Version 4.80

Part No. 315000-D Rev 00
August 2003

600 Technology Park Drive
Billerica, MA 01821-4130

Contivity Secure IP Services Gateway 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* Secure IP Services Gateway Version 4.80.

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 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 Basic Features for the Contivity Secure IP Services Gateway* introduces the product and provides information about initial setup and configuration.
- *Configuring TunnelGuard for the Contivity Secure IP Services Gateway* provides information about configuring and using the TunnelGuard feature.
- *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 RIP, OSPF, and VRRP, as well as instructions for configuring ECMP, routing policy services, and client address redistribution (CAR).
- *Managing and Troubleshooting the Contivity Secure IP Services Gateway* provides information about system administrator tasks such as backup and recovery, file management, and upgrading software, and instructions for monitoring gateway status and performance. Also, provides troubleshooting information and inter operability considerations.
- *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.

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 Contivity Secure IP Services Gateway Version 4.80 release includes new features added since the release of the Contivity Secure IP Services Gateway Version 4.70. These release notes contain the latest information about the Contivity Secure IP Services Gateway.

Refer to your Contivity hardware installation guide for instructions on getting your gateway up and running. After you configure an IP address, a subnet mask, and a gateway address (if applicable), you can view online Help from the management interface.

Version 4.80 new features

This section highlights the new Contivity Secure IP Services Gateway features that are supported in Version 4.80. For additional information, refer to the documentation set or the online Help.

- TunnelGuard enables you to enforce certain policies on remote access end points. It runs on the client and is responsible for checking that any required components for a personal firewall are installed and active. For further information on the TunnelGuard feature and installation instructions, see *Configuring TunnelGuard for the Contivity Secure IP Services Gateway* book (cfg_tg.pdf).
- SSL Administration enables secure management of the Contivity over SSL-enabled HTTP and can be used over all tunnel and interface types.
- Backup Interface Services (BIS) provides an automated mechanism to enable a backup interface when a primary connection fails.
- Circuit-less IP (CLIP) allows you to create virtual IP addresses on the Contivity that is not associated with any physical interface. It is an address that can be routed and redistributed through other dynamic routing protocols.

- Firewall enhancements include SSL-enabled user authentication, port scanning, enhanced logging for FTP and HTTP, and implied rules.
- Firewall User Authentication (FWUA) allows users to individually authenticate themselves.
- NAT enhancements include a management GUI integrated with the Contivity Stateful Firewall, port forwarding service, proxy ARP, dynamic routing and DHCP support, and NAT statistics.

Nortel Networks CD

The Nortel Networks CD contains all the software files you need to configure and manage your Contivity gateway. The directories on the CD are described in the following sections.

The directory named V04_80.124 contains the Nortel Networks Contivity Secure IP Services Gateway software. You would use this directory to upgrade your gateway from an older version of the product.

Doc (Documentation) directory

The doc directory contains the documentation set for the Contivity Secure IP Services Gateway. These guides are provided in Adobe Acrobat PDF format. The documentation set provides configuration, monitoring, administration, and troubleshooting information.

The documentation directory also contains the management information base (MIB) files.

Tools directory

The tools directory contains the following items:

- IP address configuration utility (ExtNetIP.exe) that configures the management IP interface on a newly installed Contivity gateway. After you run this utility, you can configure and manage the gateway using a Web browser from a PC.

- The Java* subdirectory contains the installation files for the Sun Microsystems* Java Runtime Environment (JRE) Version 1.4.1_02. This application is needed to load the Policy Manager configuration utility. The JRE should automatically be installed when these Java applets are first accessed; however, the installation files are included on this CD to allow for manual installation.

Restricted product - export license requirement

This product incorporates encryption technology that is highly restricted and can require an export license from the US Department of Commerce, Bureau of Export Administration, prior to international shipment.

A product that incorporates encryption with a key length up to 56 bits can be eligible for international shipment pursuant to a license exception. However, any product that incorporates encryption technology exceeding 56 bits will require an export license from the US Department of Commerce.

Pursuant to such license, the product can be marketed and sold only to a limited class of international users. Any entity, other than Nortel Networks, Inc., that wants to export this product must first obtain license approval from the US Department of Commerce.

Further, the user of this product cannot re-export, transfer, or divert the product to any country to which such re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries, or provide the product to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

Chapter 2
Considerations and issues

The following sections describe issues and considerations that apply to the Version 4.80 release of the Contivity Secure IP Services Gateway.

Fixed in this release

Table 1 lists customer issues from previous releases that are fixed in this release. In addition to these, it contains bug fixes from Version 4.75_140 except for the PPPoE TCP Clamping feature and CRs Q00600801, Q00602294-03, Q00587354-01, Q00605075, and Q00601671.

Table 1 Fixed in this release

Q00656394-02	Tunnel remains active after deleting parent group of a branch office tunnel from the GUI
Q00648183-02	Memory leak in tSesAsync when using external LDAP Proxy
Q00646761-02	Memory leak in tIsakmp using certificates and external LDAP proxy
Q00638497-02	Telnet sessions can get into semaphore lock.
Q00633759-02	Administrative user with switch manage rights and user view rights make changes
Q00633504-01	CES 1700 does not support WANic 700 HSSI I/O card
Q00629020-01	Default routes show up in the routing table with NextHopInterface unreachable
Q00628553-02	crlCollection is not freed which causes memory leak in extLdapAuthServerCLS
Q00627252-02	Only one of public default routes with equal cost shows up in the routing table
Q00627252-01	Only one of public default routes with equal cost shows up in the routing table
Q00627024-01	Static routes associated with WAN interface disappear upon reboot
Q00626971-02	Auto backup problem if directory tree has length 0f 68 or more
Q00620283-02	Contivity 1100 fails manufacturing boot due to bad ethernet frames
Q00620218-02	show running-config file not creating usable file
Q00620173-01	network add command will not allow multiple networks

Table 1 Fixed in this release

Q00618285-05	No accounting record sent
Q00618251-01	Disappearing default route if there are two public interfaces.
Q00610869-03	Cannot telnet through a restricted mode control tunnel
Q00605645-01	Problem with installing advanced routing key from QoS screen
Q00604987-04	Send One issue with SNMP traps
Q00601996-04	Problem when blank space put in Event log Sorting Key Wo
Q00600801-03	Contivity fails to authenticate against Novell LDAP when SSL enabled
Q00599590-02	4600 showing 257MB of RAM
Q00598323-01	Problem doing report graphs with corrupted DClog file
Q00589548-02	Radius server failover not working as TimeStamp attribute not in the LDAP
Q00582383-01	Deleted Group Assignment instance corrupted LDAP
Q00580858-03	Problem tBackup-Disk Sync while freeing a memory pointer
Q00580646-01	Radius authentication failing when using form of domain\login
Q00579340-02	Group Access Control not working
Q00579141-02	OSPF does not update next hops for external routes with non-zero forwarding address
Q00576223-02	Problem in IP reassembly code
Q00567519-02	Not able to Initiate large numbers of Main Mode BOT due to SessionAsync Task Max
Q00567181-04	CAR user tunnels are left in closing state
Q00566192-02	IPSec Tunnel sessions fail to establish and/or drop when session queries are run
Q00565632-01	Problem when entering 20+ characters within data collection field
Q00562673-04	Lock up occurs when trying to re-establish a QM tunnel
Q00560870-03	tBackup cores when path is too deep
Q00559042-02	Contivity sends out malformed SNMP trap 1004
Q00558783-02	SNMP on HSSI Interface, ifSpeed always return 43,008,000
Q00552367-04	Contivity Alert light remaining on.
Q00546837-02	Missing WAN statistics if using WAN card with T1 interface.
Q00541819-01	Enhancement request to get an acknowledgement pop-up that a
Q00540898-03	Problem with tBofInit suspended
Q00540424-03	User profile Static IP/Mask does not save through Telnet/Prov with certificate user
Q00503722-04	No FIPS status when FIPS disabled
Q00498165-02	Request to set password length of length 32 characters or more for IPSec user tunnels
Q00492007-03	IPsec Dynamic OSPF tunnel does not re-establish OSPF adjacency after OSPF bounce

