

Nortel VPN Gateway 5.1.7

Release Notes

part number: 216372-H, May 2006

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

Copyright © 2006 Nortel Networks. All rights reserved.

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.

Nortel Application Switch, Nortel 2208, Nortel 2216, Nortel 2224, Nortel 2424, Nortel 2424-SSL, Nortel 3408, Nortel 180, Nortel 180e, Nortel 184, Nortel AD3, Nortel AD4, and ACEswitch are trademarks of Nortel, Inc. in the United States and certain other countries.

BEA, and WebLogic are registered trademarks of BEA Systems, Inc.
Netegrity SiteMinder® is a trademark of Netegrity, Inc.
CryptoSwift® HSM is a registered trademark of Rainbow Technologies, Inc.
Portions of this manual are Copyright 2001 Rainbow Technologies, Inc. All rights reserved.
Any other trademarks appearing in this manual are owned by their respective companies.

Export

This product, software and related technology is subject to U.S. export control and may be subject to export or import regulations in other countries. Purchaser must strictly comply with all such laws and regulations. A license to export or reexport may be required by the U.S. Department of Commerce.

Licensing

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes a TAP-Win32 driver derived from the CIPE-Win32 kernel driver, Copyright © Damion K. Wilson, and is licensed under the GPL.

See Appendix D, “License Information”, in the *User’s Guide* for more information

Release Notes

These Release Notes provide the latest information regarding your Nortel VPN Gateway (NVG) with version 5.1.7 software. This supplement lists the new features/fixes and modifies some information found in the complete documentation:

- *VPN Gateway 5.1 User's Guide*
  (part number 216368-C, March 2005)
- *VPN Gateway 5.1 Command Reference*
  (part number 216369-C, March 2005)
- *VPN Gateway 5.1 Application Guide for SSL Acceleration*
  (part number 216370-C, March 2005)
- *VPN Gateway 5.1 CLI Application Guide for VPN*
  (part number 216371-C, March 2005)
- *VPN Gateway 5.1 BBI Application Guide for VPN*
  (part number 217239-B, March 2005)
- *VPN Gateway 5.1 VPN Administrator's Guide*
  (part number 217238-B, March 2005)
- *VPN Gateway 3050/3070 Hardware Installation Guide*
  (part number 216213-B, March 2005)
- *Configuring Tunnel Guard Guide*
  (part number 317017-A, August 2003)

Documentation Download

These manuals are available for download from Nortel's Customer Support Web site:

1. **Point your browser to: http://www.nortel.com.**
2. **Under Support and Training, select Technical Support>Technical Documentation.**
3. **In the first step of the three-step Product Finder guide, choose 'Select from Product Families' in the list box.**
4. **Then select the following:**

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

New Features/Enhancements

This section lists features and enhancements added since version 5.1.5. Note that these features are not documented in the 5.1 manuals listed on page 3.

- 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)
- 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`

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)
- Syslog messages added. A syslog message is now generated when the SiteMinder agent is timed out during initialization, when the SiteMinder agent is timed out during authentication request, and when login time reaches a quarter of the Siteminder timeout value.
- Fixed port range acceptance. A backward port range like 89-80 is not allowed for the following command. `/cfg/vpn #/aaa/service`
(CR Q01173644)
- Fixed packets sent to client with interface IP source address. In some cases, during the SSL-VPN logout procedure, packets could be sent to the client using the public interface IP address rather than the VIP as source address. This has only been observed on SSL-VPN when using a special test client.
(CR Q01227011)
- Fixed `oper` CLI user rights. The `oper` CLI user no longer has access to the following commands: `/cfg/sys/dns`, `/cfg/lang/import,export,vlist,del`, `/cfg/quick` and `/cfg/test`.
(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 the Citrix Java applet. Previously, the Citrix Java applet used an old regedit proxy extraction method that required administrator rights. Now the applet uses the getproxy utility, i.e. the same method as the regular port forwarder applets.
  (CR Q01285170)

- The Java applets have been re-signed with certificates that are valid until January 2008. (CR Q01281857)
- Fixed reverse rewrite problem. Previously, a reverse rewrite problem caused a customer-specific application to not load pages correctly.
- 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.
- Fixed problem with rewritten URL links in forwarded e-mails. Previously, rewritten URL links in forwarded e-mails could not be clicked by users who were not running through the NVG. This has now been fixed. (CR Q01260321-01 and Q01267751)
- Fixed problem with simpleproxy crashes. Rewrite of spanned internal buffers could in rare cases cause the simpleproxy to crash. (The simpleproxy is the NVG’s engine, responsible for connecting, disconnecting, rewriting etc.).

