Version 6.00

Part No. 315000-K Rev 00
December 2005

600 Technology Park Drive
Billerica, MA 01821-4130

Contivity Secure IP Services Gateway Release Notes

NORTEL

Copyright © 2005 Nortel Networks. All rights reserved.

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 VPN Router Version 6.00.310, formerly known as the Contivity Secure IP Services Gateway.

Before you begin

These release notes are intended for network managers who are responsible for the Nortel VPN Router. 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 Nortel VPN Router, 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 Demand Services, DLSw, IPX, and SSL VPN.
- *Configuring Tunneling Protocols for the Contivity Secure IP Services Gateway* provides configuration information for the tunneling protocols IPsec, L2TP, PPTP, and L2F.
- *Configuring Routing for the Contivity Secure IP Services Gateway* provides instructions for configuring BGP, RIP, OSPF, and VRRP, as well as instructions for configuring ECMP, routing policy services, and client address redistribution (CAR).
- *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. This book also provides troubleshooting information and interoperability 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.nortel.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

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

Getting Help from the Nortel Web site

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

http://www.nortel.com/support

This site enables customers to:

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

Getting Help over the phone from a Nortel Solutions Center

If you have a Nortel support contract and cannot find the information you require on the Nortel Support Web site, you can get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the Web site below and look up the phone number that applies in your region:

http://www.nortel.com/callus

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

http://www.nortel.com/erc

Getting Help through a Nortel distributor or reseller

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

Chapter 1
Overview

These release notes contain the latest information about the Contivity Secure IP Services Gateway Version 5.07 and 6.00.

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 online help for the Contivity 1010, 1050, or 1100, enter the location of the help files on the CD or on a server.

This release will become the default version of VPN Router software loaded in the factory. Note that the CD-ROM included with the VPN Router from the factory may contain an earlier release of software, so customers are advised to back up the 6_00.310 in case the image must be restored. Refer to Managing and Troubleshooting the Contivity IP Services Gateway (part number 315900-D, Rev 00) for information on backing up the system.

Version 6.00 features

Version 6.00 of the Contivity gateway provides support for the following:

- 256 bit AES for branch tunnels

  AES uses a block size of 128 bits and key sizes of 128, 192 or 256 bits. The three types of AES based on the key size are: AES-128, AES-192, and AES-256. The Contivity Extranet Switch has supported AES-128 for Branch Office tunnels since the V04_50 release. This feature adds AES-256 for Branch Office Tunnels.

- Multinetting

IP multinetting allows a maximum of eight addresses to be configured on a single Ethernet interface. The first IP address configured on the interface is the primary address. Subsequent IP addresses are secondary addresses, or subnets. All of the subnets on a physical interface share the security rules configured for the primary subnet. You can configure only one set of Interface Filter rules per physical interface.

- Demand Services

  Demand services brings up a backup interface based on a trigger, such as traffic, interface group, hour, unreachable route, or ping. Demand services has two sets of functionality: Backup Interfaces, formerly known as BIS, and Dial on Demand (DoD). Backup interfaces provides an automated mechanism to enable a backup interface when a designated primary connection fails. DoD activates the dial interface when traffic must be routed over a dial interface route and then deactivates the dial interface when there is no traffic to be routed.

- Framed E1

  There are two choices for E1 line framing: framed E1 and unframed E1. Framed E1 permits fractional E1 services and supports 30 or 31 DS0 channels. Unframed E1 permits the maximum E1 user bandwidth of 32 DS0 channels.

- Border Gateway Protocol 4

  Border Gateway Protocol (BGP) is a path vector protocol used to carry routing information between Autonomous Systems (AS). BGP imposes no restrictions on the underlying network topology. It assumes that routing within an AS is done through an intra-AS routing protocol. BGP considers the entire Internet as a graph of ASs, with each AS identified by a unique autonomous number. Connections between ASs together form a path, and the collection of path information forms a route to reach a specific destination. BGP uses the path information associated with a given destination to ensure loop-free interdomain routing.

  BGP-4 provides a new set of mechanisms for supporting classless interdomain routing. These mechanisms include support for advertising an IP prefix and eliminate the concept of network **class** within BGP. BGP-4 also introduces mechanisms that allow aggregation of routes, including aggregation of AS paths.

- Cone NAT

NAT translates IP addresses and port numbers in private address ranges into public addresses when traffic traverses between private and public networks. The IP endpoints in a VoIP network (IP Phones, Soft Clients) are typically assigned private addresses to hide their identity from the public network. Voice calls from and to the public network must reach endpoints in the private network and, as a result, network address translation is required to allow proper routing of media to endpoints with private addresses.

VoIP protocols introduce a number of complexities for NAT, because they carry IP address and port information within the body of the message that is not accessible to NAT. NAT cannot conduct translation on private IP addresses within the payload of application layer messages. Therefore, the voice media, which is directed to the private IP address identified in the signaling message, cannot be routed to the private address, which results in a one-way speech path.

Two of the most common solutions that have been proposed to fix the NAT traversal issue are:

— Application Level Gateways (ALG)

— Address/port discovery

Cone NAT focuses on the address/port discovery mechanisms for VoIP.

- NAT SIP ALG

  Traditional NATs do not translate Layer 5 addresses. Therefore, the VoIP signaling and Real Time Transport Protocol/Real Time Transport Control Protocol (RTP/RTCP) become unreachable after NAT translation (one-way signaling and audio), due to the embedded IP address and port specified within the IP payload. ALG is one of the solutions to correct the NAT traversal issue.

  The ALG inspects every SIP packet, performs the necessary translation of the IP addresses embedded in the SIP messages, and updates the SIP message before sending the packet out.

- FW SIP ALG

  Firewalls, by default, do not have the intelligence to identify port numbers within the payload of signaling protocols and cannot dynamically open ports for media traversal, resulting in blocking of voice traffic. Firewalls are designed to operate with layer 3/layer 4 information and cannot access information in higher layer protocols.

