Version 4.5

Part No. NN46110-307 02.01
317017-D Rev 01
13 October 2008
Document status: Standard

600 Technology Park Drive
Billerica, MA 01821-4130

Nortel VPN Router Configuration — TunnelGuard

NORTEL

Copyright © 2008 Nortel Networks. All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Check Point and FireWall-1 are trademarks of Check Point Software Technologies Ltd.

Cisco and Cisco Systems are trademarks of Cisco Systems, Inc.

Entrust and Entrust Authority are trademarks of Entrust Technologies, Incorporated.

Java and Solaris are trademarks of Sun Microsystems.

Linux and Linux FreeS/WAN are trademarks of Linus Torvalds.

Microsoft, Windows, Windows NT, and MS-DOS are trademarks of Microsoft Corporation.

Netscape, Netscape Communicator, Netscape Navigator, and Netscape Directory Server are trademarks of Netscape Communications Corporation.

SPARC is a trademark of Sparc International, Inc.

All other trademarks are the property of their respective owners.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks Inc. software license agreement

This Software License Agreement (“License Agreement”) is between you, the end-user (“Customer”) and Nortel Networks Corporation and its subsidiaries and affiliates (“Nortel Networks”). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

“Software” is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment (“CFE”), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer’s Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided “AS IS” without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER’S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN

ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Preface 9

Before you begin 9
Text conventions 10
Related publications 12
Printed technical manuals 13
How to get help 13
Finding the most recent updates on the Nortel Web site 14
Getting help from the Nortel Web site 15
Getting help over the phone from a Nortel Solutions Center 15
Getting help from a specialist by using an Express Routing Code 15
Getting help through a Nortel distributor or reseller 16

New in this release. 17

Features 17
TunnelGuard enhancements 17

Chapter 1
TunnelGuard 19

TunnelGuard Agent 20
Disconnect or restrict Nortel VPN Client if no TunnelGuard Agent installed 21
Access denied message 22
TunnelGuard icons 22
Supported platforms 23
TunnelGuard Agent installation 23
JRE installation 23
Installation kits 24
Command line and silent installation 26
Nortel VPN Client with TunnelGuard 26
Custom installation 27

Custom installation options 30
TunnelGuard system tray icon 31
TunnelGuard logs 31
No or limited messages 33
TunnelGuard Agent error message 34
Initial Failure Recovery Mode 35
TunnelGuard banner support 35

Chapter 2
TunnelGuard configuration 37

TunnelGuard Server configuration 37
Configuring TunnelGuard filters 37
Configuring TunnelGuard group settings 39

Chapter 3
TunnelGuard administration 43

TunnelGuard Administration GUI 43
Logging on to TunnelGuard Administration 43
Selecting and modifying a predefined software definition 44
Creating a software definition 45
Creating a rule definition 48
Registry-based rules 50
Operating system types 50
Registry entry creation 51
Creating a registry entry 53
OnDisk and Memory Module entries 55
Registry-based file or module 55
Registry-based path variables 55
Adding an OnDisk file entry 56
Adding a Memory Module entry 57

Chapter 4
FWUA with TunnelGuard configuration 61

Proxy IP address 61
Anonymous FWUA User option 61

TunnelGuard timeouts 62
TunGuardCheckInterval 62
TunGuardHbInterval 62
TunGuardHbRetry 62
Configuring FWUA with TunnelGuard 62

Appendix A
TunnelGuard Administration GUI 65

TunnelGuard Administration window 65
Editing options for TunnelGuard SRS entries 65
Menu Commands and icons 67
File menu 67
Edit menu 68
Predefined Software Definition menu 68
Custom Software Definition menu 69
Software Definition Entry menu 70
TunnelGuard Rule menu 71
Tool menu 71
Predefined Software Definitions window 72
Predefined Software Definition toolbar 72
Software Definition 72
Available Software Definitions 73
Selected Definition Entries 73
SRS Display Message 73
Antivirus and AntiSpyware Configuration 73
Firewall Configuration 73
Custom Software Definition window 74
Software Definition toolbar 74
Software Definition list 76
Software Definition table 76
New Software Definition window 78
Create New OnDisk SRS Entry window 79
Create New Memory Module SRS Entry window 81
Registry Entry window 84
Memory snapshot 84

Rule Definition window 85
Rule Definition toolbar 85
Rule Definition table 85
Rule Action Constructor 86
Rule Expression Constructor 87

Preface

This guide introduces you to the installation procedures for the Nortel VPN Router TunnelGuard. Topics include

- installing the TunnelGuard Agent
- configuring TunnelGuard server settings
- configuring TunnelGuard Administration

This guide is intended for network managers who configure the TunnelGuard Agent software for the Nortel VPN Router and clients. This guide is based on the assumption that you have experience with windows-based systems or graphical user interfaces (GUIs) and that you are familiar with network management.

Before you begin

The minimum PC requirements for the Nortel VPN Router TunnelGuard are

- Windows 2000 and XP
- 200 MHz Pentium
- 64 MB memory
- 10 MB free hard disk space
- Java Virtual Machine (JVM)1.4.1_02 or later if you have the installation kit without the JVM

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicates that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command. Example: If the command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**
bold Courier text	Indicates command names, options, or text that you need to enter. Example: Use the **show health** command. Example: Enter **terminal paging** {**off** | **on**}.
braces ({ })	Indicates required elements in syntax descriptions where more than one option exists. You must choose only one option. Do not type the braces when you enter the command. Example: If the command syntax is **ldap-server source {external | internal}**, you must enter either **ldap-server source external** or **ldap-server source internal**, but not both.
brackets ([ ])	Indicates optional elements in syntax descriptions. Do not type the brackets when you enter the command. Example: If the command syntax is **show ntp [associations]**, you can enter either **show ntp** or **show ntp associations**. Example: If the command syntax is **default rsvp** [**token-bucket** {**depth** | **rate**}], you can enter **default rsvp**, **default rsvp token-bucket depth**, or **default rsvp token-bucket rate**.
ellipsis (. . .)	Indicates that you repeat the last element of the command as needed. Example: If the command syntax is **more disk***n***:***<directory>***/...***<file_name>***, you enter **more** and the fully qualified name of the file.

italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, an underscore connects the words. Example: If the command syntax is **ping** <*ip_address*>, *ip_address* is one variable and you substitute one value for it.
`plain Courier text`	Indicates system output, for example, prompts and system messages. Example: `File not found.`
comma (,)	Shows menu paths. Example: Choose **Status**, **Health Check**.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one choice. Do not type the vertical line when you enter the command. Example: If the command syntax is **terminal paging** {**off** | **on**}, you enter either **terminal paging off** or **terminal paging on**, but not both.

Related publications

For more information about the VPN Client, see the following publications:

- Release notes provide the most recent information, including brief descriptions of the new features, problems fixed in this release, and known problems and workarounds.
- *VPN Client Configuration—Client* (NN46110-306) provides information to install and configure client software for the VPN TunnelGuard.
- *Nortel VPN Router Upgrades—Server Software Release 8.0* (NN46110-407) provides information to upgrade the server software to the most recent release.
- *Nortel VPN Router Installation and Upgrades—Client Software Release 8.01* (NN46110-409) provides information to upgrade the Nortel VPN Client to the most recent release.
- *VPN Client Configuration—Basic Features* (NN46110-500) introduces the product and provides information about initial setup and configuration.
- *VPN Client Configuration—SSL VPN Services* (NN46110-501) provides instructions to configure services on the SSL VPN Module 1000, including authentication, networks, user groups, and portal links.
- *Nortel VPN Router Configuration—Advanced Features* (NN46110-502) provides configuration information for advanced features, such as the Point-to-Point Protocol (PPP), Frame Relay, and interoperability with other vendors.
- *VPN Client Configuration—Tunneling Protocols* (NN46110-503) provides configuration information for the tunneling protocols IPsec, Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), and Layer 2 Forwarding (L2F).
- *VPN Client Configuration—Routing* (NN46110-504) provides instructions to configure the Border Gateway Protocol (BGP), Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Virtual Router Redundancy Protocol (VRRP), Equal Cost Multipath (ECMP), routing policy services, and client address redistribution (CAR).
- *VPN Client Using the Command Line Interface* (NN46110-507) provides syntax, descriptions, and examples for the commands that you can use from the command line interface (CLI).
- *VPN Client Configuration—Firewalls, Filters, NAT, and QoS* (NN46110-508) provides instructions to configure the Stateful Firewall and VPN TunnelGuard interface and tunnel filters.

- *VPN Client Security—Servers, Authentication, and Certificates* (NN46110-600) provides instructions to configure authentication services and digital certificates.
- *VPN Client Troubleshooting—Server* (NN46110-602) provides information about system administrator tasks, such as recovery and instructions to monitor VPN Router status and performance. This document provides troubleshooting information and event log messages.
- *Nortel VPN Router Administration* (NN46110-603) provides information about system administrator tasks, such as backups, file management, serial connections, initial passwords, and general network management functions.
- *VPN Client Troubleshooting—Client* (NN46110-700) provides information to troubleshoot installation and connectivity problems with the Nortel VPN Client.

Printed technical manuals

To print selected technical manuals and release notes for free, directly from the Internet, go to www.nortel.com/documentation. Find the product for which you need documentation, and then locate the specific category and model or version for the hardware or software product. Use Adobe Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to the Adobe Systems Web site at www.adobe.com to download a free copy of the Adobe Reader.

How to get help

This section explains how to get help for Nortel products and services.

Finding the most recent updates on the Nortel Web site

The content of this documentation was current at the time of product release. To check for updates to the most recent documentation and software for VPN TunnelGuard, click one of the following links.

