Version 2.0

Part No. 317393-B Rev 00
September 2005

600 Technology Park Drive
Billerica, MA 01821-4130

Contivity TunnelGuard Release Notes

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

Preface

These release notes contain the latest information about the Nortel* Contivity* TunnelGuard Version 2.0.

Before you begin

These release notes are intended for network managers who are responsible for the Contivity Secure IP Services Gateway. It is assumed that you have experience with windowing systems or graphical user interfaces (GUI), and familiarity with network management.

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`**.
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.

Related publications

For more information about TunnelGuard, refer to the *Configuring TunnelGuard for the Contivity Secure IP Services Gateway,* which provides information about configuring and using the TunnelGuard feature.

You can print selected technical manuals and release notes free, directly from the Internet. Go to www.nortel.com/documentation, find the product for which you need documentation, and 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.

Overview

The Nortel Contivity TunnelGuard Version 2.0 release notes contain the latest information about TunnelGuard.

It is not necessary for users to upgrade their client in order to create a user tunnel to the switch. Nortel provides backwards compatibility for Contivity VPN Client (CVC) user tunnel support. The addition of features adds enhancements and will not break the basic tunnel establishment.

TunnelGuard features for software release V2.0

The TunnelGuard features for software release V2.0 are:

- NOT operand for Software Requirement Set (SRS) and rules
- Support for registry-based rules and registry-checking functionality on Agent
- Manual editing of SRS entries
- File age check
- Clickable link in TunnelGuard Agent
- Clickable link in Contivity VPN Client (CVC) for absent TunnelGuard Agent
- Disconnect CVC or put CVC in restricted mode if no TunnelGuard Agent communication
- Custom install options
- Miscellaneous features

The following sections describe these features in more detail.

NOT operand for Software Requirement Set and rules

The NOT expression is part of the administrator tool applet. It is added to the AND and OR expressions to make rules from other existing rules. Where the AND and OR expressions are used to create rules to verify the existence of software packages, either installed or running on desktop PCs, the NOT feature is used to make rules based on the opposite of existing rules. 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.

Support for registry-based rules and registry-checking functionality on Agent

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.

Manual editing of SRS entries

The administrator tool applet provides On Disk and Memory Module buttons to create custom SRS entries and rules 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.

File Age check

When TunnelGuard is used, most of the 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.

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 name 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 represents a URL, such as http://, https://, or ftp://, automatically transforms to a clickable link.

Clickable link in CVC 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 the TunnelGuard Agent is not installed. A clickable link on the page directs the user to a location where the agent can be downloaded.

Disconnect CVC or put CVC in restricted mode if no TunnelGuard Agent communication

The TunnelGuard daemon tries to connect to the host agent seven times before stopping. The VPN administrator can configure a specific action for users who don't have TunnelGuard Agent installed.

The two configuration options are:

- Leave restricted and send banner if configured.
- Tear down and send banner if configured.

Custom install options

This release separates TunnelGuard core functionality from the desktop monitoring application. This separation allows the administrator to configure MSI installer to provide customized installer to the end user. TunnelGuard Core contains all of the TunnelGuard core functionality that includes TunnelGuard service, but excludes the desktop monitoring application. The desktop monitor

application puts its icon in the system tray and provides pop-up messages for failures and menu options. The administrator who selects the TunnelGuard Agent chooses the options available to the user. The custom install options provide the following:

- Optional TunnelGuard logs
- No or limited pop-up messages

Note: TunnelGuard Agent system tray icon previously provided a menu option **Exit** to the user when right-clicked. This feature is discontinued in this release.

Optional TunnelGuard Logs

TunnelGuard Agent logs are an optional feature with Windows Installer property **DisableLogging**. If set, no logs are created on the desktop PC. This feature works on registry settings on the desktop PC. If required, the end user can modify the registry setting to enable or disable TunnelGuard logging.