The SIP ALG performs the necessary translation of the IP addresses embedded in the SIP messages and updates the SDP information. The Firewall ALG examines the SDP information, identifies the RTP port number for the call, and opens the port in the firewall during call setup. The Firewall ALG also raises a flag to indicate that NAT must perform an application level translation. The ALG then performs the address/port mapping and state setup to ensure that the data channels are mapped according to the information in the SDP. The ALG closes the port after call termination. This provides a mechanism to dynamically open and close ports in the firewall, and increases network security by restricting the voice traffic to active sessions only.

- NAT Hairpinning

  Contivity NAT blocks packets coming from the private side of the NAT that are destined to an endpoint on the private side for which a NAT binding to a specific port already exists. This does not allow peer-to-peer communication between two endpoints behind the same NAT if they try to use their public address. NAT Hairpinning corrects that problem by allowing two endpoints on the internal side of the NAT to communicate, even if they use each other's external IP addresses and ports.

- Frame Relay

  Frame Relay Forwarding Priority to a virtual circuit provides an interface-level priority queuing scheme in which prioritization is based on destination permanent virtual circuit (PVC) rather than packet contents. FR Forwarding Priority to a VC allows you to configure a PVC transporting voice traffic to have absolute priority over a PVC transporting signaling traffic, and a PVC transporting signaling traffic to have absolute priority over a PVC transporting data. You assign priority to a PVC within a Frame Relay map class. All PVCs using or inheriting that map class are classed according to the configured priority.

- FRF.12

  Frame Relay Forwarding Priority to a VC works with or without FRF.12. The interface-level priority forwarding takes the place of the FIFO queuing or dual FIFO queuing normally used by FRF.12.

  PVC priority assigned within FR Forwarding Priority to a VC takes precedence over FRF.12 priority, which means that all packets destined for the same PVC are queued on the same interface queue regardless of whether they are fragmented.

FRF.12 defines Frame Relay extensions that fragments the packets within a VC. FRF.12 fragmentation allows high-priority packets of one VC to be sent (interleaved) between fragments of lower priorities of the same VC or other VCs.

The FRF.12 fragmentation is implemented within Frame Relay stack, and the associated interleaving is implemented within QoS queues in T1 T3 contexts. Interleaving uses two classes of packets, voice and non-voice, and no reordering of packets occur within either class.

- 802.1Q Phase 2

  The following implementations are made for 802.1Q:

  — Configurable mapping for 802.1p tag to DSCP—changes made to the GUI enable custom mapping with precedence.

  — VRRP support per VLAN interface—changes made to the Routing Interfaces GUI allow you to configure VRRP on VLAN, such as enabling VRRP backups.

  — Stateful firewall and FWUA policies per VLAN—changes made in the Firewall *Interface Specific Rules* tab GUI enable users to select a Source and Destination configurable subinterface. This feature resembles the current selection method for user and branch office tunnels.

  — ABOT Initiator tunnel per VLAN interface—Asymmetric Branch Office Tunnels (ABOT) is supported as a service on VLAN on the Branch Office GUI. The Virtual circuit appears as an IP address in the End Points menu.

- Management virtual address

  The Management virtual address (MVA) is a unique CLIP address that is used only for management and is separate from other CLIP addresses. Using a CLIP address ensures that no dependency occurs on any particular physical interface. This eliminates a single point of failure. As long as a route through an interface to the MVA exists, you can manage the Contivity Gateway. Access to the MVA is supported on a public interface through a VPN tunnel.

The following features from Version 5.07 are included in Version 6.00:

- Event log enhancements

  The event log is a detailed recording of all events that take place on the system. These entries are not necessarily written to disk, as with the system log. The event log retains all system activity in memory, but you must configure the system to save the event log, either automatically or in a specified file.

  The event log includes information on tunneling, security, backups, debugging, hardware, daemon processes, software drivers, and interface card driver events.

- Token authentication through FWUA

  FWUA by SecurID extends the authentication approach of FWUA, which enforces user authentication on traffic between branch office (BO) connections in the VPN environment. This authentication method can also be applied to non-tunneled traffic FWUA, when the CES acts as a router and as a firewall edge device.

- Configurable http and https ports for administrators

  An administrator can change the ports that the http, https, FTP, telnet & SNMP listen on. This is done through the SERVICES->AVAILABLE page.

- LDAP proxy user authentication and password management

  User authentication and password management support the LDAP V3-compliant servers, such as IBM RACF and Netscape/Novell directory server. It uses the LDAP controls within the bind response from the LDAP server combined with the error message within the bind response to find the password status: expired, expiring, or valid password. The Contivity VPN Client can change its password to the proxy server if the password has expired.

- Next hop traffic filters (A.K.A. Policy Based Routing)

  Next hop traffic filters allow customers to control the next hop selection and route traffic within their domain. If a packet matches filter criteria, a forwarding lookup is performed using the configured next hop and is forwarded using that routing table instance. If the lookup fails, then traditional destination-based routing occurs using the routing table.

- Configurable Ethernet interface speed reporting for carrier managed service, MIB reporting only

  A configurable Ethernet interface speed for SNMP queries provides the ability to change the Ethernet interface speed to values other than just 10 Mbps or 100 Mbps. This allows SNMP queries to reflect the actual speed of the interface uplink. If the parameter is not configured, there is no change in the value passed to MIB queries; it is the Ethernet line speed (10 mbps, 100 mbps).

- SNMP support to find expired certificate

  You can specify the number of days (between 7, the default, and 365) before you receive a warning that a certificate is about to expire. The parameter you enter on the System > Certificates screen applies to all certificates.

- Configurable PPP TX ring buffer to reduce jitter

  You can configure a transmit ring size on LMC1000 and LMC1200 interfaces to reduce jitter during VoIP calls.

- Ping to validate public default route

  You can use ping to verify the status of the link from a public interface to its remote endpoint on broadband remote access servers.

- DNS suffix from DHCP server

  When requesting an address from a DHCP server, the DNS, WINS, and Domain Name are also requested. If these options are returned in the packet, the information is stored along with the IP address until needed. When constructing the config mode packet, these DHCP retrieved values are used only if no group settings are specified.

- FQDN registration

  When the Contivity requests an address from a DHCP server, it also requests the domain name attribute. This domain name is passed to the client on connection if the domain name group setting is enabled and left blank. The client uses its own hostname pre-pended to the domain name to register itself through Dynamic DNS. The only change in behavior is that the domain name requested from DHCP may be passed down to the client.