Link	Web site
Most recent software	Nortel page for **VPN Router** software located at support.nortel.com/go/main.jsp?cscat=SOFTWARE&poid=12325
Most recent documentation	Nortel page for **VPN Router** documentation located at support.nortel.com/go/main.jsp?cscat=DOCUMENTATION&poid=12325

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can perform the following activities:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to the following Web site:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

New in this release

The following sections detail what's new in *Nortel VPN Router Configuration — TunnelGuard* for Release 4.5:

Features

See the following section for information about feature changes:

TunnelGuard enhancements

Nortel enhanced the TunnelGuard feature. In prior releases, you implemented and bundled a third-party Application Programming Interface (API) to make TunnelGuard work in your implementation. TunnelGuard now supports a preconfigured Software Requirement Set (SRS) that you can modify. For more information about preconfigured SRS and the changes in the TunnelGuard applet, see the following sections:

- "Selecting and modifying a predefined software definition" on page 44
- "Predefined Software Definitions window" on page 72

Chapter 1
TunnelGuard

Use TunnelGuard to impose a security policy on the client PC when it connects to the corporate network through the Nortel VPN Router. This policy dictates the firewall and security software, or Software Requirement Set (SRS), that you must install and activate on the client PC when the PC connects to the gateway.

TunnelGuard is comprised of the following components:

- TunnelGuard Agent—the desktop application that runs on client desktop PCs that connect to the VPN router for VPN connections. This application monitors the state of rules on desktops that the TunnelGuard Daemon on the VPN router enforces, and reports their status back to VPN Router.
- TunnelGuard Applet—the clientless solution that provides similar functionality as TunnelGuard Agent. This applet runs in Web browser context and provides compliance check and monitoring. This applet acts as a policy enforcer on the
  - — Nortel Secure Network Access (NSNA) for LAN-based connections
  - — Nortel VPN Gateway (NVG) for Secure Sockets Layer (SSL)-based connections
  - — Nortel VPN Router (NVR) for Firewall User connection
- TunnelGuard Server—runs on a VPN router that communicates rules to the TunnelGuard Agent. It takes action, such as connection termination, based on the status reported back by the Agent.
- Nortel VPN Client—the application responsible for providing secure tunnel from desktop to the Nortel VPN Router or Gateway. The TunnelGuard Agent communication with TunnelGuard Administration can only occur through through a secure tunnel.
- TunnelGuard Administration—provides an easy-to-use User Interface for you to create and modify rules and modify SRSs. You can assign these requirements and rules to groups of users and enforce them on client PCs that connect to the VPN router. You launch TunnelGuard Administration as a Java

Web-start application for Nortel VPN Router or a browser-based applet for Nortel VPN Gateway browser-base interface (BBI) tool. You can also launch TunnelGuard Administration as part of an application in Security and Routing Element Manager (SREM) for NSNA.

TunnelGuard Agent

The TunnelGuard Agent runs on the client desktop PC and processes and checks the SRS rules. For example, the TunnelGuard Agent checks that the required components (executable files, DLLs, and configuration files) necessary to comprise a personal firewall are installed and active. Because the TunnelGuard Agent resides on the the gateway, the TunnelGuard Agent is invisible to the end user.

The TunnelGuard Agent

1. starts at bootup
2. remains inactive in a listening state until a tunnel establishes
3. returns to the listening state after a tunnel tears down

The TunnelGuard Agent exists as a separate component and not as a part of the Nortel VPN Client application. The TunnelGuard Agent assumes an authenticated VPN tunnel connection to a gateway, but requires neither a specific VPN client nor specific functionality of a particular VPN client.

The TunnelGuard Agent performs the following activities:

- Listens for a Transmission Control Protocol (TCP) message from the TunnelGuard Server that runs on the gateway, and announces that the tunnel is active.
- Initiates a TCP/IP connection to the TunnelGuard Server, and specifies a hash for authentication.
- Requests the personal firewall data (SRS rules) from the TunnelGuard Server.
- Accepts the data from the TunnelGuard Server.
- Validates the personal firewall data by hashing the local modules and comparing against the data specified in the SRSs.

- Calls a vendor-supplied API to validate the personal firewall operation and waits for a response.
- Responds to the TunnelGuard Server with a status as to whether the server must open up or tear down the tunnel, or leave the tunnel in restricted mode.
- Checks the personal firewall data at regular intervals, as requested by the gateway, and sends a status to the daemon as to the state of the personal firewall.
- Listens for a TCP message from the TunnelGuard Server that announces that the tunnel came down and discontinues checking.

The TunnelGuard Agent and Nortel VPN Router ensure that the end user cannot access the private network unless the personal firewall (or other gateway administrator-defined software) runs on the end-user system. This allows administrators to confirm that their VPN users have all required security software, such as a personal firewall, running on the end-user system. Configure the requirement at the group level on the Groups > Edit > Connectivity window.

Disconnect or restrict Nortel VPN Client if no TunnelGuard Agent installed

The TunnelGuard Server tries to connect to the host Agent seven times before it stops. Whether the tunnel tears down, remains up in restricted mode, or changes to an unrestricted filter, depends on the configuration of the Initial Policy Failure action. At the Groups window, you can configure the VPN Router Client to disconnect if the server fails to connect to an Agent. The user receives a notification that access is denied because the TunnelGuard Agent is not installed. In addition to banner text that describes the problem, the notification message also contains delete payloads for tearing the tunnel down.

If you configure the Group level configuration option to Restricted mode, the appropriate filter applies to the tunnel and the banner text appears. To configure the VPN Router Client to disconnect if the server fails to connect to an Agent, select Teardown Tunnel and send banner if configured from the TunnelGuard: Agent Absent Action list at Groups > Edit > Connectivity window.

Access denied message

If the switch does not receive a response from the TunnelGuard Agent, the user receives a message that access is denied because TunnelGuard Agent is not installed. A protected notification message requests that the VPN Router Client display a banner with the appropriate link. The message is not acknowledged or resent. After the Nortel VPN Client receives the Notify message, it performs the usual decryption and hash authentication. It then displays the banner with a Windows Control dialog box and initiates tunnel disconnection.

You configure the banner text on the Groups > Edit > Connectivity window. The banner text describes the requirement for the TunnelGuard Agent and provides a hyperlink to a location where you can download the Agent.



Note: This feature requires version 6.01+ of the Nortel VPN Client on the server.

TunnelGuard icons

Each of the three TunnelGuard states uses an icon. The following table shows the color and state of each icon.

Table 1 Icon colors and states

Color	State
Gray	There is no connection to the server. TunnelGuard is in an idle state.
Green	TunnelGuard is connected to the server and compliant to policies.
Red	Compliance fails and a new error is reported.

Supported platforms

TunnelGuard is supported on the following operating system platforms:

- Windows 2000 or XP
- In release 3.0, SRS Operating System Type supports only Windows and SRS Entry supports only Windows 2000, Windows XP, and Windows 2003.

TunnelGuard Agent installation

Nortel provides TunnelGuard installation kits on the Nortel VPN Router Client and TunnelGuard CD in the TunnelGuard directory.

Note: You must have administrative rights to install TunnelGuard on Windows 2000 or XP Professional.

JRE installation

Nortel provides two installation kits for the Jave Runtime Environment (JRE): one with the Java virtual machine (VM) (1.60_b06) bundled, and one without VM bundled. The NoVM installation kit, without the bundled VM, minimizes the size of kit for download.

JRE 1.60_b06 is required for TunnelGuard installation. The VM version of TunnelGuard installation allows the user to install bundled VM, which is Version 1.60_b06, with TunnelGuard. The VM installs under the *<TG install dir>\jre* directory. This JRE is local to the TunnelGuard and only TunnelGuard uses it. Web browsers are not affected by JRE.

Use the Select JVM dialog box to select

- bundled JVM (not available for NoVM kit)
- JVM installed on local machine (with a version greater than or equal to 1.60_b06)

- a list of JVMs currently installed on the local machine

Note: If you upgrade JRI after you install the TunnelGuard Agent, the TunnelGuard service can fail to start because the HKEY_LOCAL_MACHINE\SOFTWARE\Nortel\TunnelGuard\RuntimeLib Registry Key does not automatically update. If this happens, reinstall the TunnelGuard Agent or use the regedit command to update this Register Key to restart the TunnelGuard service. If you frequently update JRE, Nortel recommends you use bundled JVM.

If you select bundled JVM, a jre directory installs under the installation directory from which you can launch the TunnelGuard application.

If you select a JVM installed on the local machine, the jre directory does not install. TunnelGuard uses the selected local JVM.

Use the property NN_JREPATH to set the JRE path. If you configure NN_JREPATH, the Select JVM dialog box does not appear. TunnelGuard uses the JVM represented by NN_JREPATH.

In silent mode, if you configure the JRE path, TunnelGuard uses the corresponding JRE. If you do not configure the JRE path for a VM kit, the default bundled JRE installs and runs. If you do not configure NN_JREPATH for a NoVM kit in silent mode, the installation fails.

Installation kits

Nortel provides two sets of kits for TunnelGuard installation: a custom installation kit and a standard installation kit. Each kit has two versions: VM and NoVM.

If download time is not a concern, administrators can deploy the VM version of TunnelGuard. The VM version of TunnelGuard gives you the option to install the bundled JVM or use one already installed on the machine (1.60_b06).

If users have an older version of JRE installed and want to keep that version (for example, JRE 1.3.1) to be used by browsers, they can install the bundled JVM and limit the use of that JVM to TunnelGuard.

The NoVM version has no bundled JVM, thus the kit is smaller and it downloads faster. In this case, users must have the right version of JRE (1.60_b06) installed on the machine.

Custom VM kit

The custom VM TunnelGuard installation kit is bundled with JRE 1.60_b06.

Launch TgExeVm.exe if there is no correct version of Windows MSI service on the target machine (such as a Windows 98 machine). After you install MSI service, TGExeVm.msi automatically launches.

You can directly launch TgExeVm.msi if there is a correct version of Windows MSI on the machine. You can customize the installation by using tools, such as ORCA. For more information, see "Custom installation" on page 27.

Customizable NoVM kit

The custom NoVM TunnelGuard installation kit does not have JRE bundled.

Launch TgExeNoVm.exe if there is no correct version of Windows MSI service on the machine (such as a Window 98 machine). After you install MSI service, TGExeVm.msi automatically launches.

