Version 5.00

Part No. 315897-D Rev 00
June 2004

600 Technology Park Drive
Billerica, MA 01821-4130

Configuring Servers, Authentication, and Certificates 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.

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

Figures

Tables

Preface

This guide provides instructions for configuring LDAP and RADIUS authentication, RADIUS accounting, and certificates on the Nortel Networks* Contivity* Secure IP Services Gateway.

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 the 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.

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 Firewalls, Filters, NAT, and QoS for the Contivity Secure IP Services Gateway* provides instructions for configuring the Contivity Stateful Firewall and Contivity interface and tunnel filters.
- *Configuring Advanced Features for the Contivity Secure IP Services Gateway* provides instructions for configuring advanced LAN and WAN settings, PPP, frame relay, PPPoE, ADSL and ATM, T1CSU/DSU, dial services and BIS, DLSw, IPX, and SSL VPN.
- *Configuring Tunneling Protocols for the Contivity Secure IP Services Gateway* configuration information for the tunneling protocols IPsec, L2TP, PPTP, and L2F.
- *Configuring Routing for the Contivity Secure IP Services Gateway* provides instructions for configuring RIP, OSPF, and VRRP, as well as instructions for configuring ECMP, routing policy services, and client address redistribution (CAR).
- *Managing and Troubleshooting the Contivity Secure IP Services Gateway* provides information about system administrator tasks such as backup and recovery, file management, and upgrading software, and instructions for monitoring gateway status and performance. Also, provides troubleshooting information and inter operability considerations.
- *Reference for the Contivity Secure IP Services Gateway Command Line Interface* provides syntax, descriptions, and examples for the commands that you can use from the command line interface.
- *Configuring 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.

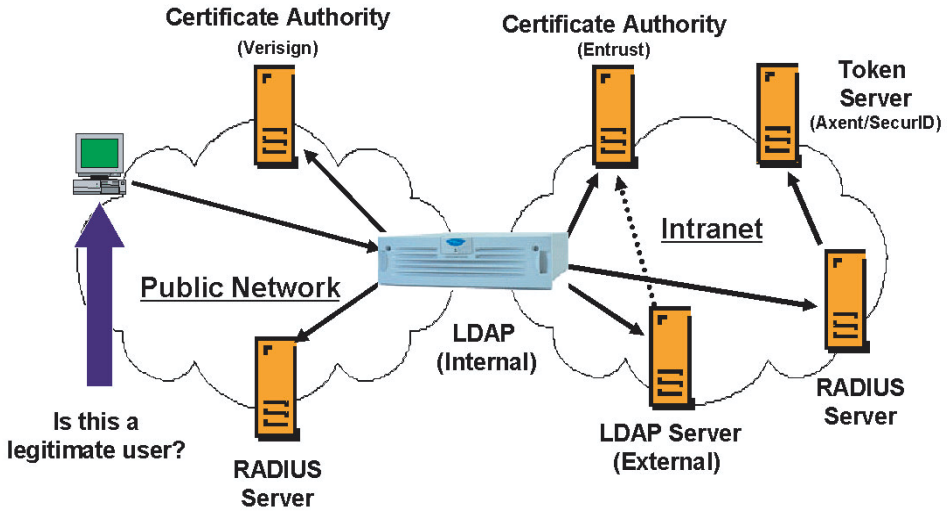
An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the http://www.nortelnetworks.com/help/contact/erc/index.html URL.

Chapter 1
Authentication services

The remote user attempting to dial in to the Contivity gateway must be authenticated before gaining access to the corporate network. Authentication is one of the most important functions that the Contivity gateway provides because it identifies users and drives many other aspects of the user-centric functionality.

For authentication and access control, the Contivity gateway supports an internal or external Lightweight Directory Access Protocol (LDAP) server and external Remote Authentication Dial-In User Services (RADIUS) servers. External LDAP proxy server support allows authentication of users against existing LDAP databases.

Figure 1 Authenticating users



The Contivity gateway augments support for several authentication services with a group profile mechanism. When a remote user attempts access into the network, the Contivity gateway references a particular group profile to determine encryption strength, filtering profile, quality of service attributes, and more for that user.

With user- and group-specific profiles you can group common attributes, while preserving the flexibility to make exceptions for individual users. The product features and network access that apply to a user can be controlled by the user identity, rather than by the source IP address or another mechanism. This is necessary to support mobile users and users coming from other organizations.

LDAP

The Lightweight Directory Access Protocol (LDAP) emerged from the X.500 directory service. LDAP is gaining acceptance as the directory model for the Internet. Microsoft*, Netscape*, and Novell* all support LDAP in their directory service strategies. LDAP is based on directory entries; it has an Internet person schema that defines standard attributes and can be extended to include other attributes. A directory service is a central repository of user information; for example, the Contivity gateway supports the following elements using LDAP:

- Groups
- Users
- Filters
- Services

RADIUS

Remote Authentication Dial-In User Services (RADIUS) is a distributed security system that uses an authentication server to verify dial-up connection attributes and authenticate connections. RADIUS is commonly used for remote access authentication.

Many security systems can be configured with a RADIUS front end to facilitate remote access authentication. RADIUS is also the most common authentication mechanism used by ISPs. Novell NDS*, Microsoft Windows NT* Domains, Security Dynamics ACE Server*, and AXENT* OmniGuard Defender*, among others, all support RADIUS authentication. Windows NT Domain authentication is used to control access to NT file servers and other resources on NT networks. The RADIUS server provides a place to store user passwords, because users generally remember their file server passwords.

The X.509 digital certificates authentication mechanism work with public key encryption to provide a level of assurance that users are who they say they are. Eventually, this type of authentication will be the most common.

SSL and digital certificates

The Secure Socket Layer (SSL) protocol can use digital certificates to establish secure, authenticated connections between SSL clients and servers.

The Contivity gateway uses a digital certificate sent from an SSL-capable LDAP server to authenticate that server. In order for digital certificate authentication to succeed, a certificate from the authority certifying the LDAP server must be imported into the Contivity gateway's certificate store. This type of certificate is often referred to as a CA root certificate.

A single CA root certificate can be used to certify the authenticity of multiple LDAP servers, depending on the organization of your environment's certification hierarchy.

Tunnel certificates

The Contivity gateway uses X.509 certificates for authentication to IPsec-based tunnel connections. The Contivity gateway supports RSA* digital signature authentication in the IPsec ISAKMP key management protocol. Remote users can authenticate themselves to the Contivity gateway using a public key pair and a certificate as credentials. In addition, the Contivity gateway uses its own key pair and certificate to authenticate the Contivity gateway to the user. The Contivity gateway currently supports the Entrust* product suite and VeriSign* certificates.

The Contivity gateway also supports retrieval of X.509v3 certificates from Microsoft certificate storage through the Microsoft CryptoAPI (MS CAPI). Microsoft certificate storage also provides a mechanism to import digital certificates granted by third-party certificate authorities through the use of standard messages (PKCS #12). This allows the Contivity Secure IP Services Gateway and Contivity VPN Client to use CAs that have not been tightly integrated with the client and Contivity gateway.

Certificate payload provides a means to transport certificates or other certificate-related information via ISAKMP and can appear in any ISAKMP message. Certificate payloads should be included in an exchange whenever an appropriate directory service (such as Secure DNS) is not available to distribute certificates. The Contivity gateway supports Microsoft native client (L2TP/IPsec) PKCS #7 termination in chained environments.

Using certificates for tunnel connections requires the creation of a *public key infrastructure* (PKI) to issue and manage certificates for remote users and Contivity gateway servers.

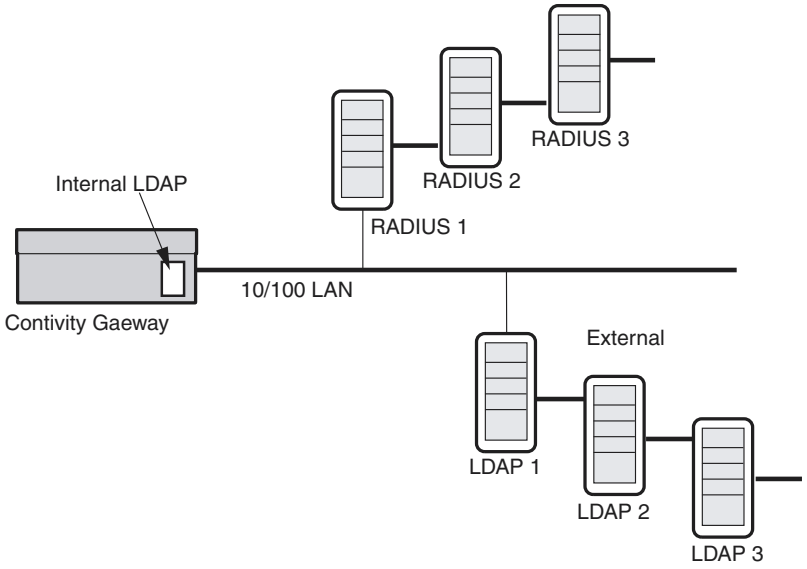
Authentication servers

The Contivity gateway supports LDAP and RADIUS authentication servers. The Contivity gateway always attempts to authenticate a remote user against the internal or external LDAP profiles.

Note: If you authenticate using RADIUS or LDAP authentication, you must use unique names for the Group ID and User ID.

Figure 2 shows a Contivity gateway and authentication servers.

Figure 2 Authentication servers



The user ID (UID) is checked against the LDAP profile database. If the UID is found in the LDAP database, the user is assigned to a group and acquires that group's attributes. Next, the password is checked, and if it is correct, the Contivity gateway allows a tunnel to be formed.

If the UID is not in the profile LDAP (internal or external) database and if you specified RADIUS as the next server to check, the UID and password will be checked against the RADIUS database. If the UID and password are correct, the Contivity gateway checks to see if the RADIUS server returned a class attribute. The RADIUS Class Attribute is treated as an LDAP group name. If a RADIUS class attribute is returned, and it names an existing LDAP group, the Contivity gateway applies the attributes of this group to this user's session, and forms a tunnel. If the group name does not exist, the user is given the RADIUS default group's attributes. If the UID and password are incorrect, the Contivity gateway rejects the user request.

IPsec behaves the same as a PPTP session; the RADIUS server defines the group for that user after authentication using the class attribute group identifier. The only difference between IPsec and PPTP is that in the event the RADIUS server does not return a class attribute, the group associated with the IPsec group ID is used

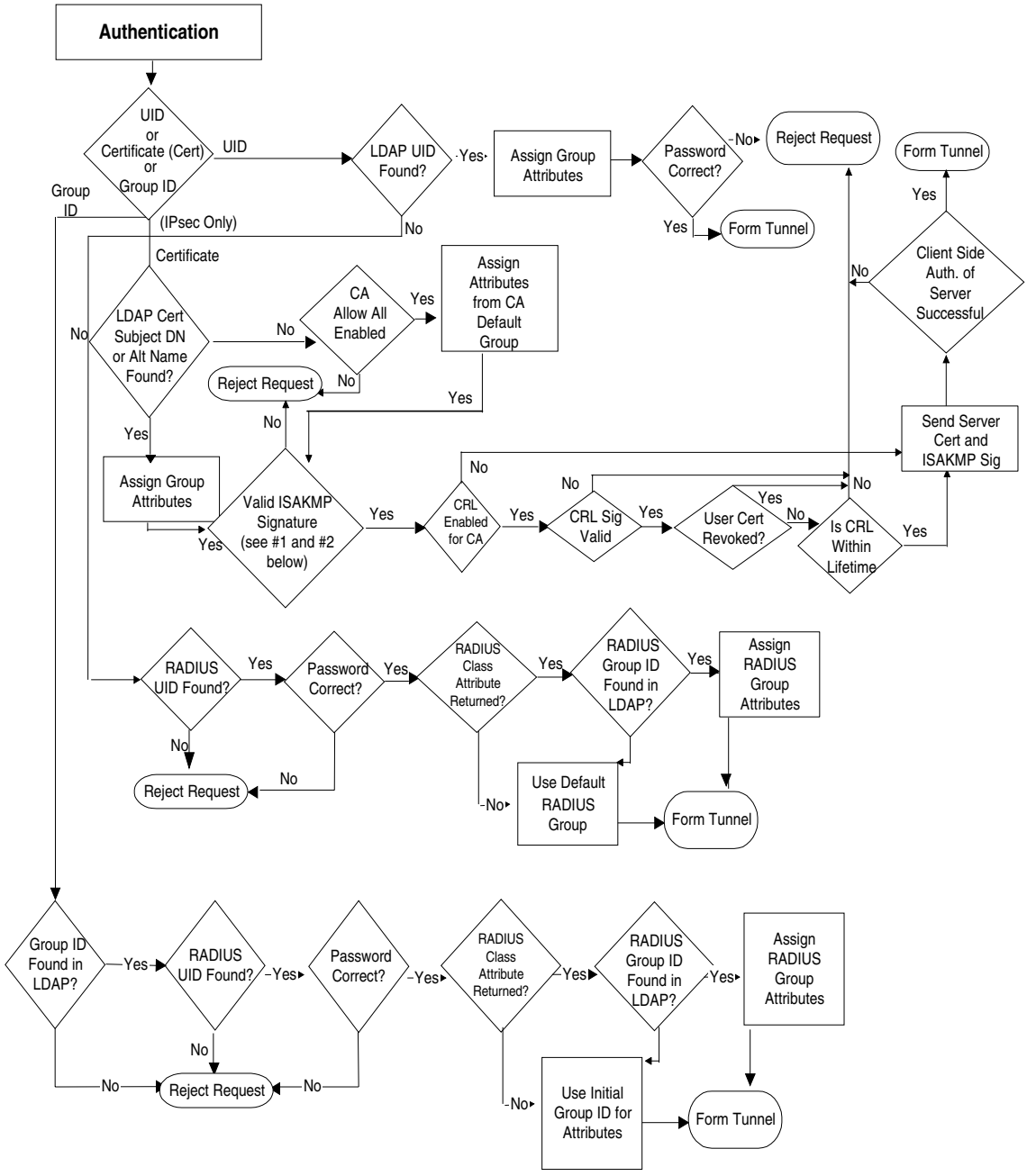
instead of the RADIUS default group. You configure the IPsec Group ID in the Authentication section of the Profiles > Groups > Edit > Configure IPsec screen. You configure the PPTP default group on the Servers > RADIUS Auth screen, RADIUS Users Obtain Default Settings from the Group option.

