Nortel VPN Gateway

Release Notes — Software Release 6.0.5

part number: 216372-M Rev.02, April 2007

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

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 (VPN Gateway) with version 6.0.5 software. This supplement lists the new features and modifies some information found in the complete documentation:

- *VPN Gateway 6.0 User's Guide*
  (part number 216368-D, April 2006)
- *VPN Gateway 6.0 Command Reference*
  (part number 216369-D, April 2006)
- *VPN Gateway 6.0 Application Guide for SSL Acceleration*
  (part number 216370-D, April 2006)
- *VPN Gateway 6.0 CLI (Command Line Interface) Application Guide for VPN*
  (part number 216371-D, April 2006)
- *VPN Gateway 6.0 BBI (Browser-Based Interface) Application Guide for VPN*
  (part number 217239-C, April 2006)
- *VPN Gateway 6.0 VPN Administrator's Guide*
  (part number 217238-C, April 2006)
- *VPN Gateway 3050/3070 Hardware Installation Guide*
  (part number 216213-B, March 2005)

Documentation download

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

1. **Point your browser to: http://www.nortel.com.**
2. **Under Support and Training, select Technical Support>Technical Documentation.**
3. **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 in Software Version 6.0.5

This section lists software features and enhancements added since version 6.0.3.

General

- Added support for Emergency Remote Access (ERA) licensing in version 6.0.5.

  SSL and IPSec VPN ERA licenses

  Clients need a way to plan for a temporary increase in the number of users for the NVG product. This spike in activity can be caused by several scenarios - such as a winter storm that causes an increased number of employees to connect to the network from remote locations. Clients can purchase a discounted, temporary license to help address these transitory requirements.

  With NVG SW 6.0.5 and later, clients may purchase SSL and IPSec VPN ERA licenses or "spike licenses." These temporary licenses provide users with a sixty-day increase in capacity enabling them to accommodate unforeseen events.

The licenses are available in four versions. The user may install one and only one of these ERA licenses:

CPC	PEC	DESCRIPTION:
N0143130	EB0016010	500 User Emergency License
N0143160	EB0016011	1000 User Emergency License
N0143161	EB0016012	2000 User Emergency License
N0143162	EB0016013	5000 User Emergency License

The licenses are purchased and installed the same as normal licenses. As a pre-requisite for ordering this product the client must have a Software Maintenance Agreement. Once installed, the user may verify the installation by issuing the following command:

```
>> Main# /info/licenses
  Global License Pools     VPN         Used          Size
------------------------------------------------------
SSL                        -            0            50
IPSEC                      -            0            50
SPIKE                      -            0            10  <- 10 installed

  License usage per        VPN         Used
-----------------------------------------
SSL                        1            0
IPSEC                      1            0
SPIKE                      1            0 <- none used currently
```

ERA licenses do not have a shelf-life and will not expire until they have been activated and used. The SSL and IPSec VPN ERA license is activated when existing capacity has been exhausted. The new capacity remains in effect for sixty (60) days. After sixty days, ERA will expire and the capacity of the switch will return to the level of the permanent license. Once ERA has been activated, the client may request KRS to regenerate the license. This may be done before or after ERA expires. When a replacement spike license is installed, the existing spike license is deleted and any remaining time from the 60 day period will be lost. The newly installed license will be inactive until the next time the capacity exceeds the installed regular licenses. So it is recommended that spike license be reinstalled only after the spike in number of users is over, or when approaching the 60 day limit after activation. In addition, if a spike license is installed in multiple members of the cluster, they should be replaced together.

- Added support for Microsoft Internet Explorer 7® browser

Net Direct

- Added support to NetDirect client for Microsoft Windows Vista® Operating System. (Q01449041)
- Added support for a split tunnel network configuration on a per group basis. (Q01427701) This enhancement has added the following new command to the Command Line Interface:

  ```
  /cfg/vpn#/aaa/group #/
  ```

Portal

- Added support for NTLM proxy authentication support in the port forwarder and citrix proxy. (Q01336663)

Software installation and upgrade notice

SSL VPN server software

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

- `SSL-6.0.5-upgrade_complete.pkg`

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

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

  Note! TFTP cannot be used when upgrading to version 6.0.5 from an earlier version.

