Version 2.0

Part No. 317017-B Rev 00
August 2005

600 Technology Park Drive
Billerica, MA 01821-4130

Configuring TunnelGuard for the Contivity Secure IP Services Gateway

NORTEL

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

Figures

Preface

This guide introduces you to the installation procedures for the Nortel* Contivity TunnelGuard. Topics include:

- Installing the TunnelGuard Agent
- Creating custom icons
- Installing a custom client

This guide is intended for network managers who are setting up TunnelGuard Agent software for the Contivity Secure IP Services Gateway and clients. This guide assumes that you have experience with windowing systems or graphical user interfaces (GUIs) and familiarity with network management.

Before you begin

The minimum PC requirements for running the Contivity TunnelGuard are:

- Windows 2000 or better
- 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 install kit without the JVM

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**
bold Courier text	Indicates command names and options and text that you need to enter. Example: Use the **show health** command. Example: Enter **terminal paging** {**off** | **on**}.
braces ({ })	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering 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 ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering 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 points (. . .)	Indicate 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, the words are connected by an underscore. 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.`
separator (>)	Shows menu paths. Example: Choose Status > Health Check.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering 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.

Acronyms

This guide uses the following acronyms:

CES	Contivity Extranet Switch
CVC	Contivity VPN Client
CSF	Contivity Stateful Firewall
SRS	Software Requirement Set
CA	Certification Authority
CRL	Certificate Revocation List
LDAP	Lightweight Directory Access Protocol
PKCS	Public Key Cryptography Standards
PKCS #7	Cryptographic Message Standard. (Reply with digital certificate.)

PKCS #10	Certification Request Syntax Standard.
PKCS #12	Personal Information Exchange Syntax.
SRS	Software Requirement Set
TCP	Transmission Control Protocol
TG	TunnelGuard
UDP	User Data Protocol
X.509	Standard certificate format.

Related publications

For more information about the Contivity Secure IP Services Gateway, refer to the following publications:

- Release notes provide the latest information, including brief descriptions of the new features, problems fixed in this release, and known problems and workarounds.
- *Configuring Authentication and Certificates for the Contivity Secure IP Services Gateway* provides instructions for configuring authentication services and digital certificates.
- *Configuring Firewalls and Filters for the Contivity Secure IP Services Gateway* provides instructions for configuring the Contivity Stateful Firewall and Contivity interface and tunnel filters.
- *Configuring Tunneling Protocols and Advanced WAN Settings for the Contivity Secure IP Services Gateway* provides instructions for configuring the tunneling protocols IPsec, L2TP, PPTP, and L2F, as well as instructions for configuring PPP, frame relay, PPPoE, and advanced WAN settings.
- *Configuring Routing for the Contivity Secure IP Services Gateway* provides instructions for configuring BGP, RIP, OSPF, and VRRP, as well as instructions for configuring ECMP, routing policy services, and client address redistribution (CAR).
- *Reference for the Contivity Secure IP Services Gateway Command Line Interface* provides syntax, descriptions, and examples for the commands that you can use from the command line interface.

To print selected technical manuals and release notes for free, go to www.nortel.com/documentation. Find the product for which you need documentation, then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat 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 website at www.adobe.com to download a free copy of the Adobe Acrobat Reader.

How to get Help

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

Getting Help from the Nortel Web site

The best source of support for Nortel products is the Nortel Support Web site:

http://www.nortel.com/support

This site enables customers to:

- download software and related tools
- download technical documents, release notes, and product bulletins
- sign up for automatic notification of new software and documentation
- search the Support Web site and Nortel Knowledge Base
- open and manage technical support cases

Getting Help over the phone from a Nortel Solutions Center

If you have a Nortel support contract and cannot find the information you require on the Nortel Support Web site, you can 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 Web site below and look up the phone number that applies in your region:

http://www.nortel.com/callus

When you speak to the phone agent, you can reference an Express Routing Code (ERC) to more quickly route your call to the appropriate support specialist. To locate the ERC for your product or service, go to:

http://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, you can contact the technical support staff for that distributor or reseller.

Chapter 1
TunnelGuard

TunnelGuard enables you to impose a security policy on the client PC when it is connected to the corporate network through the Contivity Secure IP Services Gateway. This policy dictates the firewall and security software, or Software Requirement Set (SRS), that must be installed and activated on the client PC while the PC is connected to the gateway.

TunnelGuard is comprised of the following components:

- TunnelGuard Agent — is the desktop application running on client desktop PCs that connect to the VPN router for VPN connections. This application is responsible for monitoring the state of rules on desktops that are enforced by TunnelGuard Daemon on VPN router and for reporting their status back to the VPN router.
- TunnelGuard Daemon — runs on a VPN router that communicates rules to the TunnelGuard Agent. It is also responsible for taking action based on status reported back by the Agent. This action can be anything from terminating the connection, to keeping it restricted, to doing nothing at all.
- Software Requirement Set (SRS) builder — provides an easy-to-use User Interface for administrators to create and modify Software Requirement Sets (SRS) and rules. These requirements and rules are assigned to groups of users and enforced on client PCs connecting to the VPN router.

TunnelGuard Agent

The TunnelGuard Agent runs on the client desktop PC and is responsible for processing and checking the SRS rules. For example, the TunnelGuard Agent checks that the required components (executable files, DLLs, configuration files) necessary to comprise a personal firewall are installed and active. Because it is completely provisioned from 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 is established
3. returns to the listening state once a tunnel is torn down

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

The TunnelGuard Agent:

- Listens for a Transmission Control Protocol (TCP) message from the daemon running on the gateway, announcing that the tunnel has come up.
- Initiates a TCP/IP connection to the daemon, specifying a hash for authentication.
- Requests the personal firewall data (SRS, rules) from the daemon.
- Accepts the data from the daemon.
- 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 daemon with a status as to whether or not the tunnel should be opened up, torn down, or left 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 daemon announcing that the tunnel has come down and to discontinue checking.

The TunnelGuard Agent and Contivity Secure IP Services Gateway ensure that the end user cannot get access to the private network unless the personal firewall (or other gateway administrator-defined software) is running 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. The requirement is configured at the group level on the Profiles > Groups > Edit > Edit Connectivity screen.

Disconnect or restrict Contivity VPN Client if no TunnelGuard Agent

The TunnelGuard daemon tries to connect to the host Agent seven times before stopping. Whether the tunnel is torn down, remains up in restricted mode, or gets changed to an unrestricted filter, depends on the configuration of the Initial Policy Failure action. There is an option, at the Profiles > Groups page, to configure the CVC 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 describing the problem, the notification message also contains delete payloads for tearing the tunnel down.

If the Group level configuration option is set to Restricted Mode, the appropriate filter is applied to the tunnel and the banner text displayed. To configure the CVC 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 drop-down menu at Profiles > Groups > Edit > Group Name page.

Clickable link in Contivity VPN Client for absent TunnelGuard Agent

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 CVC display a banner with the appropriate link. The message is not acknowledged or re-sent. After receiving the Notify message, the CVC 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 Profiles > Groups > Edit > Configure page. The banner text describes the requirement for having the TunnelGuard Agent and a clickable link directing the user to a location where the Agent can be downloaded.

Note: This feature depends on the user having version 6.01+ of the Contivity Client loaded on the server.

TunnelGuard icons

There is an icon defined for each of the three TunnelGuard states. Table 1 shows the color and state of each icon.

Table 1 TunnelGuard icons

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 has failed and a new error is reported.

Supported platforms

TunnelGuard is supported on the following operating system platforms:

- Windows 95, 98, ME, NT, 2000, XP, and Win2K+

Installing the TunnelGuard Agent

TunnelGuard installation kits are provided on the Contivity VPN Client/ TunnelGuard CD in the TunnelGuard directory.

Note: Administrative rights are required if you are installing TunnelGuard on Windows 2000 or XP Professional.

Java Runtime Environment (JRE) Selection

There are two installation kits provided, one with the Java virtual machine (VM) (1.4.1_02) bundled, one without VM bundled. NoVm installation kit is provided to minimize the size of kit for downloading.

JRE 1.4.1_02 (or later versions) is required for TunnelGuard installation. The VM version of TunnelGuard installation allows the user to install bundled VM (which is 1.4.1_02) with TunnelGuard. The VM is installed under the <*TG install dir*>*jre* directory. This JRE is local to the TunnelGuard and is only used by TunnelGuard. Web browsers are not affected by it.

A “Select JVM" dialog box allows users to select:

- bundled JVM (not available for NoVM kit)
- JVM installed on local machine (with version greater than or equal to 1.4.1_02)
- a list of JVMs currently installed on the local machine

If the user selects bundled JVM, a jre directory is installed under the installation directory and is used to launch the TunnelGuard application.