Portal

- Fixed non-translated messages in the Portal. Error messages given on failed login to the portal were not translated. (CR Q01177727)
- Fixed problem with starting applets from multiple portals. Previously, when starting applets from more then one Portal in the same browser session, applets from the second Portal would stay pending with the message "Applet is initializing, please wait". (CR Q01288347)

- 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)
- Fixed problem with shutting down the Port forwarder applet window. Previously, when the application that was started using the port forwarder was shut down, the Port forwarder applet window was not shut down. Now this has been fixed for applications started directly from the port forwarder (i.e. not for applications is started by way of a port forwarder via the Command window(cmd)).
  (CR Q01082046)

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 port forwarder failure. If a certificate in the CaChain had not set the Path Length Constraint value, a port forwarder would fail when setting up the tunnel.
  (CR Q01262835)
- 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 file names including special characters (e.g. `@#$%foo.txt`) to SMB and FTP file servers.
  (CR Q01161886)
- Fixed problem with SMB servers not working when a directory name starts with a period, for example `.files`.
  (CR Q01287834)
- Fixed Japanese directory and file deletion error. On deleting directories and files with Japanese names from SMB and FTP servers, the deletion was successful but error messages were displayed. The paths are properly encoded now.
  (CR Q01195775)
- 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 memory allocation bug in the MD4 code when doing NTLM authentication. An incorrect memory allocation could potentially cause a system crash/restart.
- Fixed Siteminder Agent premature timeouts and cyclic restarts. In the event of a Policy Server becoming unreachable, the AAA subsystem would restart the Siteminder Agent due to long response times. In some cases it would go into a state of continuously restarting the Siteminder Agent before it could initialize properly. The Siteminder Agent API has also been upgraded (5.50.0323.860) to provide faster initialization when Policy Servers are unavailable.
  (CR Q01253126)

- 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)
- Fixed Single Sign-On (SSO) setting for SiteMinder authentication. Setting `/cfg/vpn #/aaa/auth #/siteminder/sso` (VPN Gateways>Authentication>SiteMinder>SiteMinder Settings (Allow Single Sign-On) to `true` could revert to the default value of `false` when the system was rebooted.
- Fixed problem with import of local database. Previously, the `/cfg/vpn #/aaa/auth #/local/import` command imported a local database even if the password supplied on import was not the same as the export password. Note that a local database exported prior to this release will not be possible to import.
- Fixed problem with the NVG sending an NTLM message type 1 to a backend server if the backend server is included in the SSO (single sign-on) domain. If the backend server did not require authentication, it would send a HTTP 200 reply message. The NVG, expecting an NTLM type 1 message reply, shut down the connection resulting in no data was sent back to the client.
(Case number 051213-82708)
- Removed possible deadlock situation when using LDAPS (LDAP over SSL) authentication.
- The default group is now also used for IPsec client certificate authentication if no groups are found based on the client certificate.
CLI path: `/cfg/vpn #/aaa/defgroup`
BBI path: VPN Gateways>Group Settings>Groups

- Previously, if using LDAP expired account check (`/cfg/vpn #/aaa/auth/ldap /activedire/enaexpired` or VPN Gateways>Authentication>LDAP>Active Directory (Expired Account Check)), the Portal would sometimes display an error message when the user logged back into the Portal after having acknowledged the expired password pop-up window and logged out. This behaviour was however only seen when `/cfg/vpn #/portal/ieclear` (VPN Gateways>Portal Display>General (Use IE Clear Authentication Cache)) was set to off. The problem is now fixed.
  (CR Q01343602)

