Version 5.00

Part No. 318438-A Rev 00
June 2004

600 Technology Park Drive
Billerica, MA 01821-4130

Configuring Tunneling Protocols for the Contivity Secure IP Services Gateway

NORTEL
NETWORKS™

Copyright © 2004 Nortel Networks

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

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

Trademarks

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

AXENT and OmniGuard Defender are trademarks of AXENT Technologies, Inc.

Check Point and FireWall-1 are trademarks of Check Point Software Technologies Ltd.

Cisco and Cisco Systems are trademarks of Cisco Systems, Inc.

Entrust and Entrust Authority are trademarks of Entrust Technologies, Incorporated.

Java is a trademark of Sun Microsystems.

Linux and Linux FreeS/WAN are trademarks of Linus Torvalds.

Macintosh is a trademark of Apple Computer, Inc.

Microsoft, Windows, Windows NT, and MS-DOS are trademarks of Microsoft Corporation.

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

NETVIEW is a trademark of International Business Machines Corp (IBM).

NetWARE, NDS, and Novel intraNetWare are trademarks of Novell, Inc.

OPENView is a trademark of Hewlett-Packard Company.

SafeNet/Soft-PK Security Policy Database Editor is a trademark of Information Resource Engineering, Inc.

SecurID and Security Dynamics ACE Server are trademarks of RSA Security Inc.

SPECTRUM is a trademark of Cabletron Systems, Inc.

VeriSign is a trademark of VeriSign, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

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

Chapter 4

Chapter 5

Figures

Preface

This guide describes the Nortel Networks* Contivity* Secure IP Services Gateway tunneling protocols. It provides configuration information and advanced WAN settings.

Before you begin

This guide is for network managers who are responsible for setting up and configuring the Contivity Secure IP Services Gateway. This guide assumes 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**.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is **more disk***n***:***<directory>***/...***<file_name>*, you enter **more** and the fully qualified name of the file.
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.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is **`terminal paging`** {**`off`** | **`on`**}, you enter either **`terminal paging off`** or **`terminal paging on`**, but not both.

Acronyms

This guide uses the following acronyms:

FTP	File Transfer Protocol
IP	Internet Protocol
IKE	IPSec Key Exchange
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet service provider
L2TP	Layer2 Tunneling Protocol
LDAP	Lightweight Directory Access Protocol
LAN	local area network
PDN	public data networks
POP	point-of-presence
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
UDP	User Datagram Protocol
VPN	virtual private network
WAN	wide area network

Related publications

For more information about the Contivity Secure IP Services Gateway, refer to the following publications:

- Release notes provide the latest information, including brief descriptions of the new features, problems fixed in this release, and known problems and workarounds.
- *Configuring Basic Features for the Contivity Secure IP Services Gateway* introduces the product and provides information about initial setup and configuration.
- *Configuring 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 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 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 of tunnel protocols

The gateway uses the Internet and remote connectivity to create secure extranets, or Virtual Private Networks (VPNs). Remote connectivity through the public data network (PDN) requires a protocol for safe transport and a connection from the remote user’s PC to the PDN. The gateway uses the most popular tunneling protocols: IPsec, PPTP, L2TP, and L2F.

To form a tunnel, the following takes place:

- The remote user establishes a connection with the PDN point-of-presence (POP), typically through an Internet Service Provider (ISP).
- After the Internet connection is up, the remote user launches a second connection that specifies a connection to a gateway. Instead of a telephone number to establish the link, the second connection uses an IP address (or a name if the IP address has been entered into a Domain Name Service server). This second connection could use either the Point-to-Point Tunneling Protocol (PPTP) or the IP Security (IPsec) tunneling protocol.
- Tunnels built using L2F are slightly different. The tunnel begins at a piece of networking equipment (network access server or NAS) located at the ISP instead of the remote user’s PC. The user simply dials into the ISP with a telephone number that causes an L2TP or L2F tunnel to connect directly to a specific corporation. This is similar to a traditional remote dial service except that the modems are maintained by the ISP and not the corporation.

All tunneling protocols are enabled on the public and private networks by default. Because data in tunnels is encrypted, the default setting guarantees that all interactions with the gateway are private. By leaving IPsec, PPTP, L2TP, and L2F enabled on the private side, you can establish tunneled connections to the gateway using any of the tunnel types from within your corporation. To prevent tunnel connections of a particular type (for all users, including administrators), you can simply disable the tunnel type.

For example, if you want to use IPsec as your only public tunneling protocol, then disable the Public selection for PPTP, L2TP, and L2F.

To configure tunnel access to the gateway:

1. Go to the Services > Available screen.
2. Select the tunnel type.

See *Configuring Basic Features for the Contivity Secure IP Services Gateway* for more information on configuring tunnels. See the appropriate chapter in this book for steps on how to change default tunnel protocol settings.

Chapter 2
Configuring IPsec

The IPsec tunneling protocol is supported by Nortel Networks and other third-party vendors. IPsec is a standard that offers a strong level of encryption (DES, Triple DES and AES), integrity protection (MD5 and SHA), and the IETF-recommended ISAKMP and Oakley Key Determination protocols, and token codes from SecurID* and AXENT*. IPsec offers the following features:

- Client support is available from Nortel Networks and other vendors. No special ISP services are required.
- Support for IP address translation via encapsulation, packet-by-packet authentication.
- Strong encryption and token codes.

Nortel Networks provides the IPsec remote access user client software on the CD that came with your gateway. You can install the client software on a network server for your remote users to download. The client software is a Microsoft* application available for the latest releases of Windows* 95, Windows 98, Windows NT*, Windows 2000 Workstation, and Windows NT Server. The software comes with complete online help.

Nortel Networks provides two versions of the IPsec client due to export restrictions. The standard version supports DES (56-bit key) encryption, and the enhanced version supports Triple DES (3DES, 168-bit key).

The self-extracting installation files for DES and Triple DES are labeled accordingly on the CD. The installation is simple; the self-extracting installation includes everything necessary to create IPsec tunnels with the gateway.

- AES128-SHA1
- AES256-SHA1
- AES128 Diffie Hellman Group 2, 5, and 8

- AES256 Diffie Hellman Group 5 and 8

For more details, refer to the instructions included as part of the client installation.

Note: AES256 SHA1 with AES Diffie Hellman Group 8 provides better performance than AES256 SHA1 with IKE AES256 Diffie Hellman Group 5.

Configuring IPsec settings

To configure the gateway for IPsec tunneling, you first configure the parameters on a global level on the Services > IPsec screen. You can individually configure IPsec parameters for groups, users, and branch offices from the Profiles menu.

- Global IPsec Settings

  IPsec is configured globally on the Services > IPsec screen.

- Group IPsec Settings

  Group IPsec settings are configured on the Profiles > Groups > Edit > IPsec screen.

- Branch Office Connection IPsec Settings

  Branch office IPsec settings are configured on the Profiles>Branch Office>Edit Connection > IPsec tunnel type screen.

- Branch Office Group IPsec Settings

  Branch office group IPsec settings are configured on the Profiles > Branch Office>Edit Group > IPsec screen.

To configure IPsec settings:

1. Select Services > IPsec. The Services > IPsec Settings screen appears.
2. Configure the IPsec Authentication settings. Select User Name and Password/ Pre-Shared Key, or RSA Digital Signature.

3 Configure the IPsec RADIUS Authentication settings for the connection. Click to Enable support for the authentication types that your RADIUS Server supports and that you expect to use:

- AXENT Technologies Defender--AXENT OmniGuard/Defender authentication.
- Security Dynamics SecurID--Security Dynamics SecurID authentication.
- User Name and Password--Username and password authentication; the username and password are encrypted.

4 Configure the IPsec Encryption settings for the connection. Click the appropriate box to either enable or disable the supported Encryption methods for this group. The encryption methods are shown on the screen in order of strength, from strongest to weakest.

➡ **Note:** Triple DES encryption requires more processing power than DES, potentially reducing the performance of the switch. AES provides stronger encryption than 3DES, and requires less processing power than 3DES, providing a potential performance improvement for branch office tunnels.

5 Configure the IPsec IKE Encryption and Diffie-Hellman Group settings for the connection. If you select more than one encryption type, you can select the encryption you would like to use on a per group basis in the Profiles > Branch Office > Edit > IPsec screen or the Profiles > Groups > Edit > IPsec screen.

6 Configure the IPsec NAT Traversal settings for the connection. NAT (Network Address Translation) Traversal allows a number of devices on a private network to access the Internet simultaneously without each requiring its own external IP address. To use NAT Traversal, a UDP port must be defined. It is used for all client connections to the gateway. This port must be a unique and unused UDP port within the private network within the range 1025-49151.

By default, NAT Traversal is disabled and no UDP port is defined.

➡ **Note:** To allow NAT Traversal with the IPsec client, you must enable the NAT Traversal setting on the Profiles > Groups > Edit > IPsec screen.

