Nortel VPN Gateway

Release Notes

Release: 7.0
Document Revision: 01.01

www.nortel.com

NN46120-400 216372-P

Nortel VPN Gateway
Release: 7.0
Publication: NN46120-400
Document status: Standard
Document release date: 10 September 2007

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.

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.

Contents

Release Notes

These Release Notes provide the latest information regarding your Nortel VPN Gateway (NVG) with version 7.0 software. This supplement lists the new features and modifies some information found in the complete documentation:

- *VPN Gateway 7.0 User's Guide*
(NN46120-104)
- *VPN Gateway 7.0 Command Reference*
(NN46120-103)
- *VPN Gateway 7.0 Application Guide for SSL Acceleration*
(NN46120-100)
- *VPN Gateway 7.0 CLI (Command Line Interface) Application Guide for VPN*
(NN46120-101)
- *VPN Gateway 7.0 BBI (Browser-Based Interface) Application Guide for VPN*
(NN46120-102)
- *VPN Gateway 7.0 VPN Administrator's Guide*
(NN46120-105)
- *VPN Gateway 3050/3070 Hardware Installation Guide*
(part number 216213-B, March 2005)

Documentation Download

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

Step	Action
1	**Point your browser to: http://www.nortel.com.**
2	**Under Support and Training, select Technical Support>Technical Documentation**
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 document from the Documentation.**

--End--

New Features/Enhancements in Software Version 7.0

This section lists software features and enhancements added since version 6.0.1.

General

- **Enhanced Usability**
  - Administration Web UI
    - Improved look-and-feel: the overall navigation and user-experience within the NVG 7.0 Web UI has been updated and simplified.
    - Change “Setup”, “Normal”, and “Expert” tabs to “Config” and “Monitor” to better reflect how the Web UI is utilized by administrators.
    - Removal of “dead end” pages (that is pages that could be accessed directly, even though they did not have an object associated with them. This usually resulted in an error printed on the page.)
    - Tabbed and breadcrumb navigation. The depth of the original NVG 6.0 hierarchical tree has been decreased, and configuration pages are displayed as a collection of tabs. Breadcrumbs at the top of the page are used to ease navigation.
    - Wizards for all common workflows, including: SSL Offload, Net Direct, TunnelGuard, Portal Linksets, Authentication, LDAP Active Directory, SSL VPN, IPsec VPN, Certificates, Portal, Administrative Access, and Users/Groups.
    - Help text incorporated directly into Web UI pages.
    - Copy-and-paste of objects, including IP Pools, Groups, Authentication Servers, and Portal Linksets between VPNs.
    - Dashboard page which provides Cluster Status, Interface Status, and User status tabs.
    - Tool Tips for input fields provide additional details on what a particular response field actually means.
    - Context sensitive help button moved from the global toolbar into the individual pages.
    - Advanced settings grouped under an advanced tab, to clearly denote that they should only be modified by experienced users.

    - Simplified Extended Profile presentation, with Client Filters and Extended Profiles being combined into a single page and a tabular view.
    - VPN summary table provides a compact view of all relevant configuration for a single VPN.
    - Cluster Manager enhancements, including a new License tab that displays license information for each host in the cluster and allows it to be stored in Excel format.
    - SSL VPN 1000 Web UI support.
  - Citrix / WTS (Windows Terminal Services) Setup
    - WTS link type modified from a custom port forwarder to an RDP-specific link that supports most standard options and allows single sign-on using Portal username and password. Works with Windows, Linux, and Mac.
    - New Citrix link type that allows ICA link creation to published applications and desktops. Works with Windows, Linux, Mac.
- NVG BBI enhanced to recognize Contivity 1000 HW – the following features are no longer accessible (or configurable)
  - IPsec user and branch
  - Local authentication
  - SSP
  - Clustering
  - The ’Standalone Status’ field
  - The "Standalone Mode" and "Transparent Proxy Mode" fields
- Added Quick VPN wizard
- Added support for NVG that hosts the ActiveX and Java versions of the Citrix and WTS clients and can install them on demand. Users will no longer need to have the client already installed.
  CLI path: `/cfg/vpn #/linkset #/link #/type/WTS/cfg/vpn #/linkset #/link #/type/Citrix`
- Added support to increase cookies per database and removing special case handling which introduces more powerful database.
  CLI path: `/cfg/vpn #/server/portal/cookiedb`
- Added support to allow group information to be retrieved from LDAP servers using either type of schema. At a minimum, it will support ActiveDirectory, Sun iPlanet and Novell eDictionary.
- Added support to give the user the option to use either NTLM or LDAP to talk to the server.

