Nortel VPN Gateway

Release Notes - Software Release 7.0.7.0

Release: 7.0.7.0
Document Revision: 01.09

www.nortel.com

NN46120-400

Nortel VPN Gateway
Release: 7.0.7.0
Publication: NN46120-400
Document release date: 19 December 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 7.0.7.0 software. These release notes detail the added feature enhancements, resolved issues, known issues, known anomalies, and known limitations since Release 7.0.3.

For a list of related publications, see "Related documentation" (page 39). The documentation suite for NVG 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 41).

The following topics are discussed in this document:

New feature enhancements for Release 7.0.7.0

This section lists software feature enhancements added in version 7.0.7.0

SSL

- The command /maint/tsdmp creates a dump of the local information, status of nodes , statistics, events and alarms, and configuration in one place. The results of the CLI commands, /info/local, /info/isdlist, /stats/dump, /info/events/cur, /cfg/dump are displayed one after the other (Q00980212).

  CLI path: /maint/tsdmp

- Syslog message is generated for a successful and failed SSL connection.New command (log) will enable the users to enable or disable the logging functionality. (Q01899479 & Q01899480)

  CLI path: /cfg/ssl/server #/ssl/log
  Default Value is none.

  Other options are:
  accept - Generate syslog only for successful SSL connections
  reject - Generate syslog only for unsuccessful SSL connections
  both - Generate syslog for both successful and unsuccessful SSL connections

IP Pool

- When the remaining IP’s in pool reaches 10% of the configured IP pool range, a syslog message will be generated.(Q01320410).

LDAP

- 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 LDAP password change feature for IPSec users added as part of 7.0.5 is enhanced to have the following features:
  - — The user account is used for binding with the MSAD servers rather than the isdbinddn account which is configured for the LDAP auth server. This helps in avoiding the overhead in configuring/giving the permissions to the isdbinddn account in the MS AD to update the password for other users. (Q01946867).
  - — Whenever a user logs in and the password is already expired for that user, the user password change popup is thrown to the user and after the password change the user is moved to the proper group returned by the LDAP server rather than having in the password expired group. But this will not change the ip allocated to the user, which will be in the password expired group. All the user tunnel details (under /cfg/vpn #/ipsec/utunprof #/) like split nets, split tuns, banners, mobility, client PC menu details (like screensaver password, store password) and client policies inside the user tunnel menu will not be updated to the client. These details will be matching the expired group user tunnel details only. But a logout and a login again will have the user placed in the proper group. (Q01935548)

Net Direct

- Net Direct provides authentication to NTLM proxy servers on Windows operating systems. Net Direct captures username, password and domain name on identifying NTLM proxy authentication (Q01529467).
- Net Direct Heartbeat feature is enhanced with silent keepalives over UDP. If Net Direct is using UDP as transport and no traffic is sent for a period of time, client-side and/or server-side NAPT routers/firewalls may timeout the corresponding UDP entries. This enhancement

enables silent keepalives to be sent from the Net Direct client (ND and ND installed clients) to prevent NAPT session time-outs. The interval of the keepalives can be configured via CLI.

CLI path: /cfg/vpn #/sslclient/keepalive
Default value is 0.

Existing heartbeat interval over TCP is also made configurable.
CLI path: /cfg/vpn #/server/tcp/sinterval
Default value is 1 minute.

Additional Enhancements

- In Cluster Manager, MAC address of each ISD in the cluster is included with the IP Address (Q01677067).
- Sequential Dual Authentication feature provides enhanced security by prompting portal users for dual authentication credentials to gain access to the portal. The portal user has to authenticate with two authentication servers sequentially in two distinct login pages. Once the user successfully authenticates with the primary authentication server, the second login screen will be displayed to enter login credentials for secondary authentication. If the secondary authentication fails, user will be prompted for retries before switching back to the primary login screen.