Table 1 Fixed in this release

Q00481009-02	SERVICES > RADIUS should be enabled when client is enabled
Q00480997-02	No error message when SERVICES -> RADIUS client max secret value exceeded
Q00428674-04	System Log not capturing remote physical IP address
Q00415610-03	Enhancement to not use random ports when NAT traversal is disabled in group
Q00302433-03	Invalid IP address in pool caused banner text and banner sock error in clients
Q00252824-02	MIB-II ifadminstatus and ifOperstatus report down if lcp/ncp debug enabled
Q00088174-03	Admin > Administrator allows invalid characters

Product considerations

The following sections discuss product considerations or limitations.

Number of versions

Nortel Networks recommends that you maintain no more than two versions of the software on your gateways in addition to the version that is currently running.

Monitoring hard disk usage

Monitor the amount of space remaining on the hard disk drives; a full file system will produce unexpected behavior. (To check the hard disk usage level, choose Status > Health Check.) Because log files can consume a significant amount of disk space, especially in large configurations, remove old log files periodically.

Load-balancing and hardware encryption accelerator cards

When one or two optional hardware encryption accelerator cards are installed, Contivity software tries to ensure optimal tunnel throughput by balancing tunnels across available system resources, that is, the CPUs and the hardware encryption accelerator cards. Several parameters, such as the number of active tunnels and the current load on the resources, are evaluated during new tunnel establishment or rekeys to determine the assignment of a new tunnel.

After a tunnel has been assigned to a hardware encryption accelerator card or to the CPU, the gateway does not dynamically reassign the tunnel to a new resource due to the dynamic nature of the load balancing algorithm. Therefore, you may see some tunnels assigned to software (to a CPU) even if there are hardware encryption accelerator cards available.

Support considerations

- Version 4.80 does not support Check Point Firewall-1.
- Diffie-Hellman Group 5 does not interoperate with Version 4.0 or Version 4.70.
- Version 4.80 supports upgrades from Versions 4.50, 4.07, 4.06, and 4.70. If you are running an older version, you must upgrade to a supported version before you upgrade to Version 4.80.
- The amount of disk space required to upgrade to the latest version is configuration-specific. If you receive disk space error messages, you need to remove any unnecessary files from your Contivity system.
- Windows 95 does not support JRE 1.4.1_02 and therefore, Version 4.70 and subsequent releases do not support running the UI on Windows 95.
- Shasta Server Farm is not supported by Version 4.80.
- A T1 interface does not support packets larger than 47 KB.
- The Contivity UI and CLI support only 7-bit ASCII characters.
- The Contivity works with all RFC-compliant FTP servers.
- The Contivity supports the current version and generally the two previous versions of the Contivity VPN Client. If you have any concerns, contact Nortel Networks support organization for the latest information.

Contivity hardware and software compatibility

Table 1 shows Contivity Secure IP Services hardware and software compatibility.

Table 2 Hardware platform and server software compatibility

	Software version and release date						
Hardware platform	**4.06_180**	**4.07**	**4.50**	**4.50** **4.55_120**	**4.70** **4.75**	**4.76**	**4.80**
	11/8/02	**6/20/02**	**9/11/02**	**9/11/02** **12/09/02**	**12/20/02**	**5/23/03**	**8/08/03**
1010		X			X	X	X
1050		X			X	X	X
1100		X			X	X	X
600	X		X	X	X	X	X
1500	X						
1510	X						
1600	X		X	X	X	X	X
1700	X		X	X	X	X	X
1740							X
2000	X		X	X			
2500	X		X	X			
2600	X		X	X	X	X	X
2700	X		X	X	X	X	X
4000	X		X	X			
4500	X		X	X	X	X	X
4600	X		X	X	X	X	X
5000			X			X	X
	Minimum memory required (MB)						
	64	128	128	128	128	128	128

Tunnel licensing

The following tunnel licensing options are available for the Contivity 1010, 1050, 1100, 1700, and 2700:

- Base unit (low-cost router option) supports five tunnels. You can upgrade the license to support the maximum possible number of tunnels for the Contivity model.
- VPN bundle option supports the maximum number of tunnels for the Contivity model.

Table 3 lists the maximum number of tunnels for each Contivity model and indicates whether each model has a five-tunnel base unit version.

Table 3 Maximum number of tunnels by Contivity model

Contivity model	Maximum number of tunnels	Five-tunnel base unit available? (Yes/No)
1010, 1050, 1100	30	Yes
600	50	No
1700	500	Yes
2700	2000	Yes
4600	5000	No
5000	5000	No

BIS using dial interface with CHAP authentication

When using dial interfaces as backup interfaces in BIS and using CHAP authentication, you must configure the username and password in the Dial Interface Configuration screen. The username and password configured under the BIS configuration only works when using PAP authentication.

Multiple BIS interfaces using the same primary interface

Multiple BIS interface configurations that point to the same primary interface or use the same primary interface as the triggering interface is not supported. Do not configure multiple BIS interface in that manner. It will cause BIS to not function correctly.

Dial interfaces LCP Echo Request settings

The default setting for LCP Echo Request over dial lines is set such that Contivity sends out echo-requests every 10 seconds and an echo-response is expected back by the Contivity in 20 seconds. If no response is received within 20 seconds, Contivity will drop the call. If you run into call drops because of “Excessive Lack of LCP Echo replies” you may want to increase the fault threshold value accordingly. Alternatively, LCP Echo Requests can be completely turned off by setting the Echo Interval to 0.

PPP multi-link with BayRS over dial interfaces

When using PPP multi-link to connect to a BayRS router, turn LCP Echo requests off on the Contivity dial interface by setting the LCP Echo Interval to 0. There is an issue with BayRS software that causes the LCP replies to not get sent out correctly when multi-link is active. This will result in the call getting dropped if the LCP echo requests are not turned off on the Contivity.

Legacy option cards not supported in Contivity 5000

The Contivity 5000 does not support the following legacy option cards (neither of which is now sold):

- Ethernet LAN cards with the 82557 and 82558 chip sets
- Original Contivity hardware encryption accelerator card (order numbers DM0011041 and DM0011042)

The Contivity 5000 supports the following option cards in slots 3, 4, and 5 only:

- HSSI WAN option card (order numbers DM2104003 and DM2111003)
- Dual V.35 option card (order numbers DM2104001 and DM2111001)

This card can no longer be ordered. However, you can install existing dual V.35 cards in slots 3, 4, and 5 only.

