Nortel VPN Gateway 5.1.5

Release Notes

part number: 216372-F, November 2006

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

Release Notes

These Release Notes provide the latest information regarding your Nortel VPN Gateway (NVG) with version 5.1.5 software. This supplement lists the new features/fixes and modifies some information found in the complete documentation:

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

Documentation Download

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

1. **Point your browser to: http://www.nortel.com.**
2. **Under Support and Training, select Technical 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. **Select the desired document.**

New Features/Enhancements

This section lists features and enhancements added since version 5.1.3. Note that these features are not documented in the 5.1 manuals listed on page 3.

- The LDAP/Active Directory expired accounts feature now handles expired passwords as well as expired accounts. In addition, the NVG computes (if possible) the number of days before the password will expire. This is displayed at Portal login when 5 days (or less) remains before the password expires. You can also configure groups in which users with expired accounts/passwords should be placed.
  CLI path: `/cfg/vpn #/aaa/auth #/ldap/activedirectory /enaexpired`, `expiredgro` and `expasgrou`
  BBI path: VPN Gateways>Authentication>Auth Servers (LDAP). Scroll down to Active Directory Settings (Enable Expired Account/Password Check, Expired Account Group and Expired Password Group).
- Added support for LDAP recursive membership. If the remote user belongs to an Active Directory group which, in its turn, belongs to another group, you can specify whether all groups or only the first group should be returned.
  CLI path: `/cfg/vpn #/aaa/auth #/ldap/activedirectory /recursivemember`
  BBI path: VPN Gateways>Authentication>Auth Servers (LDAP). Scroll down to Active Directory Settings (Recursive Group Membership).

- Added support for controlling whether or not Nortel SSL VPN clients (LSP/TDI clients) should be allowed to log in to the VPN. The default value is `enabled`, i.e. SSL VPN clients are allowed to log in.
  CLI path: `/cfg/vpn #/sslclient/clients`
  BBI path: VPN Gateways>VPN Client>LSP/TDI Clients
- The default objectclass=person filter has been removed from the Active Directory authentication search. You can now configure the desired search filter attribute/value yourself.
  CLI path: `/cfg/vpn #/aaa/auth #/ldap/adv`
  BBI path: VPN Gateways>Authentication>Auth Servers (LDAP). Scroll down to Extra Search Filter, Extra Search Filter Attribute and Extra Search Filter Attribute Value.
- Added support for setting maximum session time (for a remote user's VPN session). Previously, maximum session time could only be set via RADIUS authentication.
  CLI path: `/cfg/vpn #/aaa/sessionttl`
  BBI path: VPN Gateways>Gateway Setup>Session (Maximum Session Length)

Fixes

This section lists fixes added since version 5.1.3.

General

- Fixed problem with the user getting logged out from a backend web server when following a link pointing to an XML document. This was caused by a bad detection of XML content due to bad Content-Type header sent by intranet web server. Code has now been added to determine if a page with a Content-Type: text/html in fact is xml.
  (CR Q01152538)
- Removed ping test for TFTP transfer. When performing `/maint/dumplogs` and `/maint/dumpstats` (Maintenance>Dump Logs and Statistics) via TFTP, a connectivity test using ping was done before the actual transfer, with the result that the transfer was aborted if ICMP echo request/reply was blocked in the network. These commands now use a TFTP client implementation that correctly detects and reports failure to reach the TFTP server.
  (CR Q01184292)
- Fixed deadlock in AAA subsystem. When using LDAP authentication, if a user had modified "user preferences" and was then logged out due to idle timeout, the AAA subsystem could deadlock. This prevented further authentication and caused the `/info/users` command (Administration>Monitor>Users) to hang.
  (CR Q01184159)

- Fixed problem with importing a user database. Previously, import of a user database failed if a user definition exceeded 256 characters. The limit has now been increased to 8192 characters.
  (CR Q01202870)
- Fixed vulnerability issue found by SEC Consult. Now port forwarder links in pre 5.0 format (i.e created in a 4.x-based system) are converted at system upgrade and system restart (to cover for load of an old configuration using `/cfg/gtcfg` (Operation>Configuration>Import Cluster Configuration)). Links are converted to the new port forwarder link format introduced in the 5.0 release. And, the tunnelform.yaws page no longer accepts the `a` (application) and `aa` (application argument) parameters. Thus, if an old link is loaded due to a `gtcfg`/Import Cluster Configuration without a restart, the client will be informed to contact the system administrator in order to reconfigure the system to handle this link.
- Fixed logging of malformed HTTP request. In some cases, the SSL proxy logging the contents of a malformed HTTP request (with the message "missing request http version") could cause random data to be logged, or potentially cause a crash/restart of the SSL proxy.
  (CR Q01226566)
- Fixed various rewrite problems. Rewrite was switched off in the middle of a document due to a misplaced <?XML> tag. The NVG now uses isolated handling of <!DOCTYPE> tags to better guess the type of document. Added specific rewrite for OWA in Exchange Server 2000. This corrected forward mail and broken links when choosing different message views.
  (CR Q01218778, Case 050901-75074, Case 050922-97168)
- Fixed rewrite problem with Outlook Web Access 2000 and 2003. Outlook Web Access uses anchor tags to store information about folders and folder content. The id attribute of the anchor tag contains the URL to the document on the back end server. Previously, the id tag was not rewritten, now it is. This code change has been verified against Exchange Server2000 and Exchange Server2003.
  (CR Q01218778, Case 050901-75074, Case 050922-97168)
- Fixed logging problem. Previously, FTP and connection attempts were never logged to the syslog server, even though `/cfg/vpn #/adv/log` (VPN Gateways>Gateway Setup>Session (User Session Logging) was set to `all`.
  (CR Q01223066)
- Fixed problem with connection pooling and delayed POST data. Previously, this bug would sometimes cause the server side connection to be put back on the connection pool if the response from the server was slow. The bug was only triggered if the client request was a POST and the POST data was incomplete or very slow in arriving.