Launch TgExeNoVm.msi directly if there is a correct version of Windows MSI on the machine. You can customize the installation by using tools, such as ORCA. For more information, see "Custom installation" on page 27.

Standard VM kit

TgVM.exe is a single file installer. It installs MSI if it is not on the machine. The kit includes JRE 1.60_b06.

Standard NoVM kit

TgNoVM.exe is a single file installer. It installs MSI if it is not on the machine. The kit does not include JRE.

Command line and silent installation

Msiexec.exe can be used for installation from the command line. Use the command line switch /qn to indicate a silent installation.

For silent installation, the reboot dialog box is not necessary as a reboot occurs automatically.

You can configure the property NN_CVC701PATH as an installation parameter. For example:

```
Msiexec NN_CVC701FORCEREBOOT=1 /I tgExeVM.msi /qn
```

More examples:

```
Msiexec /I tgExeVM.msi /qn
Msiexec /I tgExeNoVM.msi /qn
```

Other switches include:

```
/I - install
/X - uninstall
```

Nortel VPN Client with TunnelGuard

You can configure the property NN_CVC701PATH as an installation parameter. For example:

```
Msiexec /I tgExeVM.msi NN_CVC701PATH=<path to CVC7.01 setup.exe>
```

If you do not configure NN_CVC701PATH during a full user interface installation, the installation program searches for SETUP.EXE using the assumed path on the CD. If the installation program finds the CVC7.01 installation file, you have the following choices:

- do not install CVC7.01
- install CVC7.01 Domestic version (if domestic kit exists)
- install CVC7.01 Export version (if export kit exists)

If you do not perform a full user interface installation, for example, a silent installation, only NN_CVC701PATH is checked. If you do not configure NN_CVC701PATH, VPN Router Client does not install.

```
Msiexec /I tgExeVM.msi NN_CVC701VERSION=V04_65.22
```

Before the system starts the CVC7.01 installation, the system checks if the user has the same or a later version of the Nortel VPN Router Client installed. If so, installation of CVC7.01 does not launch.

By default, NN_CVC701VERSION is the version that Nortel ships with the CD. If you change the CVC7.01 installation kit, provide the changed version of the kit.

If CVC7.01 launches, whether or not the installation is successful, a reminder to reboot appears at the end of TunnelGuard installation for all nonsilent installations. For silent installation, the reboot dialog box does not appear.

Custom installation

TunnelGuard installation uses Microsoft Installer in MSI file format. A number of tools are available to modify the MSI database, such as ORCA. With an MSI installation file, you can customize the installation, such as change the title, icon, and files to install.

Modify Installation properties

The following sections identify the tables and rows you must modify to make the indicated change.



Caution: All commands are case sensitive.

Change default folder

Table: Directory
Row: Directory = INSTALLDIR1 and its parent directories
Modify: DefaultDir field; replace Nortel Networks with the default folder.

Change default Program menu folder

Table: Directory
Row: Directory = Nortel_Networks_TunnelGuard
Modify: DefaultDir field; replace Nortel Networks TunnelGuard with the default folder name.

Change shortcut icon

Table: Icon
Row: Add new row
Modify: Name = MyCustomIcon.ico

Data: upload the icon file: MyCustomIcon.ico

Table: Shortcut
Rows: Shortcut = TGIconApp.EXE2 and Shortcut = TGIconApp.EXE3
Modify: Icon_ = MyCustomIcon.ico

IconIndex = 0

Change TunnelGuard Icon

The TunnelGuard Agent displays an icon in the Windows system tray. The icon indicates TunnelGuard status. This icon also appears in the About dialog box of the TunnelGuard Agent.

To change the icons for the Agent, perform the following steps:

1. Provide two customized icons: one shown at the start time, the other one shown in the system tray when there is failure.
2. Name the two icon files iconNormal.ico and iconError.ico.
3. Modify the MSI file to replace the two files under [INSTALLDIR]\resources*.ico with the two icon files.

Modify Agent.properties

The Agent.properties file includes settings for how the Agent runs. Administrators can customize and include it in the custom installation.

To change Agent.properties, perform the following steps:

1. Install or extract the Agent.properties file from MSI.
2. Modify Agent.properties according to your requirements.
3. Modify the MSI file to replace Agent.properties under [INSTALLDIR]\resources with the modified file.

Custom TunnelGuard MSI installation example

This example provides sample steps to modify MSI file and replace icon and property files. For more detailed information, see MSI documentation.

This example uses the Microsoft SDK tools ORCA and cabarc.exe to extract the cab file and rebundle cab files.

1. Open TgExeVm.msi with ORCA.
2. In the Cabs table, export the cab file that contains the icon files and property file to a file, for example: mycab.cab.
3. At a command prompt, go to the directory where mycab.cab is saved (ensure cabarc.exe is in the path).
4. Enter the command:
   ```
   cabarc L mycab.cab > list.txt
   ```
5. Modify text file list.txt, so that it only contains a list of file names.

For example:

```
log4j1.2.3.jar
TunnelGuard.jar
AgentTerminator.exe
TGIconApp.EXE
TGIcon.DLL
ProcessInfoWIN.DLL
PartnerAPI.DLL
TGIconAppRC.DLL
Agent.properties
CueAgent_srv.exe
CueAgent_app.exe
curves.jar1
EccpressoCore.jar2
EccpressoJcae.jar3
license.txt
iconError.ico
iconNormal.ico
```

6. To extract all the files from the cab file, enter the command:
   `cabarc X mycab.cab`.
7. Replace the icon files and Agent.properties file with the custom files, ensure you do not change the file names.
8. Enter the command:
   `cabarc n mynewcab.cab @list.txt`
9. In ORCA, in the Cabs table, import `mynewcab.cab`.

Custom installation options

TunnelGuard core functionality is separate from the desktop monitoring application. Custom installation options provide the end user with two features:

- TunnelGuard Core
- Desktop Monitor

This separation allows the administrator to configure the MSI installer to provide a customized installer to the end user. TunnelGuard Core contains all TunnelGuard functionality that includes TunnelGuard Service, but excludes the Desktop Monitor application. The Desktop Monitor application places an icon in the system tray and provides popups for failures and menu options.

The custom installation options provide the following items to the end user:

- system tray icon
- optional TunnelGuard logs
- no or limited popups
- hyperlink in TunnelGuard Agent

TunnelGuard system tray icon

When the TunnelGuard Agent runs on a system, the TunnelGuard icon appears in the system tray in the lower-right corner of the window. This icon provides configuration and failure notification.

When you right-click the TunnelGuard icon, the shortcut menu contains the following commands:

- Show Status Information—displays the TunnelGuard log
- Configuration—configures log settings
- About—provides version and copyright information

If there is a check failure, the TunnelGuard icon shows a slash through it, which indicates a failure condition. After you read the information in the Status dialog box, the slash clears.



Note: The TunnelGuard Agent system tray icon formerly provided the menu command Exit. This feature is discontinued.

TunnelGuard logs

The TunnelGuard log file is in the \Program Files\Nortel Networks\TunnelGuard\logs directory. This file contains the same alert information as the status display and additional information.

VPN Router event log

The VPN Router event log contains information regarding TunnelGuard status. It notes if a check fails, the restricted filter drops, or no communication establishes with the Agent.

Nortel VPN Client log

The Nortel VPN Client log file does not contain information regarding TunnelGuard. If TunnelGuard disconnects a Nortel VPN Client session, the only information noted in the client log is that the server requested the disconnection.

TunnelGuard Agent logs

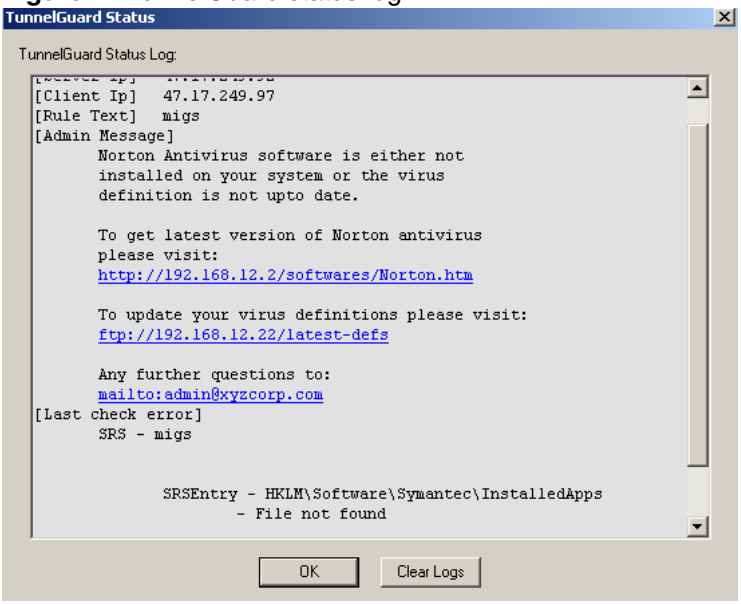
TunnelGuard Agent logs are an optional feature included with Windows Installer. By default, logging is enabled for standard installation. To view the TunnelGuard Status log, right-click the TunnelGuard icon in the system tray and choose the Status Information menu command.

You can modify the registry settings on the desktop PC to enable or disable TunnelGuard logging. To disable logs from being created on the desktop PC, set DisableLogging to 1, as follows:

DisableLogging=1

The following figure shows the TunnelGuard Status log that appears in the TunnelGuard Status console window when an SRS rule fails. The log provides links to update the missing software.

Figure 1 TunnelGuard status log



No or limited messages

The TunnelGuard Agent provides a dialog box when an SRS check failure occurs, regardless of the policy on the Nortel VPN Router for the rule. In some installation scenarios, this feature is not desirable. When SRS checks log failures, the Detail switch reveals all of the information about rule contents and exact expectations for system compliancy. Some VPN administrators choose to hide some or all of this information from end users.

You can hide messages in the following ways:

- Install TunnelGuard without the Desktop Monitor feature to ensure no pop-up messages generate on the desktop PC.
- Install TunnelGuard with the Installer property DisablePopup set to 1 to ensure no messages generate on the desktop PC, even after you install Desktop Monitor. This feature works on registry settings on desktop PCs, so you can modify the registry settings to change the behavior.