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)
- Fixed problem with BBI system hanging when the Traceroute operation is performed in Secure Service Partitioning configurations (under VPN Gateways>Gateway Setup>Trace).
  (CR Q01252770)
- The BBI login menu can now be accessed by SSL VPN Module 1000 users.
  (CR Q01326933)
- Fixed problem with sorting the CA certificate chain in the BBI. Previously, the certificates were sorted by reference number, even if you had saved the certificates according to the preferred chain order. This would result in the CLI displaying the order as e.g. 29,27, while the BBI displayed the order as 27,29.
  (CR Q01345254)

Software Installation and Upgrade Notice

VPN Gateway Server Software

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

- `SSL-5.1.7-upgrade_complete.pkg`

  Using this package is the preferred method for upgrading an existing NVG cluster, as the upgrade is propagated across the cluster and all current configuration is preserved.

  The upgrade procedure is described in "Performing Minor/Major Release Upgrades" in Chapter 4 in the *VPN Gateway User's Guide*.

- `SSL-5.1.7-boot.img`

  Using this image will reset the VPN Gateway to its factory default configuration. It must be used when an VPN Gateway with a different software installed is to be added to a cluster, to bring the additional device to the same software version as in the cluster before joining it to the cluster.

  The software reinstall procedure is described in "Reinstalling the Software" in Chapter 3 in the *VPN Gateway User's Guide*.

Server Software Download

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

1. **Point your browser to: http://www.nortel.com.**
2. **Under Support and Training, select Software Downloads.**
3. **In the first step of the three-step Product Finder guide, choose 'Select from Product Families' in the list box.**
4. **Then select one of the following:**

   VPN Gateway ▸ VPN Gateway 3050/3070 ▸ Software

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

   Downloading software requires that you enter the registered user name and password previously assigned to you by Nortel Customer Support. If you are not a registered user at Nortel, click on **Register** on the left-hand column of the Nortel's Customer Support Web site, and follow the 5-step registration process.

Nortel SSL VPN Client

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

The SSL VPN client comes in two versions (for limitations, see page 18):

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

Nortel IPsec VPN Client (formerly Contivity VPN Client)

The IPsec VPN client can be downloaded from Nortel's Customer Support Web site. In the three-step Product Finder guide, select **Contivity ▸ VPN Client ▸ Software.**

Disk Repartitioning Required for Version 5.x on Some Systems

This applies to the following systems:

- ASA 310, ASA 310 FIPS, ASA 410, delivered with a software version prior to 4.0 pre-installed
- AAS 2424-SSL delivered with a software version prior to 5.0 pre-installed.

On these systems, the existing disk partitioning does not allow for a 5.x version to be installed simultaneously with version 4.2 or later. I.e. it isn't possible to do a standard upgrade from 4.2 to 5.x, or from one version of 5.x to another. Upgrade from versions earlier than 4.2 to 5.x, and software reinstall using a 5.x version, is still possible.

Hence, the following applies regarding standard upgrade to version 5.x from versions prior to 5.0 for clusters that include systems of the above type:

Current version	Procedure
4.1.x or earlier	Upgrade to 5.x, and repartition before subsequent upgrade
4.2.x before 4.2.1.11	Upgrade to 4.2.1.11 or later 4.x, repartition, and then upgrade to 5.x.
4.2.1.11 or later 4.x	Repartition before upgrade to 5.x.

When 5.x is installed, the `/boot/software/download` command will give an error if one or more systems of the above type are running in the cluster, listing the hosts that need disk repartitioning.

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

- `/boot/software/repartcheck`
  Checks for and reports hosts in the cluster that need repartitioning.
- `/boot/repartition`
  Initiates repartitioning for the local host.
- `/cfg/sys/cluster/host #/repartition` (in version 4.2)
  `/cfg/sys/host #/repartition` (in version 5.x)
  Initiates repartitioning for the given host (which must be running).

These commands are “hidden”, i.e. not shown in the menu or considered for auto-completion via <TAB>, since they shouldn't be used in normal operation. During the repartition, which includes two automatic reboots, the host will effectively be out of service.