- Fixed deadlock/hang problem. In some cases involving initiation of multiple TCP sessions within a very short period of time, the system could encounter a deadlock state, resulting in a total system lock-up and requiring a hard reset. The problem has only been reliably reproduced on AAS 2424-SSL with a continuous, high traffic load, but could potentially occur also with other platforms or traffic cases.
(CR Q01209305)

- Fixed OpenSSL vulnerability. The CAN-2005-2969 vulnerability has been removed. This vulnerability only affects the ASA/NVG if protocol version SSL 2.0 has been enabled, by changing the `/cfg/ssl/server #/ssl/protocol` (SSL Offload>Servers>SSL (Protocol)) or `/cfg/vpn #/server/ssl/protocol` (VPN Gateways>Gateway Setup>SSL>SSL (Protocol)) setting from the default `ssl3` to `ssl2` or `ssl23`. This is disrecommended regardless of this vulnerability, since the SSL 2.0 protocol has known weaknesses. See http://www.openssl.org/news/secadv_20051011.txt for further details.

IPsec

- Fixed problem with IPsec group authentication. Previously, IPsec group authentication failed if the group name configured on the NVG contained uppercase characters.
(CR Q01113227, CR Q01228085)

- Fixed certificate validation for IPsec certificate authentication. Serious flaws in the certificate validation for IPsec have been found and corrected. It is strongly recommended that certificate authentication for IPsec be disabled for all versions prior to 5.1.5, by making sure that no certificate authentication is configured under `/cfg/vpn #/aaa` (VPN Gateways>Authentication), or if configured that it is disabled, for all VPNs that have IPsec enabled.

- Fixed problem with multiple IPsec clients connecting from networks using NAT (Network Address Translation). If multiple IPsec clients behind a NAT device were connecting to the NVG, and all were NATed to the same IP address (i.e. the typical case), one of the clients at the most was able to maintain connectivity. This was due to the NVG using the wrong tunnel for the return traffic.
(CR Q01178892)

- Fixed problem with Enc/Dec KB counters in `/info/ipsec` output (Administration >Monitor IPsec Users). Previously, the counters were showing MB instead of KB values.

- Disabled IPsec client TCP ports on public interface. Previously, connections were unnecessarily accepted on the public interface for the TCP ports used by the Nortel IPsec VPN client (formerly Contivity VPN client) banner and password change functionality (17 and 586). Now they are only accessible through an established IPsec tunnel.

- Fixed problem with IPsec not accepting new connections. In some cases where IPsec certificate authentication was rejected (e.g. revoked certificate), the session-setup flow control mechanism ("credits") was not correctly updated, with the eventual result that no new sessions were accepted.
- Fixed problem with `/info/kick` and IPsec session table. When `/info/kick` (Administration>Monitor>Users (Kick)) was used to log out an IPsec user, the user was removed from the AAA tables (/info/user) but not from the IPsec session table (/info/ipsec).
  (CR Q01218958)

Certificates

Fixed problem with CRL (Certificate Revocation List) retrieval via HTTP. The HTTP GET request for CRL retrieval used the full URL, which was rejected by some servers. Now a formally correct GET request + Host header is used.
(Case 050815-55629)

SMB and FTP

- Fixed so that files that are marked as hidden are not displayed in SMB file listings.
  (CR Q01166271)
- Fixed so that SMB links with no share specified displays list of available shares.
  (CR Q01186323)
- Fixed problem with SMB shares containing lots of entries. Previously, it was impossible to access SMB shares containing more than 69 files/folders.
  (CR Q01205377)
- Fixed problem with FTP uploads being corrupted after approximately 200 sec.
  (CR Q01175146)

Portal

- Fixed problem with Full Access applet not recognizing IPsec VPN clients with version number > 5.*. It now recognizes all supported versions including future ones.
  (CR Q01192059)
- Fixed problem with Portal link not working in frames if a URL is missing relative or absolute path.
  (CR Q01187510-01)

