NORTEL NETWORKS™

VPN Gateway 5.0.3

Release Notes

part number: 216372-C, February 2005

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

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

Release Notes

These Release Notes provide the latest information regarding your VPN Gateway device with version 5.0.3 software.

NOTE – The 5.0.3 Release Notes document is almost identical to the 5.0.1 Release Notes. The main difference is that the limitation regarding IPsec functionality has been removed.

The Release Notes document lists the new features and modifies some information found in the complete documentation:

- *VPN Gateway User's Guide*
  (part number 216368-B, February 2005)
- *VPN Gateway Command Reference*
  (part number 216369-B, February 2005)
- *VPN Gateway Application Guide for SSL Acceleration*
  (part number 216370-B, February 2005)
- *VPN Gateway CLI Application Guide for VPN*
  (part number 216371-B, February 2005)
- *VPN Gateway BBI Application Guide for VPN*
  (part number 217239-A, February 2005)
- *VPN Gateway VPN Administrator's Guide*
  (part number 217238-A, February 2005)
- *VPN Gateway 3050 Hardware Installation Guide*
  (part number 216213-A, December 2003)
- *Configuring TunnelGuard 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 ▸ Documentation

   Contivity ▸ VPN TunnelGuard ▸ Documentation
4. **Select the desired document.**

New Features/Enhancements in Software Version 5.0.3

This section lists software features and enhancements added since version 4.2.1. Where applicable, a reference to where the new feature can be found is also included – both as a Command Line Interface (CLI) path or as directions to the proper web form in the Browser-Based Management Interface (BBI).

General

- The CLI has been restructured to make configuration easier. Commands related to SSL Acceleration are found under `/cfg/ssl` whereas commands used for pure VPN deployment are located under `/cfg/vpn`. The term *VPN* is now used instead of *Xnet domain*.
- Support added for access via IPsec. Users with the Contivity VPN client installed can now connect to the VPN Gateway device via a secure IPsec connection. See the "Transparent Mode" chapter in the *CLI/BBI Application Guide for VPN*.
- Secure Service Partitioning. New feature aimed at Internet Service Providers (ISPs), enabling VPN hosting of multiple customers. See the "Secure Service Partitioning" chapter in the *CLI/BBI Application Guide for VPN*.
- TunnelGuard. New feature used to check the security aspects of the remote PC client, i.e. installed antivirus software, DLLs, executables etc. Applicable for both SSL and IPsec connections. See the "Configure TunnelGuard" chapter in the *CLI/BBI Application Guide for VPN*.

NORTEL NETWORKS
216372-C, February 2005

- NetDirect. Ability to temporarily download a packet-based version of the SSL VPN client from the Portal. The NetDirect agent has more capabilities than the existing, manually installed, SSL VPN client, e.g. support for Microsoft Outlook and the ability to map network drives. See the "NetDirect" chapter in the *CLI/BBI Application Guide for VPN*.
- RSA SecurID authentication. It is now possible to configure RSA SecurID as a means of authenticating to the VPN.
  CLI path: `/cfg/sys/rsa` and `/cfg/vpn/aaa/auth/rsa`
  BBI path: Administration/RSA Servers and VPN Gateways/Authentication/Auth Servers
- Ability to create custom HTTP headers to be sent to backend servers.
  CLI path: `/cfg/ssl/server/http/dynheader`
  BBI path: SSL Offload>Servers>Types>HTTP>Dynamic Headers
- The VPN Gateway device now sets the Secure attribute on the SSL VPN session cookie and all Set-Cookie headers generated by backend servers. It directs the user agent to use only secure means to contact the origin server whenever it sends back this cookie. For more information, see RFC 2109.
  CLI paths: `/cfg/vpn/server/http/securecook` and `/cfg/ssl/server/http/securecook`
  BBI paths: VPN Gateways>Gateway Setup>SSL>HTTP>General and SSL Offload>Servers>Types>HTTP>General
- User passwords in local database encrypted.
- Ability to change a user's password or group membership in the local database without having to add the user anew.
  CLI path: `/cfg/vpn/aaa/auth/local/passwd` and `groups`
  BBI path: VPN Gateways>Authentication>Auth Servers>Modify (local)>Modify (user)
- The local database is now included when exporting the configuration.
- Support for restricting the number of concurrent VPN sessions for members of a specific group.
  CLI path: `/cfg/vpn/aaa/group/restrict`
  BBI path: VPN Gateways>Group Settings>Groups>General (Maximum Sessions)
- Support for separating accounting information per VPN.
  CLI path: `/cfg/vpn/aaa/radacct`
  BBI path: VPN Gateways>Accounting
- Support for mapping domains or hosts on the intranet to an intranet proxy server. When a match is found between the remote user's request and a domain or host listed here, the request is redirected via the proxy server that has been mapped to that domain/host.
  CLI path: `/cfg/vpn/server/proxymap`
  BBI path: VPN Gateways>Gateway Setup>SSL>Proxy Mapping