  This feature is limited to portal users, and is not supported for IPSec and Net Direct installed client users and is as per VPN setting.(Q01764154)

Sequential Authentication Menu:

enable - Enable / Disable sequential authentication

copyuser - Enforce same username for second auth

usesecond - Use secondary credentials for SSO and Iauto

retries- Number of retries for secondary login

CLI path:
cfg/vpn #/aaa/secauth

cfg/vpn #/aaa/seqauthorder

CLI command to configure secondary login text:
cfg/vpn #/portal/seclogtext

BBI path:
VPN Gateways » VPN-# » Sequential Authentication
VPN Gateways » VPN-# » Sequential Authentication Order

- Portal Domain Name Rewrite feature (Round Robin DNS feature) provides persistent connection within cluster to support inter-cluster load balance service. Persistent connection is provided once the initial contact is made to the NVG and does not provide inter-cluster session migration on failover. In a deployment scenario, multiple NVG boxes are clustered separately in different locations. To have persistent session with the same cluster, the administrator can configure the secondary DNS name which is associated to each cluster. Once the initial contact is made, the NVG will automatically replace the primary DNS name to secondary DNS name and further packets will always reach the same cluster and ensure persistent session within the cluster. Secondary DNS name in each cluster can be configured using the CLI command ’dnrewrite’. This feature does not work without proper DNS configuration.(Q01933149)

  CLI path: /cfg/vpn #/server/portal/dnrewrite

  BBI path: VPN Gateways » VPN-# » Portal » DomainRewrite

- Default Login Service Option feature allows the administrator to remove the "default" option from the portal drop down box. When default option is set to off, it mandates the display names to be configured for all authentication methods set in the authorder. (Q01922335)

  CLI path: /cfg/vpn #/aaa/defauthorder

  BBI path: VPN Gateways » VPN-# » Authentication Order » Default Authentication

- Bandwidth Test Tool for Novice User feature adds the bandwidth test tool in the portal of users classified as novice type. (Q01922341)

  CLI path: /cfg/vpn #/portal/usertype/novice/sysinfo

BBI path: VPN Gateways » VPN-# » Portal General » Sys Info and Bandwidth Test Tool for Novice User

- Add NVG Portal to Trusted Sites feature facilitates adding the VPN portal domain to the trusted sites of the Internet Explorer. When turned on, it downloads a signed ActiveX component in the login page and automatically adds the site to the trusted zone.
  Limitation: The automatic addition to trusted site will fail if IE protected mode is enabled.

  CLI path: /cfg/vpn #/portal/truststite

  BBI path: VPN Gateways » VPN-# » Portal General » Automatic Trusted Zone Addition:

- Configurable BBI Certificate feature enables to replace the default unsigned certificate used for the BBI interface with any certificate available in NVG. (Q01926303).

  CLI path: /cfg/sys/adm/https/cert

  BBI path: Administration » Remote Access » Web » Server Certificate

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-7.0.7.0-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* NN46120-104.

  > ***Note:*** TFTP cannot be used when upgrading to version 7.0.1 or later from an earlier version.

- `SSL-7.0.7.0-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* NN46120-104.

  > ***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 1.5.0.15 (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.

Disk repartitioning required for upgrade from Release 7.x to 7.0.7.0 and viceversa on NVG 3050/3070

To support the repartitioning procedure, the following commands are used:

- **/boot/repartition**
  Initiates repartitioning for the local host.
- **/cfg/sys/host #/repartition**
  Initiates repartitioning for the given host (which must be running) in the case of clustered environment.

These are "hidden" commands and hence auto-completeion through <TAB> is not possible.

Repartitioning includes multiple automatic reboots and the host will be effectively out of service.The time required for the repartition is approximately 5 to 7 minutes.

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 17)
- “Upgrading Release 6.0.7.0a to 7.x” (page 18)
- “Upgrading Release 6.0.9.0 to 7.x” (page 18)

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 19).

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 19).
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 19).