Valid local address required for branch office tunnel

You must have the proper local end point defined while configuring a branch office tunnel. If invalid addresses (addresses that are not one of the Contivity interface or CLIP addresses) are used in heavy traffic conditions, performance may suffer substantially.

NAT policy considerations

If you are currently running Contivity Secure IP Services Version 4.70 with NAT policies applied to branch offices, the policies will appear as read only in the Version 4.80 Java GUI. You will see an (old format) text message to alert you to the change. The Version 4.70 policies will still be translated, you can no longer edit them. If you want to edit a Version 4.70 policy or use the CLI show running config command to export the NAT rules, you must launch the Java GUI, select the (old format) policy, select copy and save as, and apply the new policy to the branch office.

SSL administration configuration

When using certificates, Netscape Communicator and Internet Explorer perform various and differing security checks. The following configuration is recommended to obtain the best performance when administering the CES securely using Admin SSL.

1. Make an entry in the hosts file corresponding to your Contivity management IP address.
2. Import the root certificate that issued your Contivity server certificate into your browser store.
3. Import the root certificate that issued your Contivity server certificate into your JRE.

To satisfy a further name check by Netscape browsers, the Contivity server certificate common name (filled in when you create the certificate request on system > certificates > pkcs#10 certificate request) should be either a DNS name that resolves to the management IP address or the management IP address. For further information about Netscape certificates, go to http:/home.netscape.com/eng/security/comm4-cert-download.html.

Backing up your configuration

The automatic backup feature is provided as a way to backup your current configuration on the Contivity for later restoration. It functions by saving all of the contents of the Contivity file system from the /ide0/system point down. The contents of the flash memory are not saved as part of this process.

DHCP server assigns leases when neither CSF or interface filters enabled

A change to the interaction of the DHCP server and firewalls will now allow DHCP clients to obtain IP addresses when no firewall is enabled. This new behavior does not in any way enable clear text traffic to egress a public interface; it merely allows private side DHCP clients to obtain an IP address from the pool.

NetBIOS NAT ALG

The NAT ALG for NetBIOS packets supports datagram packets only; it does not have support for name service datagrams.

Certificate subject names

- All characters of the certificate subject and issuer DN are case insensitive. The subject DN "o=nortel" is considered equivalent to "o=Nortel". This complies with RFC 3280 4.1.2.4 and 4.1.2.6.
- When a user enters a full DN, the order of the individual components is no longer important because Contivity stores it in a predetermined order. For example, if you enter the DN of cn=joe, ou=contivity, o=nortel, c=us, this is viewed by the Contivity as identical to: ou=contivity, o=nortel, c=us, cn=joe Rearranging the order allows the Contivity to correctly process certificates generated by CAs with differing DN encoding orders.

Enabling manageability mode may affect performance

When manageability mode is enabled from the System > Settings > Enable Manageability Mode screen, the priority of the HTTP management tasks is given higher priority to ensure manageability. However, the performance of the Contivity may be impacted when management access is ongoing, due to it's high priority, and other services (such as routing or tunnel creation) may not occur in a timely manner. Also, CPU or I/O intensive management operations such as secure management access (SSL enabled HTTP), and viewing large event logs will increase the possibility of service disruption.

RADIUS server disabled when upgrading

When you upgrade to Version 4.80, the RADIUS service is disabled by default even if it was previously enabled. If your configuration is using RADIUS, be sure to re-enable RADIUS service after upgrading to Version 4.80.

Asynchronous branch office tunnel with nailed-up option enabled

If a nailed-up asynchronous branch office tunnel initiator tunnel is configured, a tunnel disconnects after three minutes the first time it connects. Because the tunnel is nailed-up the connection is automatically be re-established.

Branch office support for state and cost

You can share state and cost in Branch Office > Accessible Network > Remote Endpoint with previous versions through LDAP. Nortel Networks recommends that you do not share an external LDAP server between different versions of the Contivity Secure IP Services Gateway.

NAT traversal port numbers

Nortel Networks strongly recommends that you use port 10001 for NAT Traversal. Do not use L2TP/L2F port 1701 or General Packet Radio Service (GPRS) port 3386. Make sure that any port you select does not conflict with any ports that you are already using.

Recovery floppy diskette

Any recovery floppy diskette that you created prior to release Version 4.0 will not work on a system that runs Version 4.0 or later software. Nortel Networks recommends that when you upgrade to Version 4.0, 4.50, 4.70 or 4.80 software, you create a recovery floppy diskette as soon as you complete the upgrade. This version of the recovery floppy diskette works on systems running any release up to and including Version 4.50. You must use a formatted diskette when creating the recovery diskette.

Downgrading from previous versions

You must disable the Contivity Stateful Firewall before you downgrade to any version prior to Version 3.50 of the Contivity Secure IP Services Gateway. If you fail to disable the firewall, you may encounter unexpected results when you reboot for the downgrade.

RADIUS-supplied attributes

Contivity supports RADIUS-supplied attributes, such as IP address and MPPE key and additional specific attributes, if they are returned from a RADIUS server; any other returned attributes are ignored. The specific attributes are detailed in Microsoft documentation and defined in RFC 2548. This data overrides the corresponding data stored in LDAP.

PPTP and L2TP MPPE 128-bit encryption keys

PPTP and L2TP MPPE 128-bit encryption keys do not work properly in the Contivity if they were obtained during RADIUS authentication with a Funk Software, Inc. Steel-Belted Radius* Server Version 2.2 or later. This problem also applies to other RADIUS servers derived from Steel-Belted Radius, including the Bay Networks* BSAC RADIUS server Version 2.2 and later and the Nortel Networks Preside* RADIUS server Version 1.0.49 and later.

In addition, the Microsoft RADIUS server exhibits this problem when doing MS-CHAP authentication that returns MPPE keying information. PPTP and L2TP MPPE based 40-bit encryption is unaffected by this problem. Do not use the noted RADIUS servers with the gateway if PPTP or L2TP MPPE-based 128-bit encryption is required.

Browser considerations

You should be using the latest version of your browser to ensure accurate screen displays of the Web interface for the gateway.

- Internet Explorer 5.5 or 6.0 and Netscape* 4.79 or 6.2 are the supported Web browsers. You should be using the latest version of your browser to ensure accurate screen displays of the Web interface for the gateway.
- Both Internet Explorer and Netscape browsers cache user ID and password information. If you have caching enabled in your browser, Nortel Networks recommends that you close the browser when you finish making changes to the gateway.
- America Online* (AOL*) V5.0 Web browser is not supported.
- Netscape 4.79 incorrectly does not prevent users from launching multiple copies of Contivity Firewall Configuration tool. If you click on the Manage Policies button twice or more without waiting for the configuration tool to appear, multiple copies of the tool will be launched and lead to runtime errors. If this happens, you must close all active browser windows and start a new management session.

Viewing and calculating memory usage

The minimum memory requirement for Version 4.80 is 128 MB.