Note: The group that the user is bound to must allow the authentication method that is used when the session is started.

If the UID is not in the profile LDAP (internal or external) database and if you specified LDAP proxy as the next server to check, the UID and password will be checked against the LDAP proxy database.

Figure 3 illustrates the steps in user validation.

Figure 3 Authentication server validation flowchart



Chapter 2
Configuring servers

This chapter describes how to configure the following authentication servers for users who are tunneling into the Contivity gateway:

- Internal LDAP server stores group and user profiles on the internal server of the Contivity gateway. External LDAP is the contents of the internal LDAP server exported to a separate external LDAP server.
- LDAP proxy server authenticates users against an existing LDAP database separate from the Contivity gateway's database.
- External RADIUS is a distributed security system that uses an authentication server to verify dial-up connection attributes and authenticate connections.
- RADIUS accounting logs user sessions with RADIUS-style records containing detailed connection statistics.
- The Contivity gateway can function as a simple RADIUS server.

It also describes how to configure the Contivity gateway SSL administration feature.

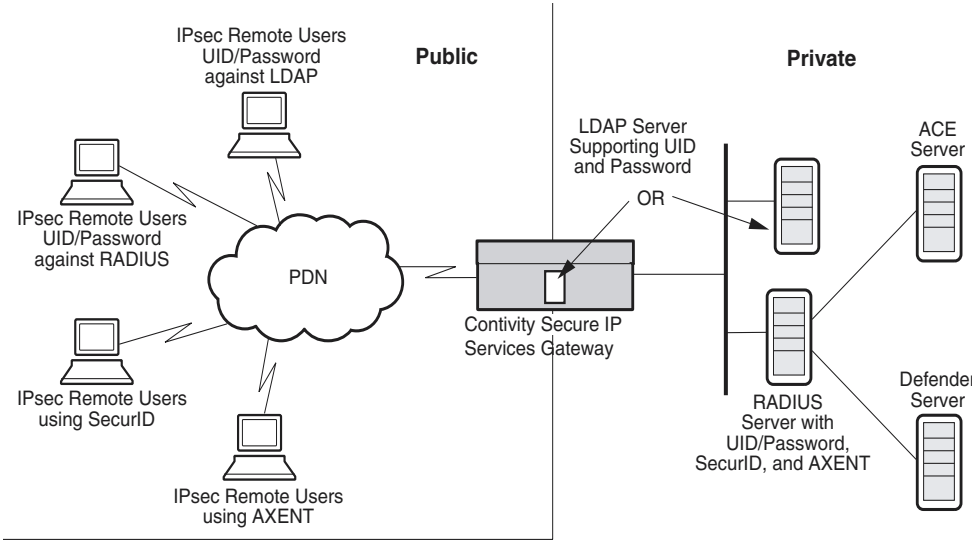
Using IPsec client

Authentication using the Nortel Networks IPsec client provides several options for remote users connecting through a Contivity gateway. These include:

- UID and password authentication against an LDAP database
- Group password authentication using a RADIUS server
- Token Security methods (RSA SecurID* and AXENT Omniguard/Defender)

Figure 4 shows IPsec client options.

Figure 4 IPsec client authentication options



Each authentication option has the following advantages:

- Diffie-Hellman key exchange (ISAKMP/Oakley Aggressive Mode) to build the security association (SA).
- User name and the password are never transmitted in the clear; a cryptographic hash function (SHA-1) is used to protect the user's identity.
- Mutual authentication between the client and the Contivity gateway using a keyed hash algorithm (HMAC).
- Protection against authentication replay attacks through the use of session "cookies."

LDAP database servers

LDAP is a standard protocol for Internet directory services that is based on directory entries. A directory service is a central repository of user information, such as groups, users, filters, and services.

An entry is a collection of attributes that has a distinguished name (DN), which refers to the entry unambiguously. Each entry attribute has a type and one or more values. Types are typically mnemonic strings; for example, **cn** represents common name and **mail** represents e-mail address. The values depend on the attribute type. For example, a mail attribute value might resemble jchirac@elysee.france.gov.

LDAP directory entries are arranged in a hierarchical tree-like structure that reflects political, geographic, and organizational boundaries. Country entries appear at the top of the tree. The next entries represent states or national organizations. The third-branch entries represent people, organizations, servers, files, or any other readable database entry. LDAP allows you to read, search, add, and remove information from the centralized database.

Note: Nortel Networks recommends that you back up your LDAP servers before you make any changes so that you have a valid copy should the file become corrupted.

The Contivity gateway uses an LDAP server to centrally store remote access profiles and corporate networking details such as the addressing mechanism; for example, group attributes including hours of access, filters, and authentication servers. The Contivity gateway queries the LDAP server for access information when a user establishes a tunnel connection. The LDAP query can be serviced locally by the internal LDAP server; or it can be redirected to an external LDAP server, such as the Netscape Directory Server.

Note: Novell Directory Services and Novell eDirectory are not supported.

Configuring internal LDAP server authentication

The Contivity gateway's internal LDAP server does not respond to external queries. Therefore, two or more Contivity gateways cannot share the same internal LDAP database. To allow sharing between gateways, and to take full advantage of LDAP-based directory service replication and centralization, you should use a dedicated directory service.

The gateway synchronizes its cache every 15 minutes. For example, if you delete a user from an external LDAP database it can take up to 15 minutes before all of the gateways recognize the change. Additionally, the LDAP server's status is recorded in the event log every 15 minutes.

To configure internal LDAP:

1. Go to the Servers > LDAP screen. The internal LDAP server is internal to the gateway. If you are using more than one Contivity Secure IP Services Gateway or if you are using LDAP authentication for other network services, you should consider using an external LDAP server.
2. Click to enable access to the internal LDAP server. The internal server is disabled if you enable an external LDAP server.
3. Under General Configuration, click to remove the user's fully qualified ID suffix from the UID before sending it to the RADIUS server. A user ID and suffix, where Rcole is the UID and acme.com is the suffix is rcole@acme.com. Specify the character that separates the suffix from the UID.
4. Click on Stop Server or Start Server, as appropriate, when you intend to back up or restore a configuration, or after you have completed the restoration of a configuration. The LDAP server must be stopped before you can perform the backup and restore procedures.
5. Under Internal Server Control, Directory shows the current directory path, which begins at the root disk drive (ide0). Be sure that you stop the LDAP before performing a backup or restore procedure. To resume operation, you must restart the LDAP server that you were running.

   To backup to a file:

   a. Enter a filename (eight characters maximum) to back up the database.
   b. Click on Backup Now to start the backup procedure. This procedure backs up changes to the internal LDAP LDIF file only (it writes to the LDAP Interchange Format file). The LDIF file is an intermediate databasefile that you can use to move data between LDAP servers.

   To restore from a file:

   a. Click the drop-down list box.
   b. Select a file with which to restore the LDAP database.

c Click on Restore Now.

Both the backup and restore processes might take extended periods of time, based on the size of the database.

6 The Installed LDAP (SSL) CA Certificates section shows whether any certificates are installed. Click on the Import Secure LDAP (SSL) CA Certificate button to import a CA certificate. When you click on the button, it takes you to an edit box that allows you to paste a PKCS#7 Base-64 certificate.

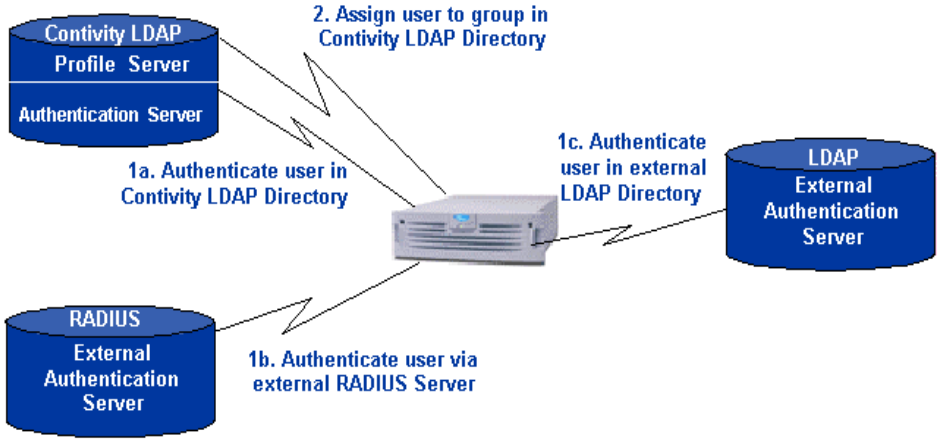
7 Select the Optimize Database option to optimize the internal LDAP database.

Configuring LDAP proxy server authentication

The gateway supports authentication against an existing LDAP server rather than creating a second user database for use with the gateway. The server can reside on either a private or public network that is connected to the gateway. You can also configure the type of authentication methods that are allowed to access the existing LDAP server. There are five options available: PAP (Bind authentication), PAP, CHAP, MS-CHAP, MS-CHAP V2 (Bindname authentication). The gateway supports LDAP V2 and LDAP V3 servers.

Figure 5 shows the authentication mechanism that is used between the gateway and the external LDAP proxy configuration.

Figure 5 LDAP proxy server



General filter specification syntax:

- If no filter is specified, the resultant search is (uid=username).
- If a filter string is specified, the search is (&(uid=username)filterstring).

For example, a filter value of (|(ou=engineering)(ou=finance)) creates a search that specifies UID=username and (ou= engineering or ou=finance) (&(uid=username)(|(ou=engineering)(ou=finance)).

Certificate LDAP query syntax is (&(SubDn=<subject DN from cert>)(CAAttribute=<issuer DN from cert>)myFilter) or (&(SubAltName=<subject alt name from cert>)(CAAttribute=<issuer DN from cert>)myFilter).

SubjectDN or Altname is determined by checking if the UID of the session is the same as the subject DN of the certificate.To configure LDAP proxy server authentication:

1 Go to the Servers > LDAP Proxy screen and select Enable Access to LDAP Proxy Server.

   a In the Remove Suffix from User ID field, select to remove the fully qualified ID suffix from the UID before sending it to the LDAP server.

   b Specify the character that separates the suffix from the UID as the delimiter value.

   c In the LDAP Proxy Server Users Obtain Default Settings from the Group field, select the default group to which users are assigned.

2 Under LDAP Proxy Servers, enter a base distinguished name (DN) for the server. This is usually in the form ou=organizational unit, o=organization, c=country.

   a For the remote LDAP server, enter the Master, Slave 1, and Slave 2 LDAP server host names or IP addresses. Should the master server become unavailable, the gateway attempts to initiate a connection with the slave servers.

   b In the Connection section, enter the port number (default 389) and the associated SSL port number (default 636) that your LDAP server listens to queries on.

c Enter the bind distinguished name (DN), which is the LDAP equivalent of a user ID and is required to access the base DN and its subentries. Leave this field blank if your LDAP server allows anonymous access.

d Enter the bind password, which can consist of up to 32 characters. This password allows the gateway to prove its identity (the bind DN) to the LDAP server.

3 In the Username/Password Access section, you can have case-insensitive character strings that are allowable in LDAP search filters. The default value for each field is blank. If you do not supply a value, the authentication will fail. Enter the user name and password. To enable additional policy checking, specify an LDAP search filter, which can be a case-insensitive character string that forms an allowable LDAP search filter (default is blank).

4 The User Certificate Access section allows you to add digital certificates support for authentication:

a Enter the Subject DN attribute, such as common name, organizational unit, organization, and country.

b Enter the Subject Alternative Name attribute.

c Enter the Certificate Authority (CA) attribute.

d Enter the LDAP filter name.

5 In the User Policy Attributes section, specify attributes used to store the Contivity gateway group, static IP address/netmask, and customized user filter. These fields can hold case-insensitive character strings that are allowable in LDAP search filters. The default value for each field is blank. Without a specified attribute name, the LDAP proxy server will not attempt to extract this information.

