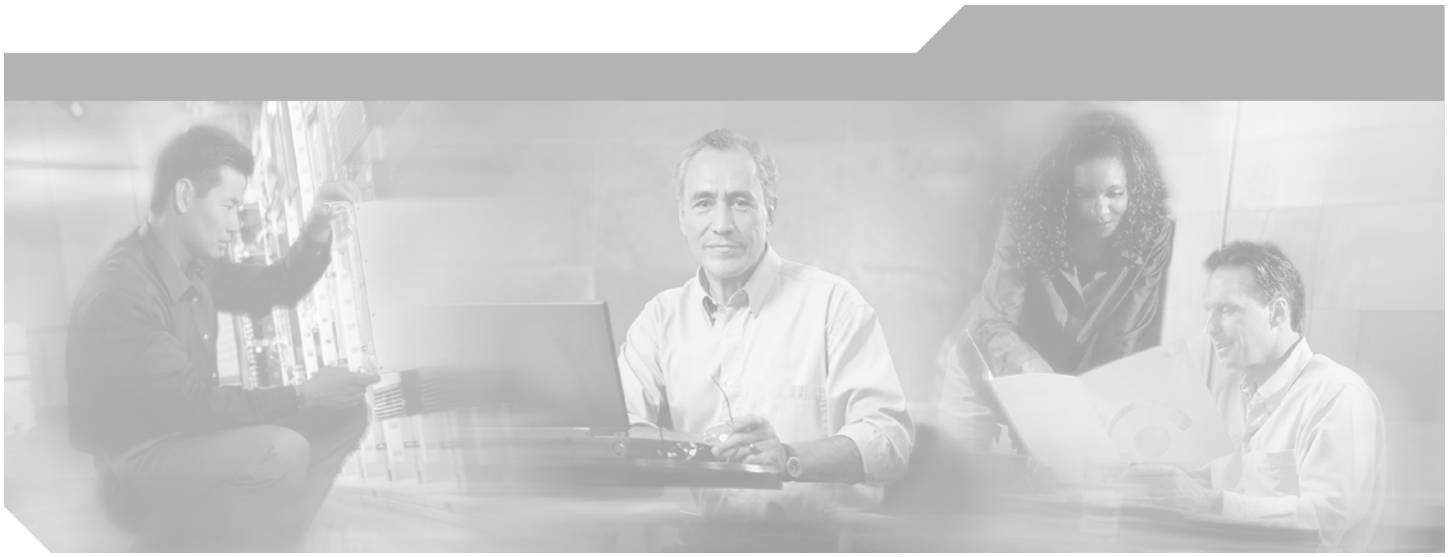


Cisco Network-Based IPSec VPN Solution Release 1.5 Implementation Guide

May, 2003

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number:
Text Part Number: OL-3132-01

About This Guide

The Cisco network-based IPSec VPN solution release 1.5 is a network-based IP security (IPsec) Virtual Private Network (VPN) integrated solution that allows a service provider to offer scalable services to securely connect remote locations to a customer's corporate VPN extranet or intranet.

This document and other documents related to this solution can be found under Cisco Network-Based IPSec VPN Solution at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/vpn/solution/index.htm.

Note All Cisco solutions documents can be found under Cisco Solutions at the following URL: http://www.cisco.com/univercd/cc/td/doc/solution/index.htm

This preface presents the following major topics:

Audience

The target audience for this guide is assumed to have familiarity with basic Cisco IOS commands and operations for configuring the following Cisco components:

- Cisco 7204 and Cisco 7206 routers
- Cisco 800 series routers
- Cisco 1700 series routers
- Cisco 2600 series routers
- Cisco 3600 series routers
- Cisco VPN 3002 hardware clients

Scope

This guide presents the fundamental design and configuration information that is required to establish the various services provided by the Cisco Network-Based IPSec VPN Release 1.5 . Service provider networks may have additional requirements that are beyond the scope of this document.

In addition, this document is primarily for Cisco products. To establish and maintain third-party products and applications that may be a part of the Cisco Network-Based IPSec VPN Release 1.5 , refer to the documentation provided by the vendors of those products.

Document Organization

The chapters of this guide are as follows:

- Chapter 1, "Establishing Solution Components" provides information on establishing required components, establishing optional components, and basic configurations.
- Chapter 2, "IPSec to MPLS Service Models" describes how to configure this deployment model.
- Chapter 3, "IPSec to L2VPN Service Model" describes how to configure this deployment model.
- Chapter 4, "IPSec to IPSec Service Model" describes how to configure this deployment model.
- Chapter 5, "IPSec to GRE Service Models" describes how to configure this and related deployment models.
- Chapter 6, "Configuring AAA Servers for Remote Clients" provides configuration information for AAA servers, Unity clients, and RADIUS servers.
- Glossary—Defines abbreviated terms used in this document.
- Index

Related Documents

Most of the documents referred to in the *Cisco Network-Based IPSec VPN Solution Release 1.5 Implementation Guide* are available online. In the electronic (PDF) version of this document you can click the URL (Uniform Resource Locator, often referred to as the website) associated with the title of a document, and the selected document will appear within the Adobe Acrobat application window. You can also use the Text Select Tool (third icon from the top, at the left of the Acrobat application window) to copy a URL from the PDF document and paste it into the location field of your browser.

Viewing Online Documents in Your Browser

As you click on links, the files you select may be added to the current document. When you close the file, you will be prompted to save the file. (You will not be able to save the file to a CD.) If you choose not to save the larger file that is created, click **No** when prompted to save the file. However, if you acquire documents that you want to save in a new file, you can save that file to another disk or drive with a new name of your own choosing. Set the following preferences within the Acrobat application to open weblinks in your browser, rather than within Acrobat.

You can obtain the latest version of Adobe Acrobat Reader at http://www.adobe.com.

Step 1 Select the browser you want to use.

a. From the Acrobat main menu, choose **File > Preferences > Weblink**. The Weblink Preferences window opens.

b. In the Weblink Preferences window, click Browse (or Select) and locate the browser you wish to use.

c. Select Connection Type from the pull-down menu. Choose Standard if your browser is not listed.

d. Click **OK** to save your settings.

Step 2 Make sure that Acrobat opens weblinks in your browser.

a. From the Acrobat main menu, choose **File > Preferences > Web Capture**. The Web Capture Preferences window opens.

b. Choose Open Weblinks: In Web Browser.

c. Click **OK** to save your settings.

Document Conventions

Command descriptions use the following conventions:

boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternate keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use the following conventions:

`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.[1]
italic screen font	Arguments for which you supply values are in *italic screen* font.
⟶	This pointer highlights an important line of text in an example.
< >	Nonprinting characters, such as passwords, are in angle brackets in contexts where italic font is not available. Also used to represent variables in command line examples where `screen` font is used.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

1. As this document makes use of annotated configurations, the rigorous use of boldface type to indicate what the user must enter is relaxed.

Note the use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Tips use the following conventions:

Tip Means the following information *will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Terms and Acronyms

For definitions of terms and acronyms used in the following chapters, refer to the glossary at the end of this document.

For an online listing of internetworking terms and acronyms, refer to the following URL:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) through the online Subscription Store:

http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) Website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/en/US/support/index.html

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before you call, check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, have your service agreement number and your product serial number available.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:

  http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html

- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:

  http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in the design, development, and operation of public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

Establishing Solution Components

Use the *Cisco Network-Based IPSec VPN Solution Release 1.5 Implementation Guide* to establish, configure, and manage the services introduced in the Cisco network-based IPSec VPN solution release 1.5. Links to this and other documentation related to this solution are available at the following URL: http://www.cisco.com/univercd/cc/td/doc/solution/index.htm.

To configure a network that takes advantage network-based IPSec VPNs, read the *Cisco Network-Based IPSec VPN Solution Release 1.5 Overview and Planning Guide*.

This chapter briefly introduces and presents links for the following major topics:

- Establishing required and optional components
- Basic configurations

The service models supported by the Network-Based IPSec VPN are as follows (refer to Chapter 2, in the *Cisco Network-Based IPSec VPN Solution Release 1.5 Overview and Planning Guide)*:

- IPSec into MPLS VPN
- IPSec to L2VPN
- IPSec to IPSec
- IPSec to GRE

Note Only the fundamental steps to establish unified communications are described in Chapter 2 of the *Cisco Network-Based IPSec VPN Solution Release 1.5 Overview and Planning Guide*, to illustrate the basic issues.

Establishing Required Components

Establishing Access Concentrators

The equipment you need for a network-based IPSec VPN may already be installed in your network. For the latest information on installing and configuring components, including release notes, refer to the URLs listed in this chapter.

The following Cisco access concentrators are required parts of the solution:

- Cisco 7204 router
- Cisco 7406 router

Cisco 7204 Router

Refer to Cisco 7206 router at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/core/7204/index.htm

For specific information, see:

- Cisco 7204 Installation and Configuration Guide
  http://www.cisco.com/univercd/cc/td/doc/product/core/7204/7204ig/index.htm
- Quick Reference For Cisco 7204 Installation
  http://www.cisco.com/univercd/cc/td/doc/product/core/7204/7204qrc/index.htm
- Cisco 7200 Regulatory Compliance and Safety Information
  http://www.cisco.com/univercd/cc/td/doc/product/core/7206/3419pnc6.htm
- Site Preparation and Safety Guide
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/hw_doc/safety/index.htm
- Cisco 7200 Series Port Adapter Hardware Configuration Guidelines
  http://www.cisco.com/univercd/cc/td/doc/product/core/7206/port_adp/config/index.htm
- Port Adapters
  http://www.cisco.com/univercd/cc/td/doc/product/core/7204/portadpt/index.htm
- Field Replaceable Units (FRUs)
  http://www.cisco.com/univercd/cc/td/doc/product/core/7204/fru/index.htm
- Cisco 7200 Troubleshooting
  http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/7200trbl.htm
- Links to Other Documentation and Sites
  http://www.cisco.com/univercd/cc/td/doc/product/core/7202/7200link.htm
- Cisco 7200 Series Routers Boot Image Information
  http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/14936b.htm

Installing VPN Acceleration Module

For information on the VPN Acceleration Module (VAM), see:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122y/122ye/1229ye/12ye_vam.htm.

To install VAM cards, see:
http://www.cisco.com/en/US/products/hw/modules/ps2797/products_module_installation_guide_book09186a008007c95c.html.

Configuring Cisco IOS Software

For information on the Cisco IOS software release used with the Cisco 7204 router for the Cisco network-based IPSec VPN solution release 1.5, see
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/index.htm.

Cisco 7206 Router

Refer to Cisco 7206 router at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/core/7206/index.htm

For specific information, see:

- Cisco 7200 Series Routers and Cisco 7401ASR Documentation
  http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/12767f.htm
- Cisco 7206 Installation and Configuration Guide
  http://www.cisco.com/univercd/cc/td/doc/product/core/7206/7206ig/index.htm
- Cisco 7206 Quick Start Guide
  http://www.cisco.com/univercd/cc/td/doc/product/core/7206/12771q.htm
- Quick Reference For Cisco 7206 Installation
  http://www.cisco.com/univercd/cc/td/doc/product/core/7206/7206qrc/index.htm
- Cisco 7200 Regulatory Compliance and Safety Information
  http://www.cisco.com/univercd/cc/td/doc/product/core/7206/7206qrc/index.htm
- Site Preparation and Safety Guide
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/hw_doc/safety/index.htm
- Cisco 7200 Series Port Adapter Hardware Configuration Guidelines
  http://www.cisco.com/univercd/cc/td/doc/product/core/7206/port_adp/config/index.htm
- Port Adapters
  http://www.cisco.com/univercd/cc/td/doc/product/core/7206/port_adp/index.htm
- Field Replaceable Units (FRUs)
  http://www.cisco.com/univercd/cc/td/doc/product/core/7206/fru/index.htm
- Cisco 7200 Troubleshooting
  http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/7200trbl.htm
- Links to Other Documentation and Sites
  http://www.cisco.com/univercd/cc/td/doc/product/core/7202/7200link.htm
- Cisco 7200 Series Routers Boot Image Information
  http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/14936b.htm

Installing VPN Acceleration Module

To install VAM cards, see:
http://www.cisco.com/en/US/products/hw/modules/ps2797/products_module_installation_guide_book09186a008007c95c.html.

Configuring Cisco IOS Software

For information on the Cisco IOS release used with the Cisco 7204 router for the Cisco network-based IPSec VPN solution release 1.5, see:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/index.htm.

Establishing Internet Protocol Solutions Center Version 3.0

Cisco Internet Protocol Solutions Center (ISC) Version 3.0 offers support for IPSec as well as support for MPLS (multiprotocol label switching). It provides a customizable service and network layers FCAPS (fault, configuration management, accounting, performance, security) management solution to facilitate rapid IP VPN service deployment and reduce ongoing operational costs.

For information on using ISC Version 3.0 to set up devices in an IPSec environment as well as defining IPSec networks and customers, see
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/index.htm.

Establishing Optional Components

The following Cisco platforms can be used as customer premises equipment at the remote locations for IPSec termination to the Cisco 7200 series router:

Cisco PIX Firewall with EzVPN client

Refer to Cisco PIX Firewall with EzVPN client at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_62/config/basclnt.htm#xtocid0.

Cisco VPN 3002 Hardware Client

Refer to Cisco VPN 3002 hardware client at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3002/3_6/index.htm.

Cisco 800 Series Routers

Refer to the following Cisco 800 series routers at the following URLs:

- Cisco 801 through 804 routers:
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/800/index.htm
- Cisco 805 router:
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/805/index.htm
- Cisco 806 router
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/806/index.htm
- Cisco 811 and Cisco 813 routers
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/811-813/index.htm
- Cisco 826 router
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/826/index.htm
- Cisco 827 routers
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/827/index.htm
- Cisco 828 and SOHO 78 routers
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/828/index.htm

Cisco 1700 Series Routers

Refer to Cisco 1700 series routers at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/index.htm

Cisco 2600 Series Routers

Refer to Cisco 2600 series routers at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/index.htm

Cisco 3600 Series Routers

Refer to Cisco 3600 series routers at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3600/index.htm

Cisco 7200 Series Routers

Refer to Cisco 7200 series routers at the following URL:

- Cisco 7200
  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7000/index.htm
- Cisco 7010
  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7010/index.htm
- Cisco 7100
  http://www.cisco.com/univercd/cc/td/doc/product/core/7100/index.htm
- Cisco 7200VXR
  http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/index.htm
- Cisco 7202
  http://www.cisco.com/univercd/cc/td/doc/product/core/7202/index.htm
- Cisco 7204
  http://www.cisco.com/univercd/cc/td/doc/product/core/7204/index.htm
- Cisco 7206
  http://www.cisco.com/univercd/cc/td/doc/product/core/7206/index.htm

IPSec to MPLS Service Models

This chapter describes how to configure the IPSec to MPLS and GRE+IPSec into MPLS service models for the Cisco Network-Based IPSec VPN Release 1.5 .

Configuring the IPSec to MPLS Service Model

In the IPSec to MPLS configuration, the service provider has an existing MPLS backbone and operates an MPLS VPN that interconnects all customer sites. This includes remote customer sites that are part of the MPLS VPN.

This configuration enables secure off-net access to MPLS VPNs through IPSec. It allows MPLS providers to extend access to their on-net MPLS VPNs to include worldwide Internet access. Customers who wish to deploy a dynamic routing model can use GRE combined with IPSec (see Configuring GRE+IPSec to MPLS Service Model, page 2-15).

A remote customer site initiates an IPSec session from the CE that terminates on a unique interface on the aggregating Cisco 7200 PE. The Cisco 7200 PE then maps the site from the interface to its respective VPN.

Each VPN is associated with one or more VPN routing or forwarding instances (VRFs). A VRF consists of an IP routing table, a derived Cisco express forwarding (CEF) table and a set of interfaces that use this forwarding table. VRF provides multiple routing instances with each instance independent of others within an IPSec aggregator. You can associate the VRF with one or more VPNs.

As a provider edge (PE) router on the MPLS network, the Cisco 7200 series router advertises the connected routes to the remote PEs containing the same VPN.

Before You Begin

The procedures provided here are specific to configuring IPSec to MPLS and are based on the following assumptions:

1. That the following setup and configuration tasks have already been completed:
   - Setup of the core MPLS network
   - Setup of the customer VPN
   - Configuration of the links between the PE and the CE
   - Customer-specific information is complete

2. That you have a good understanding of the architecture and features you are using and that you have selected the means you will use to implement those features (for example, which of several strategies to use for address management or for user authentication and authorization).

IPSec to MPLS Configuration Checklist

This section deals with configuring the router to function as both the IPSec Aggregator and the PE router.

Procedures for competing each task are described in the sections that follow. If you are viewing this document online, you can click on highlighted text to get details on the procedure.

Note Read the Release Notes, which supplement and, if different, take precedence over information here.

Table 2-1 IPSec to MPLS Configuration Checklist

Task 1: Configure Authentication and Authorization Lists for Clients to RADIUS, page 2-3
Task 2: Configure VRFs, page 2-3.
Task 3: Enable CEF Switching, page 2-3.
Task 4: Configure the Keyring, page 2-4
Task 5: Configure ISAKMP Policy for Phase 1 Negotiations, page 2-4
Task 6: Configure DPD Keepalives, page 2-4
Task 7: Configure Client Group for Local Authorization, page 2-4
Task 8: Configure ISAKMP Profile for VPN Sites, page 2-4
Task 9: Configure Dynamic VRF Association for VPN Sites, page 2-5
Task 10: Configure ISAKMP Profile for VPN Clients, page 2-5
Task 11: Configure Dynamic VRF Association for VPN Clients, page 2-5
Task 12: Configure XAUTH, Group Authorization, and Mode-Config, page 2-5
Task 13: Configure the Transform Set for Data Encryption, page 2-6
Task 14: Configure Dynamic Crypto Map and Apply Transform Set, page 2-6
Task 15: Configure ISAKMP Client Profile Reference, page 2-6
Task 16: Configure RRI, page 2-6
Task 17: Configure Static Crypto Map for Sites, page 2-6
Task 18: Configure ISAKMP Site Profile Reference, page 2-7
Task 19: Configure Dynamic Crypto Map for Clients, page 2-7
Task 20: Configure BGP Peering Source Interface, page 2-7
Task 21: Configure Internet-Facing Interface and Corresponding Crypto Maps, page 2-7
Task 22: Configure Interface for Tag Switching, page 2-8
Task 23: Configure IGP Used in Core for BGP Access, page 2-8
Task 24: Configure BGP to Carry VPN Routes, page 2-8
Task 25: Configure Peers to Receive VPNv4 Routes, page 2-8
Task 26: Configure IPv4 Address-Family for Each VPN, page 2-9

Table 2-1 IPSec to MPLS Configuration Checklist (continued)

Task 27: Configure Pool to Distribute IP Addresses to VPN Clients, page 2-9
Task 28: Configure Global Default Route, page 2-9
Task 29: Configure Static VPN Routes, page 2-10
Task 30: Configure the Crypto Access List to Define Traffic to be Encrypted, page 2-10

IPSec to MPLS Configuration Tasks

Typical IPSec to MPLS configuration tasks are shown below. Refer to the section titled IPSec to MPLS Configuration Sample, page 2-11.