The time required for the repartition is approximately:

- 4-5 minutes for ASA
- 7-10 minutes for AAS 2424-SSL

NOTE – It is vitally important to avoid power cycle, reset, or any other manually initiated reboot of the host while the repartition procedure is running - this may lead to a totally non-functional system.

NOTE – On the AAS 2424-SSL, after repartition is completed, it will not be possible to down-grade to software versions prior to 4.2.1.8, even via software reinstall.

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

Upgrading from Versions Earlier than 2.0.11.15

If you are currently running a software version earlier than 2.0.11.15, upgrade to version 2.0.11.15 (or a later 2.0.11.x version) prior to upgrading to version 3.x or later. The “intermediate” upgrade to version 2.0.11.15 is necessary in order to maintain your current configuration, and to provide reliable fallback in case the upgrade should fail.

Downgrading to Versions Prior to 5.0

SSL VPN clusters running software version 5.x or later cannot be downgraded to software version 4.x or earlier and still retain the configuration. To downgrade such a cluster to a version lower than 5.0, a complete software reinstall using the boot.img must be performed, followed by manual reconfiguration of the cluster. This is due to changes in the internal database format.

Supported Hardware Platforms

The VPN Gateway 5.1.7 server software version is currently supported on the following hardware platforms:

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

TFTP Server Support

- The following TFTP server (for Microsoft Windows 95/NT) has been tested and verified to handle the upgrade process correctly:
  - TFTPd32 software (use any search engine to search for "`tftpd32`")
- The following TFTP server software are *not* supported when upgrading the SSL VPN software:
  - Cisco TFTP server software (for Microsoft Windows 95/98/NT)
  - 3Com TFTP server software (for MS-DOS 5.x or higher)

Known Limitations

Browser Requirements

Basic Portal Access (no applets)

When using the NVG software for basic portal access, i.e. when not using the applets (see below), the following browsers are recommended:

- Internet Explorer 5 or later
- Mozilla 1.1 or later
- Netscape 4 or later
- Firefox
- Opera

Applet Support

To support the Telnet/SSH Access, HTTP Proxy, FTP Proxy, Port forwarder and Citrix applets, the following browser and Java combinations are recommended:

- Windows:
  Internet Explorer 5 or later with Microsoft's JVM 4 or later Sun's JRE 1.4.2 or later
  Mozilla 1.5 or later with Sun's JRE 1.4.2 or later
  Firefox with Microsoft's JVM 4 or later or Sun's JRE 1.4.2 or later
- Unix/Linux:
  Mozilla 1.5 or later with Sun's JRE 1.4.2 or later
  Firefox with Sun's JRE 1.4.2 or later

Tunnel Guard Applet Support

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

The following browsers support the Tunnel Guard management applet (used for configuring SRS rules):

Windows:
Internet Explorer 5.5 or later
Netscape Navigator 7.1 or later
Mozilla 1.5 or later
Firefox 1.0
Java 1.4.2 or later is required

BBI Support

Configuration via the Browser-Based Management Interface (BBI) is supported when the following browsers are used:

- Windows:
  Internet Explorer 5.5 or later
  Netscape Navigator 7.1 or later
  Mozilla 1.5 or later
  Firefox 1.0
- Unix/Linux:
  Netscape Navigator 7.1 or later
  Mozilla 1.5 or later

Net Direct Client

- The Net Direct client is only supported on Internet Explorer running on Windows 2000 and Windows XP.
- To be able to install and run the Net Direct agent, the remote user should have administrator rights on the client PC.

Tunnel Guard

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

Nortel IPsec VPN Client (formerly the Contivity VPN Client)

- For IPsec termination on the VPN Gateway, the following Nortel IPsec VPN client versions have been tested: 4.15, 4.86, 4.91, 5.01 and 5.11.
- For use with the Portal's Full Access feature, version 4.91 and later are supported.

Nortel SSL VPN Client

The installable SSL VPN client comes in two versions:

- Version 1.1.0.4 (LSP client): Compatible with Windows 98, ME, NT (with IE 5 or later), and XP. This client does not support UDP.
- Version 1.5.0.9 (TDI client): Compatible with Windows 2000 and XP. This client supports UDP as well as TCP. Native Microsoft Outlook is not supported because not fully qualified domain names cannot be resolved.

