finding end of script (</script>). Previously, when the script contained regular expressions with quote characters, the system sometimes failed to find the right </script> tag.
- Fixed problem with large cookies. Previously, large cookies (in total more than 4K) were not handled properly which caused internal web pages to not display properly.

- Fixed problem with rewrite of addImport. Previously, the first argument of the addImport() method was not properly rewritten. addImport is a stylesheet object method in the DOM object in Internet Explorer.
- Fixed problem with script rewriting. Previously, empty src URLs in Java script, VB script and HTML refs were incorrectly rewritten with xct1, xct2 and xct3 tags.
- Fixed problem with apply time when changing network definitions in large configurations. Previously, any change to a network definition caused a long apply time and new Java applications (port forwarders or terminal applets) would not start for several minutes. This blocking time has now been reduced to a few seconds.
(CR Q01135096)
- Fixed problem with IP pool crashing when a VPN is deleted.
(CR Q01122121)
- Fixed problem with the VPN Gateway 3050 hanging while running script with an “apply” operation after each configuration.
(CR Q01134544)
- The system’s internal validation of IP addresses (e.g. NTP or DNS) in the CLI and BBI now allows specifying 0 for the last octet. Previously, validation was too strict.
- Fixed problem when importing configurations with users in the local database where the user passwords were very long.
(CR Q0113028)
- Fixed problem with the VPN Gateway host name being too long to fit as a NetBIOS host name. The host name will now be truncated to 15 characters if this should be needed.
- Fixed problem with users not being logged out due to inactivity. Previously, in clusters consisting of several VPN Gateways, the inactivity auto logout did not trigger properly when a user was load balanced to another NVG in the cluster.
- Fixed problem with the `license_expire_soon` alarm. The alarm was not cleared when a new time-limited license was loaded.
- Fixed problem with port configuration when upgrading from version 3.1. Previously, in clusters consisting of several VPN Gateways, it was not possible to reconfigure the ports on VPN Gateways that were slaves.
- Fixed problem with the CLI being accessible after having performed a `/boot/delete` and the delete operation has not yet been completed. Now, an administrator cannot login to the CLI until the delete operation has been completed.
(CR Q01150394)

- Fixed security bug in yaws. Previously, if a null byte was appended to the file name of a yaws script (.yaws), the yaws web server returned a page containing the source code of the according script.
- Fixed problem with generation of Via header. Previously, if a HTTP client sent a Host header that was longer than approximately 4060 bytes, the generation of the Via header for the response could cause random data to be sent to the client, or possibly a crash of the SSL proxy. Now the Via header is omitted if its length would exceed the 4096 byte maximum recommended by the HTTP 1.1 RFC.
- Fixed problem with crashing traffic subsystem. Previously, the traffic subsystem could crash if a bad DNS server (e.g. a non-existing DNS IP address) was configured in the system.
- Fixed problem with internal error 46a. Previously, internal error 46a was sometimes generated due to a bug in the session timeout code.
- The event “License due to expire in 7 days” did not produce alarms, traps and messages. This has now been fixed.
  (CR Q01153316)

IPsec

- Fixed IPsec statistics. The total encrypted/decrypted kBytes counters in the IPsec statistics previously reported the numbers for the last minute. Now the accumulated numbers since the last clearing of the statistics are shown.
  (CR Q01034561)
- Fixed switch load balancing with IPsec. Previously, it was not possible to run IPsec with a VPN that had standalone mode set to off, which is the required setting when using a load balancing switch.
- Fixed problem with SecurID “Next Token Mode” failure. Previously, when an IPsec user authenticated with a SecurID card and provided incorrect credentials, the SecurID card entered Next Token Mode and could not get out.
  (CR Q01115810)
- Fixed problem with IPsec logout. Previously, when a user logged out from an IPsec session that had lasted longer than the time specified with the CLI command `/cfg/vpn #/aaa/ttl` or in the BBI under VPN Gateways>Gateway Setup>Session (Login Session Time-to-Live), the user was not logged out of the AAA subsystem.
- Fixed problem with IPsec crashing when deleting a VPN that has active user tunnels.
  (CR Q01140647)

Certificates

- Fixed automatic certificate CRL handling to use bound interfaces in a Secure Service Partitioning configuration. Both DNS lookups and server connections are done using the correct interface and DNS settings per gateway/VPN.
- Fixed problem with importing a server certificate into a certificate location without the correct private key.
  (CR Q01095676-01)
- Fixed problem with certificates requiring all fields to be filled in. Now only Common Name or E-mail Address needs to be filled in.
  (CR Q01093452-01)
- Fixed problem with inconsistent CLI output for certificates. Previously, whenever `cert` <TAB> was entered, only the numbers of existing certificates were printed. Now, both the certificate numbers and names will be printed.
  (CR Q01093359)

SMB and FTP

- Long SMB (Windows file share) share names (>12 characters) are now supported.
  (CR Q00911219) (CR Q00911472)
- The SMB shares list on the Portal's Files tab can now show a large number of shares. Previously, no more than 76 shares could be listed.
- Fixed problem with the SMB protocol when talking to a NetWare server.
- Fixed problem with FTP directory deletion.
  (CR Q01045228)
- The FTP client now always tries to use passive mode. If the server does not support passive mode, active mode is used instead. Applies to CLI and Portal FTP.

