Version 1.1

Part No. 317393-A Rev 00
August 2003

600 Technology Park Drive
Billerica, MA 01821-4130

Contivity TunnelGuard Release Notes

NORTEL
NETWORKS™

Copyright © 2003 Nortel Networks

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

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

Trademarks

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

America Online and AOL are trademarks of America Online, Inc.

iPlanet, Java, and Sun Microsystems are trademarks of Sun Microsystems.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation.

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

Steel-Belted Radius is a trademark of Funk Software, Inc.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

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

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

Statement of conditions

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

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

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

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

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

Nortel Networks Inc. software license agreement

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

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

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

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

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

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

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

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

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

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

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

Contents

Preface

These release notes contain the latest information about the Nortel Networks* Contivity* TunnelGuard Version 1.1.

Before you begin

These release notes are intended for network managers who are responsible for the Contivity Secure IP Services Gateway. They assume that you have experience with windowing systems or graphical user interfaces (GUIs) 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 the www.nortelnetworks.com/documentation URL. 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 Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

You can purchase printed books and documentation sets from Vervante. To order printed documentation, go to Vervante at the www.vervante.com/nortel URL.

How to get help

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

If you purchased a Nortel Networks service program, contact Nortel Networks Technical Support. To obtain contact information online, go to the www.nortelnetworks.com/cgi-bin/comments/comments.cgi URL, then click on Technical Support.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, you can call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the http://www.nortelnetworks.com/help/contact/erc/index.html URL.

Chapter 1
Overview

The Nortel Networks Contivity TunnelGuard Version 1.1 release notes contain the latest information about TunnelGuard.

Description

TunnelGuard Version 1.1 is a new Java application, which runs on a client PC and is responsible for checking that any required components for a personal firewall are installed and active. TunnelGuard enables you to enforce certain policies on remote access end points.

TunnelGuard is separate from the Contivity VPN Client application. Because the Contivity VPN Client and TunnelGuard do not communicate, it works with any version of the Contivity VPN Client. If you currently have the Contivity VPN Client installed, you do not need to uninstall it before, during, or after installing the agent.

For further information on the TunnelGuard feature and installation instructions, see *Configuring TunnelGuard for the Contivity Secure IP Services Gateway* book (cfg_tg.pdf).

TunnelGuard directory

The TunnelGuard directory is on the client CD and contains the software files you need to configure and manage TunnelGuard. The TunnelGuard release notes are also located on the CD (tg_relnotes.pdf) that came with your software. The subdirectories on the CD are described in the following sections:

Windows

The Windows directory contains the Custom directory and the following executable files:

- TgNoVm_1_1.exe -- use when you already have JRE Version 1.4.2 or later
- TgVm_1_1.exe -- use when you do not have JRE

The Custom directory should be used if you want to modify the TunnelGuard installation and contains the following directories:

- NOVM -- customizable installation files without JRE
  - instmsi.exe
  - instmsiw.exe
  - TGCstNoVm_1_1.exe
  - TgCstNoVm_1_1.ini
  - TgCstNoVm_1_1.msi
- VM -- customizable installation files with JRE
  - instmsi.exe
  - instmsiw.exe
  - TGCstVm_1_1.exe
  - TgCstVm_1_1.ini
  - TgCstVm_1_1.msi

TunnelGuard considerations

The following sections describe TunnelGuard considerations.

Managing user groups being used by multiple versions of clients

By setting the client version threshold of a group to the highest value possible (Future ID 32), even the latest Windows-based Contivity VPN Client users will be blocked from getting into that particular group, as Version 4.65 comes with a version ID of only 12. However, Netlock clients present a high version number

(65535), so it will still can get in using this group. Using the version threshold in this manner allows the administrator to create a user group that only Netlock clients can log into. The requirement for the TunnelGuard agent would be disabled for that group.

Deleting rules or software definitions

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

TunnelGuard known anomalies

The following sections describe TunnelGuard issues.

Agent not sending status change while in restricted mode (Q00709476)

When the tunnel is fully opened and the PC goes out of SRS compliance, the new status is sent to the Contivity on the agent interval and the tunnel is torn down appropriately. However, 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 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.