7 Configure the Authentication Order. The IPsec, PPTP, L2TP, and L2F tunnel types each have an Authentication Order table, which lists the corresponding

servers, authentication types, associated groups, and actions. The LDAP server is always queried first, then RADIUS, if applicable.

8 Configure the Load Balance settings. Click to enable Load Balancing of one gateway with an alternate gateway. Load Balancing is a protocol between two gateways that exchanges information about the number of sessions of each connection priority and the CPU utilization. When a connection is being established, the first gateway determines which of the two gateways should service the session. The gateway and the alternate gateway must be in the same location (they must be in communication via the private interface).

9 Configure the Fail-Over settings. Click to enable Fail-over of the selected gateway. A Fail-over condition is detected in approximately two minutes. If a connection is somehow terminated or lost, the client then attempts to connect to the first-listed Fail-over gateway. It tries each gateway in succession and if no connection is established, it stops.

Configuring group IPsec settings

To configure group IPsec settings:

1 Select Profiles > Groups and then click Edit for the group whose IPsec settings you want to configure. The Groups > Edit screen appears.

2 Click Configure in the IPsec section of the screen. The Groups > Edit > IPsec screen appears.

3 Click the Configure button for a specific parameter to make changes to that parameter. Click Configure in the All Fields section to edit all parameters at the same time. Use the Inherited button to set all fields to their inherited values.

4 Configure Split Tunneling. All IPsec client traffic is tunneled through the gateway by default. Split Tunneling allows you to configure specific network routes that are downloaded to the client. Only these network routes are then tunneled; any other traffic goes to the local PC interface. Split tunneling allows you to print locally, for example, even while you are tunneled into the gateway.

5 Configure Split Tunnel Networks. Click to select one of the networks to which you want to send encrypted tunnel traffic only. These networks are designated from the Profiles>Networks screen.

Configure Client Selection. The Client Selection feature enables you to configure your gateway to accept tunnel connections from third-party clients, in addition to the Nortel Networks Contivity VPN Client. Refer to the *Contivity Secure IP Services Gateway Release Notes* for a list of supported third-party clients.

If you choose the Configure for Both Contivity and non-Contivity Clients selection, the gateway provides support as described above, depending upon the type of client being used. For example, if you enable RADIUS Authentication, it is only used for Contivity clients, and you must have either preshared keys or RSA digital signature authentication enabled for non-Contivity clients.

6 Specify the Allowed Clients parameter. Use the menu to specify the type of clients that are allowed to create tunnels to your gateway.

7 Set the Allow undefined networks for non-Contivity clients parameter. Enabling this selection allows supported third-party clients to create IPsec tunnels to any internal networks. Nortel Networks recommends that you not allow undefined networks for third-party clients, and use Split Tunneling instead. This selection is ignored for Contivity clients.

8 Configure Authentication. Authentication is performed with a protected User ID and Password through the ISAKMP key management protocol. When you click configure, the Group Security Credentials (RADIUS) dialog box appears.

9 Configure Database Authentication (LDAP).

10 Specify User Name and Password. Click to enable the LDAP User Name and Password to authenticate user identity. Authentication is performed with a protected User ID and Password through the ISAKMP key management protocol.

11 Click to enable the Entrust certificate authentication. You must then click the drop-down list box to choose a Default Server Certificate. Servers are configured from the System > Certificates screen.

12 Configure RADIUS Authentication. The following attributes are associated with RADIUS Authentication when using IPsec tunneling. This is a two step process where (1) the gateway authenticates the remote user with the User Name and Password authentication mechanism, AXENT or SecurID hardware or software tokens, and (2) the client uses the Group ID and Group Password to authenticate the gateway's identity.

- User Name and Password

  Click to enable the RADIUS User Name and Password to authenticate user identity. Authentication is performed with a protected User ID and Password through the ISAKMP key management protocol.

- AXENT Technologies Defender

  Click to enable the AXENT OmniGuard/Defender challenge response token security authentication. The AXENT OmniGuard/Defender uses a personal identification number (PIN) and password, coupled with a challenge response security dialog, to authenticate user identity.

- Security Dynamics SecurID

  Click to enable the Security Dynamics SecurID token security authentication. The SecurID uses a PIN and the current code generated by a token assigned to the user to authenticate user identity.

  Enter the Group ID and Password, which are encrypted for transmission. The Group ID provides access to the gateway. Subsequent LDAP and RADIUS authentication is verified against the User ID

  Enter and confirm the Group Password, which provides access to the gateway. Subsequent LDAP and RADIUS authentication is verified against the User Password.

Note: The Group ID and User ID must not be the same.

13 Configure Encryption. Click Configure, then click the box to either enable or disable the supported Encryption methods for this group.

The encryption methods are presented in order of strength, from strongest to weakest. All of the following encryption methods ensure that the packet came from the original source at the secure end of the tunnel. Some of the encryption types do not appear on non-US models that are restricted by US Domestic export laws. Also, MD5 (Message Digest) provides integrity that detects packet modifications.

➡ **Note:** Triple DES encryption requires more processing power than DES, potentially reducing the performance of the switch. AES provides stronger encryption than 3DES, and requires less processing power than 3DES, providing a potential performance improvement for Branch Office tunnels.

14 Select the Diffie-Hellman Group level to apply to IKE (Internet Key Exchange) encryptions.

➡ **Note:** The choice of the IKE encryption algorithm does not affect the choice of the encryption algorithm used to encrypt data in IPsec. For example, you can use DES to encrypt the IKE exchanges, and then negotiate Triple DES for use in IPsec.

The Services > IPsec screen contains a section labeled “IKE Encryption and Diffie-Hellman Group.”

15 Set the Accept ISAKMP Initial Contact Payload to enabled to tear down the existing connection if an incoming connection has the same User ID as the existing connection. This is disabled by default.

16 Click to enable Perfect Forward Secrecy (PFS). With PFS, keys are not derived from previous keys. This ensures that one key being compromised cannot result in the compromise of subsequent keys.

17 Configure Forced Logoff. For IPsec tunneling, you can specify a time after which all active users are automatically logged off. The default is 0, which means the option is turned off. The possible range is 00:00:01 to 23:59:59.

18 Configure Client Auto Connect. The Client Auto Connect feature enables remote Contivity VPN Clients to connect their IPsec tunnel sessions in a single step. With Auto Connect, client users simply click on the desired destination, for example, a Web page on the private internal network. This first starts their ISP connection, then makes the tunnel connection to the gateway, and finally makes the connection to the requested destination.

Click on Any Network Traffic to use the autoconnect feature for all client connection requests to authorized destinations. Now, when any network activity is detected on the user's workstation, a tunnel connection is automatically launched to the gateway.

19 Configure the Specify Networks and/or Domains parameters. Click on this selection to limit autoconnection use to specific domains or networks. Specify the authorized domains or networks in the following two fields.

Use the Domains selection to designate specific domains or host names that trigger the autoconnect feature. The domains that you specify must be configured on the Profiles > Domains page. Select None if you want to limit the autoconnection feature to specific networks, which you specify in the following Networks field.

Use the Networks selection to designate specific networks that trigger the autoconnect feature (the networks must be configured on the Profiles > Networks page). Select None if you do not want to designate any networks.

20 Configure the Banner setting. You can customize an enterprise login banner for the Contivity VPN Client by entering text into the space provided. This banner appears at the top of the IPsec client upon login.

21 Enable the Display Banner. Click to enable the banner and have it appear when a remote user logs into the gateway.

22 Set the Client Screen Saver Password Required parameter. Setting this security feature forces the client to use a password in association with a screen saver. When enabled, if the user leaves the system and is connected to a tunnel, the system then gets locked out of the tunnel once the screen saver kicks in. The end user would enable this feature from the Start > Settings > Control Panel > Display > Screen Saver Password Protected box. Default is Disabled.

23 Set the Client Screen Saver Activation Time. This setting is used together with the Client Screen Saver Password Required setting. It defines the maximum time (in minutes) before the client's screen saver is activated. The value on the Client PC can be changed from the Start > Settings > Control Panel > Display > Strengthener Wait list box. Default is 5 Minutes.

24 Configure Client Fail-Over Tuning.

Check the Enabled box to enable client fail-over. Client fail-over uses small packets to check and maintain, or keep alive, the connection between the client and the gateway.

In the Interval section, specify the time interval that the client waits between VPN activity checks. Nortel Networks recommends a low interval when users are connecting via the client. You should use a higher setting for situations such as when a lease line is used and charges are based on traffic.

Specify the maximum number of retransmissions. This is the number of times that the client re-transmits a keepalive packet to the gateway to check for connectivity.

25 You can optionally enable the anti-replay service. While the default handling calls for the sender to increment the Sequence Number used for anti-replay, the service is effective only if the receiver checks the Sequence Number.

➡ **Note:** Anti-Replay must be disabled when using IPSEC tunnels over LANs or WANs (the typical usage). If it is enabled, it causes DiffServ sorting to be incorrect. Anti-Replay does not acknowledge DiffServ and has its own methods of discarding packets, which adversely affects the DiffServ sorting.