6 Click on the SSL Encryption hyperlink to go to the LDAP server SSL encryption screen. This allows you to select the encryption types the gateway uses during negotiation with the external LDAP server.

7 Go to the Services > IPsec screen and use the Swap Server Order 2 and 3 to change the order in which the gateway applies authentication. External LDAP proxy is disabled by default and must be added as an option before it can be swapped.

8 Go to the Profiles > Groups screen and either add or select the group that you want to be the default group for LDAP users (this is the group a user is assigned to if the LDAP server does not send back a class attribute).

9 Go to the Profiles > Groups Edit > Edit IPsec screen. In the Authentication area, click on the Configure button. Enter the Group ID, the Group Password, and confirm the group password. The group ID and the user ID must not be the same. Consider using the LDAP group name as the default group, because you must remember a default name once you enter it.

Note: The Start/Stop button disappears when you restore the LDAP database. If you need to refresh the screen after the restore completes and the restore status popup is dismissed, you can reselect the screen using the menu item selection.

To configure IPsec and LDAP on the client:

1 In the Contivity VPN Client UI, go to Options > Authentication Options, and select Group Security Authentication.

2 Enter the group ID and group password.

3 Select one of the group authentication options.

4 Click on OK.

Monitoring LDAP servers

If the Contivity gateway cannot reach the LDAP proxy server, it still operates and passes traffic. However, it does not authenticate users whose information exists in a third party directory. The Contivity gateway simply pings the LDAP proxy servers every few minutes to check for their status. If it receives an ICMP reply, an attempt is made (considered available) to the LDAP proxy server. This is similar to the way the Contivity gateway monitors RADIUS servers.

External LDAP servers behaves differently where the server must reply to Contivity gateway ICMP echo requests and accept a directory bind before Contivity gateway considers it available. On initialization of the external LDAP server, the Contivity gateway monitors the health of each external LDAP server to determine if the server is available. If it cannot contact its directory the Contivity gateway will run, but it will not terminate tunnels or pass network traffic.

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

The Contivity gateway monitors the status of all configured external LDAP servers. If the Contivity gateway has marked a server as up, it will monitor the status of the server by binding and conducting a search against the directory every 15 minutes. If the Contivity gateway has marked a server down, it first monitors the status of the server by issuing an ICMP echo request to the server every 15 minutes. If an echo reply is received, the Contivity gateway then attempts to bind and search the server's directory. If the bind and search is successful the Contivity gateway will change the server's status to up and return the server back into the server list for operation. If either the bind or search is unsuccessful the server will remain in the down state.

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

Once the primary external LDAP server has been initialized, the Contivity gateway issues an ICMP echo request to all secondary server IP addresses and follows the previous procedure for each secondary server.

Because the Contivity gateway assumes only read/write access to the primary external LDAP server, it does not configure any secondary server directories for Contivity gateway directory storage. Instead, the Contivity gateway relies on the LDAP replication agreements between the primary LDAP server and secondary LDAP servers to populate the secondary servers with the appropriate directory information.

During normal operations, the Contivity gateway utilizes the primary external LDAP server. In the event of primary LDAP server failure, the Contivity gateway will fail-over to the next secondary LDAP server in succession. Only the servers marked up will be attempted. Once the Contivity gateway detects the return of the primary server, it returns to normal operations and utilizes the primary server exclusively.

RADIUS authentication service

RADIUS is a distributed security system that verifies connection attributes and authenticates connections. It is a service running on the Contivity gateway that responds to RADIUS authentication requests from clients. It is available on both public and private interfaces. You can enable this service for the Services > RADIUS screen. Packet flow is from external clients to the Contivity interface IP and port. You configure the port on the Services > RADIUS > port screen. You configure filters from the Services > Available > Authentication Protocol > RADIUS (public and private) screen.

RADIUS client authentication allows the Contivity gateway to act as a RAIUS authentication client to external RADIUS authentication servers. You enable client authentication on the Servers > RADIUS auth screen. External authentication servers can be located on either public or private networks. You determine the packet flow from the IP address/port that you configured on the Servers > RADIUS auth > RADIUS Servers > interface screen to external servers and back. You control the filters from the Servers > RADIUS auth > Enable Access to RADIUS Authentication screen. When you enable it, it put public and private filters in place.

RADIUS client accounting allows the Contivity gateway to act as a RADIUS accounting client to external RADIUS accounting servers. You enable accounting on the Servers > RADIUS acct screen. External accounting servers can be located on either public or private networks. The packet flow is from the IP address/port that you configure on the Servers > RADIUS acct > External RADIUS Accounting Server > Interface screen to external servers and back. You configure filters on the Services > Available > RADIUS accounting (public and private) screen.The RADIUS Authentication Servers screen allows you to configure up to three servers for remote authentication. It is imperative that the RADIUS servers contain the same user data. The alternative RADIUS servers are used only when no response is received from the primary RADIUS server.

Most RADIUS servers support CHAP and PAP authentication, and some support MS-CHAP (Funk, for example).

Note: If you require PPTP-encrypted tunnels and RADIUS authentication, then you must use a RADIUS server that supports MS-CHAP. The alternative is to use an LDAP server for PPTP authentication.

Configuring RADIUS authentication

The gateway supports authentication against a RADIUS server. This server can reside on either a private or public network that is connected to the gateway. To enable RADIUS authentication, you must configure the gateway with the RADIUS server host name, port number (typically 1645, but port 1812 is the RFC standard), and a shared secret. Access the gateway management screen from the Servers > RADIUS Authentication screen.

The RADIUS Authentication screen also allows you to configure the type of authentication methods that are allowed to access the RADIUS server. There are five options, of which only four are IPsec-related: AXENT, SecurID, CHAP, and PAP. MS-CHAP is available for PPTP tunnel users only (it is not applicable to IPsec tunneling applications).

If you are using token cards for authentication, you must select the appropriate technologies (AXENT, SecurID, or both). For example, the SecurID passcode is the pin plus the token code. The RADIUS Authentication screen also allows you to configure the type of authentication methods that are allowed to access the RADIUS server.

Note: Neither the UID nor password are ever passed in the clear for an IPsec client either from the remote client or from the gateway communicating with the RADIUS server. If you use PAP authentication for a PPTP session, both the user name and the password are passed in the clear to the gateway over the Internet.

There is no significant security benefit between using CHAP or PAP. Because the connection between the gateway and the RADIUS server is protected by encryption, PAP authentication consumes fewer instructions during the authentication process, which is a minor consideration.

When you are using RADIUS-based authentication, the IPsec client and the gateway require a second set of credentials that are used for mutual authentication. These credentials are referred to as the group ID and group password.

The remote access client information is documented in the Contivity VPN Client online Help. On the IPsec client side, the remote user must:

1. Select Options > Authentication Options.
2. Click on User Group Security Authentication.
3. Enter the group ID and group password that you provide.
4. Select one of these options:
   - Challenge Response Token
   - Response Only Token
   - Group Password Authentication

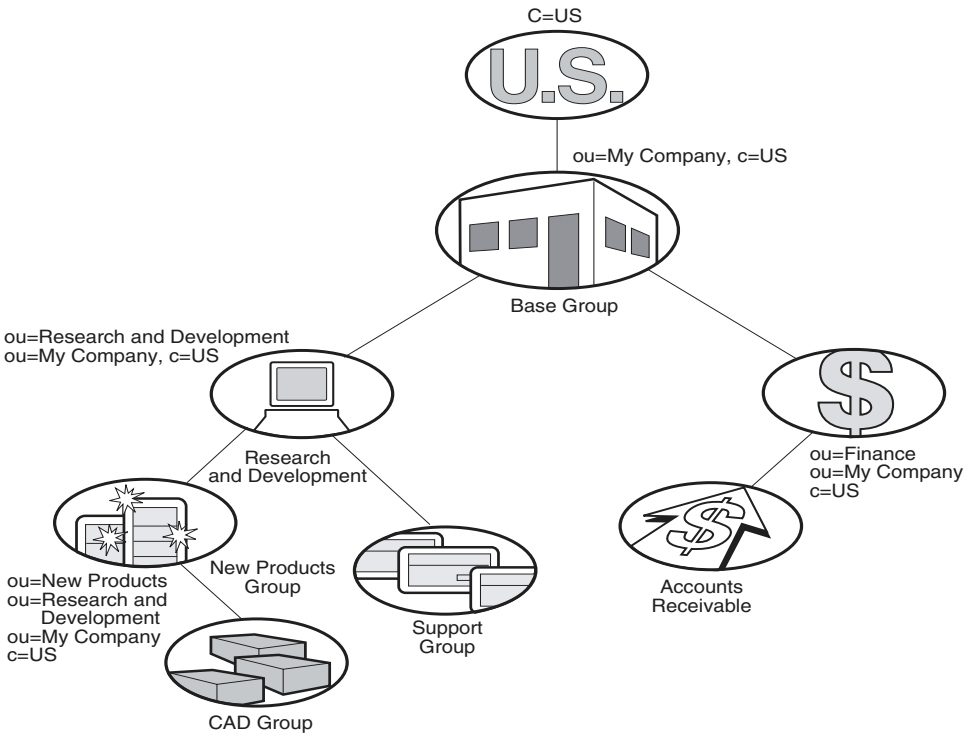
To complete the RADIUS setup, you must configure at least one group profile for RADIUS users. In this profile, you need to enter the group ID, password, and the allowed group authentication options. You can configure the group profile from the Profiles > Groups > IPsec: Edit screen.

1. Set up and test the operation of the RADIUS server with ACE and/or Defender servers, depending on the type of token security you want. You should do this before attempting authentication by an IPsec client to verify that everything on this side of the network is operating properly.
2. Identify and create the groups for authenticating token users, and supply the group ID and password to all users doing either token card or group password authentication. AXENT and SecurID users are created and maintained in their respective servers, not in the gateway. Add the groups in the Profiles > Groups > IPsec screen.
3. Define the RADIUS server configuration settings for token security.
4. Define the Tunnels settings for IPsec. Add a RADIUS server, if necessary (see “Configuring IPsec authentication” on page 41).

RADIUS authentication class attribute values

Figure 6 shows the relationship between RADIUS authentication class attribute values for gateway users. C is the class attribute for country, and OU is the class attribute for organizational unit.

Figure 6 RADIUS authentication class attribute values



The gateway supports RADIUS-supplied attributes, such as IP address and MPPE key and additional specific attributes, if they are returned from a RADIUS server; any other returned attributes are ignored. The specific attributes are detailed in Microsoft documentation and defined in RFC 2548. This data overrides the corresponding data stored in LDAP, if any. Table 1 shows common examples of class attributes.

Table 1 RADIUS class attributes

Name	Value format	Function
Class	ou=groupname	The user is assigned to the group 'groupname', if it exists.
Framed-IP-Address	dotted decimal	If static addresses are allowed, this IP address is used for the tunnel session.
Framed-IP-NetMask	dotted decimal	Subnet mask to be used with above IP address.
Filter-ID	filter name	If defined, this filter name is applied to the tunnel session.
DNS	domain server name	If used, the domain name system server name.
NBNS	protocol name	NetBIOS protocol; an internet naming service. If used, translates the NetBIOS Windows domain name to the IP address.

Table 2 shows sample details that you enter into your RADIUS server.

Table 2 RADIUS example details

User ID	Class attribute value	Assigned group
Lee Madison	ou=New Products, ou=Research and Development	New Products
Julie Lane	None	Default
Bill Sullivan	ou=Staff	Default (ou=Staff does not exist)

The RADIUS server uses the class attribute value to associate the user ID with a group in the LDAP database.

RADIUS-Assigned Framed-IP-Address attribute

You can configure a RADIUS-Assigned Framed-IP-Address attribute on the RADIUS server for the ID being authenticated by the gateway. If the option Allow Static Addresses (Profiles > Groups > Edit > Connectivity screen) is enabled for the assigned group, then the returned IP address is used for the tunnel session. Otherwise, an IP pool address is assigned.

Note: Only a single IP address is returned by the RADIUS server; therefore, only one active tunnel connection is permitted per user ID.

Configuring IPsec authentication

The following procedures describe how to configure the gateway to interoperate with a RADIUS server while using either IPsec or PPTP.

To configure IPsec and RADIUS on the gateway:

1. Go to the Servers > Radius Auth screen and select Enable Access to RADIUS Authentication.
   - **a** In the Remove Suffix from User ID field, select to remove the fully-qualified ID suffix from the UID before sending it to the RADIUS server. Specify the character that separates the suffix from the UID as the delimiter value.
   - **b** In the Remove Prefix from User ID field, select to remove the fully-qualified ID prefix from the UID before sending it to the RADIUS server. Specify the character that separates the suffix from the UID as the delimiter value.
   - **c** Select Error Code Pass Thru to allow an error message sent to the Contivity gateway by the RADIUS server to pass through the gateway to the originating client.
   - **d** In the RADIUS Users Obtain Default Settings from the Group field, select the default group to which users are assigned.
2. Enable an authentication method from the Server Supported Authentication Options:
   - Challenge/Response Token Cards.