The Memory Calculator tool is a Microsoft Excel spreadsheet that provides information on determining the memory requirements for a Contivity system based on the configuration of tunneling, routing, and firewall. The configuration values can be input in the Memory Calculator tool to determine the base memory recommended for the specified configuration. Given the dynamic nature of memory usage, the result provided by the tool is only an estimate.

Nortel Networks recommends that you evaluate the memory requirement using the Memory Calculator tool to ensure that sufficient memory is installed for the configuration prior to upgrading to Version 4.50. Contact your Nortel Networks sales representative if your configuration requires additional memory.

The parameters affecting Contivity memory usage are:

- Contivity software version
- Single or dual CPU (if single CPU model or dual CPU model Contivity Secure IP Services Gateway)
- Internal or External LDAP shows whether internal or external LDAP configured
- Number and type is the number and type of branch office and user tunnels
- Static routes is the number of static route entries in the IP routing table
- RIP routes is the number of RIP route entries in the IP routing table
- OSPF Routes is the number of OSPF route entries in the IP routing table
- Redistributed OSPF and RIP Routes is the number of routes redistributed into RIP and OSPF Routing protocols
- FW/NAT Max connections is the maximum number of connections as configured from Services > Firewall/NAT > Edit screen
- FW/NAT Number of Sessions is the total number of Firewall/NAT sessions
- BO NAT number of Sessions is the number of Branch Office NAT sessions
- CSFW Enabled shows if CSIF (Contivity Stateful Firewall with Interface Filter) is on
- Interface NAT Enabled shows if Interface NAT is on
- Antispoofing Enabled shows if Antispoofing is on

The Memory Calculator Tool is available at:

`www.nortelnetworks.com/documentation`

Select Data and Internet and then Contivity Secure IP Services Gateway Portfolio. Go to Technical Support Documentation and then Engineering Notes and Guidelines.

To view the Contivity system memory status, use the Status > System screen. The Memory field under System Hardware displays the total amount of memory provisioned, as well as how much memory is currently free.

IPTunnel SNMP MIB

If the IPTunnel SNMP MIB is currently enabled in Version 3.50 or Version 3.60 software, it will be disabled after you upgrade to Version 4.0 or higher. You can reenable it on the Admin > SNMP screen.

Gateway disconnects with PC client through LinkSys

If you are using a Linksys Etherfast Cable/DSL router in IPSec passthru mode, and if two or more PCs connect through it to a gateway, then one or both of these PCs will be disconnected and/or their communications disrupted unless NAT Traversal mode is used on the gateway. (The client monitor will continue running and will not display a message that the connection is disconnected or disrupted.) This occurs because the LinkSys does not support more than one IPSec session. To prevent this, select the Auto-Detect NAT option on the Profiles > Groups > *GroupName* > Edit IPsec screen, which activates NAT Traversal and allows multiple PCs behind the NAT box to function properly.

Windows 2000 client using L2TP over IPSec

You cannot run the Windows* 2000 client using L2TP over IPSec if the Contivity VPN Client is installed. The IPSec driver conflicts with the native IPSec driver in Windows 2000. You must disable the Windows 2000 IPSec driver, which effectively prevents the use of the Windows 2000 Client using L2TP/IPSec. If you go to the Services > IPSec screen and change the IPSec Policy Manager setting from Disabled to Automatic and reboot the system, the client detects the loading of the Windows 2000 IPSec driver and disables the client's IPSec driver.

Online Help files

You can print the online Help files by going to Help > Help Contents and selecting the topic that you want to print.

Contivity Stateful Inspection firewall UI

The Contivity Stateful Inspection Firewall Java UI requires Version 1.4.1_02 of the Java Runtime Environment for proper operation. The JRE 1.4.1_02 is distributed with the Contivity Secure IP Services Gateway image; it can also be downloaded from Sun Microsystems, Inc.

Using OSPF virtual links

Because Version 3.*x* does not support OSPF vlinks, you must turn on or off a flag using the CLI **`Compat_3_6 enable`** command. However, this flag does not permit gateways running Version 4.0 to form a virtual link over tunnels.

If all the gateways in the network are running Version 4.0, then Nortel Networks recommends that you use the no Compat_3_6 enable flag on all of the gateways. Even if only one gateway running Version 3.*x* participates in OSPF through tunnels, then every gateway with Version 4.0 needs to be set with the Compat_3_6 enable flag.

For example, if end-point A is running Version 4.0 and end-point B is running Version 3.*x*, end-point A should have the Compat_3_6 flag enabled for OSPF to work properly. However, if both end-point A and end-point B are running Version 4.0 and both have enabled the Compat_3_6 enable flag, OSPF will work properly, but vlink over this tunnel may not work properly. Also, if you set the flag for end-point A to Compat_3_6 enable and end-point B to no Compat_3_6 enable, OSPF may not work properly.

If you set the flag for end-point A to no Compat_3_6 enable and set end-point B to no Compat_3_6 enable, OSPF and vlink will both work properly over this tunnel.

Post implied rules tab removed

The Post implied tab of the Contivity Stateful Firewall was removed in this release. This was done without loss in functionality, to present a less complicated firewall configuration environment.

Branch office test fails when traffic is passed over non-nailed up tunnel

Testing a branch office tunnel might fail if the tunnel is being initiated from both sides at the same time. This occurs when the initiation is due to live traffic or a test button tunnel initiation.

Inactive PPP connection through LMC 1200 board

If you are using an LMC 1200 board (V.35) and you suspect that your PPP connection is not working properly, perform the following steps to check the connection. The connection might appear to be working (for example, the board's LEDs might be active) but no data is being passed through.

1. Go to your gateway’s System > WAN screen. Select the Statistics button for the interface.
2. On the Statistics screen, check the IP Packets Sent field. If the field shows that zero packets have been sent, this indicates that the PPP connection is not active.

You must re-initialize the board to activate the PPP session: power off the gateway, wait a few seconds, and then power it back on.

Changing an interface card that has many branch office tunnels

If you remove or move to another slot an interface card that has hundreds or thousands of branch office tunnels configured on it (that is, the local tunnel end point is configured on that card), an extended delay may occur when you reboot the system as the gateway attempts to initialize the branch office tunnels using the nonexistent local end-point IP address.

To avoid a lengthy delay after moving or removing an interface card:

1. Before you move or remove the interface card, enable manageability mode.

On the Web management interface, choose System > Settings. Or, from the CLI Global Configuration mode, enter this command:

```
CES(config)# scheduler manageability enable
```

2 Shut down the gateway and then move or remove the interface card.

3 Restart the gateway.

4 While the gateway is rebooting, configure the proper interface IP address so that the branch offices can be initialized in the normal time frame.

Obsolete CLI commands

Table 4 lists the CLI commands that are not displayed in interactive mode for Version 4.80. However, these commands are still supported and will continue to function properly if you are using them in scripts.