- ABOT (Asynchronous over TCP) for 4800 BPS and 9600 BPS

  Asynchronous data over TCP is a protocol that enables transport of asynchronous data packets over a TCP/IP network. A TCP packet is decapsulated and the data is then forwarded from the synchronous driver to the asynchronous device or host. The asynchronous protocol is used for communication of an alarm device with an alarm host on a slow speed serial line. Unlike synchronous transmission, asynchronous transmission does not use clocking signals to time the data transmission. Instead, asynchronous transmission uses start and stop bits to control the transmission.

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, 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 Version 6.00 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 V5.05_121 release.

Table 1 Software release V5.05_121

CR number	Description
Q00694828-01	The time passed to the client and shown in the client log was not adjusted to GMT.
Q00746625-01	The “crl delete” option was not available in CLI.
Q00778885-02	The wildcard mask entered for the network while in the CLI “router ospf” configuration menu was not saved, resulting in failures during provisioning.
Q00785286-03	Reverse (wildcard) subnet mask was considered non-continuous and therefore disallowed.
Q00809510-01	The abilities to specify public side default DHCP lease time and disallow RFC1918 public leases were added.
Q00828414-01	The Contivity gateway might hang when the file system was full and a “save configuration” procedure was started.
Q00841811-01	CRL retrieval failed over public interfaces for large CRLs due to the former security check when the limit of 70 packets per minute was set and everything above that was dropped.
Q00847926-02	ICMP was not recovering after a routing table change due to the termination of a tunnel.
Q00852275-01	The restricted filter was redefined to allow only client banner during authentication to prevent any possible security breaches.

Table 1 Software release V5.05_121 (continued)

CR number	Description
Q00864753-01	Enhancement. A support for LDAP over SSL on public interfaces was added.
Q00882905-01	Updates to the information displayed in the event log during IPSec tunnel establishment were made.
Q00882926-02	The Contivity did not recognize initial contact payload received from third party VPN vendors.
Q00892573	The GUI statistics for the Frame Relay PVC displayed incorrect count for outbound DE (discard eligible) packets.
Q00900495-02	The "show run" CLI command displayed administrator's password incorrectly.
Q00912336-02	The Contivity file system errors were logged when a file was accessed on an optional hard disk on a diskless box (Bluefin).
Q00914781	Users from a group that had an Access Network Name defined could not HTTP to Contivity gateway.
Q00914821-01	The ABOT tunnel was not establishing when PPPoE dynamic routing information was being updated.
Q00929065-01	The dual CPU Contivity gateway could stop sending ESP traffic due to the code changes implemented with the specific bandwidth metering functionality.
Q00932255-01	New versions of Contivity gateway sent RADIUS authentication requests sequentially (single threaded mode) instead of concurrently (multi threaded mode); thus, until the first user was authenticated, no attempt was made to authenticate other users.
Q00935101-01	The diskless Contivity gateway (Bluefin) allowed configuration of an FTP coredump without entering FTP User ID/Password.
Q00937672-01	The Ping trigger mechanism brought the BIS interface up when source address was a LAN interface and destination route was over a Frame Relay PVC.
Q00942570-01	Contivity was not adjusting the time appropriately with Arizona time zone.
Q00946913-01	A warning was not shown when deleting a main group that contained any subgroups that were configured for certificates authentication and set as a default group.
Q00953190	The Contivity Secure IP Services gateway did not extend its active DHCP lease when configured as a DHCP client.
Q00953824	The Contivity gateway might core when a concurrent management was performed, in particular when several administrators deleted the same object in the same time.
Q00955558	The OSPF LSA external route was not aging out from the LSDB.

Table 1 Software release V5.05_121 (continued)

CR number	Description
Q00956438-02	The ABOT tunnel established two IPSec SAs after initial tunnel was terminated abnormally with Initial Contact Payload enabled on both ends and Initiator was set as Nailed Up.
Q00958566-02	Two different IPSec SAs were created in a nailed up control tunnel scenario when continuous traffic was sent during tunnel reestablishment after the initial tunnel was terminated abnormally.
Q00959911	Dead Peer Detection was not working between the Contivity Entranet Switch and a Cisco Router.
Q00960592-02	The Tunnelguard was reporting Diffie-Hellman errors and rejecting new logins if client tried to reconnect after SRS check failure.
Q00962151-02	Special character support was not working with SSL/TLS HTTPS administration using FWUA.
Q00962298-02	The Primary circuit was not brought back up when BIS with Ping trigger was used in a branch office scenario.
Q00964349-01	A change was made to encode all LDAP attributes according to RFC2253.
Q00971902-01	Creating a new tunnel while multiple tunnels are brought up caused Contivity Secure IP Services gateway to core.
Q00974716	The SIP invite packets were not forwarded when NAT and PPP were used.
Q00975028-02	Many TunnelGuard event messages were not sent to SysLog.
Q00975132	An incorrect MAC address was used as a source MAC address after a BIS interface failover when Ping trigger was used.
Q00976087-02	The Contivity gateway might core if a client disconnected after a TunnelGuard recheck was started but had not been fully processed.
Q00976210-01	The IP address associated with the Frame Relay VC was not reported in the MIB when interface was disconnected.
Q00976553	The Contivity gateway might core when provisioned with an output of a “show running config” containing DLSW/SDLC configuration.
Q00985465-01	The MIB instances for Frame Relay VCs were set incorrectly.
Q00986406-02	A memory leak was discovered on a Contivity 5000 when logging off IPSec users with TunnelGuard enabled.
Q00989508-02	The Contivity gateway might core when logging off IPSec sessions with TunnelGuard enabled.
Q00991243	The Advance LDAP Proxy displayed an incorrect LDAP search filter for certificates authentication.
Q01000186	User tunnels could not be brought up when CRL checking was set to mandatory and Microsoft distribution point was used.

