Version 5.00

Part No. 315000-G Rev 01
August 2004

600 Technology Park Drive
Billerica, MA 01821-4130

Contivity Secure IP Services Gateway Release Notes

NORTEL NETWORKS™

Copyright © 2004 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, Netscape Communicator, Netscape Directory Server, and 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 5.00.

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 work arounds.
- *Configuring Basic Features for the Contivity Secure IP Services Gateway* introduces the product and provides information about initial setup and configuration.
- *Configuring SSL VPN Services on the Contivity Secure IP Services Gateway* provides instructions for configuring services on the SSL VPN Module 1000, including authentication, networks, user groups, and portal links.
- *Configuring Servers, Authentication, and Certificates for the Contivity Secure IP Services Gateway* provides instructions for configuring authentication services and digital certificates.
- *Configuring Firewalls, Filters, NAT, and QoS for the Contivity Secure IP Services Gateway* provides instructions for configuring the Contivity Stateful Firewall and Contivity interface and tunnel filters.
- *Configuring Advanced Features for the Contivity Secure IP Services Gateway* provides instructions for configuring advanced LAN and WAN settings, PPP, frame relay, PPPoE, ADSL and ATM, T1CSU/DSU, dial services and BIS, DLSw, IPX, and SSL VPN.
- *Configuring Tunneling Protocols for the Contivity Secure IP Services Gateway* configuration information for the tunneling protocols IPsec, L2TP, PPTP, and L2F.
- *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.

- *Configuring the Contivity VPN Client* provides information for setting up client software for the Contivity gateway.
- *Configuring TunnelGuard for the Contivity Secure IP Services Gateway* provides information about configuring and using the TunnelGuard feature.

Hard-copy technical manuals

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.

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

These release contain the latest information about the Contivity Secure IP Services Gateway Version 5.00.

Refer to your Contivity hardware installation guide for instructions on getting your Contivity 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.

To obtain on-line help for the Contivity 1010, 1050, or 1100, enter the location of the help files on the CD or on a server.

Version 5.00 feature summary

Version 5.00 of the Contivity gateway provides support for the following:

- SSL VPN integration

  The SSL VPN Module 1000 provides full-featured SSL VPN capability to the Contivity gateway. It provides a unified solution for IPsec and remote access SSL VPN. It can configure and manage both IPsec and SSL remote access accounts through one GUI; integrated user accessibility is through a unified remote access portal. The SSL VPN Module 1000 can be installed on the 1740, 2700, and 5000.

- Contivity IPsec mobility

  IPsec mobility allows IPsec connections to be maintained for mobile users, allowing them to roam from subnet to subnet without losing the VPN tunnel connection.

- Persistent Contivity VPN Client tunnels

  Persistent tunneling provides a continuous connection. After successfully establishing a tunnel session to the Contivity gateway, the Contivity VPN Client makes every attempt to maintain a viable VPN connection without additional user intervention.

- Inverse split tunneling

  Inverse split tunneling provides the ability to specify networks that are allowed access outside of a mandatory tunnel. You can also allow only locally connected subnets to be accessed.

- Data Link Switching (DLSw)

  DLSw provides support for IBM SNA protocol networking in IP networks. This feature includes DLSw IP encapsulation and session-oriented IP networking. It also includes support for SDLC and LLC2 interfaces for integration of native SNA traffic. It provides the ability to deploy the Contivity gateway to support future application migration from SNA to IP in a secure environment.

- Quad T1/E1 support

  The quad T1/E1 interface card is basically a four-port version of the current single-port T1/E1 card supported on the Contivity gateway. The quad T1/E1 card supports 4 RJ48C for direct connection to T1 or E1 services. The following is an overview of the T1/E1 parameters supported on the card; this is not an all inclusive list.

  — Line formats - T1 and E1, impedance is set to 100 Ohms for T1 and 120 Ohms for E1

  — Line Coding - AMI (T1), B8ZS (T1), HDB3 (E1)

  — Line framing - T1 SF, T1 ESF, E1 unframed

  — CRC-4

  The Quad T1/E1 card is supported on the Contivity 1700, 1740, 2600, 2700, 4600, and 5000. The Contivity 1700 supports one T1/E1 card, while the other supported platforms can support up to 3 cards per system. There is an RJ48C to coax balun available for E1 applications. For further information on the quad T1/E1 card, see the appropriate installation guide for your Contivity gateway and the *Configuring Advanced Features for the Contivity Secure IP Services Gateway* book.