Task 1: Configure Authentication and Authorization Lists for Clients to RADIUS

	Command	Purpose
Step 1	**aaa authentication login**	Set authentication, authorization, and accounting (AAA) authentication at login.
Step 2	**aaa authorization**	Set parameters that restrict user access to a network.

Task 2: Configure VRFs

	Command	Purpose
Step 1	`ip vrf`	Configure a VPN routing and forwarding (VRF) routing table.
Step 2	`rd route-distinguisher`	Create routing and forwarding tables for a VRF.
Step 3	`route-target {import | export | both}`	Create a route-target extended community for a VRF.

Task 3: Enable CEF Switching

	Command	Purpose
Step 1	`ip cef`	Enable Cisco Express Forwarding (CEF).
Step 2	`mpls label protocol {ldp | tdp}`	Specify the default label distribution protocol.
Step 3	`tag-switching ip default-route`	Enable the distribution of labels associated with the IP default route.

Task 4: Configure the Keyring

	Command	Purpose
Step 1	**crypto keyring** keyring-name [**vrf** fvrf]	Configure a new keyring for the shared secret keys to be used during Internet Key Exchange (IKE) authentication.
Step 2	**pre-shared-key** {**address** address [mask] | **hostname** hostname} **key** key	Configure the addressed preshared key to be used during IKE authentication.

Task 5: Configure ISAKMP Policy for Phase 1 Negotiations

	Command	Purpose
Step 1	**crypto isakmp policy** priority	Configure an IKE policy.
Step 2	**encryption {des | 3des | aes | aes 192 | aes 256}**	Specify the encryption algorithm within an IKE policy.
Step 3	**authentication {rsa-sig | rsa-encr | pre-share}**	Specify the authentication method within an IKE policy.

Task 6: Configure DPD Keepalives

Command	Purpose
crypto isakmp keepalive secs retries	Allow the gateway to send dead peer detection (DPD) messages to the router.

Task 7: Configure Client Group for Local Authorization

	Command	Purpose
Step 1	**crypto isakmp client configuration group** {group-name | default}	Specify which group's policy profile will be defined.
Step 2	**key** name	Configure the IKE preshared key for group policy attribute definition.
Step 3	**pool** (name)	Configure a local pool address.

Task 8: Configure ISAKMP Profile for VPN Sites

Command	Purpose
crypto isakmp profile profile-name	Define an ISAKMP profile for a VPN.

Task 9: Configure Dynamic VRF Association for VPN Sites

	Command	Purpose
Step 1	**vrf** name	Associate the on-demand address pool with a VPN routing and forwarding instance (VRF) name.
Step 2	**keyring** keyring-name	Associate a keyring with an isakmp profile.
Step 3	**match identity address** address [mask] [fvrf]	Match an acceptable Phase 1 identity from a peer to a particular ISAKMP profile.

Task 10: Configure ISAKMP Profile for VPN Clients

	Command	Purpose
Step 1	**crypto isakmp profile** profile-name	Define an ISAKMP profile for a VPN.
Step 2	**vrf** name	Associate the on-demand address pool with a VPN routing and VRF name.

Note The Remote sites can be configured to match each peer. This is configured using sequence numbers in the crypto map definition. The peer can be matched on IP address or the hostname. The IP address match list for traffic to be encrypted is also defined for each peer. In the case of VPN clients, the dynamic profile defined earlier is used to match the clients.

Task 11: Configure Dynamic VRF Association for VPN Clients

	Command	Purpose
Step 1	**vrf** name	Associate the on-demand address pool with a VPN routing and VRF name. See vrf for information on using this command.
Step 2	**match identity** group-name	Match an acceptable Phase 1 identity from a peer to a Unity group.

Task 12: Configure XAUTH, Group Authorization, and Mode-Config

	Command	Purpose
Step 1	**client authentication list** list-name	Configure IKE extended authentication (Xauth) on your router. The list-name must match the list-name defined during authentication, authorization, and accounting (AAA) configuration

Step 2	**isakmp authorization list** list-name	Configure group authorization IKE querying of AAA for tunnel attributes in aggressive mode.
Step 3	**client configuration address [initiate | respond]**	Configure IKE mode configuration (Mode-Config).

Task 13: Configure the Transform Set for Data Encryption

Command	Purpose
crypto IPSec transform-set transform-set-name transform1 [transform2] [transform3] [transform4]	Define the transform set.

Task 14: Configure Dynamic Crypto Map and Apply Transform Set

	Command	Purpose
Step 1	**crypto dynamic-map** dynamic-map-name dynamic-seq-num	Create a dynamic crypto map entry and enter the crypto map configuration command mode.
Step 2	**set transform-set** transform-set-name	Specify which transform sets can be used with the crypto map entry.

Task 15: Configure ISAKMP Client Profile Reference

Command	Purpose
set isakmp-profile profile-name	Set the ISAKMP profile name for client.

Task 16: Configure RRI

Command	Purpose
reverse-route [remote-peer]	Create source proxy information for a crypto map entry through RRI.

Task 17: Configure Static Crypto Map for Sites

	Command	Purpose
Step 1	**crypto map** map-name seq-num [**IPSec-isakmp**]	Create a crypto map entry that uses IKE to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.
Step 2	**set peer** {hostname | ip-address}	Specify an IP Security peer in a crypto map entry.
Step 3	**set transform-set** transform-set-name	Specify which transform sets can be used with the crypto map entry.

Task 18: Configure ISAKMP Site Profile Reference

	Command	Purpose
Step 1	**set isakmp-profile** profile-name	Set the ISAKMP profile name reference.
Step 2	**match identity address** address [mask] [fvrf]	Match an acceptable Phase 1 identity from a peer to a particular ISAKMP profile.

Task 19: Configure Dynamic Crypto Map for Clients

Command	Purpose
crypto map map-name seq-num [**IPSec-isakmp**]	Create a crypto map entry that uses IKE to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.

Task 20: Configure BGP Peering Source Interface

	Command	Purpose
Step 1	**interface** type	Configure a loopback interface (emulates an interface that is always up).
Step 2	**ip address** ip-address mask	Set an IP address for an interface.

Task 21: Configure Internet-Facing Interface and Corresponding Crypto Maps

	Command	Purpose
Step 1	**interface** type	Configure a loopback interface (emulates an interface that is always up).
Step 2	**ip address** ip-address mask	Set an IP address for an interface.
Step 3	**encapsulation dot1q** vlan-id **[native]**	Enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN).
Step 4	**crypto map** map-name	Apply a previously defined crypto map set to an interface.

Note Each interface services one VPN as the IPSec tunnel endpoint for both the sites and clients.

Task 22: Configure Interface for Tag Switching

	Command	Purpose
Step 1	**interface** type	Configure a loopback interface (emulates an interface that is always up).
Step 2	**ip address** ip-address mask	Set an IP address for an interface.
Step 3	**encapsulation dot1q** vlan-id **[native]**	Enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.
Step 4	**tag-switching ip**	Allow label switching of IPv4 packets.

Task 23: Configure IGP Used in Core for BGP Access

	Command	Purpose
Step 1	**router ospf** process-id	Configure an OSPF routing process.
Step 2	**log-adjacency-changes**	Generate a log message.
Step 3	**network ip**-address wildcard-mask **area** area-id	Configure the interfaces on which OSPF runs and to define the area ID for those interfaces.

Task 24: Configure BGP to Carry VPN Routes

	Command	Purpose
Step 1	**router bgp** as-number	Configure the BGP routing process.
Step 2	**no synchronization**	Disable the synchronization between BGP and your Interior Gateway Protocol (IGP) system.
Step 3	**bgp log-neighbor-changes**	Enable logging of BGP neighbor resets.
Step 4	**neighbor** {ip-address | peer-group-name} **remote-as** number	Add an entry to the BGP neighbor table.
Step 5	**no auto-summary**	Disable the default behavior of automatic summarization of subnet routes into network-level routes.

Task 25: Configure Peers to Receive VPNv4 Routes

	Command	Purpose
Step 1	**address-family**	Enter the address family submode for configuring routing protocols such as BGP, RIP, and static routing.
Step 2	**neighbor** {ip-address | peer-group-name} **activate**	Enable the exchange of information with a neighboring router.

Step 3	**no auto-summary**	Disable the default behavior of automatic summarization of subnet routes into network-level routes.
Step 4	**exit-address-family**	Exit from the address family configuration submode.

Task 26: Configure IPv4 Address-Family for Each VPN

	Command	Purpose
Step 1	**address-family**	Enter the address family submode for configuring routing protocols such as BGP, RIP, and static routing.
Step 2	**redistribute** protocol	Redistribute routes from one routing domain into another routing domain.
Step 3	**no auto-summary**	Disable the default behavior of automatic summarization of subnet routes into network-level routes.
Step 4	**no synchronization**	Disable the synchronization between BGP and your IGP system.
Step 5	**exit-address-family**	Exit from the address family configuration submode.

Task 27: Configure Pool to Distribute IP Addresses to VPN Clients

Command	Purpose
ip local pool {**default** | pool-name low-ip-address [**high-ip-address**]}	Configure a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.

Task 28: Configure Global Default Route

Command	Purpose
ip route network-number network-mask {**ip-address** | **interface-name**} **[distance] [name** name]	Establish static routes and define the next hop for large-scale dial-out.

Task 29: Configure Static VPN Routes

Command	Purpose
ip route vrf vrf-name prefix mask **[next-hop-address] [interface {interface-number}] [global] [distance] [permanent] [tag** tag**]**	Establish static routes for a VPN routing and forwarding (VRF) instance.

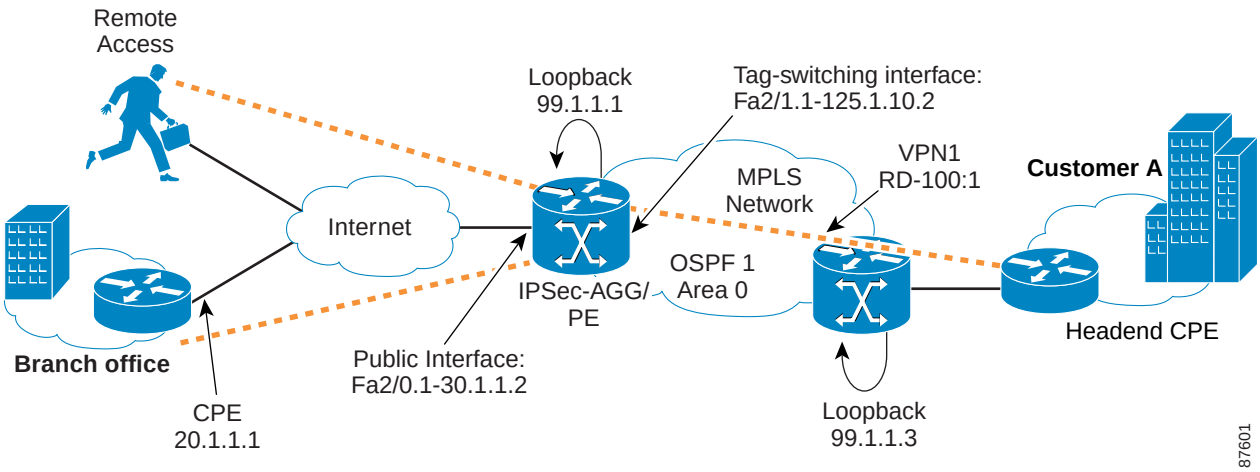
Task 30: Configure the Crypto Access List to Define Traffic to be Encrypted

Command	Purpose
access-list access-list-number **{deny** | **permit}** source **[source-wildcard] [log]**	Configure a standard IP access list.

IPSec to MPLS Configuration Sample

Figure 2-1 illustrates the following IPSec to MPLS configuration.

Figure 2-1 IPSec to MPLS Configuration




```
pe1#sh run
Building configuration...

Current configuration : 3874 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname pe1
enable password cisco
!
username cisco password 0 cisco
aaa new-model
```

Step 1 Configure Authentication and Authorization for RADIUS.

```
aaa authentication login localist local
aaa authorization network localist local
aaa session-id common
ip subnet-zero
no ip domain lookup
!
```

Step 2 Configure the VRFs.

```
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
```

Step 3 Enable CEF switching.

```
ip cef
mpls label protocol ldp
mpls ldp logging neighbor-changes
tag-switching ip default-route
```

Step 4 Configure the keyring VPN.

```
crypto keyring vpn1
  pre-shared-key address 20.1.1.1 key cisco123
pre-shared-key address 40.1.1.2 key cisco123
```

Step 5 Configure the ISAKMP policy for Phase 1 negotiations.

```
crypto isakmp policy 1
 authentication pre-share
 group 2

crypto isakmp policy 2
 encr 3des
 authentication pre-share
```

Step 6 Configure DPD keepalives.

```
crypto isakmp keepalive 30
crypto isakmp xauth timeout 30
```

Step 7 Configure client group for local authorization.

```
crypto isakmp client configuration group ezvpn
 key cisco123
 pool hw-pool
```

Step 8 Configure ISAKMP profile for VPN sites.

```
crypto isakmp profile vpn1
```

Step 9 Configure dynamic VRF association for sites.

```
   vrf vpn1
   keyring vpn1
   match identity address 20.1.1.1 255.255.255.255
   match identity address 40.1.1.2 255.255.255.255
```

Step 10 Configure ISAKMP profile for VPN clients.

```
crypto isakmp profile vpn1-ez
   vrf vpn1
```

Step 11 Configure dynamic VRF association for VPN clients.

```
   match identity group ezvpn
```

Step 12 Configure XAUTH, group authorization, and mode-config.

```
   client authentication list localist
   isakmp authorization list localist
   client configuration address respond
```

Step 13 Configure the transform Set.

```
crypto IPSec transform-set tset1 esp-3des esp-sha-hmac
```

Step 14 Configure dynamic cryptomap and apply transform set.

```
crypto dynamic-map dyna 1
 set security-association idle-time 3600
 set transform-set tset1
```

Step 15 Configure ISAKMP client profile reference.

```
 set isakmp-profile vpn1-ez
```

Step 16 Configure RRI.

```
 reverse-route
```

Step 17 Configure static crypto map for site.

```
crypto map vpn 10 IPSec-isakmp
 set peer 20.1.1.1
 set transform-set tset1
```

Step 18 Configure ISAKMP site profile reference.

```
 set isakmp-profile vpn1
 match address 101
```

Step 19 Configure Dynamic crypto map for clients.

```
crypto map vpn 1000 IPSec-isakmp dynamic dyna
!
interface Loopback0
```

Step 20 Configure BGP peering source interface.

```
 ip address 99.1.1.1 255.255.255.255
!
interface FastEthernet2/0
 no ip address
 duplex auto
 speed auto
```

Step 21 Configure Internet facing interfaces and corresponding crypto maps.

```
interface FastEthernet2/0.1
 encapsulation dot1Q 10
 ip address 30.1.1.2 255.255.255.0
 crypto map vpn
!
interface FastEthernet2/1
 no ip address
 duplex auto
 speed auto
```

Step 22 Configure the interface for tag switching.

```
interface FastEthernet2/1.1
 encapsulation dot1Q 10
 ip address 125.1.10.2 255.255.255.0
 tag-switching ip
!
```

Step 23 Configure the IGP used in the Core for BGP Reachability.

```
router ospf 1
 log-adjacency-changes
 network 99.1.1.1 0.0.0.0 area 0
 network 125.1.10.0 0.0.0.255 area 0
```

Step 24 Configure BGP to carry VPN routes.

```
router bgp 100

 no synchronization
 bgp log-neighbor-changes
 neighbor 99.1.1.3 remote-as 100
 neighbor 99.1.1.3 update-source Loopback0
```

```
 no auto-summary
```

Step 25 Configure peers to receive VPNv4 routes.

```
address-family vpnv4
 neighbor 99.1.1.3 activate
 neighbor 99.1.1.3 send-community both
 no auto-summary
 exit-address-family
```

Step 26 Configure IPv4 address-family for each VPN.

```
 address-family ipv4 vrf vpn1
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
```

Step 27 Configure the pool to distribute IP addresses to VPN clients.

```
ip local pool hw-pool 192.168.1.1 192.168.1.254
ip classless
```

Step 28 Configure static routes for public IP addresses global default route.

```
ip route 0.0.0.0 0.0.0.0 FastEthernet2/0.1 30.1.1.1
```

Step 29 Configure static VPN routes if not using IGP with in the VPN.

```
ip route vrf vpn1 101.1.1.0 255.255.255.0 30.1.1.1 global
no ip http server
no ip http secure-server
```

Step 30 Configure the crypto access list to define traffic to be encrypted.

```
access-list 101 permit ip 101.1.2.0 0.0.0.255 101.1.1.0 0.0.0.255
```

Configuring GRE+IPSec to MPLS Service Model

The GRE+IPSec to MPLS configuration is an extension of IPSec to MPLS. This configuration differs from the preceding IPSec to MPLS configuration in that a GRE tunnel transports routing updates between the remote CPE and the IPSec-aggregator/PE instead of IPSec. The configuration shows GRE+IPSec for site-to-site while still supporting client termination.

Before You Begin

The procedures provided here are specific to configuring GRE+IPSec to MPLS and are based on the following assumptions:

1. That the following setup and configuration tasks have already been completed:
   - Setup of the core MPLS network.
   - Setup of the customer VPN
   - Configuration of the links between the PE and the CE.
   - Customer-specific information is complete.
2. That you have a good understanding of the architecture and features you are using and that you have selected the means you will use to implement those features (for example, which of several strategies you will use for address management or for user authentication and authorization).

GRE+IPSec to MPLS Configuration Checklist

This section deals with configuring the router to function as both the IPSec Aggregator and the PE router.

Procedures for competing each task are described in the sections that follow. If you are viewing this document online, you can click on highlighted text to get details on the procedure.