- Install TunnelGuard with the Installer property HideTaskbarIcon set to 1 to ensure no pop-up messages generate and no taskbar icon appears in the system tray, even when Desktop Monitor runs on the system. This feature works on registry settings on desktop PCs, so you can modify the registry settings to change the behavior.
- By default the Agent.properties file contains displayLastCheckError = false, so there are no details about why TunnelGuard rejected the user (except the rule name). To display the detailed TunnelGuard logs, set displayLastCheckError = true in the Agent.properties file, which is located by default at C:\Program Files\Nortel Networks\TunnelGuard\resources. All commands in Agent properties are case sensitive, so ensure the commands match or no logs generate.



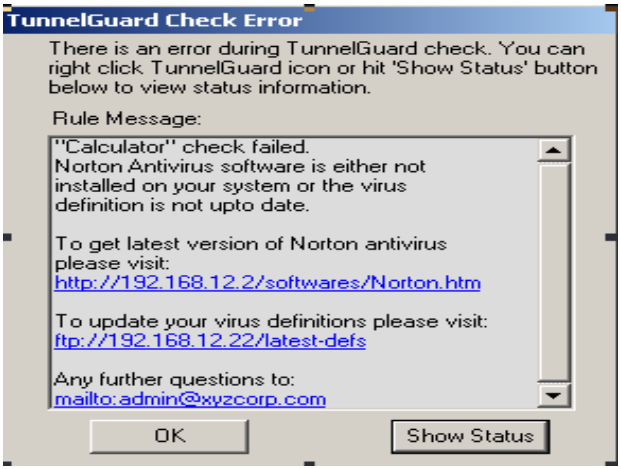
Caution: If you display log details, it can open a security hole because users can use this information to make their PC comply with the TunnelGuard rule.

TunnelGuard Agent error message

The TunnelGuard Agent presents an error message on desktop PCs when an SRS rule fails. This error message is comprised of an SRS rule and an SRS comment. The SRS comment has hyperlinks that provide rule-specific locations to download information for compliance.

The following figure shows the message with clickable links that appears on the desktop PC after an SRS rule fails.

Figure 2 TunnelGuard check error



Initial Failure Recovery Mode

Initial Failure Recovery Mode overcomes many situations that cause you to stay in restricted tunnel mode for long durations. If the TunnelGuard Agent detects SRS FAILURE/UPDATE on the first check, it goes into Initial Failure Recovery Mode. This mode enables a faster, more frequent SRS compliance check by the Agent. The TunnelGuard Agent does not engage the Nortel VPN Router until there is a change in compliance. After the system falls back into compliance, or the Failure Recovery Mode interval expires, TunnelGuard comes out of Failure Recovery Mode. The default failure recovery interval is 10 seconds. You can configure the failure recovery interface by using TunnelGuard properties. The duration of Initial Failure Recovery Mode is the length of the first intrainterval checking.

TunnelGuard banner support

You can configure TunnelGuard to effectively communicate information and instructions to end users who use the TunnelGuard Agent.

You can use the TunnelGuard banner to communicate information to the user, including a standard banner message that informs users that a restricted filter is in place until the SRS conditions are met.

Build scripts and targets stamp the executable and jar file with updated version information. The banner for the TunnelGuard Agent appears on the About the Nortel VPN Router window. The banner for the jar file appears in the Java Console logs.

Chapter 2
TunnelGuard configuration

This chapter provides information about how to configure the TunnelGuard feature to secure limited access to Nortel VPN Router connections.

You can add and delete applications for the TunnelGuard Agent to check. However, the Software Requirement Set (SRS) defines the applications that the gateway checks. The TunnelGuard server communicates directly with the TunnelGuard Agent on the client PC over a socket connection.

TunnelGuard Server configuration

This section provides you with the procedures to perform the initial configuration of TunnelGuard.

- "Configuring TunnelGuard filters" on page 37.
- "TunnelGuard administration" on page 43.
- "Configuring TunnelGuard group settings" on page 39.

Configuring TunnelGuard filters

Before you define the restricted filter, you must identify the interaction between TunnelGuard and the Nortel VPN Router Stateful Firewall (VSF) and filters.

TunnelGuard requires a User Datagram Protocol (UDP) and TCP port for communications between the TunnelGuard Server on the Nortel VPN Router and the Agent on the PC.

After the initial tunnel setup, the server attempts to contact the client on UDP port 8121. This port is not configurable. During the conversation, the server tells the Agent what TCP port to use for further communication, such as to receive the SRS. The TCP port is configurable on the Firewall/NAT window. The default TCP port is 8282. To include the UPD and TCP ports in the filters, select the TunnelGuard check box in the Remote Servers section of the Tunnel Filters > Edit window.

Tunnel Filters are separated into two logical units: Tunnel Filters and Tunnel Management Filters. Tunnel Management Filters control traffic that terminates on the management IP address of the Nortel VPN Router. Tunnel Filters control all other traffic. With respect to TunnelGuard, all communication terminates on the management IP address. Because the VSF has an implied rule for the management interface to the trusted (tunnel) interface, no additional firewall rule is needed for TunnelGuard; if the VSF runs, you can disable the Tunnel Management Filters without affecting TunnelGuard traffic flow.

To configure TunnelGuard, perform the following steps:

1. Log on to the Nortel VPN Router management interface.
2. Create a restricted filter or select a predefined one.

   The filter you use as the TunnelGuard Restricted Filter must be configured to support TunnelGuard traffic.
3. Choose **Profiles**, **Filters**.
4. From the **Current VPN Router Tunnel Filters** list, select the filter you want to enable for TunnelGuard, and then click **Edit**.

   OR

   To create a new Restricted Filter, enter a new filter name and click **Create**.

   The Tunnel Filters > Edit window appears.
5. In the **Allow Management Traffic For these Remote Servers** section, select the **TunnelGuard** check box.
6. Click **OK**.
7. Choose **Services**, **Firewall/NAT.**

   The Firewall/NAT window appears.

8 Scroll down to the **TunnelGuard Configuration** section.

9 In the **Server Port** box, enter a TCP/IP port number for the TunnelGuard Administration to use when it connects to the TunnelGuard Agent.

A separate port number is used for SSL communication. No action is required if the default port is used.

Configuring TunnelGuard group settings

After you create software and rule definitions, configure the TunnelGuard group settings. The following table lists TunnelGuard group configuration settings that the TunnelGuard agent and applet uses.

Table 2 TunnelGuard group settings

TunnelGuard group settings	Used by Agent	Used by Applet	Notes
TunnelGuard	Y	Y	Enables and disables TunnelGuard settings globally.
Restricted Filter	Y	Y	For firewall user authentication (FWUA), this setting applies after a firewall rule is matched.
Policy	Y	Y	
Periodic Check Interval (mins)	Y	Y	
Agent Query Timeout Interval (sec)	Y	N	
Agent Absent Action	Y	N	
Initial Policy Failure Action	Y	Y	For TunnelGuard-FWUA, this action applies anytime the policy fails, not just the initial time.
Banner	Y	N	FWUA has its own banner.
Agent Minimum Version	Y	N	
Heartbeat Interval (sec)	N	Y	
Heartbeat Retry	N	Y	
Display Error Detail	N	Y	
JRE Location	N	Y	
Log Level	N	Y	

To configure the TunnelGuard groups settings, perform the following steps:

1. Choose **Profiles**, **Groups**.
2. Select a group, and then click **Edit**.

   The Groups > Edit window appears.

3. In the **Connectivity** section, click **Configure.**

The Groups > Edit > Connectivity window appears.

4 Scroll down to the TunnelGuard settings section of the window.

The first setting in the TunnelGuard section is the TunnelGuard list.

5 From the **TunnelGuard** list, select **Enabled**.

6 From the **TunnelGuard: Restricted Filter** list, select a restricted filter for use with the selected group while the verification process is in progress.

If necessary, choose Profiles, Filters to define a restricted filter.

7 In the **TunnelGuard: Policy** section, select or define the TunnelGuard policy or rule to apply to the group.

SRS policies must be previously defined to appear in the list. The list includes all rules defined using the SRS Builder. If no policy is listed, you can click the Define New Policy (Firewall/NAT page) link to create one.

8 In the **TunnelGuard: Periodic Time Check Interval (mins)** box, enter the time interval at which you want to configure the periodic time check.

9 In the **TunnelGuard: Agent Query Timeout Interval (sec)** box, enter the interval at which you want the Agent query to timeout.

10 From the **TunnelGuard: Agent Absent Action** list, select one of the following options:

- **Leave Restricted and send banner if configured**
- **Tear down tunnel and send banner if configured**

11 From the **TunnelGuard: Initial Policy Failure Action** list, select one of the following options:

- **Tear down tunnel**
- **Leave Restricted**
- **No Action**

12 In the **TunnelGuard Banner** box, enter the message text.

The text you type appears on the user security banner after the user logs on to the VPN Router firewall.

13 From the TunnelGuard Agent Minimum Version lists, set the minimum allowable version of TunnelGuard.



14 In the **TunnelGuard: Heartbeat Interval (sec)** box, enter the time (seconds) to set the amount of time between Heartbeats sent by the TunnelGuard applet.

15 In the **TunnelGuard: Heartbeat Retry** box, enter the maximum number of retries for the Heartbeat Interval.

After the configured number of retries, TunnelGuard declares the server dead.

16 Select the **TunnelGuard: Display Error Detail** check box to enable users to view information about why their TunnelGuard check failed.

17 In the **TunnelGuard: JRE Location** box, enter the address string of the JRE.exe.

The user retrieves the JRE at this URL address, if not already installed.

18 Select an option from the **TunnelGuard: Log Level** list to set the type of information the agent logs send to the Java console. Options are:

- **FATAL**
- **ERROR**
- **WARN**
- **INFO**
- **DEBUG**

19 Click **OK**.

Note: Messages can appear when you change some of the TunnelGuard default settings. Nortel recommends that you read the messages and take appropriate action. For example, after you change the Restricted Filter and click OK, a message appears at the top of the Groups window. The message prompts you to follow the link to the Filters window to edit the selected TunnelGuard filter. This ensures that the selected filter allows TunnelGuard traffic.