Table 4 Obsolete CLI commands

# show running-config server address-pool	Displays pool configuration information
(config/rule)# use dest-port eq WORD	PortName
(config/rule)# use src-port eq WORD	PortName
(config)# control create WORD WORD A.B.C.D A.B.C.D A.B.C.D A.B.C.D A.B.C.D	Remote network subnet mask
(config)# control help	Description of the control tunnel help system
(config)# control show	Displays current control tunnels defined
(config)# ip default-route-preference private default	Defines that public routes will be preferred as default routes
(config)# ip dhcp address-release	Enables the address release policy
(config)# policy nat enable	Enable Interface NAT.
(config)# policy nat interface disable	Disable Interface NAT.
(config-group/ipsec)# default encryption 3des-md5	Triple DES with MD5 Integrity
(config-group/ipsec)# default encryption des40-md5	40bit DES with MD5 Integrity
(config-group/ipsec)# encryption ike 128aes-group5	AES 128 with Group 5 (1536-bit prime)
(config-if)# no ppp ip local negotiated	Specifies rejection of a negotiated local IP address
(config-if)# no ppp remote authentication chap	Disables CHAP authentication
(config-if)# ppp remote authentication chap	Enables CHAP authentication
(config-if)# ip rip export-bo-static-metric 0	Disables export branch office static route metric
(config-if)# ip rip export-static-metric 0	Disables export static route metric
(config-if)# ppp ip rip export-bo-static-metric 0	Disables export branch office static route metric
(config-if)# ppp ip rip export-static-metric 0	Disables export static route metric
(config-car)# summarization	Enables the network routes of client address to be injected to routing table for redistribution
(config-subif)# encapsulation PPPoFR	Configures PPPoFR encapsulation
(config-subif)# ip rip export-bo-static-metric 0	Disables export branch office static route metric
(config-subif)# ip rip export-static-metric 0	Disables export static route metric

Documentation notes

The following sections describe items that will be added to future versions of the documentation.

Dial interface correction (Q00725400)

In Chapter 3 Configuring Dial Interface of the *Configuring Tunneling Protocols and Advanced WAN Settings for the Contivity Secure IP Services Gateway* book, the screen shots and the description under the “Configuring Dial Interfaces” subsection, pertains to the configuration of the Contivity's serial (COM) port as a dial interface. The V.90 configuration and screen shots have not been included separately. However, the configuration of V.90 interface is similar to the configuration of the Serial Port except in the following:

- For a V.90 interface, there is no Port Mode configuration parameter. V.90 can only be used for PPP.
- For a V.90 interface there is no Baud Rate parameter. The V.90 interface auto-negotiates baud rates down starting from 56K as needed

NTP server replies ignored (Q00713605)

Previously the NTP server would open the NTP port for the management IP rather than the filter. Now if the Management IP address is higher than the LAN IP and an NTP server is configured as accessible from the private network, NTP operates properly, but the local address will show up as 0.0.0.0 on the Status > Statistics > NTP Stats screen.

Public address table works only when Firewall/Interface filters are disabled (Q00676509)

Because there are no routing protocols (RIP, etc.) running on the untrusted interfaces, there is no way to know how to route packets to the appropriate trusted interfaces. The IP public address table (PAT) provides the needed routing information. Because the sources are not trusted using this interface, the IP PAT is used to limit unauthorized sources. PAT is disabled when either the Contivity Stateful Firewall or filter firewall is enabled to provide better policy-based security.

When the firewall is disabled, PAT applies only to packets received on a public interface. PAT has a list of trusted sources that includes the remote client or branch office tunnel end point, remote Radius/CMP/CRL server address (if on the public side). PAT does not limit the packets from any of those trusted sources. For packets coming from any address that is not in the trusted source list, a rate limit (6 packet/10 second) is applied based on the source address.

The Contivity Stateful Firewall public address table information is not related to network address translation (NAT) or network address port translation (NAPT), which is often referred to as port address translation (PAT).

Default Configuration for 1010, 1050, and 1100

The 1010, 1050, 1100 default configuration is set up to meet requirements for the majority of small office connections. This configuration includes a public interface configured for IP and can receive an address via DHCP from the ISP. The private side has the DHCP server enabled and the DHCP address pool set to 192.168.1.1/24. If you require a configuration such as PPPoE, you must first delete the IP protocol and a drop down list appears. Available configuration details do not appear on the default configuration screen unless this is deleted first.

Known anomalies

The following sections describe issues that Nortel Networks has determined need to be fixed in a future release, but will not be fixed in the current release. For TunnelGuard related issues and considerations, see *tg_relnotes.pdf*.

CLI issues

The following sections describe issues that apply to the command line interface (CLI).

Provisioning with external LDAP and show running-config (Q00725303)

When you provision a Contivity using **show running-config** and an external LDAP, it does not enable all Services > IPSec encryptions. Also it disables all encryptions for /Base on Profiles > Branch Office group configuration screen.

Configuring multi-line banners for firewall user authentication (Q00719780)

The firewall **user-authentication** command does not provide a method for adding multi-line welcome banners because of parser limitations that cannot span more than one line.

Managing entity names that begin with a CLI keyword (Q00633489-01)

You cannot use the CLI to manage entities with names that begin with the same letters as a CLI keyword. For example, you cannot edit connections (branch office tunnels) whose names begin with “a,” “ad,” or “add,” because “add” is the CLI keyword used to add tunnels. You can create a branch office connection whose name begins with these letters, but when you try to edit the connection, an error message appears. The CLI parser does not recognize the input as data even if you enclose the name in quotation marks.

```
CES(config)#bo-c add add /Base
CES(config)#bo-c add /Base
                     ^
% Incomplete command. See '^' marker.
CES(config)#
```

As a workaround, use the Web GUI to rename tunnels whose names begin with “a,” “ad,” or “add” if you need to manage such tunnels with the CLI.

Provisioning time (Q00627570)

If you configure an external LDAP proxy server that is unavailable, you will experience delays in Contivity provisioning times.

Frame relay circuit issue when editing unrelated WAN card (Q00562810)

Editing an unrelated WAN card causes a virtual connection to go down and if a card is already disabled, configuration commands are either not disabled or ignored. You can configure the CSU/DSU from the CLI on cards that do not have on board CSU/DSU (the WANic 400 and LMC 1000). Also, if you make changes to a card that does have on-board CSU/DSU (LMC 1200), it brings down a frame relay VC on an unrelated card. CLI should configure CSU/DSU only on the cards that allow it.

Using show running routing dhcp-relay command (Q00506537-01)

If you use the **`show running routing dhcp-relay`** command with DHCP relay globally configured or with it disabled but still configured for the same interface, it does not show the configuration. The command should configure the feature and then disable or enable it based on its status.

Show Logging Events command (Q00488571-02)

The CLI event log may have missing events when under extremely heavy load.

CLI shows disabled IPSec encryption as enabled (Q00447373-01)

If you globally disable all IPSec encryption from the CLI and then execute the **`show bo-group /Base`** command, the last IPSec encryption that was disabled shows as enabled. The UI shows all encryption for /Base as disabled.

CLI changes to branch office groups (Q00438531-01)

If you make changes to the IPsec encryption level to a group with active tunnels, the tunnels do not bounce and then come back. The changes do not take effect until the tunnel is logged off and then reinitiated.

Editing user accounts created in CLI from UI (Q00255043-01)

If you add a user without any parameters using CLI and then use the UI to add an IPSec username and password, it does not work and the IPsec no entries found error message appears.