- E1 support for existing T1 I/O card

  Nortel Networks now offers a single-port T1/E1 CSU/DSU WAN interface card. The new T1/E1 CSU/DSU WAN interface card is a half-height card, but in other respects it resembles the older single-port T1 CSU/DSU WAN interface card. To support E1 capability, you must install this new card and upgrade the Contivity software to Version 5.0. The E1 capabilities on the single-port T1/E1 CSU/DSU WAN interface are identical to those of the Quad T1/E1 card.

- 56/64K CSU/DSU-DDS

  Nortel Networks supports direct connection to Digital Data Service (DDS) with 56/64K DDS interface with an integrated CSU/DSU. This is Data Rate selectable (56 kb/s / 64 kb/s) and supports PPP and frame relay protocols over 56/64K DDS leased lines.

In addition, Version 5.00 offers the following enhancements:

- CRL distribution points

  CRL distribution points (CDP) allow users to authenticate against only the CRL that is specified in the certificate CDP. This feature provides faster tunnel establishment.

- CA key update

  CA key updates (link certificates) provide uninterrupted certificate authenticated user and branch office tunnel connections before, during, and after the Entrust Key Update function is performed by the CA.

- LDAP special characters

  This enhancement allows certificate subject DNs to be created that include special characters, such as a comma, in compliance with RFC 2253.

- Dynamic password

  Currently two types of administrative users exist: one super-user (ADMIN) and as many as needed “users granted administrative privileges” (also known as administrative users). Dynamic password support via an external RADIUS server is now available for the administrative users.

- External LDAP proxy enhancement

  This enhancement allows a more flexible method to locate a user record when using LDAP proxy by supporting the mapping of the following certificate subject DN attributes to defined LDAP attributes:

  — User cert Common Name attribute
  — User cert e-mail address attribute
  — User cert serial number attribute
  — User cert UID attribute
  — Subject Alternative Name attribute

- Vendor-specific RADIUS attribute

  Allows Contivity gateway group membership information to be stored in a RADIUS vendor-specific attribute in addition to the class attribute.

- Upgrade OpenSSL 9.7c ' 9.7d

  This enhancement addresses a security vulnerability: CAN-2004-0079, whereby a remote attacker could perform a carefully crafted SSL/TLS handshake against a server that used the OpenSSL library in such a way as to cause OpenSSL to crash.

- Certificate CLI renewal
- Export/import CA and server certificate private key

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

This chapter describes issues and considerations that apply to the Version 5.00_133 release of the Contivity Secure IP Services Gateway.

Customer issues fixed in this release

Table 1 lists customer issues from previous releases that are fixed in this release. This includes all fixed issues from V04_85.160 with the exception of Q00738300 and Q00921504.

Table 1 Fixed customer issues

Q00498780-01	Serial interface IP address does not match with documentation
Q00750188-01	MIBs show incorrect number of user tunnels
Q00780371	Cannot setup ABOT(Initiator or responder)+Control tunnel through CLI
Q00818455	SNMP hrProcessorLoad always returns value of 0
Q00826346	Intrusion detection trap sent for multicast packets
Q00864795	Connection name field to configure BO policies not case sensitive
Q00887476-01	Built-in Gig interface, 0/2, shows down when really up
Q00892612	Tunnel Guard recheck failure over dial-up
Q00911422	Latency/RX Overrun Errors
Q00912853-01	Show Running Config fails if AR license installed and V.90 specifies local IP
Q00919183	Static routes not redistributed into RIP without firewall enabled
Q00926793	Context Sensitive Help incorrectly implies there is a “None” option

Version 5.00 product considerations

The following sections describe consideration for the Version 5.00 features.

