NORTEL

Nortel VPN Gateway

Release Notes

Release: 7.0.3
Document Revision: 01.06

www.nortel.com

NN46120-400 216372-Y

Nortel VPN Gateway
Release: 7.0.3
Publication: NN46120-400
Document status: Standard
Document release date: 17 April 2008

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Trademarks

*Nortel, Nortel Networks, the Nortel logo and the Globemark are trademarks of Nortel Networks.

Java runtime environment and JRE are registered trademark of Sun Microsystems.

Lotus Domino is the registered trademark of IBM.

Yahoo! is the registered trademark of Yahoo.

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 ().

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 .

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 *Users Guide* for more information.

Contents

Release Notes

These Release Notes provide the latest information regarding Nortel VPN Gateway (NVG) with version 7.0.3 software. These release notes detail the added feature enhancements and resolved issues since Release 7.0 (7.0.1).

For a list of related publications, see "Related documentation" (page 45). The documentation suite for Nortel Virtual Private Network Gateway can be found on the documentation CD included with the software or on the Nortel technical documentation website http://www.nortel.com/support. For more information, see "How to get help" (page 47).

The following topics are discussed in this document:

New feature enhancements for Release 7.0.3

This section lists software feature enhancements added since version 7.0.1.

Net Direct

- The proxy server can be accessed when Net Direct attempts to access links behind a proxy through the VPN Gateway with Splitnets and Splittun defined. (Q01581966-01)
  To enable or disable allowproxy, enter the following:
  - — CLI command:
    `/cfg/vpn #/sslclient/netdirect/adv/allowproxy`
  - — BBI path:
    Net Direct Proxy Settings For Split Tunnel: under **VPN Gateways » VPN-# » VPN Client » Advanced**.
- Dynamic Host Configuration Protocol (DHCP) requests generated by the Nortel VPN Gateway (NVG) now contain client name and also a Domain Name System (DNS) entry is created. (Q01502274-01)
- The Net Direct can be launched successfully in the first attempt after connecting to SSL VPN portal. (Q01500922-01)

- Installable Net Direct supports installable TunnelGuard agent. (Q01297451)
- The administrator can disable the User Datagram Protocol (UDP) mode. (Q01427056-01)
  To disable the UDP mode, enter the following:
  - CLI command:
    `/cfg/vpn #/sslclient/udpports 0-1`
  - BBI path:
    Select **VPN Gateways » VPN-1 » VPN Client » Net Direct** and change **UDP Ports** range to 0-1.

TDI client

- SSL VPN Client version 1.5.0.15 or later now supports PC's with dual CPU processors and hyperthreading. (Q01153233-01)

IPsec

- Access to IPsec client even if the group name or password does not match the group from user authentication. This is done by binding the user to the group name returned by the RADIUS or LDAP. (Q01686241-01)
  To set group match, enter the following:
  - CLI command:
    `/cfg/vpn #/ipsec/groupmatch`
  - BBI path:
    Group Matching under **VPN Gateways » VPN-# » IPsec » General**
- Nested tunneling with MS IPsec client (L2TP) through the extranet client is possible. (Q01502320-01)
  To change the IKE port on the client and server to run the MS IPsec and Contivity VPN Client (CVC) simultaneously, enter the following:
  - CLI command:
    `/cfg/vpn #/ipsec/sys/nat-t`

```
 [NAT Traversal Menu]
udpport        - Set UDP port
portswitch     - Client IKE source port switching
ena            - Enable NAT Traversal
dis            - Disable NAT Traversal
```

`/cfg/vpn #/ipsec/ikeprof #/nat`

```
[NAT Menu]
natdetect     - Set ESP UDP NAT detect
timeout       - Set detect timeout
keepalive     - Set keepalive timeout
```

