Version 5.05.180

Part No. 315000-H Rev 00
May 2005

600 Technology Park Drive
Billerica, MA 01821-4130

Contivity Secure IP Services Gateway Release Notes

NORTEL NETWORKS™

Copyright © 2005 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* Contivity* Secure IP Services Gateway Version 5.05.180.

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 5.05.180. Version 5.05.180 is a software maintenance release to Version 5.00. It supports the first release of the VPN Router Model 1750, and addresses customer-found software issues.

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 5.05.180 feature summary

Version 5.05.180 of the Contivity gateway provides support for the following:

- Nortel VPN Router (formerly known as Contivity) 1750

  The VPN Router 1750 is the replacement platform for the VPN Router 1700 and VPN Router 1740. The VPN Router 1750 provides similar performance to both the VPN Router 1700 and 1740. The VPN Router 1750 provides dual 10/100 Base T Ethernet ports on the base system as well as providing four open slots for I/O expansion. The chassis footprint of the VPN Router 1750 is identical to the VPN Router 1740. The 1750 utilizes a 3U chassis; the 1700 utilized a 2U chassis. The power requirements of the VPN Router 1750 are identical to both the 1700 and 1740.

  Like its predecessors, the VPN Router 1750 is offered in both a five-tunnel version suitable for “routing” applications and a 500-tunnel version suitable for Remote Access VPN applications.

The VPN Router 1750 can be considered a functional replacement for either the VPN Router 1700 or the VPN Router 1740; however, there is a configuration file difference due to the new slot configuration. Slot-0/port-1 and Slot-0/port-2 used for the integrated Ethernet ports is unique to the 1750.

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 5.05.180 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 Version 5.00, with the exception of Q00738300 and Q00921504.

Table 1 Fixed customer issues

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.
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.
Q00778885-02	The wildcard mask entered for the network while in the CLI “router ospf” configuration menu was not saved, and that resulted in failures during provisioning.
Q00785286-03	Reverse (wildcard) subnet mask was considered non-continuous and therefore disallowed.
Q00791307-02	The Contivity Server might core in the tPace task due to a rare timing situation where the user logs out and Contivity is still processing packets for the user tunnel.

Table 1 Fixed customer issues

Q00804828	An Hours filter profile should not be able to be deleted from a BIS profile that is still active.
Q00809510-01	The ability to specify public side default DHCP lease time and to disallow RFC1918 public leases were added.
Q00827620	The Contivity server was not responding correctly to Cisco IOS certificate requests, preventing branch office tunnels from being established.
Q00828414-01	The Contivity gateway may hang when the file system is full and a “save configuration” procedure is started.
Q00841811-01	CRL retrieval was failing 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.
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.
Q00852275-01	The restricted filter has been redefined to allow only client banner during authentication, to prevent any possible security breaches.
Q00864753-01	Enhancement. Support for LDAP over SSL on public interfaces has been added.
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.
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 was displaying incorrect count for outbound DE (discard eligible) packets.
Q00900495-02	The "show run" CLI command was displaying the administrator’s password incorrectly.

Table 1 Fixed customer issues

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.
Q00912336-02	The Contivity file system errors are logged when a file is accessed on an optional hard disk on a diskless box (Bluefin).
Q00914781	Users from a group that had an Access Network Name defined were not able to HTTP to the Contivity gateway.
Q00914821-01	The ABOT tunnel was not establishing when PPPoE dynamic routing information was being updated.
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.
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 the Contivity gateway were sending 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.
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.
Q00935101-01	The diskless Contivity gateway (Bluefin) allowed configuration of an FTP coredump without the user entering the FTP User ID/Password
Q00937672-01	The Ping trigger mechanism was bringing 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.
Q00942570-01	CES does not adjust the time correctly with NTP and the Time Zone set to GMT -07:00 Arizona.

Table 1 Fixed customer issues

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.
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.
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.
Q00953190	The Contivity Secure IP Services gateway was not extending its active DHCP lease when configured as a DHCP client.
Q00953824	The Contivity gateway might core when concurrent management is performed, in particular when several administrators delete the same object in the same time.
Q00955558	The OSPF LSA external route was not aging out from the LSDB.
Q00956438-02	The ABOT tunnel was establishing two IPSec SAs after the initial tunnel is terminated abnormally with Initial Contact Payload enabled on both ends and Initiator is set as Nailed Up.
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.
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 had been terminated abnormally.
Q00959911	Dead Peer Detection not working between the Contivity Entranet Switch and a Cisco Router.
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.
Q00960592-02	The Tunnelguard was reporting Diffie-Hellman errors and rejecting new logins if the client tried to reconnect after SRS check failure.
Q00962151-02	Special character support was not working with SSL/TLS HTTPS administration using FWUA.