Chapter 3
TunnelGuard administration

This chapter provides procedures to modify Software Requirement Set (SRS) definitions, rules, and rule expressions in the TunnelGuard Administration applet.

TunnelGuard Administration GUI

You can use the TunnelGuard Administration GUI to perform the following tasks:

- Select one or more predefined SRSs
- Modify predefined SRSs
- Create new SRSs

For more information about the Nortel TunnelGuard Administration GUI, see "TunnelGuard Administration GUI" on page 65.

Logging on to TunnelGuard Administration

To log on to TunnelGuard Administration, perform the following steps:

1. Choose **Services, Firewall/NAT**.
2. Scroll down to the **Rule Configuration** section.
3. Click **Manage Policies**.

   The Password Needed - Networking dialog box appears. The router prompts you to log on to TunnelGuard Administration.

4. Log on to the TunnelGuard Administration applet using a valid system administrator name and password.

The Nortel TunnelGuard Administration window appears with the Predefined Software Definition tab selected.

Selecting and modifying a predefined software definition

TunnelGuard Administration provides predefined sets of Software Definition Entries that you can select and use to create an SRS. The basic building blocks of these Software Definition Entries are also available.

Some configurable Software Definition Entry options are:

- age of definition files
- engine version check
- real time protection state
- last scan time
- product expiration
- trigger live update
- trigger full file system scan
- firewall state
- manage windows firewall rules

You can join predefined Software Definition Entries to create one Software Definition. You can join this definition with other custom software definition entries using boolean operands (and, or, and not) to create a TunnelGuard rule.

To select a predefined Software Definition entry, perform the following steps:

1. Launch the TunnelGuard Administration GUI.

   The Nortel TunnelGuard Administration window appears with the Predefined Software Definition tab selected.

2. Choose Predefined **Software Definition**, **New Definition**.

   The New Software Definition dialog box appears.

3. Enter a software definition name and select the operating system.

4. Click **OK**.

5 From the **Available Software Definitions** list, select a software definition entry.

You can select multiple entries by pressing the Shift key while you make contiguous selections or pressing the Control key while you make noncontiguous selections.

6 Click the add button (**<**).

7 Select either the **All** or **Any** option from the **Selected Predefined Entries** list.

- All—all selected software are required to be present
- Any—any one of them needs to be present on desktop PC

8 For each software definition entry, you can optionally configure the following settings in the **Antivirus/Antispyware Configuration** and **Firewall Configuration** tabs:

- Customize an entry to check for definition file, engine version, and other requirements based on type of entry.
- Configure the action to run if policy fails based on type of entry.
- Configure firewall settings.



Note: When you use the Predefined Software Definitions in TunnelGuard, be aware that the Trigger Definitions Update setting is considered to be part of a single rule definition. When this is enabled with other rule checks, TunnelGuard will report a failure first and then the Trigger Definitions Update will execute. Consequently, if the Administrator would like the tunnel to be torn down immediately upon failure, the NVR Groups > Connectivy Option "TunnelGuard: Initial Policy Failure Action" should be set to Teardown Tunnel and then the "Trigger Definitions Update" will run through the local interface and not the tunnel.

Creating a software definition

When you configure the first policy, ensure that the parent of the group also uses a policy. You must configure the first policy for /Base group to enable all subgroups to inherit the policy.

To create a Software Definition, perform the following steps:

1. Select the **Custom Software Definitions** tab.
2. Select **Custom Software Definition, New Software Definition**.

   The New Software Definition dialog box appears.

Note: Alternatively, you can import data for SRS, Multiple SRS, SRS rule, or Multiple SRS rules either by choosing File > Import File or File, Import All.

After you import the file, the imported SRS and SRS rules overwrite existing SRS and SRS rules.

---

3. Type a name for the SRS definition.

   For example, you can use the name Antivirus if you create an SRS definition that specifies the antivirus software modules that must be present on the client system that runs the TunnelGuard Agent.
4. From the **Operating System** list, choose an operating system.
5. From the **Add Software Definition Entry** section, click to highlight one of the following:
   - **New Disk Entry,** see "Adding an OnDisk file entry" on page 56.
   - **New Memory Module Entry,** see "Adding a Memory Module entry" on page 57
   - **New Registry Entry**, see "Creating a registry entry" on page 53
   - **None**
6. Click **OK.**

   Auto Generate TunnelGuard rule is enabled by default. This causes a rule of the same name as the SRS to be created and placed in the Available Expressions section of the Rule Definition tab.

7. Select the application, or process, that you want to include in the SRS from the process list on the left of the Memory Snapshot section.

   The Memory Snapshot section in the lower half of the Software Definition window displays all processes that currently run on the system on which you run the TunnelGuard Administration.

When you select a process on the left, all its associated modules are listed on the right.

8 Select the modules for this SRS definition that are required on client systems.

Double-click to select a module that currently runs and load the module into the memory snapshot to the SRS set or choose the Add a selected memory module menu command.

9 Create a rule definition for this software definition, see "Creating a rule definition" on page 48.

Creating a rule definition

To create a rule definition, perform the following steps:

1. To define TunnelGuard rules for the SRS that you created, click the **Rule Definition** tab.
2. Choose **TunnelGuard Rule**, **New TunnelGuard Rule**.

   The New TunnelGuard Rule dialog box appears.

3. Type a name for the rule, and then click **OK**.

   The Available Expressions section initially lists automatically-generated SRS expressions. Autogenerated rules generate automatically when the Auto Generate TunnelGuard Rule option in the Software Definition menu is enabled (default). This setting causes a rule of the same name as the SRS definition to be created and placed in the Available Expressions section of the Rule Definition window.

4. Select a rule expression from the **Available Expressions** section.
5. Click the add button (>) to move the selected expression into the **Rule Expression Constructor** section.

   When more than a single expression is available in this section, the Form TunnelGuard Rule Expression button becomes active, which you use to create a Boolean AND/OR expression comprised of the available expressions. You can also create an expression using NOT. The NOT expression is based on one rule, as compared to AND and OR, which are based on two or more rules.



Note: The NOT expression allows the creation of rules that are used as quick and basic checks against certain kinds of known viruses, worms, ad-ware, P2P file-sharing software, and spy-ware.

6. Select the expression type that you want to form, either an AND expression, an OR expression, or a NOT expression, using the option buttons.
7. Click **Form TunnelGuard Rule Expression** to construct the new expression.

   When the expression is constructed, it automatically appears in the Available Expressions list.

Combine AND expressions with OR expressions to create nested statements. For example, you can create a rule expression, such as IPsec_Client OR (Antivirus AND RemoteAccessMgr) to specify that the client system must have the software specified by the IPsec_Client SRS, OR it must have at least the minimum set of software as specified by the Antivirus AND RemoteAccessMgr SRS definitions.

8 In the **Display Message on Failure** column, click **<click to create message>,** and then click the ellipsis button (**...**).

The Rule Comment dialog box appears.

9 Enter the message that you want to display to the user.

10 In the **Rule Action** column, click **<click to create action>**, and then click the ellipsis button (**...**).

The Rule Action Constructor dialog box appears.

11 Enter an action in the **Action Name** box

12 Enter the command in the **Command Text** box

To ensure that this command executes reliably, Nortel recommends that you enter the full path to the executable, for example: c:\windows\system32\calc.exe instead of calc.exe.

13 Select the command type from the **Command Type** list.

14 Select an **Operating System**.

15 Select a type of action: **Run Once on Success** or **Run Once on Failure**.

16 Click **OK**.

You can define a local script that runs if rules are in or out-of-compliance as every SRS rule has a configurable option to run Rule Action in response to a rule success or failure. You can add the name of an executable or batch file that is available on a local PC or the network. The command runs on a PC with system account privileges, but does not have access to the user desktop.

If Run Once on Success is selected, the command text is executed after the SRS rule is successful on the PC. The command is executed exactly one time after success for a session. If policy failure is encountered after success, the counter resets and on subsequent success, the command executes again. In the same way, the Run Once on Failure command runs one time after the SRS rule failure is encountered.

Error messages are not logged in the Event Log for a failed launch of a script or executable file. SRS failure messages can appear when launching programs that are later checked as part of SRS compliance.

For example, on SRS failure, a script is run to start mustload.exe. If mustload.exe is checked for presence in the memory, then on the next SRS check the success of the script is logged.

17 Click **OK**.

The new Rule Action script is added to the rule.

18 After you complete the SRS definitions, Rules, and Rule Expressions, choose **File**, **Save**.

Registry-based rules

The TunnelGuard Agent supports checking of on-disk files, running processes, hash checking, and version numbers to verify installed software packages. Reading the registry settings on a client PC is another way of checking software packages and their installed state.

Operating system types

When compliance checking, the TunnelGuard Agent checks for the SRS compliance that belongs to its operating system type, but skips other SRS or SRS entries. If no SRS entries and SRSs belong to the TunnelGuard Agent operating system, all checking is skipped and the TunnelGuard Agent reports SUCCESS.

To create a registry on the basis of the operating system type without rule checking, create an empty SRS. Select only those operating systems in the Software Definition that you want checked for compliance. Any Software Definition entry specific to an operating system does not contribute to the final decision of compliance on other operating systems.

Registry entry creation

TunnelGuard Agent and TunnelGuard applet supports registry-checking functionality only if you use Agent 2.0 or later.

Use the administrator tool applet to add Registry Key checks into SRS entries. You can check for the existence of certain Registry Keys and enforce their values on a desktop PC before you allow access to the network. One SRS entry holds Registry Key checks, just as one SRS entry holds file checks. Contrary to file and process checks, Registry Key checks do not have hash checking, date, and version number check enabled. However, you can combine Registry Key check entries with another type of check, such as process check or on-disk entry check.

Registry-based rules are most useful in instances where rules are based on Registry Key Values. TunnelGuard supports simple regular expressions-based rules for Registry Key Values.