2 Upgrade to Release 7.x.

--End--

Upgrading from Release 7.x to 7.0.7 on Nortel Application Switch 2424-SSL

To upgrade Release 7.x to 7.0.7:

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 19).
2	Upgrade to Release 7.0.7

--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 NN46120-104) 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`**, 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 7.0.7.0 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 Manufacture Discontinued (MD) 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 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 in version 7.0.7

- Fixed memory leak issues with ike process.(Q01928237).
- Added a CLI item `/cfg/vpn #/server/http/nocachehdr` to configure the removal of cache-control header. If this is turned off, cache-control header will not be removed. (Q01931820).
- Issue with portal pda access (https://<vpn-ip>/pda) has been resolved.(Q01889036).
- Fixed the issue of backend server loadbalancing based on session persistence when the SSL-VPN is configured for ssl-offload. (Q01334444).
- Every time Net Direct starts, it adds the NVG Portal FQDN to IP address mapping in the windows hosts file for smooth operation. This hosts file shall be restored to original state when Net Direct terminates . But if the Net Direct terminates ungracefully, the windows hosts file entries will not restored properly. If the Net Direct ungraceful exit happens many times, the hosts file will be corrupted and eventually the common windows networking application like "ping" will fail to function properly. This is fixed (Q01882393).
- Net Direct terminating with a windows exception when a non-admin mode user attempts to retreive the available log-in service in the NVG server has been resolved (Q01946926).
- No warning message is displayed to portal user 1 minute before session timeout. (Q01889136).
- Bad password warning for password with characters ’<’ ’>’ has been fixed. (Q01920589).
- Intermittent failure to launch Net Direct in Windows Vista has been resolved. (Q01885586).
- NDIC displays alert message when using Wildcard SSL Certificate. Wild card characters in certificate issuer name was not considered during the time of initial handshaking with NVG and Net Direct. This issue is fixed. (Q01910078).

- The SMB link configured through BBI now adds the default workgroup to solve the issues when user leaves workgroup as blank.(Q01922432).
- Clients using Net Direct and client side proxy are not able to connect when using Internet Explorer proxy exceptions. If an IE proxy exception is not able to be resolved - Net Direct will not start.(Q01693045).
- Solved the issue with the LDAP expiry check in W2K ActiveDirectory.(Q01655800).
- High memory utilization and memory leak issue in portal node has been resolved. (Q01886590).
- Uploading issues with FTP proxy applet for advanced users has been fixed. (Q01875426).
- Net Direct randomly fails to load a user certificate in the first attempt from a smart-card using the CSP from SAFENET 7.0. (Q01858474).
- The issue of not showing the SSL users in BBI Dashboard page when a client logs in using Net Direct is solved. (Q01924849).
- Custom application displaying document in a window shows the http/1.2.3.4 rewritten url inside the document when displayed through the portal. (Q01907934).
- The issue of locking up while accessing the BBI path "Admin -> Monitor -> Users" when the number of users are high is fixed.(Q01877156)

Known limitations

VPN Limitation

VPN Gateway Release 7.0.7.0 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.

Number of VPNs	Platform	SSP License
256	3050	Yes
512	3070	Yes
256	N/A	No

Note: If there are hosts with different hardware platform in a cluster, the maximum number of VPNs is taken from the least capable device.

Browser Requirements

When using the NVG software for basic Portal access, 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, Portforwarder 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. TunnelGuard applet mode is supported in win 2k/2k3, XP and Vista. TunnelGuard is not supported in 64 bit operating systems.

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
- In Windows Vista, Internet Explorer and FireFox 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 Net Direct installable client is not available for Linux, 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. Instead, Net Direct Installable client has to be used. 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--

- SSL offload feature supports 999 offload servers when the SSP license is installed and 256 offload servers when the SSP license is not installed.
- Net Direct cannot allocate IP address from ISC 3.1.1 DHCP server (Q01931144).
- TG heart beat fails when client tries to access with squid proxy using round-robin DNS (Q01920185).
- Symantec virtual desktop (SVD) interoperability problem between 7.0.x & 7.1.x code. The problem is observed when users initally connected to 7.0.5 portal with SVD set to "force on", tries to connect back to the 7.0.5 portal after connecting to a 7.1.1 portal which also has SVD "force on". This will result in "Application launch has failed" error. (Q01930312).
  Work around:
  The workaround is to remove the sodaagent.dll file after unregistering it from the registry on the client pc. Once problem occurs, execute following commands in DOS prompt to fix it:
  ```
  cd %windir%\system32
  regsvr32.exe -u SodaAgent.dll
  del SodaAgent.dll
  ```
- WTS screensize does not work when hidepf is turned on (Q01957891).