- Added support to configure syslog server per VPN. All VPN specific syslog messages will be sent to both the global syslog and the VPN syslog.
  CLI path: `/cfg/vpn/*/syslog`
- Added support to administrator to have the control over the mobility.
  CLI path: `cfg/vpn/*/sslclient/mobility`
- Added support to disable route table monitoring. This ignores the route changes and keep NetDirect connected.
- Added Support for SecureID and Client Certificate.
- Added support for NDIC connection profiles.
- Added support for Pre-Configure NDIC for distribution.
- Added support for client based failover between NVG clusters.
  CLI path: `cfg/vpn/*/sslclient`
- Adds all known Windows machines to the “Files” tab so that user can start browsing the network shares by clicking on the Windows machine he/she is interested in. You can also drill down into workgroups and domains to reach the machine.
- Added support for stateful failover for login sessions.
- Added support for to load multiple language files and the user can select the language of their choice from it.
- Added support for Symantec Virtual Desktop Integration. Symantec Virtual Desktop” is a Java application that provides a virtual desktop environment where other applications can be run.**CLI path:** `/cfg/vpn/*/vdesktop`
- For better support of Asian language, the Portal default character set is UTF-8. The customer who is using non-English language iso-8859-1 character set must import PO file to Portal.
- The default CIPHER suite for 7.0 is HIGH!ADH-AES128-SHA!ADH-AES256-SHA!ADH-DES-CBC3-SHA per ICSA recommendation. Since Nortel Application Switch SSL health check is using SSLv2, this will cause SSL health check fail. The customer can change CIPHER to ALL@STRENGTH in SSL VPN or use TCP health check in Nortel Application Switch.

Virtual Desktop

- Symantec On-Demand Agent (SODA) provides a Virtual Desktop environment to secure Web-based applications and services.
- Files created while in the Virtual Desktop are encrypted as they are saved to a hard drive or removable media. This provides a secure environment for end users while accessing confidential information.
- Virtual Desktop will be started under the following scenarios: 1) Pre-logon: users launch Virtual Desktop before logging on – this is a per-VPN; 2) Always: users will be forced to always login from within the Virtual Desktop – this is a per-VPN; 3) “Virtual Desktop” TunnelGuard rule: users are forced to use the Virtual Desktop if the TunnelGuard check for host integrity fails – this is per-group. Licenses are available in volumes of 50,100, 1000, 2000 and 5000.

TunnelGuard

- Enhanced Administration Tool adds easier keyboard/mouse navigation, multi-row selection, progress display, and enhanced aesthetics.
- Export/Import of multiple SRS and Rules.
- Persistent configuration options for Administration Tool that allow persistent selections for look-and-feel, color scheme, icon size, default hash algorithm, default startup connection server, auto generate rule configuration, and applet size.
- Administration Tool can connect to any VPN Gateway or VPN Router.
- Introduction of a pre-defined SRS Entry. These are tied to existing antivirus, anti-spam, and firewall products, and provide for ease-of-use and ease-of-configuration.
- Operating System Identification allows one to create and validate SRS rules based upon OS type. Supported operating systems are Windows 2000, Windows XP, Windows Vista, and Windows Server 2003.
- Enhanced Software Definitions to support embedded registry entries.
- Software branding as per Nortel standards.
- Includes JRE 1.5.0_06 in TG Agent Installer bundle.
- Improved logging: log endpoint information to the system log and generate events when TunnelGuard restricts/rejects a connection.