26 Set the Allow Password Storage on Client parameter. You can allow client systems to save the login password in its password list, or you can require that the remote user enters the password each time he requests authentication and access to an IPsec tunnel. Click Enable to allow client systems to save the login password.

➡ **Note:** When using certificates, saving the password on the client is not allowed.

27 Configure Compression. Click to enable Compression for IPsec tunneling.

28 Set the Rekey Timeout. You should limit the lifetime of a single key used to encrypt data or else you compromise the effectiveness of a single session key. Use the Rekey Timeout setting to control how often new session keys are exchanged between a client and a server. You should set the Rekey Timeout setting to no less than 1 hour. The default is 08:00:00 (8 hours); a setting of

00:00:00 disables the Rekey Timeout setting. The maximum setting is 23:59:59.

29 Set the Rekey Data Count. You can choose to set a Rekey Data Count depending on how much data you expect to transmit via the tunnel with a single key. Default is 0 Kbytes; a setting of 0 disables the Rekey Data Count.

30 Configure the Domain Name setting. This setting enables you to specify the name of the domain that is used while an IPsec tunnel is connected. Specifying the domain name in this field ensures that domain lookup operations point to the correct domain. This is particularly important for clients that use Microsoft Outlook or Exchange, to ensure that the mail server is mapped to the correct domain.

When a tunnel is connected, the remote client's registry is updated to use the specified domain. When the client disconnects the tunnel, the remote client's original domain is again used.

31 Enter the Primary DNS. Enter the address of the Primary Domain Name System (DNS) server that is located on your private network. This DNS address is provided by the server to tunnel clients at setup and is used through the tunnel. The DNS server translates textual host names into IP addresses for the gateway. For example, DNS can translate the fully qualified host *www.mycompany.com* to its IP address 192.19.2.33.

The Primary DNS server is the first one addressed for servicing name resolution requests from a remote user; if the Primary DNS server is unavailable, service is requested of the Secondary DNS server. Recent versions of Microsoft Windows operating systems can simultaneously query multiple DNS servers. Always use the IP address for setting a DNS server host instead of a domain name.

32 Enter the Secondary DNS. Enter an address for the Secondary Domain Name System (DNS) server. If the Primary DNS server is unavailable, service is requested of the Secondary DNS server.

33 Enter the Primary WINS. Enter an address for the primary Windows Internet Naming Service (WINS) server. A WINS server resolves NetBIOS names (for Windows networking file and print services) to IP addresses. Using a WINS server enables normal Windows file and print services to be accessed correctly through a tunnel connection.

Windows NT Server Version 4.0 and later supports a built-in WINS server. The WINS server eliminates the need to manually map NetBIOS names to IP addresses (for example, using the textual LMHOSTS file on Windows) by updating a name-to-address mapping file dynamically on the WINS server.

The Primary WINS server is the first one addressed for servicing name resolution requests from a remote user; if the Primary WINS server is unavailable, service is requested of the Secondary WINS server. Always use the IP address for setting a WINS server host instead of a name.

Note: If no WINS servers are specified, the client is forced to broadcast for NetBIOS names.

34 Enter an address for the Secondary Windows Internet Naming Service (WINS) server; if the Primary WINS server is unavailable, service is requested of the Secondary WINS server.

35 Configure the Nortel Client Requirements settings.

a In the Minimum Version field, select the minimum version of Contivity VPN Client that is required.

b In the Action field, specify the action to take upon detection of a noncompliant client.

c In the Message field, type a message giving users the URL for a Web site or FTP site from which they can download the required version of the Contivity VPN Client software.

d Select a filter to apply from the list of available filters.

e Click on the New Filter link to create a new filter, if needed.

36 Configure the Client Policy setting. Select a client policy as appropriate. Client Policy helps prevent potential security violations that could occur when you are using the split tunneling feature. Split tunneling allows client data to travel either through a tunnel to the enterprise network or directly to the Internet.

37 Set the Allow IPsec Data Protection parameter. Enable or disable IPsec.

38 Set the Client Dynamic DNS Registration parameter to enable or disable. You can only use this parameter with the Contivity VPN Client. Also, your DNS server must support Dynamic DNS and be configured to allow Dynamic DNS registration.

Configuring branch office connection IPsec settings

To configure branch office IPsec settings:

1 Select Profiles > Branch Office, then click Edit for the associated connection that you want to configure. The Branch Office > Edit Connection screen appears.

2 Use the drop-down list to change the tunnel type for the connection. To configure IPsec settings, select IPsec as the tunnel type. The default type is IPsec.

> **Note:** If you change the Tunnel Type, the fields in the Authentication portion of this screen change to reflect the different configuration requirements for the selected Tunnel Type.

3 Configure the IPsec authentication attributes in the Authentication section of the screen. This portion of the screen allows you to configure the authentication that is used between the local and remote branch office gateways. The fields that appear in this screen depend on whether you are using an IPsec, PPTP, or L2TP tunnel type. The IPsec authentication fields are described in the following steps.

4 Enter the Pre-Shared Key: Text or Hex String. This is an alphanumeric text or hexadecimal string that is used between the local and remote branches for authentication. In order for authentication to occur, you must use the same pre-shared string on both the local and remote branch offices.

5 Configure the Certificates section of the screen. Certificates are associated with each endpoint gateway and allow for mutual authentication between two connections. The certificate portion of the screen includes information about the remote branch office system, the authority that issued the certificate, and the certificate identification.

6 Configure the Remote Identity. This is the name of the remote peer initiating the tunnel connection. You can use either a Subject Distinguished Name (Subject DN) or a Subject Alternative Name to uniquely identify the remote

branch office system. Specifying both a full subject DN and a subject alternative name on this screen allows the remote peer to use either identity form when making a connection.

7 Select a Valid Issuer Certificate Authority from the drop-down list box. This CA is the issuer of the remote peer's certificate or a higher level CA in the remote peer's certificate hierarchy. The CA must have the trusted flag set via the certificates screen. If a CA hierarchy is being used, all intermediary CAs below the trusted CA must have been imported to the gateway. These Certificate Authorities are configured from the System > Certificates: Generate Certificate Request screen.

8 Configure the Subject Distinguished Name. If you are using a distinguished name to identify the remote branch office site, you can choose to enter the DN as either a relative distinguished name or a full distinguished name. The DN entered here must exactly match the DN in the remote peer's certificate.

9 Configure the Relative distinguished name. The Relative distinguished name has the following supported components:

Note: Do not include the attribute type as part of your entries in the Relative section. For example, for a name of CN=Mygateway, your entry would be Mygateway (without the CN attribute type).

- Common Name -- Enter the Common Name with which the server is associated.
- Org Unit -- Enter the Organizational Unit with which the server is associated.
- Organization -- Enter the Organization with which the server is associated.
- Locality -- Enter the Locality in which the server resides.
- State/Province -- Enter the State or Province in which the server resides.
- Country -- Enter the Country in which the user resides.

10 Enter the Full distinguished name. You can directly enter the Full Distinguished Name (FDN) in this field rather than entering the individual components in the previously described Relative distinguished name fields. For example:

```
CN=Mygateway, O=MyCompany, C=US
```

11 Configure the Subject Alternative Name. You can optionally use a Subject Alternative Name in place of a Subject DN, and specify the format of the name. The following formats are acceptable.

- Email Name (for example, net_admin@company.com)
- DNS Name (for example, gateway.cleveland.company.com)
- IP Address (for example, 192.168.34.21)

12 Specify the Local Identity. The Local Identity is the name your gateway that you want to use to identify itself when initiating or responding to a connection request. You can use either a Subject Distinguished Name (Subject DN) or a Subject Alternative Name to uniquely identify your system. If you select a subject alternative name from your gateway's certificate, then that identity is used in place of your gateway's subject DN when communicating with peers.

Note: Your gateway's server certificate only has subject alternative names if your CA issued the certificate with the alternative names. For example, with the Entrust PKI the VPN connector can issue certificates with DNS names, IP addresses, or Email alternative names.

13 Configure the Server Certificate. Click the drop-down list box to view all certificates that have been issued to the server. Server Certificates are configured from the System > Certificates: Generate Certificate Request screen.

Configuring branch office group IPsec settings

To configure branch office group IPsec settings:

1 Select Profiles > Branch Office, then click Edit for the associated group that you want to configure. The Branch Office > Edit Group screen appears.

2 Click Configure in the IPsec section of the Branch Office > Edit Group screen. The Branch Office > Edit Group > Edit IPsec screen appears.

3 Click the Configure button for a specific parameter to make changes to that parameter. Click Configure in the All Fields section to edit all parameters at the same time. Use the Inherited button to set all fields to their inherited values.

4 Configure Encryption. Click Configure, then click the appropriate box to either enable or disable the supported Encryption methods for this group.

➡ **Note:** Triple DES encryption requires more processing power than DES, potentially reducing the performance of the switch. AES provides stronger encryption than 3DES, and requires less processing power than 3DES, providing a potential performance improvement for Branch Office tunnels.