Table 1 Software release V5.05_121 (continued)

CR number	Description
Q01010815	The SSL VPN module was not handling large internal packets.
Q01012595-01	Configuration of LDAP using CLI produced incorrect LDAP search filter.
Q01016723	If an error occured while importing server certificate, Contivity could hang HTTP sessions.
Q01019184-01	Contivity gateway might core on stopping/starting LDAP when external LDAP was used for client authentication.
Q01022391	Contivity might core when importing a certificate with no CRL distribution point configured.

Table 2 lists customer issues from previous releases that are fixed in V5_05.180 release.

Table 2 Software release V5_05.180

CR number	Description
Q00769854-01	The branch office InOctet statistics counter was reset when security associations (SAs) were renegotiated and as a result SNMP was reporting incorrect total number of ifInOctets per tunnel session.
Q00777202	An incorrect node definition in the ces_id.mib file resulted in an error when loading the file into HP Open View NNM.
Q00791307-02	The Contivity Server might core in the tPace task due to a rare timing situation when user logs out and Contivity is still processing packets for the user tunnel.
Q00804828	An Hours filter profile should not be able to be deleted from a BIS profile which is still active.
Q00827620	The Contivity Server was not responding correctly to Cisco IOS certificate requests preventing branch office tunnels from being established.
Q00850382	When performing an SNMP walk on the Contivity server OIDs are not returned in numerical order if their instances are stored internally by IP Address. This may cause incorrect reports from some MIB browsers.
Q00876209	An IPsec User tunnel with NAT traversal to the Contivity Server CLIP address will not receive data and will appear to be hung after receiving the banner text.

Table 2 Software release V5_05.180 (continued)

CR number	Description
Q00909925	Under specific circumstances a user tunnel can be established successfully after the Server certificate has been revoked. This was a specific set of circumstances whereby the Client was unable to determine that the certificate had been revoked and the user had an open HTTP connection to the Contivity Server prior to the certificate being revoked.
Q00927767	The Contivity Server SNMP agent was not properly responding to SNMP get next requests for the IP Tunnel mib when requests contained an incomplete instance ID.
Q00934948	When an administrator is accessing the graphing utility from Status -> Reports -> Graphs the session will not be timed out due to inactivity therefore the user will not be prompted to re-enter the admin password.
Q00942962	When deleting a branch office or user tunnel on the Contivity Server the specific firewall policies for that tunnel are not removed. The tunnel should not be deleted before removing the corresponding policies and an error message is now displayed.
Q00951196	An admin user with management rights to the Contivity server and view only right to users was able to execute the “show running-config” command once logged in through a Telnet session.
Q00958417	Traffic is not forwarded to a branch office tunnel if the tunnel routing is static and remote endpoint is learned through OSPF or RIP.
Q00995161	A user authenticated by Radius will be bound to the default Radius group if the Radius Class attribute notation in the Radius server’s configuration (“ou”) contains an upper case character. (IE: Ou=xxxx, OU=xxxx).
Q00999752	The Contivity Server routing table is not properly updated when a RIP Accept Policy removes lowest cost route.
Q00960032	When the LDAP process is restarted on the Contivity Server incomplete information is passed to the task that stores the current configuration information for a branch office tunnel. Specifically the status of NAT on the tunnel is lost and results in the failure of the tunnel to re-establish if NAT was enabled.
Q00985465	On a Contivity Server Frame Relay connection with one or more virtual circuits (VC) configured, each VC has its own ifEntry instance. When the VC is operationally down, the MIB attribute ifEntry.ifAdminStatus for the VC is incorrectly reported as disabled.
Q00986813-01	The value for the Contivity Server DLSw Slow Contact Counter is set to 65535 by default; it should have been set to 8.
Q00994013	The process that parses and validate IPsec passwords would accept up to 33 characters but parse only 32. Passwords of greater than 32 characters would always be rejected.

Table 2 Software release V5_05.180 (continued)

CR number	Description
Q01014968	The Global CLI command 'snmp-server enable trap hardware' would fail when specifying wan 3/1 as an option indicating it was an incomplete command on a 1740 Contivity Server. This was due to the failure to recognize slot 3 as valid.
Q01016691	The branch office tunnel could be established using a revoked certificate in the case where only one side of the tunnel had access to the CRL, or access to the CRL was over the tunnel.
Q01016700	The Contivity Server Fiber Gig Ethernet interface was incompatible with Passport 8600 Fiber Gig Ethernet interface, causing disruptions in the operation of two devices when connected back to back.
Q01018372	The Contivity Server might core when a server certificate is being updated dynamically through the CLI and the renewed server certificate is large then 2 Kbytes.
Q01019288-02	The TunnelGuard daemon will not disconnect the tunnel when it loses communications with the Contivity Agent.
Q01038735	On the Contivity Server the ifAdminStatus and ifOperStatus of Circuitless IP interfaces report a down state
Q01041168	The Contivity Server with Firewall enabled was selecting only one ECMP default route when multiple routes were available. A change has been made to allow round robin selection of available ECMP defaults routes.
Q01045320	The "Renew <number> days before expiration" attribute of Certificate Enrollment configuration was not carried over when a certificate was renewed resetting the number of days to default value of 3 days.
Q01048109	The T1 line on a quad T1 would stop transmitting after encountering a particular transmit error.
Q01052701	The Contivity Server was incorrectly calculating MTU values causing 7854 hardware accelerator card to stop processing packets.
Q01052710	The initial contact payload received from the initiator of an ABOT tunnel was not deleting previous SAs causing tunnel establishment to fail.
Q01053410	The Contivity Server code was modified to drop non local ARP requests.
Q01056887	The Contivity Server might core if corrupted password was passed to the LDAP task
Q01057079	The ECMP functionality on the Contivity Server was not handling OSPF routes with non-zero forwarding address correctly causing only one of the equal cost routes to be added to the routing table.