If user selects a JVM installed on the local machine, the jre directory is not installed. The selected local JVM is used.

Property **`NN_JREPATH`** can be used to set the JRE path. If **`NN_JREPATH`** is set, the "Select JVM" dialog box is not shown. JVM represented by **`NN_JREPATH`** is used.

In silent mode, if **NN_JREPATH** is provided, the corresponding JRE is used. If **NN_JREPATH** is not provided for a VM kit, the default bundled JRE is installed and used. If **NN_JREPATH** is not provided for a NoVM kit in silent mode, the installation will fail.

Installation kits

Two sets of kits are provided for TunnelGuard installation — a customizable installation kit and a standard installation kit. Each kit has two versions.

If download time (size of the kit) is not a concern, administrators can deploy the VM version of TunnelGuard. The VM version of TunnelGuard gives users the option of installing the bundled JVM or using one already installed on the machine (if it is JRE 1.4.1_02 or a later version).

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 downloads faster. In this case, users must have the right version of JRE (1.4.1_02) installed on the machine.

Customizable Installation Kit

Customizable VM kit

The customizable VM TunnelGuard installation kit is bundled with JRE 1.4.1_02.

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 is automatically launched.

TgExeVm.msi can be launched directly if there is a correct version of Windows MSI on the machine. It can be customized using tools such as ORCA. See "Custom installation" on page 25 for more information.

Customizable NoVM kit

The customizable 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 is automatically launched.

Launch TgExeNoVm.msi directly if there is a correct version of Windows MSI on the machine. It can be customized using tools such as ORCA. See "Custom installation" on page 25 for more information.

Standard Installation Kit

Standard VM kit

TgVM.exe is a single file installer. It installs MSI if it is not on the machine. JRE 1.4.1_02 is included.

Standard NoVM kit

TgNoVM.exe is a single file installer. It installs MSI if it is not on the machine. No JRE is included.

Command line and silent installation

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

For silent installation, the reboot dialog box is not shown. A reboot is performed.

The property **`NN_CVC601PATH`** can be set as an installation parameter. For example:

```
Msiexec NN_CVC601FORCEREBOOT=1 /I tgExeVM.msi /qn
```

More examples:

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

Other switches include:

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

Installing the Contivitiy VPN Client with TunnelGuard

The property **NN_CVC601PATH** can be set as installation parameter. For example:

```
Msiexec /I tgExeVM.msi NN_CVC601PATH=<path to CVC6.01 setup.exe>
```

If **NN_CVC601PATH** is not set during a full user interface installation, the installation program searches for SETUP.EXE using the assumed path on the CD. If the CVC6.01 installation file is found, the user is given the following choices:

- not install CVC6.01
- install CVC6.01 Domestic version (if domestic kit exists)
- install CVC6.01 Export version (if export kit exists)

During a non-full user interface installation, such as silent install, only **NN_CVC601PATH** is checked. If **NN_CVC601PATH** is not set, Contivity VPN Client is not installed.

```
Msiexec /I tgExeVM.msi NN_CVC601VERSION=V04_65.22
```

Before launching CVC6.01 installation, the system makes a check to see if the user has the same or a later version of the Contivity VPN Client installed. If so, installation of CVC6.01 is not launched.

By default, **NN_CVC601VERSION** is set to the version that is shipped with the CD. If you change the CVC6.01 installation kit, provide the changed version of the kit.

If CVC6.01 is launched, whether or not the install is successful, a reminder of Reboot is shown at the end of TunnelGuard installation for all non-silent installations. For silent installation, the reboot dialog box is not shown.

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 do many installation customizations, such as changing the title, changing the icon, and changing the files to be installed.

Here are examples of how to make some of these changes using ORCA (all properties are case sensitive):

Modify Installation properties

Change default folder

Table: Directory

Row(s): Directory = INSTALLDIR1 and its parent directories

Modify: DefaultDir field; replace "Nortel Networks" with your default folder.

Change default Program menu folder

Table: Directory

Row(s): Directory = Nortel_Networks_TunnelGuard

Modify: DefaultDir field; replace "Nortel Networks TunnelGuard" with your default folder name.

Change shortcut icon

Table: Icon

Row: Add new row

Modify: Name = MyCustomIcon.ico

Data: upload your 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, do the following:

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

Modify Agent.properties

The Agent.properties file has settings for how the Agent will run. Administrators can customize it and include it in the custom installation.

To change Agent.properties, do the following:

1. Do an installation or extract the Agent.properties from MSI.
2. Modify Agent.properties according to requirement.
3. Modify MSI file to replace Agent.properties under [INSTALLDIR]\resources with the modified file. [*]

Example of modifying TunnelGuard MSI installation file

These are the steps to modify MSI file and replace icon and property files. Please refer to MSI documents for more detailed information.

The Microsoft SDK tools ORCA and cabarc.exe are used to extract the cab file and re-bundle cab files. Here are the sample steps with TgExeVm.ms:

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

```
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
```

5. Run command: `cabarc X mycab.cab`, which extracts all the files from the cab file.
6. Replace the icon files and Agent.properties file with the files you have customized. Make sure the file names are not changed.
7. Run command: `cabarc n mynewcab.cab @list.txt`
8. In ORCA, in the Cabs table, import `mynewcab.cab`.

TgExeVm.msi is now successfully updated with the new files.

Custom install options

Currently TunnelGuard Agent installs TunnelGuard Service as well as Desktop Application to monitor and report SRS Rule failures as one feature. This release separates TunnelGuard core functionality from desktop monitoring application. Custom install options provide the end user with two features:

- TunnelGuard Core
- Desktop Monitor

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

The custom install options provide the following options to the end user:

- System tray icon
- Optional TunnelGuard logs
- No or limited popups
- Clickable link in TunnelGuard Agent

TunnelGuard system tray icon

When the TunnelGuard Agent is running on a system, the TunnelGuard icon appears in the system tray in the lower right corner of the screen. This icon is used for configuration and failure notification.

When you right-click on the TunnelGuard icon, the context menu shows these commands:

- Show Status Information — displays the TunnelGuard log.
- Configuration — enables a user to configure logging settings.
- About — provides version and copyright information.

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

Note: The TunnelGuard Agent system tray icon formerly provided a menu option **Exit** to the user when right-clicked. This feature has been discontinued.

TunnelGuard logs

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

Contivity Secure IP Services Gateway event log

The Contivity Secure IP Services Gateway Event log contains information regarding TunnelGuard status. It notes if a check failed, if the restricted filter was lifted, or if no communication could be established with the Agent.

Contivity VPN Client log

The client-side log file for the CVC does not contain information regarding TunnelGuard. If a CVC session is disconnected by TunnelGuard, the only information noted in the client log is that the server requested the disconnection.

TunnelGuard Status log

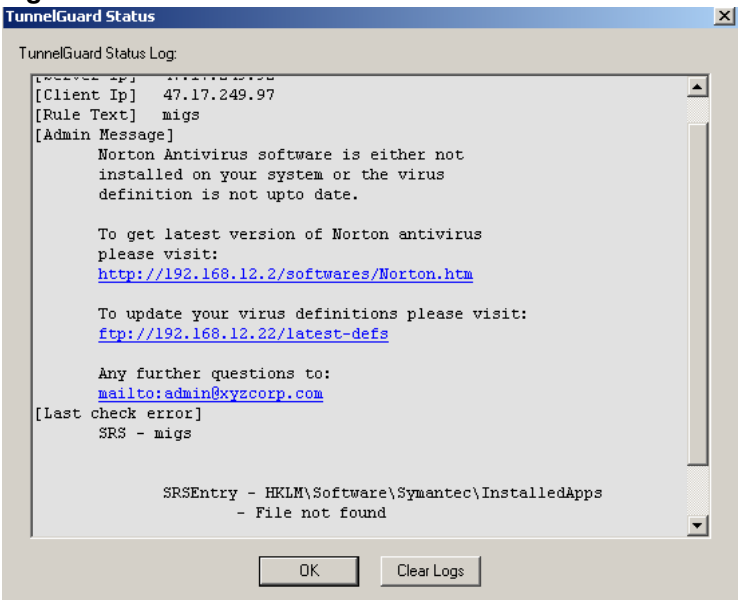
TunnelGuard Agent logs are an optional feature with Windows Installer. By default, logging is enabled for standard install. To view the TunnelGuard Status log, right-click the TunnelGuard icon in the system tray and select the Status Information menu option.

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

Figure 1 shows the TunnelGuard Status log that appears in the TunnelGuard Status console window when an SRS rule fails. The log has clickable links to update the missing software.