- Support for setting the type of behaviour when the HTTP server is down.
  CLI path: `/cfg/ssl/server/http/downstatus` and `/cfg/vpn/server/http/downstatus`
  BBI path: SSL Offload>Servers>Types>HTTP>General (Down Status) and VPN Gateways>Gateway Setup>SSL>HTTP>General (Down Status)
- Support for RADIUS authentication of CLI/BBI administrator users.
  CLI path: `/cfg/sys/adm/auth`
  BBI path: Administration>RADIUS
- Support for SNMP version 3 added. For more information, see Appendix B, "The SNMP Agent" in the *User's Guide*.
  CLI path: `/cfg/sys/adm/snmp`
  BBI path: Administration>SNMP
- Support for file import/export to/from the VPN Gateway device via SFTP and SCP, including support for managing known SSH host keys. For more information, see Appendix G, "SSH Host Keys" in the *User's Guide*.
  CLI path: `/cfg/sys/adm/sshkeys/knownhosts`
  BBI path: Administration>SSH Keys

Portal

- New Portal layout, including new link icons (configurable), adjustable number of link columns and link area width. Ability to customize the Portal's look and feel using color themes. Ability to configure URL field (visible or not) on the Home tab.
  CLI path: `/cfg/vpn/portal`
  BBI path: VPN Gateways>Portal Display (General and Presentation)
- Support for creating Portal links to Citrix Metaframe servers as ordinary web links.
  CLI path: `/cfg/vpn/portal/citrix`
  BBI path: VPN Gateways>Portal Display>General
- Ability to select IPsec mode for the Full Access feature. Contivity mode implies connection to a Contivity server. Native mode implies connection to the VPN Gateway device.
  CLI path: `/cfg/vpn/portal/faccess/ipsecmode`
  BBI path: VPN Gateways>Portal Display>Full Access (IPsec mode)
- Support added for linksets, i.e. a set of links. Eliminates the need to create the same portal links for each user group. Linksets are mapped to the desired user groups.
  CLI path: `/cfg/vpn/linkset`
  BBI path: VPN Gateways>Portal Linksets

NORTEL NETWORKS
216372-C, February 2005

- Support for moving links.
  CLI path: `/cfg/vpn/linkset/link/move`
  BBI path: VPN Gateways>Portal Linksets>Links (Reorder)
- Support for adding cookie strings to iauto (Internal Auto Login URL) links.
  CLI path: `/cfg/vpn/linkset/link/iauto/cookies`
  BBI path: VPN Gateways>Portal Linksets>Links>Iauto>Auto Configuration
- Support added (under Tools menu) for changing user passwords stored in the local database.
- Support added (under Tools menu) for clearing the VPN Gateway device's cache from login information supplied during a Portal session.
- Support added (under Tools menu) for viewing server information (e.g. version) and client information (e.g. logged in user and browser type/version). This page also provides the ability to perform a bandwidth test.
- Support added (under Tools menu) for accessing the Browser-Based Management Interface (BBI) from the Portal. This option is used together with the Secure Service Partitioning feature and enables authorized end-customer users to administer their VPNs.
- Support for bookmarks added to Portal. Requires an LDAP/Active Directory database and that User Preferences is enabled for the LDAP Authentication method on the VPN Gateway device.
- Support for creating different extended profiles depending on access method (SSL, IPsec or NetDirect agent).
  CLI path: `/cfg/vpn/aaa/filter/methods`
  BBI path: VPN Gateways>Group Settings>Client Filters
- Support for creating different extended profiles depending on whether the TunnelGuard checks succeed or not.
  CLI path: `/cfg/vpn/aaa/filter/tg`
  BBI path: VPN Gateways>Group Settings>Client Filters
- HTTP to HTTPS redirection made simpler. Added to the VPN Quick Setup wizard in the initial setup procedure. Also see the "HTTP to HTTPS Redirection" chapter in the *Application Guides for VPN*.
- HTTP to HTTPS redirect mappings. Enables redirect of requests for an internal host using HTTP to another (or the same) internal host via HTTPS.
  CLI path: `/cfg/ssl/server/http/redirmap`
  BBI path: SSL Offload>Servers>Types>HTTP>HTTPS Redirect