Slot requirements for SSL VPN Module 1000 PCI card

Slot installation requirements for the SSL VPN Module 1000 PCI card for the Contivity 1740/2700:

- slot 1: SSL
- slot 2: any low-profile/half-height card (e.g. 10/100-TX)
- slot 3: any card
- slot 4: any card

Slot installation requirements for the SSL VPN Module 1000 PCI card for the Contivity 5000:

- slot 1: SSL
- slot 2: GigE (secondary)
- slots 3-5: Hardware Accelerator/CSA or any other cards
- slot 6: or Hardware Accelerator/CSA GigE (primary)

Note the following:

- The V.90 modem card cannot be installed in slot 2 when an SSL card is in slot 1 because there is too much mechanical interference. All other released cards will physically fit in slot 2.
- The Contivity 5000 with just one power supply installed is capable of supporting maximum I/O configurations such as one SSL, one Hardware Accelerator/CSA, two HSSI, and two GigE cards.
- On the Contivity 1740 and the Contivity 2700:
  - Only one Hardware Accelerator/CSA card is allowed per chassis. You can install a second Hardware Accelerator/CSA card if there are no GigE or HSSI cards in the chassis.
  - Only one GigE card per chassis. You can install a second GigE card if there are no Hardware Accelerator/CSA or HSSI cards in the chassis.
  - Only one HSSI card per chassis.

General SSL VPN considerations

The following list explains SSL VPN considerations.

- Java Runtime Environment 1.4.2_04 must be installed in order to manage the SSL VPN and the Contivity Stateful Inspection Firewall UI. The JRE 1.4.2_04 is distributed with the Contivity Secure IP Services Gateway image; it can also be downloaded from Sun Microsystems, Inc.
- Native Outlook 2003 is not supported.
- Netdrive Mapping is not supported on Windows XP or Windows 98 clients.
- SSL VPN user browser considerations include:
  - Windows

    IE 5.5 or better with Sun's JDK 1.3/4 or better

    IE 5.5 or better with Microsoft JVM 4 or better

    Netscape 7 with Sun's JDK 1.3/4 or better

    Mozilla 1.3 or better with Sun's JDK 1.3/4 or better
  - Linux

    Netscape 7 with Sun's JDK 1.3/4 or better

    Mozilla 1.3 or better with Sun's JDK 1.3/4 or better
- Managing the Contivity gateway over an SSL VPN created with a “Browse Intranet” link does not work and is not supported. You will have problems with all of the java applets, including the one that draws the left hand side menu tree. To successfully manage the Contivity gateway via an SSL VPN, you must start two port forwarders:

  1. On the SSL VPN portal, go to the Advanced > Port Forwarder tab.

  2. Start the following two forwarders:

Mode	Source IP	port	alias	Dest host	port
TCP	127.0.0.1	80	(leave blank)	CES-mgmt	80
TCP	127.0.0.1	22	(leave blank)	ASA-mgmt	22

  The second port forwarder must talk directly to the SSL-VPN management address, not the Contivity gateway management address.

  3. Start your browser and point it to http://127.0.0.1.

All the Java applets, including the ssl-vpn manager, will now function.

If your PC is not running a Web server or an SSL server, the port forwarder will fail with a “port in use” error.

For information on using the backup and restore features of the SSL VPN Module 1000, refer to the SSL VPN management interface on-line Help.

DLSw

The following list explains DLSw considerations.

- You cannot create a second DLSw circuit between the same local MAC/SAP pair and the same remote MAC (with another SAP) for Contivity to BayRS or Contivity to Cisco peering. You can create such a circuit between two Contivity gateways.
- When the Contivity gateway connects to an already defined remote BayRS (with unconfigured peer support activated or Contivity gateway defined earlier as peer in BayRS, but the previous connections were unsuccessful), the connection is established. However, in BayRS the peer is seen as Version 2.0 unicast and not RFC2166. This is correct because the Contivity gateway does not support UDP multicast and Multicast Vector is missing from Capability Exchange message.
- After a Version 2.0 unicast connection between the Contivity gateway and BayRS Version 2.0 unicast enters quescing state and there is a delay in DLSw circuit establishment from the BayRS side. This occurs because BayRS sends UDP multicast packets several times and then restores the TCP connection towards the remote Contivity gateway.
- After a V2.0 unicast connection between a Contivity gateway and BayRS, Version 2.0 unicast enters in quescing state. The connection when DLSw circuits are made from the BayRS side will be V1 (RFC1795). This is because BayRS tries to connect first on V1 sockets and not on V2 sockets as the Contivity gateway does.