— BBI path:
VPN Gateways » VPN-# » IPsec » NAT Traversal

- When there is a request to VPN client connection while there is already a connection established, the VPN Gateway terminates the existing connection and creates a new connection. (Q01767878)
  To configure ICP (Initial Contact Payload), enter the following command in CLI:
  `/cfg/vpn #/ipsec/ikeprof #/icp on`

- The banner displayed is the banner text configured for the group that the user is assigned from the RADIUS or LDAP. It is the subset of the group binding feature. (Q01767884)

- Dynamic network access is available. The VPN Gateway can be configured to retrieve the filter attributes from the external RADIUS server. (Q01763270)
  The access enables the NVG to take filter information from RADIUS and applies the filter to the user tunnel.
  To set the filter attributes, enter the following:

  — CLI command:
  `/cfg/vpn #/aaa/auth #/radius/filtattr`

```
[RADIUS Filter Attributes Menu]
filterid        - Set vendor id for filter attribute
filtertype      - Set vendor type for filter attribute
ena             - Enable RADIUS Filter Attribute
dis             - Disable RADIUS Filter Attribute
```

  — BBI path:
  VPN Gateways » VPN-# » Auth Server-# [RADIUS] » Filter Attributes

- NAT Traversal Menu (NAT-T) is added for IKE port switching. The IPsec is accessible even when it is connected from behind the NAT device. (Q01416706-01)
  To view NAT-T menu, enter the following:

  — CLI command:
  `/cfg/vpn #/ipsec/sys/nat-t`

  — BBI path:

VPN Gateways » VPN-# » IPsec » NAT Traversal

- IPSec failover occurs similar to the Contivity failover. After the initial connection, IPsec pushes the IP list of failover sites that the client may access if the primary site is unavailable. (Q01139578-01)
  To access the IPsec failover menu and set the failover site to primary, secondary or tertiary, enter the following:
  - — CLI command:
    `/cfg/vpn #/ipsec/sys/failover`
  - — BBI path:
    VPN Gateways » VPN-# » IPsec » Failover

Portal

- Portal VIP to pop-up the unblock list in the Internet Explorer. (Q01764071)
  To add a site to the pop-up unblock list, enter the following:
  - — CLI command:
    `/cfg/vpn #/portal/punblock`
  - — BBI path:
    Pop-up Unblock: under **VPN Gateways » VPN-# » Portal General**
- Autofill passcode or tokencode using RSA soft token software is available. (Q01763315)
  To set the RSA soft token autofill, enter the following:
  - — CLI command:
    `cfg/vpn #/portal/rsaauto`
  - — BBI path:
    RSA Soft Token Autofill: under **VPN Gateways » VPN-# » Portal General**.

TunnelGuard

- Java Runtime Environment (JRE) is automatically installed if it is not available in the client PC. (Q01763318)
  In portal menu, option autojre is added. It can be enabled/disabled using On/Off for automatic download of JRE. By default, it is On.
  To change the status of the auto JRE install, enter the following:
  - — CLI command:
    `/cfg/vpn #/portal/autojre`
  - — BBI path:

Silent JRE Auto Installation: under **VPN Gateways » VPN-# » Portal General**

- When a TunnelGuard user tries to login from an unsupported operating system it is checked or bypassed accordingly. (Q01767916)
  To set bypass TunnelGuard check menu, enter the following:

  — CLI command:
  `/cfg/vpn #/aaa/tg/bypass`
  Enter `on` or `off` to allow or deny access to the portal from an unsupported operating system. If the access is denied then the reason is displayed.

  — BBI path:
  VPN Gateways » VPN-# » TunnelGuard » Setup Bypass TunnelGuard Check menu

Browser-Based Interface

- Java applet launches a pop-up browser window to display the Lightweight Directory Access Protocol (LDAP) server attributes to set LDAP authentication. (Q01667572)
  To set the LDAP attributes, enter the following:

  — CLI command:
  Not applicable

  — BBI path:
  SearchBaseUserAttribute, **GroupAttribute**, **GroupSearchBase**, and **MemberAttribute** under **VPN Gateways >> VPN # >> Auth Server-# [LDAP] >> Settings**
  Click **LDAP Browser** to launch LDAP browser.