- `SSL-6.0.5-boot.img`

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

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

  Note! TFTP cannot be used when installing version 6.0.5 through the reinstall procedure.

Server software download

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

1. **Point your browser to: http://www.nortel.com.**

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

3. **In the first step of the three-step Product Finder guide, choose 'Select from Product Families' in the list box. Then select the following:**

   VPN Gateway ▸ VPN Gateway 3050/3070 ▸ Software

4. **Click Go and select the desired software release.**

5. **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:

- Version 1.1.0.4 (LSP client): Compatible with Windows 98, ME, NT (with IE 5 or later) Windows 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. It isn't possible to do a standard upgrade from 4.x to 5.x, or from one version of 5.x to another. Software reinstall using a 5.x version is still possible.

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

Current version	Procedure
Prior to 4.2.1.11	Upgrade to 4.2.1.11 or later 4.x, repartition, and then upgrade to 5.x.
4.2.1.11 or later 4.x	Repartition before upgrade to 5.x.

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

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

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

These commands are “hidden”, i.e. not shown in the menu or considered for auto-completion 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 7-10 minutes.

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

NOTE – After repartition is completed, it will not be possible to downgrade to software versions prior to 4.2.1.8, even through software reinstall.

NOTE – When doing the repartition after an upgrade, the new SW version must be "permanent" (see Chapter 4 of the User's Guide) before the repartitioning is started. If the 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 6.x. The “intermediate” upgrade to version 2.0.11.15 is necessary in order to maintain your current configuration, and to provide reliable fallback in case the upgrade should fail.

Downgrading to versions prior to 5.1.5.4

NVG clusters running software version 6.0 or later cannot be downgraded directly to software versions prior to 5.1.5.4. This is due to changes in the internal database format. To downgrade such a cluster to a version lower than 5.1.5.4, first perform an intermediate downgrade to 5.1.5.4 (or later 5.x).

Downgrading to 5.1.5.4 or later

- If a ClearTrust authentication scheme has been configured, downgrading to a version prior to 6.x will fail. Delete the ClearTrust authentication scheme before downgrading.
- In version 6.x, several IP pools may exist for a VPN. In version 5.x, only one IP pool per VPN may exist in the configuration. On downgrading from 6.x or later to 5.1.5.4 or later 5.x, the settings for the default IP pool in the 6.x configuration will be kept in the 5.x configuration, provided the default IP pool is of the type `local`. The Net Direct and IPsec network attributes are configured accordingly. If the default IP pool in the 6.x configuration is not of the type `local`, the first found local IP pool (lowest number) is selected to form the IP pool in the 5.x configuration. If no local IP pool is found, the IP pool will be disabled in the 5.x configuration.
- The TunnelGuard features introduced in 6.0 will be filtered out during the downgrade.
- If Net Direct, IE Wiper and/or Citrix Metaframe support has been set to `group`, the setting will be changed to the respective default value.

Reload license after upgrade

In version 6.0 and later, the default license has been increased from 10 to 50 concurrent users, for SSL and IPsec connections. On upgrades from earlier versions where additional licenses (besides the default license) have been loaded to the devices, the additional license must be reloaded in order to make use of the extra 40 number of users in the default license.

Supported hardware platforms

The 6.0.5 server software is currently supported on the following hardware platforms:

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

Software - support on hardware that has reached MD (Manufacture Discontinued) product status

Software releases may operate on Hardware that has reached MD (Manufacture Discontinued) Product Status. In this situation, the Software will be supported as per the Software Standard Life Cycle Support Practice - but not to exceed twelve (12) months from date of Hardware MD (Manufacture Discontinued) and is limited to supporting only the current software release on HW at time of MD declaration.

According to the above principle, the hardware models Nortel SSL Accelerator 310, 410 and 310-FIPS are not supported from NVG release 6.0 and onwards.

Fixes

This section lists fixes added since version 6.0.3.