The TunnelGuard Agent leverages the advantage of being a Java-based application and uses the pattern and regular expression support available in JRE. TunnelGuard Agent provides all relevant pattern-matching facilities based on regular expressions provided by JRE.

Registry Key values of type string and integer are supported. Binary data type for Registry Key values is not supported.

Supported operands for integer values are:

- >=
- <=
- ==
- !=
- <
- >

Examples of regular expressions for integer Registry Key values are:

- >= 20
- = 100

- < 50
- != 200

The following table show supported constructs for string-based regular expressions.:

Table 3 Constructs for string-based regular expressions

String regular expression	Description
x	The character *x*
.	Any character
\\	The backslash character
\0*n*	The character with octal value 0*n* (0 <= n <= 7)
xhh	The character with the hexadecimal value 0*xhh*
\t	The tab character ('\u0009')
\n	The newline (line feed) character ('\u000A')
\d	A digit: [0-9]
\D	A non-digit: [^0-9]
\s	A whitespace character: [\t\n\x0B\f\r]
\S	A nonwhitespace character [^\s]
\w	A word character: [a-zA-Z_0-9]
\W	A nonword character [^\w]
[abc]	a, b, or c
[^abc]	not a, b, or c
[a-z]	characters a through z
[a-d[m-p]]	a through d, or m through p: [a-dm-p] (union)
[a-z&&[def]]	d, e, or f (intersection)
[a-z&&[^bc]]	a through z, except for b and c: [ad-z] (subtraction)
X?	*X*, once or not at all
*X**	*X*, zero or more times
X+	*X*, one or more times
X{*n*}	*X*, exactly *n* times
X{*n*,}	*X*, at least *n* times
X{*n*,*m*}	*X*, at least *n* but not more than *m* times

Table 3 Constructs for string-based regular expressions (continued)

String regular expression	Description
\	Nothing, but quotes the following character
\E	Nothing, but ends quoting started by \Q
\Q	Nothing, but quotes all characters until \E
^	The beginning of a line
$	The end of a line
\b	A word boundary

The following list shows examples of regular expressions for string-based Registry Key values:

- ^Nortel .*Networks — matches anything that starts with Nortel and ends with Networks
- \w* — matches TunnelGuard_2; does not match TunnelGuard_2.0.0 (word definition includes_but not ".")
- [a-z] {2}_[\.\d]+ — matching tg_2.0.0; does not match Tg_2.0.0; does not match tg_; does not match tg_two; does not match tug_2.0.0

Creating a registry entry

To create a registry entry, perform the following steps:

1. Click the **Custom Software Definition** tab.
2. Choose **Custom Software Definition**, **New Software Definition Entry**.

   The New Software Definition dialog box appears.
3. Select **New Registry Entry**.

   The Registry Entry window appears.
4. In the **Registry Key Path**, enter the filepath to the Registry Key.
5. Type the key value.
6. Select the **Check for Expressions** check box.
7. From the **Key Value Type** list, select an option: **String** or **Integer.**

8 In the **Key Value Data Expression** box, enter the key value data expression.

9 From the **Operating System** list, select an option.

You can select more than one option. To select all operating systems, select the **All Windows** check box.

10 Click **OK**.



Note: If you want to create multiple entries, click Save and More. This operation saves this entry and another window opens for you to create another Registry entry.

OnDisk and Memory Module entries

The TunnelGuard applet provides OnDisk and Memory Module buttons to create custom SRS entries and rules without installation on a desktop PC. To create these rules, you must know the name of the executables or files to check. Because these rules are created manually, extra care is required to avoid mistakes. The TunnelGuard Agent and TunnelGuard Applet support the wildcard expression (*) in the file path for On Disk-based SRS Entries. You can use the wildcard (*) for filenames, but not for directory names. For example, you can use C:\Program Files*.txt, but not C:*\abc.txt.

Registry-based file or module

If the file or module path or name is not known to the administrator or is not static for SRS rule creation, the filename or module is sometimes available as Registry Key Value data. You can define a Registry Key to look for and derive a File or Module path and name from the Registry Key Value data. This path is then treated exactly as other OnDisk entries or Memory Module entries that you define.

Registry-based path variables

OnDisk and Memory Module SRS entries support registry-based path variables and regular file path entries, such as C:\Program Files\Nortel\TunnelGuard\myApplication.exe. TunnelGuard parses the registry-based path variables to fetch actual Key Value data that replaces these variables before actual on disk files or process scanning begins.

Registry-based path variables are embedded inside file or module paths and process names with <REG> and </REG> tags as shown in the following example:

C:\<REG>HKLM\Software\Nortel\TG\Key1</
REG>\TunnelGuard\<REG>HKLM\Software\Key2</REG>

The actual Registry Key value of Key1 replaces the path variable <REG>HKLM\Software\Nortel\TG\Key1</REG>. The actual Registry Key value of Key2 replaces <REG>HKLM\Software\Key2</REG>. Multiple registry-based variables can exist inside one path, but they cannot be embedded inside one another.

Adding an OnDisk file entry

To add an OnDisk SRS file entry, perform the following steps:

1. Select the **Software Definition** tab.
2. Choose **Software Definition Entry**, **New Disk Entry.**

   The Create New OnDisk SRS Entry window opens.
3. Click **Browse Local System** to select the file or module path.

   The file or module path appears in the text box and the rest of the information in the window is filled in automatically.
4. If you select the **Fetch Module Path from Registry Entry** check box, you must manually enter the **Registry Entry** and the **Key Value**.

   The other fields on the window must also be completed manually. You can use the wildcard expression (*) in the file path.

   Enter a regular file path name or registry-based path variables into the text box.
5. To enable Hash Checking, select the **Enable Hash Checking** check box and enter a hash key.
6. To enable Vendor APIs, select the **Vendor AP Call Check** check box.
7. Select an option for **Min Version**.

   If you select Any, the dates are deselected and the boxes are cleared. If you select Specify Min Version, enter the minimum version in x.x.x.x format.
8. Select an option for **Max Version**.

   If you select Any, the dates are deselected and the boxes are cleared. If you select Specify Max Version, enter the maximum version in x.x.x.x format.
9. Select either the **Relative Date/Time Range** or **Specific Date/Time Range** check box.

   When TunnelGuard is used, most desktop PCs have antivirus software with virus-definition files that are updated weekly, biweekly, or monthly. In this situation, you can create a rule to not allow users with virus definitions older than, for example, seven days.

Use the Relative Date/Time Range option to specify a Not Older Than option. If this option is selected, To and From dates are automatically deselected.

a If you select **Relative Date/Time Range**, enter the number of days in the **Not Older Than (in days)** text box.

b If you select **Specific Date/Time Range**, select the option for either **Any** or **Specify Date/Time** from the **From Date/Time** and **To Date/Time**.

— If you selected **Specify Date/Time**, enter the specific date and time in the **From Date/Time** and **To Date/Time** text boxes.

10 Select an **Operating System**.

If you want to enable all operating systems for selection, select the All Windows check box. To enable specific operating system types, select the Windows operating systems check boxes.

11 Click **OK**.

If you want to check that the pathway is valid or that the variables in a registry-based path can be parsed correctly, click Check Validity. If you want to create multiple entries, click Save and More to save this entry and another window opens for you to create another Registry entry.

Adding a Memory Module entry

To add a Memory Module entry, perform the following steps:

1 Click the **Custom Software Definition** tab.

2 Choose **Software Definition Entry**, **New Memory Module Entry**.

The Create New Memory Module SRS Entry window appears.

3 Enter the process name in the **Process Name** box.

4 To disable path checking, select the **Ignore Path Checking** check box.

5 Click **Browse Local System** to select the file or module path.

The file or module path appears in the box and the rest of the information in the window is automatically populated.

6 To enable the system to fetch the module path from the registry entry, select the **Fetch Module Path from Registry Entry** check box.

If you choose to enable the Fetch Module Path from Registry Entry setting, you must manually enter the Registry Entry and the Key Value. The other fields on the window must also be completed manually.

7 To enable hash checking, enter a hash key in the **Enable Hash Checking** box.

8 To enable vendor API call check, select the **Vendor API Call Check** check box.

9 Select an option for **Min Version**.

If you select Any, the dates are deselected and the boxes are cleared. If you select Specify Min Version, enter the minimum version in x.x.x.x format.

10 Select an option for **Max Version**.

If you select Any, the dates are deselected and the boxes are cleared. If you select Specify Max Version, enter the maximum version in x.x.x.x format.

11 Select either the **Relative Date/Time Range** or **Specific Date/Time Range** check boxes.

When TunnelGuard is used, most desktop PCs have antivirus software with virus-definition files that are updated weekly, biweekly, or monthly. In this situation, you can create a rule not to allow users with virus definitions older than, for example, seven days.

The Relative Date/Time Range option allows you to specify a Not Older Than option. If this option is selected, To and From dates are automatically deselected.

a If you select **Relative Date/Time Range**, enter the number of days in the **Not Older Than (in days)** text box.

b If you select **Specific Date/Time Range**, click a radio button for either **Any** or **Specify Date/Time** from the **From Date/Time** and **To Date/Time**.

— If you selected **Specify Date/Time**, enter the specific date and time in the **From Date/Time** and **To Date/Time** text boxes.

12 Select an **Operating System**.

If you want to enable all operating systems for selection, check the All Windows check box. To enable one for more specific operating system types, select the Windows operating systems check boxes

13 Click **OK**.

If you want to check that the pathway is valid or that the variables in a registry-based path can be parsed correctly, click Check Validity. If you want to create multiple entries, click Save and More to saves this entry and another window opens for you to create another Registry entry.

Chapter 4
FWUA with TunnelGuard configuration

Firewall user authentication (FWUA) with TunnelGuard extends the capabilities of FWUA. FWUA downloads the TunnelGuard applet after the user authenticates. TunnelGuard then verifies that the PC has the proper patches installed and runs antivirus software before it grants access to the network.