Viewing invalid default route through serial menu or CLI (Q00227717-01)

Because invalid default routes do not appear either with CLI or through the serial menu, they cannot be deleted. However, they can be viewed and deleted through the UI.

Caching configuration screens (Q00207522-01)

Your Internet browser might be caching configuration screens. This becomes an issue if another UI session or CLI session is changing parameters displayed on the same screen. In this case, refreshing the screen might not display the latest version of these parameters. To ensure that the latest values are displayed, you can either disable browser caching or restart the management session by logging out and logging in again. You should check how many management sessions are open before making any critical configuration changes. Two users modifying the same functional area simultaneously could lead to an inconsistent configuration.

Boot system version command (Q00173683-01)

The CLI **`boot system`** `[<`*`version`*`>]` command does not work. Instead of rebooting the device it displays warning message indicating that reboot is not possible because there are users logged on to the gateway. Use the **`boot system`** `[<`*`version`*`>]` **`recurse`** command to reboot the device through the CLI interface (Telnet or serial connection).

Incorrect master-delay output (Q00173616-01)

The **`show running-config vrrp`** command does not produce correct output for master-delay parameters. It always displays the delay as 00:00:00 regardless of what is actually configured on the box. If a script generated this way is used to provision other boxes, you have to manually insert the proper value.

CLI network command (Q00072440-01)

For the CLI **`network`** {*`<network-address>`*} {*`<wildcard-mask>`*} **`area`** {*`<area-id>`*} command, the network address on the gateway refers to an actual IP address on a physical interface.

For example, if the gateway has three IP interfaces defined as 192.32.54.37, 192.32.54.65, and 192.32.54.97, you need to use the following three commands for all the interfaces to be configured in area 0.0.0.0:

```
network 192.32.54.37 0.255.255.255 area 0.0.0.0
network 192.32.54.65 0.255.255.255 area 0.0.0.0
network 192.32.54.97 0.255.255.255 area 0.0.0.0
```

Routing issues

The following sections describe issues related to routing.

Dynamic changes to CAR options incorrect in routing table (Q00708960)

You can switch freely between the various CAR modes (disabled, host only, static aggregation, and dynamic aggregation). However, this can create some unpredictable behavior in the routing table. For example, if one or more clients were already logged in when you switched from static aggregation to host only mode, the aggregated route would remain and the host routes would not be added to the table. In this situation, only new client logins would get their host routes added to the routing table.

Anti-spoofing and routing configuration (Q00660243)

Anti-spoofing ensures that packets arriving on an public interface do not have a source address in the Contivity private network space. Because learned routes constitute private addresses, you must disable direct nets and direct hosts as route sources from the Routing > Policy configuration screen.

OSPF DD packets with incompatible MTU size accepted (Q00657955-01)

RFC 2178 specifies that when a device (such as a router or gateway) receives an OSPF database description (DD) packet that advertises an MTU larger than the device can receive, the router or gateway should drop this packet to prevent an OSPF adjacency from forming. However, the Contivity gateway does not drop such DD packets and instead tries to form an OSPF adjacency.

Configuring two interfaces within same subnet (Q00559903)

To avoid routing problems, be sure that you do not have two interfaces in the same subnet.

Responder tunnels cannot use multicast boundary list (Q00537232-01)

You can only use the multicast boundary list on a interface that has an IP address. Asynchronous branch office responder tunnels do not have an IP address and therefore cannot use the multicast boundary list.

Multicast boundary list cannot be enabled or disabled (Q00535443-01)

You cannot disable multicast boundary through the Add Multicast Boundary screen, but you can use the Enable and Disable buttons on the Routing > Multicast screen.

Adding and deleting RIP from interfaces (Q00527130-02)

Host routes do not appear even when they are redistributed. If you delete the interface while RIP is configured and enabled and the redistribution of host and net is enabled, the host and net should show up on the database. However, only the net shows up and not the interface.

Exiting browser during VRRP configuration (Q00458703-01)

If you start to configure VRRP and instead of cancelling the configuration, exit the browser (click on the back button), the UI creates OM records and leaves it in a default state (0 for VRID). This creates unusable records that are never cleaned unless you specifically remove them. However, it does not prevent the application from running properly.

Incorrect routing error message (Q00447493-01)

The UI incorrectly informs you that a license key is required to change the Default Route Preference option located on the Routing > Configure screen. If you need to change this option, you can ignore this warning.

Verify changes to RIP configuration (Q00281283-02)

When making changes to the RIP configuration using the UI, you may need to click on the OK button more than once for your changes to take effect. To verify that your chances have taken effect, go back to the RIP configuration screen.

Two unique LSIDs must exist in backbone area (Q00067571-02)

RFC 2328 supplies an algorithm for the assignment of LSIDs for more specific/ less specific routes. For example, if IP address (a) 192.50.10.66/27 is in OSPF area 2.0.0.0 and IP address (b) 192.50.10.67/26 is in OSPF area 2.0.0.0, address (a) has 30 possible host addresses and address (b) has 62 possible host addresses. Both (a) and (b) need to have entries in the OSPF backbone to ensure full connectivity. Therefore, for the backbone area to differentiate the same summary network (in this case, 192.50.10.64), two unique LSIDs must exist in the backbone area. This functionality is supported for AS external-LSAs but not for summary-LSAs.

Authentication and certificate issues

The following sections describe issues that apply to authentication.

RADIUS authentication of Contivity VPN Client requires PAP or CHAP (Q00693226)

When you configure RADIUS authentication from the Servers > Radius Auth screen, you must enable PAP or CHAP for successful authentication of the Contivity VPN Client over RADIUS. Support for conversion to MSCHAP will be in a future release.

Certificate referencing issue when changing LDAP location (Q00632976)

When changing from internal to external LDAP or from external to internal LDAP, you must reload the server certificates used for SSL/TLS connections.

Compatibility between versions when using AES with group 5 (Q00609054)

If you configure AES group 5 within a branch office group between two Contivity gateways, and only one of the gateways is running Version 4.76, the two gateways will not interoperate. If you configure AES group 5 on a gateway that is running a software version earlier than Version 4.76, that gateway will not work with third-party devices or with a Contivity gateway running Version 4.76. (A gateway running Version 4.76 and AES group 5 will work with third-party devices.) Nortel Networks recommends that you use AES group 8 instead of group 5.

LDAP authentication over SSL does not work with active directory (Q00504327-01)

When trying to use LDAP authentication over SSL to Active Directory, the SSL connection cannot be established. A cipher suite appears to be negotiated, but the connection fails with an Unknown Error.

Windows 2000 VPN server (Q00228485)

For the current release of the Windows 2000 VPN server, you must disable IPSec compression (LZS) in the branch office group to allow the gateway to successfully initiate branch connections with Windows 2000.

Using certificate RDN fields for a remote identity (Q00154595-01)

If you are using RDN fields to identify a certificate user (either branch office or user tunnel), you must clear the current contents of all RDN fields, save the empty values, and then enter correct values.

NAT and Contivity Stateful Firewall issues

The following issues pertain to Network Address Translation and Contivity Stateful firewall.