Table 2-2 GRE+IPSec to MPLS Configuration Checklist

Task 1: Configure Authentication and Authorization Lists for Clients to RADIUS, page 2-16.
Task 2: Configure the VRFs, page 2-16.
Task 3: Enable CEF Switching, page 2-17.
Task 4: Configure the Keyring, page 2-17
Task 5: Configure ISAKMP Policy for Phase 1 Negotiations, page 2-17
Task 6: Configure DPD Keepalives, page 2-17
Task 7: Configure Client Group for Local Authorization, page 2-18
Task 8: Configure ISAKMP Profile for VPN Sites, page 2-18
Task 9: Configure Dynamic VRF Association for VPN Sites, page 2-18
Task 10: Configure XAUTH, Group Authorization, and Mode-Config, page 2-18
Task 11: Configure ISAKMP Profile for GRE, page 2-18
Task 12: Configure the Transform Set for Data Encryption, page 2-19
Task 13: Configure IPSec Profile for GRE and Apply Transform Set, page 2-19

Table 2-2 GRE+IPSec to MPLS Configuration Checklist (continued)

Task 14: Configure ISAKMP Client Profile Reference, page 2-19
Task 15: Configure RRI, page 2-19
Task 16: Configure Dynamic Crypto Map for Clients, page 2-20
Task 17: Configure GRE Tunnel to Customer Site, page 2-20
Task 18: Configure IPSec Profile, page 2-20
Task 19: Configure Internet-Facing Interface and Corresponding Crypto Maps, page 2-20
Task 20: Configure Interface for Tag Switching, page 2-21
Task 21: Configure the IGP Used in the Core, page 2-21
Task 22: Configure Routing Protocol Across GRE Tunnel, page 2-21
Task 23: Configure Address Family Definition per VRF, page 2-21
Task 24: Redistribute VPN Routes Learned Through BGP, page 2-21
Task 25: Configure BGP to Carry VPN Routes, page 2-22
Task 26: Configure Peers to Receive VPNv4 Routes, page 2-22
Task 27: Configure IPv4 Address-Family for Each VPN, page 2-22
Task 28: Redistribute Routes Learned Over GRE Into VPN, page 2-23
Task 29: Configure Pool to Distribute IP Addresses to VPN Clients, page 2-23
Task 30: Configure Global Default Route, page 2-23

GRE+IPSec to MPLS Configuration Tasks

Typical GRE+IPSec to MPLS configuration tasks are shown below. Refer to the section titled GRE+IPSec to MPLS Configuration Sample, page 2-24.

Task 1: Configure Authentication and Authorization Lists for Clients to RADIUS

	Command	Purpose
Step 1	**aaa authentication login**	Set authentication, authorization, and accounting (AAA) authentication at login.
Step 2	**aaa authorization**	Set parameters that restrict user access to a network.

Task 2: Configure the VRFs

	Command	Purpose
Step 1	`ip vrf`	Configure a VPN routing and forwarding (VRF) routing table.

	Command	Purpose
Step 2	**rd** route-distinguisher	Create routing and forwarding tables for a VRF.
Step 3	**route-target {import | export | both}**	Create a route-target extended community for a VRF.

Task 3: Enable CEF Switching

	Command	Purpose
Step 1	**ip cef**	Enable Cisco Express Forwarding (CEF).
Step 2	**mpls label protocol {ldp | tdp}**	Specify the default label distribution protocol.
Step 3	**tag-switching ip default-route**	Enable the distribution of labels associated with the IP default route.

Task 4: Configure the Keyring

	Command	Purpose
Step 1	**crypto keyring** keyring-name [**vrf** fvrf]	Configure a new keyring for the shared secret keys to be used during Internet Key Exchange (IKE) authentication.
Step 2	**pre-shared-key** {**address** address [mask] | **hostname** hostname} **key** key	Configure the addressed preshared key to be used during IKE authentication.

Task 5: Configure ISAKMP Policy for Phase 1 Negotiations

	Command	Purpose
Step 1	**crypto isakmp policy** priority	Configure an IKE policy.
Step 2	**encryption {des | 3des | aes | aes 192 | aes 256}**	Specify the encryption algorithm within an IKE policy.
Step 3	**authentication {rsa-sig | rsa-encr | pre-share}**	Specify the authentication method within an IKE policy.

Task 6: Configure DPD Keepalives

Command	Purpose
crypto isakmp keepalive secs retries	Allow the gateway to send dead peer detection (DPD) messages to the router.

Task 7: Configure Client Group for Local Authorization

	Command	Purpose
Step 1	**crypto isakmp client configuration group** {group-name | default}	Specify which group's policy profile will be defined.
Step 2	**key** name	Configure the IKE preshared key for group policy attribute definition.
Step 3	**pool** (name)	Configure a local pool address.

Task 8: Configure ISAKMP Profile for VPN Sites

Command	Purpose
crypto isakmp profile profile-name	Define an ISAKMP profile for a VPN.

Task 9: Configure Dynamic VRF Association for VPN Sites

	Command	Purpose
Step 1	**vrf** name	Associate the on-demand address pool with a VPN routing and forwarding instance (VRF) name.
Step 2	**match identity address** address [mask] [fvrf]	Match an acceptable Phase 1 identity from a peer to a particular ISAKMP profile.

Task 10: Configure XAUTH, Group Authorization, and Mode-Config

	Command	Purpose
Step 1	**client authentication list** list-name	Configure IKE extended authentication (Xauth) on your router. The list-name must match the list-name defined during AAA configuration
Step 2	**isakmp authorization list** list-name	Configure group authorization IKE querying of authentication, authorization, and accounting (AAA) for tunnel attributes in aggressive mode.
Step 3	**client configuration address [initiate | respond]**	Configure IKE mode configuration (Mode-Config).

Task 11: Configure ISAKMP Profile for GRE

	Command	Purpose
Step 1	**crypto isakmp profile** profile-name	Define an ISAKMP profile for a VPN.

Step 2	**keyring** *keyring-name*	Associate a keyring with an isakmp profile.
Step 3	**match identity address** address [mask] [fvrf]	Match an acceptable Phase 1 identity from a peer to a particular ISAKMP profile.

Note You can configure the Remote sites to match each peer using sequence numbers in the crypto map definition.You can match the peer on IP address or the hostname. The IP address match list for traffic to be encrypted is also defined for each peer. In case of VPN clients, the dynamic profile defined earlier is used to match the clients.

Task 12: Configure the Transform Set for Data Encryption

Command	Purpose
crypto IPSec transform-set transform-set-name transform1 [transform2] [transform3] [transform4]	Define the transform set.

Task 13: Configure IPSec Profile for GRE and Apply Transform Set

	Command	Purpose
Step 1	**crypto IPSec profile** name	Define the IP Security (IPSec) parameters that are to be used for IPSec encryption between two IPSec routers.
Step 2	**set transform-set** transform-set-name	Specify which transform sets can be used with the crypto map entry.

Task 14: Configure ISAKMP Client Profile Reference

Command	Purpose
set isakmp-profile profile-name	Set the ISAKMP profile name for client.

Task 15: Configure RRI

Command	Purpose
reverse-route [remote-peer]	Create source proxy information for a crypto map entry through RRI.

Task 16: Configure Dynamic Crypto Map for Clients

Command	Purpose
crypto map map-name seq-num [**IPSec-isakmp**]	Create a crypto map entry that uses IKE to establish IPSec SAs for protecting the traffic specified by this crypto map entry.

Task 17: Configure GRE Tunnel to Customer Site

	Command	Purpose
Step 1	**interface** type	Configure an interface type and enter interface configuration mode.
Step 2	**ip vrf forwarding** *vrf-name*	Associate a VPN routing and forwarding (VRF) instance with an interface or subinterface.
Step 3	**ip address** ip-address mask	Set an IP address for an interface.
Step 4	**tunnel source** {**ip-address** | ***type*** number}	Set source address for a tunnel interface.
Step 5	**tunnel destination** {***hostname*** | ***ip-address***}	Specify the destination for a tunnel interface.

Task 18: Configure IPSec Profile

Command	Purpose
tunnel protection ipsec-profile name	Associate a tunnel interface with an IPSec profile.

Task 19: Configure Internet-Facing Interface and Corresponding Crypto Maps

	Command	Purpose
Step 1	**interface** type	Configure a loopback interface (emulates an interface that is always up).
Step 2	**ip address** ip-address mask	Set an IP address for an interface.
Step 3	**encapsulation dot1q** vlan-id **[native]**	Enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN).
Step 4	**crypto map** map-name	Apply a previously defined crypto map set to an interface.

Note Each interface services one VPN as the IPSec tunnel endpoint for both the sites and clients.

Task 20: Configure Interface for Tag Switching

	Command	Purpose
Step 1	**interface** type	Configure a loopback interface (emulates an interface that is always up).
Step 2	**ip address** ip-address mask	Set an IP address for an interface.
Step 3	**encapsulation dot1q** vlan-id **[native]**	Enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN).
Step 4	**tag-switching ip**	Allow label switching of IPv4 packets.

Task 21: Configure the IGP Used in the Core

	Command	Purpose
Step 1	**router ospf** process-id	Configure an OSPF routing process.
Step 2	**log-adjacency-changes**	Generate a log message.
Step 3	**network** ip-address wildcard-mask **area** area-id	Configure the interfaces on which OSPF runs and to define the area ID for those interfaces.

Task 22: Configure Routing Protocol Across GRE Tunnel

	Command	Purpose
Step 1	**router rip**	Configure the Routing Information Protocol (RIP) routing process.
Step 2	**version** {1 | 2}	Specify a RIP version used globally by the router.

Task 23: Configure Address Family Definition per VRF

	Command	Purpose
Step 1	**address-family**	Enter the address family submode for configuring routing protocols such as BGP, RIP, and static routing.
Step 2	**version** {1 | 2}	Specify a RIP version used globally by the router.

Task 24: Redistribute VPN Routes Learned Through BGP

	Command	Purpose
Step 1	**redistribute** protocol	Redistribute routes from one routing domain into another routing domain.

Step 2	**network** *ip-address*	Specify a list of networks for the Routing Information Protocol (RIP) routing process.
Step 3	**no auto-summary**	Disable the default behavior of automatic summarization of subnet routes into network-level routes.
Step 4	**exit-address-family**	Exit from the address family configuration submode.

Task 25: Configure BGP to Carry VPN Routes

	Command	Purpose
Step 1	**router bgp** as-number	Configure the BGP routing process.
Step 2	**no synchronization**	Disable the synchronization between BGP and your Interior Gateway Protocol (IGP) system.
Step 3	**bgp log-neighbor-changes**	Enable logging of BGP neighbor resets.
Step 4	**neighbor** {ip-address | peer-group-name} **remote-as** number	Add an entry to the BGP neighbor table.
Step 5	**no auto-summary**	Disable the default behavior of automatic summarization of subnet routes into network-level routes.

Task 26: Configure Peers to Receive VPNv4 Routes

	Command	Purpose
Step 1	**address-family**	Enter the address family submode for configuring routing protocols such as BGP, RIP, and static routing.
Step 2	**neighbor** {ip-address | peer-group-name} **activate**	Enable the exchange of information with a neighboring router.
Step 3	**no auto-summary**	Disable the default behavior of automatic summarization of subnet routes into network-level routes.
Step 4	**exit-address-family**	Exit from the address family configuration submode.

Task 27: Configure IPv4 Address-Family for Each VPN

	Command	Purpose
Step 1	**address-family**	Enter the address family submode for configuring routing protocols such as BGP, RIP, and static routing.

Step 2	**redistribute** protocol	Redistribute routes from one routing domain into another routing domain.
Step 3	**no auto-summary**	Disable the default behavior of automatic summarization of subnet routes into network-level routes.
Step 4	**no synchronization**	Disable the synchronization between BGP and your Interior Gateway Protocol (IGP) system.
Step 5	**exit-address-family**	Exit from the address family configuration submode.

Task 28: Redistribute Routes Learned Over GRE Into VPN

	Command	Purpose
Step 1	**redistribute** protocol	Redistribute routes from one routing domain into another routing domain.
Step 2	**no auto-summary**	Disable the default behavior of automatic summarization of subnet routes into network-level routes.
Step 3	**no synchronization**	Disable the synchronization between BGP and your Interior Gateway Protocol (IGP) system.
Step 4	**exit-address-family**	Exit from the address family configuration submode.

Task 29: Configure Pool to Distribute IP Addresses to VPN Clients

	Command	Purpose
Step 1	**ip local pool** {**default** | pool-name low-ip-address [**high-ip-address**]}	Configure a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.
Step 2	**ip classless**	Configure the router to send any packets it receives that are destined for a subnet of a network that has no network default route to the best supernet route possible.

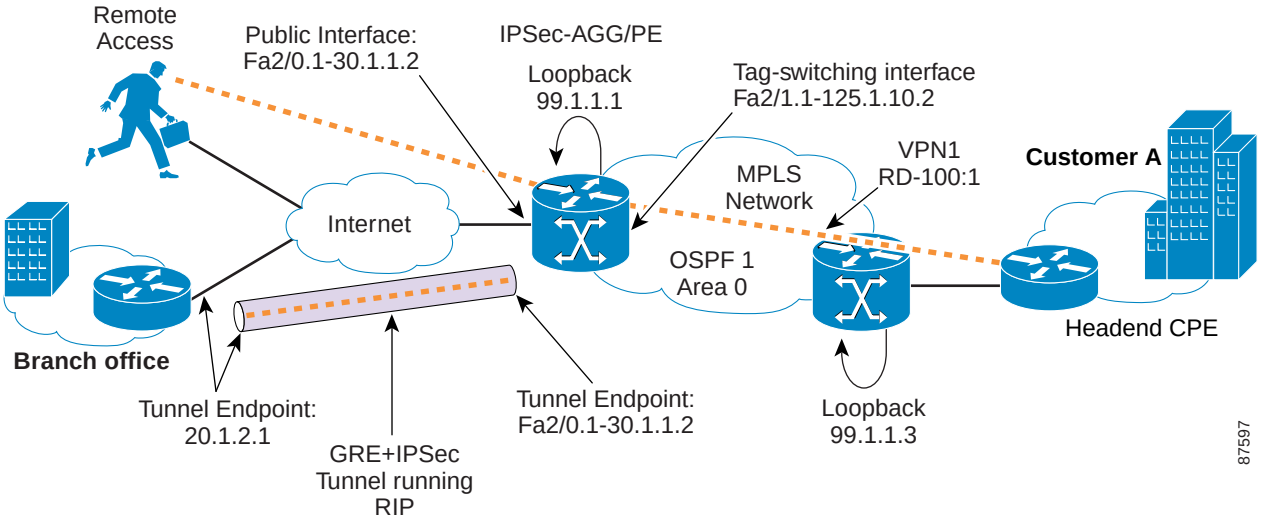
Task 30: Configure Global Default Route

Command	Purpose
ip route network-number network-mask {**ip-address** | **interface-name**} **[distance] [name** name]	Establish static routes and define the next hop for large-scale dial-out.

GRE+IPSec to MPLS Configuration Sample

Figure 2-2 illustrates the following GRE+IPSec IPSec to MPLS configuration.

Figure 2-2 .GRE+IPSec IPSec to MPLS configuration




```
Building configuration...

Current configuration : 4093 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname pe2
username cisco password 0 cisco
aaa new-model
!
```

Step 1 Configure authentication and authorization lists for clients to RADIUS.

```
aaa authentication login localist local
aaa authorization network localist local
aaa session-id common
ip subnet-zero
no ip domain lookup
```

Step 2 Configure VRFs.

```
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
```

Step 3 Configure CEF.

```
ip cef
mpls label protocol ldp
mpls ldp logging neighbor-changes
tag-switching ip default-route
```

Step 4 Configure Keyring/VPN.

```
crypto keyring gre
  pre-shared-key address 20.1.2.1 key cisco123
!
```

Step 5 Configure the ISAKMP policy for Phase 1 negotiations.

```
crypto isakmp policy 1
 authentication pre-share
 group 2
!
crypto isakmp policy 2
 encr 3des
 authentication pre-share
```

Step 6 Configure the DPD keepalives.

```
crypto isakmp keepalive 30
crypto isakmp xauth timeout 30
```

Step 7 Configure client group for local authorization.

```
crypto isakmp client configuration group ezvpn
 key cisco123
 pool hw-pool
```

Step 8 Configure ISAKMP profile for VPN clients.

```
crypto isakmp profile vpn1-ez
```

Step 9 Configure dynamic VRF association for VPN clients.

```
 vrf vpn1
   match identity group ezvpn
```

Step 10 Configure XAUTH, group authorization, and mode-config.

```
   client authentication list localist
   isakmp authorization list localist
   client configuration address respond
```

Step 11 Configure ISAKMP profile for GRE.

```
crypto isakmp profile gre
   keyring gre
   match identity address 20.1.2.1 255.255.255.255
```

Step 12 Configure the transform set.

```
crypto IPSec transform-set tset1 esp-3des esp-sha-hmac
```

Step 13 Configure IPSec profile for GRE and apply transform set.

```
crypto IPSec profile gre
 set transform-set tset1
 set isakmp-profile gre

crypto dynamic-map dyna 1
 set security-association idle-time 3600
 set transform-set tset1
```

Step 14 Configure ISAKMP client profile reference.

```
 set isakmp-profile vpn1-ez
```

Step 15 Configure RRI.

```
 reverse-route
```

Step 16 Configure dynamic crypto map for clients.

```
crypto map vpn 1000 IPSec-isakmp dynamic dyna
!
interface Loopback0
 ip address 99.1.1.2 255.255.255.255
```

Step 17 Configure encrypted GRE tunnel to customer site.

```
interface Tunnel1
 ip vrf forwarding vpn1
 ip address 12.1.1.1 255.255.255.252
 tunnel source 30.1.1.3
 tunnel destination 20.1.2.1
```

Step 18 Configure IPSec profile.

```
 tunnel protection IPSec profile gre
!
interface FastEthernet2/0
 no ip address
 duplex auto
 speed auto
```

Step 19 Configure Internet facing interface and corresponding crypto maps.

```
interface FastEthernet2/0.1
 encapsulation dot1Q 10
 ip address 30.1.1.3 255.255.255.0
 crypto map vpn
!
interface FastEthernet2/1
 no ip address
 duplex auto
 speed auto
```

Step 20 Configure interface for tag switching.

```
interface FastEthernet2/1.1
 encapsulation dot1Q 10
 ip address 125.1.10.3 255.255.255.0
 tag-switching ip
```

Step 21 Configure IGP used in core.

```
router ospf 1
 log-adjacency-changes
 network 99.1.1.2 0.0.0.0 area 0
 network 125.1.10.0 0.0.0.255 area 0
```

Step 22 Configure routing protocol across the GRE tunnel.

```
router rip
 version 2
```

Step 23 Configure address family definition per VRF.

```
address-family ipv4 vrf vpn1
 version 2
```

Step 24 Redistribute VPN routes learned through BGP.

```
 redistribute bgp 100 metric 1
 network 12.0.0.0
 no auto-summary
```

```
 exit-address-family
```

Step 25 Configure BGP to carry VPN routes.

```
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 99.1.1.3 remote-as 100
 neighbor 99.1.1.3 update-source Loopback0
 no auto-summary
```

Step 26 Configure peers to receive VPNv4 routes.

```
 address-family vpnv4
 neighbor 99.1.1.3 activate
 neighbor 99.1.1.3 send-community both
 no auto-summary
 exit-address-family
```

Step 27 Configure Ipv4 address family for each VPN.

```
 address-family ipv4 vrf vpn1
 redistribute static
```

Step 28 Redistribute routes learned over GRE into VPN.

```
redistribute rip
 no auto-summary
 no synchronization
 exit-address-family
```

Step 29 Configure the pool to distribute IP addresses to VPN clients.

```
ip local pool hw-pool 192.168.2.1 192.168.2.254
ip classless
```

Step 30 Configure global default route.

```
ip route 0.0.0.0 0.0.0.0 FastEthernet2/0.1 30.1.1.1
```

IPSec to L2VPN Service Model

This chapter describes how to configure the IPSec to L2VPN service model for the Cisco Network-Based IPSec VPN Release 1.5 .