General

- OpenSSL vulnerability issues - Denial of Service Attacks (Q01472955)

  Resolved issue of DoS attacks relevant to client authentication.
- OpenSSL RSA Signature Forgery (CVE-2006-4339) (Q01456517-01)

  Resolved vulnerability to possible forgery attempts.
- Duplicate IPSec sessions break IPTables. (Q01470636)

  If two or more clients receive the same Tunnel IP from the IP pool a failure occurred in the IPTables rule insertion.
- Auto proxy configuration needed to be replaced after using an HTTP proxy link. (Q01148743)
- Citrix PF applet ignored proxy settings. (Q01407973)
- OpenSSH was prone to a remote denial-of-service vulnerability because it failed to properly handle incoming duplicate blocks. Portable OpenSSH was prone to a remote code-execution vulnerability. (Q01481457)
- Received Yaws error with "Active Directory"and password expired popup in some configurations where Daylight Savings Time is not used. (Q01437201)
- TDI and LSP showed incorrect version number. (Q01317325)
- "Restarting proxy due to config change" message appeared due to “meminfo” file not closing properly (Q01482281-01)
- SSL SMB access added support for "modified" or "last accessed" date to folder/file. (Q01448518)
- Recursive group lookup did not work when using an NTLM server as an authentication server. (Q01450176)
- SNMP Agent Crashing (Q01400068-01)

  The SNMP Agent crashed when it received unexpected data for disk statistics (NULL or empty string).
- A syslog entry is requested to indicate when certification validation fails. (Q01236503)

Net Direct

- NetDirect installation has improved logic to check for Admin level user when installing on Win XP. (Q01500414)
- Exiting NetDirect while in cached mode and reinvoking NetDirect link in the portal produced the error: “Failed to install NetDirect driver”. (Q01442855)
- NetDirect did not work with long usernames and non admin login. (Q01471951)
- NetDirect reconnection retry count was increased from 60 to 180. (Q01511600)
- NetDirect doesn't launch when dial-up access is used if Internet Explorer LAN proxy is configured. (Q01410053-01)
- Incorrect NetDirect version number shown and not synchronized with NVG version. (Q01504413)
- NDIC installation failed due to invalid Windows registry key. (Q01461049)
- NDDC showed an incorrect message in the log for idle timeout. (Q01304265)
- Installable NetDirect (6.0.3) launched with incorrect warning message when the user reconnected to NetDirect. (Q01499838)
- After upgrading from 6.0.1.3 to 6.0.3 the blank NetDirect Banner and License Banner still appeared, the NetDirect client did not overwrite the NetDirect and IEwiper control. (Q01508173)
- Incorrect version number shown for NDIC in ActiveX control in Internet Explorer (Q01369739)
- SQA 6.0.0.17 NDIC - DeviceIoControl call. Error code = 57 Error.log created. (Q01324692)

  Netdirect generated a warning in the log when a successful connection had been established and gracefully shutdown. No indication of issues was sent over the tunnel that startup and shutdown was successful.
- WPI - VPN 3070 6.0.0 - Certificate name mismatched with NetDirect windows native client. (Q01441442)
- Split tunneling “enabled_inverse_local” did not work. (Q01463753)

  In the “enabled_inverse_local” mode, packets to the backend machine (whose IP is added in the splitnets) was going through the TapAdapter.
- Split tunneling disabled did not send traffic over tunnel in one particular configuration, NDIC did not tunnel the traffic. (Q01326905)

- With split tunneling enabled on NetDirect a default route is added by Windows (Q01425656)
- Cannot RDP from LAN PC to a NetDirect connected XP/SP2 PC. (Q01314666-01)
- NDIC automated upgrade prompt for client was not working. (Q01363191)
- NetDirect cached version prompts for authentication with non-admin user. (Q01530087)

  The documentation for Nortel VPN Gateway 6.0 CLI Application Guide for VPN (216371-D) incorrectly stated that a non-admin user can run NetDirect if caching is enabled. This is not the case as administrator rights are required to run NetDirect even in the cached mode. This is now fixed in 216371-D Rev.01 of the Nortel VPN Gateway 6.0 CLI Application Guide for VPN

BBI (Browser-Based Management Interface)

- Scp and sftp was not supported for language import/export. (Q01348655)
- Sorted cachain by reference number and does not display it in the order it was saved. (Q01345254)
- Chinese text could not be entered in the text description associated with a link through WebUI BBI.(Q01446154)
- "OPER" user privilege did not allow user to view language list. (Q01347782)
- Added “CLI change not reflected in BBI” syslog entry when certification validation failed. (Q01502071)
- BBI: Provided a pull down selector menu for Default Group configuration. (Q01247984)
- Special characters like Swedish characters are not supported in the link text. (Q01469159)

  BBI has been updated to accept non-English characters as a valid input.