Portal

- Internet Explorer cache wiper now closes the history warning dialog automatically.
  (CR Q00876591)
- The HTTP Proxy applet (available as a Portal link and as a feature on the Portal's Advanced tab) can now automatically set proxy settings in Internet Explorer for dial-up connections as well.

- Fixed link type problem when upgrading from 4.x. Previously, all links showed up as href type. Now the correct link type will be set for the following link types (BBI denomination within parenthesis where needed): SMB, FTP, proxy (HTTP Proxy), iauto (Internal Auto Login URL), Terminal, internal (Internal Website) and external (External Website). Custom and Outlook port forwarders are still treated as being of the href type. If such a link has to be modified it has to be recreated by the administrator.
- Fixed problem with the VPN Gateway's traffic subsystem corrupting certain Set-Cookie headers from the server. Previously, this caused the browser to ignore the Set-Cookie and consequently not send the cookie at the next request.
(CR Q01095268)
- Fixed problem with RSA/RADIUS authentication not working together with second authentication (LDAP) in Portal PDA mode.
(CR Q01109550)
- The output from the `dump` command for links can now be pasted back without changing the hrefs, i.e. the internal href format is now parsed and created properly.
(CR Q01145298) and (CR Q01145383)
- LDAP or RADIUS macros (variables) for server name were not expanded in Portal link specifications when the link was configured via the CLI wizard. This has now been fixed.
(CR Q01104870)

Authentication

- NTLM authentication now works with Microsoft 2003 server.
(CR Q00907091) (CR Q01050164)
- Fixed problem with LDAP macros not working when LDAP is configured as secondary authentication method or group authentication method.
(CR Q01105213)
- Previously, usage of RADIUS macros could cause RADIUS authentication to fail. This has now been fixed.
(CR Q01140539)
- Fixed problem with missing user ID (User="") in syslog on SiteMinder cookie login.
- Fixed problem with looping backend authentication. Previously, the backend authentication would sometimes loop, trying to send the same credentials to the backend server instead of querying the user for a new password.
- Fixed broken NTLM authentication when logging in with the wrong credentials. Also fixed problem with uppercase/lowercase characters in group name.
(CR Q01113227)

- Fixed problem when trying to retrieve LDAP group information when the LDAP server is unreachable.
- Fixed problem with joining a new VPN Gateway to the cluster when RADIUS authentication is used and the RADIUS servers are not reachable.

Tunnel Guard

- Maximum Tunnel Guard recheck interval is now 24h.
(CR Q01043045)
- Tunnel Guard previously showed the (restricted) Portal page instead of the login page when teardown mode was selected. This has now been fixed. If the user clicks the Back button before the Tunnel Guard check is completed, the login page is displayed.
(CR Q01043045)

Net Direct

- Feature added to warn and stop installation if the Windows built-in feature RRAS (Routing and Remote Access Service) is active.
- Fixed problem with auto-closing the Windows digital signature warning dialog. This feature now works with all character sets.
- Net Direct now works with PPPoE (PPP over Ethernet).
(CR Q01059649)
- Previously, connectivity via Net Direct could be lost when the default gateway in Windows was changed. This has now been fixed.
- Previously, problems could occur when running Net Direct via a proxy server if the proxy server was configured as a fully qualified name (FQDN) instead of an IP address in Internet Explorer. This has now been fixed.
- Sending encrypted UDP packets to the VPN Gateway (UDP optimization) via the preconfigured UDP ports on the NVG now works properly.
- Changed the name of the Net Direct cleaner utility to a more user-friendly name, as anti-spyware is showing an alert while the utility is added in the registry.

Secure Service Partitioning

Previously, routing of backend traffic for Secure Service Partitioning (SSP) did not work for the 10th interface and above. This has now been fixed.

Browser-Based Management Interface

Fixed problem with unintentionally typed spaces before or after group names in the BBI. Spaces (if any) are now automatically trimmed.
(CR Q01082344)

Software Installation and Upgrade Notice

SSL VPN Server Software

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

- `SSL-5.1.3-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-5.1.3-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 23):

- 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 5.1.3 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
- Opera

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.

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` CLI command or Operation>Configuration (Export Cluster Configuration) in the BBI. 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 in the CLI and under VPN Gateways>Portal Linksets>Links (Internal Auto Login URL) in the BBI.
- 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`. In the BBI, go to VPN Gateways>Portal Linksets>Links>Iauto>Auto Configuration. Under Internal Auto Configuration, in the Mode List box, select 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.

- To create a WTS port forwarder link that works on Windows XP systems that have not yet been upgraded to Service Pack 2, configure the port forwarder to listen on 127.0.0.2 instead of 127.0.0.1 (localhost). Then configure the Remote Desktop client to connect to 127.0.0.2. With the Windows XP SP2 version of the Remote Desktop client, it is possible to connect to 127.0.0.1 (localhost) as long as the port being used is other than the default (3389). Note that connections through 127.0.0.2 do not work on Windows XP SP2.

General

A maximum of 32,000 sessions is allowed on the VPN Gateway 3070 with 2 GB RAM.

Known Issues

This section lists known issues with software version 5.1.3.

- 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)
- 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)
- The Portal does not function with >250 VPNs when each VPN is bound to an interface. This will be fixed in a coming patch release.
(Q01161146)