Table 2 Software release V5_05.180 (continued)

CR number	Description
Q01059115	The Contivity Server branch office and user IPsec tunnels were not re-establishing after PPPoE session was reset by the remote PPPoE server.
Q01062122	The Nortel Vendor-Specific class attribute could not be used to bind a Radius user to a specific group.
Q01064902	The SSL VPN Manager was not accepting underscore (_), hyphen (-) or dot (.) characters as a part of email address for the certificate.
Q01066626	The Contivity Server may core if an unutilized SSL VPN card is accessed through the Management Screen.
Q01067062	The PPP idle timer was causing a memory leak when the timer was reset.
Q01073668	Bouncing a T1 line on a quad T1 card was causing transmission to abort.
Q01073707	The Contivity Server was displaying the same number of InBytes and OutBytes for a T1 port statistics.
Q01081961	An inactive Frame Relay Virtual Circuit will never recover if the physical interface is disabled and re-enabled before the Virtual Circuit is activated by the Frame Relay switch.
Q01082844	The Quad T1 module on the Contivity Server may get into a state in which it will no longer process incoming packets after periods of heavy bursts of traffic.
Q01089054	The ECMP per Destination and per Source routing algorithms were not functioning properly.
Q01089067	An attempt to open an HTTPS connection to a Contivity Server with no certificates installed was causing a memory leak.
Q01089495-01	The Contivity Server might core during TunnelGuard user verification process when multiple users are being authenticated and TunnelGuard was configured with long SRS rule sets.
Q01090732	The Contivity Server might core if hardware accelerator card receives an IP packet with IP options in IP header.

Table 3 lists customer issues from previous releases that are fixed in V5_05.200 release.

Table 3 Software release V5_05.200

CR number	Description
Q00935154-01	The 7811 Hardware Accelerator card may crash due to an internal error, and not recover gracefully even though the auto-recovery option is enabled. This would result in the termination of all VPN tunnels routed through it.
Q00942962	When deleting a user group or a Branch Office connection, the Firewall policies stored in the LDAP file are not being searched for rules involving the user tunnel or branch office tunnel to be deleted. The associated rules are therefore not being deleted.
Q01097151	An interface configured for VRRP with the deactivate option enabled on the associated Critical Interface group and designated as the VRRP master will never be elected VRRP master again once the interface goes down.
Q01069148	The Radius Accounting files are deleted based on the default value of 60 days rather than the configured value when the request for deletion is made while the LDAP server was not accessible.
Q01070117	When enabling the “Enforce TCP Conversation Rules” on the incoming packets a test was made to see if the packet was a TCP SYN packet. This check did not account for SYN packets with either the ECN or CWR bits set and would drop valid packets.
Q01079635	The Nortel VPN Router will not send an SNMP link down trap for a Branch Office Tunnel down event.
Q01079713	The Nortel VPN Router CLI command “show running config” does not display the NTP configuration information.
Q01080024	When "ping trigger" is used in a BIS configuration the Nortel VPN Router may run out of system buffers and become unmanageable and eventually hang. The problem happened every 4-5 hours at the particular site. If any other method (such as Interface group or route unreachable) is used, the problem does not happen.
Q01080729	The Nortel VPN Router occasionally incorrectly reports the IfOperStatus for a Branch Office Tunnel as down even when the tunnel association is still valid.
Q01089050	When NAT’d traffic exits the box on one interface and returns on another (ie:ECMP), the Contivity firewall checks the interface to see if the traffic is expected. If it is not expected traffic the packet is dropped. This should not be the case if the NAT translation exists within the table.

Table 3 Software release V5_05.200 (continued)

CR number	Description
Q01092900	The Nortel VPN Router has a timer mechanism which polls for nailed-up tunnels every 60 seconds to see if any require initiation. When IP is deleted, a tunnel indicator used by the timer mechanism is set to NULL resulting in the timer trying to bring the tunnel up on the next poll. Because IP is deleted, the initiate fails but the tunnel indicator is not reset. Therefore, nailed-up Branch Office Tunnels will fail to come up again after IP re-added.
Q01101724	The Nortel VPN Router may core while processing numerous simultaneous failed authentication attempts with SNMP traps enabled. This is a timing issue and is rarely seen.
Q01105397	SSL-VPN servers configured on a public CLIP address do not function because packets being returned by the Panther card are being routed through private routes rather than public routes.
Q01105803	In a Nortel VPN Router with the Quad T1 PCI card, transmit traffic may be delayed if the receive side is nominally quiet. The transmission of data is not interrupt driven, it is initiated by the queuing of additional transmit data or by receive data. This can cause the above mentioned symptom in certain cases.
Q01117695	The Nortel VPN Router may core while processing an illegally formed IKE packet from an outside source.
Q01133958	The Nortel VPN Router may core while processing multiple simultaneous tunnel creations. This is a timing issue and is rarely seen.

Table 4 lists customer issues from previous releases that are fixed in V5_05.202 release.

Table 4 Software release V5_05.202

CR number	Description
Q01113703	The Nortel VPN Router may core while initiating an ABOT tunnel. This may occur if the tunnel session information is accessed before the tunnel is completely established. This may be the result of a configuration change or query, or statistics query from the GUI interface.

Table 4 Software release V5_05.202

CR number	Description
Q01155819	A Nortel VPN Router configuration with the CRL Distribution Point feature and CRL optimization enabled may experience a slow and constant memory leak during Certificate authentication.
Q01122892	A Nortel VPN Router with Certificate authentication may experience a memory leak while tunnels are being established and terminated. This leak was recently introduced with the added support for multiple Certificate payloads in a single authentication packet.

Table 5 lists customer issues from previous releases that are fixed in V5_05.220 release.

Table 5 Software release V5_05.220

CR number	Description
Q00738300	Extended VRRP packets of size greater than 64 Bytes are not handled correctly and may cause the Nortel VPN Router to stop transmitting VRRP advertisements.
Q00797639	The Nortel VPN Router allows an administrative user to login with an otherwise valid username which was entered using the wrong capitalization. The login appears successful, but will cause problems when the user rights and permissions are applied.
Q01014456	On Nortel VPN router there was no way to unlock a user's Administrative account after max failed logins have been reached other than to delete and then re-create the user.
Q01020298	The Nortel VPN Router may core while possessing SNMPv2 trap messages if the SNMP ALG is enabled.
Q01040626	When an external LDAP server becomes unavailable, the Nortel VPN Router may appear to hang while trying to locate this server. The hang is due to large timeout values, and other issues regarding the processing of simultaneous LDAP requests.
Q01060824	The Nortel VPN Router may core during the processing of an authentication packet through the Hardware Accelerator module if the authentication packet verification fails and the hardware simultaneously reports a non-fatal memory transfer (DMA) error.
Q01078802	The ‘Specified DHCP Server’ option will did work on the Nortel VPN Router if the DHCP server IP address is not in the same network class as that of the DHCP client.
Q01080729	The Nortel VPN Router occasionally incorrectly reports the IfOperStatus for a Branch Office Tunnel as down even when the tunnel association is still valid.