- Response Only Token Cards.
- MSCHAPV2 Microsoft encrypted CHAP Version 2.
- MSCHAP Microsoft encrypted Chap Version; check RFC-2548 to enable the gateway to interoperate with a Microsoft RADIUS Server Version 2.2 or later, or a Version 2.1 with the Microsoft Hotfix applied. Leave this box empty if using a Microsoft RADIUS Server V2.1 (without the Hotfix) or earlier.
- CHAP (Challenge Handshake Authentication Protocol.
- PAP (Password Authentication Protocol).

3 Under RADIUS Servers, check the box next to the server type. Click to enable the RADIUS servers that you want to use for authentication (up to three servers). The primary server receives all RADIUS authentication inquiries unless it is out of service. A RADIUS server that fails to respond five times is temporarily taken off the server list for 30 minutes. After 30 minutes, the server is tried again. In the event that the primary server is unreachable, the gateway queries the first and second alternate RADIUS servers.

a Enter either the Host Name or IP Address of the servers. For example, finance.mycompany.com or 145.22.120.111. You can also use simple names (for example, finance) if you have a DNS server configured on your gateway. For Primary, enter the primary RADIUS server host name (required if RADIUS is enabled). The primary server is normally used to process incoming authentication requests. For Alternate 1, enter the first alternate RADIUS Server host name (this server processes incoming authentication requests if the primary RADIUS server is unavailable). For Alternate 2, enter the second alternate RADIUS server host name (this server processes incoming authentication requests if the primary RADIUS Server and the first alternate server are unavailable).

b Under Interface, specify whether you want the RADIUS server to be accessed from the gateway's private or public interface. The address of the interface is used to configure the RADIUS client address information on the remote RADIUS server. You must enable RADIUS authentication as an allowed service on the Services > Available screen. Select Private if the RADIUS server is reached through the private interface. The gateway's management address is used. Select Public if the RADIUS server is accessed through the gateway's public interface. You must also specify the IP address for the public interface. The public IP address list is dynamically built from the information on the System > LAN screen. Any

change, such as removing an interface card or changing an IP address, is automatically reflected in the drop-down list.

c In the Port field, enter the Server Port Number that you want the RADIUS authentication requests to use. Default is Port 1645.

d In the Secret field, enter the Secret (password) to share with the gateway. To enhance overall security, this secret should be different for each server. The shared secret encrypts the password between the gateway and the server when the tunnel connection uses PAP or SecurID. It also verifies the authenticity of each accounting request sent by the gateway to the RADIUS server. Furthermore, it verifies the authenticity of each response sent by the RADIUS server to the gateway.

e Confirm Secret by reentering the server's Secret to verify that you typed the password correctly.

f The reply-source-port option allows you to configure the port that the RADIUS server will use as a Source in the RADIUS authentication reply. The default value is 0 (only allow a reply packet with the source port of 1645). The UDP port that is used is the port configured in the Port attribute of the RADIUS server configuration on the server Servers > RADIUS Authentication screen. The default value is 1645.

Reply-source-port is only necessary if you have a RADIUS server that sends a RADIUS authentication reply with a UDP port that differs from the originating UDP port. For example. if a RADIUS authentication packet is sent from the Contivity using the UDP source port 1100 and UDP destination port 1645, the RADIUS server responds with a UDP source port of 8500 and a destination UDP port of 1100. The Contivity is expecting a reply with a source UDP port of 1645 and a destination UDP port of 1100. Therefore, this packet will be dropped because the UDP port 8500 is not open (by default) and the packet is filtered.

g Suppress-service-type removes the service type 8 attribute from the radius access message and allows attributes to be returned to the Contivity Secure IP Services Gateway. It is implemented to maintain forward compatibility with newer versions of SBR.

4 In the Response Timeout Interval field, enter the frequency in seconds that you want the gateway to wait before retrying to connect to the RADIUS servers. By default, the gateway tries once every three seconds; minimum setting is 1.

5 In the Maximum Transmit Attempts, enter the number of times that you want the gateway to attempt to connect to the RADIUS servers before failing. By default, the gateway tries three times.

6 Click on the RADIUS Diagnostic Report link to use the RADIUS Diagnostic Report test to check that your RADIUS Authentication configuration is correct. This report compares the settings that you entered on the RADIUS Authentication screen to the corresponding settings that are specified on other gateway configuration screens. The title of each section of the diagnostic report lists the name of the related screen. For example, the IPsec RADIUS Configuration section of the report contains information related to the Services > IPsec screen.

7 Enable a server and enter the server's host name or IP address, the interface type, port number (1645), and secret. Click on OK.

8 Go to the Services > IPsec screen and use the Add RADIUS button to add a RADIUS server to the Authentication Order table.

9 Go to the Profiles > Groups screen and either add or select the group that you want to be the default group for RADIUS users (this is the group a user is assigned to if the RADIUS server does not send back a class attribute).

10 Next, go to the Profiles > Groups > IPsec Configure screen. In the Authentication area, click on the Configure button.

11 On the next screen, the Authentication method for the group is already selected. Enter the group ID and group password. Consider using the LDAP group name as the default group, because you must remember a default name once you enter it. If your RADIUS server returns a class attribute, ensure that the authentication method is enabled for that group. However, you do not need a group ID and group password for the group that is being returned as a class attribute.

To configure IPsec and RADIUS on the client:

1 In the Contivity VPN Client GUI, go to Options > Authentication Options, select Group Security Authentication, and enter the group ID and group password.

2 Select one of the group authentication options.

3 Click on OK.

Configuring PPTP and RADIUS

To configure PPTP and RADIUS on the gateway:

1. Go to the Servers > Radius Auth(entication) screen and select Enable Access to RADIUS Authentication.
2. Enable an authentication method.

If a valid class attribute is not returned, then PPTP users are placed in the default group as configured on the Servers > RADIUS Auth(entication) screen.

Note: Everything about the authentication type must match; for example, if you send an encrypted password, then MS-CHAP must be enabled on the RADIUS authentication screen and the RADIUS server must support MS-CHAP.

Configuring group-level RADIUS authentication

In remote access deployments, you may want to partition users across several different RADIUS servers, with the Contivity Secure IP Services Gateway able to connect to the appropriate server when authenticating a specific user. This group-level authentication can be particularly useful for large installations with many different databases, and for carriers that have a business need to keep customer authentication domains separate.

To configure the group-level RADIUS authentication server for each group:

1. Go to the Profiles > Groups > Edit > IPsec Edit screen.
2. Click on the “Configure Group Level RADIUS Servers” link in the Authentication section of the IPsec Edit screen to access the Group Level RADIUS configuration screen. You can configure the following:
   - A primary and two alternate RADIUS servers
   - IP address, interface, port, and secret
   - UserID suffix removal and delimiter value
   - Response Time out and Maximum Transmission Attempts

- For user name/password authentication, the PAP/CHAP settings are retrieved from the Servers > RADIUS Authentication Servers page settings.

Group-level RADIUS authentication works only with clients that use Group ID/Password. This excludes all non-IPsec client implementations. Each client in the group must be configured for group authentication using the group ID and group password.

Note: There are no separate group levels of authentication on a RADIUS configuration for the firewall user authentication (FWUA) users. Because they can only be members of the global group configuration, if you have multiple RADIUS servers, you must add these users to the group on the Contivity gateway global RADIUS configuration screen. This also applies to PPTP and L2TP user tunnels.

Vendor-specific RADIUS attribute

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

Configuring RADIUS accounting

The RADIUS accounting configuration screen allows you to specify how your gateway saves RADIUS accounting results. By default, the results are stored locally. You can also save the RADIUS accounting information to a remote RADIUS server.

Note: If you set the date ahead and then set it back, external RADIUS accounting no longer works.

To configure RADIUS accounting:

1. Go to the Servers > Radius Acct screen.
2. Click to enable or disable internal RADIUS accounting. Internal RADIUS accounting is enabled by default.

3. Enter an interval when a snapshot of the current active tunnel sessions is recorded to a journal file. Use the format, hh:mm:ss, for the interval. The journal file stores the session information until the user logs out of the tunnel session, after which the session stop record is saved on the local disk. In the event of a system crash, upon reinitialization the gateway translates the journal file into a series of stop records on a per-session basis. This minimizes accounting data loss. A low interval creates system overhead and requires additional processing. The default interval is 00:10:00 (10 minutes).
4. Click to enable or disable the Interim RADIUS Accounting Record feature. This selection is enabled by default.
5. Enter the interval at which time interim RADIUS records are sent to the specified external RADIUS server. Use the format *hh:mm:ss* for the interval. A short interval creates system overhead which requires additional processing. The default interval is 00:10:00 (10 minutes).
6. Click on Enable to send accounting records to the external RADIUS accounting server.
7. Enter the external RADIUS server host name or IP address. If you enter a host name, use a fully qualified domain name, such as Finance.mycompany.com.
8. Enter the server port number that you want the RADIUS accounting requests to use. The default is port 1646.
9. Enter the external RADIUS server's required secret (password).
10. Reenter the remote server's secret (password) to verify that you typed the password correctly.
11. Click on the Test Server button to verify the connectivity from your gateway to the external RADIUS server. A message at the top of the screen shows the results of the test.

The gateway can send RADIUS accounting active session interim start and stop records to an external RADIUS server. These interim records provide information about the currently active sessions on the gateway. An administrator might use this information to evaluate gateway usage, such as connection start and stop times.

To identify the external RADIUS server and specify how often the accounting information is sent to the external server:

1. Click Enable to specify that the gateway send its accounting records to the external RADIUS accounting server.
2. Enter the external RADIUS server's host name or IP address. If you enter a host name, use a fully qualified domain name, such as sales.mycompany.com.
3. Enter the server port number that you want the RADIUS accounting requests to use. The default is Port 1646.
4. Enter the external RADIUS server's required secret (password).
5. Re-enter the remote server's secret (password) to verify that you typed the password correctly.
6. Use the Test Server button to verify the connectivity from your gateway to the external RADIUS Server. Click to test the connection to the external server. A message at the top of the screen shows the results of the test.

Configuring DHCP servers

Dynamic Host Configuration Protocol (DHCP) dynamically assigns IP configuration parameters to clients and provides for centralized network administration. DHCP pushes configuration information to clients, including network address parameters and standard options. It also provides for interaction with DNS.

DHCP uses the concept of IP address leases. When a DHCP client requests an IP address, a DHCP server grants the client exclusive use of an assigned IP address for a specified period of time.

You can configure both the DHCP server and DHCP relay on the same interface. When both DHCP server and DHCP relay are configured for an interface, the DHCP server takes precedence and the DHCP packets received by the Contivity gateway are processed by the DHCP server. For DHCP relay to be functional, the DHCP server on the Contivity gateway must be disabled for the interface on which the DHCP relay is configured.

The DHCP server requires that either the Contivity Stateful Firewall or interface filter must be enabled. Incoming DHCP packets are discarded if the CSFW or interface filter is not enabled. This restriction is placed by the software in accordance with the Contivity gateway as a security device where the default action is to discard packets rather than to forward them.

Note: The Contivity Secure IP Services Gateway includes a full implementation of a DHCP server that is in compliance with RFC 2131 and RFC 2132.

DHCP pushes configuration information to clients and provides for interaction with DNS.The following restrictions apply to the DHCP server:

- DHCP server is enabled by default on the private (trusted) interface
- DHCP Relay and the DHCP Server are mutually exclusive on a physical port.

Note: You can enter duplicate IP addresses for the DNS servers without error messages stating that there are duplicate addresses. This applies to both the UI and CLI interfaces.

To configure the DHCP server:

1. Go to the Servers > DHCP screen.
2. Click on the Enable/Disable Server button to select the state of the DHCP server.
3. In the Default Options section, specify the lease time in the ddd:hh:mm:ss format or select Infinite to indicate an unspecified period of time.
4. Click on Add in the Standard Options section to access the Add Option screen. The standard options section shows the current status of any added options and lets you add new options:
   - Select the desired options from the drop-down list.
   - Select the desired Type from the drop-down list.
   - Enter the appropriate value.
5. In the Pool section, click on the Add button to add a pool. The Add Pool screen appears:

a Enter the base IP address for the pool.

b Enter the subnet mask for the pool.

c Enter a pool name. The name must match the group profile for DHCP.

d Enter a description of the pool.

e Click on OK.

6 Select Pool and click on the Configure button to return to the Pool screen.

7 The Inclusion Range section allows you to add blocks of IP addresses that you can then give out.

a Under Inclusion Range, click on the Add button. The Pool Inclusion screen appears.

b Enter the base IP address for the Start Address.

c Enter the End IP address.

d Click on OK.

8 Optionally, you can select an Exclusion Range for further control of the IP addresses that you give out.

a Under Exclusion Range, click on the Add button. The Pool Exclusion screen appears.

b Enter the Start Address for the range.

c Enter the End Address for the range.

d Click on OK.

9 Optionally, you can force the DHCP server to assign a fixed IP address to a host every time it logs in. You can do this with host reservations under the Host section.

a Click on the Add button. The Host screen appears.

b Enter the host name that is registered with DNS.

c Enter the IP address that you always want to reserve.

d Enter the Ethernet (MAC) address.

e Click on OK.