The encryption methods are presented in order of strength, from strongest to weakest. All of the following encryption methods ensure that the packet came from the original source at the secure end of the tunnel. Some of the encryption types do not appear on non-US models that are restricted by US Domestic export laws. Also, MD5 (Message Digest) provides integrity that detects packet modifications.

➡ **Note:** Existing profiles will not be automatically changed to reflect that the global settings have changed. For example, if you change the global settings for IKE Deffie-Hellman Group, it can invalidate IKE Deffie-Hellman Group selections. You must go to Profiles > Groups or Profiles > Branch Office screen to check IKE Deffie-Hellman Group settings in each group. Any IKE Deffie-Hellman Group selected in user groups must also be selected globally.

If two devices have different encryption settings (due to either US export laws or administrative configuration), the two devices negotiate downward until each has a compatible encryption capability. For example, if a client in the US attempts to negotiate Triple DES encryption with a gateway in Australia, then the Australian gateway rejects Triple DES encryption in favor of DES.

5 Select the Diffie-Hellman Group level to apply to IKE (Internet Key Exchange) encryptions.

Note: The choice of the IKE encryption algorithm does not affect the choice of the encryption algorithm used to encrypt data in IPsec. For example, one can use DES to encrypt the IKE exchanges, and then negotiate Triple DES for use in IPsec.

The Services>IPsec screen contains a section labeled “IKE Encryption and Diffie-Hellman Group.” This section provides two choices for use with IPsec.

6 Click to enable Perfect Forward Secrecy (PFS). With PFS, keys are not derived from previous keys. This ensures that one key being compromised cannot result in the compromise of subsequent keys.

7 Click to enable Compression for IPsec tunneling.

8 Specify the Rekey Timeout. You should limit the lifetime of a single key used to encrypt data or else you compromise the effectiveness of a single session key. Use the Rekey Timeout setting to control how often new session keys are exchanged between a client and a server. You should set the Rekey Timeout setting to no less than 1 hour. The default is 08:00:00 (8 hours); a setting of 00:00:00 disables the Rekey Timeout setting. The maximum setting is 23:59:59.

9 Set the Rekey Data Count. You can choose to set a Rekey Data Count depending on how much data you expect to transmit via the tunnel with a single key. Default is 0 Kbytes; a setting of 0 disables the Rekey Data Count.

10 Set the ISAKMP Retransmission Interval. This specifies the time interval at which to make the ISAKMP retransmission.

11 Set the ISAKMP Retransmission Max Attempts parameter. This is the maximum number of attempts to make the ISAKMP retransmission.

12 Set the Keepalive Interval. This is the polling frequency used to determine if a keepalive exchange is needed. The default is one minute. The allowed range is 1 second to 60 minutes. This interval is used when the branch connection is Nailed-Up or when Keepalives are enabled for on-demand connections.

13 Set the Keepalive (on-demand connections) parameter. Keepalive (on-demand connections) has a default of disabled. Enabling this allows for a quicker detection of lost connectivity.

IPsec client features

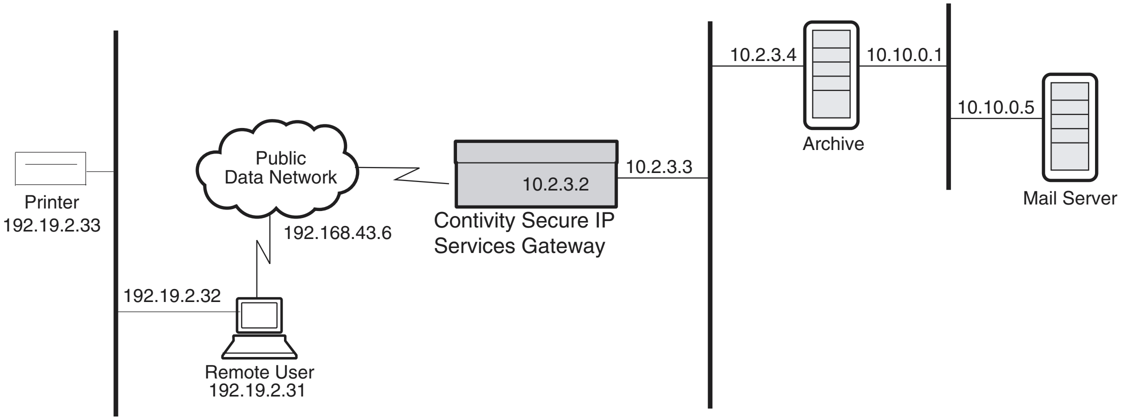
The gateway supports the following IPsec client features:

- Split tunneling
- Third-party IPsec clients
- Forced logout
- Client fail-over
- Client auto connect
- Banner
- Password storage
- Client screen saver
- Client Keepalive
- Domain name
- Client policy

Split tunneling

All IPsec client traffic is tunneled through the gateway by default. Split tunneling allows you to configure specific network routes that are downloaded to the client. Only these network routes are then tunneled; any other traffic goes to the local PC interface. Split tunneling allows you to print locally, for example, even while you are tunneled into the gateway. Figure 1 shows a sample split tunneling environment.

Figure 1 Sample split tunneling environment



The previous figure shows split tunneling enabled and split tunnel network IP addresses 10.2.3.4 and 10.10.0.5. When a client establishes an IPsec tunnel, these addresses are loaded into the client application.

The remote user, for example, then downloads his email from the mail server at 10.10.0.5, and downloads a document from the Archive at 10.2.3.4. Next, without exiting the tunnel, the remote user can print the document through the PC's local network interface 192.19.2.32 to the printer at 192.19.2.33. You can enable split tunneling through the Profiles > Groups > IPsec > Edit screen split tunneling field.

You designate which network routes to tunnel through the gateway from the Profile>Networks screen. Next, you associate specific network routes to specific groups through the Profiles > Groups > IPsec > Edit screen by configuring the Split Tunnel Networks field.

The gateway takes precautions against violators potentially hacking tunneled information when the gateway is operating in split tunneling mode. The primary precaution is to drop packets that do not have the IP address that is assigned to the tunnel connection as its source address. For example, if you have a PPP dial-up connection to the Internet with an IP address of 192.168.21.3, and then you set up a tunneled connection to a gateway and you are assigned a tunnel IP address of 192.192.192.192, then any packets that attempt to pass through the tunnel connection with a source IP address of 192.168.21.3 (or any address other than 192.192.192.192) are dropped.

Furthermore, you can enable filters on the gateway to limit the protocol types that can pass through a tunneled connection.

The Client Selection feature enables you to configure your gateway to accept tunnel connections from third-party clients, in addition to the Nortel Networks Contivity VPN Client.

To completely eliminate security risks, you should not use the split tunneling feature.

Third-party IPsec clients

The client selection feature enables you to configure your gateway to accept tunnel connections from third-party clients, in addition to the Contivity VPN Client.

The Client Selection feature provides more flexibility and mobility than was previously available to remote users who want to connect to your gateway using a client other than the Contivity VPN Client. The alternate method of connecting third-party clients requires you to set up a branch office connection and configure the remote client's IP address as the connection's remote gateway address. This branch office method binds a client machine to a fixed IP address. This can be limiting if a user needs to be able to create tunnels from multiple systems, for example, a work desktop system and a mobile laptop.

With the client selection feature, you establish an account for a remote user, rather than for a remote machine. You set up the account within the realm of remote access users, as has always been done for the Contivity VPN Client users. This gives the remote user the freedom to create tunnels to your gateway from different machines, and from different locations.

When configuring for Contivity VPN Clients, the gateway ignores the "Allow undefined networks for non-Contivity clients" field for clients that are not Contivity clients. The gateway never allows Contivity VPN Clients to connect to undefined networks. All reachable networks must be defined on the Profiles>Networks screen.

When configuring for clients that are not Contivity VPN Clients, the fields that are preceded by an asterisk are not supported. You must select either the Split Tunneling or “Allow undefined networks field for non-Contivity clients” field for clients that are not Contivity VPN Clients. If you select both, the gateway uses the Split Tunneling feature and ignores the “Allow undefined networks” selection.

Note: Nortel Networks recommends that you always specify Split Tunneling for groups used by clients other than Contivity VPN Clients. With Split Tunneling enabled, the third-party clients can only connect to networks that are listed as split tunnel networks on your gateway. This ensures that your gateway has control over the networks that the third-party client can access. If Split Tunneling is disabled and “Allow undefined networks for non-Contivity VPN Clients” is enabled, the clients can connect to all internal networks.

The gateway supports both preshared key and RSA digital signature authentication methods. For clients that are not Contivity VPN Clients, you must specify at least one of these authentication methods on the Services > IPsec screen.

Note: You must ensure that your remote third-party client uses the same Internet Key Exchange (IKE) Phase 1 mode that your gateway uses. For Preshared Key authentication, the gateway uses IKE Aggressive mode. If the client only supports IKE Main mode, it must be configured as a branch office due to the IKE restrictions. For RSA Digital Signature authentication, the gateway uses IKE Main mode.

