Nortel VPN Gateway

Release Notes — Software Release 6.0.15

part number: 325279-A, October 2008

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

Contents

325279-A, October 2008

Release notes

These Release Notes provide the latest information regarding your VPN Gateway (NVG) with version 6.0.15 software. This supplement lists the new features and modifies some information found in the complete documentation:

- *VPN Gateway 6.0 Users Guide*
  (part number 216368-D, April 2006)
- *VPN Gateway 6.0 Command Reference*
  (part number 216369-D, April 2007)
- *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, October 2007)
- *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. **Choose 'Security & VPN' from Documentation, Software, and Bulletins in the listed Categories.**
4. **Then select the following:**
   - VPN Gateway 3050 or VPN Gateway 3070 Documentation
   - SSL VPN Module 1000
   - Application Switch 2424-SSL (from the Content Networking category)
5. **Select the desired documentation or Show All for a listing of all documents associated with the product.**

New Features/Enhancements in Software Version 6.0.15

This section lists software features and enhancements added for version 6.0.15.

General

- The isdbinddn account is enabled to write the isdUserPref attribute in the AD server. The isdbinddn user should be part of Administrator group and should have the permissions to update the user attributes. This enhancement prevents the user from using their own account to write the isdUserPref attribute or any other attributes which is a security concern. It also addresses the issue of micro-managing AD permissions at the user level. (Q01839264)
- The idle TTL and session TTL timeout override option is now available for the siteminder users. New control is provided to override the timeout values returned by the siteminder server with the values configred in NVG.(Q01860194).

  CLI command: /cfg/vpn #/ aaa/auth id/siteminder/override

When set to OFF, NVG uses the session timeout and idle timeout returned by the siteminder server.When set to ON, NVG uses only the configured session TTL and idle TTL values and ignores the values returned by the siteminder server.

Default value is OFF

BBI

- The support to provide SSL statistics for all configured SSL server VIP's is added in BBI. The CLI support for the same was provided in earlier release (Q01619542)."

Software installation and upgrade notice

SSL VPN server software

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

- `SSL-6.0.15.0-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 6.0.15 from an earlier version.

- `SSL-6.0.15.0-boot.img`

  Using this image will reset the NVG to its factory default configuration. It must be used when a NVG with 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 6.0.15 through 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. **Choose Security & VPN from Documentation, Software, and Bulletins in the listed Categories.**
4. **Select VPN Gateway 3050 or VPN Gateway 3070 Software**

5. **Select the desired software or Show All for a listing of all software associated with the product.**

6. **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.

The 6.0.7.0a and releases after 6.0.11.0 cannot be installed on the same platform due to an increase in software image sizes and limited storage space available in the 2424-SSL. However, 6.0.11.0 and later releases have a new disk repartitioning feature to accommodate any future releases.

The following options are available to install 6.0.15.0 (or 6.0.11.0/6.0.13.0) in 2424-SSL with 6.0.7.0a:

1. **6.0.15.0 image upgrade: all configurations are lost.**

2. **Downgrade to 6.0.5 and upgrade to 6.0.15.0: the existing configuration is retained**

To upgrade from Release 6.0.13.0 to 6.0.15.0, use standard upgrade procedures.

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:

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

Nortel IPsec VPN client (formerly Contivity)

The IPsec VPN client software can be downloaded from Nortel's Customer Support Web site. (http://www.nortel.com) Select **Security & VPN ▸ VPN Client ▸ Software.** Choose **Show All** for a complete list of software available.

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. 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 through <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 through 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 re-partitioning 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`, the setting will be changed to the respective default value.

Reload license after upgrade

In version 6.0 and later, 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. (See *VPN Gateway 6.0 CLI (Command Line Interface) Application Guide for VPN* (part number 216371-D, October 2007))

Supported hardware platforms

The 6.0.15 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.

Resolved issues

This section lists fixes added for version 6.0.15.

General

- Fixed the issue with 'allowdoc' command to work with *.csv files. Now the 'no cache' field in http header is removed when allowdoc is enabled for the server.
- The extra space appended by NVG at the end of userid has been removed in the string token, and DN certificates are now parsed properly (Q01918424).
- The javascript errors caused by eroom resulting in a break in plugin install have been solved. (Q01921419).
- Simpleproxy failure (and non-automatic recovery) while accessing zip files has been solved (Q01588528).
- The feature `/info/kick` works with more than 10000 users without displaying the list of users.(Q01878383).
- The access issues for the SMB shared folder with Swedish characters in share name is fixed (Q01656067).