10 The server does not implement configuration changes until it is restarted. Return to the Server > DHCP screen and select the Restart Server option to restart the DHCP server.

11 To verify the configuration changes, go to the Status > Health Check screen or click on the DHCP Stats button on the Status > Statistics screen.

Configuring remote user IP address pool

Remote access users who are using tunneling protocols require two IP addresses to form packets. The addresses are normally referred to as *outer* and *inner* addresses. The outer address, or public address, is visible when packets are traveling through the public data networks (PDNs). This address is negotiated between the client and the ISP to which it is connected. The gateway does not control this address.

The inner IP address is the one that eventually appears on the private network when the outer layers of the packet are removed. Therefore, this address must lie within the private network address space. The gateway provides the remote user with the inner IP address during tunnel setup. This address can come from an internal address pool, an external DHCP server, a RADIUS server, or from an external LDAP proxy server.

The gateway assigns the inner IP address from one of several sources, using the following order:

1 User-specified (excluding IPsec)

2 Static address, either the gateway's LDAP database, the RADIUS server, or the external LDAP proxy servers

3 Local address pool, either the gateway’s internal address pool or the DHCP-acquired address pool

The Remote User IP Address Pool screen allows you to select a method for users to obtain IP addresses for access to the private network. These addresses are serviced by the gateway and are available to remote users accessing the gateway on demand. You can choose to have IP addresses assigned from one of the following:

- External Dynamic Host Configuration Protocol (DHCP) pool
- Internal address pool

A DHCP server on the private LAN segment dynamically assigns IP addresses on behalf of remote users. You must have an existing DHCP server in your environment to choose this option. The DHCP server is contacted by a broadcast or unicast (depending on the option selected) DHCP request through the network adapter associated with the Management IP address.

The internal DHCP server option also provides:

- A cache of pre-negotiated DHCP addresses so that the client does not have to wait to acquire an address at logon.
- All DHCP controls (such as cache size, immediate release, blackout time, blackout override) can be used to fine tune the behavior of the DHCP client.
- Named pools are supported. The pool name from the user/group profile can be used to select which of the internal DHCP server pools a local address comes from.
- A default pool can be used to provide addresses when the preferred pool is exhausted or unavailable. The default fail over control enables/disables use of the default pool.

To configure a DHCP address pool:

1. Go to Servers > User IP address pool.
2. Click on the DHCP button.
3. Click on Any DHCP Server to allow any available DHCP server to provide the requested IP addresses. Any DHCP Server is the External DHCP default selection.
4. Click on Internal DHCP Server to allow a block of addresses. These addresses must also be specified in the user's group profile.
5. Click on Specified DHCP Server to allow IP addresses to be provided from a Specified DHCP Server only. Indicate the IP addresses of the servers that provide DHCP service, including Primary, Secondary, and Tertiary. A status field provides information on the associated servers. Configuring a Secondary or Tertiary server is optional.

6. Enter the DHCP Cache Size. This is the number of IP addresses that is held in the gateway cache. The minimum number of IP addresses held is one (1), and the maximum is derived from the maximum number of tunnel sessions that the gateway supports.
7. Check Immediate Address Release to have the gateway release the IP address back to the DHCP server immediately. If you have a limited number of IP addresses available, then you should enable this option. IP addresses from disconnected tunnel sessions remain unavailable for the time you specify (300 to 7200 seconds). This delay prohibits immediate reuse by another user that could represent a security risk.
8. For DHCP Blackout Interval, enter the amount of time in seconds that a DHCP address is held in a blackout state before it is returned to the DHCP server or the DHCP cache.
9. Check Override Blackout Interval when no addresses are available to enable this option.

To add a user IP address pool:

1. Go to Servers > User IP address pool.
2. Click on Add to add a new address pool.
3. Enter the base IP address for this pool. Make sure that none of the pool addresses are the same as those used for the LAN interfaces or the Management interface IP address. The gateway does not check the IP address supplied by a PPTP client to see if it has been assigned to a LAN interface, Management interface, or address pool.

   The Use Client-Specified Address option is disabled by default. To avoid potential conflicts, you can verify the current state of this option from the Profiles > Groups > Edit > Configure PPTP screen.
4. Enter the Subnet Mask for the pool that you are configuring. You can later edit the Subnet Mask as necessary.
5. Enter the name of the pool. The name must match the group profile for either DHCP or for a local address pool.

   Go to Profiles > Groups > Edit > Connectivity and click on the list to select the address pools used by remote users to access the gateway. The list shows all pools that have been defined on the gateway.

Optionally, select the New Address Pool link to define a new pool. This option is set to Default Pool by default.

6 Enter a text description of the pool.

7 Click on OK to save the entries for the IP address pool and return to the Remote User IP Address Pool screen.

Internal address pools allow you to select the block of addresses that a particular user's local address comes from. You can name internal pools, but the pool name must be also specified in the user's group profile. For example, a profile for software engineering and hardware engineering groups could select addresses from the engineering address pool. You can also define a default internal address pool to supply an address when the preferred pool is exhausted or otherwise unavailable.

Configuring DHCP relay

The DHCP relay agent on a Contivity gateway forwards DHCP and BOOTP messages between a server and a client on different subnets. When a locally attached host issues a DHCP or BOOTP request as a broadcast message, the Contivity gateway will relay the message to a specified DHCP or BOOTP server. The DHCP relay agent also forwards DHCP replies from server to client.

Note: The DHCP relay agent can run only on all the private physical interfaces and tunnels.

You can enable or disable DHCP relay for each interface and specify the DHCP servers for each interface. when DHCP relay is enabled on an interface, the Contivity gateway forwards DHCP requests from the interface to the DHCP server configured for the same interface.

The DHCP relay agent will unicast DHCP packets only to the specified Helper servers (up to 3). Server 1 address is required. Server 2 and Server 3 addresses are optional. Additionally, you can enable and disable each DHCP server by checking or unchecking the Enable box.

To add a DHCP relay interface:

1. From the Servers > DHCP screen, click on the Add button.
2. On the Upgrades screen, click on the Configure IP Address link if you do not already have one listed
3. For the state, select either Enabled or Disabled.
4. For DHCP Server, enter the IP address and then check Enabled for Helper 1, Helper 2, and/or Helper 3.
5. Click OK.

Select the Statistics button in the DHCP Relay screen to view the DHCP Relay Statistics screen.

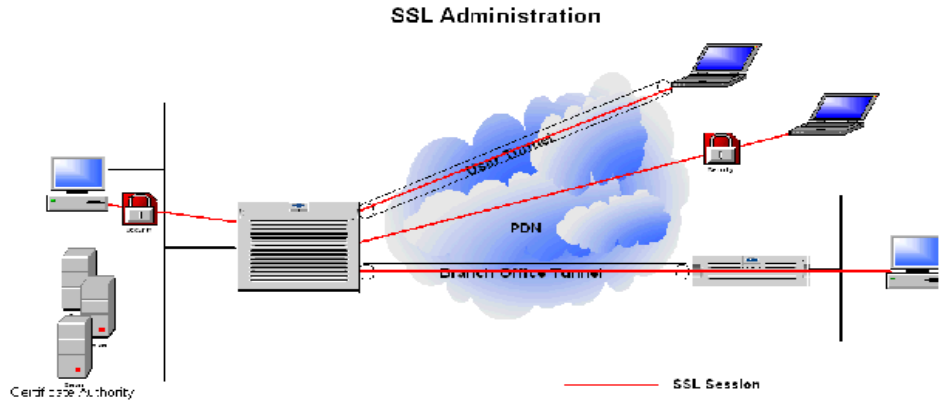
The DHCP Relay Statistics screen provides the following details:

- In--total number of all of the incoming DHCP packets.
- Out-- total number of forwarded DHCP packets.
- Discarded--total number of incoming packets that were ignored because of bad content.
- Relayed To Server--total number of packets forwarded to a DHCP server(s).
- Relayed To Client--total number of packets forwarded to DHCP client(s).

Configuring SSL administration

The SSL Administration feature enables secure management of the Contivity gateway over SSL-enabled HTTP (HTTPS) and can be used over all tunnel and interface types. Remote management of a Contivity gateway device only requires an SSL-enabled Web browser on the administrator's computer. SSL-enabled Web browsers are included with most operating systems today.

Figure 7 SSL administration



SSL/TLS uses TCP port 443 for secure HTTP communication. Interface and tunnel filters can be used to govern HTTPS packets destined to the management address. If tunnel filters are enabled, HTTPS must be allowed for SSL management through a VPN tunnel.

The Contivity Stateful Firewall only applies to HTTPS traffic routed through the device and not to the management IP address. An HTTPS service object has been added to the implied rule set and cannot be modified.

The Contivity gateway uses HTTPS services for Firewall User Authentication (FWUA) and SSL-Enabled Administration.

The following cipher combinations are available:

- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- RC4-SHA
- RC4-MD5
- EXP1024-RC4-SHAEXP1024-DES-CBC-SHA
- EXP1024-RC4-MD5
- EDH-RSA-DES-CBC-SHA
- DES-CBC-SHA
- EXP-EDH-RSA-DES-CBC-SHA

- EXP-EDH-DSS-DES-CBC-SHA
- EXP-DES-CBC-SHA

To use SSL Administration, you must:

- Have HTTPS services enabled for the public and/or private interface on the Services > Available screen.
- Explicitly allow HTTPS if tunnel filters are enabled on the Profiles > Filters screen for management through a VPN tunnel.
- Install a valid server certificate on the Contivity gateway and applied to the SSL/TLS services to authenticate and validate SSL connections.
- Select ciphers and apply the server certificate on the Services > SSL/TLS screen.
- Have an SSL-enabled Web browser
- Have a valid administrator user name and password.

Browser security checks

When using certificates, Netscape Communicator and Internet Explorer perform different security checks. The following configuration is recommended to obtain the best performance when administering the Contivity gateway securely using SSL administration.

1. Make an entry in the hosts file corresponding to your Contivity gateway management IP address, such as 11.0.0.12 Contivity1.
2. Import the root certificate that issued your Contivity gateway server certificate into the browser store as follows:
   - For Netscape Communicator to accept the mime type application/ x-x509-ca-cert:

   a. Go to Edit >Preferences.

   b. Click on Applications.

   c. Click on New Type. Anew window appears.

   d. Fill in the following information in the new window:

   — Description of type--CAcert
   — File extension--cacert

— MIME Type--application/x-x509-ca-cert

— Application to use--netscape.exe

e Click on Ok to complete the Netscape configuration.

f Save the base64 format root CA certificate onto a file with extension .cacert.

g Go to File > Open Page and open the file. Netscape Communicator will guide you in installing the CA certificate.

- In Internet Explorer, go to Tools > Internet options > content > certificates > trusted root certification authority tab and select import.

3 Import the root certificate that issued your Contivity gateway server certificate into the JRE certificate store.

Note: To satisfy a further name check by Netscape browsers, the Contivity gateway server certificate common name should be either a DNS name that resolves to the management IP address or the management IP address.

Configuring SSL/TLS and configuring HTTP services

To configure SSL/TLS and enable HTTP services:

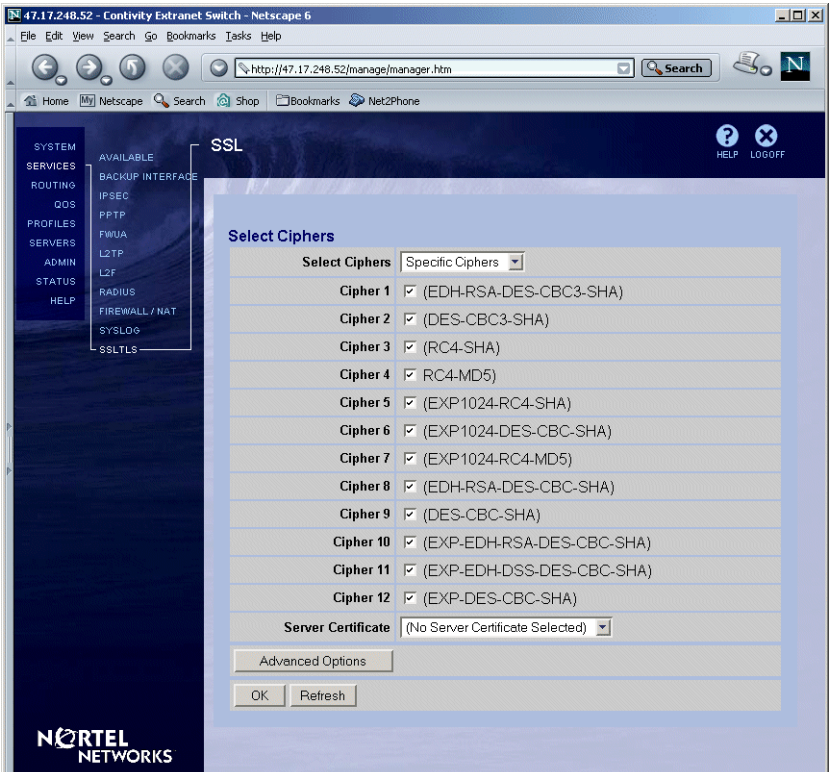
1 Go to Services > Available and check HTTPS services on the public and/or private interfaces. This allows TCP port 443 through the system filter. If you enable HTTPS on both the public and private interfaces, it allows port 443 through either interface.

