Nortel VPN Gateway 6.0

Release Notes

part number: 216372-G, April 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 6.0.1 software. This supplement lists the new features and modifies some information found in the complete documentation:

- *VPN Gateway 6.0 User's Guide*
  (part number 216368-D, April 2006)
- *VPN Gateway 6.0 Command Reference*
  (part number 216369-D, April 2006)
- *VPN Gateway 6.0 Application Guide for SSL Acceleration*
  (part number 216370-D, April 2006)
- *VPN Gateway 6.0 CLI (Command Line Interface) Application Guide for VPN*
  (part number 216371-D, April 2006)
- *VPN Gateway 6.0 BBI (Browser-Based Interface) Application Guide for VPN*
  (part number 217239-C, April 2006)
- *VPN Gateway 6.0 VPN Administrator's Guide*
  (part number 217238-C, April 2006)
- *VPN Gateway 3050/3070 Hardware Installation Guide*
  (part number 216213-B, March 2005)

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 in Software Version 6.0.1

This section lists software features and enhancements added since version 5.1.5.

General

- Added support for assignment of network attributes (including IP address) via RADIUS or DHCP for Net Direct and IPsec VPN client connections. Several IP pools with different pool mechanisms (local, RADIUS or DHCP) can be created and mapped to different user groups, extended profiles, or be used as default IP pools. See the "Net Direct" and "Transparent Mode" chapters in the *Application Guide for VPN*.
  CLI path: `/cfg/vpn #/ippool #/type`
  BBI path: VPN Gateways>Gateway Setup>IP Pool>General (Type)
- Added support for configuring maximum session time (for a remote user's VPN session) on a per group level. The best value of the user's different groups/extended profiles and the VPN's default maximum session time will be selected at user login.
  CLI path: `/cfg/vpn #/aaa/group #/sessionttl` and `/cfg/vpn #/aaa/group #/extend #/sessionttl`
  BBI path: VPN Gateways>Group Settings>Groups>General (Maximum Sessions) and VPN Gateways>Group Settings>Groups>Extended Profile (Maximum Session Length)

- Added support for configuring the idle timeout (for a remote user's VPN session) on a per group level. The best value of the user's different groups/extended profiles and the VPN's default idle timeout will be selected at user login. The idle timeout can also be set for extended profiles. The idle timeout setting has been removed from the IP pool.
  CLI path: `/cfg/vpn #/aaa/group #/idlettl` and `/cfg/vpn #/aaa/group #/extend #/idlettl`
  BBI path: VPN Gateways>Group Settings>Groups>General (Maximum Sessions) and VPN Gateways>Group Settings>Groups>Extended Profile (Session Idle Time)
- Moved the RADIUS idle timeout attribute settings (regarding a remote user's VPN session) to new locations in the CLI and BBI.
  CLI path: `/cfg/vpn #/aaa/auth #/radius/idletimeout`
  BBI path: VPN Gateways>Authentication>RADIUS>RADIUS Settings (Idle Timeout Settings
- Added general functionality in the CLI to not expose passwords/secrets. When the `cur` and `diff` commands are used, any passwords/secrets will be displayed as "(SECRET)". When the `dump` command is used, no secret value will be dumped unless a dump password has been given, and in this case the secret value is encrypted. To paste a dump, the `paste` command should be used. The password given at the `dump` command should then be supplied.
- Changed license behaviour. If one of the VPN Gateways in the cluster would fail, the license installed on the device will continue being valid for a grace period of 30 days. If a user logs in via IPsec and there is no IPsec user license available, an SSL user license will instead be used (if available).
- The default license has been increased from 10 to 50 concurrent users, for SSL connections as well as IPsec connections.

Portal

- Added support for enabling Nortel IE cache wiper support on a per group level.
  CLI path: `/cfg/vpn #/portal/wiper` and `/cfg/vpn #/aaa/group #/wiper`
  BBI path: VPN Gateways>Portal Display>General (Use ActiveX Component For Clearing Cache) and VPN Gateways>Group Settings>Groups>General (Wiper)
- Added support for enabling Citrix Metaframe support on a per group level.
  CLI path: `/cfg/vpn #/portal/citrix` and `/cfg/vpn #/aaa/group #/citrix`
  BBI path: VPN Gateways>Portal Display>General (Citrix Support) and VPN Gateways>Group Settings>Groups>General (Citrix Support)