Firewall Policy Rules disappear when moved and copied (Q00722486-01)

When the rule is cut and pasted, the parenthesis is removed from the key word, resulting in an error when the policy is copied. You can use either of the following ways to work around this issue:

- Use the save policy as option instead of copy from the Firewall - Select Policy screen.
- Change the event log type from none to brief, detail, or trap to correct the missing parenthesis.

Firewall shows interface not present (Q00697364)

When you create a firewall rule, under Interface Specific Rules, it lists Slot 7 Interface 1, which is the serial port. The serial port listing does not appear on versions of Contivity prior to Version 4.80.

Using quotation marks with FWUA welcome banner (Q00683336)

Quotation marks should not be included in the text field of a firewall user authentication (FWUA) banner. This applies to FWUA banners created on the Services > FWUA and on the Profiles > Groups > FWUA screens.

SNMP traps affected when NAT policy modified (Q00660225)

If you modify a NAT policy to a new translated NAT address or apply a new NAT policy, the traps sent use the original NAT address. The active NAT policy shows the correct NAT translation, but the NAT cache has to be flushed before the modified NAT policy works correctly. Traps are only sent from the first applied NAT policy.

Enabling NAT and then firewall (Q00626964)

If you are running an a slower version of Windows, the rate of refresh may give you time to re-select some check boxes and click on OK again during the refresh process. This will cause incorrect behavior if you are trying to enable NAT and then the firewall.

International characters in group names (Q00039540-01)

Do not use non-ASCII (US) characters in the names of branch office groups, user groups, firewall and NAT rules or other named entities.

Contivity 1010/1050/1100 issues

The following describe issues that were identified with the Contivity 1010/1050/1100.

Deleting previous version before upgrade (Q00536634)

Because the Contivity 1010, 1050, and 1100 are diskless systems with limited storage space, you must delete the last non-loaded version of code on the box before you can upgrade.

Incorrect restart system message (Q00457593-01)

When running the recovery process on a Contivity 1010/1050/1100, the restart system description incorrectly states “To restart the system, remove the diskette and press the Reset button on the back of the Switch.” These units do not have a diskette and you just need to turn the power off and on again.

General issues

The following release notes apply to the Contivity Secure IP Services Gateway.

Windows 2000 PPP/L2TP multi-link (Q00727615)

The Contivity sends the LCP echo requests but does not recognize the LCP replies received from the tunnel and determines that no replies were received. To work around this issue, you need to turn of multi-link negotiation on the client:

1. Right click on the Windows 2000 client and select Properties.
2. Under the Networking tab, select Settings.
3. Check to be sure that “Negotiate multi-link for single link connections” is disabled.

Boot drive selection on Contivity 5000 (Q00725494)

A software error will result during a disk synchronization operation if ide1 is selected for the boot drive. Ide0 is the default boot drive and should remain so unless a hardware failure of ide0 necessitates the use of ide1 for boot.

BIS ping trigger on networks with devices that disallow Ethernet broadcast (Q00725466)

BIS Ping trigger cannot be used where the primary (source) interface is an Ethernet interface that connects to a networks device that does not allow forwarding of Ethernet (MAC level) broadcast packets. Use another BIS trigger instead of Ping Trigger in such situations.

Using square brackets in event logs (Q00725362)

Do not use strings that contains square brackets [] in the Sorting Key Words field on the Status > Event Log screen.

ISDN service provider interoperability in Switzerland (Q00722686)

For the Contivity ISDN interface to work with some of the ISDN service providers in Switzerland, the firmware version on the ISDN card must be upgraded to firmware “Version 2.39. August 2003.”

Restoring a backup image from recovery disk (Q00721362)

An extra slash (/) character is erroneously appended to the beginning of the backup path every time an auto-backup occurs. This error does not impact the successful completion of the auto-backup, but you need to adjust the path and remove the extra characters before executing a Restore Backup from the recovery image/disk.

Using PPPoE as secondary On Demand circuit (Q00719478)

If you use a PPPoE interface as the backup interface in BIS, you must disable the On Demand parameter of PPPoE. Configuring PPPoE as a backup interface with On Demand enabled causes BIS to repeatedly bounce the circuit.

Using dial interface as backup in BIS (Q00701773)

To use a dial interface as the backup interface in BIS, you must configure the PPP Authentication protocol under the Dial Interfaces PPP configuration. You must configure the user-name and password parameters under the BIS configuration.

Sharing external LDAPs causes instability (Q00701008)

When multiple systems share an external LDAP, any parameters added or removed from the external database by one system are not visible to the other system until the database caches are flushed. The cache flush is a timed interval.

Error when attempting to view branch office group (Q00696932)

If there is an apostrophe in the group name, the link to the group configuration screen generates an error. To resolve this issue, add key values directly to the dictionary to avoid any parsing issues.

Setting WAN PPP IP via serial menu (Q00696510-01)

You must configure a WAN PPP interface through the CLI or GUI. If you attempt to configure a WAN PPP interface through the serial menu, the IP address will create a core situation.

Changing from dynamic to static branch office tunnel (Q00692438)

When you change from a dynamic to a static branch office tunnel and enter the remote network, the tunnel goes down. The tunnel should stay up until you are entirely finished with the branch office configuration and not when you configure the routing part of the branch office tunnel.

L2TP/IPSEC IPsec Transport Mode Connections (Q00671793)

If you use inheritance to enable IPsec Transport Mode Connections, the L2TP authentication never takes place and the end user connection attempt times out. The IPsec transport connection is established, but the L2TP authentication never occurs. If you do not use inheritance on the group and IPsec Transport Mode Connections is explicitly enabled on the group, the tunnel is established.

Status Health Check and SNMP Trap screens (Q00634001-01)

To display the most recent status, some management screens perform network activity before the display. For example, the Health Check screen tries to contact servers, such as DNS and SNMP, before it displays the server status. Displaying such screens could be delayed if there is a network problem or if the servers do not respond within a time limit.

Changing branch office tunnel type (Q00627074-01)

If you configure a branch office for a tunnel type of IPsec or L2TP over IPsec and then later change the tunnel type to L2TP or PPTP, ISAKMP still comes up if the remote peer tries to initiate it.

Incorrect WAN status in system report (Q00560429)

The system report for WAN cards for frame relay interfaces incorrectly reports that the card is local when it is public, and public when it is private (local). Also, the IP address is not displayed and the mask is incorrect. PPP WAN interfaces are shown correctly.

Error message when adding branch office groups (Q00548286-01)

You cannot add multiple branch office connections using the Apply button in the GUI. After a connection is added, click on OK and proceed to configure the connection. Once the connection is fully configured, click on Add to configure additional branch office connections.

Some DHCP server options are not configurable (Q00532773)

The DHCP Policy Filter Option requires a list of IP address and mask combinations. The DHCP Static Route Option requires a list of pairs of IP addresses. For both options the length must be 8 bytes or multiples of 8 bytes. Neither of these options are configurable.

Using comma with network name (Q00532630)

Do not use comma in network names. If you create a new network that has a comma in its name, you get an error message when you add new subnet and the network name is not saved in the network list.

Misleading branch office information (Q00461065-01)

Branch office session information can be misleading on the Status > Accounting screen because re-keyed branch office tunnels are displayed as separate entries. RADIUS accounting records are not sent to external servers for branch office connections.