Portal

- The simpleproxy crash when the Outlook Web Access link is launched through NVG is fixed (Q01893312).
- Webauthor activeX plug-in loads properly via VPN (Q01829381).
- The cookie handling issue that leads to reloading the login page when NVG is used to proxy requests to an external site has been solved. (Q01466192).
- Problem in uploading files using FTP proxy applet is resolved (Q01875426).

SSL

- Fixed the issue of backend server loadbalancing based on session persistence when the SSL-VPN is configured for ssl-offload. (Q01334444).
- HTTP Host header corruption sent out from NVG over SSL accelerator, resulting in HTTP code 404, has been resolved. (Q01528238).

NetDirect

- The instance of multiple default gateways assigned to a single user tunnel has been corrected. (Q01771448).
- Fixed the issue of NetDirect communicating to Portal IP address via the default gateway even when the NVG portal is on the same network as the client. (Q01576528)
- Fixed the issue that the Netdirect ignores the PACS settings to detect Proxy servers. (Q01778272)
- NetDirect sets default gateway on MAC with splitnet. Gateways are updated properly in NetDirect with splittunnel. (Q01908766)
- NetDirect connections build a correct route table when used with split tunnel in "enabled" mode. (Q01917341)
- NetDirect starts when launched through the portal from a Windows Vista machine. (Q01885586)
- Nortel NetDirect and NDIC works in Windows 2000. Separate NDIC binaries are used for windows 2000, XP and Vista. (Q01924033)
  NDIC binary files to be used in different windows versions are:
  - Windows 2000 - NetDirectWin2K_Setup.zip;
  - Windows Vista - NetDirectVista_Setup.zip
  - Windows XP - NetDirect_Setup.zip;

BBI

- High CPU utilization while monitoring users via Admin ->Monitor ->Users when very large number of users in the system has been resolved. (Q01877156)
- The error "Binay string not null terminated" on attempting to kick user from BBI has been resolved. (Q01586381)
- The SMB link configured through BBI adds the default workgroup. (Q01922432)
- System time can be changed in BBI succesfully. (Q01341831).

TunnelGuard

- The problem of IPSec consuming two licenses per user when Tunnelguard is enabled with the IPSec licenses exhausted and SSL licenses available for the user has been resolved (Q01860523).

- TG 4.5 noVM msi NN_JREPATH works correctly and the Tunnel Guard starts successfully. (Q01813164).
- TG 4.5 msi does not reboot by default after uninstall. (Q01813909)
- TG 4.5 noVM msi shows the correct version. The version key within the registry key is updated to 4.5. (Q01813177)

Known limitations

Browser Requirements

Basic Portal Access (no applets)

When using the NVG software for basic Portal access, that is 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 2.0
- Opera 2.0
- 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 2.0 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 2.0 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 2.0
Java 1.4.2 or later is required

BBI Support

Configuration through 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 2.0
- 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, XP andVista.
- Firefox on Linux, Windows 2000, and XP.
- Safari 2.0 on Intel Mac OS version 10.4.

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

- RedHat 7.3, Kernel 2.4.18
- RedHat 9.0, Kernel 2.4.20
- Knoppix 4.0.2, Kernel 2.6.12.4
- Fedora Core 2, Kernel 2.6.5
- Fedora Core 3, Kernel 2.6.2
- Fedora Core 4, Kernel 2.6.11
- SUSE 10.0, Kernel 2.6.16

NOTE – Other distributions work if they have a tun driver.

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.
- 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.
- Downgrade of IE cache wiper does not happen automatically.

  a. When downgrading Netdirect, you need to manually delete the IEwiper Control and the NetDirect cab files.

  b. When logged on to the portal page it will install the cab files from the server.

  c. If you want to use the downgraded version then delete the cab files in **Tools->Internet options->Settings->View Objects.** Otherwise no action is required.

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 NVG, the following Nortel IPsec VPN client versions have been tested: 4.15, 4.86, 4.91, 5.01, 5.11 6.1, 6.1.0.102., 6.07d, and 7.01.