- Ability to upload custom content (Java applets, HTML pages, executables etc) to a content area on the Portal. Given the path, remote users can access and execute the content, e.g. an application, without logging in to the Portal.
  CLI path: `/cfg/vpn #/portal/content`
  BBI path: VPN Gateways>Portal Display>Custom Content
- API for developing a custom application that automatically logs in the user to the desired VPN and executes a previously configured Port forwarder link on the Portal's Home tab. For further instructions, see "Appendix I" in the *User's Guide*.
- Added support for SSHv2 for the Telnet/SSH terminal applet (available on the Portal's Advanced tab). SSHv2 supports X11 forwarding.
- Added command used for listing all character sets that can be used in backend conversion.
  CLI path: `/cfg/vpn #/portal/lang/beconv/codesets`
  BBI path: VPN Gateways>Portal Display>Language>Backend Conversion>Codesets
- Added support for specifying a default value for Windows workgroup for SMB (Windows file share) servers. The default value is suggested in the [Workgroup] field on the Portal's Files tab and when creating SMB links.
  CLI path: `/cfg/vpn #/portal/smbworkgrp`
  BBI path: VPN Gateways>Portal Display>General (Default SMB Workgroup Name)
- Added support for clearing all cookies set by the browser when the user logs out/is logged out from the Portal. This also includes the SiteMinder SMSESSION and the ClearTrust CTSESSION cookies. If set to `off`, the NVG only clears cookies set by the NVG itself. The default setting is `on`
  CLI path: `/cfg/vpn #/server/portal/wipecookie`
  BBI path: VPN Gateways>Gateway Setup>SSL>Portal (Clear All Session Cookies)

IPsec

Added support for IPsec-based branch office tunnels. See the "Branch Office Tunnels" chapter in the *CLI/BBI Application Guide for VPN*.

Certificates

Added support for automatic CRL retrieval via LDAP with anonymous bind. Now the authDN and password strings can be kept when anonymous bind is enabled. Previously, the user had to clear these strings before using anonymous binding.
(CR Q01301133)
CLI path: `/cfg/cert #/revoke/automatic/anonymous`
BBI: Not supported in BBI

Authentication

- Added support for RSA ClearTrust authentication with additional support for client certificate authentication.
  CLI path: `/cfg/vpn #/aaa/auth #/cleartrust` and `/cfg/vpn #/aaa/auth #/cert/adv/validatedn`
  BBI path: VPN Gateways>Authentication>ClearTrust and VPN Gateways>Authentication>CERT>Cert Settings (Validate Cert-DN by ClearTrust Server)
- Added support for stripping the domain name from the user name before performing LDAP authentication.
  CLI path: `/cfg/vpn #/aaa/auth #/ldap/enacutdomain`
  BBI path: VPN Gateways>Authentication>LDAP>LDAP Settings (Cut Domain from User Name)
- Added new method for finding LDAP group information suited for iPlanet.
  CLI path: `/cfg/vpn #/aaa/auth #/ldap/groupsearch`
  BBI path: VPN Gateways>Authentication>LDAP>Group Search
- Added command to extract the first part of a returned Distinguished Name as the group name to be used. Example: CN=My Group,CN=User,DC=company,DC=com will use 'My Group' as the actual group name. This makes it easier to configure the group name in the VPN as you do not have to configure the entire DN string as group name.
  CLI path: `/cfg/vpn #/aaa/auth #/ldap/enashortgrp`
  BBI path: VPN Gateways>Authentication>LDAP>LDAP Settings (Short Group Format)

Net Direct

- Added support for Net Direct on Linux and Mac OS X (for PowerPC).
- Added support for installable Net Direct client (Windows only). By downloading a setup.zip file from the Portal, the administrator/remote user can install a permanently installed version of the Net Direct client on client PCs (as opposed to downloading Net Direct on a per session basis). The behaviour of the installable Net Direct is controlled via the same commands as the existing downloadable Net Direct client.
  See the "Net Direct" chapter in the *Application Guide for VPN*.
- Added support for caching Net Direct components on the client machine to enable quicker download of the Net Direct client the next time the user clicks the Net Direct link (Windows only).
  CLI path: `/cfg/vpn #/sslclient/caching`
  BBI path: VPN Gateways>VPN Client>Net Direct Client (Caching)

- Added support for enabling Net Direct support on a per group level.
  CLI path: `/cfg/vpn #/sslclient/netdirect` and `/cfg/vpn #/aaa/group #/netdirect`
  BBI path: VPN Gateways>VPN Client>Net Direct Client and VPN Gateways>Group Settings>Groups>General (Net Direct Client)
- Added support for filtering out untrusted operating systems.
  CLI path: `/cfg/vpn #/sslclient/oslist`
  BBI path: VPN Gateways>VPN Client>Net Direct Client (Operating Systems)
- Added support for storing a Windows administrator user name and password on a per group level on the NVG. This enables group members to install and run the Net Direct client without having administrative rights.
  CLI path: `/cfg/vpn #/aaa/group #/ndwauser` and `ndwapassword`
  BBI path: VPN Gateways>Group Settings>Groups>General (Net Direct Windows Admin User Name/Password)
- Added support for configuring a Net Direct banner message. The message is displayed when Net Direct is started on the remote user's machine.
  CLI path: `/cfg/vpn #/sslclient/ndbanner`
  BBI path: VPN Gateways>VPN Client>Net Direct Client (Net Direct Banner)
- Added support for configuring a Net Direct license message. The message is displayed when Net Direct is started on the remote user's machine (not for installable client).
  CLI path: `/cfg/vpn #/sslclient/ndlicense`
  BBI path: VPN Gateways>VPN Client>Net Direct Client (Net Direct License)