Figure 1 Clickable links in TunnelGuard Status console window



No or limited pop-up messages

TunnelGuard Agent pops up a dialog window whenever there is SRS check failure, regardless of the policy set on the VPN router for the rule. In some installation scenarios, this feature is not desirable. When SRS check failures are logged, the Detail switch reveals all of the information about rule contents and exactly what is expected on the system in order to be compliant. Some VPN administrators choose to hide some or all of this information from end users. Having no pop-up messages can be achieved in the following ways:

- Install TunnelGuard without Desktop Monitor feature. This ensures no pop-up messages are generated on the desktop PC.
- Install TunnelGuard with Installer property **DisablePopup** set to **1**. This ensures no pop-up messages are generated on the desktop PC, even when Desktop Monitor is installed. This feature works on registry settings on desktop PCs, so you can modify the registry settings to change the behavior.

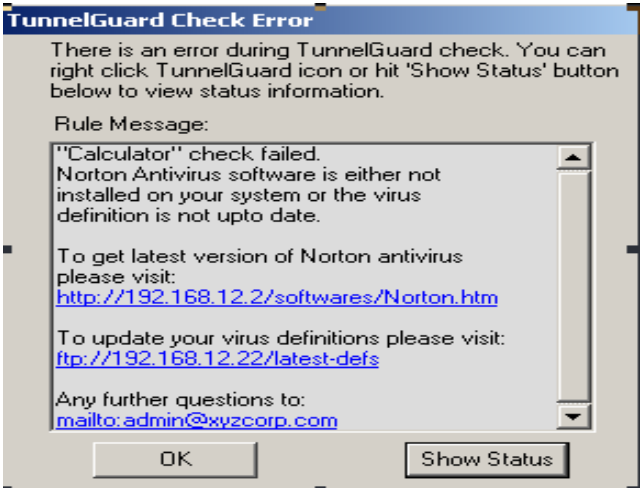
- Install TunnelGuard with Installer property **HideTaskbarIcon** set to **1**. This ensures no pop-up messages are generated and no taskbar icon appears in the system tray, even when Desktop Monitor is installed and running on the system. This feature works on registry settings on desktop PCs, so you can modify the registry settings to change the behavior.
- Install TunnelGuard Agent having **Agent.properties** file with **DisplayLastCheckError = true.** This ensures that no detailed information about the SRS failure is displayed.

Clickable link in TunnelGuard Agent

TunnelGuard Agent presents an error message on desktop PCs whenever an SRS rule fails. This error message is comprised of an SRS rule and an SRS comment. The SRS comment has clickable links that provide rule-specific locations to download information for compliance in cases where the user fails to comply. Any text that begins with http:// or https:// automatically transforms to a clickable link.

Figure 2 on page 32 shows the pop-up message with clickable links that appears on your desktop PC when an SRS rule fails.

Figure 2 Clickable links in TunnelGuard Agent pop-up message



Better response for initial check failure

Initial Failure Recovery Mode overcomes many situations that make you stay in restricted mode of tunnel for long durations. If the TunnelGuard Agent detects SRS FAILURE/UPDATE on the first check, it goes into **Failure Recovery Mode**. This mode enables a faster, more frequent SRS compliance checking by the Agent. The TunnelGuard Agent does not engage the VPN router until there is a change in compliance. Once the system falls into compliance, or the Failure Recovery Mode interval expires, TunnelGuard comes out of Failure Recovery Mode. The default failure recovery interval is 10 seconds and is configured using TunnelGuard properties. The duration of Failure Recovery Mode is the length of the first intra-interval checking.

TunnelGuard from the user perspective

It is important that TunnelGuard is configured to effectively communicate information and instructions to end users who are expected to use the TunnelGuard Agent.

The TunnelGuard banner is a mechanism that you use to communicate information to the user, including a standard banner message informing users that a restricted filter is in place until the SRS conditions are met.

Chapter 2
Configuring TunnelGuard

Configuration Overview

This section provides information about how to configure the TunnelGuard feature for securing limited access to Contivity Secure IP Services Gateway connections.

Administrators can add and delete applications that the TunnelGuard Agent and gateway check for. The applications that the gateway checks for is defined by a Software Requirement Set (SRS) that specifies the file name and location of the application.

The TunnelGuard server communicates directly with the TunnelGuard Agent on the client PC over a socket connection.

TunnelGuard Server Setup

Defining TunnelGuard Software Requirement Sets requires some knowledge of the applications that must be checked. There are various means of accommodating multiple versions of an application on different PC platforms. Some of these methods provide a more secure validation than others. The purpose of this section is to allow the initial configuration of TunnelGuard by:

1. defining the restricted filter
2. launching the SRS editor and define the Software Requirements Set
3. enabling TunnelGuard on the desired group or groups

Filter, Firewall, and Port Notes

Before defining the restricted filter, you should be aware of the interaction between TunnelGuard and the Contivity Stateful Firewall (CSF) and filters.

TunnelGuard requires a UDP and TCP port for communications between the TunnelGuard daemon on Contivity and the Agent on the PC. After the initial tunnel setup, the daemon attempts to contact the client on UDP port 8121. This port is not configurable. During that conversation, the daemon tells the Agent what TCP port to use for further communication, such as to receive the SRS (Software Requirement Set) to check. This port is configurable on the Services > Firewall/NAT screen. The default for this TCP port is 8282. These ports are included in the filters by checking the TunnelGuard box in the Remote Servers section of the Profiles > Filters > Edit screen.

In releases prior to 4.80, you could have the Contivity Stateful Firewall enabled, Tunnel Filters enabled, or both enabled. Typically, administrators that configured the CSF disabled Tunnel Filters after the CSF rules were tested, as there was no need to filter the same traffic twice.

In release 4.80, the Tunnel Filters were 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 Contivity. Tunnel Filters control all other traffic. With respect to TunnelGuard, all communication terminates on the management IP address. Since the CSF has an implied rule for the management interface to the trusted (tunnel) interface, no additional firewall rule are needed for TunnelGuard, and if the CSF is running, the Tunnel Management Filters can be disabled without affecting TunnelGuard traffic flow.

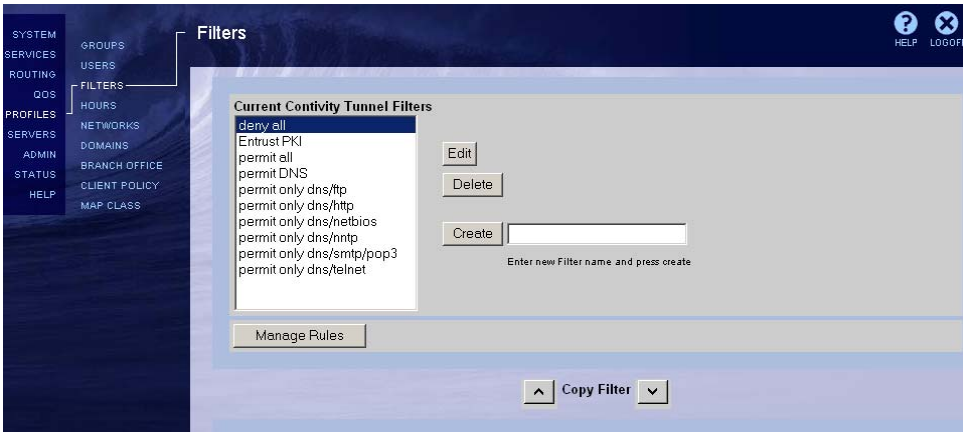
Configuring TunnelGuard

To configure TunnelGuard:

1. Log on to the Contivity Secure IP Services Gateway 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. Select Profiles > Filters.

The Profiles > Filters page opens. Figure 3 shows the Profiles > Filters page.

Figure 3 Profiles > Filters page



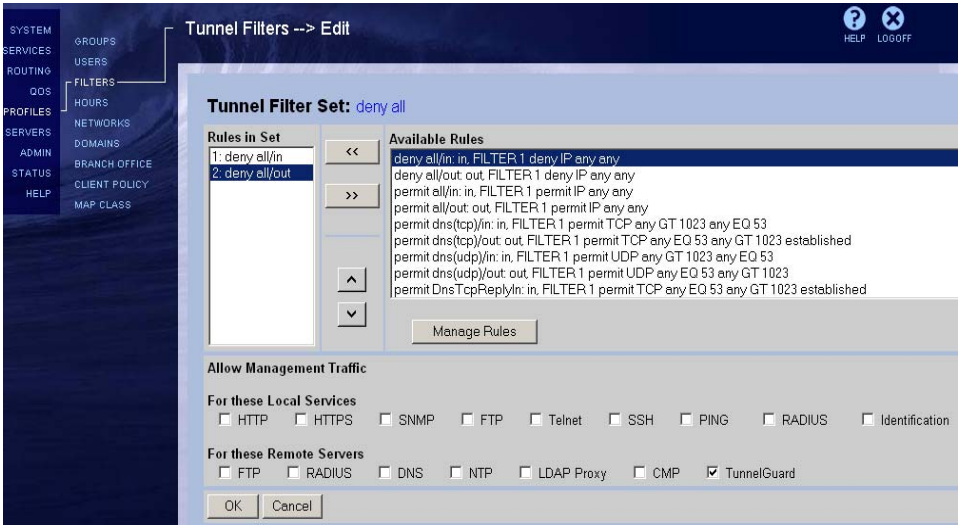
4 Select the filter you want to enable for TunnelGuard.