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 7.0.7.0 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 7.0.7.0 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.
- IPsec mobility feature is not a fully supported and tested feature. (Q01777355).

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 1.5.0.15 (TDI client): Compatible with Windows 2000 and XP. This client supports UDP as well as TCP. Native Microsoft Outlook is not supported because not fully qualified domain names cannot be resolved.
- The NVG software includes commands for allowing/rejecting access for certain SSL VPN clients, based on client version and which operating system the client currently runs on. These commands have been added as a preparation for future releases of the TDI/LSP clients, where the clients will be capable of sending version number and OS version to the NVG. Until the new TDI/LSP clients are released, existing TDI/LSP clients will be regarded as "old clients".

CLI path: /cfg/vpn #/sslclient/tdiclientand 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

Portforwarder features) is only supported if SSL is enabled on the portal server.

- Proxy chaining is not supported for the Outlook Portforwarder feature.
- Microsoft Outlook 2003 is not supported when using the Outlook Portforwarder in combination with Exchange 2003.
- Running the Outlook Portforwarder 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 Portforwarder 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 Portforwarder 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 Portforwarder) 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 Portforwarder 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 Portforwarder link that works on Windows XP systems that have not yet been upgraded to Service Pack 2, configure the Portforwarder 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".
- Default cipher string configuration leaves out the following 6 authentic ciphers - (IDEA-CBC-SHA, RC4-SHA, RC4-MD5, IDEA-CBC-MD5 , RC2-CBC-MD5, RC4-MD5 (Q01823581)

  Workaround: Set the cipher string as "ALL!EXPORT!LOW!ADH:-SSLv2 :IDEA-CBC-MD5:RC2-CBC-MD5:RC4-MD5" to include all ciphers.
- Vdesktop "force" option is bypassed when persistent portal cookies are enabled (Q01959358).
- Local user authentication password does not support ’\’ backslash character. Local portal auth fails when password contains backslash ’\’. (Q01956522) (Q01956522).

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.

- 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.
- 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.
- When Citrix 4.5 server configured in `/cfg/vpn 1/linkset 1/link 13/` is used with web interface, the user is able to login normally (SSLVPN is not used). A link is created in the web interface which causes the browser to display a blank page and continually reload. (Q01830278)
- Vdesktop fails with Kaspersky Internet Security 6.0. Kaspersky prompts for permissions to allow Vdesktop process to run. When it is launched, Vdesktop covers the prompts and the system hangs. (Q01716029).

  Workaround: Add to trusted zone.

- Cirtix Applet crashes when `urlobscure` is turned on. (Q01692215)
- Change to AAA causes delay in portal traffic. (Q01689436)
- Accessing certain sites may generate java script parse errors in the logs (Q01926277)

Known anomalies

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

- While accessing Net Direct for the first time, error "**Route table cannot be altered when Net Direct is active trying to reconnect**" appears. (Q01297873)
- NVG software re-image using bootshell causes `/cfg/cert` option to disappear. (Q01800810)
- 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)
- The SSL Portforwarder is not working with Outlook XP for the software versions 6.0.3 and 6.0.5. It shows an error *incorrect username/domain* when the user enters the login credentials for Outlook. However, when the software version is 6.0.1 or 5.1.11 the user is able to login to the Outlook XP with the same credentials. (Q01567469)

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:

www.nortel.com/callus

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 - Software Release 7.0.7.0

Release: 7.0.7.0
Publication: NN46120-400
Document revision: 01.09
Document release date: 19 December 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.