Nortel SSL VPN Client

The installable SSL VPN client comes in two versions, the LSP (Layered Service Provider) client and the TDI (Transport Driver Interface) client. For information about capabilities and limitations, see "Known Limitations" on page 20.

- Added support for allowing/denying SSL VPN client access.
  CLI path: `/cfg/vpn #/sslclient/tdiclient`, `lspclient` and `oldclients`
  BBI path: VPN Gateways>VPN Client>TDI Client/LSP Client/Old Clients
- Added support for filtering out untrusted operating systems.
  CLI path: `/cfg/vpn #/sslclient/tdioslist` and `lsposlist`
  BBI path: VPN Gateways>VPN Client>TDI Client/LSP Client (Operating Systems)
- Added support for filtering out untrusted client versions.
  CLI path: `/cfg/vpn #/sslclient/tdivsn` and `lspvsn`
  BBI path: VPN Gateways>VPN Client>TDI Client/LSP Client (Minimum Version)

Client Security

- Added support for Symantec WholeSecurity Confidence Online. If enabled, a scan of the client machine can be performed to identify any eavesdropping threats (including Trojan horses, remote controls, keystroke loggers and worms). See the "WholeSecurity" chapter in the *CLI/BBI Application Guides* for VPN.
  CLI path: `/cfg/vpn #/aaa/wholesec`
  BBI path: VPN Gateways>WholeSecurity

- Enhancements in the Tunnel Guard administration applet (used to configure SRS rules). Enhancements include file age, registry and version checking, NOT operand for creating logical expressions. See the "Configure Tunnel Guard" chapter in the *CLI/BBI Application Guides* for VPN.
  CLI path: Not accessible from the CLI
  BBI path: VPN Gateways>Tunnel Guard>SRS Rules

- New menu added to handle settings for the Tunnel Guard agent, i.e. when Tunnel Guard is used in combination with the Nortel IPsec VPN client (formerly the Contivity VPN client). The menu includes commands to set the Tunnel Guard agent query timeout interval and Tunnel Guard agent minimum version.
  CLI path: `/cfg/vpn #/aaa/tg/agent`
  BBI path: VPN Gateways>Tunnel Guard>Agent

- New command added to control whether or not Tunnel Guard failure details should be displayed to the user. The setting does not have any impact on the *installed* Tunnel Guard agent's behaviour.
  CLI path: `/cfg/vpn #/aaa/tg/details`
  BBI path: VPN Gateways>Tunnel Guard>Setup (Display SRS Failure Details)

Administration

- Added support for authorizing administrator users based on a group attribute sent by a RADIUS authentication server. When the user is successfully authenticated, the RADIUS server returns the groups to which the user belongs. The groups are compared to the fixed administrator groups on the VPN Gateway, i.e. `tunnelguard`, `admin`, `oper` and `certadmin`. If a match is found, the logged on user is given the administration rights pertaining to matching group(s). If not, the user is denied access. To sum up, a RADIUS system administrator can add a VPN Gateway administrator user to the RADIUS configuration, i.e. this user need not be configured locally on the NVG.
  CLI path: `/cfg/sys/adm/auth/group`
  BBI path: Administration>RADIUS>Group Attributes

- Support for SONMP (SynOptics Network Management Protocol), a Nortel-proprietary layer-2 topology discovery protocol.
  CLI path: `/cfg/sys/adm/sonmp` and `/info/sonmp`
  BBI path: Administration>SONMP and Administration>Monitor>SONMP Topology

- Added support for setting the desired authentication and privacy protocols for SNMP transmissions.
  CLI path: `/cfg/sys/adm/snmp/users/authproto` and `/cfg/sys/adm/snmp/users/privproto`
  BBI path: Administration>SNMP>Users (Authentication Protocol and Privacy Protocol)

- Added `tunnelguard` to the system administrator groups. Members of the tunnelguard group are only allowed to manage Tunnel Guard SRS rules via the Tunnel Guard administration applet in the BBI.
  CLI path: `/cfg/sys/user/edit <user>/groups`
  BBI path: Administration>Users

- Added support for the DISMAN-EVENT-MIB. The feature lets you define a monitor for polling an object from the MIB and configure a value to which the polled object's value should be compared. If a match is found, a corresponding event is generated.
  CLI path: `/cfg/sys/adm/snmp/event`
  BBI path: Administration>SNMP>DISMAN EVENT MIB

BBI (Browser-Based Management Interface)

- Added the SSL VPN Cluster Manager application to the BBI. The Cluster Manager is a tool used for centralized cluster and user management. See the "SSL VPN Cluster Manager" chapter in the *BBI Application Guide for VPN*.