5 Click Edit.

The Profiles > Filters > Edit page opens.

Figure 4 shows the Profiles > Filters > Edit page.

Figure 4 Profiles > Filters > Edit page



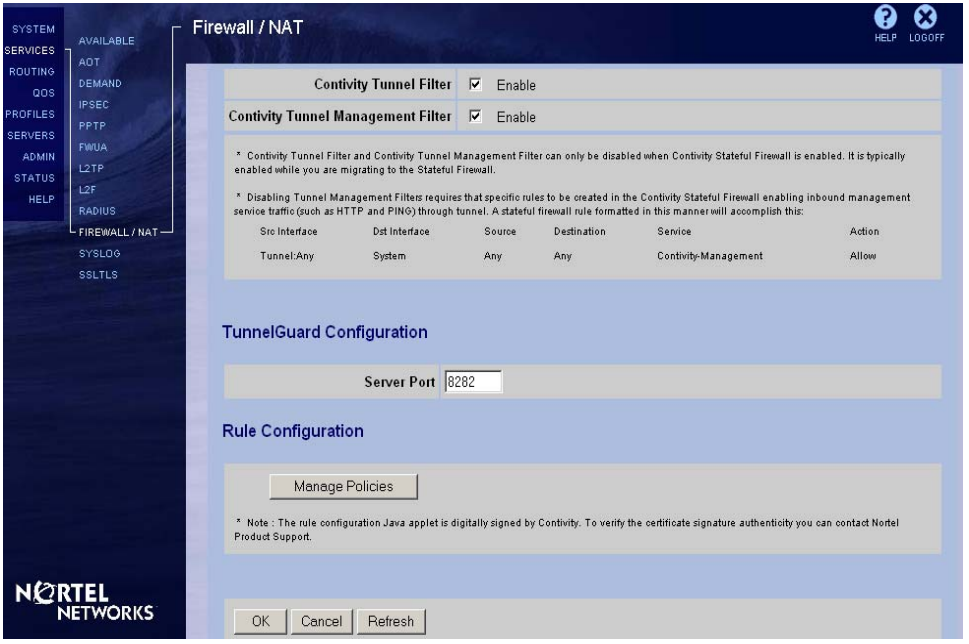
6 Under Allow Management Traffic For these Remote Servers, click TunnelGuard. This enables TunnelGuard traffic support.

7 Click OK.

8 Select Services > Firewall/NAT. The Services > Firewall/NAT page appears.

Figure 5 shows the Services > Firewall/NAT page.

Figure 5 Services > Firewall/NAT

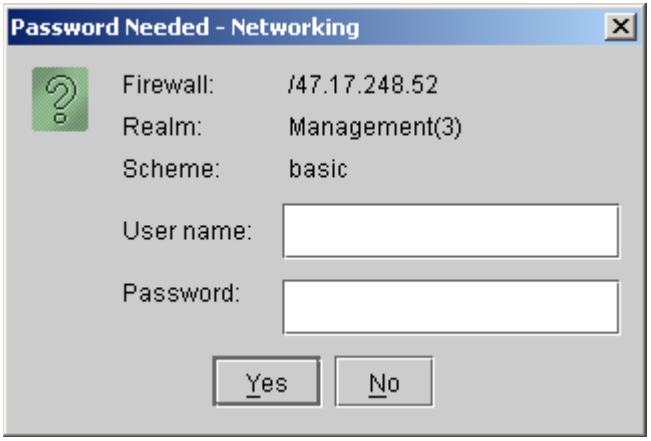


9 Configure a TCP/IP port number for the TunnelGuard daemon to use when connecting to the TunnelGuard Agent. (A separate port number is used for SSL communication.) No action is required if the default is used.

10 Click Manage Policies in the Rule Configuration section to launch the SRS Builder applet. You are prompted to log on to the TunnelGuard SRS Builder applet.

Figure 6 on page 39 shows the SRS Builder Logon page.

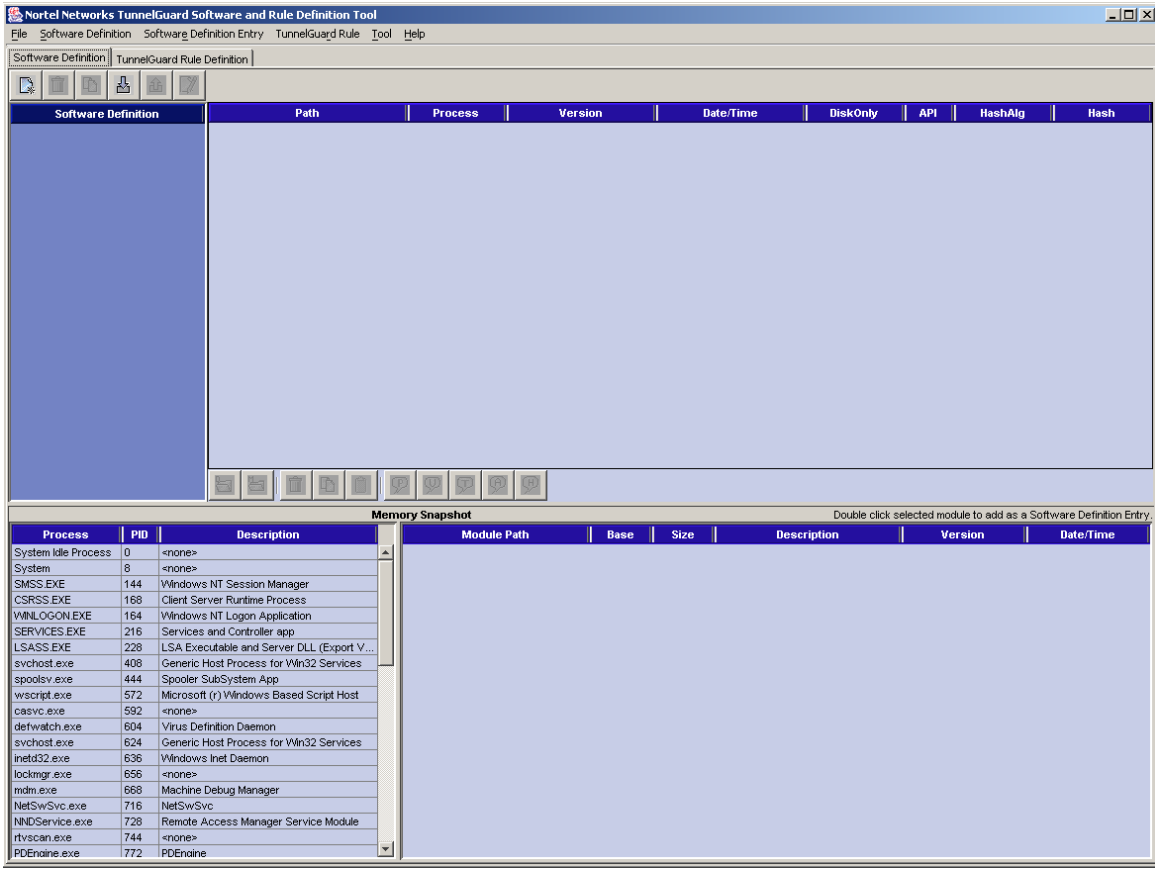
Figure 6 TunnelGuard SRS Builder Logon



11 Log on to the SRS Builder utility using a valid system administrator name and password. The SRS Builder main screen with the Software Definition tab selected appears. The SRS Builder is used to create one or more Software Requirement Sets.

Figure 7 on page 40 shows the SRS Builder main screen with the Software Definition tab selected.

Figure 7 SRS Builder Software Definition screen

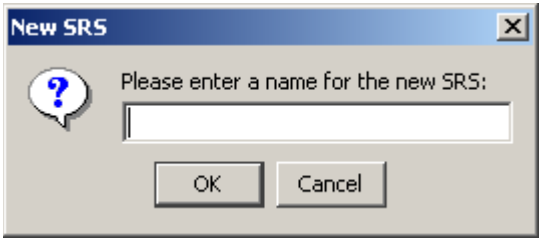


12 To create a Software Requirement Set, select New Software Definition in the Software Definition menu or click the New Software Definition icon above the Software Definition column.