Configuring the IPSec to L2VPN Service Model

The IPSec to L2VPN model is very similar to the IPSec to MPLS topology, except the service provider has an L2 core instead of an MPLS core. The L2 core can be Frame Relay, ATM, 802.1q, or wireless.

This configuration enables a Layer 2 service provider to extend secured access service beyond its core into the internet. As in the IPSec to MPLS model, the sessions are terminated on the IPSec Aggregator. Using the Multi-VRF CE feature, users are mapped into an L2 infrastructure.

At an L3 level, the IPSec aggregator connects directly to the customer site that has L2 service. The service provider does not need to address the customer routing issue in its core. The IPSec aggregator and the L2 customer site can use either static routes or a dynamic routing protocol to establish end-to-end connectivity.

Before You Begin

The procedures provided here are specific to configuring IPSec to L2VPN and are based on the following assumptions:

1. That the following setup and configuration tasks have already been completed:
   - Setup of the core MPLS network
   - Setup of the customer VPN
   - Configuration of the links between the PE and the CE
   - Customer-specific information is complete

- That you have a good understanding of the architecture and features you are using and that you have selected the means you will use to implement those features (for example, which of several strategies to use for address management or for user authentication and authorization).

IPSec to L2VPN Configuration Checklist

This section deals with configuring the router to function as the IPSec aggregator.

Procedures for competing each task are described in the sections that follow. If you are viewing this document online, you can click highlighted text to view details on the procedure.

Table 3-1 IPSec to L2VPN Configuration Checklist

Task 1: Configure Authentication and Authorization Lists for Clients to RADIUS, page 3-3
Task 2: Configure the VRFs, page 3-3
Task 3: Enable CEF Switching, page 3-3
Task 4: Configure the Keyring, page 3-3
Task 5: Configure ISAKMP Policy, page 3-3
Task 6: Configure DPD Keepalives, page 3-4
Task 7: Configure Client Group for Local Authorization, page 3-4
Task 8: Configure ISAKMP Profile for VPN Sites, page 3-4
Task 9: Configure Dynamic VRF Association for VPN Sites, page 3-4
Task 10: Configure ISAKMP Profile for VPN Clients, page 3-4
Task 11: Configure Dynamic VRF Association for VPN Clients, page 3-5
Task 12: Configure XAUTH, Group Authorization, and Mode-Config, page 3-5
Task 13: Configure the Transform Set for Data Encryption, page 3-5
Task 14: Configure Dynamic Crypto Map and Apply Transform Set, page 3-5
Task 15: Configure ISAKMP Client Profile Reference, page 3-5
Task 16: Configure RRI, page 3-6
Task 17: Configure Static Crypto Map for Sites, page 3-6
Task 18: Configure ISAKMP Site Profile Reference, page 3-6
Task 19: Configure Dynamic Crypto Map for Clients, page 3-6
Task 20: Configure Internet-Facing Interface and Corresponding Crypto Maps, page 3-6
Task 21: Configure Interface for L2VPN, page 3-7
Task 22: Configure Pool to Distribute IP Addresses to VPN Clients, page 3-8
Task 23: Configure Static Routes for Public IP Addresses, page 3-8
Task 24: Configure Static VPN Routes If No IGP Within VPN, page 3-8
Task 25: Configure the Crypto Access List to Define Traffic to be Encrypted, page 3-8

IPSec to L2VPN Configuration Tasks

Typical IPSec to L2VPN configuration tasks are shown below. See IPSec to L2VPN Configuration Sample, page 3-9.

Task 1: Configure Authentication and Authorization Lists for Clients to RADIUS

	Command	Purpose
Step 1	**aaa authentication login**	Set authentication, authorization, and accounting (AAA) authentication at login.
Step 2	**aaa authorization**	Set parameters that restrict user access to a network.

Task 2: Configure the VRFs

	Command	Purpose
Step 1	**ip vrf**	Configure a VPN routing and forwarding (VRF) routing table.
Step 2	**rd** route-distinguisher	Create routing and forwarding tables for a VRF.

Task 3: Enable CEF Switching

	Command	Purpose
Step 1	**ip cef**	Enable Cisco Express Forwarding (CEF).
Step 2	**tag-switching ip default-route**	Enable the distribution of labels associated with the IP default route.

Task 4: Configure the Keyring

	Command	Purpose
Step 1	**crypto keyring** keyring-name [**vrf** fvrf]	Configure a new keyring for the shared secret keys to be used during Internet Key Exchange (IKE) authentication.
Step 2	**pre-shared-key** {**address** address [mask] | **hostname** hostname} **key** key	Configure the addressed preshared key to be used during IKE) authentication.

Task 5: Configure ISAKMP Policy

	Command	Purpose
Step 1	**crypto isakmp policy** priority	Configure an IKE policy.
Step 2	**encryption {des | 3des | aes | aes 192 | aes 256}**	Specify the encryption algorithm within an IKE policy.
Step 3	**authentication {rsa-sig | rsa-encr | pre-share}**	Specify the authentication method within an IKE policy.

Task 6: Configure DPD Keepalives

Command	Purpose
crypto isakmp keepalive secs retries	Allow the gateway to send dead peer detection (DPD) messages to the router.

Task 7: Configure Client Group for Local Authorization

	Command	Purpose
Step 1	**crypto isakmp client configuration group** {group-name | default}	Specify which group's policy profile will be defined.
Step 2	**key** name	Configure the IKE preshared key for group policy attribute definition.
Step 3	**pool** (name)	Configure a local pool address.

Task 8: Configure ISAKMP Profile for VPN Sites

Command	Purpose
crypto isakmp profile profile-name	Define an ISAKMP profile for a VPN.

Task 9: Configure Dynamic VRF Association for VPN Sites

	Command	Purpose
Step 1	**vrf** name	Associate the on-demand address pool with a VPN routing and forwarding instance (VRF) name.
Step 2	**keyring** keyring-name	Associate a keyring with an ISAKMP profile.
Step 3	**match identity address** address [mask] [fvrf]	Match an acceptable Phase 1 identity from a peer to a particular ISAKMP profile.

Task 10: Configure ISAKMP Profile for VPN Clients

Command	Purpose
crypto isakmp profile profile-name	Define an ISAKMP profile for a VPN.

Note You can configure the Remote sites to match each peer using sequence numbers in the crypto map definition.You can match the peer on IP address or the hostname. The IP address match list for traffic to be encrypted is also defined for each peer. In case of VPN clients, the dynamic profile defined earlier is used to match the clients.

Task 11: Configure Dynamic VRF Association for VPN Clients

	Command	Purpose
Step 1	**vrf** name	Associate the on-demand address pool with a VPN VRF name.
Step 2	**match identity** group-name	Match an acceptable Phase 1 identity from a peer to a Unity group.

Task 12: Configure XAUTH, Group Authorization, and Mode-Config

	Command	Purpose
Step 1	**client authentication list** list-name	Configure IKE extended authentication (Xauth) on your router. The list-name must match the list-name defined during AAA configuration
Step 2	**isakmp authorization list** list-name	Configure group authorization IKE querying of AAA for tunnel attributes in aggressive mode.
Step 3	**client configuration address [initiate | respond]**	Configure IKE Mode Configuration (Mode-Config).

Task 13: Configure the Transform Set for Data Encryption

Command	Purpose
crypto IPSec transform-set transform-set-name transform1 [transform2] [transform3] [transform4]	Define the transform set.

Task 14: Configure Dynamic Crypto Map and Apply Transform Set

	Command	Purpose
Step 1	**crypto dynamic-map** dynamic-map-name dynamic-seq-num	Create a dynamic crypto map entry and enter the crypto map configuration command mode.
Step 2	**set transform-set** transform-set-name	Specify which transform sets can be used with the crypto map entry.

Task 15: Configure ISAKMP Client Profile Reference

Command	Purpose
set isakmp-profile profile-name	Set the ISAKMP profile name for client.

Task 16: Configure RRI

Command	Purpose
reverse-route [remote-peer]	Create source proxy information for a crypto map entry through RRI.

Task 17: Configure Static Crypto Map for Sites

	Command	Purpose
Step 1	**crypto map** map-name seq-num [**IPSec-isakmp**]	Create a crypto map entry that uses IKE to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.
Step 2	**set peer** {hostname | ip-address}	Specify an IP Security peer in a crypto map entry.
Step 3	**set transform-set** transform-set-name	Specify which transform sets can be used with the crypto map entry.

Task 18: Configure ISAKMP Site Profile Reference

	Command	Purpose
Step 1	**set isakmp-profile** profile-name	Set the ISAKMP profile name reference.
Step 2	**match identity address** address [mask] [fvrf]	Match an acceptable Phase 1 identity from a peer to a particular ISAKMP profile.

Task 19: Configure Dynamic Crypto Map for Clients

Command	Purpose
crypto map map-name seq-num [**IPSec-isakmp**]	Create a crypto map entry that uses IKE to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.

Task 20: Configure Internet-Facing Interface and Corresponding Crypto Maps

	Command	Purpose
Step 1	**interface** type	Configure a loopback interface (emulates an interface that is always up).
Step 2	**ip address** ip-address mask	Set an IP address for an interface.
Step 3	**encapsulation dot1q** vlan-id **[native]**	Enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN).
Step 4	**crypto map** map-name	Apply a previously defined crypto map set to an interface.

Note Each interface services one VPN as the IPSec tunnel endpoint for both the sites and clients.

Task 21: Configure Interface for L2VPN

	Command	Purpose
Step 1	**interface** *type slot*/port.subinterface-number **[multipoint** | **point-to-point]**	Configure an interface type and enter interface configuration mode.
Step 2	**ip vrf forwarding** vrf-name	Associate a VRF instance with an interface or subinterface.
Step 3	**ip address** ip-address mask	Set an IP address for an interface.
Step 4	**pvc [name] vpi/**vci **[ces** | **ilmi** | **qsaal** | **smds]**	Create an ATM permanent virtual circuit (PVC).

Task 22: Configure Pool to Distribute IP Addresses to VPN Clients

Command	Purpose
ip local pool {**default** | pool-name low-ip-address [**high-ip-address**]}	Configure a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.

Task 23: Configure Static Routes for Public IP Addresses

Command	Purpose
ip route network-number network-mask {**ip-address** | **interface-name**} **[distance] [name** name]	Establish static routes and define the next hop for large-scale dial-out.

Task 24: Configure Static VPN Routes If No IGP Within VPN

Command	Purpose
ip route vrf vrf-name prefix mask **[next-hop-address] [interface {interface-number}] [global] [distance] [permanent] [tag** tag]	Establish static routes for a VRF instance.

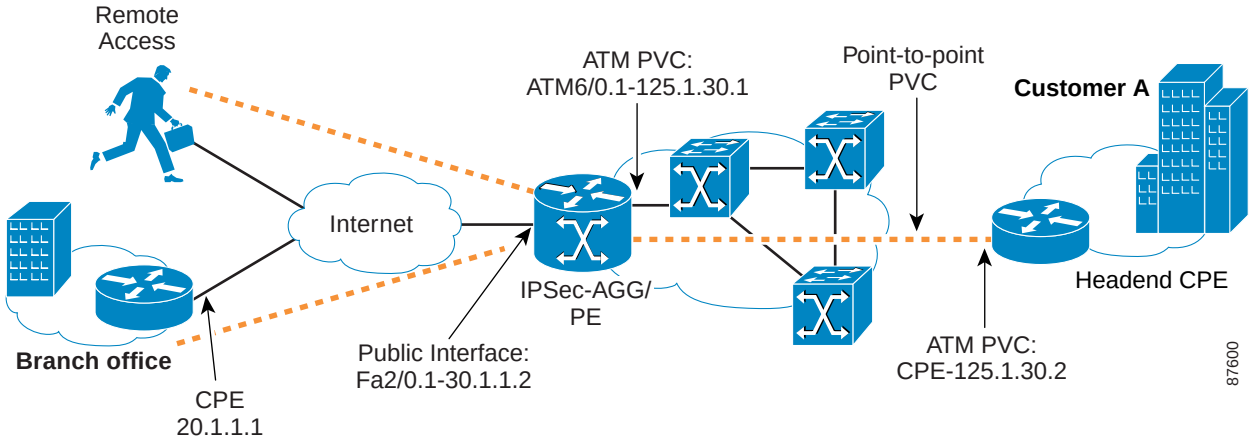
Task 25: Configure the Crypto Access List to Define Traffic to be Encrypted

Command	Purpose
access-list access-list-number {**deny** | **permit**} source **[source-wildcard] [log]**	Configure a standard IP access list.

IPSec to L2VPN Configuration Sample

Figure 3-1 illustrates the following IPSec to MPLS configuration.

Figure 3-1 IPSec to L2VPN Configuration




```
pe1#sh run
Building configuration...

Current configuration : 3874 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname pe1
enable password cisco
!
username cisco password 0 cisco
aaa new-model
```

Step 1 Configure authentication and authorization list for clients to RADIUS.

```
aaa authentication login localist local
aaa authorization network localist local
aaa session-id common
ip subnet-zero
no ip domain lookup
```

Step 2 Configure VRFs.

```
ip vrf vpn1
 rd 100:1
```

Step 3 Enable CEF switching.

```
ip cef
tag-switching ip default-route
```

Step 4 Configure Keyring.

```
crypto keyring vpn1
```

```
 pre-shared-key address 20.1.1.1 key cisco123
 pre-shared-key address 40.1.1.2 key cisco123
```

Step 5 Configure ISAKMP policy.

```
crypto isakmp policy 1
 authentication pre-share
 group 2
!
crypto isakmp policy 2
 encr 3des
 authentication pre-share
```

Step 6 Configure DPD keepalives.

```
crypto isakmp keepalive 30
crypto isakmp xauth timeout 30
```

Step 7 Configure client group for local authorization.

```
crypto isakmp client configuration group ezvpn
 key cisco123
 pool hw-pool
```

Step 8 Configure ISAKMP profile for VPN sites.

```
crypto isakmp profile vpn1
```

Step 9 Configure dynamic VRF association.

```
   vrf vpn1
   keyring vpn1
   match identity address 20.1.1.1 255.255.255.255
   match identity address 40.1.1.2 255.255.255.255
```

Step 10 Configure ISAKMP profile for VPN clients.

```
crypto isakmp profile vpn1-ez
```

Step 11 Configure dynamic VRF association.

```
vrf vpn1
   match identity group ezvpn
```

Step 12 Configure XAUTH, group authorization, and mode-config.

```
   client authentication list localist
   isakmp authorization list localist
   client configuration address respond
```

Step 13 Configure the transform set

```
crypto IPSec transform-set tset1 esp-3des esp-sha-hmac
!
```

Step 14 Configure dynamic crypto map.

```
crypto dynamic-map dyna 1
 set security-association idle-time 3600
 set transform-set tset1
```

Step 15 Configure ISAKMP client profile reference.

```
 set isakmp-profile vpn1-ez
```

Step 16 Configure RRI.

```
 reverse-route
```

Step 17 Configure static crypto map for a site.

```
crypto map vpn 10 IPSec-isakmp
 set peer 20.1.1.1
 set transform-set tset1
```

Step 18 Configure ISAKMP site profile reference.

```
 set isakmp-profile vpn1
 match address 101
```

Step 19 Configure dynamic crypto map for clients.

```
crypto map vpn 1000 IPSec-isakmp dynamic dyna
!
interface FastEthernet2/0
 no ip address
 duplex auto
 speed auto
```

Step 20 Configure Internet facing interface and corresponding crypto maps.

```
interface FastEthernet2/0.1
 encapsulation dot1Q 10
 ip address 30.1.1.2 255.255.255.0
 crypto map vpn
!
interface ATM6/0
 no ip address
 no atm ilmi-keepalive
```

Step 21 Configure the interface for L2VPN.

```
interface ATM6/0.1 point-to-point
 ip vrf forwarding vpn1
 ip address 125.1.30.1 255.255.255.252
 pvc 0/100
```

Step 22 Configure the pool to distribute IP addresses to VPN clients.

```
ip local pool hw-pool 192.168.1.1 192.168.1.254
ip classless
```

Step 23 Configure static routes for public IP addresses.

```
ip route 0.0.0.0 0.0.0.0 FastEthernet2/0.1 30.1.1.1
```

Step 24 Configure static VPN routes if not using a IGP within the VPN.

```
ip route vrf vpn1 101.1.1.0 255.255.255.0 30.1.1.1 global
ip route vrf vpn1 101.1.2.0 255.255.255.0 125.1.10.2
no ip http server
no ip http secure-server
```

Step 25 Configure the crypto access list to define traffic to be encrypted.

```
access-list 101 permit ip 101.1.2.0 0.0.0.255 101.1.1.0 0.0.0.255
```

Note You can run VRF aware routing protocols like EBPG, RIP, STATIC and OSPF between the routers.

IPSec to IPSec Service Model

This chapter describes how to configure the IPSec to IPSec service model for the Cisco Network-Based IPSec VPN Release 1.5 .