RADIUS authentication is not supported. Also, you can configure a static address for the tunnel from a client other than a Contivity VPN Client, or you can allow the client to use its own IP address as the address used within the tunnel.

Configuring IPsec client selections

To configure the client selection:

1 Go to the Profiles > Groups > Edit > IPsec screen.

2 Under Forced logout, you can specify a time after which all active users are automatically logged off for IPsec tunneling. The default is 0, which means the option is turned off. The possible range is 00:00:01 to 23:59:59.

3 Client keepalive uses small packets to check and maintain, or keep alive, the connection between the client and the gateway. Use the Contivity VPN Client to disable keepalives between the gateway and the client. This option allows you to disable keepalives when tunneling over an ISDN link, since the link is not always active. If an idle time-out has been set on the gateway, and keepalives have been disabled on the client, the client might not receive notice that the connection has been closed (due to the Idle Time-out), when the physical ISDN connection is not active.

Note: If the idle time-out on the gateway logs off the client, and the client has client fail-over configured on the Services > IPsec screen, that client then fails over to the defined failover server, rather than being disconnected as desired.

When the Keep Alive parameter is disabled on the client it prevents the gateway and client from exchanging keep alive messages. Therefore, if the connection is lost, the gateway does not realize that the client is no longer connected until the idle time is reached. If the idle time-out can be set to Never, the resulting connection could remain established for a long time, which wastes gateway resources.

If the number of Logins is set to 1, which is the default, the client cannot reconnect until the rekey happens, which by default is in 8 hours. If the user has the Disable Keep Alive parameter set on the client, and the connection goes down, the user could be prohibited from reconnecting for 8 hours or more, depending on the rekey value.

Also, do not set the idle time-out to 0. If you lose the connection in this situation, you must delete the session from the gateway to reconnect.

4 When a static branch office tunnel fails, all packets flowing through the tunnel are dropped. The static tunnel failover feature provides a means to detect and recover from these failures. Static tunnel failover interacts with static route API directly to remove and add static routes associated with a remote network. When a tunneling protocol detects a network failure, the static tunnel

API removes static routes associated with the remote network from the route table manager.

Note: When setting up static tunnel failover, you need to configure the primary tunnel as nailed up from the Profiles > Branch Office > Edit > Connectivity screen. It should also have less cost than any secondary tunnels.

5 The client auto connect feature enables remote clients to connect their IPsec tunnel sessions in a single step. This is similar to the way Microsoft Dial-Up Networking automatically connects to an ISP when a Web browser is launched. With auto connect, client users simply click on the desired destination, for example, a Web page on the private internal network. This first starts their dialup connection, then makes the tunnel connection to the gateway, and finally makes the connection to the requested destination. What has, in the past, taken three distinct user operations is now accomplished by a single action.

The client auto connect settings specify those network connections that trigger the client's autoconnect feature. For example, you can specify that whenever a remote client attempts to connect to a site in the xyz.com domain, the client auto connect feature is started.

You must make sure that the gateway is configured to allow connections to potential destinations. If the gateway is not configured properly, the remote user might be able to make the connection to the gateway, but cannot access the requested destination. For example, the gateway's filters might be set up to deny access to finance.xyz.com, while the client auto connect is configured to start when connections to the xyz.com domain are received. With this configuration, when a remote client tries to access finance.xyz.com, their connection to their ISP and then to the gateway is automatically started. However, because of the filters, access to finance.xyz.com is denied.

Note: After you enable client auto connect, you must reboot the PC on which the client is running and manually make sure the client can connect to the gateway.

When the client successfully connects to the gateway, the gateway downloads the list of networks and domains that trigger the autoconnect feature. This list, which is stored in the client's registry, is used to determine whether a tunnel connection should automatically be started when one is not already active.

The following client features apply only to the Contivity VPN Client:

- Banner--You can customize an enterprise login banner for the Contivity VPN Client by entering text into the space provided. This banner appears at the top of the IPsec client upon login.
- Password storage on client--You can allow client systems to save the login password in this password list, or you can require that a remote user enter the password with each request for authentication and access to an IPsec tunnel. Click on Enable to allow client systems to save the login password. When using certificates, saving the password on the client is not allowed.
- Client policy--Client policy helps prevent potential security violations that could occur when you are using the split tunneling feature. Split tunneling allows client data to travel either through a tunnel to the enterprise network or directly to the Internet.
- Client screen saver--Setting this security feature forces the client to use a password in association with the screen saver. When it is enabled, if the user leaves the system while connected to a tunnel, the system then gets locked out of the tunnel when the screen saver kicks in.
- Domain name--This setting enables you to specify the name of the domain used while an IPsec tunnel is connected. Specifying the domain name in this field ensures that domain lookup operations point to the correct domain. This is particularly important for clients that use Microsoft Outlook or Exchange, to ensure that the mail server is mapped to the correct domain. When a tunnel is connected, the remote client's registry is updated to use the specified domain. When the client disconnects the tunnel, the remote client's original domain is again used.

Chapter 3 Configuring PPTP

The Point-to-Point Tunneling Protocol (PPTP) is supported by Nortel Networks and several other vendors. The Microsoft PPTP client is available for Windows* 95, Windows NT Workstation (Version 4.0), Windows ME, and Windows NT* Server (except Version 3.51). The Microsoft PPTP client is bundled with Windows 98 software. Network TeleSystems (www.nts.com) provides tunneling product support for Windows 3.1 and Macintosh* operating systems.

You can obtain the PPTP client upgrade for Windows 95 directly from Microsoft (www.microsoft.com). Installation instructions are also available from this site.

The PPTP client software is on the Contivity Secure IP Services Gateway CD and is built into the Windows NT operating system. PPTP offers the following features:

- Connections can be made from a range of clients without requiring special ISP services.
- The PPTP client is available for the most common client operating systems.
- PPTP supports IP address translation using encapsulation, support for IPX tunneling, and RC4 encryption (either 56- or 128-bit, within the limits of United States export law).

Nested tunnels allow you to create a PPTP end user tunnel inside an IPSec branch office tunnel or an asynchronous branch office tunnel. You can have a nested tunnel from within the private network or from the public side. You can individually log off nested tunnel sessions from the Status > Sessions > Active Session screen.

Configuring PPTP settings

You can change the default values for PPTP settings at any of these levels:

- Services > PPTP
- Profiles > Groups > Edit > PPTP Settings
- Profiles > Branch Office > Edit Connection > PPTP Tunnel Type

To change global PPTP settings:

1 Select Services > PPTP from the Contivity Secure IP Services Gateway menu.

2 Configure the Authentication settings. PPTP settings allow you to select a specific authentication server type, for example, RADIUS. Each server type allows you to specify an authentication scheme: MS-CHAP, CHAP, PAP, None or PAP or CHAP.

> **Note:** Not all RADIUS servers support all forms of authentication. Failure to match PPP authentication methods with RADIUS server capabilities results in user-authentication failures. Check your vendor's RADIUS documentation for additional information.

3 Configure the PPP Multilink setting. Use the list box to toggle the PPP Multilink between enabled and disabled. PPP Multilink allows a user to open multiple PPP connections to a given host. (Refer to RFC 2701 for a complete description of PPP Multilink.)

4 Configure the Authentication Order. The Authentication Order table lists the corresponding servers, authentication types, associated groups, and actions. The LDAP server is always queried first, then RADIUS, if applicable.

Configuring group PPTP settings

To change group PPTP settings:

1 Select Profiles > Groups, then click Edit for the associated group that you want to configure.

2 Click Configure in the PPTP section of the screen. The PPTP screen appears.

3 Click the Configure button for a specific parameter to make changes to that parameter. Click Configure in the All Fields section to edit all parameters at the same time. Use the Inherited button to set all fields to their inherited values.

4 Select one or more of the PPTP Authentication methods.

5 Configure the compression setting. Click to enable the PPTP Microsoft Point-to-Point Compression (MPPC) packet compression. Compression should be used when encryption is selected on analog modems. This is because encryption renders a modem's compression ineffective, and it can severely affect the performance of compressible applications. Also, data that is compressed before being transmitted makes more efficient use of lower speed network links.

You should use data compression in most typical situations. Users with cable modems or *x*DSL connections to the ISP, or locally on the LAN, would find it is probably unnecessary to compress packets. This is because the speed of the link, relative to the rate of compression and the benefit of compressing before encrypting, might be negligible or might not increase performance.

Also, some data cannot be compressed; for example, a previously compressed file does not lend itself well to additional compression.

6 Set the Use Client-Specified Address parameter. Click to enable use of a Client-Specified Address. This option allows the gateways to accept the IP address from a remote user's system during tunnel setup. This option is Disabled by default.

When enabled and the client provides an IP address, this is the IP address that is used by the client for the duration of the tunneled session (it becomes the first or default choice).

7 Enter the Primary DNS. Enter the address of the Primary Domain Name System (DNS) server that is located on your private network. This DNS address is provided by the server to tunnel clients at setup and is used through the tunnel. The DNS server translates textual host names into IP addresses for the gateways. For example, DNS can translate the fully qualified host *www.mycompany.com* to its IP address 192.19.2.33.