Figure 8 on page 41 shows the New SRS Definition Name dialog box that appears.

Note: You can import data for an SRS by selecting the import icon or by selecting Import Software Definition in the Software Definition menu.

Figure 8 New SRS Definition Name dialog box



13 Enter a name for the SRS definition. For example, the name Antivirus might be entered if you are creating an SRS definition that specifies the antivirus software modules that must be present on the client system running the TunnelGuard Agent.

Note: The Auto Generate TunnelGuard Rule option in the Software Definition menu 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 TunnelGuard Rule Definition screen.

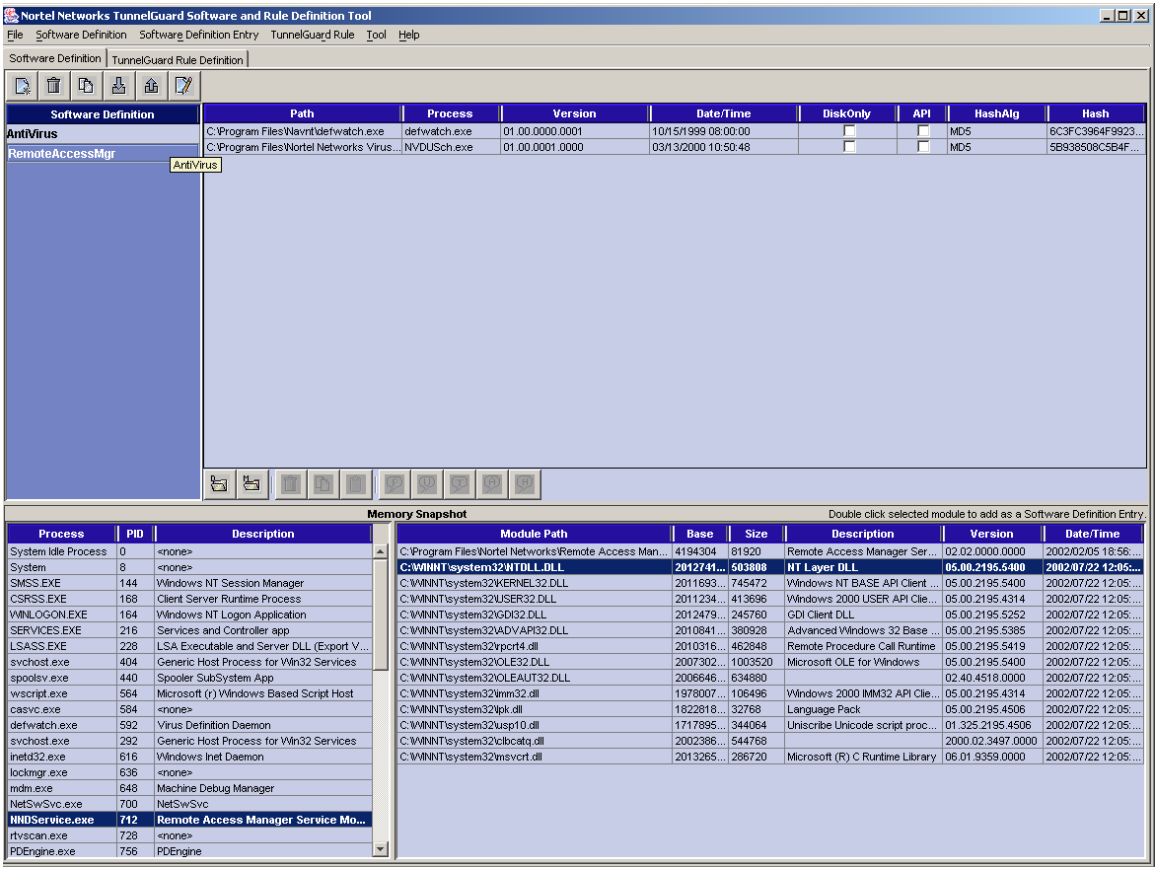
14 Select the application, or process, that you want to include in the SRS from the process list on the left of the memory snapshot section. The memory snapshot section in the lower half of the TunnelGuard SRS Builder Software Definition screen displays all processes currently running on the system on which you have executed and are running the TunnelGuard SRS Builder.

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

15 Select the modules for this SRS definition that are required on client systems. Select and add any module currently running and loaded into the memory snapshot to the SRS set by double-clicking on it or by using the Add a selected memory module menu command.

Figure 9 on page 42 shows an example of the SRS Builder Software Definition screen with an SRS Definition and the included modules.

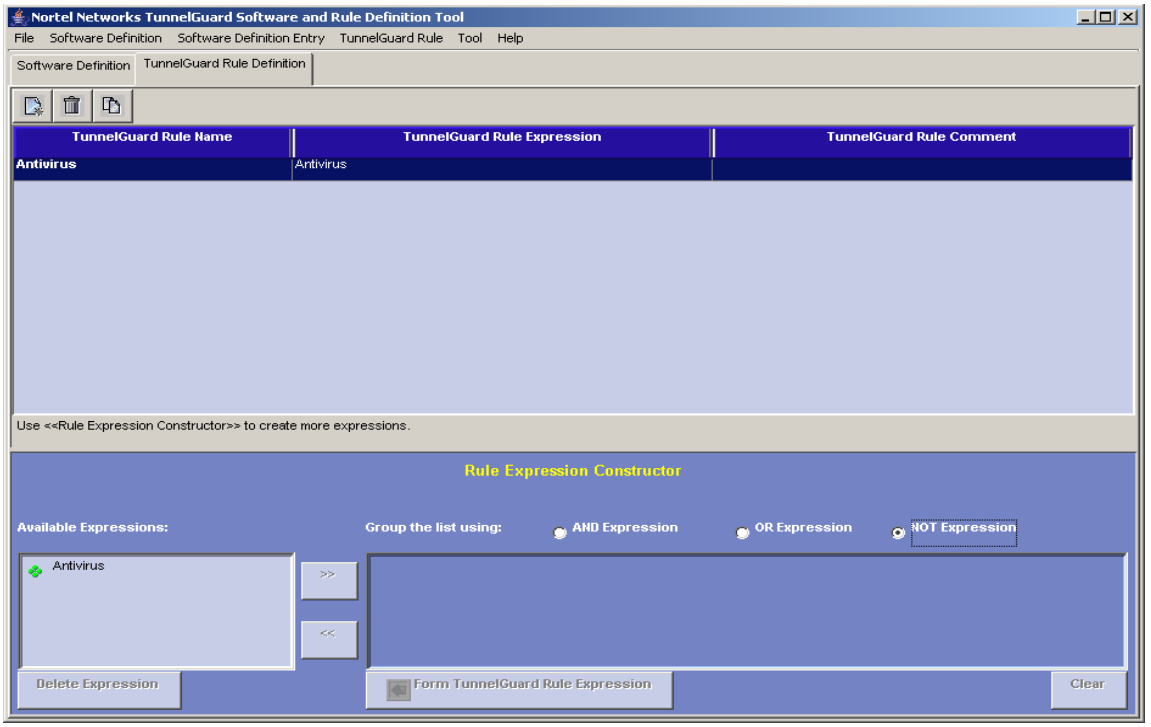
Figure 9 SRS Builder screen with software definitions and modules



16 Select the TunnelGuard Rule Definition tab to define TunnelGuard rules for the Software Requirement Sets that you created.

Figure 10 on page 43 shows the SRS Rule Definition screen.

Figure 10 TunnelGuard SRS Builder Rule Definition screen



17 To create a TunnelGuard rule, select New TunnelGuard Rule in the TunnelGuard Rule menu or click on the New Rule icon above the TunnelGuard Rule Name column. The New SRS Rule dialog box appears.