License

The license is not part of the configuration and will not be included when exporting the configuration using the `/cfg/ptcfg` CLI command or Operation>Configuration (Export Cluster Configuration) in the BBI. If a configuration is deleted, the license will be deleted as well.

Portal

- Sun's JRE earlier than 1.4 cannot download any applets from the VPN Gateway if the device has been setup to use a key length above 4096. This is supported in the native Microsoft JVM and may be supported in Sun's JRE 1.5 (yet unclear).
- Proxy chaining (option to specify an intermediate HTTP Proxy host and port, e.g. for the Portal's Telnet/SSH and Custom Port forwarder features) is only supported if SSL is enabled on the portal server.
- Proxy chaining is not supported for the Outlook Port forwarder feature.
- Microsoft Outlook 2003 is not supported when using the Outlook Port forwarder in combination with Exchange 2003.
- Running the Outlook Port forwarder on a Windows 2000 client requires installing the latest service pack for the operating system.

- Applications using *dynamic* UDP port number allocation (e.g. NetMeeting, FTP and all streaming media) are not supported by the Port forwarder feature. Applications using *static* port number allocation (e.g. DNS, SNMP) are supported.
- When specifying a URL without a path for an iauto (automatic login) link, e.g. http://www.example.com, enter the URL as `http://www.example.com/`. This will ensure that the root path is implied in the link. Iauto links are created using the `/cfg/vpn #/linkset #/link #/iauto` command in the CLI and under VPN Gateways>Portal Linksets>Links (Internal Auto Login URL) in the BBI.
- When an iauto link should be used for login to web servers using two-tier basic authentication with domain (i.e. one field for domain\user and one for password), the `/cfg /vpn #/linkset #/link #/iauto/mode` command must be set to `add_domain`. In the BBI, go to VPN Gateways>Portal Linksets>Links>Iauto>Auto Configuration. Under Internal Auto Configuration, in the Mode List box, select add_domain.
- Creating a Port forwarder link for mapping a network drive is not supported on Windows 98 and XP clients.
- The features available on the Portal's Advanced tab (i.e. Telnet/SSH access, FTP Proxy, HTTP Proxy and Port forwarder) are supported only with SSL v3 and cipher type RC4-MD5.
- The features available on the Portal's Advanced tab are not supported for the TLS protocol.
- To create a Port forwarder link for mapping a network drive – and the link is to be used on a Windows 2003 server acting as client – port 445 has to be used instead of the suggested port 139. On the Windows 2003 server, port 445 should be disabled by following these steps:
  - Click Start, select Run and enter `regedit`. The registry editor is started.
  - Locate and select the following key: `HKLM\System\CurrentControlSet\Services\NetBT\Parameters`.
  - On the right panel, double-click the `TransportBindName` entry.
  - In the **Edit string** dialog, delete the displayed value. No value should be specified.
  - Click OK, exit the registry editor and restart the computer.
- Some SSH versions may not be supported when using the SSH feature on the Portal's Advanced tab, e.g. Alteon 184 SSH-1.5-1.2.27.
- Some of Microsoft's Telnet server versions may not be supported when using the Telnet feature on the Portal's Advanced tab.

- To create a WTS port forwarder link that works on Windows XP systems that have not yet been upgraded to Service Pack 2, configure the port forwarder to listen on 127.0.0.2 instead of 127.0.0.1 (localhost). Then configure the Remote Desktop client to connect to 127.0.0.2. With the Windows XP SP2 version of the Remote Desktop client, it is possible to connect to 127.0.0.1 (localhost) as long as the port being used is other than the default (3389). Note that connections through 127.0.0.2 do not work on Windows XP SP2.

General

A maximum of 32,000 sessions is allowed on the VPN Gateway 3070 with 2 GB RAM.

Known Issues

This section lists known issues with software version 5.1.7.

For the Full Access feature to work, the fully qualified domain name (FQDN) of the VPN *must* be specified as the server alias in the SSL VPN client (Servers tab>Add>Alias field). (Q01043664)