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)

Dual V.35 WAN interface card software support

Version 5.00 is the last release of Contivity software that will run on the dual V.35 WAN interface card. (This option card is no longer available for purchase.) Future versions of Contivity software will not work on the dual V.35 WAN interface card.

Version 5.00 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.

Q00825683-01 - Intermittent issues with graphics on Stateful FW/NAT Java GUI

On occasion when the java/firewall-nat policy window is opened, the graphics appear distorted. To correct the problem, stop and re-start the GUI.

Q00886119 - Client error when using persistence and roaming

Occasionally, when the client is in persistence mode and connectivity is re-established, an “Unable to Initiate Packet” error will occur. If this occurs, exit the client and re-start it.

Q00893277 - External profile LDAP consideration

When using external LDAP as a profile server (Servers > LDAP), be sure that the listening port of the LDAP server is correctly configured. If the LDAP server is listening on a different port than the configured port, the Contivity gateway will not be manageable until all attempts to connect to that server have timed out.

Q00899986 - Unable to delete old version of SSL VPN Module from applet

Only unpacked versions can be deleted. You can delete an old version that is stored on the card by uploading a new version.

Q00902015 - Using Internet Explorer to schedule shutdowns

When using IE browsers, selecting the “safe mode” boot option will result in an erroneous message being displayed. It can be safely ignored.

Q00903018 - FWUA special character not allowed

The Contivity gateway permits a user name and password for FWUA that contains special characters. However if you use an open-parenthesis “(“character, you will not be able to login using FWUA.

Q00904181 - Static text on a link page using macros displays improperly

When extracting information to put on a portal page using one of the built-in macros, embedded spaces are incorrectly displayed as %20. For example, if your Windows Domain is named TEST DOMAIN, your portal is configured with this domain name, and you then create Static Text on the Link Page (Link Text in General tab on Portal configuration page), your static text (calls the <domain> macro) is Domain Name = <domain>. The portal page shows the text as Domain Name = TEST%20DOMAIN.

Q00906500 - Using LDIF files to restore configurations

Nortel Networks recommends that you do not try to restore a Contivity gateway configuration using an LDIF file that was generated by a Contivity server version higher than the current version.

Q00909485 - Using copy and paste functionality in the SSL VPN Manager

Copy and paste options are currently not available in the “Edit” menu; however, the equivalent keyboard shortcuts of ctrl+X,+C,+V work for cut, copy, and paste, respectively.

Q00911301 - Changing WAN protocol and line format causes configuration errors

Changing line format and interface protocol simultaneously on LMC1200 may create configuration errors.

Q00921243 - LMC1000 missing receiving byte from AS400

When beginning and ending flags share a zero as with the AS400, under some circumstances the AS400 fails to respond to RR polls and fails SDLC communication. The new PROM revision number is 4903 A8.

Q00923269 - DLSw fails to properly control RTS/CTS on SDLC

An error in Contivity DLSw SDLC processing creates issues in certain multidrop configurations where RTS/CTS signaling is required. To work around this, configure the devices as Duplex: *FULL*. This sets “constant carrier” and the peer device will not do RTS/CTS signaling.

Q00926857 - Domain quick wizard for large numbers of groups

When there are more than 1000 Contivity groups configured on a Contivity gateway and the domain quick wizard is used to mirror the Contivity groups, the wizard may take half an hour or more to complete.

Q00926934 - Domain quick wizard fails with more than 1023 groups

You cannot define more than 1023 groups. If you define more than 1023 groups, not all the groups are going to be copied.

Q00930221 - No response after changing safe mode duration

If you set the Safe Mode Duration to an other value on the System > Settings screen and then go to the Admin > Configs page and create a safe mode configuration, the Contivity gateway doesn't respond using GUI or Serial connection.You must restart the Contivity gateway from the reset switch. If you do not create the Safe Mode Configuration immediately after setting the Safe Mode Duration, the process works correctly.

Q00930299 - Unable to import certificates presented as a single line

The SSL VPN module cannot import certificates that are presented as a single line.You can manually insert a line-feed to solve this problem.

Q00936545 - Default private route exists after WAN interface change to public

A display error in the “routing > static routes” page results in the private default route still showing up after a WAN interface has been changed from private to public. This error is a display error only, the route table is correct.