Tunnel Guard Agent

- TG failure breaks iauto links and triggers logout. (Q01412529-01)

Portal

- Portal URL link only allowed lower case URI schemes. (Q01466344)
- 6.0 PF broke the portal session with proxy and JRE 1.4.2 (Q01437613)
- "beconv" did not support lowercase "gb2312" character set. (Q01448027)

- Chinese directory path display error at bar when using FTP portal through Internet Explorer. (Q01448030)
- Port forwarding problem occurred when using Chinese Win XP. (Q01472693)
- Software patch 6.0.3.2 caused lbxlaunch.asp rewrite to fail. (Q01470107)

Known limitations

Browser Requirements

Basic Portal Access (no applets)

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

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

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 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

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.

- The Net Direct mobility capabilities are not supported for Linux and Mac OS X.
- The split tunneling modes `enabled_inverse` and `disabled` are not supported for Mac OS X. For non-supported split tunneling modes, Net Direct falls back to the `enabled_inverse_local` mode.
- The split tunneling mode `enabled_inverse` is not supported for Linux. For non-supported split tunneling modes, Net Direct falls back to the `enabled_inverse_local` mode.
- If the remote user has proxy settings configured in Internet Explorer and split tunneling is enabled, Net Direct will use the proxy settings but split tunneling will be disabled, i.e all traffic will be tunneled.
- When using Net Direct on Linux and Mac OS X, the DNS server(s) specified on the NVG (in the IP pool or under `/cfg/sys/dns/servers`) must be able to resolve all host names that should be accessible (internal as well as external host names). This is because no external DNS server will be used as fallback.
- Downloading and installing Net Direct on Windows, requires the user to be administrator on his/her PC. For users that are not administrators, the Windows administrator user name and password can be stored (on group level) on the NVG. If the user is not administrator and the credentials are not stored on the NVG, the user will be prompted for the Windows administrator user name and password upon downloading Net Direct.
- Downloading and installing Net Direct on Mac OS X requires the user to be member of the admin group. If the user is not a member of the admin group or enters the wrong password when prompted, he/she can log in with the root password as an alternative option. This in its turn requires that the user account is authorized to perform the command `su root`.
- Downloading and installing Net Direct on Linux requires the user to be root user or see to it that the user account is authorized to perform the command `su root`. If the user is not running as root when attempting to download Net Direct, a window is displayed prompting the user for the root password.

Tunnel Guard Agent

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

Nortel IPsec VPN Client (formerly Contivity VPN Client)

- For IPsec termination on the 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

- When accessing an FTP server through the NVG portal, the maximum supported file size is 2 gigabytes. (Q01435793)
- Sun’s JRE earlier than 1.4 cannot download any applets from the 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.
- When an iauto link should be used for login to web servers using two-tier basic authentication with domain (i.e. one field for domain\user and one for password), the `/cfg /vpn #/linkset #/link #/iauto/mode` command must be set to `add_domain`.
- Creating a Port forwarder link for mapping a network drive is not supported on Windows 98 and XP clients.
- The features available on the Portal's Advanced tab (i.e. Telnet/SSH access, HTTP Proxy and Port forwarder) are supported only with SSL v3 and cipher type RC4-MD5.
- The features available on the Portal's Advanced tab are not supported for the TLS protocol.
- To create a Port forwarder link for mapping a network drive – and the link is to be used on a Windows 2003 server acting as client – port 445 has to be used instead of the suggested port 139. On the Windows 2003 server, port 445 should be disabled by following these steps:
  - Click Start, select Run and enter `regedit`. The registry editor is started.
  - Locate and select the following key: `HKLM\System\CurrentControlSet\Services\NetBT\Parameters`.
  - On the right panel, double-click the `TransportBindName` entry.
  - In the **Edit string** dialog, delete the displayed value. No value should be specified.
  - Click OK, exit the registry editor and restart the computer.
- Some SSH versions may not be supported when using the SSH feature on the Portal's Advanced tab, e.g. Alteon 184 SSH-1.5-1.2.27.
- Some of Microsoft's Telnet server versions may not be supported when using the Telnet feature on the Portal's Advanced tab.
- To create a WTS port forwarder link that works on Windows XP systems that have not yet been upgraded to Service Pack 2, configure the port forwarder to listen on 127.0.0.2 instead of 127.0.0.1 (localhost). Then configure the Remote Desktop client to connect to

127.0.0.2. With the Windows XP SP2 version of the Remote Desktop client, it is possible to connect to 127.0.0.1 (localhost) as long as the port being used is other than the default (3389). Note that connections through 127.0.0.2 do not work on Windows XP SP2.