No or limited pop-up messages

TunnelGuard Agent opens a dialog window whenever there is SRS check failure, regardless of the policy set on VPN router for the rule. In some installation scenarios, this feature is not desirable. Also, 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 to be compliant. Some VPN administrators may choose to hide some or all of this information from end users. This release of TunnelGuard provides custom install option as well as Agent property to control this behavior.

Miscellaneous features

Better response for initial check failure

Initial Failure Recovery Mode resolves many situations that would otherwise keep the end user 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 is a faster, more frequent SRS compliance checking

by the Agent. Failure Recovery Mode does not involve the VPN router until a change is detected 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 can be configured using TunnelGuard properties. The duration of Failure Recovery Mode is the length of the first intra-interval checking.

TunnelGuard feature for Software release V1.1.3.0

Support for Alteon IPsec termination

The TunnelGuard Agent has been enhanced to support Alteon IPsec termination. To support both Contivity and Alteon, TunnelGuard Agent supports both Certicom Elliptic Curve from Contivity and ECDH from OpenSSL.

Customer issues fixed in this release

Table 1 lists customer issues from previous releases that are fixed in this release.

Table 1 Fixed customer issues

CR	Description
Q00709476	When the tunnel is in restricted mode and the status changes from non-compliance to compliance, the tunnel status is not changed until check status interval is defined at the Contivity. If the interval on the SRS recheck interval on the Contivity is set to the default, you have to wait 15 minutes before gaining full access to the network.
Q00925902	There can be a delay of 30 seconds to 10 minutes in TunnelGuard when removing Restricted Filter in Contivity 4600.
Q00852688	TunnelGuard icon drops from system tray after using the move window option.

TunnelGuard considerations

The following section describes TunnelGuard considerations.

Deleting rules or software definitions

When deleting an existing rule or software definition, you must first remove that definition from any group setting that references it. You must place a different policy on that particular group because (none) is not an option for setting the policy.

Upgrading TunnelGuard

TunnelGuard Agent software is offered with two installation packages. One package contains the Tunnel Guard agent software only, while the other package includes the JVM (Java Virtual Machine) required for TunnelGuard. When upgrading from a currently installed TunnelGuard Agent, it is necessary to upgrade using the same package as was originally installed. It is not possible to upgrade from one install package to a different package without uninstalling the previous copy. For example, customer who have installed TunnelGuard with VM can only upgrade to a newer TunnelGuard with VM.

Customized installation kit

The following 3 parameters, as referenced in the Customized Installation Kit section of Configuring TunnelGuard for the Contivity Secure IP Services Gateway, have been changed to:

NN_CVC601PATH -> NN_CVCPATH

NN_CVC601VERSION -> NN_CVCVERSION

NN_CVC601FORCEREBOOT -> NN_CVCFORCEREBOOT

There are no changes in the functionality of these parameters.

Version 2.0 known anomalies

The following section describes TunnelGuard issues.

Q01131617 — TunnelGuard Admin Tool Applet should not be cached on desktop PCs

TunnelGuard Admin Tool Applet is cached on the local PC when downloaded from the switch. Different versions of the TunnelGuard Admin Tool Applet are supported for different versions of the Contivity. If you use the same PC to access management of different Contivity switches, you may use the wrong cached version of the TunnelGuard Admin Tool Applet for the Contivity you are working on.

Q01200639 — Setting TunnelGuard policy in subgroup sets policy in /Base

Setting the TunnelGuard policy in the Connectivity section of a subgroup sets the TunnelGuard Policy for the /Base group, and any groups that inherit from it. This only happens the first time the policy is set. Setting the policy again in a subgroup does not change the first setting for the /Base group. Once a policy is set, there is no way to unset a policy through the GUI, so the policy cannot be deleted. Setting the TunnelGuard enable/disable option does not create the same problem.

The workaround is:

- Set policy only for group specified (and groups that inherit from it.)
- Allow a "No policy" option to unset TunnelGuard policies.