Q00937962 - Using frame relay in direct (back to back) mode

Health check will erroneously report that the circuit is down because there is no LMI when direct mode is used. This error message can be ignored.

Q00937978 - Incorrect status displayed after LDAP backup

An incorrect status of “stopped” is displays after an LDAP backup has been completed and the “LDAP Server will auto restart upon completion of Backup” option has been selected. To see the correct status of the LDAP server, refresh the screen.

Q00944885-01 - Disable/enable remote V.35 requires disable/enable local WAN

When disabling and then re-enabling a remote V.35 interface, UDP port 500 does not reinitialize. If it does not reinitialize, the port cannot be used for tunneling. To

correct the problem, you must disable and enable the local WAN port from the GUI screen on the 4500. This issue applies only to dual V.35.

Q00948717 - Go to links page first to update links

When you go to the Add page and the device is rediscovered, it does not obtain the links or ensure that you cannot choose an already configured link. If you enter new information, the existing information at that index location is overwritten.

Q00950213 - Frame relay VC status incorrectly reported

Third-party SNMP tools will have incorrect virtual circuit status on frame relay circuits that are down.

Q00950717 - Outlook server name field requires FQDN

When you create a portal link of type “outlook,” you must use a fully qualified domain name in the Server Name field.

Q00954241 - Refresh button does not update contents

If you start editing a text field and you continue editing while you press refresh (you did not move focus to another field), the field content is not overwritten with the newly refreshed value. All other fields on the page are refreshed properly. To work around this issue, click on any other field before clicking refresh button or use the per-parameter refresh by right clicking on the status icon.

General Contivity gateway considerations

The following sections contain general considerations for this product.

Upgrade procedure considerations

- The Contivity 1010, 1050, and 1100 require a 64 Mb flash disk.
- Version 5.00 supports upgrades from Versions 4.70, 4,80, and 4.90. If you are running an older version, you may have to upgrade to a later version before you upgrade to Version 5.00.
- 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.
- 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 5.00 software, you create a recovery floppy diskette as soon as you complete the upgrade. You must use a formatted diskette when creating the recovery diskette.
- 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.
- 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.

- 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.

Viewing and calculating memory usage

The minimum memory requirement for Version 5.00 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 5.00. Contact your Nortel Networks sales representative if your configuration requires additional memory. The Memory Calculator tool is available at:

www.nortelnetworks.com/documentation

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

Software and hardware compatibility

The minimum Contivity VPN Client version that is supported by Version 5.00 is 4.65.

Table 2 shows Contivity Secure IP Services hardware and software compatibility. An X in the table indicates which platforms support this version of the Contivity gateway software.

Note: The SSL VPN Module 1000 can be installed only in the Contivity 1740, 2700, and 5000 platforms.

Table 2 Hardware platform and server software compatibility

Hardware platform	4.76 5/03	4.80 8/03	4.90 05/04	5.00 08/04
1010	X	X	X	X
1050	X	X	X	X
1100	X	X	X	X
600	X	X	X	X
1500				
1510				
1600	X	X	X	X
1700	X	X	X	X
1740		X	X	X

Table 2 Hardware platform and server software compatibility (continued)

Hardware platform	4.76 5/03	4.80 8/03	4.90 05/04	5.00 08/04
2000				
2500				
2600	X	X	X	X
2700	X	X	X	X
4000				
4500	X	X	X	X
4600	X	X	X	X
5000	X	X	X	X

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.

General support considerations

General support considerations include the following:

- The output generated by the CLI command show running-config (SRC) does not always produce usable scripts that can be applied directly to provision a Contivity gateway. This applies both to the use of SRC within an affected software version and across versions. You should not use the output from SRC

without inspection and if necessary, editing and reordering the output to provision a Contivity gateway. For further information about SRC, see Reference for the Contivity Secure IP Services Gateway Command Line Interface.