Table 5 Software release V5_05.220 (continued)

CR number	Description
Q01098880	The Quad T1 module may cease processing received packets when all four ports are utilizing the full bandwidth simultaneously.
Q01102176	An ADSL module might fail to recover after a loss of the physical link.
Q01106009	The Nortel VPN Router no longer reports the status of branch office tunnel when the IP Tunnel MIB is polled using the TunnelConfigID parameter.
Q01107861	The Quad T1 module may cease processing received packets on all four ports due to a lost hardware interrupt.
Q01111555	An FTP connection initiated to the Nortel VPN Router while it is initializing may cause a core and system restart. The FTP connection will appear to hang as the box is not initialized. If it is then cancelled and a new connection initiated a core may result.
Q01113703	The Nortel VPN Router may core while initiating an ABOT tunnel. This may occur if the tunnel session information is accessed before the tunnel is completely established. This may be the result of a configuration change or query, or statistics query from the GUI interface.
Q01118755	The Nortel VPN Router may core after the TunnelGuard rule set is modified and one of the rules contains an empty string.
Q01122892	A Nortel VPN Router with Certificate authentication may experience a memory leak while tunnels are being established and terminated. This leak was recently introduced with the added support for multiple Certificate payloads in a single authentication packet.
Q01123312	The Nortel VPN Router may core after enabling BIS when the Primary BOT tunnel is up, the Remote Networks are configured as 0.0.0.0/0.0.0.0 and Ping trigger is set.
Q01124087	The Nortel VPN Router may core due an error in the processing of ICMP flows. The Firewall may attempt to process ICMP packets from a session that has already been terminated.
Q01126660	The Quad T1 port on a Nortel VPN Router ceases to process received packets once a request for a system buffer fails to allocate one.
Q01126851	The Nortel VPN Router may erroneously log an authentication failure when setting up dynamic route using OSPF with MD5 Authentication.
Q01133600	The Nortel VPN Router command to clear the NAT Flow Cache does not work properly for static Branch Office Tunnels.
Q01138272	Frame Relay performance on the Nortel VPN Router with Traffic Shaping configured will have wildly oscillating transfer rates, with peak rates well in excess of the configured CIR.

Table 5 Software release V5_05.220 (continued)

CR number	Description
Q01148960	The Nortel VPN router has a moderate size memory leak while processing SNMP requests for the information contained in the IP Tunnel mib.
Q01155081	The Nortel VPN Router was logging the OSPF neighbor state changes to the event log only. A change has been made to log these events to the system log as well.
Q01155819	A Nortel VPN Router configuration with the CRL Distribution Point feature and CRL optimization enabled may experience a slow and constant memory leak during Certificate authentication.
Q01160057	Spurious ‘voltage out of range’ alarms were generated by the Nortel VPN Router 1010, 1050 and 1100.
Q01172417	A recent security vulnerability fix (CR Q01117695) caused an incompatibility with the Nortel VPN Client and the processing of IKE keepalive messages.
Q01174315	When CRL retrieval is enabled on the Nortel VPN Router and the external LDAP server which stores the CRL is unavailable a memory leak may occur.

Table 6 lists customer issues from previous releases that are fixed in V6_00.151

Table 6 Software release V6_00.151

CR number	Description
Q01213204	The VPN Router will core when running 8 or more VLANs configured on a port.

Table 7 on page 35 lists customer issues from previous releases that are fixed in V6_00.310 release.

Table 7 Software release V6_00.310

CR number	Description
Q01199301	During or after upgrading to V06_00.151, when the active Firewall Policy is saved, user-defined objects may become unavailable. This may prevent the Nortel VPN Router from routing packets correctly.
Q01246301	Public default gateway address when received from DHCP not in routing table. If the VPN Router public interface obtained its IP address from a DHCP server, this address was not being loaded into the routing table when the VPN Router was initialized to serve as the default route.
Q01247735	Default Route over T1 PPP link not added to routing table after reboot. Similar to Q01246301 in that the default route is not active in the routing table.
Q011247816	QoS does not work with FRF.12 enabled. Diffserv code points and corresponding QoS behaviors were not being honored when running FRF.12.

Version 6.00 product considerations

Nortel no longer supports Axent defender. It has been removed from the management GUI.

If a STUN client and server are used to determine the type and capabilities of local NAT, the reported type can be incorrect when Branch Office NAT is used.

Multinet addresses are not supported as Initiators in ABOT’s definitions.

The saved event log file contains binary data and is only readable by a dump log utility, Dumplog.exe. This utility takes a binary log file and converts it to ASCII text. Dumplog.exe requires the evl.txt file from the Contivity's /system/log directory. Dumplog.exe is in Contivity \tools directory.

Usage: dumplog [options] <evl_file> <log_file>

The following options are currently available:

-e <Entity>	Only display messages for this entity/subentity

-c <Code> Only display messages with the specified code

-s <Severity> Only display messages with specified severity

Severities are specified as follows:

(E)mergency

(A)lert

(C)ritical

E(R)ror

(W)arning

(N)otice

(I)nfo

(D)ebug

-a <Directory> All autolog files are treated as a single saved log.

Autolog files are stored in <Directory>

-t <Time> Print log starting at this time (24 hour time)

-d <Date> Print log starting at this date

If you are upgrading from Version 5.05 to Version 6.00, you must disable the demand interface before upgrading to the 6.00 version. Once the upgrade is completed, change the Ping source to IP, add the interface IP, and then enable the demand interface. A straight upgrade results in the backup connecting right away.

If the BGP local preference is set to 0, no remote routes are accepted into the BGP routing table and, therefore, those routes are not advertised to the other neighbors.