  Key features:

  - Customizable tree view where you can create your own hierarchy by adding geographical domains, clusters and hosts.
  - Software/configuration management. Upgrade several clusters with a new software version at the same time. Export/import configurations across clusters.
  - Performance graphing. View memory and CPU usage per cluster or host. View current sessions per cluster. The information is displayed as graphs that can be customized and saved.
  - Alarms view displaying alarms generated for all clusters or for specific clusters.

- New design, including the ability to sort columns by clicking the column header.

Fixes

This section lists fixes added since version 5.1.5.

General

- Fixed problem with apostrophe in language definition file. Apostrophes in the language definition file were not handled correctly.
(CR Q01177838)
- Fixed problem with MAC address getting changed. In some cases, e.g. when adding port 3 to an existing interface on NVG 3050, the "host" MAC address as given by `/info/local` would get changed, causing a mismatch with existing licenses.
(CR Q01263974)
- Fixed port range backward range acceptance. The port range backward range like 89-80 is not allowed for the following command. `/cfg/vpn #/aaa/service`. This is not fixed in the BBI.
(CR Q01173644)
- Fixed `oper` user rights in CLI. The `oper` user no longer has access to the following commands: `/cfg/sys/dns`, `/cfg/lang/import,export,vlist,del`, `/cfg/quick` and `/cfg/test`. The corresponding changes has been made to the BBI.
(CR Q01257387)
- Fixed an internal AAA subsystem restart. The system allows the AAA subsystem to restart due to eventual internal software failures. However, a control channel to the traffic handling subsystem was not reinitialized properly which much later could lead to a new AAA subsystem restart (due to reuse of resources). Note: the AAA restart only affects current login attempts (not already authenticated sessions), i.e. the users have to do a new login attempt.
- Previously, when configuring a service definition using the `/cfg/vpn #/aaa /service #/icmp` command, the CLI prompted for a port number. A port number is not needed for ICMP so the prompt has been removed.
(CR Q01163667)
- Fixed SSL proxy restart after 497 days of uptime. Previously, if the system had been running for 497 days without reboot, the SSL proxy would restart due to an inconsistent return value from a kernel timer function. Also the reported uptime from `/info/local` would start over at 0 after 497 days.
(CR Q01249382)

- Fixed memory leak when using HTTP compression. Enabling compression of HTTP data (`/cfg/ssl/server #/http/compress on`), caused memory leaks in sessions where compression was done. This could eventually lead to a restart of the SSL proxy (error message "internal error 179").
  (CR Q01242859)
- Enhanced tab completion for the `/cfg/vpn #/aaa/network/subnet` CLI command. Depending on how the subnet is configured, either the name or a combination of host/mask is used.
  (CR Q01173628)
- Enhanced tab completion for the `/cfg/vpn #/linkset/link` CLI command. The configurable link text is used for tab completion. The link text is truncated at 20 characters, then postfixed with "..."
  (CR Q01123899)
- Raised limits on X-SSL header. The Subject and Issuer information, included in the X-SSL header when `/cfg/ssl/server #/http/sslheader` (SSL Offload>Servers >Types>HTTP>General (SSL Header) is set to `on`, was limited to max 255 characters each (truncated if longer). This limit is now raised to 1000 characters.
  (CR Q01290075)
- Fixed reverse rewrite problem of URLs. Different URLs are tagged with a type when they are rewritten by the NVG. For example, the Javascript src URL myscript.js is tagged like `myscript.js,xct1`. Previously, the `,xct1` was not removed when doing reverse rewrite. This has now been corrected.
- Fixed SSL proxy crash. Some combinations of HTTP and HTTPS requests made through the HTTP proxy applet (available on the Portal's Advanced tab or as a Portal link) could cause the SSL proxy to crash and restart.
- Fixed problem with NVG sending compressed `xnet.js` file to a Microsoft IE 5.5 client. Microsoft IE 5.5 has a compression bug (see MS knowledge base #313712) causing the browser to drop the first 2048 bytes of compressed data. There is a setting in the CLI which governs if the NVG produces compressed content to the client or not. When set to `off` (default value), no compressed content is sent to the client browser. When set to `on`, the content from the intranet and from the NVG will be compressed if the client browser accepts compressed content. This change makes the NVG portal code take into account this setting when delivering the javascript file `xnet.js` to the client.
  (CR Q01270920)
- If a SOCKS/Net Direct user logged in and the RADIUS server replied with a challenge response, this could previously cause a crash when the system tried to encode the AAA challenge response. This has now been fixed.