Net Direct

- Mobility: Client will detect link changes and try to re-connect immediately. Administrator can set the maximum roaming time for users. Application session will be preserved, for the specified amount of roaming time.
- Increased robustness: Route table changes that do not affect the Net Direct tunnel will be ignored.
- Net Direct Installable Client (NDIC):
  - Provided in MSI (Microsoft Installer Package) format to allow easy deployment to remote machines using SMS, as well as rollback upon errors.
  - Client Certificate authentication support (MSCAPI).
  - Secondary authentication support.
  - Ability to pre-configure client for distribution to end users.
  - RSA SecurID New Pin / Next Token modes.
  - Client fail over support. If destination is unreachable, NVG will try connecting to fail over servers. (/cfg/vpn 2/sslclient/failover).
  - Connection profile enhancements.
  - Provide access to connection logs from the client .
  - Support client dns registration as a configurable option from the client.

Miscellaneous

- Multilanguage Portal Support: auto-detect language in browser and display strings/labels appropriately.
- Improved Multi-OS Support: Ability to use client OS in policy decisions tied to Extended Profiles.
- Non-System User Support: TunnelGuard works in deployments in which users do not have system-level access.
- Group-Based Controls: Ability to manage policies on a per-group rather than a per-VPN basis.
- User Session Failover: Automatic servicing of user by another cluster device when device becomes unavailable. Trigger a failover in a cluster if the public interface connection becomes unavailable.
- Use Native Groups from LDAP: NVG natively obtain policy information from the following LDAP-based directory servers: Active Directory, iPlanet, Novell eDirectory.

- Logging, Monitoring, Accounting
  - — Simultaneous reporting to Global Syslog and Per-VPN Syslog.
  - — Ability to collect accounting information about both a per-VPN as well as a total system level.
  - — Direct RADIUS accounting traffic either to the VLAN or to a branch tunnel associated with the VPN.
  - — System log message for Ethernet port link up/down.
  - — Log all Website accesses by users and the port forwarder links they use.
- Use Network Neighborhood in portal to find network drives.
- SNMP trap to alert if CRL retrieval is not working.

Fixes

This section lists fixes added since version 6.0.1.

