Nortel VPN Gateway 5.1.11

Release Notes

part number: 216372-L, November 2006

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 5.1.11 software. This supplement lists the new features/fixes 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 Support>Technical Documentation.**
3. **In the first step of the three-step Product Finder guide, choose 'Select from Product Families' in the list box.**
4. **Then select the following:**

   VPN Gateway ▸ VPN Gateway 3050/3070 ▸ Documentation
5. **Click Go and select the desired document.**

New Features/Enhancements

There are no new features introduced in VPN Gateway 5.1.11.

An enhancement has been added to SSL-VPN BBI where it is now possible to add the SMB link path when setting up the SMB link in BBI or CLI. (CR Q01329751)

Fixes

This section lists fixes added to version 5.1.11.

General

- Fixed problem with SSL-VPN TunnelGuard not working when starting from a 5.1.9 boot image (boot.img) or downgrading to 5.1.7. (CR Q01438432)
- Fixed problem with SSL-VPN NetStorage facility when downloading one or multiple files in a batch. When accessed through the portal, this function did nothing.. (CR Q01395856)
- Fixed problem with OpenSSL RSA Signature forgery as detailed in CVE-2006-4339 where if an RSA key with exponent 3 is used it is possible to forge a PKCS #1 v1.5 signature signed by that key. (CR Q01456517)
- Fixed problem with SSL-VPN NetDirect tunnel where a client request would remain unencrypted and not go through NetDirect but was routed to a proxy server. (CR Q01150899)
- Fixed problem where SSL-VPN NetDirect would fail when a client used a proxy which did private DNS resolution. NetDirect would fail as it attempted to resolve through the client's DNS server rather than through the proxy server. (CR Q01320867)
- Fixed problem where SSL-VPN failed to properly rewrite some intranet links, resulting in erroneous displays on SSL User Web page. (CR Q01357356)
- Fixed problem where SSL-VPN NetDirect didn't launch when using dial-up access if Internet Explorer LAN proxy was set. (CR Q01410053)
- Fixed problem where SSL-VPN "iauto" would fail when using LDAP to return multiple group names with lengths exceeding 600 characters. (CR Q01413357)
- Fixed problem with SSL-VPN where Form Submit did not properly redirect when the submit button was clicked. (CR Q01415225)
- Fixed problem with SSL-VPN where "iauto" link was performing a VPN session logout due to AAA message size limit of 1024 bytes (CR Q01420024)
- Fixed problem with SSL-VPN where no connection was allowed through RDP from LAN PC to a NetDirect connected PC running Windows XP Pro SP2. (CR Q01314666)
- Fixed problem with SNMP MIB "walk" with 32 bit data collection in the 3070 being handled as 31 bit causing a "general failure occurred in Agent" message to be displayed. (CR Q01409525)

Portal

- Fixed problem with Japanese language not being activated on the Portal page after a "/cfg/gtcfg" function call. (CR Q00951251)
- Fixed problem with SSL-VPN Portal page when uploading a file with Japanese characters in the file name that would cause an error message to be displayed. (CR Q01343587)
- Fixed problem with SSL-VPN Portal where NetDirect session remained open and the Net-Direct user could not be removed when the Internet Explorer or Fire Fox brower was abruptly closed, by clicking the X on the window.(CR Q01395015)

Certificates

- Fixed problem with Port forwarder failing with errors when using an SSL chain certificate. All certificates in the chain are now checked against the client certificate for a possible match. (CR Q01128789)

BBI

- Fixed problem with SSL-VPN BBI where Help information for the HTTP Proxy Link "Exception" was incorrect. (CR Q01420383)
- Created an enhancement with SSL-VPN BBI where it is now possible to add the SMB link path when setting up the SMB link in BBI or CLI. (CR Q01329751)

Software Installation and Upgrade Notice

VPN Gateway Server Software

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

- `SSL-5.1.11-upgrade_complete.pkg`

  Using this package is the preferred method for upgrading an existing NVG 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-5.1.11-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 first step of the three-step Product Finder guide, choose 'Select from Product Families' in the list box.**
4. **Then select one of the following:**

   VPN Gateway ▸ VPN Gateway 3050/3070 ▸ Software

5. **Select the desired software release.**

   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

The manually installable SSL VPN transparent client software is available on request. Contact Nortel Support.

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

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

Nortel IPsec VPN Client (formerly Contivity VPN Client)

The IPsec VPN client 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 down-grade to software versions prior to 4.2.1.8, even via software reinstall.

NOTE – When doing the repartition after an upgrade, the new SW version must be "permanent" (see Chapter 4 of the User's Guide) before the repartitioning is started. If the repartioning is started while the new SW version is "current", the system will be non-functional after repartitioning, requiring a complete SW reinstall using the boot.img.

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 VPN Gateway 5.1.11 server software version is currently supported on the following hardware platforms:

- Nortel VPN Gateway 3050
- Nortel VPN Gateway 3070
- Nortel SSL Accelerator 310 (IPsec not supported)
- Nortel SSL Accelerator 410 (IPsec not supported)
- Nortel SSL Accelerator 310-FIPS (IPsec not supported)
- Nortel Application Switch 2424-SSL
- Nortel SSL VPN Module 1000

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, FTP 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 Client

- The Net Direct client 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 administrator 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 the Contivity VPN Client)

- 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.

Nortel SSL VPN Client

The installable SSL VPN client comes in two versions:

- Version 1.1.0.4 (LSP client): Compatible with Windows 98, ME, NT (with IE 5 or later), and XP. This client does not support UDP.
- Version 1.5.0.9 (TDI client): 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, FTP Proxy, 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 5.1.11.

- 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). (CR Q01043664)
- SSL-VPN “keep alives” causes traffic to fail when originating from IIS 6. (CR Q01399305)
- SSL-VPN NetDirect does not go through a proxy server when reconnecting after a disconnect. (CR Q01411163)