Command Line Interface

- Uptime of all ISDs in a cluster can now be viewed using a single command. **Uptime** column in the isdlist output table shows uptime. (Q01677124-01)
  To view uptime of all ISDs, enter the following:

  — CLI command:
  `/info/isdlist`

  — BBI path:
  Dashboard » Cluster Status

- Imported custom contents can be viewed. (Q01753304)
  To view the custom content directory, enter the following:

  — CLI command:

  `/cfg/vpn #/portal/content/show`
  - BBI path:
    Access to Custom Content: under **VPN Gateways » VPN-# » Portal Custom Content**

- Users logged in using SSL through portal or Net Direct can be viewed. (Q01676487-01)
  To view the logged in users, enter the following:
  - CLI command:
    `/info/users` and enter `all`, `ssl` or `ipsec`
  - BBI path:
    Set **Users Login Type:** under **Monitor » Logged In Users**

Additional enhancements

- The command `/cfg/dump`, now displays the platform information along with the configuration data. (Q01251010)
- The virtual desktop can be enabled on a group basis. (Q01764073)
  To enable virtual desktop, enter the following:
  - CLI command:
    `/cfg/vpn #/vdesktop/ena` and enter on, off or group.

    > ***Note:*** In vdesktop new menu item is added and is visible only when the VPN setting for vdesktop is set to group. To set vdesktop status, enter `/cfg/vpn #/aaa/group #`

  - BBI path:
    VPN Gateways » VPN-# » Virtual Desktop
- The Virtual desktop supports Malware detection and connection control. These features are a part of the Virtual desktop licensing scheme. Connection control prevents all the traffic other than to portal VIP from within the Virtual desktop. (Q01762198)
  To set Malware detection and connection control, enter the following:
  - CLI command:
    `/cfg/vpn #/vdesktop/mcd` and `/cfg/vpn #/vdesktop/conncntrl`
  - BBI path:
    VPN Gateways » VPN-# » Malware Detection and **VPN Gateways » VPN-# » Virtual Desktop**
- The `groupfromuserdn` returns the Distinguished Name (DN) only when the Active Directory (AD) does not return any groups. This is enabled if the option is set to extract the group name from the DN. (Q01647905-02)

- Local authentication password enhancements done to indicate the password age, post warning when the password is due to expire. When password expires, the portal cannot be used until the password is changed and a pop-up dialogue box appears for new password with confirmation or error message if the password provided is correct or incorrect. Also, passwords are of minimum length and old passwords cannot be reused. (Q01576163-01)
  To set password age, password warning, and length of the password, enter the following:
  - — CLI command:
    `/cfg/vpn #/aaa/auth #/local/pwdage`
    `/cfg/vpn #/aaa/auth #/local/expirewarn`
    `/cfg/vpn #/aaa/auth #/local/pwdtext`
  - — BBI path:
    VPN Gateways >> VPN-# >> Auth-Server-# >> Password Change
- Filtering access to back-end resources is based on filename or file extension. (Q01616118-01)
  To set filename extension, enter the following:
  - — CLI command:
    `/cfg/vpn #/aaa/extspec`
  - — BBI path:
    VPN Gateways » VPN-# » Authorization » Filename Extension Specific Entries
- Administrators can configure HTTP authentication as an authentication method in NVG. The HTTP Authentication can be used for portal, IPsec, and Net Direct logon. The WWW-Authenticate handshake takes place resulting in the validation of credentials. If authentication is not enabled on the back-end HTTP server, the validation fails and the access is rejected. (Q01667081)
  To set HTTP authentication, enter the following:
  - — CLI command:
    `/cfg/vpn #/aaa/auth #/http`
  - — BBI path
    VPN Gateways » VPN-1 » Authorization » Services Add/Modify
- Support for logging 2000 syslog messages in the internal memory. (Q01616631)
- When the administrator tries to delete a user from local data base using the command `/cfg/vpn 1/aaa/auth local/local/del <username>` and if the user being deleted is an active user (active in portal aaa_cache list), a warning message appears. The administrator is prompted to confirm if the active user still needs to be deleted. The

administrator can delete or allow the active user in the local database by entering Yes or No respectively. (Q01614830-01)