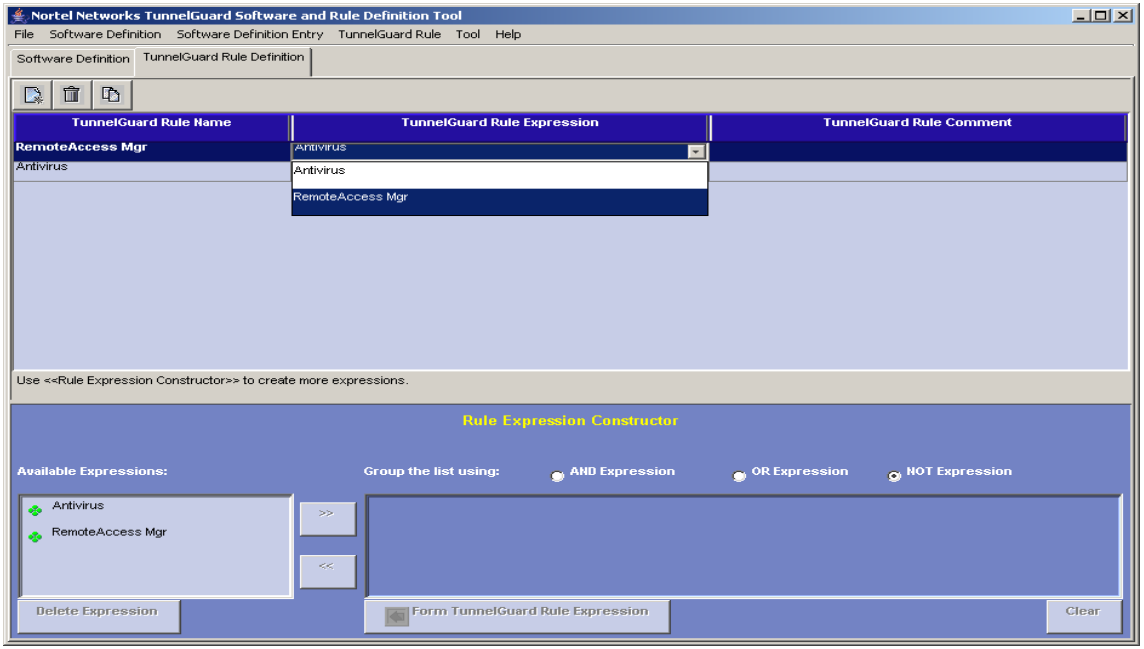
Figure 8 on page 41 shows the New SRS Rule dialog box.

18 Enter a name for the rule in the New SRS Rule dialog box.

19 Select a rule expression for the rule from the available expressions. Click in the TunnelGuard Rule Expression column. A drop-down list of existing expressions appears.

Figure 11 on page 44 shows the TunnelGuard Rule Expression drop-down list.

Figure 11 TunnelGuard Rule Expression drop-down list



20 To create a new expression, you use existing expressions to form Boolean constructions.

The Available Expressions section initially lists any SRS expressions that are auto-generated. Auto-generated rules are created automatically when the Auto Generate TunnelGuard Rule option in the Software Definition menu is enabled, which is the 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 TunnelGuard Rule Definition screen.

In Figure 11, the Available Expressions list at the bottom left of the screen includes the two expressions with the same names as two SRS definitions previously defined. One represents an Antivirus SRS definition, to ensure that the tunneling systems have the required antivirus software modules, and the other represents a remote access management application for administrative access to the remote system.

21 Select a rule expression from the Available Expressions section.

22 Click the >> button to move a selected expression into the Rule Expression Constructor section of the window on the right side above the Form TunnelGuard Rule Expression button.

When more than a single expression is available in this section, the Form TunnelGuard Rule Expression button becomes active, enabling you to create a Boolean AND/OR expression comprised of the available expressions. You may 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 feature allows the creation of rules that are used as quick and basic checks against certain kinds of known viruses, worms, ad-wares, P2P file-sharing software, and spy-wares.

23 Select the expression type that you want to form, either an AND expression, an OR expression, or a NOT expression, using the option buttons.

24 Click the Form TunnelGuard Rule Expression button to construct the new AND/OR/NOT expression.

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

You create nested statements by combining AND expressions with OR expressions. 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 some minimum set of software as specified by the Antivirus AND RemoteAccessMgr SRS definitions.

Note: Before saving the rule, you can set up a message to be shown to the user if the rule fails.

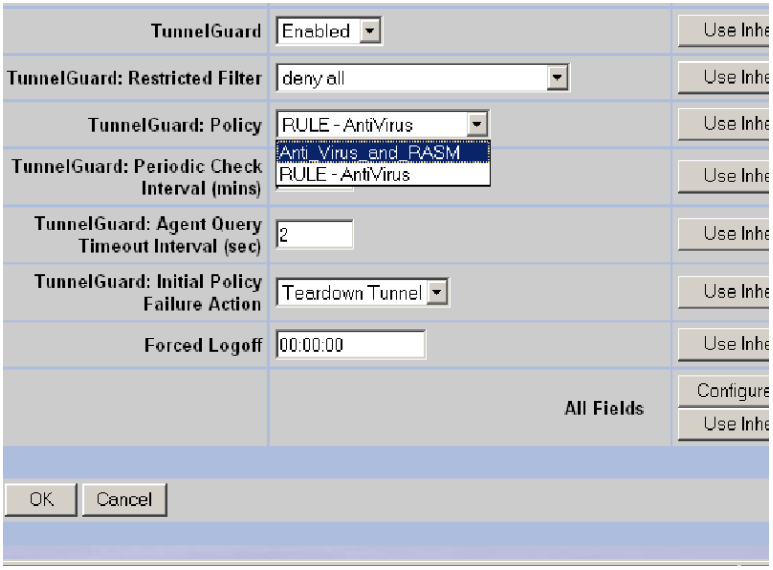
25 When you have completed creating SRS definitions, Rules and Rule Expressions, select File > Save and exit TunnelGuard SRS Builder.

26 Select the groups to which you want to apply TunnelGuard on the Profiles > Groups screen.

27 Click Edit for the group you want to configure for TunnelGuard. The Profiles > Groups > Edit > Connectivity screen appears. Scroll down to the TunnelGuard settings section of the screen.

Figure 12 shows the TunnelGuard settings of the Connectivity screen.

Figure 12 Profiles > Groups > Edit > Connectivity screen — TunnelGuard settings



28 Set the TunnelGuard parameter to Enabled.

29 Set the restricted filter to be used with the selected group while the verification process is in progress. Select Profiles > Filters to define a restricted filter, if necessary.

30 Specify 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.

31 Configure the periodic time check interval, if necessary.

32 Configure the Agent query timeout interval, if necessary.

33 Select the Initial Policy Failure action, either Tear down tunnel, Leave Restricted, or No Action.

34 Click OK.

You may receive pop-up messages if you change some of the TunnelGuard default settings. It is recommended that you read the messages and take any appropriate action. For example, when you change the Restricted Filter and click OK, a message appears at the top of the Groups page. The message prompts you to follow the link to the Profiles > Filters screen to edit the selected TunnelGuard filter. This ensures that the filter selected allows TunnelGuard traffic.

Registry-based rules

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's PC is another way of checking software packages and their installed state.

Registry-only SRS entry

Both TunnelGuard Agent and TunnelGuard administrator applet support registry-checking functionality. The administrator tool applet is used 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 allowing access to the network. One SRS entry holds any number of registry key checks, just as one SRS entry holds any number of file checks. Contrary to file and process checks, registry key checks do not have hash checking, date, and version number checking enabled. However, you can combine registry key checking entry with any other type of checking, such as process check or on-disk entry check.

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

TunnelGuard Agent leverages the advantage of being a Java-based application and uses the pattern and regular expression support available in JRE. It provides all of the relevant pattern-matching facility 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:

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

Some examples of regular expressions for integer Registry Key values are:

- >= 20
- = 100
- < 50
- != 200

Supported constructs for string-based regular expressions are:

Table 2 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 non-whitespace character [^\s]
\w	A word character: [a-zA-Z_0-9]
\W	A non-word character [^\w]
[abc]	a, b, or c

Table 2 Constructs for string-based regular expressions (continued)

String regular expression	Description
[^abc]	not a, b, or c
[a-z]	any character 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
\	Nothing, but quotes the following character
\Q	Nothing, but quotes all characters until \E
\E	Nothing, but ends quoting started by \Q
^	The beginning of a line
$	The end of a line
\b	A word boundary

Some 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

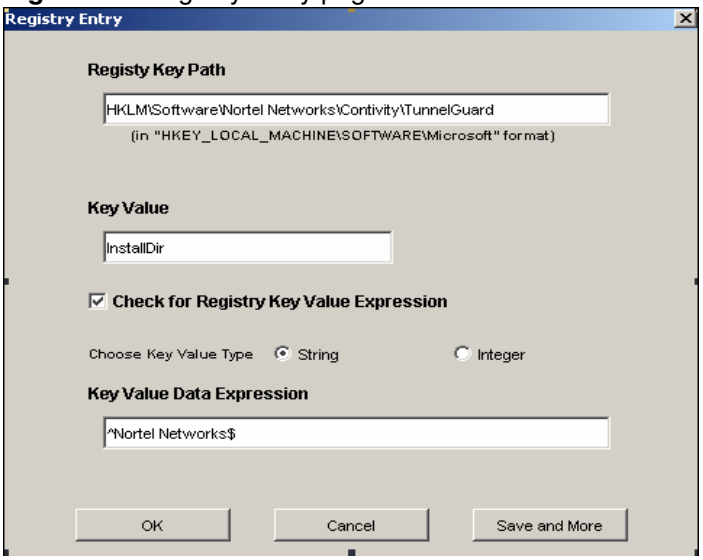
Creating a registry entry

To create a registry entry:

1. Click the Software Definition tab in the TunnelGuard Software and Rule Definition Tool page.
2. Click the Software Definition Entry menu and select Add Registry Key Entry. The Registry Entry page opens.