- The system now performs a stricter check to detect the “Upgrade in progress” system status. The purpose is to prevent the user from accidentally executing the `reboot`, `halt` or `repartition` commands before the system is completely operational.

Portal

- Fixed non-translated messages in the Portal. Error messages given on failed login to the Portal were not translated.
  (CR Q01177727)
- Fixed link on Portal’s Full Access tab. Previously, the link to **www.java.com** did not work due to incorrect quoting.
  (CR Q01274927)
- Fixed problem with deactivating the Full Access applet on the Portal’s Access tab not shutting down IPsec client.
  (CR Q01307340)
- Added support for exporting a modified language file. Previously, only the language definition template (in English) could be exported.
  (CR Q01142805)
  CLI path: `/cfg/lang/export`
  BBI path: Operation>Language (Import/Export Language Definition)

Certificates

- Fixed Sub-CA Certificates authentication and authorization. Previously, configuring the Sub-CA alone in the CA chain caused user authentication and authorization to fail.
  (CR Q01154557)
- Fixed problem with client certificates. Previously, client certificates with a Subject DN longer than 255 characters did not work for extended profiles or certificate authentication.
  (CR Q01325115)

SMB (Windows File Share) and FTP

- Fixed problem with uploading files with filenames including special characters (e.g. `@#$%foo.txt`) to SMB and FTP file servers.
  (CR Q01161886)
- Fixed problem with NetBIOS keep-alive packets being picked up by the NVG while waiting for an outstanding SMB call reply. The keep-alive packets are now discarded.

Authentication

- Fixed problem with aaa/LDAP attribute parsing being case sensitive. It is now case insensitive.
- Fixed secondary authentication in combination with certificate login.
  (CR Q01255568)
- Fixed problem when sending client certificates to portal server. When `/cfg/vpn # /server/http/addclicert` (VPN Gateways>Gateway Setup>SSL>HTTP>General (Client-Cert) is set to on and certificate authentication is used, the authentication could fail in some cases. In particular, this has been observed with some certificates issued by an intermediary CA in combination with a secondary authentication method.
  (Found in verification of CR Q01255568)
- Fixed so that non-ASCII passwords are handled correctly. This is when using an NTLM type of login service.
- Fixed problem when importing a sdconf.rec file of the wrong size for RSA SecurID authentication by adding a check for the sdconf.rec file size. From the RSA knowledge base, the sdconf.rec file should always be 1024 bytes in all instances of ACE/Server 5.x and ACE/Agent 5.x. If in future RSA ACE releases, the sdconf.rec file size changes, then this fix should be revisited.
- Fixed the display of password expiry alert for LDAP user. Previously, when used with the IE cache wiper, the password expiry alert was blocked by the cache wiper. Password expiry information will be displayed at login to the Portal, only when 5 days (or less) remain before the password expires.
- Fixed PKI authentication loop with Tunnel Guard. Previously, if certificate authentication was used in combination with Tunnel Guard and the Tunnel Guard checks failed, the user was redirected to the login page which would automatically cause a new certificate login attempt. The user will now be redirected to the auto login page in case of a Tunnel Guard check failure. The page will show the failure reason just like the normal login page.
  (CR Q01264690)

Accounting

Improved RADIUS accounting for VPN users. The RADIUS accounting information now includes the Calling-Station-Id (client IP address) attribute, and in the case of Net Direct or IPsec sessions, also the Framed-IP-Address (assigned IP address) attribute.
(CR Q01216792)

BBI (Browser-Based Management Interface)

- Fixed buffer overflow in BBI code. Sending an extremely long username when attempting login to the admin BBI would cause a crash in the backend server due to a buffer overflow. In principle the buffer overflow could also be exploited to give interactive OS access without authentication if the username contents was carefully crafted.
  (CR Q01256093)
- Fixed problem with setting Session Idle Time and Maximum Session length (under VPN Gateways>Gateway Setup>Sessions). Previously, when setting the hour value>0 and all other values to 0, an error message was returned.
  (CR Q01297035-01)

Software Installation and Upgrade Notice

SSL VPN Server Software

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

- `SSL-6.0.1-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*.

  Note! TFTP cannot be used when upgrading to version 6.0.1 from an earlier version.

- `SSL-6.0.1-boot.img`

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

  Note! TFTP cannot be used when installing version 6.0.1 via the reinstall procedure.