- The Certificate Revocation List (CRL) is validated properly. (Q01616116-01)
  To configure CRL, enter the following:
  - CLI command:
    `/cfg/cert #/revoke/automatic/verify on`
  - BBI path:
    Certificates » Certificate-# » Automatic CRL
- While adding URLs to the blacklist, the URL is rewritten but the file contents are not. (Q01730718-01)
- The NVG supports the web application authored using Lotus Domino and Yahoo! SiteBuilder Javascript. (Q01743776-02)
- Information deleted by IEWiper cannot be recovered using the undelete tools. (Q01529704-01)
- When NVG rejects access to the portal based on ACL, a syslog/trace message is generated. The message includes the user name, rule number, and profile number that helps the administrator to identify the access deny reason. (Q01475298)
- Added capability to enter a LDAP server address by DNS name. (Q00975670-01)
  To add LDAP server by DNS name, enter the following:
  - CLI command:
    `/cfg/vpn #/aaa/auth #/ldap/servername`
  - BBI path:
    VPN Gateways » VPN-# » Auth Server-# » General
    (Q01782407-01)
- The number of IP pools is increased to 1024 and this value is applicable across all VPNs. Also the number of IP pools for each VPN can be specified through the CLI command `numippool`. (Q01479508-01)
  To enable the number of IP pools to 1024, enter the following:
  - CLI command:
    `/cfg/sys/adm/enanumpool`

Documentation download

The complete set of NVG documentation is available for download from Nortel Customer Support website:

Step	Action
1	Point your browser to: http://www.nortel.com.
2	Under **Support and Training**, select **Technical Support > Technical Documentation**
3	Select **Security** and **VPN** from the list.
4	Select **VPN Gateway 3050 or VPN Gateway 3070** from the Virtual Private Networking (VPN), IPSEC, and SSL list.
5	Select the desired document from the Documentation.

--End--

Software installation and upgrade notice

SSL VPN Server Software

The SSL VPN server software is delivered in two different forms, as described following:

- `SSL-7.0.3.0-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 7.0.1 or later from an earlier version.

- `SSL-7.0.3.0-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 7.0.1 or later through the reinstall procedure.

Server Software Download

The server software is available for download from Nortel's Customer Support website. To access the site, proceed as follows:

Step	Action
1	Open **http://www.nortel.com**.

2 Under **Support and Training**, select **Technical Support > Software Downloads.**

3 Select **Security & VPN** from the list.

4 Select **VPN Gateway 3050** or **VPN Gateway 3070** from the Virtual Private Networking (VPN), IPsec, and SSL list.

5 Select the desired software release which you want to download.

6 Enter the user name and password.

> ***Note:*** Downloading the software requires registered user name and password that is assigned 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 website, and follow the 5-step registration process.

--End--

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) 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 website. In the three-step Product Finder guide, select Contivity VPN Client Software.

Upgrading from Release 6.x to 7.x on Nortel Application Switch 2424-SSL

New disk repartitioning feature is available for Releases 6.0.9.0 and later to accommodate the future releases. This is due to the increase in image size from Release 6.0.7.0a (and later) and limited storage space available in the NAS 2424-SSL. To upgrade from Releases 6.0.5.0, 6.0.7.0a, or 6.0.9.0 to Release 7.x there are specific upgrade procedures. For more information, see:

- "Upgrading Release 6.0.5.0 to 7.x" (page 19)
- "Upgrading Release 6.0.7.0a to 7.x" (page 19)
- "Upgrading Release 6.0.9.0 to 7.x" (page 20)

Upgrading Release 6.0.5.0 to 7.x

To upgrade Release 6.0.5.0 to 7.x:

Procedure steps

Step	Action
1	Upgrade to Release 6.0.9.0.
2	Run repartition command. For more information, see "Disk repartitioning required for Releases 5.x to 6.x on Nortel Application Switch 2424-SSL" (page 20).
3	Upgrade to Release 7.x .