Figure 8 HTTPS services

2 Go to Services > SSLTLS, check the necessary ciphers and select a digital server certificate (for example, CN=ces1, O=MyOrg, C=US).

3 Click on the Advanced Options button and check the box if you do not want to have empty fragment for CBC ciphers inserted and click on Apply.

Figure 9 Select ciphers



4 Verify SSL is enabled on the Web browser of the management PC.

To test the SSL administration feature, direct an SSL-enabled Web browser to the private interface of the Contivity gateway. To use this service from the public side of the Contivity gateway, you must direct your browser to the public IP address.

Configuring DNS servers

The Domain Name Service (DNS) is a method for mapping host names to IP addresses. It allows the Internet to provide an updated set of mappings for all Internet devices.

A DNS server holds the segment of the DNS database for which it has authority. DNS clients are any TCP/IP applications that refer to hosts by host name. When an application needs to convert a host name to its IP address, it uses the client portion, which creates a DNS query specifying the host name and sends the query to a server. The server tries to find the host IP address by looking in its database or by making queries to other servers. Eventually, a DNS response is returned to the application, which contains the IP address or an error indicating that the host name is unknown.

It is common for companies to set up their own domain name system internally, and leave it to the ISP to handle all external DNS. These companies have their own DNS servers, but use the external DNS servers for non-company names. This *splits* the DNS names into two separate systems: the private, company-controlled DNS names and the Internet DNS names.

The Contivity gateway provides the following DNS services:

- DNS Proxy where the Contivity gateway caches information from corporate DNS for faster address resolution. This eliminates the need for separate branch office server. See Configuring DHCP and DNS Servers in *Configuring Authentication and Certificates for the Contivity Secure IP Services Gateway.*
- Split Proxy DNS occurs when a negative response from a DNS server (private) prompts the Contivity gateway to try a second DNS server (Internet). Split DNS supports private and Internet names without mixing the two and eliminates the need to publish private names on public DNS. See Configuring DHCP and DNS Servers in *Configuring Authentication and Certificates for the Contivity Secure IP Services Gateway.*

You can configure the Contivity 1010, 1050, or 1100 as a DNS proxy, which means that it can act like a DNS server for any PC on the private network. The PCs are configured to send their DNS queries to the DNS proxy, which in turn passes the query to its set of *true* DNS servers. Whether you have configured DHCP client or PPPoE determines which DNS servers will respond. When the DNS proxy receives a DNS query form a PC, it passes the query on to the DNS servers until it receives a response, which is subsequently returned to the PC.

You can configure up to four DNS servers. The ISP can assign more than one DNS server, which are displayed on the screen, but cannot be changed. You should enable split DNS if your DNS name space has been split into private names and public names; a DNS server knows the private names while another server knows the public Internet DNS names.

To configure a DNS server:

1. Got to the System > Identity screen.
2. The DNS Proxy Enabled/Disabled check box allows you to select whether you want the DNS Proxy to act as a DNS server to the private side. It resolves names for locally connected hosts and those from other DNS zones. It it enabled by default.
3. Click on the Split DNS check box if you have a split name space.
4. For Primary, enter the address of the DNS server that the DNS proxy tries to contact first.
5. For Second, enter an address for the Second Domain Name System (DNS) server. If the Primary DNS server doesn't respond in a few seconds, service is requested of the Second DNS server (if present).
6. For Third, enter an address for the Third Domain Name System (DNS) server. If the Primary and Secondary DNS servers doesn't respond, service is requested of the third DNS server (if present).
7. For Fourth, enter an address for the Fourth Domain Name System (DNS) server. If the preceding servers doesn't respond, service is requested of the fourth DNS server (if present).
8. Click on OK. The Contivity gateway checks all of the DNS addresses to see if they respond and then provides an operational or error status.

Chapter 3
Using certificates

Digital certificates are a means of binding an entity's public encryption or signing key to its identity, and having that identity verified and vouched for by a trusted third party (the certification authority). Digital certificates are used for authenticating both LDAP and VPN connections.

LDAP server SSL encryption

Secure socket layer (SSL) provides Internet security and privacy and ensures privacy between the Contivity gateway and the external LDAP server. The SSL protocol negotiates encryption keys and authenticates the server before any data is exchanged. SSL maintains the transmission channels security and integrity through encryption, authentication, and message authentication codes. The SSL implementation supports the following encryption methods:

- RC4 128-bit MD5 allows clients to request RC4 128-bit MD5 encryption, which is the most secure method. The longer the encryption key, the more secure the encryption. US export law controls the export of 128-bit encryption keys.
- DES 56-bit SHA allows clients to request DES 56-bit SHA encryption, which is the mid-level encryption method, less secure than RC4-128, but more secure than RC4-40.
- RC4 40-bit MD5 allows clients to request RC4 40-bit MD5 encryption, which is the least secure method of encryption.

You can configure SSL parameters when you switch from internal to external LDAP servers.

Installing LDAP certificates

The LDAP connection between the Contivity gateway and the directory server is authenticated asymmetrically. Initially a one-way authenticated SSL connection is established when the directory server passes its certificate to the Contivity gateway. After SSL authentication is established, the Contivity gateway authenticates itself to the directory server by presenting its LDAP bind DN and password.

For the SSL connection to be successful, the Contivity gateway must trust the issuer of the certificate being presented by the directory server during the initial SSL authentication.

To import SSL certificates:

1. Go to the System > Certificates screen and select Import > SSL Certificate.
2. Paste the PKCS #7 formatted CA certificate into the input box.
3. Click on OK.

LDAP special characters

The LDAP special character enhancement allows certificate subject DNs to be created containing previously unsupported special characters, such as the comma. This enhancement is compliant with RFC 2253.

It's not necessary to enable the special character support if the certificate subject DN does not contain special characters such as comma (,), quotes (") or backslash (\) as valid characters.

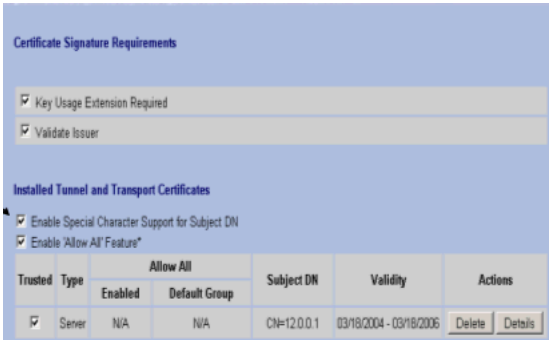
Note: You may need to update the LDAP to use this feature if upgraded from an older version and the cert subject DN already contains special characters. Contact Nortel technical support for details to update of the LDAP.

To configure LDAP special characters:

1. Go to System > Certificates.

2 Under the Installed Tunnel and Transport Certificates section, select the Enable Special Character Support for Subject DN checkbox. The default is disabled.

Figure 10 LDAP special characters



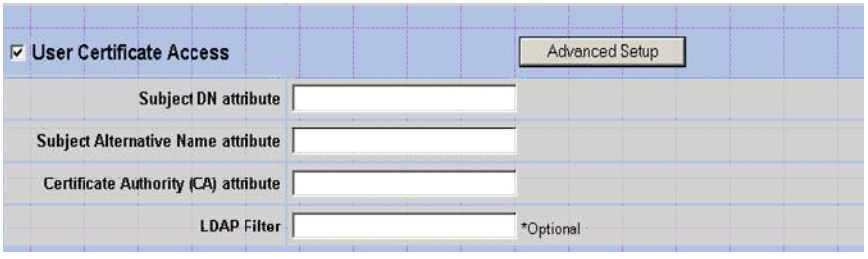
External LDAP proxy

An enhancement to the external LDAP proxy allows a more flexible method to locate the user record. It supports the mapping of the following certificate subject DN attributes to defined LDAP attributes:

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

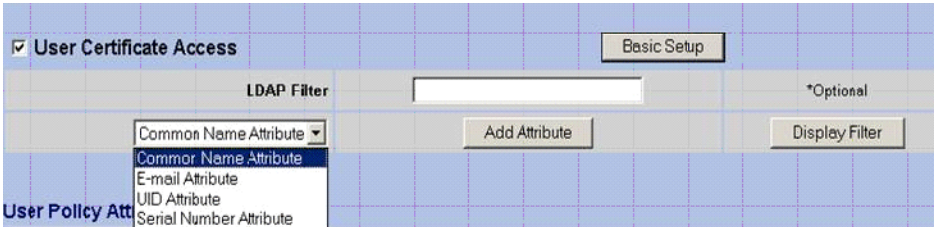
The basic setup is the current method, and is the default on upgrade.

Figure 11 External LDAP default



The advanced setup includes the new flexible mapping.

Figure 12 External LDAP advanced setup



VPN security using digital certificates

You can use X.509 certificates to authenticate IPsec tunnels and L2TP/IPsec tunnels. The Contivity gateway supports RSA digital signature authentication for the IPsec IKE key management protocol. Remote users can authenticate themselves to the Contivity gateway using a public key pair and a certificate as credentials. The Contivity gateway uses its own key pair and certificate to authenticate the Contivity gateway to the user. The Contivity gateway must explicitly import and trust the CA certificate that issued the certificate to the tunnel initiator.

Setting up public key infrastructure (PKI)

A PKI is used to issue and manage certificates for both network hosts and end users. An important decision about the design of a PKI is how to implement CA services:

- You may use commercially available products from a vendor such as Entrust, where the CA resides in your facility and is operated by you.
- You can subscribe to a CA provider, such as the VeriSign OnSite service, where the CA is operated by VeriSign from a remote location.

CA and X.509 certificates

The CA issues and revokes certificates within a PKI. The CA certifies certificates are valid by signing each certificate with its own digital signature. A copy of all signed certificates are stored in a publicly accessible certificate repository. Certificate users use this repository to verify that other user's certificates are valid.

Loading certificates

Two types of certificate must be installed in the Contivity gateway: server certificates and trusted CA certificates. Server certificates are certificates that the Contivity gateway requests for itself, and uses to prove its identity to connecting tunnels. Trusted CA certificates are certificates that are issuing end user or branch office tunnel certificates, and are imported by the Contivity gateway to establish a common trust.

Server certificates can be requested either manually (using cut and paste #7 and #10) or automatically with Certificate Management Protocol (CMP) support.

Generating a server certificate request

Consult the CA user documentation for instructions on generating reference numbers and authorization codes, as well as general CA administration information. When you use Entrust CA generated certificates with your Contivity Secure IP Services Gateway

- When you use HTTP-based cut and paste operations, either Entrust Web certificates or Entrust Enterprise certificates will work properly.
- When you use CMP automated lifecycle management for requesting and renewing certificates, be aware that Entrust does not support CMP renewal for Web certificates.

Installing server certificates using cut and paste #7 and #10

To install server certificates using PKCS #7 and #10:

1. Go to System > Certificates: Generate Certificate Request screen.
2. Click on PKCS #10 (or PKCS #7) Certificate Request.

3 If prompted, enter a password to secure the certificate on the Contivity gateway.

4 Fill out the required information for the certificate request.

5 Click OK.

6 Copy and paste or save your encoded certificate request (including certificate request begin and certificate request end lines) to a file.

7 Follow the instructions from your CA provider on how to obtain a certificate.

8 Submit the request to the applicable CA by pasting the encoding into the CA's request screen, following the instructions provided by the CA for signing the certificate request.

9 Click on Server Certificate to indicate that you are importing a server certificate. Import the signed certificate request and click on OK.

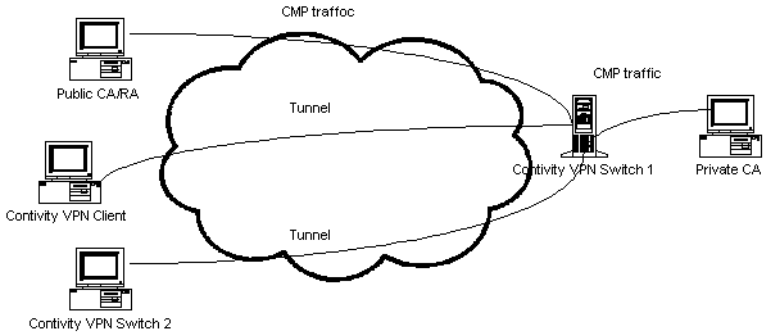
Note: When you are using Entrust CA, this request must have a subject distinguished name with a common name that is equal to the Entrust reference number that is used to preauthorize the certificate issuance.

Installing server certificates using CMP

The Certificate Management Protocol (CMP) allows you to create a CMP compliant certificate request. CMP targets management functions for the entire certificate/key life for enrollment, renewal, recovery and revocation. It defines message formats and includes its own message protection. The CA can be located on the private network if it has a publicly accessible IP address.

Figure 13 shows a CMP environment.