FWUA with TunnelGuard employs the same process of stateful firewall rules as does FWUA without TunnelGuard. However, if FWUA with TunnelGuard is enabled and the user is out-of-compliance, TunnelGuard performs an extra check. The TunnelGuard restricted filter runs against the packet to determine if that packet is allowed, and returns the appropriate pass or fail result.

Proxy IP address

FWUA typically allows for a proxy IP address where one user can log on to FWUA on behalf of another IP address. This ability is incompatible with TunnelGuard because the TunnelGuard rules must run on the PC of the user who is obtaining access. If a user in such a group attempts to utilize the proxy IP address feature, an error is received and the FWUA logon fails.

Anonymous FWUA User option

When you use the Anonymous FWUA User option, all anonymous user group properties are in effect, including the number of logons. You must increase the number of logons to the maximum number of FWUA users that you want to concurrently access the switch.

TunnelGuard timeouts

Three configuration parameters determine TunnelGuard timeout functionality:

- TunGuardCheckInterval
- TunGuardHbInterval
- TunGuardHbRetry

TunGuardCheckInterval

TunGuardCheckInterval determines how often the TunnelGuard server requires the agent to perform a status check. After this amount of time passes, the server responds to the next heartbeat with a check request. The agent performs interval checks. If the agent notices the expiration and changes state, it indicates this in its heartbeat. This change in state causes the server to immediately issue a proper check request. The agent status check must complete within the TunGuardCheckInterval time or the agent is disconnected.

TunGuardHbInterval

TunGuardHbInterval defines the time between heartbeats that the agent sends.

TunGuardHbRetry

TunGuardHbRetry indicates the amount of heartbeats that the agent and server can miss before each decides the other is unreachable and terminates the session. Therefore, the two can be out-of-communication for the amount of time (in seconds) calculated as the TunGuardHbInterval multiplied by the TunGuardHbRetry before they disconnect.

Configuring FWUA with TunnelGuard

To configure FWUA with TunnelGuard, perform the following steps:

1. Configure FWUA.

   For more information about FWUA, see *Nortel VPN Router Configuration—Firewalls, Filters, NAT, and QoS* (NN46110-508).

   Note the check box for TunnelGuard Checking Only (Anonymous FWUA User option) on the Firewall UA Settings window. When selected, FWUA for TunnelGuard enforcement only is enabled, which removes the need for the user to log on to FWUA. This option also provides the name and password fields in which you provide a user name and password for the user. All FWUA users use this user name and password to anonymously log on. You must create this user account and configure its group appropriately.

2. Configure TunnelGuard Administration. For more information about TunnelGuard Administration, see "TunnelGuard Server configuration" on page 37.

Appendix A
TunnelGuard Administration GUI

Use the TunnelGuard Administration GUI to create SRS definitions, rules and rule expressions.

TunnelGuard Administration window

The TunnelGuard Administration window appears after you successfully log on with a valid administrator user name and password.

Editing options for TunnelGuard SRS entries

TunnelGuard Administration provides the following options to help you edit TunnelGuard SRS entries:

- Multi row selection—you can select multiple SRS entries by using the Control or Shift keys, and then either delete or copy and paste them at different locations.
- Keyboard shortcuts—keyboard shortcuts exist for most menu tasks. For example, you can press the Delete key to delete a TunnelGuard Administration SRS entry.
- Double-click to edit—double-click an SRS entry to open one consolidated editing window when modifying SRS entry attributes.
- Right-click options—a shortcut menu is available for most tasks. You can right-click an SRS, SRS entry, or SRS rule, and then choose a relevant command from the shortcut menu. For example, to customize a Software Definition, select the definition, right-click and choose Edit from the menu, or click the Edit SRS icon on the toolbar.

- Progress bar—TunnelGuard Administration can stop responding when you use the Save command, the memory snapshot, or when numerous tasks are implemented at the same time. TunnelGuard Administration displays a progress bar to show you the current status of the task until the task is complete.

Menu Commands and icons

The TunnelGuard menu commands correspond to the icons on the toolbars.

Table 4

Menu	Icons
File	Save, Export, and Exit icons
Edit	Preferences
Predefined Software Definition	New, Delete, Clone, Export, and Edit Software Definition
Custom Software Definition	New, Delete, Clone, Export, and Edit Software Definition
Software Definition Entry	New Disk, New Memory Module, New Registry, Delete, Copy, and Paste Entry
TunnelGuard Rule	New, Delete, Clone, and Export TunnelGuard
Tool	Show Memory Snapshot and Refresh Memory Snapshot
Help	Help and About displays version information as well as information about the server from where it was downloaded.

File menu

The File menu includes the commands in the following sections.

Save

Save the SRS definition in the gateway LDAP database.

Connect to

Import All

Import data for an SRS, Multiple SRSs, an SRS rule, or Multiple SRS rules.

Using Import All can overwrite existing SRSs or SRS rules. You cannot save changes after importing as the imported file can overwrite existing SRSs or SRS rules by mistake.

Export All

Export data for an SRS, Multiple SRSs, an SRS rule, or Multiple SRS rules.

You can also select one or multiple SRSs and click Export Software Definition to XML file from the SRS toolbar or shortcut menu. This exports only the selected SRS to a file. You can also export one or multiple SRS rules by selecting an SRS rule and click Export Rule on the toolbar or shortcut menu to export only the selected SRS rule and the SRSs that make up those rules.

Exit

Edit menu

The Edit menu includes the commands in the following sections.

Preferences

Create an XML-based configuration file that resides locally on the desktop PC and can be modified every time you change the settings. Some configuration settings take effect immediately while others take effect on restart of the TunnelGuard Administration. Settings that require a restart display a notification. The following commands display in the Edit menu:

- Look and feel
- Color Scheme
- Default Hash Algorithm —MD5 or SHA1
- Icon size
- Auto Generate TunnelGuard Rule
- Run Memory Snapshot at startup
- Default Size—save current size of Administration applet.

Predefined Software Definition menu

The Predefined Software Definition menu includes the commands in the following sections.

New Definition

Create a new definition.

Delete Definition

Delete the selected definition.

Clone Definition

Clone the selected definition.

Export Definition

Export the selected definition (includes Multiple SRS).

Edit Definition

Edit the selected definition.

Custom Software Definition menu

New Software Definition

Create a new definition.

Delete Software Definition

Delete the selected definition.

Clone Software Definition

Clone the selected definition.

Export Software Definition

Export the selected definition (includes Multiple SRS).

Edit Software Definition

Edit the selected definition.

Software Definition Entry menu

The Software Definition Entry menu includes the commands in the following sections.

New Disk Entry

Select a file from the local file system, for example a text configuration file, and add it as one component of the SRS.

New Memory Module Entry

Add the selected memory module from the current memory snapshot as a required entry.

New Registry entry

Add the Registry Key entry.

Delete Entry

Delete the selected component.

Copy Entry

Copy the selected component.

Paste Entry

Paste the component (from one SRS definition to another).

Edit SRS Entry

Select this command to edit an SRS entry.

TunnelGuard Rule menu

New TunnelGuard Rule

Create a new rule.

Delete TunnelGuard Rule

Delete a selected rule.

Clone TunnelGuard Rule

Clone a selected rule

Export Rule

Export a selected rule or Multiple SRS rules.

Tool menu

Show memory snapshot

Shows the list of processes shown in the Memory Snapshot section of the main window.

Refresh memory snapshot

Refreshes the list of processes shown in the Memory Snapshot section of the main window. You can refresh the view if you launched other applications while running the SRS builder or if other processes started after the SRS builder.

Predefined Software Definitions window

Click the Predefined Software Definition tab to access the Predefined Software Definition window. You use this window to select and manage predefined SRS definitions. The Predefined Software Definition toolbar appears at the top of the window.

Predefined Software Definition toolbar

Use the buttons on the Predefine Software Definition toolbar to select and manage software requirement sets.

New Definition

Use this command to create a new SRS definition.

For more information, see New Software Definition window.

Delete Definition

Use this command to delete the currently selected SRS definition.

Clone Definition

Select this command to create a copy of the currently selected SRS.

Export Definition

Use this command to export an SRS definition to an XML-formatted file.

The Export functions is useful for creating and distributing canned SRS solutions.

Software Definition

The Software Definition section displays a list of SRSs from which you can select and edit the predefined Software Definitions.

Available Software Definitions

The available Software Definition list shown in the Software Definition window is initially retrieved from the Nortel VPN Router and updated when you make changes while running the SRS Builder.

Selected Definition Entries

The Selected Definition Entries section displays the software definitions you selected from the Available Software Definitions list. You can select each entry and configure the Antivirus, AntiSpyware, and firewall settings.

SRS Display Message

Antivirus and AntiSpyware Configuration

This section allows you to configure the Antivirus and Antispyware settings.

Firewall Configuration

This section allows you to configure the firewall settings.

Custom Software Definition window

Click the Custom Software Definition tab to access the Software Definition window. You use this window to create and manage SRS definitions. The Custom Software Definition toolbar appears at the top of the window.

Software Definition toolbar

Use the buttons on the SRS definition toolbar to create, delete, and manage software requirement sets.

Create a new Software Definition

Use this command to create a new SRS definition.

For more information, see New Software Definition window.

Delete an existing Software Definition

Use this command to delete the currently selected SRS definition.

Clone a Software Definition

Use this command to create a copy of the currently selected SRS.

Export a Software Definition to an XML file

Use this command to export SRS definitions to an XML-formatted file.

The Export function is useful for creating and distributing canned SRS solutions.

Edit Software comments

Use this command to add a comment. If the check fails, the specified comment is written to the log.

New Disk Entry

Use this command to create a new disk entry.

For more information, see Create New OnDisk SRS Entry window.

New Memory Module Entry

Use this command to create a new memory module.

For more information, see Create New Memory Module SRS Entry window.

New Registry Entry

Use this command to create a new registry entry.

The TunnelGuard Agent and TunnelGuard Administrator applet supports registry-checking functionality only when using Agent 2.0 or later.

For more information, see Registry Entry window.

Edit SRS Entry

Use this command to edit an SRS entry.

Delete Entry

Use this command to delete the selected command.