--End--

> ***Note:*** The existing configuration is retained while upgrading directly from Release 6.0.5 to Release 7.x. But due to the image size without repartition it does not work with future releases.

Upgrading Release 6.0.7.0a to 7.x

The following are the options to upgrade Release 6.0.7.0a to 7.x:

- Upgrade through Release 7.x boot image.

  > ***Note:*** After upgrade, the configurations are lost.

- Use the following procedure to upgrade:

Procedure steps

Step	Action
1	Downgrade to Release 6.0.5.
2	Upgrade to Release 6.0.9.0.
3	Run repartition command.

For more information, see “Disk repartitioning required for Releases 5.x to 6.x on Nortel Application Switch 2424-SSL” (page 20).

4 Upgrade to Release 7.x.

--End--

Upgrading Release 6.0.9.0 to 7.x

To upgrade Release 6.0.9.0 to 7.x:

Procedure steps

Step	Action
1	Run repartition command. For more information, see “Disk repartitioning required for Releases 5.x to 6.x on Nortel Application Switch 2424-SSL” (page 20).
2	Upgrade to Release 7.x.

--End--

Disk repartitioning required for Releases 5.x to 6.x on Nortel Application Switch 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 5.x version to be installed simultaneously with version 4.x. It is not 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 preceding 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 gives an error if one or more systems of the preceding type are running in the cluster, listing the hosts that need disk repartitioning.

To support the repartitioning procedure, the following commands are present in version 4.2.1.11:

- **`/boot/software/repartcheck`**
  Checks 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", that is not shown in the menu or considered for auto-completion through <TAB>, they cannot be used in normal operation. Repartition includes two automatic reboots, the host is effectively out of service.

The time required for the repartition is approximately 7 to 10 minutes.

> ***Note 1:*** 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 2:*** 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 3:*** 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 repartitioning 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 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 7.0 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 6.0.1 will be filtered out during the downgrade.
- If Net Direct, IE Wiper and/or Citrix Metaframe support has been set to **`group`** (see), the setting will be changed to the respective default value.
- The TunnelGuard pre-defined SRS entries will be lost, if the software is downgraded from 7.0.x release to 6.0.x or 5.1.x release. The pre-defined SRS is introduced for the first time in 7.0.x as OPSWAT feature. It is recommended to delete the pre-defined SRS entries from TG SRS rule definitions before downgrade.
- During upgrade and downgrade, the cached version of TG admin applet can be invoked. It is recommended to delete the browser cache.
- Single TunnelGuard SRS data cannot have more than 255 pre-defined software entries.
- Due to changes in RADIUS accounting server information in the configuration. Downgrade to 6.0.x and 5.0.x release and upgrade to 7.0.x will cause RADIUS server information inconsistency. Administrator must re-configure the RADIUS account server again once upgrade back to 7.0.x again.

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 to make use of the extra 40 number of users in the default license.

Downgrade IE Cache Wiper and Net Direct Cab files

If the server is downgraded, the upgraded version will not be cleaned up. That is, the object files, the IE cache wiper, and the Net Direct file is same and shows the upgraded version. You have to manually delete the IE Wiper Control and Net Direct .cab files. Follow these steps to delete the files:

Step	Action
1	Open Internet explorer.
2	Select **Tools**. Drop-down menu appears.
3	Select **Internet Options**.
4	Click **Settings**.
5	Click **View Objects**.
6	Select the files and remove.