- JVM 1.5 and later includes support for using the browser’s certificate database. If the NVG is set to ask for client certificates, any Java applet started during a Portal session may display a window asking for a client certificate, even though the user has already logged in to the Portal with a client certificate. The solution is to click Cancel without selecting a certificate.
- Some web applications, if started, takes over existing instances of Internet Explorer, which may cause problems for the Portal session. For example, if the Portal page is reused by a web application and the Net Direct client is running, the client will be shut down. To solve this problem in IE, go to Tools>Internet options. On the Advanced tab, under Browsing, disable the setting “Reuse windows for launching shortcuts”.

SSL VPN Module 1000 (SVM 1000)

When using the BBI (Browser-Based Management Interface) to configure the SVM 1000, some options in the BBI are available but not supported. The following features in the NVG software are not supported on the SVM 1000:

- Local authentication.
  BBI path: VPN Gateways>Authentication>Local
- Standalone mode.
  BBI path: VPN Gateways>Gateway Setup>Standalone and SSL Offload>Servers>General (Standalone Mode)
- Transparent proxy mode.
  BBI path: SSL Offload>Servers>General (Transparent Proxy Mode)
- Tunnel Guard Agent settings.
  BBI path: VPN Gateways>TunnelGuard>Agent

General

- A maximum of 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 Tunnel Guard agent, the result of the Tunnel Guard check cannot lead to an IP address being allocated from an IP pool that is assigned to an extended profile. This is because the IP address has to be allocated before the Tunnel Guard check is run.

Known Issues

This section lists known issues with the NVG software.

- For the Full Access feature (available on the Portal's Access tab) to work, the fully qualified domain name (FQDN) of the VPN *must* be specified as the server alias in the SSL VPN client (Servers tab>Add>Alias field).
  (CR Q01043664)
- Problem with Internet Explorer version 6.0.2800.1106.xpsp2_gdr.040517-1325.
  When HTTPS is used, this version of Internet Explorer does not permit download of files that require an external program for processing, or that should be saved in the file system (e.g. files with extension .txt, .exe, .zip), even if the SSL VPN server HTTP setting of `addnostore` is set to `off`. Thus it cannot be used to download such files via the Portal.
- In WholeSecurity Confidence Online versions prior to 5.0.2, there is no built-in support for the NVG. In order 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_vpn%",
  "/https/%eeserver%/cgi-bin/rr.fcgi", "WholeSecurity", "_OD_");
  ```

  ```
  INSERT INTO integrationparameter (parametername, displayname, ven-
  dor, type, paramorder, required, validationfunction, owner)
  ```

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

  (CR Q01245774)
- 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* Tunnel Guard agent. If a user tries to connect to a VPN for which Tunnel Guard is enabled, the user cannot log in to that VPN if using the installed Net Direct client. This will be fixed in a coming patch release.
- The Tunnel Guard applet (client security check launched from the Portal) is not applicable when accessing a VPN using *installed* VPN clients.
(CR Q01297451)
- 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 able to 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)
- 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, i.e. 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)
- 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. This will be fixed in the next patch release.
(CR Q01343418)
- 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.
- NetDirect will not launch with SecureRemote installed. (Q01409539)
- After performing an upgrade the "securecook" value should be set to “OFF” in SSL acceleration mode. (Q01452086)

  If you are upgrading from a version older than 4.2.1.25, after the upgrade, the "secure cookie" option will be automatically enabled for all existing SSL servers (/cfg/ssl/server #/http/securecookie). This will cause problems for web sites that want to share the cookies between http and https sessions. If this happens, you must disable the securecookie option manually.
- If a remote user runs an old version of the installable Net Direct client, the client should be able to detect this upon connecting to NVG and a dialog where the user can choose to update the client or continue with the old version should be presented. In this release the dialog is not displayed. This will be fixed in the next patch release.