Copy Entry

Use this command to copy the selected command.

Paste Entry

Use this command to paste the selected command.

Software Definition list

The available Software Definition list shown in the Software Definition window is initially retrieved from the Nortel VPN Router and is updated when you make changes while running the SRS Builder.

Software Definition table

When an SRS is selected in the Software Definition list, the components of the SRS are shown on the right-hand side in the SRS Components table. The table includes the following information about the components.

Path

This column shows the full directory path to the file location.

Process

The process name, in which the component runs. For files that only exist on disk and do not load in memory, this column does not apply.

Version

This column shows version information of the component.

Date/Time

This column shows the last modified time of the component.

Registry Key

This column shows the Registry Key number.

Registry Exp

This column states the date and time the Registry Key expires.

DiskOnly

If selected, the file does not load in memory. If this option is combined with the API option, the file is loaded and the API called.

API

If selected, the component contains a third-party API for further checking.

About API support

One of the features of TunnelGuard is its ability to interact with other software vendor applications. You can configure TunnelGuard to communicate with other applications and ask for their status. The result of the status check is treated the same as other checks and is reported back to the server. This capability allows administrators to use TunnelGuard to retrieve status from other software packages, such as personal firewalls and virus checkers, to make sure they are running properly.

API calls

TunnelGuard requires a Java class that implements a DLL for Windows platforms that offers at least one common entry point as described below.

```
#include <windows.h>
/*  return values */
#define STATUS_SUCCESS 0
#define STATUS _FAILURE  -1
#define STATUS_REQUIRES_UPDATE 1
/* simple check */
int WINAPI CheckStatus(void);
```

This API blocks information until one of the required statuses is returned in 10 seconds or less. If an answer is not returned in a timely manner, it is assumed the personal firewall software is unavailable, and the call times out and returns an error message.

The basic functionality required for Phase I implementation is the vendor must supply an API that the PFW client can call to check the status of the firewall. The simplest approach is that such a call blocks activity until one of the three following answers returns:

- yes (ok to open the tunnel completely)
- no (tear the tunnel down)
- update_required (leave the tunnel restricted)

Because the Nortel VPN Router cannot support going from the open state back to restricted mode in the initial release, you cannot send the update_required status after a Yes status is sent. This results in the tunnel staying in an unrestricted state.

HashAlg

Hash algorithm used to generate the hash.

Hash

Hash value of the file.

New Software Definition window

Software Definition Name

Enter a name for the SRS definition. For example, you can enter the name Antivirus if you create an SRS definition that specifies the antivirus software modules that must be present on the client system that runs the TunnelGuard Agent.

Operating System

Select an operating system from the list.

Add Software Definition Entry

Click to open one of the following windows:

New Disk Entry—see Create New OnDisk SRS Entry window.

New Memory Module Entry—see Create New Memory Module SRS Entry window.

New Registry Entry—see Registry Entry window.

None —creates only the software definition.

Create New OnDisk SRS Entry window

You can use the wildcard (*) for filenames, but not for directory names. For example, C:\Program Files*.txt can be used, but C:*\abc.txt does not work.

File or Module Path

Click Browse Local System to select the file or module path.

Browse Local System

The file or module path appears in the text box and the rest of the information in the window is filled in automatically.

Fetch Module Path from Registry Entry

If you select Fetch Module Path from Registry Entry, you must manually enter the Registry Entry. Enter a regular file path name or registry-based path variables into the text box.

Key Value

If you select Fetch Module Path from Registry Entry, you must manually enter the the Key Value.

Enable Hash Checking

Enables Hash Checking.

Vendor AP Call Check

Checks Vendor APIs. See also About API support.

Min Version

The minimum version of TunnelGuard that can run. If Any is selected, the dates are deselected and the boxes are cleared.

Max Version

The maximum version of TunnelGuard that can run. If Any is selected, the dates are deselected and the boxes are cleared.

Relative Date/Time Range

The Relative Date/Time Range allows you to specify a Not Older Than option. If this option is selected, To and From dates are automatically deselected.

Enter the number of days in the Not Older Than (in days) text box.

Specific Date/Time Range

If you select Specific Date/Time Range, select either the Any or Specify Date/Time option from the From Date/Time and To Date/Time.

If you selected Specify Date/Time, enter the specific date and time in the From Date/Time and To Date/Time text boxes.

Operating System

If you want all operating systems to be enabled for selection, select the All Windows check box or for a specific operating system type, select one of the Windows operating systems check boxes.

Check Validity/Save and More

If you want to check that the pathway is valid, click Check Validity. If you want to create multiple entries, click Save and More to save this entry and another window opens for you to create another Registry entry

Create New Memory Module SRS Entry window

You can use the wildcard (*) for filenames but not for directory names. For example, C:\Program Files*.txt can be used, but C:*\abc.txt does not work.

Process Name

Enter a process filepath for the process.

Ignore Path Checking

Click to ignore path checking.

File or Module Path

Click Browse Local System to select the file or module path.

Browse Local System

The file or module path appears in the text box and the rest of the information in the window is filled in automatically.

Fetch Module Path from Registry Entry

If you select Fetch Module Path from Registry Entry, you must manually enter the Registry Entry. Enter a regular file path name or registry-based path variables into the text box.

You can use the wildcard (*) in the file path.

Key Value

If you select Fetch Module Path from Registry Entry, you must manually enter the the Key Value.

Enable Hash Checking

Enables Hash Checking.

Vendor AP Call Check

Checks Vendor APIs. See also About API support.

Min Version

The minimum version of TunnelGuard that can run. If Any is selected, the dates are deselected and the boxes are cleared.

Max Version

The maximum version of TunnelGuard that can run. If Any is selected, the dates are deselected and the boxes are cleared.

Relative Date/Time Range

The Relative Date/Time Range allows you to specify a Not Older Than option. If this option is selected, To and From dates are automatically deselected.

Enter the number of days in the Not Older Than (in days) text box.

Specific Date/Time Range

If you select the Specific Date/Time Range check box, select either Any or Specify Date/Time from the From Date/Time and To Date/Time.

If you selected Specify Date/Time, enter the specific date and time in the From Date/Time and To Date/Time text boxes.

Operating System

If you want all operating systems to be enabled for selection, check the All Windows box or for a specific operating system type, select one of the Windows operating systems check boxes.

Check Validity/Save and More

If you want to check that the pathway is valid, click Check Validity. If you want to create multiple entries, click Save and More. That saves this entry and another window opens for you to create another Registry entry

Registry Entry window

Registry Key Path

Select the Registry Key Path from the Registry Editor.

Key Value Type

Enter the Key Value Type.

Check for Expressions

Choose a Key Value Type, and then enter the Key Value Data Expression.

Operating System

If you want all operating systems to be enabled for selection, check the All Windows box or for a specific operating system type, select one of the Windows operating systems check boxes.

Save and More

If you want to create multiple entries, click Save and More to save this entry and another window opens for you to create another Registry entry

Memory snapshot

The Memory Snapshot section in the lower half of the of the TunnelGuard Administration Software Definition window displays all processes currently running on the administrator system.

You can double-click to select and add processes currently running and loaded into the memory snapshot to the SRS set, or you can use the New Memory Module Entry menu command.

You can use the memory snapshot on demand or program memory snapshot to run at launch time. To run memory snapshot at launch time, go to Edit > Preferences > Run Memory Snapshot at startup.

Process

This column shows the name of the process or file currently in memory.

PID

This column shows the unique system process ID for each running process.

Description

This column shows a text description, if available, for each process.

Rule Definition window

Click the Rule Definition tab to access the Rule Definition window. You use this window to create and manage rules. The SRS rule toolbar appears at the top of the window.

Rule Definition toolbar

The SRS rule toolbar icons allow you to

- **New TunnelGuard Rule**—define a new TunnelGuard rule
- **Delete TunnelGuard Rule**—delete the selected SRS rule
- **Clone TunnelGuard Rule**—clone a SRS rule
- **Export Rule**—export the selected SRS rule

  You can export one or multiple SRS rules or use the shortcut menu command to export only the selected SRS rules.

Rule Definition table

The Rule Definition table shows the existing SRS rules. These rules are retrieved from the gateway at the TunnelGuard SRS Builder applet start-up time.

Rule Name

This column shows the name of the rule.

Rule Expression

This column provides the rule expression.

Display Message on Failure

This column shows comments related to the rule.

Click <click to create message>, and then the ellipsis button (...) to open the Rule Comment window.

Rule Action

This column shows rule actions.

Click <click to create action>, and then ellipsis button (...) to open the Rule Action Constructor.

Rule Action Constructor

You use this section of the window to define a rule action.

Action Name

Enter a descriptive name for the rule.

Command Text

Enter the name of the executable file or command text.

To ensure that this command runs reliably, Nortel recommends that you enter the full path to the executable, for example, c:\windows\system32\calc.exe instead of calc.exe.

Command Type

Select the scripting preference, for example, Local script: a script that resides on the local PC.

Operating System

Select an operating system. Only Microsoft Windows operating systems are supported.

Type of Action

Run Once on Success: the command text executes after the SRS rule is successful on the PC. The command is executed exactly one time after success for a session. If a policy failure is encountered after success, the counter resets and on subsequent success, the command executes again.

Run Once on Failure: the command executes one time after the SRS rule failure is encountered.

Error messages are not logged in the Event Log for a failed launch of a script or executable file. SRS failure messages can appear when launching programs that are later checked as part of SRS Compliance.

For example, on SRS failure, a script is run to start mustload.exe. If mustload.exe is checked for presence in the memory, and then on the next SRS check the success of the script is logged.

Rule Expression Constructor

You use this section of the window to define SRS rule expressions.

Available Expressions list

The Available Expressions list contains the elements you need to construct the Boolean expression. The expressions can be basic SRS definitions or expressions you construct.

Rule Expression Constructor

You can group multiple SRS rule expressions into more compound expressions using the and, or, or not operators.

Form TunnelGuard rule expression

Select this option to place the expression you created into the Available Rule Expressions list.

After the expression is formed, it is available for Rule definitions.