The SSL VPN card supports version 5.0.1.1 of the VPN gateway code and is backwards compatible with 4.2.1.7 and 4.2.1.19.

H.323 does not work when NAT is enabled, nor does H.323 video traffic pass with an allow H.323 only policy.

Version 6.00 known anomalies

The following sections describe issues that Nortel has determined need to be fixed in a future release.

Frame Relay

Q01141806 — FR Virtual Circuits can be erased when OSPF is configured

If you delete the VC from the GUI or CLI when OSPF is configured on the VC, the operation does not fail and you do not receive an error message, as is the case for LAN interfaces with OSPF configured.

You can modify the Local IP Address for a private VC with OSPF configured. This operation should also fail, because this operation means that the VC with OSPF configured is first deleted and then replaced with another private VC.

Q01201807 — CES crashes when a VC with no DLCI is created from the CLI

When a VC does not have a DLCI created from the CLI, the CES crashes.

DHCP

Q01078645 — Incorrect message when IP of private interface is set as external IP address source

If you create a user tunnel, using a CES configured as DHCP as the User IP Address Source, and the IP of a private interface as the Specified External Server, the tunnel comes up and there appears to be no problems. However, the CES the clients use displays an incorrect notification of No recent offers received from this DHCP server, instead of the correct message of Configured.

Q01142400 — DHCP Server always offers packets with management IP as source

When a relay is used, the DHCP client gets its address from the DHCP server through the relay. The server provides the client with a default gateway. All DHCP packets received by the client from the server have the server's management IP address as source, and the server identifier field is set to the server's management IP address, regardless of the physical interface the server sent the packets through. Halfway through the lease's duration, the client tries to renew its lease by sending unicast requests to the server's management IP address. DHCP clients are unable to renew their lease, because the DHCP request packets sent by the client are trying to directly reach the DHCP server management IP address, which is unreachable.

You can renew your lease if the equipment used as the default gateway by the DHCP clients can reach the management IP address of the CES that acts as the DHCP server. Otherwise, you will remain without your IP address for a few seconds until new IP addresses are negotiated with the DHCP server through the DHCP relay.

Limitations when the DHCP client is configured on a sub-interface

After the VPN Router is rebooted, the IP address given to the sub-interface may be different from the original one.

If the primary interface of the sub-interface is disabled or the IP address of the DHCP server is deleted, the IP address of that sub-interface will be removed from the routing table but the routes related to that IP address (direct host, direct net, and default gateway) may remain. In addition, if the disabled interface is then enabled and the route received from the DHCP server has since changed, the default gateway routing table information may not be correctly updated.

Tunnels

Q01074094 — Different types of tunnels have different behavior with firewall enabled

When you configure an ABOT on public interfaces between two servers with firewall enabled on both, the IPsec and PPTP ABOTs come up even if the initiator does not have IPsec or PPTP enabled in Service > Available page. An L2TP ABOT does not come up unless L2TP is enabled in Service > Available page.

Q01098723 — P2P tunnels can be made using dynamic LAN and VLAN, but not dynamic PPoE

There is an inconsistency between the creation of a Peer to Peer (P2P) tunnel using a dynamic LAN or dynamic VLAN as a local IP address, and the creation of a P2P tunnel using a dynamic PPPoE as a local IP address. The client can create functional P2P tunnels using a dynamic LAN or a dynamic VLAN. The client cannot define a P2P tunnel in the same manner using a dynamic PPPoE as a local IP address.

Q01137058 — No traffic passes through Branch Office tunnel with filter "permit only dns/ftp" applied

No traffic passes through a branch office tunnel if the filter permit only dns/ftp is applied on the tunnel. Also, the filter permit only dns/http does not allow any traffic to pass. Other filters, such as Entrust PKI, work appropriately for user tunnels.

BGP

Q1193203 — CES crashes with 100000 BGP routes when BGP is disabled

When BGP is disabled from either the GUI or the CLI, the CES crashes when it reaches 100000 BGP routes.

Demand Services

Q01141767 — If Demand is enabled for the first time from CLI, an error message appears

When Demand is enabled for the first time from the CLI, an error message appears. Despite this error, Demand is enabled on the CES box.

Multinetting

Q01191923 — TCP MSS options not configurable under secondary multinet interfaces

TCP MSS options are available only for the primary interface. You cannot configure the secondary multinet interfaces.

Q01193299 — CLI mode permits adding of multiple secondary IP addresses from the same network

When you use the GUI to add more than one multinet IP from the same network, you get the error message: Error creating new record; IP address conflicts with:. However, from the CLI, you can add multiple secondary IP addresses from the same network without getting an error message.

Others

Q01128397 — Ping to validate default route: static route not installed

When you use the feature Ping to Validate Default Route and the ping address is not on the local LAN, a static route is added to reach the destination. This works when creating the default route, ping destination. However, when the device is rebooted, an attempt is made to add the static route before the interface is up. The attempt fails and after several retries, the DUT stops trying to add the route. The interface then finishes coming up and the static routes are never installed. Since there is no route to the ping default route destination address, the ping fails and the default route is disabled. The workaround is bounce Ping to Validate Default Route.

Q01167469 — Errors and incorrect messages in event log after reboot

Incorrect messages are found in the event log when a newly installed CES is rebooted. Some of these messages are marked as errors.

Q01190797 — Applet for configuring Firewall and NAT policies does not work with Opera browser

The applet for NAT and Firewall policies configuration no longer works with Opera browser. A custom Event Queue replaces the SystemEventQueue of the Java Virtual Machine (JVM). Opera is written in Java and uses its own instance of JVM. When Opera tries to open an applet, it uses the browser JVM for the applet, not a different instance. The function getSystemEventQueue from the Java API returns the SystemEventQueue if no security policy is defined, or if a security policy that allows the execution of the function is defined. Opera has a security policy that does not permit the above mentioned function to return the SystemEventQueue.