--End--

Supported software platforms

The 7.0.3 server software is currently supported on the following hardware platforms:

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

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 preceding 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 since version 7.0.1.

- The `Print` command does not display `access rules`. (Q01799436)
- The Java Net Direct window automatically minimizes after it connects. (Q01531182-01)
- When server is upgraded with syslog server configured it fails. (Q01823300)
- The Net Direct client drops and restarts. (Q01788219)
- Administrators using Windows Vista cannot launch Net Direct. (Q01590870-01)
- Port forwarder does not work and the error message "**Authentication with proxy failed**" appears. (Q01808013)
- The BBI displays error message, "**LDAP Server Not configured**" when LDAP server is added. (Q01782407-01)
- When Net Direct caching is enabled, empty license banner is displayed. (Q01772169)
- The Samba client crashes when the system starts. (Q01765214)
- For proxy link setting, the validation checked does not match the info provided in BBI (Q01434147-01)
- In Nortel VPN 3070, client authentication is required with client certificate. This works fine if the client sends only the client certificate. Authentication fails if the client sends a certificate chain along with the issuer certificates. (Q01509534-01)
- Net Direct (NDIC/ActiveX) client is not compatible with Kaspersky Antivirus and other Internet security programs. (Q01531880-01)
- In VPN 1000 module, test/quick VPNs are not accessible after upgrading to 7.0.3. (Q01752167)
- The VPN 1000 card with Net Direct proxy ARP does not work correctly with NVR. (Q01743159-01)

- The error message, "**Catastrophic failure**" appears while sending E-mail using OWA (Outlook Web Access) with S/MIME client PC plugins. (Q01743719-01)
- Error occurs while upgrading. The System.Web.HttpException is unable to validate data. (Q01647178-01)
- The SSL web application fails. (Q01565698-01)
- Cluster manager does not sync with the network and service names in access lists. (Q01665748-01)
- The PF link window does not auto minimize. (Q01622704-01)
- The iauto to Exchange Server 2007 with Internet Explorer does not work correctly. (Q01591376-01)
- When split tunneling is enabled, Net Direct does not add the networks configured in the routing table of the PC. (Q01425656-01)
- Port forwarder fails with errors while using SSL chain certificate. (Q01128789-02)
- The IP address is not returned through SBR radius. (Q01565880-01)
- The NVG is not able to rewrite dynamic javascript correctly. (Q01598751-01)
- The Employee Self Service (ESS) application does not work correctly after upgrading the Application Switch SSL 2424 to code version 23.0.2 and SSL version 5.1.5.3. (Q01561899-01)
- The NVG does not work correctly for files of length greater than 64 K. (Q01480610-02)
- Corrupted message about IECacheWiper appears while using Japanese template. (Q01504940-01)
- NVG issues a redirect when web form uses HTTP Post method. (Q01426162-03)
- After upgrading the NVG software, the links are not processed correctly by the HTML rewriter. (Q01564715-01)
- The urlobscure breaks portal home page when the internal link is present in linkset. (Q01573279-01)
- The date/time changes do not reflect correctly in the In-memory log. (Q01733429)
- In BBI, when the mouse is moved over the input fields the relevant help information is not displayed. (Q01733285)
- In BBI, under **VPN Gateways >> VPN # >> Vdesktop**, the help information is not displayed for mcd command. (Q01812331)

- The NDIC fails to connect to additional VPN Gateways when the first gateway is unresponsive. (Q01531149-01)
- The SSL VPN portal links does not work correctly. (Q01489842-01)

Known limitations

VPN Limitation

VPN Gateway Release 7.0.3 supports 256 VPNs, even though the CLI and Web UI allows you to create 1024 VPNs. Therefore, the user should create up to 256 VPNs only.