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 Technical Support>Software Downloads.**
3. **In the first step of the three-step Product Finder guide, choose 'Select from Product Families' in the list box. Then select the following:**

   VPN Gateway ▸ VPN Gateway 3050/3070 ▸ Software
4. **Click Go and 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

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 24):

- 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)

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 or Later on NAS 2424-SSL

This applies to the Nortel Application Switch 2424-SSL delivered with a software version prior to 5.0 pre-installed.

In the following text, 5.x should be interpreted as 5.x *or later*.

On this system, the existing disk partitioning does not allow for a 5.x version to be installed simultaneously with version 4.x. I.e. it isn't possible to do a standard upgrade from 4.x to 5.x, or from one version of 5.x to another. 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 a system of the above type:

Current version	Procedure
Prior to 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 7-10 minutes.

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 – After repartition is completed, it will not be possible to downgrade 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 6.x. 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 5.1.5.4

NVG clusters running software version 6.0 or later cannot be downgraded directly to software versions prior to 5.1.5.4. This is due to changes in the internal database format. To downgrade such a cluster to a version lower than 5.1.5.4, first perform an intermediate downgrade to 5.1.5.4 (or later 5.x).

Downgrading to 5.1.5.4 or Later

- If a ClearTrust authentication scheme has been configured, downgrading to a version prior to 6.x will fail. Delete the ClearTrust authentication scheme before downgrading.
- In version 6.x, several IP pools may exist for a VPN. In version 5.x, only one IP pool per VPN may exist in the configuration. On downgrading from 6.x or later to 5.1.5.4 or later 5.x, the settings for the default IP pool in the 6.x configuration will be kept in the 5.x configuration, provided the default IP pool is of the type `local`. The Net Direct and IPsec network attributes are configured accordingly. If the default IP pool in the 6.x configuration is not of the type `local`, the first found local IP pool (lowest number) is selected to form the IP pool in the 5.x configuration. If no local IP pool is found, the IP pool will be disabled in the 5.x configuration.
- The TunnelGuard features introduced in 6.0 will be filtered out during the downgrade.
- If Net Direct, IE Wiper and/or Citrix Metaframe support has been set to `group` (see page 5), the setting will be changed to the respective default value.

Reload License After Upgrade

In version 6.0.1, the default license has been increased from 10 to 50 concurrent users, for SSL and IPsec connections. On upgrades from earlier versions where additional licenses (besides the default license) have been loaded to the devices, the additional license must be reloaded in order to make use of the extra 40 number of users in the default license.

Supported Hardware Platforms

The 6.0.1 server software is currently supported on the following hardware platforms:

- Nortel VPN Gateway 3050
- Nortel VPN Gateway 3070
- Nortel Application Switch 2424-SSL
- Nortel SSL VPN Module 1000

Software - Support on Hardware that has reached MD (Manufacture Discontinued) Product Status

Software releases may operate on Hardware that has reached MD (Manufacture Discontinued) Product Status. In this situation, the Software will be supported as per the Software Standard Life Cycle Support Practice - but not to exceed twelve (12) months from date of Hardware MD (Manufacture Discontinued) and is limited to supporting only the current software release on HW at time of MD declaration.

According to the above principle, the hardware models Nortel SSL Accelerator 310, 410 and 310-FIPS are not supported from NVG release 6.0 and onwards.

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
- Safari 2.0

Applet Support

To support the Telnet/SSH Access, HTTP Proxy, FTP Proxy, Port forwarder applets (available on the Portal's Advanced tab) and the Citrix Metaframe applet, the following browser and Java combinations are recommended:

- Windows:
  Internet Explorer 5 or later with Sun's JRE 1.4.2 or later
  Mozilla 1.5 or later with Sun's JRE 1.4.2 or later
  Firefox with 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
- Mac OS X:
  Safari 2.0 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 supported using the following browser and platform combinations:

- Internet Explorer on Windows 2000 and XP.
- Firefox on Linux, Windows 2000 and XP.
- Safari 2.0 on Mac OS version 10.4

The following Linux distributions have been verified to support Net Direct and Firefox:

- Fedora Core 2
- Fedora Core 3
- Fedora Core 4
- Red Hat 9.0
- Knoppix 4.0.2
- SUSE 10.0

Other Limitations

- The installable Net Direct client is not available for Linux and Mac OS X.
- Caching of Net Direct components is not supported for Linux and Mac OS X.
- The Net Direct mobility capabilities are not supported for Linux and Mac OS X.
- The split tunneling modes `enabled_inverse` and `disabled` are not supported for Mac OS X. For non-supported split tunneling modes, Net Direct falls back to the `enabled_inverse_local` mode.