NOTE – Version 6.07d can be installed only in Windows Vista.

- 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), Vista and XP. This client does not support UDP.
- Version 1.5.0.9 (TDI client): Compatible with Windows 2000, Vista 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 command: `/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

- When accessing an FTP server through the NVG Portal, the maximum supported file size is 2 gigabytes. (Q01435793)
- Sun’s JRE earlier than 1.4 cannot download any applets from the NVG 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".
- The SMB server can not be accessed when portal language is Japanese.

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 32000 sessions is allowed on the NVG 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.
- Citrix 4.5 is not supported by VPN Gateway.

Known issues

This section lists known issues with the NVG software.

- 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). (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 through the Portal.
- When running Net Direct on Knoppix, the tun device node must be set up manually. (Q01281449)

  To set up the tun device node manually, run the following commands as root:

  ```
  mkdir /dev/net
  mknod /dev/net/tun c 10 200
  ```
- 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`. (Q01278965)
- After performing an upgrade the "securecookie" value should be set to "OFF" in SSL acceleration mode. (Q01452086)

  If you are upgrading from a version older than 4.2.1.25, after the upgrade, the "secure cookie" option will be automatically enabled for all existing SSL servers (`/cfg/ssl/server #/http/securecookie`). This will cause problems for web sites that want to share the cookies between http and https sessions. If this happens, you must disable the securecookie option manually.
- 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. (Q01297451)
- The NVG does not support NDIC for Windows Vista.

- Net Direct (NDIC/ActiveX) client is not compatible with Kaspersky Antivirus and other Internet security programs. (Q01531880-01)
- 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; 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. (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. (Q01341793)
- 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.
- When using iauto with Internet Explorer an error is produced with Exchange Server 2007. (Q01591376)
- Following the user login and attempting to access Siemen's MagicWeb application a rewrite error is produced. (Q01513601)
- When the depth of a requested html page and the frame inside the html page is different, the image which is called by the frame is taking the depth as the html page's depth making the requesting path of the image wrong. (Q01483997)
- The Windows Vista portal Netdirect does not work for nonadmin users in Java applet mode.
- The splitnet is enabled on the local network if the network is not functioning as expected.
- In Windows Vista, the feature Netdirect splitnet functions only in disabled mode. The other modes are not functional.

- 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. (Q01748004)
- The Siebel portal does a client check before the application loads, but if it is run through proxy the client check fails. (Q01464430-01)

  Workaround:

  Connect the portal through Net Ditect and after the client check passes, open the site through proxy.
- The Outlook Web Access (OWA) works correctly only when the account and password entered in the Active Directory (AD) matches the account and password configured in the local database. If there is a mismatch, then the error message is not displayed and the window hangs. (Q01799870)
- After booting re-image of the NVG, the /cfg/cert menu does not appear on the initial startup.

  Workaround:

  Exit and re-login, wait for the initalization or the boot process to complete and then login. The /cfg/cert menu appears. (Q01800810)
- The SSL interface sends the FIN to the the client instead of sending it to the VIP. (Q01714204)

  Workaround:

  Set the ckeep timer value to less than 100sec.

NOTE – The conntrack timeout depends on the socket state.

- The NVG does not receive Internet Control Message Protocol (ICMP) packet (type 3 code4) when the packet exceeds Maximum Transmission Unit (MTU) on a router. As a result of this, the NVG keeps on sending (IPSEC) packets that are too large and are dropped on certain routers or firewalls. In coming future releases, the VPN client will be modified to respond to the MTU discovery path and according to the connection and tunnel, the MTU will be dynamically reduced. (Q01779003)
- The Office 2007 .pptx files cannot be accessed through FTP/SMB when the portal is opened in Internet Explorer 6.0 browser. (Q01850642)
- Auto-completion of CLI commands in portal terminal does not work with JRE 1.5.0 and 1.6.0. (Q01862153)

Nortel VPN Gateway - Release Notes - Software Release 6.0.15

VPN Gateway
Release 6.0.15

Document Number: **216372-X**
Document Status: **Standard**
Document Version: **Rev 01**
Part Code: **325279-A**
Release Date: **October 2008**

To provide feedback, or to report a problem in this document, go to www.nortel.com/documentfeedback.