Figure 13 shows the Registry Entry page.

Figure 13 Registry Entry page



3. Select the Registry Key Path from the Registry Editor.
4. Select the Key Value Type.
5. Enter the Key Value Data Expression.
6. Click OK.

   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 based File/Module

If the File/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. Administrators can define a Registry Key to look for and derive a File/Module path and name from the Registry Key Value data. This path is then treated exactly as any other OnDisk entry or Memory Module entry as defined by the administrator.

Manual editing of SRS entries

The administrator tool applet provides OnDisk and Memory Module buttons to create custom SRS entries and rules without anything installed on a desktop PC. In order to create these rules, you must know the name of the executables or files to be checked. Since these rules are created manually, extra care is required to avoid any mistakes.

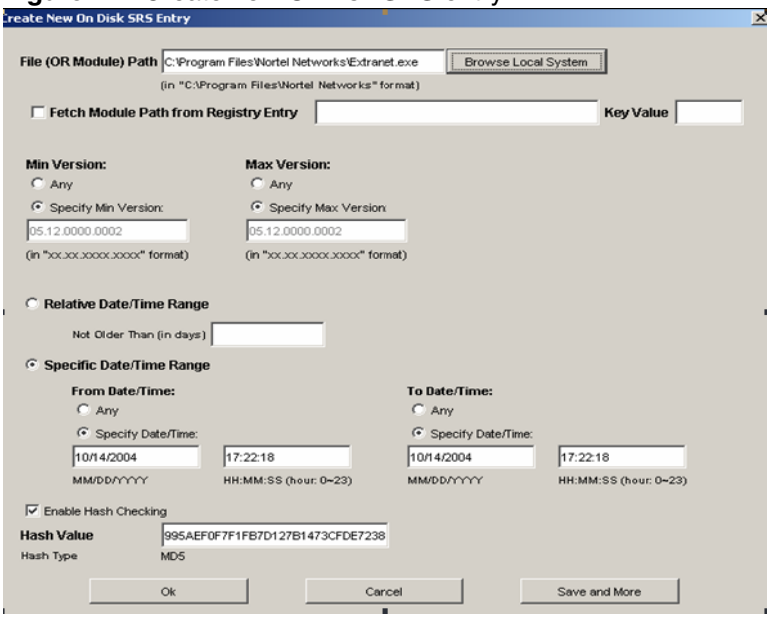
Manually creating an OnDisk file entry

To manually create an OnDisk SRS file entry:

1. Click the Software Definition tab in the TunnelGuard Software and Rule Definition Tool page.
2. Click the Software Definition Entry menu and select Create New OnDisk SRS Entry. The Create New OnDisk SRS Entry page opens.

Figure 14 on page 52 shows the interface used to manually create an On Disk file entry.

Figure 14 Create new OnDisk SRS entry



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 on the page is filled in automatically.

Note: If you select Fetch Module Path from Registry Entry, you must manually enter the Registry Entry and the Key Value. The other fields on the page must also be completed manually.

4 Click an option button for Min Version.

If Any is selected, the dates are deselected and the boxes are cleared.

5 Click an option button for Max Version.

If Any is selected, the dates are deselected and the boxes are cleared.

6 Click an option button for either Relative Date/Time Range or Specific Date/Time Range.

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.

7 To enable Hash Checking, click the Enable Hash Checking box.

8 Click OK.

If you want to create multiple entries, click Save and More. That saves this entry and another window will opens so that you can create another OnDisk SRS entry.

Manually creating a Memory Module entry

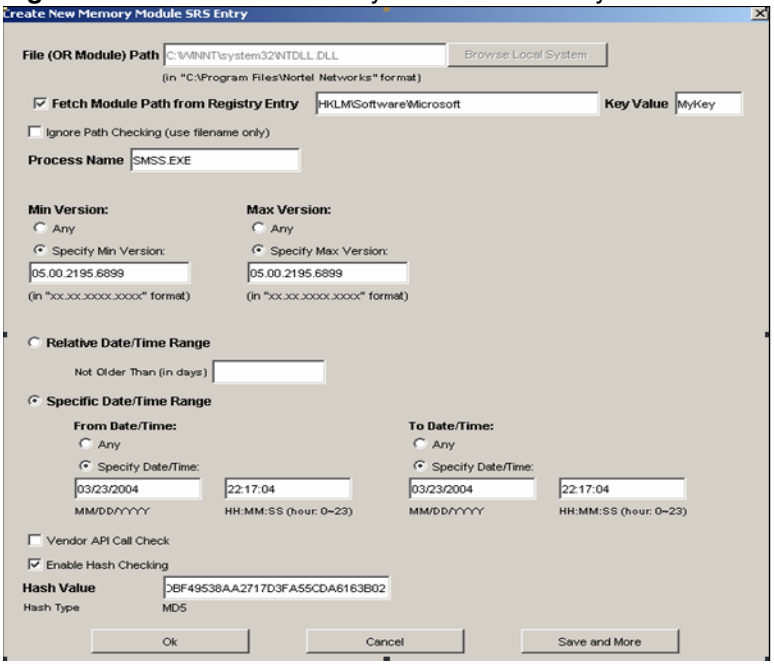
To manually create a Memory Module entry:

1 Click the Software Definition tab in the TunnelGuard Software and Rule Definition Tool page.

2 Click the Software Definition Entry menu and select Create New Memory Module SRS Entry. The Create New Memory Module SRS Entry page opens.

Figure 15 on page 54 shows the interface used to manually create a Memory Module entry.

Figure 15 Create new Memory Module SRS entry



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 on the page is filled in automatically.

Note: If you select Fetch Module Path from Registry Entry, you must enter the Registry Entry and the Key Value. The rest of the fields on the page must also be completed manually.

4 Enter the process name in the Process Name text box.

5 Click an option button for Min Version.

6 Click an option button for Max Version.

7 Click an option button for either Relative Date/Time Range or Specific Date/Time Range.

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 an option button for either Any or Specify Date/Time from the From Date/Time and To Date/Time:

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

The information below each text box tells you the format of the information.

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

9 To enable hash checking, click the Enable Hash Checking box.

10 Click OK.

If you want to create multiple entries, click Save and More. That saves this entry and another window will pop up so that you can create another Memory Module SRS entry.

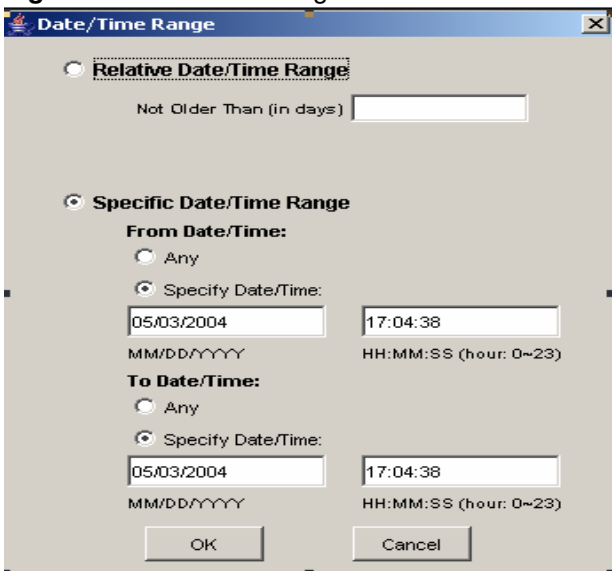
File age check

When TunnelGuard is used, most desktop PCs have anti-virus 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 administrator tool applet's Set Date/Time Range button allows you to specify a Not older than option. If this option is selected, To and From dates are automatically deselected.

Figure 16 on page 56 shows the interface you use to set the relative date and time range. This interface is accessed from a button in the middle of the TunnelGuard Software and Rule Definition Tool page.

Figure 16 Date/Time range



Chapter 3
TunnelGuard SRS Builder

TunnelGuard SRS Builder main screen

The TunnelGuard Software Requirement Set (SRS) Builder utility main screen appears after you successfully logon with a valid administrator user name and password.

The main screen includes:

Menu Commands

Software Definition — Available SRS list

SRS definition toolbar

SRS Components table

Memory snapshot

TunnelGuard Rule Definition screen

Menu Commands

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

File menu

Software Definition menu

File Menu

Save

Save the SRS definition in the gateway LDAP database.

Software Definition Entry menu

Add OnDisk file as entry

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

Add Selected memory module as entry

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

Add Registry Key entry

Add the registry key entry.