The Primary DNS server is the first one addressed for servicing name resolution requests from a remote user; if the Primary DNS server is unavailable, service is requested of the Secondary DNS server. Recent versions of Microsoft Windows operating systems can simultaneously query multiple DNS servers.

Always use the IP address for setting a DNS server host instead of a domain name.

8 Enter the Secondary DNS. Enter an address for the Secondary Domain Name System (DNS) server. If the Primary DNS server is unavailable, service is requested of the Secondary DNS server.

9 Enter the Primary WINS. Enter an address for the primary Windows Internet Naming Service (WINS) server. A WINS server resolves NetBIOS names (for Windows networking file and print services) to IP addresses. Using a WINS server enables normal Windows file and print services to be accessed correctly through a tunnel connection.

Windows NT Server Version 4.0 and later supports a built-in WINS server. The WINS server eliminates the need to manually map NetBIOS names to IP addresses (for example, using the textual LMHOSTS file on Windows) by updating a name-to-address mapping file dynamically on the WINS server.

The Primary WINS server is the first one addressed for servicing name resolution requests from a remote user; if the Primary WINS server is unavailable, service is requested of the Secondary WINS server. Always use the IP address for setting a WINS server host instead of a name.

Note: If no WINS servers are specified, the client is forced to broadcast for NetBIOS names.

10 Enter an address for the Secondary Windows Internet Naming Service (WINS) server; if the Primary WINS server is unavailable, service is requested of the Secondary WINS server.

Configuring branch office connection PPTP settings

To change PPTP settings for a branch office connection:

1. Select Profiles > Branch Office, then click Edit for the associated connection that you want to configure.
2. To configure PPTP settings, select PPTP as the tunnel type.
3. Select one of the PPTP Authentication methods. Click the drop-down list and select the authentication method that you want to use for the branch office connection.

> **Note:** When you change the Authentication Type, the screen immediately changes to reflect the requirements of the new authentication method. Any changes that you might have made on the Authentication part of the previous screen are lost.

4. Enter the local user ID and password for the local gateways that you are configuring.
5. Enter the user ID of the remote gateways that you are configuring in the Peer field.
6. Enter the password for the UID, then confirm the password to verify that you entered it correctly. If you selected a variation of MS-CHAP V2 authentication, no password is required for the Local UID.
7. Select a Compression setting. Click to Enable or Disable compression. Click to enable the IPsec Hi/fn LZS compression or the PPTP, L2TP, or L2F Microsoft Point-to-Point Compression (MPPC) packet compression. Compression should be used when encryption is selected on analog modems. This is because encryption renders a modem’s compression ineffective, and it can severely affect the performance of compressible applications. Also, data that is compressed before being transmitted makes more efficient use of lower speed network links.
8. Select the Compression/encryption stateless mode. Click to Enable or Disable this selection. This selection is not used if encryption and compression are both disabled.

Chapter 4
Configuring L2TP

Layer 2 Tunneling Protocol (L2TP) is supported by Nortel Networks and other vendors. L2TP combines the best features of the L2F and PPTP tunneling protocols. L2TP tunneling allows secure remote access to corporate networks across the public Internet. L2TP tunnels are generally established between a network access server (NAS) at the ISP and the gateway.

L2TP allows you to specify MS-CHAP, CHAP, or PAP authentication, enable compression, and assign DNS and WINS servers to the tunnel.

You can use IPsec transport-protected L2TP tunneling for both remote access traffic and branch office tunnel traffic. Windows 2000 can act as a peer in a branch office connection using L2TP/IPsec or IPsec tunnel mode. Also, Windows 2000 can act as a client using L2TP/IPsec. Authentication for L2TP/IPsec tunnels can be either shared secret or digital certificate. It also provides configuration support for both voluntary and compulsory L2TP/IPsec remote access connections. (Windows 2000 authentication must be digital certificate.)

The gateway supports IPsec transport mode to support the termination of Microsoft Windows 2000 L2TP/IPsec connections and to provide security for L2TP traffic for client-to-gateway connections and gateway-to-gateway connections.

Note: You must use stateless mode for L2TP tunnels if you have an environment where packets might be lost. Stateful mode forces the tunnel to drop more packets once a packet loss is detected. Multicast does not work over a Contivity gateway OSPF L2TP tunnel through a Cisco router.

Configuring L2TP settings

L2TP parameters are configured on a global level on the Services > L2TP screen and individually for groups and branch office connections from the Profiles menu.

- Global IPsec

  L2TP is configured globally on the Services > L2TP screen.

- Group L2TP

  Group L2TP settings are configured on the Profiles > Groups > Edit > L2TP screen.

- Branch Office Connection L2TP

  Branch office connection L2TP settings are configured on the Profiles > Branch Office > Edit Connection screen.

To change global L2TP settings:

1 Select Services > L2TP. The Services > L2TP screen appears.

2 Configure L2TP authentication. L2TP settings allow you to select a specific authentication server type; for example, RADIUS. Each server type allows you to specify an authentication scheme: MS-CHAP, CHAP, PAP, None or PAP or CHAP.

> **Note:** Not all RADIUS servers support all forms of authentication. Failure to match PPP authentication methods with RADIUS server capabilities results in user-authentication failures. Check your vendor's RADIUS documentation for additional information.

3 To enable PPP Multilink, select Enabled in the list box.

4 Configure L2TP Authentication Order. The Authentication Order table lists the corresponding servers, authentication types, associated groups, and actions. The LDAP server is always queried first, then RADIUS, if applicable.

5 Configure L2TP Access Concentrators.

- Delete–Click to remove the configured concentrator. You are prompted to confirm your deletion request.
- Add–Click to go to the Add L2TP Access Concentrator screen.

- Edit–Click to go to the Edit L2TP Access Concentrator screen and modify the settings of an existing concentrator.

The L2TP Add Access Concentrators screen allows you to configure the authentication between the gateway and the NAS. Use the Edit Access Concentrators screen to modify the information for an existing concentrator.

Configuring group L2TP settings

To change group level L2TP settings:

1. Select Profiles > Groups, then click Edit for the associated group that you want to configure. The Edit Group screen appears.
2. Click Configure in the L2TP section of the screen. The Groups > Edit > L2TP screen appears.
3. Click the Configure button for a specific parameter to make changes to that parameter. Click Configure in the All Fields section to edit all parameters at the same time. Use the Inherited button to set all fields to their inherited values.
4. Select one or more of the L2TP Authentication methods.
5. Configure the compression setting. Click to enable the L2TP Microsoft Point-to-Point Compression (MPPC) packet compression. Compression should be used when encryption is selected on analog modems. This is because encryption renders a modem’s compression ineffective, and it can severely affect the performance of compressible applications. Also, data that is compressed before being transmitted makes more efficient use of lower speed network links.

   You should use data compression in most situations. Users with cable modems or *x*DSL connections to the ISP, or locally on the LAN, would find it is probably unnecessary to compress packets. This is because the speed of the link, relative to the rate of compression and the benefit of compressing before encrypting, might be negligible or might not increase performance.

   Also, some data cannot be compressed; for example, a previously compressed file does not lend itself well to additional compression.

6. Set the Use Client-Specified Address parameter. Click to enable use of a Client-Specified Address. This option allows the gateway to accept the IP address from a remote user's system during tunnel setup. This option is Disabled by default.

   When enabled and the client provides an IP address, this is the IP address that is used by the client for the duration of the tunneled session (it becomes the first or default choice).

7. Enter the Primary DNS. Enter the address of the Primary Domain Name System (DNS) server that is located on your private network. This DNS address is provided by the server to tunnel clients at setup and is used through the tunnel. The DNS server translates textual host names into IP addresses for the gateway. For example, DNS can translate the fully qualified host *www.mycompany.com* to its IP address 192.19.2.33.

   The Primary DNS server is the first one addressed for servicing name resolution requests from a remote user; if the Primary DNS server is unavailable, service is requested of the Secondary DNS server. Recent versions of Microsoft Windows operating systems can simultaneously query multiple DNS servers.

   Always use the IP address for setting a DNS server host instead of a domain name.

8. Enter the Secondary DNS. Enter an address for the Secondary Domain Name System (DNS) server. If the Primary DNS server is unavailable, service is requested of the Secondary DNS server.

9. Enter the Primary WINS. Enter an address for the primary Windows Internet Naming Service (WINS) server. A WINS server resolves NetBIOS names (for Windows networking file and print services) to IP addresses. Using a WINS server enables normal Windows file and print services to be accessed correctly through a tunnel connection.

   Windows NT Server Version 4.0 and later supports a built-in WINS server. The WINS server eliminates the need to manually map NetBIOS names to IP addresses (for example, using the textual LMHOSTS file on Windows) by updating a name-to-address mapping file dynamically on the WINS server.

   The Primary WINS server is the first one addressed for servicing name resolution requests from a remote user; if the Primary WINS server is unavailable, service is requested of the Secondary WINS server. Always use the IP address for setting a WINS server host instead of a name.