General

- NetDirect fails loading after code downgrade v5.1.3.4+ -> v5.1.3.3- (this is closed as no fix planned) (CR: Q01224780).
- ER: Enhance status window to include connection name (CR: Q01479178)
- ER: SAIC: Split tunnel networks configurable on per group basis (CR: Q0142770).
- Add support for URL obfuscation (CR: Q01479231).
- NVG Customer wants a syslog entry when certification validation fails (CR: Q01236503).
- Syslog message for any link up/down of any Ethernet port (RFF824-14217670) (CR: Q01475232).
- For the Full Access feature (available on the Portal's Access tab) to work, the fully qualified domain name (FQDN) of the VPN *must* be specified as the server alias in the SSL VPN client (Servers tab>Add>Alias field) (CR: Q01043664).
- In WholeSecurity Confidence Online versions prior to 5.0.2, there is no built-in support for the NVG. To get Confidence Online to work with the NVG, proceed as follows:
  In the MySQL database, go to the command line and enter the following commands:

  ```
  USE LANLORD

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

  INSERT INTO integrationparameter (parametername,
  displayname, vendor, type, paramorder, required,
  validationfunction, owner)

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

  (CR: Q01245774)
- If a downgrade from the NVG software release 5.1.3.6 to 5.1.3.2 is necessary, any Net Direct ActiveX controls installed on the remote users' machines adhering to the more recent software version requires

manual removal. If the ActiveX control is not removed, Net Direct will not be can operate on PCs accessing a Portal with the older software version. To remove the ActiveX control, open Windows Explorer and go to C:\Windows\ Downloaded Program Files. Select Netdirect and press Delete (CR: Q01224780).

- Configuring IPsec support through the VPN quick setup wizard during the initial setup procedure (see Chapter 3, "Initial Setup" in the *User's Guide*), will result in failure to complete the setup. The solution is to configure IPsec support manually or use the CLI IPsec wizard (**`/cfg/vpn/*/ipsec/quick`**). Also see the "Transparent Mode" chapter in the *Application Guide for VPN* (CR: Q01356592).
- It is not possible for the **`oper`** user to list loaded languages in the BBI (VPN Gateways>Portal Display>Language>General). (CR: Q01347782).
- It is not possible to modify or delete a VPN created in the BBI if the VPN name contains an apostrophe or a space. The VPN can still be modified or deleted in the CLI. (CR: Q01343418).
- System Log facility option is not available due to global Nortel operability requirements. (CR: Q01733965).

Software Installation and Upgrade Notice

SSL VPN Server Software

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

- `SSL-7.0.1.0-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 7.0.0.17 from an earlier version.

- `SSL-7.0.1.0-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 through the reinstall procedure.

Server Software Download

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

Step	Action
1	**Point your browser to: 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	**Downloading the software requires registered user name and password that 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 Web site, 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 (for limitations, see):

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

Nortel IPsec VPN Client (formerly Contivity)

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

Disk Repartitioning Required for Version 5.x or Later on NAS 2424-SSL

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

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

On this system, the existing disk partitioning does not allow for a 5.x version to be installed simultaneously with version 4.x. that is it isn’t possible to do a standard upgrade from 4.x to 5.x, or from one version of 5.x to another. Software reinstall using a 5.x version is still possible.

Hence, the following applies regarding standard upgrade to version 5.x from versions prior to 5.0 for clusters that include a system of the 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 will give 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 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", that is not shown in the menu or considered for auto-completion through <TAB>, because they shouldn't be used in normal operation. During the repartition, which includes two automatic reboots, the host will effectively be out of service.

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

> ***Note 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 NetDirectCab 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 netdirect filesis same shows the upgraded version. You have to manually delete the IE Wiper Control and NetDirect cab files. Follow these steps to delete the files:

Step	Action
1	**Open up Internet explorer.**
2	**Go to Tools menu.**
3	**Select Internet Options.**
4	**Click Settings.**
5	**Click View Objects.**
6	**Select the files and Remove.**

--End--

Supported Hardware Platforms

The 7.0.1 server software is currently supported on the following hardware platforms:

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

ATTENTION
Nortel does not support the SSL VPN Module 1000 feature in Release 7.0.1.0. Therefore, users who are integrating into this platform should stay with the 6.0 stream until it is supported in a future release.

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.

Known Limitations

VPN Limitation

VPN Gateway Release 7.0.1.0 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.

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 7.1 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 7.1 or later
  Mozilla 1.5 or later
  Firefox 1.0
- Unix/Linux:
  Netscape Navigator 7.1 or later
  Mozilla 1.5 or later

Net Direct Client

The Net Direct client is supported using the following browser and platform combinations:

- Internet Explorer on Windows 2000 and XP.
- Firefox on Linux, Windows 2000 and XP.
- Safari 2.0 on Mac OS version 10.4.
- Internet Explorer and FireFox for Vista is supported for administrator user only.

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

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

Other Limitations

- The installable Net Direct client is not available for Linux and Mac OS X.
- Caching of Net Direct components is not supported for Linux and Mac OS X.
- 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 on the User Account and Family safety.**
3	**Click on User accounts.**
4	**Turn User Control On or Off.**
5	**Uncheck the option "Use User Control (UAC) to protect your computer".**
6	**Click OK and restart the Vista Client.**
7	**Launch the Net Direct.**