- GigE fiber and copper cards will not fit into the connector on slot 4 on the Contivity 4600.
- If more than approximately 10 CMP enrollments occur at the same time, the administrative functions of the Contivity gateway (GUI/CLI) may be non-responsive for short periods of time.
- Shasta Server Farm is not supported by Version 5.00.
- 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.
- 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.
- 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.
- 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 or later Java GUI. You will see an (old format) text message to alert you to the change. The Version 4.70 policies are translated, but 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

- When you upgrade to Version 4.80 or later, 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
- 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.
- 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

Contivity gateway admin browser considerations

The following considerations pertain to admin users:

- 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.
- Java Runtime Environment 1.4.2_04 must be installed in order to manage the SSL VPN and the Contivity Stateful Inspection Firewall UI. The JRE 1.4.2_04 is distributed with the Contivity Secure IP Services Gateway image; it can also be downloaded from Sun Microsystems, Inc.
- A Microsoft issue in Internet Explorer 6.0 SP1 creates problems when attempting to launch the SSL VPN Manager over HTTPS. Internet Explorer SP2 corrects this issue.
- The off-line help stored on local computer cannot be accessed from the links in the help page due to security constraints which are implemented in Netscape 4.1 or higher and Internet Explorer 6.0 SP1 which have hotfixes. regarding this issue. (Q00818628) There are two workarounds;
    - — Add the site to the trusted zone of IE
    - — Add machine name to the URL

- 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.
- When using HTTPS to secure administrator access to the Contivity gateway, Netscape Communicator and Internet Explorer perform various and differing security checks. The following configuration is recommended to obtain the best performance when administering the Contivity gateway securely using Admin SSL.
  - Make an entry in the hosts file corresponding to your Contivity management IP address.
  - Import the root certificate that issued your Contivity server certificate into your browser store.
  - 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.
- Using Internet Explorer Version 6.0.2800.1106IC on Windows NT 4.0, the GUI presents inconsistent information in firewall java section.
- If you launch two Java applets from one Web GUI session on the same PC, it can cause inconsistencies with firewall policy rules.

The following considerations pertain to SSL VPN end users:

- To support the Telnet/SSH Access, HTTP Proxy and Port forwarder features, the following browser and Java combinations are recommended:

  Windows:

  - Internet Explorer 5 or better with Sun’s JRE 1.3 or better
  - Internet Explorer 5 or better with Microsoft’s JVM 4 or better
  - Netscape Navigator 7 with Sun’s JRE 1.3 or better
  - Mozilla 1.3 or better with Sun’s JRE 1.3 or better

*nix:

— Netscape Navigator 7 with Sun's JRE 1.3 or better

— Mozilla 1.3 or better with Sun's JRE 1.3 or better

Configuration via the Browser-Based Management Interface is supported when the following browsers are used:

Windows:

— Internet Explorer 5.5 or better

— Netscape Navigator 7.1 or better

— Mozilla 1.5 or better

*nix:

— Netscape Navigator 7.1 or better

— Mozilla 1.5 or better

- 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.

Tunnel considerations

- 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.
- For nailed-up connections, the IPSec SA may go down due to inactivity. Only the ISAKMP SA stays up all of the time.
- 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
- The following tunnel licensing options are available for the SSL VPN Module 1000:
  - Alteon SSL VPN Software license – 50 users
  - Alteon SSL VPN Software license – 100 users
  - Alteon SSL VPN Software license – 250 users
  - Alteon SSL VPN Software license – 500 users
  - Alteon SSL VPN Software license – 1000 users
- 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, 1740	500	Yes
2700	2000	Yes
4600	5000	No
5000	5000	No

Certificate considerations

VeriSign certificates use a unique e-mail identifier that is different from Microsoft and Entrust so you must use the full subject distinguished name when configuring branch office connections authenticated using certificates.

- The output of the certificate export must contain a blank line after the password hash information for the certificate to import successfully.
- 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.

Documentation considerations

The following documentation issues will be fixed in future versions of the documentation.

- CLI command reference needs clarification when exiting Global Configuration Mode. Not all configuration changes made through the CLI take effect immediately. The commands that do not take effect immediately will be deferred until a terminator command is encountered. However, there are two ways to enter a terminator command:
  - The normal terminator is the EXIT or END command to accept and execute all deferred commands.
  - The abort termination (Ctrl-Z or <end-of-file>) discards and does not execute any deferred commands.
- When configuring a critical interface or interface groups for critical interface failover (CIF), the interfaces cannot have VRRP configured on them. If you include an interface that is running VRRP as a critical interface or part of an interface group (for CIF), it is an unsupported configuration. Where VRRP is configured on the interface, there is already a failover/availability solution provided in case of loss of that interface.