Configuring IPSec to IPSec Service Model

In this model, the IPSec Aggregator aggregates any remote sites/clients and then forwards the information to a headend enterprise VPN device. Since traffic is going over a open IP network, IPSec provides the necessary encryption over the IP backbone. This also permits private overlapping IP addressing schemes between enterprises.

Before You Begin

The procedures provided here are specific to configuring IPSec to IPSec with one box and are based on the following assumptions:

1. That the following setup and configuration tasks have already been completed:
   - Setup of the core IP/MPLS network.
   - Setup of the customer VPN
   - Configuration of the links between the PE and the CE.
   - Customer-specific information is complete.
2. That you have a good understanding of the architecture and features you are using and that you have selected the means you will use to implement those features (for example, which of several strategies you will use for address management or for user authentication and authorization).

IPSec to IPSec Configuration Checklist

This section deals with configuring the router to function as an IPSec aggregator.

Procedures for competing each task are described in the sections that follow. If you are viewing this document online, you can click on highlighted text to get details on the procedure.

Table 4-1 IPSec to IPSec Configuration Checklist

Task 1: Configure Authentication and Authorization Lists for Clients to RADIUS, page 4-3
Task 2: Configure the VRFs, page 4-3
Task 3: Configure CEF Switching, page 4-3
Task 4: Configure the Keyring/VPN, page 4-3
Task 5: Configure ISAKMP Policy for Phase 1 Negotiations, page 4-3
Task 6: Configure DPD Keepalives, page 4-4
Task 7: Configure Client Group Definition for Local Authorization, page 4-4
Task 8: Configure ISAKMP Profile for VPN Sites, page 4-4
Task 9: Configure Dynamic VRF Association for VPN Sites, page 4-4
Task 10: Configure ISAKMP Profile for VPN Clients, page 4-4
Task 11: Configure Dynamic VRF Association for VPN Clients, page 4-5
Task 12: Configure XAUTH, Group Authorization, and Mode-Config, page 4-5
Task 13: Configure the Transform Set for Data Encryption, page 4-5
Task 14: Configure Dynamic Crypto Map and Apply Transform Set, page 4-5
Task 15: Configure ISAKMP Client Profile Reference, page 4-5
Task 16: Configure RRI, page 4-6
Task 17: Configure Static Crypto Map for Sites, page 4-6
Task 18: Configure ISAKMP Site Profile Reference, page 4-6
Task 19: Configure Dynamic Crypto Map for Clients, page 4-6
Task 20: Configure Crypto Map to HQ, page 4-6
Task 21: Configure ISAKMP Site Profile Reference, page 4-7
Task 22: Connect Internet-Facing Interface and Corresponding Crypto Maps, page 4-7
Task 23: Apply Crypto Map towards HQ, page 4-7
Task 24: Configure the Interior Gateway Protocol (IGP) Used in the Core, page 4-7
Task 25: Configure the Pools to Distribute IP Addresses to VPN Clients, page 4-8
Task 26: Configure Global Default Route, page 4-8
Task 27: Configure Static VPN Routes, page 4-8
Task 28: Configure the Crypto ACL to Define Traffic to be Encrypted towards Sites, page 4-8
Task 29: Configure the Crypto ACL to Define Traffic to be Encrypted towards HQ, page 4-8

IPSec to IPSec Configuration Tasks

Typical IPSec to IPSec configuration tasks are shown below. See IPSec to IPSec Configuration Sample, page 4-9.

Task 1: Configure Authentication and Authorization Lists for Clients to RADIUS

	Command	Purpose
Step 1	**aaa authentication login**	Set authentication, authorization, and accounting (AAA) authentication at login.
Step 2	**aaa authorization**	Set parameters that restrict user access to a network.

Task 2: Configure the VRFs

	Command	Purpose
Step 1	**ip vrf**	Configure a VPN routing and forwarding (VRF) routing table.
Step 2	**rd** route-distinguisher	Create routing and forwarding tables for a VRF.

Task 3: Configure CEF Switching

	Command	Purpose
Step 1	**ip cef**	Enable CEF switching.
Step 2	**tag-switching ip default-route**	Enable the distribution of labels associated with the IP default route.

Task 4: Configure the Keyring/VPN

	Command	Purpose
Step 1	**crypto keyring** keyring-name [**vrf** fvrf]	Configure a new keyring for the shared secret keys to be used during IKE authentication.
Step 2	**pre-shared-key** {**address** address [mask] | **hostname** hostname} **key** key	Configure the addressed preshared key to be used during IKE authentication.

Task 5: Configure ISAKMP Policy for Phase 1 Negotiations

	Command	Purpose
Step 1	**crypto isakmp policy** priority	Configure an IKE policy.
Step 2	**encryption {des | 3des | aes | aes 192 | aes 256}**	Specify the encryption algorithm within an IKE policy.
Step 3	**authentication {rsa-sig | rsa-encr | pre-share}**	Specify the authentication method within an IKE policy.

Task 6: Configure DPD Keepalives

Command	Purpose
crypto isakmp keepalive secs retries	Allow the gateway to send dead peer detection (DPD) messages to the router.

Task 7: Configure Client Group Definition for Local Authorization

	Command	Purpose
Step 1	**crypto isakmp client configuration group** {group-name | default}	Specify which group's policy profile will be defined.
Step 2	**key** name	Configure the IKE preshared key for group policy attribute definition.
Step 3	**pool** (name)	Configure a local pool address.

Task 8: Configure ISAKMP Profile for VPN Sites

Command	Purpose
crypto isakmp profile profile-name	Define an ISAKMP profile for a VPN.

Task 9: Configure Dynamic VRF Association for VPN Sites

	Command	Purpose
Step 1	**vrf** name	Associate the on-demand address pool with a VRF name.
Step 2	**keyring** keyring-name	Associate a keyring with an ISAKMP profile.
Step 3	**match identity address** address [mask] [fvrf]	Match an acceptable Phase 1 identity from a peer to a particular ISAKMP profile.

Task 10: Configure ISAKMP Profile for VPN Clients

Command	Purpose
crypto isakmp profile profile-name	Define an ISAKMP profile for a VPN.

Note You can configure the Remote sites to match each peer using sequence numbers in the crypto map definition.You can match the peer on IP address or the hostname. The IP address match list for traffic to be encrypted is also defined for each peer. In case of VPN clients, the dynamic profile defined earlier is used to match the clients..

Task 11: Configure Dynamic VRF Association for VPN Clients

	Command	Purpose
Step 1	**vrf** name	Associate the on-demand address pool with a VRF name.
Step 2	**match identity** group-name	Match an acceptable Phase 1 identity from a peer to a Unity group.

Task 12: Configure XAUTH, Group Authorization, and Mode-Config

	Command	Purpose
Step 1	**client authentication list** list-name	Configure IKE extended authentication (Xauth) on your router. The list-name must match the list-name defined during AAA configuration
Step 2	**isakmp authorization list** list-name	Configure group authorization IKE querying of AAA for tunnel attributes in aggressive mode.
Step 3	**client configuration address [initiate | respond]**	Configure IKE Mode Configuration (Mode-Config).

Task 13: Configure the Transform Set for Data Encryption

Command	Purpose
crypto IPSec transform-set transform-set-name transform1 [transform2] [transform3] [transform4]	Define the transform set.

Task 14: Configure Dynamic Crypto Map and Apply Transform Set

	Command	Purpose
Step 1	**crypto dynamic-map** dynamic-map-name dynamic-seq-num	Create a dynamic crypto map entry and enter the crypto map configuration command mode.
Step 2	**set transform-set** transform-set-name	Specify which transform sets can be used with the crypto map entry.

Task 15: Configure ISAKMP Client Profile Reference

Command	Purpose
set isakmp-profile profile-name	Set the ISAKMP profile name for client.

Task 16: Configure RRI

Command	Purpose
reverse-route [remote-peer]	Create source proxy information for a crypto map entry through RRI.

Task 17: Configure Static Crypto Map for Sites

	Command	Purpose
Step 1	**crypto map** map-name seq-num [**IPSec-isakmp**]	Create a crypto map entry that uses IKE to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.
Step 2	**set peer** {hostname | ip-address}	Specify an IP Security peer in a crypto map entry.
Step 3	**set transform-set** transform-set-name	Specify which transform sets can be used with the crypto map entry.

Task 18: Configure ISAKMP Site Profile Reference

	Command	Purpose
Step 1	**set isakmp-profile** profile-name	Set the ISAKMP profile name reference.
Step 2	**match identity address** address [mask] [fvrf]	Match an acceptable Phase 1 identity from a peer to a particular isakmp profile.

Task 19: Configure Dynamic Crypto Map for Clients

Command	Purpose
crypto map map-name seq-num [**IPSec-isakmp**]	Create a crypto map entry that uses IKE to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.

Task 20: Configure Crypto Map to HQ

	Command	Purpose
Step 1	**crypto map** map-name seq-num [**IPSec-isakmp**]	Create a crypto map entry that uses IKE to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.
Step 2	**set peer** {hostname | ip-address}	Specify an IP Security peer in a crypto map entry.
Step 3	**set transform-set** transform-set-name	Specify which transform sets can be used with the crypto map entry.

Task 21: Configure ISAKMP Site Profile Reference

	Command	Purpose
Step 1	**set isakmp-profile** profile-name	Set the ISAKMP profile name reference.
Step 2	**match identity address** address [mask] [fvrf]	Match an acceptable Phase 1 identity from a peer to a particular ISAKMP profile.

Task 22: Connect Internet-Facing Interface and Corresponding Crypto Maps

	Command	Purpose
Step 1	**interface** type	Configure a loopback interface.
Step 2	**ip address** ip-address mask	Set an IP address for an interface.
Step 3	**encapsulation dot1q** vlan-id **[native]**	Enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN).
Step 4	**crypto map** map-name	Apply a previously defined crypto map set to an interface.

Note Each interface services one VPN as the IPSec tunnel endpoint for both the sites and clients.

Task 23: Apply Crypto Map towards HQ

	Command	Purpose
Step 1	**interface** type	Configure a loopback interface (emulates an interface that is always up).
Step 1	**encapsulation dot1q** vlan-id **[native]**	Enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN).
Step 2	**ip address** ip-address mask	Set an IP address for an interface.
Step 3	**crypto map** map-name	Apply a previously defined crypto map set to an interface.

Task 24: Configure the Interior Gateway Protocol (IGP) Used in the Core

	Command	Purpose
Step 1	**router ospf** process-id	Configure an OSPF routing process.
Step 2	**log-adjacency-changes**	Generate a log message.
Step 3	**network ip**-address wildcard-mask **area** area-id	Configure the interfaces on which OSPF runs and to define the area ID for those interfaces.

Task 25: Configure the Pools to Distribute IP Addresses to VPN Clients

	Command	Purpose
Step 1	**ip local pool** {**default** | pool-name low-ip-address [**high-ip-address**]}	Configure a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.
Step 2	**ip classless**	Configure the router to send any packets it receives that are destined for a subnet of a network that has no network default route to the best supernet route possible.

Task 26: Configure Global Default Route

Command	Purpose
ip route network-number network-mask {**ip-address** | **interface-name**} **[distance] [name** name]	Establish static routes and define the next hop for large-scale dial-out.

Task 27: Configure Static VPN Routes

ip route vrf vrf-name prefix mask **[next-hop-address] [interface {interface-number}] [global] [distance] [permanent] [tag** tag]	Establish static routes for a VRF instance.

Task 28: Configure the Crypto ACL to Define Traffic to be Encrypted towards Sites

access-list access-list-number {**deny** | **permit**} source **[source-wildcard] [log]**	Configure a standard IP access list.

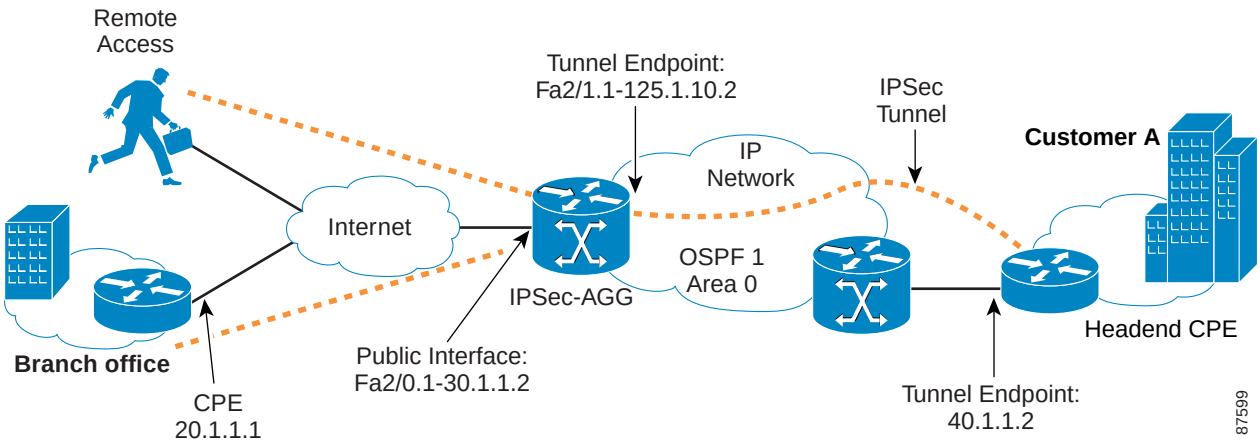
Task 29: Configure the Crypto ACL to Define Traffic to be Encrypted towards HQ

access-list access-list-number {**deny** | **permit**} source **[source-wildcard] [log]**	Configure a standard IP access list.

IPSec to IPSec Configuration Sample

Figure 4-1 illustrates the following IPSec to IPSec configuration.

Figure 4-1 IPSec to IPSec Configuration




```
IPSec to IPSec

pe1#sh run
Building configuration...

Current configuration : 4124 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname pe1
enable password cisco
!
username cisco password 0 cisco
aaa new-model
```

Step 1 Configure authentication and authorization lists for clients to RADIUS.

```
aaa authentication login localist local
aaa authorization network localist local
aaa session-id common
ip subnet-zero
no ip domain lookup
```

Step 2 Configure the VRFs.

```
ip vrf vpn1
 rd 100:1
```

Step 3 Enable CEF switching.

```
ip cef
mpls ldp logging neighbor-changes
tag-switching ip default-route
```

Step 4 Configure Keyring.

```
crypto keyring vpn1
  pre-shared-key address 20.1.1.1 key cisco123
  pre-shared-key address 40.1.1.2 key cisco123
```

Step 5 Configure the ISAKMP policy for Phase 1 negotiations.

```
crypto isakmp policy 1
 authentication pre-share
 group 2
!
crypto isakmp policy 2
 encr 3des
 authentication pre-share
```

Step 6 Configure DPD keepalives.

```
crypto isakmp keepalive 30
crypto isakmp xauth timeout 30
```

Step 7 Configure client group for local authorization.

```
crypto isakmp client configuration group ezvpn
 key cisco123
 pool hw-pool
```

Step 8 Configure ISAKMP profile for VPN sites.

```
crypto isakmp profile vpn1
```

Step 9 Configure dynamic VRF association.

```
   vrf vpn1
   keyring vpn1
   match identity address 20.1.1.1 255.255.255.255
   match identity address 40.1.1.2 255.255.255.255
```

Step 10 Configure ISAKMP profile for VPN clients.

```
crypto isakmp profile vpn1-ez
```

Step 11 Configure dynamic VRF association.

```
   vrf vpn1
   match identity group ezvpn
```

Step 12 Configure XAUTH, group authorization, and mode-config.

```
   client authentication list localist
   isakmp authorization list localist
   client configuration address respond
```

Step 13 Configure transform set for data encryption.

```
crypto IPSec transform-set tset1 esp-3des esp-sha-hmac
```

Step 14 Configure dynamic crypto map and apply transform set.

```
crypto dynamic-map dyna 1
 set security-association idle-time 3600
 set transform-set tset1
```

Step 15 Configure ISAKMP client profile reference.

```
 set isakmp-profile vpn1-ez
```

Step 16 Configure client RRI.

```
 reverse-route
```

Step 17 Configure static map for a site.

```
crypto map vpn 10 IPSec-isakmp
 set peer 20.1.1.1
 set transform-set tset1
```

Step 18 Configure ISAKMP site profile reference.

```
 set isakmp-profile vpn1
 match address 101
```

Step 19 Configure dynamic crypto map for clients.

```
crypto map vpn 1000 IPSec-isakmp dynamic dyna
```

Step 20 Configure crypto map towards HQ.

```
crypto map vpn_out 10 IPSec-isakmp
 set peer 40.1.1.2
 set transform-set tset1
```

Step 21 Configure ISAKMP site profile reference.

```
 set isakmp-profile vpn1
 match address 151
!
interface FastEthernet2/0
 no ip address
 duplex auto
 speed auto
```

Step 22 Configure Internet-facing interface and corresponding crypto maps.

```
interface FastEthernet2/0.1
 encapsulation dot1Q 10
 ip address 30.1.1.2 255.255.255.0
 crypto map vpn
!
interface FastEthernet2/1
 no ip address
 duplex auto
 speed auto
```

Step 23 Apply crypto maps towards HQ.

```
interface FastEthernet2/1.1
 encapsulation dot1Q 10
 ip address 125.1.10.2 255.255.255.0
 crypto map vpn_out
```

Step 24 Configure the IGP used in the core.

```
router ospf 1
 log-adjacency-changes
 network 125.1.10.0 0.0.0.255 area 0
```

Step 25 Configure the pool to distribute IP addresses to VPN clients.

```
ip local pool hw-pool 192.168.1.1 192.168.1.254
```

```
ip classless
```

Step 26 Configure global default route.

```
ip route 0.0.0.0 0.0.0.0 FastEthernet2/0.1 30.1.1.1
```

Step 27 Configure static VPN routes.

```
ip route vrf vpn1 101.1.1.0 255.255.255.0 30.1.1.1 global
ip route vrf vpn1 101.1.2.0 255.255.255.0 125.1.10.1 global
```

Step 28 Configure the crypto access list defining traffic to be encrypted toward the sites.

```
access-list 101 permit ip 101.1.2.0 0.0.0.255 101.1.1.0 0.0.0.255
```

Step 29 Configure the Crypto access list defining traffic to be encrypted towards HQ.

```
access-list 151 permit ip 101.1.1.0 0.0.0.255 101.1.2.0 0.0.0.255
```

IPSec to GRE Service Models

This chapter describes how to configure the IPSec to GRE, IPSec to GRE+IPSec, and the PE to PE Encryption service models for the Cisco Network-Based IPSec VPN Release 1.5 .