- Fixed proxy auto configuration for port forwarder applets (available on the Portal's Advanced tab). Previously, port forwarder applets did not work when proxy auto configuration in Internet Explorer was enabled.
  (Case 050930-06115)
- Fixed problem using many VLAN-tagged interfaces. When configuring more than 100 VLAN-tagged interfaces (e.g. for Secure Service Partitioning with many VPNs), parts of the networking setup would fail. In particular, Portal access was not possible.
  (CR Q01161146)

PDA Portal

- Fixed problem with LDAP macros not being expanded in PDA Portal.
  (CR Q01104870-1)
- Fixed so that PDA Portal is sensitive to user type settings when presenting tabs.
  (CR Q01109503)
- Fixed language problem with the PDA Portal. Previously, it was not possible to configure the PDA Portal's language completely via the language file which resulted in a different appearance compared to the Web Portal.
  (CR Q01221359)
- Fixed problem with PDA Portal not handling the Login Service list box correctly. The Login Service list box should not be displayed on the PDA Portal's login page if no display name has been configured for any of the authentication methods used.
  (CR Q01222328).

Authentication

- Fixed problem with redirection after login to a SiteMinder server. The users had to close the browser window and reopen it to avoid the redirect page from SiteMinder server to be executed. This was caused by a rewrite problem when document.open() was called in Javascript (or implicitly called from an onload handler).
  (CR Q01159893)
- Fixed looping SiteMinder agent. A problem in the SiteMinder agent could cause the agent to start looping, with the result that the system showed a constant 100% CPU usage (SiteMinder authentication still worked since a new agent instance was started automatically).

- Fixed problem with LDAPS auth connection. Previously, if the the SSL connection handshake for LDAPS authentication failed to complete, the login could hang indefinitely and also block subsequent login attempts. Now the timeout configured via `/cfg/vpn #/aaa/auth #/ldap/timeout` (VPN Gateways>Authentication>LDAP>LDAP Settings (Server Timeout)) covers also the SSL connection setup.
(Case 050808-48008)

Tunnel Guard

The Tunnel Guard Java Applet has been signed with a new Verisign certificate. The new certificate expires July 2006.
(CR Q01233672)

SSL Acceleration

- Fixed problem with transparent proxy not closing backend session. When using transparent proxy mode for SSL acceleration, if the client closed the session by sending RST before all data had been received from the backend server, the ASA/NVG would drop the backend session without notification to the backend server. Now RST is sent to the backend server in response to the first data packet after client close, but not until ACK-OF-FIN has been received from the backend server.
(CR Q01160752, CR Q01227999)
- Fixed problem with transparent proxy using specific client source port. When using transparent proxy mode for SSL acceleration, if a client connection originated from one of certain TCP ports that are used internally by the ASA/NVG (e.g. 4369, 5004, 7995), the backend connection would fail.
(CR Q01158961)

Browser-Based Management Interface (BBI)

- Fixed problem with deleting users from the local database when the user name contained spaces.
(CR Q01199218)
- Fixed problem with updating passwords for certain user names
(CR Q01180816)
- Fixed vulnerabilities in BBI interface. Previously, the BBI interface had directory traversal and cross-site scripting vulnerabilities, that could potentially allow an attacker to retrieve arbitrary files from the system via an authenticated admin session.

Software Installation and Upgrade Notice

VPN Gateway Server Software

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

- `SSL-5.1.5-upgrade_complete.pkg`

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

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

- `SSL-5.1.5-boot.img`

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

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

Server Software Download

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

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

   VPN Gateway ▸ VPN Gateway 3050/3070 ▸ Software

   Alteon ▸ SSL Accelerator/SSL VPN ▸ Software

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

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

Nortel SSL VPN Client

The SSL VPN client can be downloaded from Nortel's Customer Support Web site. In the three-step Product Finder guide, select **VPN Gateway ▸ VPN Gateway 3050/3070 ▸ Software.**

The installable SSL VPN client comes in two versions (for limitations, see page 17):

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

Nortel IPsec VPN Client (formerly Contivity VPN Client)

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

Disk Repartitioning Required for Version 5.x on Some Systems

This applies to the following systems:

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

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

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

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

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

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

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

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

The time required for the repartition is approximately:

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

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

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

Upgrading from Versions Earlier than 2.0.11.15

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

Downgrading to Versions Prior to 5.0

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

Supported Hardware Platforms

The VPN Gateway 5.1.5 server software version is currently supported on the following hardware platforms:

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

TFTP Server Support

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

Known Limitations

Browser Requirements

Basic Portal Access (no applets)

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

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

Applet Support

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

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

Tunnel Guard Applet Support

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

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

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

BBI Support

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

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

Net Direct Client

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

Tunnel Guard

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

Nortel IPsec VPN Client (formerly the Contivity VPN Client)

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

Nortel SSL VPN Client

The installable SSL VPN client comes in two versions:

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

License

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

Portal

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

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

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

General

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

Known Issues

This section lists known issues with software version 5.1.5.

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