Browser Requirements

When using the NVG software for basic Portal access, that is when not using the applets, the following browsers are recommended:

Basic Portal Access (no applets)

When using the NVG software for basic Portal access, that is when not using the applets, 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

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 7.0 or later
Mozilla 1.5 or later
Firefox 1.0
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 7.0 or later
  Mozilla 1.5 or later
  Firefox 1.0
- Unix/Linux:
  Netscape Navigator 7.0 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
- Internet Explorer and FireFox for Vista is supported for administrator user only.

The following Linux distributions and Kernel versions 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

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.
- Mobility Feature is not supported for MAC and Linux platforms.
- Portal Net Direct in Vista will not work for non-administrator user. Installable Net Direct has to be used instead. For Portal Net Direct to work in Vista for user with administrator rights follow these steps:

Step	Action
1	Go to the Control Panel.
2	Click **User Account** and **Family safety**.
3	Click **User accounts.**
4	Turn User Control On or Off.
5	Uncheck **Use User Control (UAC) to protect your computer**.
6	Click OK and restart the Vista Client.
7	Launch the Net Direct.

--End--

TunnelGuard Agent

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

Special notice for customers using both Nortel VPN Gateway (NVG) release 7.0.3 and Nortel Secure Network Access (NSNA) release 1.6.1 products

The installable TunnelGuard 4.0 client shipped with this release does not have all of the functionality contained in TunnelGuard 3.5 that was shipped with Nortel NSNA 1.6.1 Customers who need complete NSNA 1.6.1 and NVG 7.0.3 functionality should use version 4.5 of TunnelGuard which includes the full functionality of both TunnelGuard releases. Customer can get the software through their normal support channels

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, 5.0, 5.11, 6.01, 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), 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 command:

`/cfg/vpn #/sslclient/tdiclient` and **`lspclient`** (these commands currently have no effect) and **`cfg/vpn #/sslclient/oldclients`**

— BBI path:
VPN Gateways >> VPN # >> TDI Client and LSP Client (these options currently have no effect) and **VPN Gateways >> VPN # >> 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, for example 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 (for example NetMeeting, FTP and all streaming media) are not supported by the Port forwarder feature. Applications using *static* port number allocation (for example DNS, SNMP) are supported.
- When specifying a URL without a path for an iauto (automatic login) link, for example 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 (that is 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 (that is 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, for example 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".

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 TunnelGuard agent, the result of the TunnelGuard 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 TunnelGuard check is run.

Known issues

This section lists known issues with the NVG software.

- The NVG fails after creating 258 VPNs. (Q01752153)
- When 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 coming future releases, the ClearTrust server pools on the NVG will be refreshed periodically. (Q01341793)
- 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, that is 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)
- The output for command **`/maint/starttrace`** is not available in WebUI. (Q01475271)
- Problem with Internet Explorer version 7.0.2800.1106.xpsp2_gdr.04051 7-1325.
  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 (for example 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. To set the tun node, run the following commands as root:
  ```
  mkdir /dev/net mknod /dev/net/tun c 10 200
  ```
  (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`**. (Q01278965)

- 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 future release. (Q01341831)
- 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.
- 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 the remote user runs an old version of installable Net Direct client, there is no message displayed to upgrade or continue the old version. This will be fixed in future release.
- Error appears when Net Direct is connected with vdesktop enabled. (Q01546498)
- There is reconnection issue in Net Direct. (Q01619895)
- CLI session does not time out automatically in VPN 1000 module. (Q01300186)
- VPN+2 groups+diff mobility time per group-ND gets crashed while launching. So it is recommended to set Roaming values only on per-VPN basis. There is a known issue if we set Roaming values based on per-group basis. (Q01747740)
- If the VPN 3050 is upgraded to version 6.0.7.0 it does not work correctly. (Q01721644-01)
- When configuring to add User Preferences Attribute to AD the nortelSSLOffload class cannot be added to the User Class. (Q01801966)

Known documentation issues

Changes affecting the customer documentation will be addressed in the delivery of Release 7.1 document suite.

- 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.