Configuring the IPSec to GRE Service Model

The IPSec to GRE model is useful when the service provider has a IP backbone but still wants to provide VPN-like functionality. Remote sites and clients terminate as in the IPSec to IPSec model, however they are then encapsulated into GRE and forwarded to a customer headend router that is the other endpoint for GRE.

GRE also lets you run a routing protocol on per-VRF basis with the headend customer router. The GRE tunnels towards the headend can also be encrypted. The packets traveling from remote clients and sites are decrypted, routed to the GRE tunnel interface where they are encapsulated with the GRE header, and then the GRE packet is encrypted by IPSec to provide secure connectivity across the IP backbone.

Before You Begin

The procedures provided here are specific to configuring IPSec to IPSec with one box and are based on the following assumptions:

1. That the following setup and configuration tasks have already been completed:

- Setup of the core IP/MPLS network.
- Setup of the customer VPN
- Configuration of the links between the PE and the CE.
- Customer-specific information is complete.
- That you have a good understanding of the architecture and features you are using and that you have selected the means you will use to implement those features (for example, which of several strategies you will use for address management or for user authentication and authorization).

IPSec to GRE Integration Configuration Checklist

This section deals with configuring the router to function as the IPSec aggregator.

Procedures for competing each task are described in the sections that follow. If you are viewing this document online, you can click on highlighted text to get details on the procedure.

Table 5-1 IPSec to GRE Configuration Checklist

Task 1: Configure Authentication and Authorization Lists for Clients to RADIUS, page 5-3
Task 2: Configure the VRFs, page 5-3
Task 3: Enable CEF Switching, page 5-3
Task 4: Configure the Keyring, page 5-3
Task 5: Configure ISAKMP Policy for Phase 1 Negotiations, page 5-3
Task 6: Configure DPD Keepalives, page 5-4
Task 7: Configure Client Group Definition for Local Authorization, page 5-4
Task 8: Configure ISAKMP Profile for VPN Sites, page 5-4
Task 9: Configure Dynamic VRF Association for VPN Sites, page 5-4
Task 10: Configure ISAKMP Profile for VPN Clients, page 5-4
Task 11: Configure Dynamic VRF Association for VPN Clients, page 5-5
Task 12: Configure XAUTH, Group Authorization, and Mode-Config, page 5-5
Task 13: Configure the Transform Set, page 5-5
Task 14: Configure Dynamic Crypto Map and Apply Transform Set, page 5-5
Task 15: Configure ISAKMP Client Profile Reference, page 5-5
Task 16: Configure Client RRI, page 5-6
Task 17: Configure Static Crypto Map for Sites, page 5-6
Task 18: Configure ISAKMP Site Profile Reference, page 5-6
Task 19: Configure Dynamic Crypto Map for Clients, page 5-6
Task 20: Configure GRE Tunnel to HQ, page 5-6
Task 21: Configure Internet-Facing Interface and Corresponding Crypto Maps, page 5-7
Task 22: Configure the IGP Used In Core, page 5-7
Task 23: Configure Pool to Distribute IP Addresses to VPN Clients, page 5-7
Task 24: Configure the Global Default Route, page 5-7
Task 25: Configure Static VPN Routes if not using IGP within the VPN, page 5-8
Task 26: Configure the Crypto Access List to Define Traffic to be Encrypted, page 5-8

IPSec to GRE Configuration Task List

Typical IPSec to GRE configuration tasks are shown below. See IPSec to GRE Configuration Sample, page 5-9.

Task 1: Configure Authentication and Authorization Lists for Clients to RADIUS

	Command	Purpose
Step 1	**aaa authentication login**	Set authentication, authorization, and accounting (AAA) authentication at login.
Step 2	**aaa authorization**	Set parameters that restrict user access to a network.

Task 2: Configure the VRFs

	Command	Purpose
Step 1	`ip vrf`	Configure a VPN routing and forwarding (VRF) routing table.
Step 2	`rd route-distinguisher`	Create routing and forwarding tables for a VRF.

Task 3: Enable CEF Switching

Command	Purpose
`ip cef`	Enable CEF switching.

Task 4: Configure the Keyring

	Command	Purpose
Step 1	`crypto keyring keyring-name [vrf fvrf]`	Configure a new keyring for the shared secret keys to be used during Internet Key Exchange (IKE) authentication.
Step 2	`pre-shared-key {address address [mask] | hostname hostname} key key`	Configure the addressed preshared key to be used during IKE authentication.

Task 5: Configure ISAKMP Policy for Phase 1 Negotiations

	Command	Purpose
Step 1	`crypto isakmp policy priority`	Configure an IKE policy.
Step 2	`encryption {des | 3des | aes | aes 192 | aes 256}`	Specify the encryption algorithm within an IKE policy.
Step 3	`authentication {rsa-sig | rsa-encr | pre-share}`	Specify the authentication method within an IKE policy.

Task 6: Configure DPD Keepalives

Command	Purpose
crypto isakmp keepalive secs retries	Allow the gateway to send dead peer detection (DPD) messages to the router.

Task 7: Configure Client Group Definition for Local Authorization

	Command	Purpose
Step 1	**crypto isakmp client configuration group** {group-name | default}	Specify which group's policy profile will be defined.
Step 2	**key** name	Configure the IKE preshared key for group policy attribute definition.
Step 3	**pool** (name)	Configure a local pool address.

Task 8: Configure ISAKMP Profile for VPN Sites

Command	Purpose
crypto isakmp profile profile-name	Define an ISAKMP profile for a VPN.

Task 9: Configure Dynamic VRF Association for VPN Sites

	Command	Purpose
Step 1	**vrf** name	Associate the on-demand address pool with a VRF name.
Step 2	**keyring** keyring-name	Associate a keyring with an ISAKMP profile.
Step 3	**match identity address** address [mask] [fvrf]	Match an acceptable Phase 1 identity from a peer to a particular ISAKMP profile.

Task 10: Configure ISAKMP Profile for VPN Clients

Command	Purpose
crypto isakmp profile profile-name	Define an ISAKMP profile for a VPN.

Note You can configure the Remote sites to match each peer using sequence numbers in the crypto map definition.You can match the peer on IP address or the hostname. The IP address match list for traffic to be encrypted is also defined for each peer. In case of VPN clients, the dynamic profile defined earlier is used to match the clients.

Task 11: Configure Dynamic VRF Association for VPN Clients

	Command	Purpose
Step 1	**vrf** name	Associate the on-demand address pool with a VRF name. See vrf for information on using this command.
Step 2	**match identity** group-name	Match an acceptable Phase 1 identity from a peer to a Unity group.

Task 12: Configure XAUTH, Group Authorization, and Mode-Config

	Command	Purpose
Step 1	**client authentication list** list-name	Configure IKE extended authentication (Xauth) on your router. The list-name must match the list-name defined during AAA configuration
Step 2	**isakmp authorization list** list-name	Configure group authorization IKE querying of AAA for tunnel attributes in aggressive mode.
Step 3	**client configuration address [initiate | respond]**	Configure IKE mode configuration (Mode-Config).

Task 13: Configure the Transform Set

Command	Purpose
crypto ipsec transform-set transform-set-name transform1 [transform2] [transform3] [transform4]	Define the transform set.

Task 14: Configure Dynamic Crypto Map and Apply Transform Set

	Command	Purpose
Step 1	**crypto dynamic-map** dynamic-map-name dynamic-seq-num	Create a dynamic crypto map entry and enter the crypto map configuration command mode.
Step 2	**set transform-set** transform-set-name	Specify which transform sets can be used with the crypto map entry.

Task 15: Configure ISAKMP Client Profile Reference

Command	Purpose
set isakmp-profile profile-name	Set the ISAKMP profile name for client.

Task 16: Configure Client RRI

Command	Purpose
reverse-route [remote-peer]	Create source proxy information for a crypto map entry through RRI.

Task 17: Configure Static Crypto Map for Sites

	Command	Purpose
Step 1	**crypto map** map-name seq-num [**ipsec-isakmp**]	Create a crypto map entry that uses IKE to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.
Step 2	**set peer** {hostname | ip-address}	Specify an IP Security peer in a crypto map entry.
Step 3	**set transform-set** transform-set-name	Specify which transform sets can be used with the crypto map entry.

Task 18: Configure ISAKMP Site Profile Reference

	Command	Purpose
Step 1	**set isakmp-profile** profile-name	Set the ISAKMP profile name reference.
Step 2	**match identity address** address [mask] [fvrf]	Match an acceptable Phase 1 identity from a peer to a particular ISAKMP profile.

Task 19: Configure Dynamic Crypto Map for Clients

Command	Purpose
crypto map map-name seq-num [**ipsec-isakmp**]	Create a crypto map entry that uses IKE to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.

Task 20: Configure GRE Tunnel to HQ

	Command	Purpose
Step 1	**interface** type	Configure an interface type and enter interface configuration mode.
Step 2	**ip vrf forwarding** *vrf-name*	Associate a VRF instance with an interface or subinterface.
Step 3	**ip address** ip-address mask	Set an IP address for an interface.

Step 4	**tunnel source** {**ip-address** | ***type*** number}	Set source address for a tunnel interface.
Step 5	**tunnel destination** {***hostname*** | ***ip-address***}	Specify the destination for a tunnel interface.

Task 21: Configure Internet-Facing Interface and Corresponding Crypto Maps

	Command	Purpose
Step 1	**interface** type	Configure a loopback interface (emulates an interface that is always up).
Step 2	**ip address** ip-address mask	Set an IP address for an interface.
Step 3	**encapsulation dot1q** vlan-id **[native]**	Enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN).
Step 4	**crypto map** map-name	Apply a previously defined crypto map set to an interface.

Note Each interface services one VPN as the IPSec tunnel endpoint for both the sites and clients.

Task 22: Configure the IGP Used In Core

	Command	Purpose
Step 1	**router ospf** process-id	Configure an OSPF routing process.
Step 2	**log-adjacency-changes**	Generate a log message.
Step 3	**network ip**-address wildcard-mask **area** area-id	Configure the interfaces on which OSPF runs and to define the area ID for those interfaces.

Task 23: Configure Pool to Distribute IP Addresses to VPN Clients

Command	Purpose
ip local pool {**default** | pool-name low-ip-address [**high-ip-address**]}	Configure a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.

Task 24: Configure the Global Default Route

Command	Purpose
ip route network-number network-mask {**ip-address** | **interface-name**} **[distance] [name** name]	Establish static routes and define the next hop for large-scale dial-out.

Task 25: Configure Static VPN Routes if not using IGP within the VPN

Command	Purpose
ip route vrf vrf-name prefix mask **[next-hop-address] [interface {interface-number}] [global] [distance] [permanent] [tag** tag**]**	Establish static routes for a VRF instance.

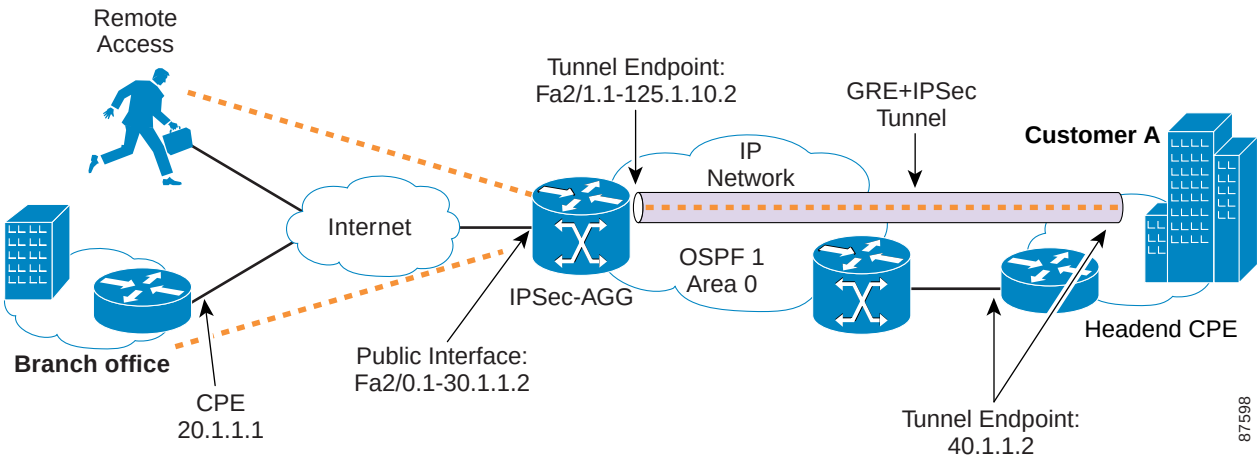
Task 26: Configure the Crypto Access List to Define Traffic to be Encrypted

Command	Purpose
access-list access-list-number **{deny** | **permit}** source **[source-wildcard] [log]**	Configure a standard IP access list.

IPSec to GRE Configuration Sample

Figure 5-1 illustrates the following IPSec to GRE configuration.

Figure 5-1 IPSec to GRE Configuration




```
pe1#sh run
Building configuration...

Current configuration : 3783 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname pe1
enable password cisco
!
username cisco password 0 cisco
aaa new-model
```

Step 1 Configure authentication and authorization lists for clients to RADIUS.

```
aaa authentication login localist local
aaa authorization network localist local
aaa session-id common
ip subnet-zero
no ip domain lookup
```

Step 2 Configure VRFs.

```
ip vrf vpn1
 rd 100:1
```

Step 3 Enable CEF switching.

```
ip cef
```

Step 4 Configure keyring.

```
crypto keyring vpn1
```

```
 pre-shared-key address 20.1.1.1 key cisco123
```

Step 5 Configure ISAKMP policy for Phase 1 negotiations.

```
crypto isakmp policy 1
 authentication pre-share
 group 2
!
crypto isakmp policy 2
 encr 3des
 authentication pre-share
```

Step 6 Configure DPD keepalives.

```
crypto isakmp keepalive 30
crypto isakmp xauth timeout 30
```

Step 7 Configure client group for local authorization**.**

```
crypto isakmp client configuration group ezvpn
 key cisco123
 pool hw-pool
```

Step 8 Configure ISAKMP profile for VPN sites.

```
crypto isakmp profile vpn1
```

Step 9 Configure dynamic VRF association for sites.

```
   vrf vpn1
   keyring vpn1
   match identity address 20.1.1.1 255.255.255.255
```

Step 10 Configure ISAKMP profile for VPN clients.

```
crypto isakmp profile vpn1-ez
```

Step 11 Configure dynamic VRF association for VPN clients.

```
   vrf vpn1
   match identity group ezvpn
```

Step 12 Configure XAUTH, group authorization, and mode-config.

```
   client authentication list localist
   isakmp authorization list localist
   client configuration address respond
```

Step 13 Configure the transform set.

```
crypto ipsec transform-set tset1 esp-3des esp-sha-hmac
```

Step 14 Configure dynamic crypto map and apply transform set.

```
crypto dynamic-map dyna 1
 set security-association idle-time 3600
 set transform-set tset1
```

Step 15 Configure ISAKMP client profile reference.

```
 set isakmp-profile vpn1-ez
```

Step 16 Configure client RRI.

```
 reverse-route
```

Step 17 Configure static map for a site.

```
crypto map vpn 10 ipsec-isakmp
 set peer 20.1.1.1
 set transform-set tset1
```

Step 18 Configure ISAKMP site profile reference.

```
 set isakmp-profile vpn1
 match address 101
```

Step 19 Configure dynamic crypto map for clients.

```
crypto map vpn 1000 ipsec-isakmp dynamic dyna
```

Step 20 Configure GRE tunnel to HQ.

```
interface Tunnel1
 ip vrf forwarding vpn1
 ip address 11.1.1.1 255.255.255.0
 tunnel source 125.1.10.2
 tunnel destination 40.1.1.2
!
interface FastEthernet2/0
 no ip address
 duplex auto
 speed auto
```

Step 21 Configure Internet-facing interface and corresponding crypto maps.

```
interface FastEthernet2/0.1
 encapsulation dot1Q 10
 ip address 30.1.1.2 255.255.255.0
 crypto map vpn
!
interface FastEthernet2/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet2/1.1
 encapsulation dot1Q 10
 ip address 125.1.10.2 255.255.255.0
```

Step 22 Configure the IGP used in the core.

```
router ospf 1
 log-adjacency-changes
 network 125.1.10.0 0.0.0.255 area 0
```

Step 23 Configure the pool to distribute IP addresses to VPN clients.

```
ip local pool hw-pool 192.168.1.1 192.168.1.254
ip classless
```

Step 24 Configure global default route.

```
ip route 0.0.0.0 0.0.0.0 FastEthernet2/0.1 30.1.1.1
```

Step 25 Configure static VPN routes if not using an IGP within the VPN.

```
ip route vrf vpn1 101.1.1.0 255.255.255.0 30.1.1.1 global
ip route vrf vpn1 101.1.2.0 255.255.255.0 Tunnel1
```

Step 26 Configure the crypto access list to define the traffic to be encrypted.

```
access-list 101 permit ip 101.1.2.0 0.0.0.255 101.1.1.0 0.0.0.255
```

Configuring IPSec to GRE+IPSec Service Model

The difference between the IPSec to GRE configuration and the IPSec to GRE+IPSec configuration is that in the IPSec to GRE configuration the GRE tunnel is not encrypted and in the IPSec to GRE+IPSec configuration the GRE tunnel is encrypted.

Before You Begin

The procedures provided here are specific to configuring IPSec to GRE+IPSec and are based on the following assumptions:

- That the following setup and configuration tasks have already been completed:
- Setup of the core MPLS network.
- Setup of the customer VPN
- Configuration of the links between the PE and the CE.
- Customer-specific information is complete.
- That you have a good understanding of the architecture and features you are using and that you have selected the means you will use to implement those features (for example, which of several strategies you will use for address management or for user authentication and authorization).

IPSec to GRE+IPSec Integration Configuration Checklist

This section deals with configuring the router to function as both the IPSec aggregator and the PE router.

Procedures for competing each task are described in the sections that follow. If you are viewing this document online, you can click on highlighted text to get details on the procedure.