Delete

Delete the selected component.

Copy

Copy the selected component.

Paste

Paste component (from one SRS definition to another).

Custom Path

Select this option to specify a customized path to a file.

Set Version Range

Use this option to specify a version or version range for an SRS component.

Set Date/Time Range

Use this option to specify a date and/or a time range for an SRS component.

Add Vendor-Customized API call check

Select this option to implement a third-party API call to do additional checking on the software.

Modify Registry Entry

Use this option to modify the registry entry.

Ignore Hash Checking

Select this to ignore the hash value checking for the selected SRS entry.

Default Hash Algorithm

Select the default hash algorithm, MD5 or SHA1.

Tool menu

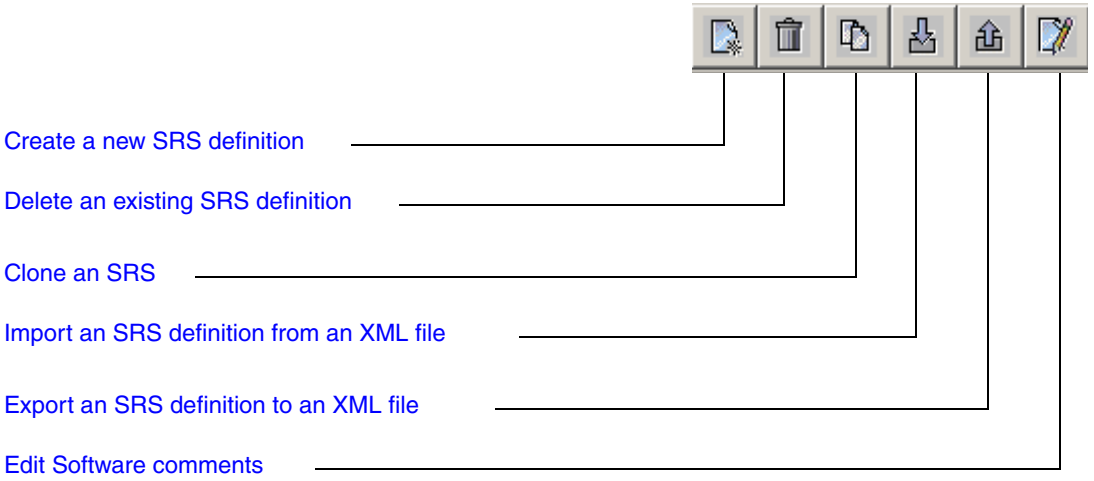
Refresh memory snapshot

Select the Tool > Refresh memory snapshot menu command to refresh the list of processes shown in the memory snapshot area of the main screen. You may want to refresh the view if you have launched other applications while running the SRS builder or if other processes started after the SRS builder started.

SRS definition toolbar

The buttons on the SRS definition toolbar allow you to create, delete, and manage software requirement sets. Each of the toolbar icons is described below, in Figure 17.

Figure 17 SRS Definition Toolbar



Create a new SRS definition

Use this command to create a new SRS definition.

Delete an existing SRS definition

Use this command to delete the currently selected SRS definition.

Clone an SRS

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

Import an SRS definition from an XML file

Use this option to import an XML-formatted SRS definition file.

Export an SRS definition to an XML file

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

The Import and Export functions are useful for creating and distributing “canned” SRS solutions.

Edit Software comments

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

Software Definition — Available SRS list

The available SRS list shown in the Software Definition section of the TunnelGuard SRS Builder main screen is initially retrieved from the Contivity Secure IP Services Gateway and is updated when you make any changes while running the SRS Builder.

SRS Components table

When an SRS is selected in the Software Definition section that lists available SRS definitions, 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 (will not be loaded 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 checked, it means the file will not be loaded in memory. If this option is combined with the API option, the file will be loaded and the API called.

API

If checked, it means the component contains third party API for further checking.

HashAlg

Hash algorithm used to generate the hash.

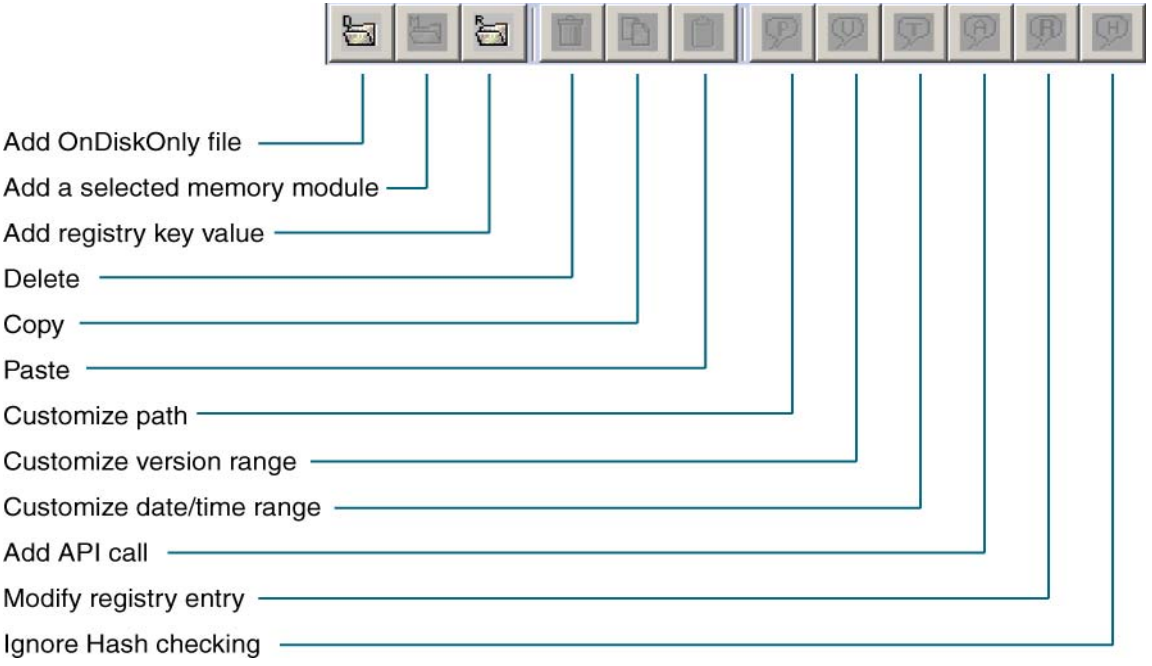
Hash

Hash value of the file.

Customizing a component

When an SRS component is selected by clicking on it, you can customize it using the toolbar below the component table, as shown in Figure 18 on page 64.

Figure 18 SRS Component Table Toolbar



Add OnDisk file as entry

Select a file from local file system and add it as one component of the SRS, for example, a text configuration file or a DLL. This enables you to make an API call to a DLL that is not yet loaded by TunnelGuard or the application.

Add a selected memory module as entry

Add the selected memory module from current memory snapshot.

Add registry key entry

Add the registry key number.

Delete entry

Delete the selected component.

Copy entry

Copy the selected component.

Paste entry

Paste component (from one SRS definition to another).

Customize path

Replace part of the path with a string of system environment variables. For example:

```
%WINNT%\xxx.dll
```

Set version range

Specify a particular version or a version range for the selected component.

Set date/time range

Specify a last modified date/time of the component, or a date/time range.

Add/Remove Vendor API call check

Indicate if third party API calls will be made using this component to do further checking.

Modify Registry entry

Modify the registry entry number.

Ignore Hash checking

Ignore hash value checking for the selected SRS entry.

Memory snapshot

The memory snapshot section in the lower half of the of the TunnelGuard SRS Builder Software Definition screen displays all processes currently running on the administrator's system.

You can select and add any process currently running and loaded into the memory snapshot to the SRS set by double-clicking on it or using the Add a selected memory module menu command.

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 one is available, for each process.

TunnelGuard Rule Definition screen

Select the TunnelGuard Rule Definition tab to access the rule definition screen. You use this screen to create and manage rules. The SRS Rule toolbar appears at the top of the screen.

SRS Rule toolbar

The SRS rule toolbar icons allow you to:

- Define a new SRS Rule
- Delete the selected SRS Rule
- Clone the selected SRS Rule

SRS Rule list

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

TunnelGuard Rule Name

This column shows the name of the rule.

TunnelGuard Rule Expression

This column provides the rule expression.

TunnelGuard Rule Comment

This column shows any comments related to the rule.

SRS Rule Expression Constructor

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

Available Expression list

The Available Expression 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 put the expression you created into the Available SRS Rule Expression list.

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

TunnelGuard support for API calls

One of the great features of a tunnel guard is its ability to interact with other software vendors applications. TunnelGuard can be configured to, above and beyond its own checks, to communicate to 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.

Making 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.

Windows

```
#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.