Figure 13 Sample CMP environment



To initialize the Contivity gateway for initial certificate enrollment with CMP, you must have:

- Issuer name - CA distinguished name
- Subject name - EE distinguished name (common name, organization, organizational unit)
- Reference number - used to identify the secret value
- Transaction ID or authorization code - initial secret value
- Enrollment URL or destination (host name or IP address) and optional port number
- Imported root CA certificate

To enter this information:

1. Go to the System > Certificates screen and click on the Certificate Management Protocol (CMP) button to go to the Certification Request - CMP screen. This screen displays the status of any outstanding requests and the fields to fill out for a new request.
2. For a new request, enter the reference number provided by the CA that is used to identify the secret value.
3. Enter the authentication key supplied by the CA.
4. Click on the drop-down list to select one of the following exportable public key sizes in bits (generally, larger keys are more secure):
   - 512
   - 768

- 1024
- 2048 (US only)

5 Enter the port number.

6 Enter the enrollment URL or destination host name or IP address.

7 Check Import Issuer CA Certificate if you want to automatically import the CA Root certificate with this request.

8 Under Subject Distinguished Name (optional), select Relative if you are providing a relative name or Full if you are providing a full name. If you select Relative, then enter the relative name details:

a Enter the common name associated with the Contivity gateway.

b Enter the organizational unit associated with the Contivity gateway.

c Enter the organization associated with the Contivity gateway.

d Enter the locality where the Contivity gateway resides.

e Enter the state or province where the Contivity gateway resides.

f Enter the country where the Contivity gateway resides.

9 Under Issuer Distinguished Name (optional), select Relative if you are providing a relative name or Full if you are providing a full name. If you select Relative, then enter the relative name details:

a Enter the common name associated with the Contivity gateway.

b Enter the organizational unit associated with the Contivity gateway.

c Enter the organization associated with the Contivity gateway.

d Enter the locality where the Contivity gateway resides.

e Enter the state or province where the Contivity gateway resides.

f Enter the country where the Contivity gateway resides.

10 Click on Apply.

11 On the System > Certificates Certificate Generation screen, select the Details option. This displays information from the certificate enrollment process. It provides the address for the key update, key recovery, and revocation purposes.

12 Enter the certificate enrollment configuration information:

a In the port field, enter the port number of the CA.

b In the Enrollment Address field, enter the IP address of the CA.

c In the Renew Certificate Now field, check to renew now.

d In the Renew Days before expiration, select and enter the number of days before the certificate expires.

e In the Recover Certificate field, enter the certificate reference number and authentication code.

f In the Revoke Certificate Now field, select to revoke the certificate.

Installing trusted CA certificates

The trusted CA certificate is the issuer of the certificate that the remote user or branch office tunnel is using to authenticate, and it must be loaded and marked as trusted in the Contivity gateway.

To import trusted CA certificates in PKCS #10 format:

1. Go to the Contivity Secure IP Services Gateway URL.
2. Go to the System > Certificates screen.
3. Select Import Tunnel Certificate.
4. Select Trusted CA Certificate (default).
5. Paste the certificate into the paste box.
6. Click on OK. The Installed Tunnel Certificates table displays the certificate entry.
7. Enable Allow All if desired.
8. Click on OK. You have now obtained the CA certificate against which remote users can authenticate. Repeat this operation if multiple CAs will be issuing user certificates.

   Optionally, you can configure a CRL distribution point to enable revocation checking of client certificates. Click on the System > Certificates: Installed Tunnel Certificates: CA Details button, enter the appropriate CRL Information, and click on OK.

The Enabled check box enables CRL checking of certificates for the particular CA. The Search Base, Host, Connection, and values must be set for proper access to the CRL LDAP directory store.

Setting certificate parameters

You can set the following parameters from the System > Certificates > Certificate Configuration screen:

1. Under Certificate Signature Requirements, select Key Usage Extension Required: to require the Key Usage V3 extension to be present in all certificates presented as part of a tunnel initiation (user and branch office).
2. Under Installed Tunnel and Transport Certificates, select Enable Allow All Feature: to enable this feature for all CA certificates. This allows all tunnel requests authenticated by a particular CA to be allowed in, providing a significant configuration savings because individual users are not required to be provisioned into the Contivity gateway.
3. Select Trusted to indicate that the certificate is trusted. For CA certificates, this indicates that tunnel requests presenting this issuer as the signer of their certificate are trusted. For server certificates, this is a method of turning off the certificate, without having to delete it.

The System > Certificate Details screen provides the following certificate details:

- This Certificate Belongs To shows the certificate owner's X.500 distinguished name.
- This Certificate Was Issued By shows the issuer of the certificate (the Certificate Authority). In addition to the main attributes, this field also shows the issuer's certificate serial number.
- Validity Dates show the starting and ending dates through which the certificate is valid (for example, 01/29/02 through 01/29/03).
- Certificate Fingerprint shows the unique identifier that is derived from MD5 hashing the certificates. The identifier should be compared with the fingerprint supplied directly by the certificate's issuer (for example, a CA). If the fingerprints do not match exactly, the certificate has been forged or modified.

- CRL query optimization enables CRL performance improvement (LDAP import only). Set this option to Disabled to disable CRL performance improvements.
- Version provides information about the version.
- Signature Algorithm provides information about the signature algorithm.
- Public Key provides information about the public key.
- Extensions provides information about the extensions being used.

You must configure a group that is using certificate-based authentication to present a server certificate to remote parties that are initiating tunnel requests. The Default Server Certificate is the Subject DN of the certificate that you want to use as the identity of the Contivity gateway when initiating or responding to a connection request associated with that group. Tunnel requests are bound to a particular group by the CA certificate that the remote party is presenting as the signer of its certificate. You can set up the local identity for the group on the Profiles > Groups > Edit screen.

Trusted CA certificate settings

Every CA certificate must be associated with a group to be used to authenticate incoming tunnel requests. The group assignment of incoming tunnel requests is accomplished by either finding the user provisioned in the Contivity gateway's directory (internal or external), or by allowing all users issued by a particular CA to gain access. If all users issued by a particular CA are allowed, there are two ways of determining the group that an initiator gets assigned to (direct assignment into the group assigned to that CA, or access control by subject DN).

Group assignment by user identification

If the subject DN of the certificate presented by the remote initiator of the tunnel is a user located on that Contivity gateway, the group that the user is bound to is the one indicated in that user's configuration.

Allow All policy

Using Allow All, the Contivity gateway trusts the CA to establish the true identity of a user. If the user's certificate is within the certificate validity period, the certificate's signature can be verified using the CA certificate, and the user's certificate is not on the CA's CRL, the tunnel connection is permitted. Using the Allow All policy means that once users are certified by the CA, they can create a tunnel connection as long as their certificate is in good standing.

You can allow all users with certificates issued by this CA to authenticate with the Contivity gateway, regardless of whether they have a user entry in the Contivity gateway's LDAP database. By default, the CA certificate does not allow all users authentication. Only users with their subject distinguished names (DNs) entered into the Profiles > Users screen are able to authenticate using certificates issued by this CA. If you enable Allow All users to authenticate, you must also select a group for these users from the Default Group drop-down list box. If you want only specific instances of users to authenticate with the CA authority, you must configure each of these users from the Profiles > Users > Edit screen, and disable Allow All authentication for this CA. Only these users can then perform IPsec RSA Digital Signature Authentication using a certificate issued by this particular CA.

The Allow All feature must be enabled for each CA certificate against which you want to permit authentication without an explicit user entry. This allows anyone with a valid certificate from the particular CA to establish a tunnel connection. Also, you must associate a default group with that certificate. The client authenticating with the Allow All feature then uses the attributes associated with that group. You can also assign Allow All users to specific groups by matching the relative DN of a connecting certificate user. You are not limited to a single default group.

Note: Branch Office connections do not support the CA Certificate Allow All feature. Therefore, you must configure an explicit Branch Office connection.

Access control by Subject DN

This form of mapping incoming requests to groups allows the subject DN of incoming certificates to be parsed to a configured depth and associated with a corresponding group. During the client authentication process, the Contivity gateway tries to match the client's certificate subject DN with all the associations of the CA. The match could be a partial match or an exact match. In case of a partial match, the longest match from the root of DN is used. After a match is found, the client is assigned to the corresponding group. If no match is found, the client is assigned to the default group of the CA.

A DN has multiple components (RDN). The most common ones are common name (CN), country name (C), locality name (L), state/province name (S), organization (O), and organizational unit (OU). The order of the RDN does not matter unless multiple OUs are present, but ordering the DN in the following sequence avoids ambiguity: C, S, L, O, OU, and CN.

The following examples show group mappings:

```
ou=Contivity, o=Nortel, c=US/base/contivity
ou=Engineering, ou=Contivity, o=Nortel, c=US/base/contivity/
Engineering
ou=Marketing, ou=Contivity, o=Nortel, c=US/base/contivity/
Marketing
ou=Engineering, o=Bay Networks, L=Boston, S=MA, c=us/base/bay
```

Group and certificate association configuration

This feature provides finer control for a user to associate a certificate with a group for IPsec tunnel connections. Each Certificate Authority user can set up a lookup table between the certificate subject DN and a Contivity gateway group. When a new tunnel using the certificate is authenticated, the Contivity gateway uses the certificate's subject DN to lookup the group in the table. If there is a match (or partial match), the new tunnel will bind to the group specified in the table.

If no match is found in the lookup table, the new tunnel is bound to the default group if it is configured and if the Allow All feature is turned on. Otherwise, the tunnel is denied.

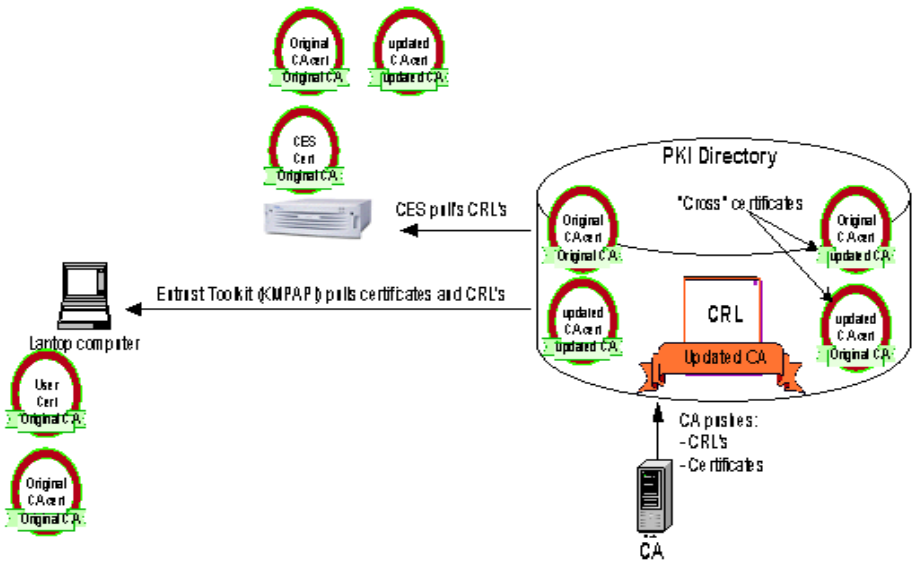
All the attributes (Lookup Table, Allow All, and default group) are CA-specific. To configure the Group and Certificate Lookup Table:

1. Select the CA.
2. Click on the Details button.
3. Click on the Add button under Group Access Control. Usually, you should use a partial Subject DN (omitting one or more left most fields) to simplify the configuration. You can select Relative or Full to specify the partial Subject DN. Relative automatically generates the DN string. If it exists in the certificate's subject DN, no field in the middle should be omitted, such as o=Nortel or st=MA.
4. Click on OK.

CA key update

The CA key update provides uninterrupted certificate authenticated user and Branch Office tunnel connections before, during, and after the “Entrust Key Update” function is performed by the CA in a given PKI environment. A key update may be performed for security or other reasons.

Figure 14 CA Key Update ready for authentication



Prior to a key update, the original CA certificate (which is a self signed root certificate in the diagram above) is pushed out to the directory by the CA, along with the CRL it produced (a list of revoked certificates, digitally signed by the CA certificate). Both the Contivity gateway and the user's PC have certificates signed by that CA, as well as the self signed CA certificate itself. The user authenticates the Contivity gateway certificate because it has the original CA certificate that was used to create the Contivity gateway certificate stored locally. Likewise the Contivity gateway can authenticate the user because it has the CA certificate that issued the user certificate. The Contivity gateway can also verify that the user's certificate is not revoked, because it is been configured to periodically retrieve the latest CRL from the directory. It is able to authenticate that CRL because it has the CA certificate that was used to sign it.

After CA Key Update occurs, the directory now contains four certificates: the original self signed, the new self signed and two "cross" certificates. From this point forward, all CRL's issued by the CA will be signed by the updated CA.

There are no user tunnel or Contivity gateway server authentication issues presented at this point, because the certificates presented by the Contivity gateway and the user are signed by the original CA, and both parties have that CA certificate stored locally for authentication.

Authenticating the CRL presents a problem for the Contivity gateway at this point because it is signed by the updated CA certificate, and the Contivity gateway does not have that updated CA certificate locally to authenticate the CRL signature. The solution is to import the updated CA certificate into the Contivity gateway.