Known anomalies

This section contains known issues where there are no plans to resolve.

- When the command `\!` is entered for sharing, the error message "`%5C%21`" appears. (Q01311087-01)
- While accessing Net Direct for the first time, error "**Route table cannot be altered when Net Direct is active trying to reconnect**" appears. (Q01297873-01)
- NVG software re-image using bootshell causes **`/cfg/cert`** option to disappear. (Q01800810-01)
- Rewrite fails on Siemens MagicWeb. (Q01513601)
- In SSL Acceleration mode (type=http), the secure option on the session cookie was introduced in v4.2.1.11 and it can be controlled by /cfg/ssl/server #/http/securecook <on/off>. The old behavior in software versions prior to 4.2.1.11 is OFF. Also, in 4.2.1.11 and later (4.x, 5.1, 6.0), the default value of "securecook" is OFF. But if the software version earlier than 4.2.1.6 to 4.2.x later than 4.2.1.11 or 5.1 or 6.0 is upgraded, the value of "secorecook" is set to ON. (Q01452086-01)
- Net Direct is only adding the first dns server in the list, so for example, if the search list containing alteonlab.com, netslab.com, abctest.com, is configured, after connecting, only alteonlab.com is seen against the adapter. In the Winxp registry under the path My computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters SearchList value is, alteonlab.com (Q01731956)

Related documentation

- *VPN Gateway 7.0 Users Guide*
  (NN46120-104) (part number 216368-F, September 2007)
- *VPN Gateway 7.0 Command Reference*
  (NN46120-103) (part number 216369-E, September 2007)
- *VPN Gateway 7.0 Application Guide for SSL Acceleration*
  (NN46120-100) (part number 216370, September 2007)
- *VPN Gateway 7.0 CLI (Command Line Interface) Application Guide for VPN*
  (NN46120-101) (part number 216371-E, September 2007)
- *VPN Gateway 7.0 BBI (Browser-Based Interface) Application Guide for VPN*
  (NN46120-102) (part number 217239-D, September 2007)
- *VPN Gateway 7.0 VPN Administrators Guide*
  (NN46120-105) (part number 217238-D, September 2007)
- *VPN Gateway 3050/3070 Hardware Installation Guide*
  (part number 216213-B, March 2005)
- *VPN Gateway 7.0 Troubleshooting Guide*
  (NN46120-700) (part number 324371-A, November 2007)

How to get help

Getting Help from the Nortel website

The best way to get technical support for Nortel products is from the Nortel Technical Support website:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. The following can be accessed from the Nortel website:

- download software, documentation, and product bulletins
- search the Technical Support website and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting Help through a Nortel distributor or reseller

If a service contract for the Nortel product is purchased from a distributor or from an authorized reseller, contact the technical support staff for the distributor or reseller.

Getting Help over the phone from a Nortel Solutions Center

If the required information is not available in the Nortel Technical Support website, and if there is a Nortel support contract, then the help can be obtained over the phone from the Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7865).

Outside North America, go to the following website to obtain the phone number for that region:

http://www.nortel.com/help/contact/global/index.html

Getting Help from a specialist by using an Express Routing Code

An Express Routing Code (ERC) is available for many Nortel products and services. When an ERC is used, the call is routed to a technical support person who specializes in supporting that product or service. To locate the ERC for the product or service, go to:

www.nortel.com/erc

Nortel VPN Gateway

Release Notes

Release: 7.0.3
Publication: NN46120-400
Document status: Standard
Document revision: 01.06
Document release date: 17 April 2008

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

www.nortel.com

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Trademarks

*Nortel, Nortel Networks, the Nortel logo and the Globemark are trademarks of Nortel Networks.

Java runtime environment and JRE are registered trademark of Sun Microsystems.

Lotus Domino is the registered trademark of IBM.

Yahoo! is the registered trademark of Yahoo.

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 ().

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 .

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 *Users Guide* for more information.