Table 1 Fixed customer issues

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 has been made to encode all LDAP attributes according to RFC2253.
Q00971902-01	Creating a new tunnel while multiple tunnels are being brought up could cause 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 no longer sent to SysLog.
Q00975132	An incorrect MAC address was used as a source MAC address after a BIS interface failover when the Ping trigger was used.
Q00976087-02	The Contivity gateway might core if a client disconnected after a TunnelGuard recheck had started but not been fully processed.
Q00976210-01	The IP address associated with the Frame Relay VC was not reported in the MIB when interface had been disconnected.
Q00976553	The Contivity gateway might core when provisioning it with an output of a “show running config” which contained DLSW/SDLC configuration.
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.
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.
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.
Q00989508-02	The Contivity gateway might core when logging off IPSec sessions with TunnelGuard enabled.
Q00991243	The Advance LDAP Proxy was displaying an incorrect LDAP search filter for certificates authentication.
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 1 Fixed customer issues

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 uppercase character. (IE: Ou=xxxx, OU=xxxx).
Q00999752	The Contivity server routing table is not properly updated when a RIP Accept Policy removes the lowest-cost route.
Q01000186	User tunnels could not be brought up when CRL checking was set to mandatory and the Microsoft distribution point was used.
Q01010815	The SSL VPN module was not handling large internal packets.
Q01012595-01	Configuration of LDAP using CLI was producing an incorrect LDAP search filter.
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 the Passport 8600 Fiber Gig Ethernet interface, causing disruptions in the operation of two devices when connected back to back.
Q01016723	If an error occurred while importing a server certificate, Contivity could hang HTTP sessions.
Q01018372	The Contivity Server might core when a server certificate was being updated dynamically through the CLI and the renewed server certificate was larger than 2 Kbytes.
Q01019184-01	The Contivity gateway might core on stopping/starting LDAP when external LDAP was used for client authentication.
Q01022391	The Contivity might core when importing a certificate with no CRL distribution point configured.
Q01038735	On the Contivity server the ifAdminStatus and ifOperStatus of Circuitless IP interfaces report a down state.

Table 1 Fixed customer issues

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 default 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 the 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 the 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 a 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.
Q01059115	The Contivity server branch office and user IPSec tunnels were not re-establishing after a 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 the 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.

Table 1 Fixed customer issues

Q01073668	Bouncing a T1 line on a quad T1 card was causing the transmission to abort.
Q01073707	The Contivity server was displaying the same number of InBytes and OutBytes for 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 the TunnelGuard user verification process when multiple users were 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.

Version 5.05.180 product considerations

The following sections describe consideration for the Version 5.05.180 features.

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)

Version 5.05.180 known anomalies

The following sections describe issues that Nortel Networks has determined need to be fixed in a future release, but are not fixed in the current release.

Q01018362 - ICMP packets sent over NAT'd ECMP Interfaces utilizing the per-packet algorithm is a special case on the Contivity server. For per-packet algorithm, the ICMP conversation is changed depending on the interface or tunnel the packets are transmitted on. Users may experience intermittent ping failures over NAT'd ECMP interfaces. The use of source or destination algorithm is recommended in this scenario.

Q01097151 - The VRRP critical interface feature will not function properly when the Deactivate option is selected.

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 5.05.180 supports upgrades from Versions 4.70, 4,80, 4.90, and 5.00. If you are running an older version, you may have to upgrade to a later version before you upgrade to Version 5.05.180.
- 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 5.05.180 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 5.05.180 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 5.05.180. 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 5.05.180 is 4.65. In order to take full advantage of this release, the following versions are recommended for the related products:

- Contivity Client -- 5.01.110
- Contivity Tunnel Guard Agent -- 1.1.3.0
- ASA -- 4.2.1.15

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, 1750, 2700, and 5000 platforms.

Nortel VPN Client version 5_01.103 or above is required to get the full benefit of Entrust Roaming Profiles and Entrust Link Certificates.

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	5.05.180 05/05
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
1750					X
2000					
2500					
2600	X	X	X	X	X
2700	X	X	X	X	X
4000					
4500	X	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, 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 5.05.180.
- 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, 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.

- 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.