➡ **Note:** If no WINS servers are specified, the client is forced to broadcast for NetBIOS names.

10 Enter an address for the Secondary Windows Internet Naming Service (WINS) server; if the Primary WINS server is unavailable, service is requested of the Secondary WINS server.

Configuring branch office connection L2TP settings

To change L2TP settings for a branch office connection:

1 Select Profiles > Branch Office, then click Edit for the associated connection that you want to configure. The Branch Office > Edit Connection screen appears.

2 To configure L2TP settings, select L2TP as the tunnel type.

3 Select one of the L2TP Authentication methods. Click the drop-down list and select the authentication method that you want to use for the branch office connection.

➡ **Note:** When you change the Authentication Type, the screen immediately changes to reflect the requirements of the new authentication method. Any changes that you might have made on the Authentication part of the previous screen are lost.

4 Enter the local user ID and password for the local gateway that you are configuring.

5 Enter the user ID of the remote gateway that you are configuring.

6 Enter the password for the UID, then confirm the password to verify that you entered it correctly. If you selected a variation of MS-CHAP V2 authentication, no password is required for the Local UID.

7 Select a Compression setting. Click to enable the L2TP Microsoft Point-to-Point Compression (MPPC) packet compression. Compression

should be used when encryption is selected on analog modems. This is because encryption renders a modem’s compression ineffective, and it can severely affect the performance of compressible applications. Also, data that is compressed before being transmitted makes more efficient use of lower speed network links.

8 Select the Compression/encryption stateless mode. Click to Enable or Disable this selection. This selection is not used if encryption and compression are both disabled.

9 Select an L2TP access concentrator. Use this entry to specify the L2TP Access Concentrator that you want to perform authentication between the gateway and the NAS. You can use the New L2TP Access Concentrator link to jump to the screen where you can create a new access concentrator.

10 Select an IPsec data protection level.

Configuring L2TP over IPsec

Windows 2000 supports only L2TP with IPsec transport mode for remote access or branch office. (L2TP cannot be used without IPsec.) It supports only RSA Digital Certificates for IPsec transport authentication with the gateway. Windows 2000 Professional Server or Advanced Server can act as a Windows 2000 L2TP/IPsec client to a gateway server.

To configure L2TP over IPsec on the gateway:

1 Configure an L2TP user account on the gateway through the Profiles > Users page and enter an L2TP user ID and password.

2 Before doing any per-user configuration, the gateway must be issued a certificate and must have the issuer’s certificate installed.

   a Generate a certificate request from the System > Certificates page. This request can be transferred to a CA server that issues the certificate. The certificate can then be installed from the same page.

   b You must also install the CA server’s certificate on the gateway through the System > Certificates page. If the Windows 2000 certificate is issued by a different CA, you must also install its certificate.

3 Configure an IPsec transport account on the gateway in one of three ways:

- Configure the Subject DN or Alternate Subject Name of the Windows 2000 certificate on the same page as the L2TP user account. Pull down the Valid Issuer Certificate Authority and select the CA who issued the Windows 2000 certificate. Pull down the Server Certificate and choose the gateway's certificate to be returned to Windows 2000. Windows 2000 checks the issuer's certificate also, so choose a certificate issued by a CA that Windows 2000 knows about. You may also check the Require Own IPsec Credentials now if you want to ensure that this L2TP user always uses this IPsec transport account.
- Go to the System > Certificates page and select the Enable Allow All Feature check box. For the CA that issued the Windows 2000 certificate, select the Allow All Enabled check box. Select a user group from the Default Group pull-down. Be sure the user group selected has Allow IPsec Transport enabled and configured (not inherited) in its IPsec group properties. This configuration is very useful when L2TP user accounts are in RADIUS, since no L2TP or IPsec transport information needs to be stored in the LDAP server per user.
- Create a separate user that contains the IPsec transport account. Set up the account as described in the first option. Do not check the Require Own IPsec Credentials for either this user or the L2TP user. This configuration is supported mainly for L2TP user accounts that are in RADIUS or compulsory tunneling (many L2TP users sharing an IPsec transport connection). Alternatively (for testing), you could install a single certificate on multiple Windows 2000 PCs, in which case they would be sharing a single IPsec transport account. Windows 2000 does not support compulsory tunneling.

4 Configure the L2TP profile for the user:

a At a minimum, you must set the desired minimum data protection level for the user. L2TP traffic arriving through an IPsec transport that does not meet this requirement is discarded. This is done in the L2TP properties of the group and therefore applies to all L2TP users under this group. No checking is done to determine whether the selection makes sense. For example, selecting 3DES as the minimum protection level implies that 3DES must be able to be negotiated with the Windows 2000 PC. To do this, DES must be enabled in the Services... IPsec page, must be enabled in the IPsec properties of the group containing the IPsec transport account, and must be configured on the Windows 2000 machine as an acceptable encryption type. Table 1 describes the mapping of minimum data protection levels.

Table 1 Mapping minimum data protection levels to encryption levels

Minimum data protection level	**Encryption levels**
128-bit AES	ESP-AES with SHA1 Integrity
Triple DES	ESP-Triple DES with SHA1 Integrity ESP-Triple DES with MD5 Integrity
56-bit DES	ESP-Triple DES with SHA1 Integrity ESP-Triple DES with MD5 Integrity ESP-56-bit DES with SHA1 Integrity ESP-56-bit DES with MD5 Integrity
40-bit DES	ESP-Triple DES with SHA1 Integrity ESP-Triple DES with MD5 Integrity ESP-56-bit DES with SHA1 Integrity ESP-56-bit DES with MD5 Integrity ESP-40-bit DES with SHA1 Integrity ESP-40-bit DES with MD5 Integrity
Authentication only	ESP-Triple DES with SHA1 Integrity ESP-Triple DES with MD5 Integrity ESP-56-bit DES with SHA1 Integrity ESP-56-bit DES with MD5 Integrity ESP-40-bit DES with MD5 Integrity ESP-40-bit DES with SHA1 Integrity ESP-NULL (Authentication Only) with SHA1 Integrity ESP-NULL (Authentication Only) with MD5 Integrity AH-Authentication Only (HMAC-SHA1) AH-Authentication Only (HMAC-MD5)

Table 1 Mapping minimum data protection levels to encryption levels (continued)

Minimum data protection level	Encryption levels
Not required	ESP-Triple DES with SHA1 Integrity ESP-Triple DES with MD5 Integrity ESP-56-bit DES with SHA1 Integrity ESP-56-bit DES with MD5 Integrity ESP-40-bit DES with SHA1 Integrity ESP-40-bit DES with MD5 Integrity ESP-NULL (Authentication Only) with SHA1 Integrity ESP-NULL (Authentication Only) with MD5 Integrity AH-Authentication Only (HMAC-SHA1) AH-Authentication Only (HMAC-MD5) Data is allowed through even if it does not come through an IPsec transport with this data protection level.

b If the Require Own IPsec Credentials check box is not selected on the L2TP user page, Require IPsec Credentials from Group must select a user group that contains a set of allowed IPsec transport accounts. These IPsec transport accounts may be contained at any level below this group. L2TP traffic that arrives through an IPsec transport not contained in this group is discarded.

c Turn on compression in the L2TP group properties if compression is desired. Compression for the PPP traffic is done if both the gateway and Windows 2000 agree that compression is enabled. Windows 2000 does not support compression at the IPsec transport level.

d Authentication may be MSCHAPV1, MSCHAPV2, CHAP, or PAP. Of these, Windows 2000 prefers to perform MSCHAPV2 followed by MSCHAPV1 followed by CHAP followed by PAP. Windows 2000 does sure the Not Encrypted check box is also enabled.

5 Configure the IPsec transport profile by making sure Allow IPsec Transport is enabled in the group containing the IPsec transport account.

6 By default, Windows 2000 does not have Perfect Forward Secrecy (PFS) enabled. It is enabled by default on the gateway. These two settings are not compatible and generate an appropriate error indicating such in the event log when a connection is attempted. To disable PFS on the gateway, go to the IPsec properties of the IPsec transport group and disable PFS.

Windows 2000 configuration

Windows 2000 Professional, Server or Advanced Server may act as a Windows 2000 L2TP/IPsec client to a gateway server. The steps for configuring the Windows 2000 side of this follow. To install a certificate on the Windows 2000 PC using a Windows 2000 Microsoft CA, connect to a CA server and get a certificate. This involves pointing a browser at the CA server with the URL <*IP address*>/certsrv.

1. Choose Request a Certificate.
2. Choose Advanced request.
3. Submit a certificate request to this CA using a form.
4. On the form provide the identifying information. This becomes the subject DN in the certificate that is entered on the gateway IPsec transport account.
5. Choose IPsec Certificate as the Intended Purpose.
6. Select Use local machine store under Key Options.
7. When the certificate has been issued at the CA server, return to the first page.
8. Choose Check on a pending certificate.
9. Click Install this certificate. This installs the certificate in the local computer certificate store. To view this store, run the mmc command from the Start > Run prompt. Select Console > Add/Remove Snap-in. From the list of snap-ins, choose Certificates and select Computer account. At the console, expand Personal > Certificates under Certificates (Local Computer). The installed certificate should appear. Clicking on it brings up an information window that indicates its validity and that a private key exists for this certificate.