Importing the updated CA certificate into the Contivity gateway is a requirement that must be undertaken immediately following the CA key update. All post key update CRL processing and therefore tunnel authentication, will fail until this action is taken.

Configuring a certificate revocation list (CRL)

A CA can revoke user and server certificates whenever the associated key pair is no longer valid, the key pair has been compromised, the user has left the organization, or a server has been retired, among other reasons. When a certificate is revoked, the CA updates an associated revocation list with the revoked certificate's serial number. This list is referred to as a certificate revocation list (CRL). A CA can have one or more associated CRLs.

Note: When you attempt to delete a certificate and that certificate is referenced you will receive an error message. The certificate will not be removed until you remove all references to that certificate.

CRLs are published by the CA in an associated LDAP-accessible directory service. The publication frequency is set by the CA administrator. In an Entrust environment, a new CRL can be automatically published at a set time, at any time manually set by an administrator, or whenever a certificate is revoked. In a VeriSign OnSite environment, new CRLs are published at a fixed interval, typically 24 hours.

Note: When a certificate revocation list (CRL) directory is located on the public side of the Contivity gateway, the gateway retrieves the CRLs through the public interface. Reply packets may be dropped if the size of the CRL is large enough that the LDAP response will include approximately 40 IP packets or more. To correct this, enable the Contivity Stateful Firewall.

The Contivity gateway can optionally use CRLs to verify the revocation status of user certificates. If enabled on the Contivity gateway, CRLs are periodically retrieved from the CA's LDAP directory store and cached into the Contivity gateway's associated LDAP database. This allows for rapid verification of user certificates during IPsec tunnel establishment. You can configure the frequency with which the Contivity gateway checks for a new CRL.

Because a CRL is signed using the CA's private key, it is protected against tampering. The Contivity gateway verifies the CRL signature each time it is used. A CRL server must be configured for each trusted CA certificate that is imported into the Contivity gateway.

Note: The LDAP server that contains CRLs for the CA certificates on the Contivity gateway must be reachable from the public or private interface.

Configuring CRL servers

The following list provides explanations for CRL settings:

- CRL Checking Enabled shows CRL usage enabled on the Contivity gateway on a per-CA basis. To enable the use of CRLs for a CA, click on the Details button on the main System > Certificates screen. The section labeled Certificate Revocation List Information is used to configure the necessary information. The Enabled check box turns on CRL checking of certificates for the particular CA. The Search Base, Host, Connection, and Update frequency values must be set for proper access to the CRL LDAP directory store.
- CRL Retrieval Enabled determines whether the Contivity gateway will try to retrieve a CRL from the configured directory. If the CRL retrieval is successful, the Contivity gateway verifies the revocation status of the presented certificates. If this option is not selected, the Contivity gateway does not attempt to retrieve a CRL, and does not verify revocation status of presented certificates; deselecting this option has the effect of turning off CRL checking.
- CRL Checking Mandatory determines if a CRL must be present when an IPsec tunnel is established to a particular CA. If this is selected, the Contivity gateway *must* have a CRL present for tunnel connections to be successful. If this is not selected, the Contivity gateway will allow certificate authenticated tunnels when no CRL is present.
- CRL Update Frequency allows you to enter a value in minutes that represents the frequency with which the Contivity gateway should query the CA’s LDAP server for a newly published CRL. The default value of 0 indicates that this Contivity gateway does not update any CRLs. This option is useful when more than one Contivity gateway share an LDAP database, but you want only

one Contivity gateway to actually perform the update operation. To minimize the load on an external LDAP server, it is important to make sure that only one or two Contivity gateways are updating a shared CRL entry in a multiple-gateway, shared external LDAP environment.

- CRL System Status is read-only and is automatically updated by the Contivity gateway to reflect the CRL updating activity.

To configure CRL servers:

1. From the System > Certificates > CA Certificate: Details screen, click on the Manage CRL Servers button to access the Manage CRL Servers screen. A list of currently configured CRL servers for the CA that you can edit or delete is shown at the top of this screen. The New CRL Server section allows you to configure and add a new CRL server.
2. In the Search Base field, enter the portion of the X.500 directory where the CA stores certificate revocation lists. Following is a sample search base entry:

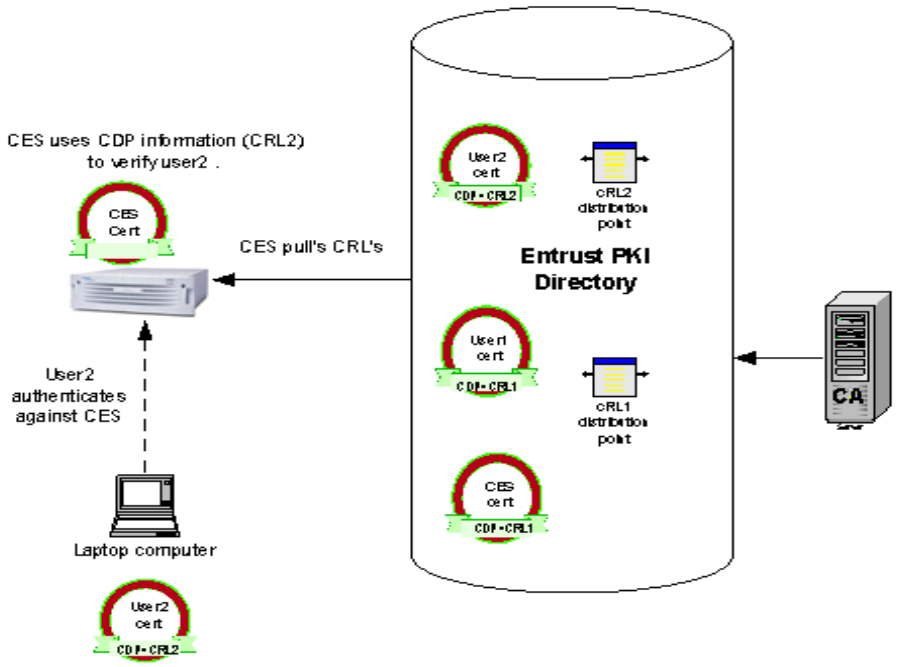
   ```
   ou=Engineering, o=Nortel Networks, c=US
   ```

3. In the host field, enter the host name or IP address of the LDAP-accessible directory server that is storing the published CRLs. If a host name is used in place of an IP address, then one or more DNS servers must be configured on the Contivity gateway's System > Identity screen.
4. In the Connection field, enter the port number that is associated with the LDAP server. Optionally, enable the use of the Secure Socket Layer (SSL) to secure the connection with the LDAP server. SSL is not required in general for handling CRLs because a CRL is signed and is therefore protected against modification and spoofing.
5. Select the Enabled or Disabled state from the list box to enable or disable the CRL server.

CRL distribution points

CRL distribution points (CDP) identifies how CRL vendor-specific information is obtained. It is supported for Entrust CAs. When implemented, users authenticate only against the CRL that is specified in the certificate CDP. This provides faster tunnel establishment.

Figure 15 CRL distribution points



Authenticating only against the CRL that is specified in certificates CDP results in a tunnel being established in a shorter time. When you present a certificate for verification, a CDP from your certificate is obtained. Using that CDP information, a filter for LDAP query is built and only CRL records that matches your CDP are obtained. That way you will be authenticated against one CRL instead of all available CRLs.

Even if the list of CRLs is long, it will not affect performance of the Contivity gateway because only one CRL will be used. If CRL checking is set to mandatory and CRLs are not present on the Contivity gateway, a request is made to CA LDAP to only obtain the CRL that is specified in the user's certificate CDP. Only that CRL will be loaded into Contivity gateway LDAP. CRL optimization enabled

When CRL optimization is enabled, CRL checking is done by using Global CRL collection. Global CRL collection is stored in Contivity gateway memory. When CDP support is implemented a user’s certificate obtained from the Entrust CA is verified against one CRL from Global CRL collection. CDP information will be obtained from the certificate and used to determine which CRL from Global CRL collection to use. The search will not be expensive since the Global CRL

collection is already located in memory. If Global CRL collection has not been loaded into memory yet we load all CRLs from Contivity gateway LDAP into Global CRL collection. When Global CRL collection is enabled users will not reference LDAP but rather Global CRL Collection. We have to keep all CRLs in Global CRL Collection for that reason.

CRL retrieval

All the CRL records are retrieved periodically. The time when CRL records have to be updated depends on a configured interval. When an Entrust user i is authenticated, only one CRL is obtained from the Contivity gateway LDAP. Each CRL record has the next update time set to determine if the CRL record is stale. If the CRL record is stale, it is refreshed from CA LDAP. Because the collection of CRLs only has one specific (CDP based) CRL, the next update time is always specific for one CRL record.

Sometimes the CA has to go through the key update procedure. Then the Contivity gateway could have two CA certificates with the same DN name (Link Certificates feature). CRL collections for both CAs will follow the same CDP support logic.

Enabling certificate use for tunnels

For IPsec, you must enable RSA digital signature support for any default groups that are associated with CAs, and the groups containing any specific instances of users who are doing certificate-based authentication.

1. From the Profiles > Groups > Edit > IPsec > Configure: RSA Digital Signature field, click on the RSA Digital Signature check box to enable RSA digital signature support.
2. Select the appropriate default server certificate from the drop-down list box. This is the certificate that is sent to clients to authenticate the Contivity gateway's identity. This server certificate should be issued from the same CA PKI that issued the remote access clients' certificates.
3. Click on OK.

For L2TP/IPsec authentication:

1 Click on the 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 made on the Authentication portion of the previous screen are lost.

2 Enter the local UID. This is the user ID of the local Contivity gateway that you are configuring.

3 Enter the peer UID. This is the user ID of the remote Contivity gateway that you are configuring.

4 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.

Identifying individual users with certificates

As an alternative to allowing all users issued by a particular CA to gain access to the Contivity gateway, users can be identified explicitly by certificate attributes.

To create IPsec certificate credentials:

1 Go to the Profiles > Users > Add User/Edit screen.

2 Select a valid issuer Certificate Authority from the drop-down list. These Certificate Authorities are configured from the System > Certificates: Generate Certificate Request screen.

3 Enter either the relative distinguished name or the full distinguished name. The relative distinguished name is a collection of the following components that uniquely identify the remote peer in an IPsec certificate environment.

   a Enter the organization with which the user is associated.

   b Enter the organizational unit with which the user is associated.

   c Enter the common name with which the user is associated.

   d Enter the country in which the user resides.

   e Enter the state or province in which the user resides.

f Enter the locality in which the user resides.

Enter the full distinguished name (FDN) in this field, rather than entering the individual components in the relative distinguished name fields. A sample entry follows:

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

4 You can optionally enter a subject alternative name in place of a subject DN, and specify the format of the name. The following formats are acceptable:

- E-mail name (for example, net_admin@company.com)
- DNS name (for example, gateway.cleveland.company.com)
- IP address (for example, 192.168.34.21)

Identifying branch offices with certificates

The Authentication section of the Profiles > Branch Office > Edit Connection screen allows you to configure the authentication that is used between the local and remote branch office Contivity gateways. The fields that appear in this screen depend on whether you are using an IPsec, PPTP, or L2TP tunnel type.

Click on the 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 made on the Authentication part of the previous screen are lost.

IPsec authentication

In the Authentication portion of the screen, fill out the following information:

1 Enter the pre-shared key as a 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.

2 Certificates are associated with each endpoint Contivity 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.

3 Remote Identity 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.

4 Select a valid issuer CA from the certificate authority list. 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 on the Certificates screen. If a CA hierarchy is being used, all intermediary CAs below the trusted CA must have been imported to the Contivity gateway. These certificate authorities are configured from the System > Certificates: Generate Certificate Request screen.

5 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.

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

6 The relative distinguished name has the following supported components:

- 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.

7 The local identity is the name of the Contivity 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 this system. If you select a subject alternative name from the Contivity gateway's certificate, then that identity is used in place of the Contivity gateway's subject DN when communicating with peers.

Note: The Contivity gateway's server certificate has subject alternative names only if the 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 E-mail alternative names.

8 Click the list to view all certificates that have been issued to the server. Server certificates are configured from the System > Certificates: Generate Certificate Request screen.

L2TP/IPsec authentication

In the Authentication section of the screen, fill out the following information:

1 Under Local UID, enter the user ID of the local Contivity gateway that you are configuring.

2 Under Peer UID, enter the user ID of the remote Contivity gateway that you are configuring.

3 Enter the password for the local 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.

4 Click on Enable or Disable to enable or disable compression.

5 Click to enable or disable the Compression/Encryption Stateless Mode option. This option is not used if encryption and compression are both disabled.

6 The L2TP Access Concentrator (for L2TP authentication only) field appears if you selected L2TP as the preferred tunnel type for the branch office connection. Use this entry to specify the L2TP access concentrator that you want to perform authentication between the Contivity gateway and the NAS.

7 Select an IPsec data protection minimum level (Triple DES, 56-bit DES, or Authentication Only).

8 Select a valid issuer CA from the drop down list.

9 Enter the DN to identify the remote branch office site.

10 Select the server certificate issued by the same CA as the remote branch certificate from the drop down list under Local Identity.

11 Click on OK.

Index

F

G

H

I

L

O

P

R

S

T

X