Table 5-2 IPSec to GRE +IPSec Configuration Checklist

Task 1: Configure Authentication and Authorization Lists for Clients to RADIUS, page 5-13
Task 2: Configure the VRFs, page 5-14
Task 3: Configure the Keyring, page 5-14
Task 4: Configure ISAKMP Policy for Phase 1 Negotiations, page 5-14
Task 5: Configure DPD Keepalives, page 5-14
Task 6: Configure Client Group Definition for Local Authorization, page 5-14
Task 7: Configure ISAKMP Profile for VPN Sites, page 5-15
Task 8: Configure Dynamic VRF Association for VPN Sites, page 5-15

Table 5-2 IPSec to GRE +IPSec Configuration Checklist (continued)

Task 9: Configure ISAKMP Profile for VPN Clients, page 5-15
Task 10: Configure Dynamic VRF Association for VPN Clients, page 5-15
Task 11: Configure XAUTH, Group Authorization, and Mode-Config, page 5-15
Task 12: Configure the Transform Set, page 5-16
Task 13: Configure GRE Tunnel Encryption Profile, page 5-16
Task 14: Configure ISAKMP Site Profile Reference, page 5-16
Task 15: Configure Dynamic Crypto Map and Apply Transform Set, page 5-16
Task 16: Configure ISAKMP Client Profile Reference, page 5-16
Task 17: Configure Client RRI, page 5-17
Task 18: Configure Static Crypto Map for Sites, page 5-17
Task 19: Configure ISAKMP Site Profile Reference, page 5-17
Task 20: Configure Dynamic Crypto Map for Clients, page 5-17
Task 21: Configure GRE Tunnel to Customer Site, page 5-17
Task 22: Configure IPSec Profile to be Used, page 5-18
Task 23: Configure Internet-Facing Interface and Corresponding Crypto Maps, page 5-18
Task 24: Configure Interface Towards IP Backbone, page 5-18
Task 25: Configure IGP Used in the Core, page 5-18
Task 26: Configure Pool Used to Distribute IP Addresses to VPN Clients, page 5-19
Task 27: Configure Global Default Route, page 5-19
Task 28: Configure Static VPN Routes if not using IGP within the VPN, page 5-19
Task 29: Configure the Crypto Access List to Define Traffic to be Encrypted, page 5-19

IPSec to GRE+IPSec Configuration Tasks

Typical IPSec to GRE+IPSec configuration tasks are shown below. See IPSec to GRE+IPSec Configuration Sample, page 5-20.

Task 1: Configure Authentication and Authorization Lists for Clients to RADIUS

	Command	Purpose
Step 1	`aaa authentication login`	Set authentication, authorization, and accounting (AAA) authentication at login.
Step 2	`aaa authorization`	Set parameters that restrict user access to a network.
Step 3	`aaa session-id [common | unique]`	Specify whether the same session ID will be used for each AAA accounting service type within a call or whether a different session ID will be assigned to each accounting service type.

Task 2: Configure the VRFs

	Command	Purpose
Step 1	**ip vrf**	Configure a VRF routing table.
Step 2	**rd** route-distinguisher	Create routing and forwarding tables for a VRF.

Task 3: Configure the Keyring

	Command	Purpose
Step 1	**crypto keyring** keyring-name [**vrf** fvrf]	Configure a new keyring for the shared secret keys to be used during IKE authentication.
Step 2	**pre-shared-key** {**address** address [mask] | **hostname** hostname} **key** key	Configure the addressed preshared key to be used during IKE authentication.

Task 4: Configure ISAKMP Policy for Phase 1 Negotiations

.

	Command	Purpose
Step 1	**crypto isakmp policy** priority	Configure an IKE policy.
Step 2	**encryption {des** | **3des** | **aes** | **aes 192** | **aes 256}**	Specify the encryption algorithm within an IKE policy.
Step 3	**authentication {rsa-sig** | **rsa-encr** | **pre-share}**	Specify the authentication method within an IKE policy.

Task 5: Configure DPD Keepalives

Command	Purpose
crypto isakmp keepalive secs retries	Allow the gateway to send dead peer detection (DPD) messages to the router.

Task 6: Configure Client Group Definition for Local Authorization

	Command	Purpose
Step 1	**crypto isakmp client configuration group** {group-name | default}	Specify which group's policy profile will be defined.
Step 2	**key** name	Configure the IKE preshared key for group policy attribute definition.
Step 3	**pool** (name)	Configure a local pool address.

Task 7: Configure ISAKMP Profile for VPN Sites

Command	Purpose
crypto isakmp profile profile-name	Define an ISAKMP profile for a VPN.

Task 8: Configure Dynamic VRF Association for VPN Sites

	Command	Purpose
Step 1	**vrf** name	Associate the on-demand address pool with a VRF name.
Step 2	**keyring** keyring-name	Associate a keyring with an ISAKMP profile.
Step 3	**match identity address** address [mask] [fvrf]	Match an acceptable Phase 1 identity from a peer to a particular ISAKMP profile.

Task 9: Configure ISAKMP Profile for VPN Clients

Command	Purpose
crypto isakmp profile profile-name	Define an ISAKMP profile for a VPN.

Note You can configure the Remote sites to match each peer using sequence numbers in the crypto map definition.You can match the peer on IP address or the hostname. The IP address match list for traffic to be encrypted is also defined for each peer. In case of VPN clients, the dynamic profile defined earlier is used to match the clients.

Task 10: Configure Dynamic VRF Association for VPN Clients

	Command	Purpose
Step 1	**vrf** name	Associate the on-demand address pool with a VRF name. See vrf for information on using this command.
Step 2	**match identity** group-name	Match an acceptable Phase 1 identity from a peer to a Unity group.

Task 11: Configure XAUTH, Group Authorization, and Mode-Config

	Command	Purpose
Step 1	**client authentication list** list-name	Configure IKE extended authentication (Xauth) on your router. The list-name must match the list-name defined during AAA configuration

Step 2	**isakmp authorization list** list-name	Configure group authorization IKE querying of AAA for tunnel attributes in aggressive mode.
Step 3	**client configuration address [initiate | respond]**	Configure IKE mode configuration (Mode-Config).

Task 12: Configure the Transform Set

Command	Purpose
crypto ipsec transform-set transform-set-name transform1 [transform2] [transform3] [transform4]	Define the transform set.

Task 13: Configure GRE Tunnel Encryption Profile

	Command	Purpose
Step 1	**crypto ipsec profile**	Configure IPSec profile.
Step 2	**set transform-set** transform-set-name	Specify which transform sets can be used with the crypto map entry.

Task 14: Configure ISAKMP Site Profile Reference

Command	Purpose
set isakmp-profile profile-name	Set the ISAKMP profile name for client.

Task 15: Configure Dynamic Crypto Map and Apply Transform Set

	Command	Purpose
Step 1	**crypto dynamic-map** dynamic-map-name dynamic-seq-num	Create a dynamic crypto map entry and enter the crypto map configuration command mode.
Step 2	**set transform-set** transform-set-name	Specify which transform sets can be used with the crypto map entry.

Task 16: Configure ISAKMP Client Profile Reference

Command	Purpose
set isakmp-profile profile-name	Set the ISAKMP profile name for client.

Task 17: Configure Client RRI

Command	Purpose
reverse-route [remote-peer]	Create source proxy information for a crypto map entry through RRI.

Task 18: Configure Static Crypto Map for Sites

	Command	Purpose
Step 1	**crypto map** map-name seq-num [**ipsec-isakmp**]	Create a crypto map entry that uses IKE to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.
Step 2	**set peer** {hostname | ip-address}	Specify an IP Security peer in a crypto map entry.
Step 3	**set transform-set** transform-set-name	Specify which transform sets can be used with the crypto map entry.

Task 19: Configure ISAKMP Site Profile Reference

	Command	Purpose
Step 1	**set isakmp-profile** profile-name	Set the ISAKMP profile name reference.
Step 2	**match identity address** address [mask] [fvrf]	Match an acceptable Phase 1 identity from a peer to a particular ISAKMP profile.

Task 20: Configure Dynamic Crypto Map for Clients

Command	Purpose
crypto map map-name seq-num [**ipsec-isakmp**]	Create a crypto map entry that uses IKE to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.

Task 21: Configure GRE Tunnel to Customer Site

	Command	Purpose
Step 1	**interface** type	Configure an interface type and enter interface configuration mode.
Step 2	**ip vrf forwarding** *vrf-name*	Associate a VRF instance with an interface or subinterface.
Step 3	**ip address** ip-address mask	Set an IP address for an interface.

Step 4	**tunnel source** {**ip-address** | ***type*** number}	Set source address for a tunnel interface.
Step 5	**tunnel destination** {***hostname*** | ***ip-address***}	Specify the destination for a tunnel interface.

Task 22: Configure IPSec Profile to be Used

Command	Purpose
tunnel protection ipsec-profile name	Associate a tunnel interface with an IPSec profile.

Task 23: Configure Internet-Facing Interface and Corresponding Crypto Maps

	Command	Purpose
Step 1	**interface** type	Configure a loopback interface (emulates an interface that is always up).
Step 2	**ip address** ip-address mask	Set an IP address for an interface.
Step 3	**encapsulation dot1q** vlan-id **[native]**	Enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN).
Step 4	**crypto map** map-name	Apply a previously defined crypto map set to an interface.

Note Each interface services one VPN as the IPSec tunnel endpoint for both the sites and clients.

Task 24: Configure Interface Towards IP Backbone

	Command	Purpose
Step 1	**interface** type	Configure a loopback interface (emulates an interface that is always up).
Step 2	**encapsulation dot1q** vlan-id **[native]**	Enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN).
Step 3	**ip address** ip-address mask	Set an IP address for an interface.

Task 25: Configure IGP Used in the Core

	Command	Purpose
Step 1	**router ospf** process-id	Configure an OSPF routing process.
Step 2	**log-adjacency-changes**	Generate a log message.
Step 3	**network** ip-address wildcard-mask **area** area-id	Configure the interfaces on which OSPF runs and to define the area ID for those interfaces.

Task 26: Configure Pool Used to Distribute IP Addresses to VPN Clients

Command	Purpose
ip local pool {**default** | pool-name low-ip-address [**high-ip-address**]}	Configure a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.

Task 27: Configure Global Default Route

Command	Purpose
ip route network-number network-mask {**ip-address** | **interface-name**} **[distance] [name** name]	Establish static routes and define the next hop for large-scale dial-out.

Task 28: Configure Static VPN Routes if not using IGP within the VPN

Command	Purpose
ip route vrf vrf-name prefix mask **[next-hop-address] [interface** {**interface-number**}] **[global] [distance] [permanent] [tag** tag]	Establish static routes for a VPN routing and forwarding (VRF) instance.

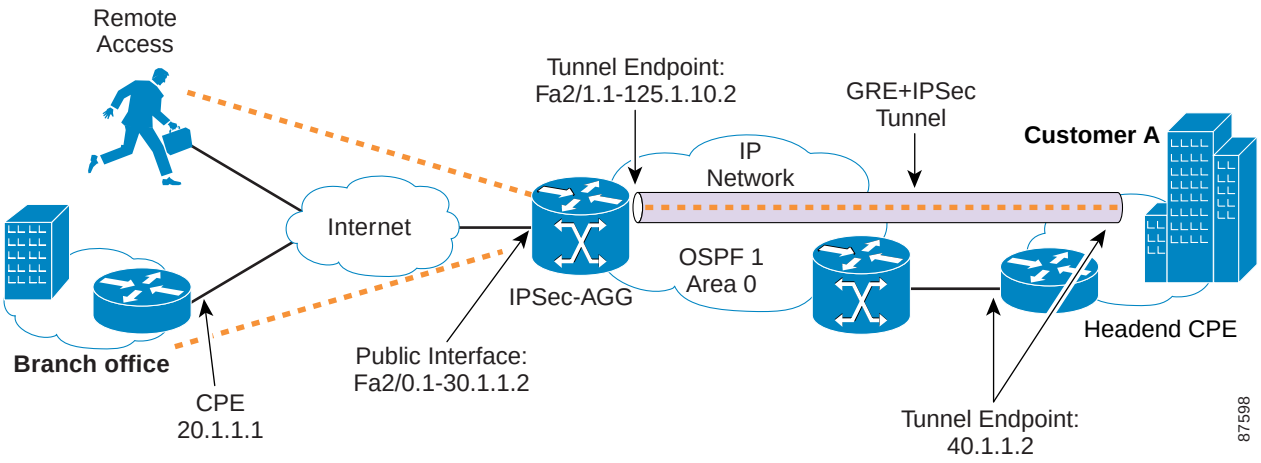
Task 29: Configure the Crypto Access List to Define Traffic to be Encrypted

Command	Purpose
access-list access-list-number {**deny** | **permit**} source **[source-wildcard] [log]**	Configure a standard IP access list.

IPSec to GRE+IPSec Configuration Sample

Figure 5-2 illustrates the following IPSec to GRE+IPSec configuration.

Figure 5-2 IPSec to GRE Configuration




```
pe1#sh run
Building configuration...

Current configuration : 4009 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname pe1
enable password cisco
!
username cisco password 0 cisco
aaa new-model
```

Step 1 Configure authentication and authorization lists for clients to RADIUS.

```
aaa authentication login localist local
aaa authorization network localist local
aaa session-id common
ip subnet-zero
no ip domain lookup
```

Step 2 Configure the VRFs.

```
ip vrf vpn1
 rd 100:1
```

Step 3 Configure keyring.

```
crypto keyring vpn1
  pre-shared-key address 20.1.1.1 key cisco123
  pre-shared-key address 40.1.1.2 key cisco123
```

Step 4 Configure the ISAKMP policy for phase 1 negotiations.

```
crypto isakmp policy 1
 authentication pre-share
 group 2
!
crypto isakmp policy 2
 encr 3des
 authentication pre-share
```

Step 5 Configure DPD keepalives.

```
crypto isakmp keepalive 30
crypto isakmp xauth timeout 30
```

Step 6 Configure client group for local authorization.

```
crypto isakmp client configuration group ezvpn
 key cisco123
 pool hw-pool
```

Step 7 Configure ISAKMP profile for VPN sites.

```
crypto isakmp profile vpn1
```

Step 8 Configure dynamic VRF association for sites.

```
vrf vpn1
   keyring vpn1
   match identity address 20.1.1.1 255.255.255.255
   match identity address 40.1.1.2 255.255.255.255
```

Step 9 Configure ISAKMP profile for VPN clients.

```
crypto isakmp profile vpn1-ez
```

Step 10 Configure dynamic VRF association for VPN clients.

```
   vrf vpn1
   match identity group ezvpn
```

Step 11 Configure XAUTH, group authorization, and mode-config.

```
   client authentication list localist
   isakmp authorization list localist
   client configuration address respond
```

Step 12 Configure transform set.

```
crypto ipsec transform-set tset1 esp-3des esp-sha-hmac
```

Step 13 Configure GRE tunnel encryption profile.

```
crypto ipsec profile pe_to_hq
 set transform-set tset1
```

Step 14 Configure ISAKMP site profile reference.

```
 set isakmp-profile vpn1
```

Step 15 Configure dynamic crypto map and apply transform set.

```
crypto dynamic-map dyna 1
 set security-association idle-time 3600
 set transform-set tset1
```

Step 16 Configure ISAKMP client profile reference.

```
 set isakmp-profile vpn1-ez
```

Step 17 Configure client RRI.

```
 reverse-route
```

Step 18 Configure static map for a site.

```
crypto map vpn 10 ipsec-isakmp
 set peer 20.1.1.1
 set transform-set tset1
```

Step 19 Configure ISAKMP site profile reference.

```
 set isakmp-profile vpn1
 match address 101
```

Step 20 Configure dynamic crypto map for clients.

```
crypto map vpn 1000 ipsec-isakmp dynamic dyna
```

Step 21 Configure encrypted GRE tunnel to customer site.

```
interface Tunnel1
 ip vrf forwarding vpn1
 ip address 11.1.1.1 255.255.255.0
 tunnel source 125.1.10.2
 tunnel destination 40.1.1.2
```

Step 22 Configure IPSec profile to be used.

```
 tunnel protection ipsec profile pe_to_hq
!
interface FastEthernet2/0
 no ip address
 duplex auto
 speed auto
```

Step 23 Configure internet-facing interface and corresponding crypto maps.

```
interface FastEthernet2/0.1
 encapsulation dot1Q 10
 ip address 30.1.1.2 255.255.255.0
 crypto map vpn
!
interface FastEthernet2/1
 no ip address
 duplex auto
 speed auto
```

Step 24 Configure interface towards IP backbone.

```
interface FastEthernet2/1.1
 encapsulation dot1Q 10
 ip address 125.1.10.2 255.255.255.0
```

Step 25 Configure IGP used in the core.

```
router ospf 1
 log-adjacency-changes
 network 99.1.1.1 0.0.0.0 area 0
 network 125.1.10.0 0.0.0.255 area 0
```

Step 26 Configure the pool to distribute IP addresses to VPN clients.

```
ip local pool hw-pool 192.168.1.1 192.168.1.254
ip classless
```

Step 27 Configure global default route.

```
ip route 0.0.0.0 0.0.0.0 FastEthernet2/0.1 30.1.1.1
```

Step 28 Configure static VPN routes if not using an IGP within the VPN.

```
ip route vrf vpn1 101.1.1.0 255.255.255.0 30.1.1.1 global
ip route vrf vpn1 101.1.2.0 255.255.255.0 Tunnel1
```

Step 29 Configure the crypto access list.

```
access-list 101 permit ip 101.1.2.0 0.0.0.255 101.1.1.0 0.0.0.255
```

Configuring PE to PE Encryption Service Model

In this configuration, a network of GRE tunnels is configured between all the PE devices. Only a single GRE tunnel is necessary between two PEs to service all the VPNs. This is because the VPN tag is maintained across the MPLS network.

Before You Begin

The procedures provided here are specific to configuring PE to PE Encryption and are based on the following assumptions:

- That the following setup and configuration tasks have already been completed:
- Setup of the core MPLS network.
- Setup of the customer VPN
- Configuration of the links between the PE and the CE.
- Customer-specific information is complete.
- That you have a good understanding of the architecture and features you are using and that you have selected the means you will use to implement those features (for example, which of several strategies you will use for address management or for user authentication and authorization).

PE to PE Encryption Configuration Checklist

This section deals with configuring the router to function as both the IPSec aggregator and the PE router.

Procedures for competing each task are described in the sections that follow. If you are viewing this document online, you can click on highlighted text to get details on the procedure.