To install the CA server certificate for the Windows 2000:

1. If the gateway's certificate was issued by a different CA, that server's certificate should also be installed. For the Microsoft CA, go back to the home page and select Retrieve the CA certificate or certificate revocation list.
2. Click on the Install this CA certification path. This installs the CA certificate as a trusted CA, which can be seen in mmc under Trusted Root Certificates > Certificates.

To set up the dial-up networking entry to use L2TP over IPsec:

1. Click on My Computer and click on Network and Dial-up Connections. Click on Make New Connection.
2. Choose Connect to a private network through the Internet for the network connection type.
3. Enter the interface address of the gateway server.
4. Edit the properties of this new connection and select the Networking tab. Change the Type of VPN server to L2TP.
5. Connect to the gateway using the L2TP user ID and password entered on the gateway. The certificate installed previously is automatically used to set up the IPsec transport connection.

Configuring branch office for L2TP over IPsec

Windows 2000 Server or Advanced Server may act as a Windows 2000 L2TP/IPsec gateway to a gateway. Both static routing and dynamic (RIP and OSPF) routing are possible through this branch connection.

To configure the gateway:

1. Configure an L2TP branch connection on the gateway. Go to Profiles > Branch Office.
2. Enter the IP address of the Windows 2000 server as the remote endpoint. Select L2TP as the tunnel type.
3. Choose MS-CHAPV2 unencrypted as the authentication type.
4. Enter a local UID for the gateway.
5. Enter a peer UID for Windows 2000.
6. Enter a shared password.
7. Select L2TP if you want compression. As with remote access, compression is not supported on Windows 2000 for the IPsec transport connection.
8. If you want L2TP tunnel authentication supported, you must provide an L2TP Access Concentrator definition. Windows 2000 does not support L2TP tunnel authentication.

9 Select the minimum data protection level. If you select anything other than Not Required, you must set up an IPsec account. Mappings of data protection levels to encryption levels are exactly as shown in Table 1 on page 54.

10 As with remote access, the IPsec transport account must be set up. By default, Windows 2000 supports only certificate authentication, so a process exactly like that described for remote access must be performed. The CA Allow All authentication option is not available for branch office connections. The L2TP branch office must use the IPsec transport account specified in the connection if data protection is required.

11 You can set up routing as either static or dynamic.

To configure Windows 2000:

1 You must install a certificate for Windows 2000 and the CA certificates as described above.

2 Start the Routing and Remote Access administrative tool.

3 Right-click on Routing Interfaces and choose New Demand-dial Interface.

4 Choose the name of the branch connection. This name becomes the L2TP user ID of the gateway. MSCHAPV2 is case sensitive for user IDs. To ensure interoperability with the gateway, use lowercase user IDs.

5 Select Connect using VPN.

6 Select L2TP as the VPN type.

7 Enter the interface address of the gateway.

8 Select Route IP packets on this interface and select Add a user account so a remote router can dial in.

9 Select a password for the gateway L2TP user ID. If the gateway initiates branch office connections to Windows 2000, this password must match that entered on the gateway Branch Office Connection page. If not, then this password does not matter.

10 Choose the Windows 2000 L2TP user ID and the shared password. If the Windows 2000 initiates branch office connections to the gateway, this password must match that entered on the gateway Branch Office Connection page. The Domain field may be left blank.

11 The gateway supports only MSCHAPV2 as a branch office L2TP authentication method, so be sure you enable this method in the properties (it is by default).

12 If you want static routes to demand dial on this connection, expand IP Routing > Static Routes and right-click on New Static Route. Select the interface just created and enter the subnet information. Be sure you enable Use this route to initiate demand-dial connections. Alternatively, you can dial the connection by right-clicking on it and selecting Connect.

Chapter 5
Configuring L2F

The L2F (Layer 2 Forwarding) tunneling protocol is supported by Nortel Networks and other vendors. L2F tunneling allows remote access to corporate networks across the public Internet. L2F tunnels are generally established between the network access server at the ISP and the Contivity Secure IP Services Gateway.

There is no direct client software required for L2F beyond the PPP dialer software, such as the dial-up networking utility provided with Windows 95 and Windows 98. L2F tunnels are actually made from the ISP to the corporate gateway on behalf of the user. These connections depend on the domain associated with the dial-in username. Therefore, ISPs must offer services that are based on L2F; currently, L2F is available on a limited basis. L2F provides IP address translation using encapsulation and support for IPX tunneling, but it does not perform encryption. L2F offers the following features:

- Requires special ISP services
- No requirement for special software on the client
- No data encryption

Configuring L2F settings

L2F parameters are configured on a global level on the Services > L2F screen and individually for groups, users, and branch offices from the Profiles menu.

- Global L2F

  L2F is configured globally on the Services > L2F screen.
- Group L2F

Group L2F settings are configured on the Profiles > Groups > Edit > L2F screen.

Configuring global L2F settings

To change global L2F settings:

1. Select Services > L2F. The L2F Settings screen appears.
2. Configure L2F authentication. L2F allows you to add a RADIUS server for authentication. The Authentication portion of this screen allows you to specify an authentication scheme of either CHAP or PAP.
3. Configure the L2F authentication order. The Authentication Order table lists the corresponding servers, authentication types, associated groups, and actions. The LDAP server is always queried first, then RADIUS, if applicable.
4. Configure Network Access Servers. This table provides the UIDs for the network access servers (NAS) and gateway, and the possible Actions you can take. The NAS acts like a middleman between the remote user and the gateway. It authenticates each side, and once validation is complete, a tunnel is formed. The user has a standard connection (for example, PPP) to the NAS, but an L2F tunnel is formed between the NAS and the gateway.

Configuring group L2F settings

To change group L2F settings:

1. Select Profiles > Groups, then click Edit for the associated group that you want to configure. The Edit Group screen appears.
2. Click Configure in the L2F section of the screen. The Groups > Edit > L2F screen appears.
3. Select one or more of the L2F Authentication methods.
4. Configure the compression setting. Click to enable the L2F Microsoft Point-to-Point Compression (MPPC) packet compression. Compression should be used when encryption is selected on analog modems. This is because encryption renders a modem’s compression ineffective, and it can

severely affect the performance of compressible applications. Also, data that is compressed before being transmitted makes more efficient use of lower speed network links.

You should use data compression in most typical situations. Users with cable modems or *x*DSL connections to the ISP, or locally on the LAN, would find it is probably unnecessary to compress packets. This is because the speed of the link, relative to the rate of compression and the benefit of compressing before encrypting, might be negligible or might not increase performance.

Also, some data cannot be compressed; for example, a previously compressed file does not lend itself well to additional compression.

5 Set the Use Client-Specified Address parameter. Click to enable use of a Client-Specified Address. This option allows the gateway to accept the IP address from a remote user's system during tunnel setup. This option is Disabled by default.

When enabled and the client provides an IP address, this is the IP address that is used by the client for the duration of the tunneled session (it becomes the first or default choice).

6 Enter the Primary DNS. Enter the address of the Primary Domain Name System (DNS) server that is located on your private network. This DNS address is provided by the server to tunnel clients at setup and is used through the tunnel. The DNS server translates textual host names into IP addresses for the gateway. For example, DNS can translate the fully qualified host *www.mycompany.com* to its IP address 192.19.2.33.

The Primary DNS server is the first one addressed for servicing name resolution requests from a remote user; if the Primary DNS server is unavailable, service is requested of the Secondary DNS server. Recent versions of Microsoft Windows operating systems can simultaneously query multiple DNS servers.

Always use the IP address for setting a DNS server host instead of a domain name.

7 Enter the Secondary DNS. Enter an address for the Secondary Domain Name System (DNS) server. If the Primary DNS server is unavailable, service is requested of the Secondary DNS server.

8 Enter the Primary WINS. Enter an address for the primary Windows Internet Naming Service (WINS) server. A WINS server resolves NetBIOS names (for Windows networking file and print services) to IP addresses. Using a WINS server enables normal Windows file and print services to be accessed correctly through a tunnel connection.

Windows NT Server Version 4.0 and later supports a built-in WINS server. The WINS server eliminates the need to manually map NetBIOS names to IP addresses (for example, using the textual LMHOSTS file on Windows) by updating a name-to-address mapping file dynamically on the WINS server.

The Primary WINS server is the first one addressed for servicing name resolution requests from a remote user; if the Primary WINS server is unavailable, service is requested of the Secondary WINS server. Always use the IP address for setting a WINS server host instead of a name.

Note: If no WINS servers are specified, the client is forced to broadcast for NetBIOS names.

9 Enter an address for the Secondary Windows Internet Naming Service (WINS) server; if the Primary WINS server is unavailable, service is requested of the Secondary WINS server.

Index