--End--

- If NetDirect is disconnected in improper way, restoration of DNS will fail. Few improper ways of disconnecting the NetDirect that a user should avoid are:
  - — Closing the portal browser when NetDirect is On.
  - — Clicking the Close(X) button in the title bar of the applet when NetDirect is On.

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 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 functionality should use version 4.5 of TunnelGuard which includes the full functionality of both TunnelGuard releases. TunnelGuard 4.5 availability is targetted for November of 2007. 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, 5.01 and 5.11.
- For use with the Portal’s Full Access feature, version 4.91 and later are supported.

Nortel SSL VPN Client

The installable SSL VPN client comes in two versions:

- Version 1.1.0.4 (LSP client): Compatible with Windows 98, ME, NT (with IE 5 or later), and XP. This client does not support UDP.
- Version 1.5.0.9 (TDI client): Compatible with Windows 2000 and XP. This client supports UDP as well as TCP. Native Microsoft Outlook is not supported because not fully qualified domain names cannot be resolved.
- The NVG software includes commands for allowing/rejecting access for certain SSL VPN clients, based on client version and which operating system the client currently runs on. These commands have been added as a preparation for future releases of the TDI/LSP clients, where the clients will be capable of sending version number and OS version to the NVG. Until the new TDI/LSP clients are released, existing TDI/LSP clients will be regarded as "old clients".
  CLI path: **`/cfg/vpn #/sslclient/tdiclient`** and **`lspclient`** (these commands currently have no effect) and **`cfg/vpn #/sslclient/oldclients`**
  BBI path: VPN Gateways>VPN Client>TDI Client and LSP Client (these options currently have no effect) and VPN Gateways>VPN Client>Old Clients.

Portal

- Sun’ s JRE earlier than 1.4 cannot download any applets from the VPN Gateway if the device has been setup to use a key length above 4096. This is supported in the native Microsoft JVM and may be supported in Sun’ s JRE 1.5 (yet unclear).
- Proxy chaining (option to specify an intermediate HTTP Proxy host and port, 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.

- /maint/starttrace output should be available in WebUI (CR: Q01475271).
- Problem with Internet Explorer version 7.0.2800.1106.xpsp2_gdr.040517-1325.
  When HTTPS is used, this version of Internet Explorer does not permit download of files that require an external program for processing, or that should be saved in the file system (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 do that, run the following commands as root:

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

  (CR: Q01281449)
- When running Net Direct on Linux, root must be enabled on the remote user's machine and the administrator must see to it that the user account is authorized to use the command **su root** (CR: Q01278965).
- The installed Net Direct client does not support client security checks using the *installed*TunnelGuard agent. If a user tries to connect to a VPN for which TunnelGuard is enabled, the user cannot log in to that VPN if using the installed Net Direct client. This will be fixed in a coming patch release.
- The TunnelGuard applet (client security check launched from the Portal) is not applicable when accessing a VPN using *installed* VPN clients (CR: Q01297451).
- Net Direct on Windows may not be compatible with some Internet security software for clients. This will be fixed in a coming patch release.
- 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 (CR: Q01341726).
- If several ClearTrust authorization servers or dispatchers are configured on the NVG, the server pools are not refreshed. For

example, if a previously failed server is up and running again, this is not reflected in the server pool list. In a coming patch release, the ClearTrust server pools on the NVG will be refreshed periodically (CR: Q01341793).

- Changing the system time in the Minute list box in the BBI (Cluster>Time) to 15 or a higher value generates an error message and may cause the BBI to hang. This will be fixed in the next patch release (CR: Q01341831).
- On Linux (SUSE 10.0) and Firefox, when starting Net Direct from the Portal, the message "Net Direct already running" may be displayed in the Java applet window although Net Direct has not been started. When this occurs, Net Direct cannot be started.
- When configuring the parameters for the downloadable Net Direct client, the administrator has the option to suppress display of the default license agreement.
  The following applies when the license agreement is suppressed (the text will be added to the relevant sections in the manuals in the next release):
  IMPORTANT: By suppressing presentation of the Nortel Software License Agreement you agree to accept the terms of the agreement on behalf of the users receiving the client software from you. If you do not wish to accept the license terms on behalf of the users, then do not suppress presentation of the agreement.
- For Net Direct, if the administrator password configured on the NVG does not match the Windows PC client’s password, the browser can in some cases be closed.
- If a remote user runs an old version of the installable Net Direct client, the client should be can detect this upon connecting to NVG and a dialog where the user can choose to update the client or continue with the old version should be presented. In this release the dialog is not displayed. This will be fixed in the next patch release.
- Log all access requests rejected by NVG Filters to syslog (CR: Q01476301).
- Outlook 2003 client does not work through native outlook port forwarder (CR: Q00757505).
- vdesktop: Cannot connect to NetDirect (CR: Q01546498).
- Error message not generated for deleting active localdb users (CR: Q01614830).
- NETDIRECT: Reconnection issue (CR: Q01619895).

- SQA 6.0.0.11 Panther - CLI does not time out when logged on through contivity (CR: Q01300186).
- VPN+2 groups+diff mobility time per group-ND is getting crash when 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. (CR: Q01747740)

Known Anomalies

This section lists known anomalies with the NVG software.

- 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).
- Netdirect 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)

Nortel VPN Gateway

Release Notes

Release: 7.0
Publication: NN46120-400
Document status: Standard
Document revision: 01.01
Document release date: 10 September 2007

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.

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

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.