- Support for single sign-on domains. Ability to add domains for which single sign-on is allowed. For SMB and FTP links, the file servers' domains now have to be added as single sign-on domains for the links to display the file system right away.
  CLI path: `/cfg/vpn/aaa/ssodomains`
  BBI path: VPN Gateways>Gateway Setup>Single Sign-On>Domains
- Support for defining custom single-sign on HTTP headers, e.g. for web servers that do not support basic or form-based authentication.
  CLI path: `/cfg/vpn/aaa/ssoheaders`
  BBI path: VPN Gateways>Gateway Setup>Single Sign-On>Headers
- Support for using LDAP and RADIUS macros in Portal links. By mapping the macro to the desired user record, the macro inserted in the link expands to the corresponding value for the user record.
  CLI path: `/cfg/vpn/aaa/auth/ldap/ldapmacro` and `/cfg/vpn/aaa/auth/radius/macro`
  BBI path: VPN Gateways>Authentication>Auth Servers (LDAP type>LDAP Macro Configuration and VPN Gateways>Authentication>Auth Servers (RADIUS type>RADIUS Macro Configuration
- Support for storing user preferences (Portal bookmarks, login information) in an external LDAP/Active Directory database.
  CLI path: `/cfg/vpn/aaa/auth/ldap/enauserpre`
  BBI path: VPN Gateways>Authentication>Auth Servers (LDAP type>User Preferences
- Support for performing a password-expired check against an LDAP/Active Directory database and directing users to default group when their passwords have expired.
  CLI path: `/cfg/vpn/aaa/auth/ldap/activedire/enaexpired`
  BBI path: VPN Gateways>Authentication>Auth Servers (LDAP type>Enable Expired Account Check
- Support for the eauto (External Auto Login URL) link type has been removed. This link type was previously used to create automatic log-on links to external web sites.

Browser-Based Management Interface

The Browser-Based Management Interface (or Web GUI) has been redesigned.

For more information about the Browser-Based Management Interface, see the *BBI Application Guide for VPN*.

NORTEL NETWORKS
216372-C, February 2005

Software Installation and Upgrade Notice

SSL VPN Server Software

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

- `SSL-5.0.3-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-5.0.3-boot.img`

  Using this image will reset the VPN Gateway device to its factory default configuration. It must be used when an VPN Gateway device 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:**

   Alteon ▸ SSL Accelerator/SSL VPN ▸ Software

   VPN Gateway ▸ VPN Gateway 3050 ▸ 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.

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 ▸ Software.**

The installable SSL VPN client comes in two versions (for limitations, see page 15):

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

Contivity VPN Client Software

The Contivity VPN client software can be downloaded from Nortel's Customer Support Web site. In the three-step Product Finder guide, select **Contivity ▸ Contivity Multi-OS 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 5.0 for clusters that include systems of the above type:

Current version	Procedure
4.1.x or earlier	Upgrade to 5.0, 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 5.0.
4.2.1.11 or later 4.x	Repartition before upgrade to 5.0.

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.

NORTEL NETWORKS
216372-C, February 2005

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.x

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.x, 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.

Full Access

If Full Access has been configured for access to a Contivity server in a version prior to 5.x, upgrading to 5.x will result in an invalid setting. After the upgrade, change the `/cfg /vpn #/portal/faccess/ipsecmode` setting from `native` to `contivity`.
BBI path: VPN Gateways>Portal Display>Full Access.

Supported Hardware Platforms

The SSL VPN 5.0.3 server software version is currently supported on the following hardware platforms:

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

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)

NORTEL NETWORKS
216372-C, February 2005

Known Limitations

Browser Requirements

Basic Portal Access (no applets)

When using the SSL VPN 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

TunnelGuard Applet Support

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

The following browsers support the TunnelGuard 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

NetDirect Agent

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

TunnelGuard

Version TG_1.1.2.0_001 of the *installed* TunnelGuard application is the minimum requirement for use with the Contivity VPN client.

Contivity VPN Client

- For IPsec termination on the VPN Gateway device, the following Contivity 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 NETWORKS
216372-C, February 2005

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 device 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.
- 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.

NORTEL NETWORKS
216372-C, February 2005

Known Issues

This section lists known issues with software version 5.0.3.

Number of VPNs

The documentation states that it is possible to configure up to 256 VPNs per SSL VPN cluster. Even if this is practically possible, the maximum number of supported interfaces bound to a VPN per cluster is 64. This will be fixed in a coming patch release. (Q01041851)

Portal

The default.htm page presented by web-based WTS (Windows Terminal Server) is not supported through the SSL VPN 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)

TunnelGuard

TunnelGuard does not work with Sun's JRE 1.5. (Q01067435)

NORTEL NETWORKS
216372-C, February 2005