Enabling SNMP MIB through the UI (Q00440453-01)

If you enable the SNMP MIB through the UI and go to the Admin > Snmp screen, it does not show it as enabled. However, the CLI **`show snmp mib`** command shows that it is enabled.

Editing last name for user profile causes errors (Q00435962-01)

When you edit the user profile to change the user's last name, you receive a no entries found error message. This also occurs through the CLI, but no error messages appear. This occurs only if you leave the first name field empty. To workaround this, configure the user first name before changing the last name.

Cannot cancel upgrade in progress (Q00433348-01)

If you click on the Cancel button when an upgrade is in progress, the upgrade process does not cancel and the FTP continues.

Branch office tunnel filters not working properly (Q00418382-02)

Filters for the branch office tunnel do not work unless you bring up all of the interface filters and modify them to add the rules to the tunnel filters.

Incorrect error message for excess rates (Q00289581-02)

When you change the excess rate in group connectivity to a value that is less than the committed rate value the "Error with 0: Excess rate must be greater than or equal to committed rate" error message is displayed. The message should say: "Excess rate must me greater than or equal to committed rate."

Serial console issues with system reset menu options (Q00284339-02)

For the recovery image, the Normal or Safe text string for the current mode is missing "System Reset Menu Options. System is currently in mode."

File retrieval counter increments FTP failure attempts (Q00250467-01)

When you upgrade the Contivity from an older version, a popup window tells you how many files have been transferred. However, if the retrieval is failing, the FTP tries three times to get a file until it quits and the counter in this window is counting these FTP attempts as actual files being transferred when they are not, which can be misleading.

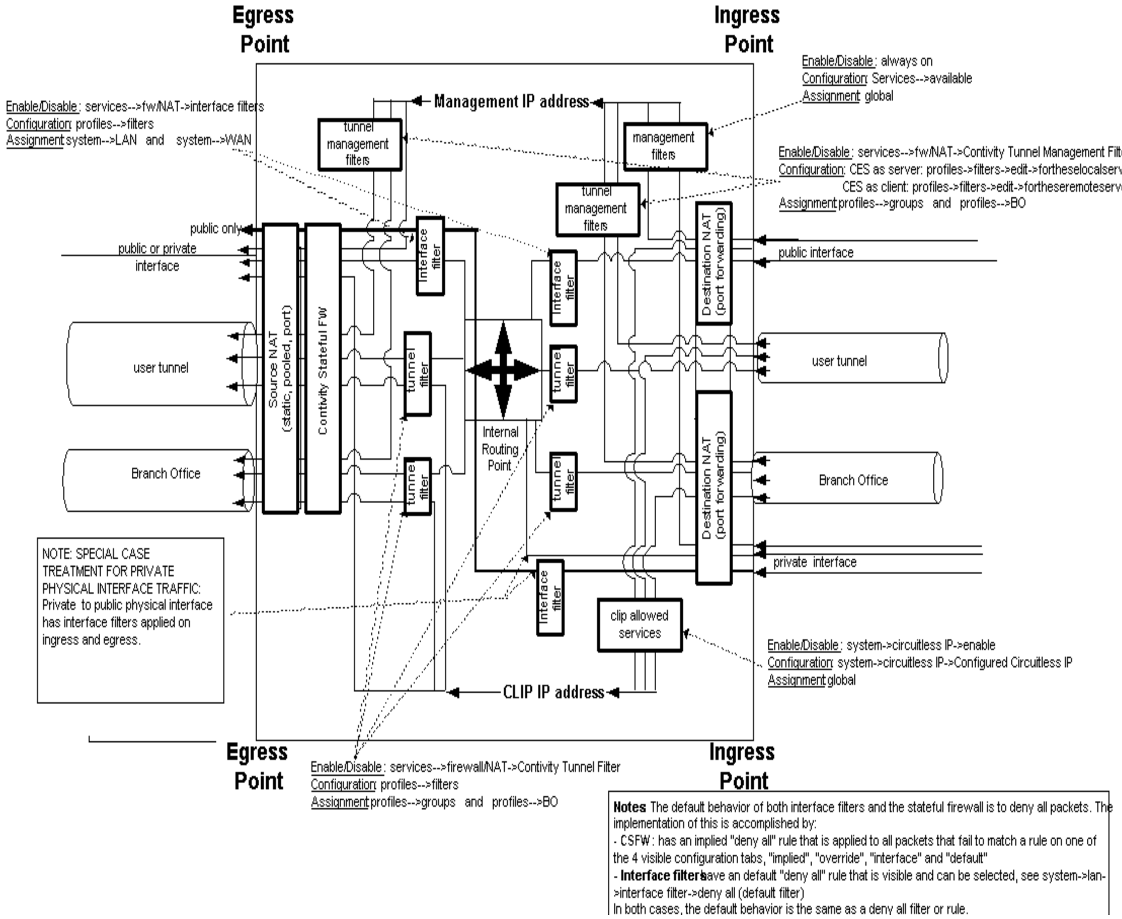
Setting LDAP to an unreachable external server (Q00155644-02)

If you set LDAP to an external server that is unreachable through either the UI or CLI, LDAP hangs and takes several minutes to time-out.

Appendix A
Firewall and Filters Example

Figure 1 shows the interaction between the Contivity Stateful Firewall and Contivity filters.

Figure 1 Sample firewall and filters configuration



Enable/Disable: always on
Configuration: Services-->available
Assignment: global

Enable/Disable: services-->fw/NAT->interface filters
Configuration: profiles-->filters
Assignment: system-->LAN and system-->WAN

Enable/Disable: services-->fw/NAT->Contivity Tunnel Management Filter
Configuration: CES as server: profiles->filters->edit->fortheselocalservices
CES as client: profiles->filters->edit->fortheseremoteservers
Assignment: profiles-->groups and profiles-->BO

NOTE: SPECIAL CASE TREATMENT FOR PRIVATE PHYSICAL INTERFACE TRAFFIC: Private to public physical interface has interface filters applied on ingress and egress.

Enable/Disable: system->circuitless IP->enable
Configuration: system->circuitless IP->Configured Circuitless IP
Assignment: global

Enable/Disable: services-->firewall/NAT->Contivity Tunnel Filter
Configuration: profiles-->filters
Assignment: profiles-->groups and profiles-->BO

Notes The default behavior of both interface filters and the stateful firewall is to deny all packets. The implementation of this is accomplished by:
- CSFW: has an implied "deny all" rule that is applied to all packets that fail to match a rule on one of the 4 visible configuration tabs, "implied", "override", "interface" and "default"
- **Interface filters** have an default "deny all" rule that is visible and can be selected, see system->lan->interface filter->deny all (default filter)
In both cases, the default behavior is the same as a deny all filter or rule.

In this figure, all traffic is shown as ingressing from the right side on one of four possible types of interfaces:

- User tunnel
- Branch office tunnel
- Private interface
- Public interface

After ingressing, the packet passes through the applicable services and then proceeds on to either the internal routing point or is terminated at an interface IP address, management IP address, or CLIP IP address.

All traffic egress points are shown as moving to the left, out the same four types of interfaces as the ingress point.