- The split tunneling mode `enabled_inverse` is not supported for Linux. For non-supported split tunneling modes, Net Direct falls back to the `enabled_inverse_local` mode.
- If the remote user has proxy settings configured in Internet Explorer and split tunneling is enabled, Net Direct will use the proxy settings but split tunneling will be disabled, i.e all traffic will be tunneled.
- When using Net Direct on Linux and Mac OS X, the DNS server(s) specified on the NVG (in the IP pool or under `/cfg/sys/dns/servers`) must be able to resolve all host names that should be accessible (internal as well as external host names). This is because no external DNS server will be used as fallback.
- Downloading and installing Net Direct on Windows, requires the user to be administrator on his/her PC. For users that are not administrators, the Windows administrator user name and password can be stored (on group level) on the NVG. If the user is not administrator and the credentials are not stored on the NVG, the user will be prompted for the Windows administrator user name and password upon downloading Net Direct.
- Downloading and installing Net Direct on Mac OS X requires the user to be member of the admin group. If the user is not a member of the admin group or enters the wrong password when prompted, he/she can log in with the root password as an alternative option. This in its turn requires that the user account is authorized to perform the command `su root`.
- Downloading and installing Net Direct on Linux requires the user to be root user or see to it that the user account is authorized to perform the command `su root`. If the user is not running as root when attempting to download Net Direct, a window is displayed prompting the user for the root password.

Tunnel Guard Agent

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

Nortel IPsec VPN Client (formerly 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.
- The NVG software includes commands for allowing/rejecting access for certain SSL VPN clients, based on client version and which operating system the client currently runs on. These commands have been added as a preparation for future releases of the TDI/LSP clients, where the clients will be capable of sending version number and OS version to the NVG. Until the new TDI/LSP clients are released, existing TDI/LSP clients will be regarded as “old clients”.
  CLI path: `/cfg/vpn #/sslclient/tdiclient` and `lspclient` (these commands currently have no effect) and `cfg/vpn #/sslclient/oldclients`
  BBI path: VPN Gateways>VPN Client>TDI Client and LSP Client (these options currently have no effect) and VPN Gateways>VPN Client>Old Clients

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.
- 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.

- JVM 1.5 and later includes support for using the browser's certificate database. If the NVG is set to ask for client certificates, any Java applet started during a Portal session may display a window asking for a client certificate, even though the user has already logged in to the Portal with a client certificate. The solution is to click Cancel without selecting a certificate.
- Some web applications, if started, takes over existing instances of Internet Explorer, which may cause problems for the Portal session. For example, if the Portal page is reused by a web application and the Net Direct client is running, the client will be shut down. To solve this problem in IE, go to Tools>Internet options. On the Advanced tab, under Browsing, disable the setting "Reuse windows for launching shortcuts".

SSL VPN Module 1000 (SVM 1000)

When using the BBI (Browser-Based Management Interface) to configure the SVM 1000, some options in the BBI are available but not supported. The following features in the NVG software are not supported on the SVM 1000:

- Local authentication.
  BBI path: VPN Gateways>Authentication>Local
- Standalone mode.
  BBI path: VPN Gateways>Gateway Setup>Standalone and SSL Offload>Servers>General (Standalone Mode)
- Transparent proxy mode.
  BBI path: SSL Offload>Servers>General (Transparent Proxy Mode)
- Tunnel Guard Agent settings.
  BBI path: VPN Gateways>TunnelGuard>Agent

General

- A maximum of 32,000 sessions is allowed on the VPN Gateway 3070 with 2 GB RAM.
- 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.
- When using the IPsec VPN client together with the installed Tunnel Guard agent, the result of the Tunnel Guard check cannot lead to an IP address being allocated from an IP pool that is assigned to an extended profile. This is because the IP address has to be allocated before the Tunnel Guard check is run.

Known Issues

This section lists known issues with the NVG software.

- For Net Direct on Windows, the split tunneling mode `enabled_inverse` does not tunnel local network traffic, i.e. the mode behaves like `enabled_inverse_local` split tunneling mode. This will be fixed in a coming patch release.
- For the Full Access feature (available on the Portal's Access tab) 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)
- Problem with Internet Explorer version 6.0.2800.1106.xpsp2_gdr.040517-1325.
  When HTTPS is used, this version of Internet Explorer does not permit download of files that require an external program for processing, or that should be saved in the file system (e.g. files with extension .txt, .exe, .zip), even if the SSL VPN server HTTP setting of `addnostore` is set to `off`. Thus it cannot be used to download such files via the Portal.
- In WholeSecurity Confidence Online versions prior to 5.0.2, there is no built-in support for the NVG. In order to get Confidence Online to work with the NVG, proceed as follows:

  In the MySQL database, go to the command line and enter the following commands:

  ```
  USE LANLORD
  ```

  ```
  INSERT INTO integrationdeploy (vendor, deploytype, eventsfile,
  ipaddressformat, cgipathformat, owner, featuretype)
  VALUES ("NortelSSLVPN", "Nortel SSL VPN", "", "%nortel_ssl_vpn%",
  "/https/%eeserver%/cgi-bin/rr.fcgi", "WholeSecurity", "_OD_");
  ```

  ```
  INSERT INTO integrationparameter (parametername, displayname, ven-
  dor, type, paramorder, required, validationfunction, owner)
  ```

  ```
  VALUES ("nortel_ssl_vpn", "Nortel SSL VPN name", "NortelSSLVPN",
  "string", 1, 1, "validateIP", "WholeSecurity");
  ```

  (CR Q01245774)
- When running Net Direct on Knoppix, the tun device node must be set up manually. To do that, run the following commands as root:

  ```
  mkdir /dev/net
  mknod /dev/net/tun c 10 200
  ```

  (CR Q01281449)

- When running Net Direct on Linux, root must be enabled on the remote user's machine and the administrator must see to it that the user account is authorized to use the command `su root`.
  (CR Q01278965)
- The installed Net Direct client does not support client security checks using the *installed* Tunnel Guard agent. If a user tries to connect to a VPN for which Tunnel Guard is enabled, the user cannot log in to that VPN if using the installed Net Direct client. This will be fixed in a coming patch release.
- The Tunnel Guard applet (client security check launched from the Portal) is not applicable when accessing a VPN using *installed* VPN clients.
  (CR Q01297451)
- If a downgrade from the NVG software release 5.1.3.6 to 5.1.3.2 is necessary, any Net Direct ActiveX controls installed on the remote users' machines adhering to the more recent software version requires manual removal. If the ActiveX control is not removed, Net Direct will not be able to operate on PCs accessing a Portal with the older software version. To remove the ActiveX control, open Windows Explorer and go to C:\Windows\Downloaded Program Files. Select Netdirect and press Delete.
  (CR Q01224780)
- Net Direct on Windows may not be compatible with some Internet security software for clients. This will be fixed in a coming patch release.
- Configuring IPsec support via the VPN quick setup wizard during the initial setup procedure (see Chapter 3, "Initial Setup" in the *User's Guide*), will result in failure to complete the setup. The solution is to configure IPsec support manually or use the CLI IPsec wizard (`/cfg/vpn #/ipsec/quick`). Also see the "Transparent Mode" chapter in the *Application Guide for VPN*.
  (CR Q01356592)
- Inconsistent ClearTrust SSO (single sign-on) behaviour. When a user connects to the NVG Portal after having received a ClearTrust single sign-on session cookie from another ClearTrust-enabled web agent (not the NVG), the Portal login page should be bypassed, i.e. the single sign-on cookie should be validated against the NVG. This only happens the first time the user connects to the NVG Portal, subsequent attempts fail.
  (CR Q01341726)
- If several ClearTrust authorization servers or dispatchers are configured on the NVG, the server pools are not refreshed. For example, if a previously failed server is up and running again, this is not reflected in the server pool list. In a coming patch release, the ClearTrust server pools on the NVG will be refreshed periodically.
  (CR Q01341793)

- It is not possible for the `oper` user to list loaded languages in the BBI (VPN Gateways>Portal Display>Language>General). This will be fixed in the next patch release. (CR Q01347782)
- Changing the system time in the Minute list box in the BBI (Cluster>Time) to 15 or a higher value generates an error message and may cause the BBI to hang. This will be fixed in the next patch release.
  (CR Q01341831)
- It is not possible to modify or delete a VPN created in the BBI if the VPN name contains an apostrophe or a space. The VPN can still be modified or deleted in the CLI. This will be fixed in the next patch release.
  (CR Q01343418)
- On Linux (SUSE 10.0) and Firefox, when starting Net Direct from the Portal, the message "Net Direct already running" may be displayed in the Java applet window although Net Direct has not been started. When this occurs, Net Direct cannot be started.
- When configuring the parameters for the downloadable Net Direct client, the administrator has the option to suppress display of the default license agreement.
  The following applies when the license agreement is suppressed (the text will be added to the relevant sections in the manuals in the next release):
  IMPORTANT: By suppressing presentation of the Nortel Software License Agreement you agree to accept the terms of the agreement on behalf of the users receiving the client software from you. If you do not wish to accept the license terms on behalf of the users, then do not suppress presentation of the agreement.
- For Net Direct, if the administrator password configured on the NVG does not match the Windows PC client's password, the browser can in some cases be closed.
- If a remote user runs an old version of the installable Net Direct client, the client should be able to detect this upon connecting to NVG and a dialog where the user can choose to update the client or continue with the old version should be presented. In this release the dialog is not displayed. This will be fixed in the next patch release.