To permit the function to return the SystemEventQueue, you must add the following line in the grant section (default permissions granted to all domains) of the file opera.policy found in the {Opera installation directory}\classes directory:

```
permission java.awt.AWTPermission "accessEventQueue"
```

Q01190820 — Page unavailable when editing a remote network with incompatible IP/mask combination

When you edit a remote network defined in a BO connection with an incompatible IP/mask combination, the Profiles > Branch Office page becomes unavailable. You receive a message saying "The requested page is temporarily unavailable. Please use your browser's back button to return to the previous page, and try the operation again." This problem occurs with both IE and Netscape browsers.

Q01191261 — Netdirect subnet error log on CES is incorrect

The Contivity event log says "SSL-VPN netdirect address (33.33.33.33) must be in the 192.32.18.0 space," but that statement is incorrect. The 33.33.33.33 is the front-end interface and should not be in the same subnet as the back-end interface.

Q01193236 — Wrong warning message when disable all IKE encryption methods

If all IKE encryption methods are disabled from the GUI or the CLI, an incorrect error message appears. The message displayed says “Value out of defined range,” when it should say “No IKE encryption selected.”

Q01193293 — Issue when change mask if interface from serial menu with unacceptable value

When you change the mask of an interface from the serial menu with a value that makes the IP equal with the network address of the subnet, the following error message appears: “Couldn't set the Subnet Mask value (255.255.255.252) for 11.9.198.20. Error: IP address can't have zero in host number.", and the previous configured IP disappears. The previous combination of IP/mask should remain unchanged.

Q01193307 — Issue when change mask of interface to specific value if secondary IP is configured

When you change the mask of an interface from the serial menu with a value that makes the IP equal with the network address of the subnet, the following error message appears: "Couldn't set the Subnet Mask value (255.255.255.252) for 11.9.198.20. Error: IP address can't have zero in host number.", but the changes are saved. The changes are reflected on Serial menu, GUI and CLI. This problem appears only if a secondary IP is configured on an interface.

Q01194428 — Command Line Interface idle-timeout not recognized after rebooting

After a reboot, a connection through the Serial Connection to the Command Line Interface times out after only 900 seconds. This occurs even though the Admin Idle-Timeout is set to 23:00 hours. This shortened time-out occurs only once after a reboot; afterwards, the configured timeout is in effect.

Q01199301 — Upgrade of CES from 4.85 to 6.00_139 resulting in firewall objects lost

After an upgrade of the CES from 4.85 to 6.00_139, some firewall rules do not work. For instance, pings that are allowed through the firewall do not get through.

Q01201847 — OSPF Announce access-lists do not work in some cases

There are scenarios when routes are advertised even though an access-list was created to block that range. However, if the access-list is applied globally (on all interfaces), the behavior is normal. The access-list also works correctly if the BO tunnel is disabled and the OSPF is bounced globally, or if the access-list is disabled and enabled again.

Q01201957 — Inconsistency when setting traffic shaping rates for an E1 LMC1200 card

There is an inconsistency between the GUI and CLI when setting traffic shaping rates for an LMC1200 interface with an E1 line format. When you create a virtual circuit from the GUI, the default Be value for the circuit is 2048000 bits. When you create a virtual circuit from the CLI, the default Be value is 1536000 bits.

Q01205726 — Settings for certain SNMP traps are removed after reboot

For an SNMP trap, you can enable it, change the interval, or enable "send one" option. For certain SNMP traps, if you perform any of these actions and reboot the CES, the settings are removed and returned to their initial value.

The affected SNMP traps are:

- Hardware traps:
  - Bulk Accelerator in slot n
- Server traps:
  - OSPF
  - Network Time Protocol
  - Global Demand Services

- — DHCP Relay
- — CLIP

- Service traps:
  - VRRP
  - Multicast Relay
  - RIP
  - DLSw
  - IPsec Failover Service
  - TunnelGuard
  - Routing Policy Server
  - Client Routes Marshaler

Contivity gateway considerations

The following sections contain general considerations for this product.

Upgrade procedure considerations:

- Contivity 1010, 1050, and 1100 require a 64 Mb flash disk.
- Version 6.00 supports upgrades from Versions 4.70, 4,80, 4.90 and 5.00. If you run an older version, you may have to upgrade to a later version before you upgrade to Version 6.00.
- The amount of disk space required to upgrade to the latest version is configuration-specific. If you receive disk space error messages, you must remove any unnecessary files from your Contivity system.
- Any recovery floppy diskette that you created prior to release Version 4.0 does not work on a system that runs Version 4.0 or later software.
- Nortel recommends that, when you upgrade to Version 6.00 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 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 6.00 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.

www.nortel.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
- BGP routes is the number of BGP route entries in the IP routing table
- OSPF Routes is the number of OSPF route entries in the IP routing table
- Redistributed OSPF, BGP and RIP Routes is the number of routes redistributed into RIP, BGP 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 6.00 is 4.65.

Table 8 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, 1750, 2700, and 5000 platforms.

Table 8 Hardware platform and server software compatibility

Hardware platform	Server software compatibility				
	4.76	**4.80**	**4.90**	**5.00**	**6.00**
	5/03	**8/03**	**05/04**	**08/04**	**08/04**
1010	X	X	X	X	X
1050	X	X	X	X	X
1100	X	X	X	X	X
600	X	X	X	X	X
1500					
1510					
1600	X	X	X	X	X
1700	X	X	X	X	X
1740		X	X	X	X
2000					
2500					
2600	X	X	X	X	X

Table 8 Hardware platform and server software compatibility (continued)

Hardware platform	Server software compatibility				
	4.76	**4.80**	**4.90**	**5.00**	**6.00**
	5/03	**8/03**	**05/04**	**08/04**	**08/04**
2700	X	X	X	X	X
4000					
4500	X	X	X	X	
4600	X	X	X	X	X
5000	X	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, such as 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 do not fit into the connector on slot 4 on the Contivity 4600.
- If more than 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 6.00.
- 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 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.
- Any configuration of route policies is lost after an upgrade from V04_7x to the latest version. You must re-enter the settings manually.

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. 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 are launched, which leads 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 actual 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

  Unix/Linux:

  - 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

  Unix/Linux:

  - 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 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 could 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 can 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.
- Table 9 lists the maximum number of tunnels for each Contivity model and indicates whether each model has a five-tunnel base unit version.

Table 9 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, 1750	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.

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.