Table 5-3 PE to PE Encryption Configuration Checklist

Task 1: Configure Authentication and Authorization Lists for Clients to RADIUS, page 5-25
Task 2: Configure the VRFs, page 5-25
Task 3: Enable CEF Switching, page 5-25
Task 4: Configure the Keyring, page 5-25
Task 5: Configure ISAKMP Policy for Phase 1 Negotiations, page 5-25

Table 5-3 PE to PE Encryption Configuration Checklist (continued)

Task 6: Configure DPD Keepalives, page 5-26
Task 7: Configure Client Group Definition for Local Authorization, page 5-26
Task 8: Configure ISAKMP Profile for VPN Sites, page 5-26
Task 9: Configure Dynamic VRF Association for VPN Sites, page 5-26
Task 10: Configure ISAKMP Profile for VPN Clients, page 5-26
Task 11: Configure Dynamic VRF Association for VPN Clients, page 5-27
Task 12: Configure XAUTH, Group Authorization, and Mode-Config, page 5-27
Task 13: Configure ISAKMP Profile for PE to PE Tunnel, page 5-27
Task 14: Configure the Transform Set, page 5-27
Task 15: Configure PE to PE GRE Tunnel Encryption Profile, page 5-27
Task 16: Configure ISAKMP Site Profile Reference, page 5-28
Task 17: Configure Client RRI, page 5-28
Task 18: Configure Static Crypto Map for Sites, page 5-28
Task 19: Configure ISAKMP Site Profile Reference, page 5-28
Task 20: Configure Dynamic Crypto Map for Clients, page 5-28
Task 21: Configure PE to PE GRE Tunnel, page 5-29
Task 22: Turn on Tag-Switching, page 5-29
Task 23: Configure IPSec Profile to be Used, page 5-29
Task 24: Configure Internet-Facing Interface and Corresponding Crypto Maps, page 5-29
Task 25: Configure Interface Towards IP Backbone, page 5-30
Task 26: Configure IGP Used in the Core, page 5-30
Task 27: Configure PE Peering for VPN Routes, page 5-30
Task 28: Configure Pool Used to Distribute IP Addresses to VPN Clients, page 5-30
Task 29: Configure Global Default Route, page 5-31
Task 30: Configure Static VPN Routes if not using IGP within the VPN, page 5-31
Task 31: Configure the Crypto Access List to Define Traffic to be Encrypted, page 5-31

Configuring PE to PE Encryption

Typical PE to PE encryption configuration tasks are shown below. See PE to PE Encryption Configuration Sample, page 5-32.

Task 1: Configure Authentication and Authorization Lists for Clients to RADIUS

	Command	Purpose
Step 1	`aaa authentication login`	Set authentication, authorization, and accounting (AAA) authentication at login.
Step 2	`aaa authorization`	Set parameters that restrict user access to a network.
Step 3	`aaa session-id [common | unique]`	Specify whether the same session ID will be used for each AAA accounting service type within a call or whether a different session ID will be assigned to each accounting service type.

Task 2: Configure the VRFs

	Command	Purpose
Step 1	`ip vrf`	Configure a VRF routing table.
Step 2	`rd route-distinguisher`	Create routing and forwarding tables for a VRF.

Task 3: Enable CEF Switching

Command	Purpose
`ip cef`	Enable CEF switching.

Task 4: Configure the Keyring

	Command	Purpose
Step 1	`crypto keyring keyring-name [vrf fvrf]`	Configure a new keyring for the shared secret keys to be used during IKE authentication.
Step 2	`pre-shared-key {address address [mask] | hostname hostname} key key`	Configure the addressed preshared key to be used during IKE authentication.

Task 5: Configure ISAKMP Policy for Phase 1 Negotiations

	Command	Purpose
Step 1	`crypto isakmp policy priority`	Configure an IKE policy.
Step 2	`encryption {des | 3des | aes | aes 192 | aes 256}`	Specify the encryption algorithm within an IKE policy.
Step 3	`authentication {rsa-sig | rsa-encr | pre-share}`	Specify the authentication method within an IKE policy.

Task 6: Configure DPD Keepalives

Command	Purpose
crypto isakmp keepalive secs retries	Allow the gateway to send dead peer detection (DPD) messages to the router.

Task 7: Configure Client Group Definition for Local Authorization

	Command	Purpose
Step 1	**crypto isakmp client configuration group** {group-name | default}	Specify which group's policy profile will be defined.
Step 2	**key** name	Configure the IKE preshared key for group policy attribute definition.
Step 3	**pool** (name)	Configure a local pool address.

Task 8: Configure ISAKMP Profile for VPN Sites

Command	Purpose
crypto isakmp profile profile-name	Define an ISAKMP profile for a VPN.

Task 9: Configure Dynamic VRF Association for VPN Sites

	Command	Purpose
Step 1	**vrf** name	Associate the on-demand address pool with a VRF name.
Step 2	**keyring** keyring-name	Associate a keyring with an ISAKMP profile.
Step 3	**match identity address** address [mask] [fvrf]	Match an acceptable Phase 1 identity from a peer to a particular ISAKMP profile.

Task 10: Configure ISAKMP Profile for VPN Clients

Command	Purpose
crypto isakmp profile profile-name	Define an ISAKMP profile for a VPN.

Note You can configure the Remote sites to match each peer using sequence numbers in the crypto map definition.You can match the peer on IP address or the hostname. The IP address match list for traffic to be encrypted is also defined for each peer. In case of VPN clients, the dynamic profile defined earlier is used to match the clients.

Task 11: Configure Dynamic VRF Association for VPN Clients

	Command	Purpose
Step 1	**vrf** name	Associate the on-demand address pool with a VRF name. See vrf for information on using this command.
Step 2	**match identity** group-name	Match an acceptable Phase 1 identity from a peer to a Unity group.

Task 12: Configure XAUTH, Group Authorization, and Mode-Config

	Command	Purpose
Step 1	**client authentication list** list-name	Configure IKE extended authentication (Xauth) on your router. The list-name must match the list-name defined during AAA configuration
Step 2	**isakmp authorization list** list-name	Configure group authorization IKE querying of AAA for tunnel attributes in aggressive mode.
Step 3	**client configuration address [initiate | respond]**	Configure IKE mode configuration (Mode-Config).

Task 13: Configure ISAKMP Profile for PE to PE Tunnel

Command	Purpose
crypto isakmp profile profile-name	Define an ISAKMP profile for a VPN.

Task 14: Configure the Transform Set

Command	Purpose
crypto ipsec transform-set transform-set-name transform1 [transform2] [transform3] [transform4]	Define the transform set.

Task 15: Configure PE to PE GRE Tunnel Encryption Profile

	Command	Purpose
Step 1	**crypto ipsec profile**	Configure IPSec profile.
Step 2	**set transform-set** transform-set-name	Specify which transform sets can be used with the crypto map entry.

Task 16: Configure ISAKMP Site Profile Reference

Command	Purpose
set isakmp-profile profile-name	Set the ISAKMP profile name for client.

Task 17: Configure Client RRI

Command	Purpose
reverse-route [remote-peer]	Create source proxy information for a crypto map entry through RRI.

Task 18: Configure Static Crypto Map for Sites

	Command	Purpose
Step 1	**crypto map** map-name seq-num [**ipsec-isakmp**]	Create a crypto map entry that uses IKE to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.
Step 2	**set peer** {hostname | ip-address}	Specify an IP Security peer in a crypto map entry.
Step 3	**set transform-set** transform-set-name	Specify which transform sets can be used with the crypto map entry.

Task 19: Configure ISAKMP Site Profile Reference

	Command	Purpose
Step 1	**set isakmp-profile** profile-name	Set the ISAKMP profile name reference.
Step 2	**match identity address** address [mask] [fvrf]	Match an acceptable Phase 1 identity from a peer to a particular isakmp profile.

Task 20: Configure Dynamic Crypto Map for Clients

Command	Purpose
crypto map map-name seq-num [**ipsec-isakmp**]	Create a crypto map entry that uses IKE to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.

Task 21: Configure PE to PE GRE Tunnel

	Command	Purpose
Step 1	**interface** type	Configure an interface type and enter interface configuration mode.
Step 2	**ip address** ip-address mask	Set an IP address for an interface.

Task 22: Turn on Tag-Switching

	Command	Purpose
Step 1	**tag-switching ip**	Configure label switching of IPv4 packets on an interface.
Step 2	**tunnel source** {**ip-address** | ***type*** number}	Set source address for a tunnel interface.
Step 3	**tunnel destination** {***hostname*** | ***ip-address***}	Specify the destination for a tunnel interface.

Task 23: Configure IPSec Profile to be Used

Command	Purpose
tunnel protection ipsec-profile name	Associate a tunnel interface with an IPSec profile.

Task 24: Configure Internet-Facing Interface and Corresponding Crypto Maps

	Command	Purpose
Step 1	**interface** type	Configure a loopback interface (emulates an interface that is always up).
Step 2	**ip address** ip-address mask	Set an IP address for an interface.
Step 3	**encapsulation dot1q** vlan-id **[native]**	Enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN).
Step 4	**crypto map** map-name	Apply a previously defined crypto map set to an interface.

Task 25: Configure Interface Towards IP Backbone

	Command	Purpose
Step 1	**interface** type	Configure a loopback interface (emulates an interface that is always up).
Step 2	**encapsulation dot1q** vlan-id **[native]**	Enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN).
Step 3	**ip address** ip-address mask	Set an IP address for an interface.
Step 4	**tag-switching ip**	Configure label switching of IPv4 packets on an interface.

Task 26: Configure IGP Used in the Core

	Command	Purpose
Step 1	**router ospf** process-id	Configure an OSPF routing process.
Step 2	**log-adjacency-changes**	Generate a log message.
Step 3	**network ip**-address wildcard-mask **area** area-id	Configure the interfaces on which OSPF runs and to define the area ID for those interfaces.

Task 27: Configure PE Peering for VPN Routes

	Command	Purpose
Step 1	**address-family vpnv4**	Configure address family configuration mode for configuring routing sessions, such as BGP, that use standard Virtual Private Network (VPN) Version 4 address prefixes.
Step 2	**neighbor** *ip address*	Configure the neighboring border elements (BEs) that interact with the local BE for the purpose of obtaining addressing information and aiding inaddress resolution.

Task 28: Configure Pool Used to Distribute IP Addresses to VPN Clients

	Command	Purpose
Step 1	**ip local pool** {**default** | pool-name low-ip-address [**high-ip-address**]}	Configure a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.

Task 29: Configure Global Default Route

Command	Purpose
ip route network-number network-mask {**ip-address** | **interface-name**} **[distance] [name** name]	Establish static routes and define the next hop for large-scale dial-out.

Task 30: Configure Static VPN Routes if not using IGP within the VPN

Command	Purpose
ip route vrf vrf-name prefix mask **[next-hop-address] [interface {interface-number}] [global] [distance] [permanent] [tag** tag]	Establish static routes for a VPN routing and forwarding (VRF) instance.

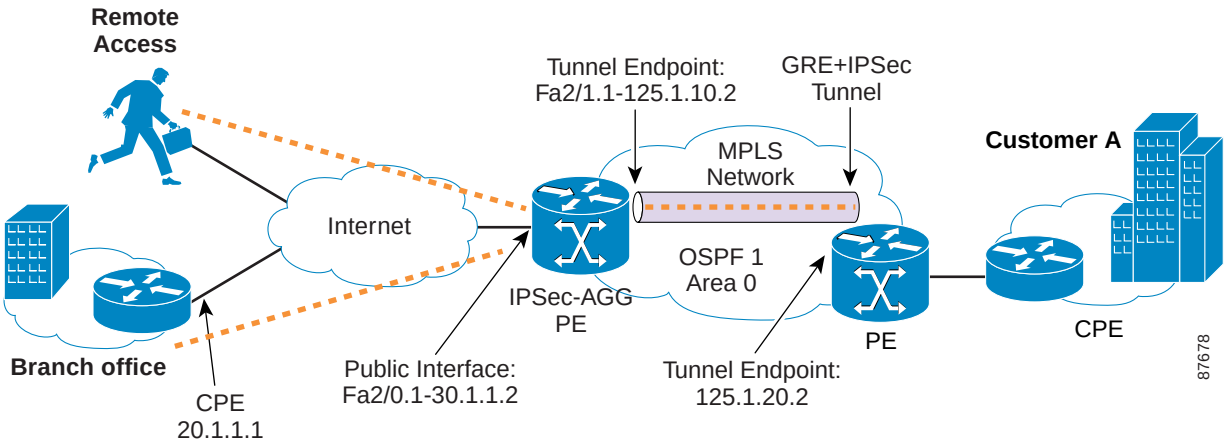
Task 31: Configure the Crypto Access List to Define Traffic to be Encrypted

Command	Purpose
access-list access-list-number **{deny** | **permit}** source **[source-wildcard] [log]**	Configure a standard IP access list.

PE to PE Encryption Configuration Sample

Figure 5-3 illustrates the following PE to PE encryption configuration.

Figure 5-3 PE to PE Encryption Configuration




```
pe1#sh run
Building configuration...

Current configuration : 4459 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname pe1
enable password cisco
username cisco password 0 cisco
aaa new-model
```

Step 1 Configure authentication and authorization lists for clients to RADIUS.

```
aaa authentication login localist local
aaa authorization network localist local
aaa session-id common
ip subnet-zero
```

Step 2 Configure the VRFs.

```
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
```

Step 3 Enable CEF switching.

```
ip cef
mpls label protocol ldp
mpls ldp logging neighbor-changes
tag-switching ip default-route
!
Keyring/VPN
```

Step 4 Configure the keyring.

```
crypto keyring vpn1
  pre-shared-key address 20.1.1.1 key cisco123
  pre-shared-key address 40.1.1.2 key cisco123
crypto keyring gre
  pre-shared-key address 125.1.20.2 key cisco321
!
```

Step 5 Configure ISAKMP policy for Phase 1 negotiations.

```
crypto isakmp policy 1
 authentication pre-share
 group 2
!
crypto isakmp policy 2
 encr 3des
 authentication pre-share
```

Step 6 Configure DPD keepalives.

```
crypto isakmp keepalive 30
crypto isakmp xauth timeout 30
```

Step 7 Configure client group for local authorization.

```
crypto isakmp client configuration group ezvpn
 key cisco123
 pool hw-pool
```

Step 8 Configure ISAKMP profile for VPN sites.

```
crypto isakmp profile vpn1
```

Step 9 Configure dynamic VRF association for sites.

```
   vrf vpn1
   keyring vpn1
   match identity address 20.1.1.1 255.255.255.255
   match identity address 40.1.1.2 255.255.255.255
```

Step 10 Configure ISAKMP profile for VPN clients.

```
crypto isakmp profile vpn1-ez
```

Step 11 Configure dynamic VRF association.

```
   vrf vpn1
   match identity group ezvpn
```

Step 12 Configure XAUTH, group authorization, and mode-config.

```
   client authentication list localist
   isakmp authorization list localist
   client configuration address respond
```

Step 13 Configure ISAKMP profile for PE-PE tunnel.

```
crypto isakmp profile gre
   keyring gre
   match identity address 125.1.20.2 255.255.255.255
```

Step 14 Configure the transform set.

```
crypto ipsec transform-set tset1 esp-3des esp-sha-hmac
crypto ipsec transform-set tset2 esp-3des esp-sha-hmac
 mode transport
```

Step 15 Configure IPSec profile for PE-PE GRE tunnel.

```
crypto ipsec profile gre1
 set transform-set tset2
 set isakmp-profile gre
!
crypto dynamic-map dyna 1
 set security-association idle-time 3600
 set transform-set tset1
```

Step 16 Configure ISAKMP client profile reference.

```
 set isakmp-profile vpn1-ez
```

Step 17 Configure client RRI.

```
 reverse-route
```

Step 18 Configure static map for a site.

```
crypto map vpn 10 ipsec-isakmp
 set peer 20.1.1.1
 set transform-set tset1
```

Step 19 Configure ISAKMP site profile reference.

```
 set isakmp-profile vpn1
 match address 101
```

Step 20 Configure dynamic crypto map for clients.

```
crypto map vpn 1000 ipsec-isakmp dynamic dyna
!
interface Loopback0
 ip address 99.1.1.1 255.255.255.255
```

Step 21 Configure PE-PE GRE tunnel.

```
interface Tunnel1
 ip address 11.1.1.1 255.255.255.252
```

Step 22 Turn on tag-switching.

```
 tag-switching ip
 tunnel source FastEthernet2/1.1
 tunnel destination 125.1.20.2
```

Step 23 Configure IPSec profile reference.

```
 tunnel protection ipsec profile gre1
!
interface FastEthernet2/0
 no ip address
 duplex auto
 speed auto
```

Step 24 Configure Internet-facing interface and corresponding crypto maps.

```
interface FastEthernet2/0.1
 encapsulation dot1Q 10
 ip address 30.1.1.2 255.255.255.0
 crypto map vpn
!
interface FastEthernet2/1
 no ip address
 duplex auto
 speed auto
```

Step 25 Configure interface towards IP backbone.

```
interface FastEthernet2/1.1
 encapsulation dot1Q 10
 ip address 125.1.10.2 255.255.255.0
 tag-switching ip
```

Step 26 Configure IGP used in the core.

```
router ospf 1
 log-adjacency-changes
 network 99.1.1.1 0.0.0.0 area 0
 network 125.1.10.0 0.0.0.255 area 0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor 11.1.1.2 remote-as 100
 no auto-summary
```

Step 27 Configure PE peering for VPN routes.

```
 address-family vpnv4
 neighbor 11.1.1.2 activate
 neighbor 11.1.1.2 send-community both
 no auto-summary
 exit-address-family
 !
 address-family ipv4 vrf vpn1
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
```

Step 28 Configure the pool to distribute IP addresses to VPN clients.

```
ip local pool hw-pool 192.168.1.1 192.168.1.254
ip classless
```

Step 29 Configure the global default route.

```
ip route 0.0.0.0 0.0.0.0 FastEthernet2/0.1 30.1.1.1
```

Step 30 Configure static VPN routes if not using IGP within the VPN.

```
ip route vrf vpn1 101.1.1.0 255.255.255.0 30.1.1.1 global
```

Step 31 Configure the crytpo access list.

```
access-list 101 permit ip 101.1.2.0 0.0.0.255 101.1.1.0 0.0.0.255
```

Configuring AAA Servers for Remote Clients

AAA Servers Overview

The AAA servers are RADIUS servers that are service provider-managed or customer-managed. The RADIUS servers may be Cisco ACS or Cisco Access Registrar or a customer's RADIUS server.

RADIUS provides user authentication (XAUTH) and authorization in the Unity protocol to the client and to the IPSec aggregator to enable a successfully authenticated client to use the service authorized. Using the RADIUS server also limits the amount of pre-provisioning and re-provisioning that is necessary on each client and on each IPSEC Aggregator.

For information on configuring RADIUS, see:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsecsp/scfrad.htm

Managed AAA Configuration

In a managed AAA configuration, you (the service provider) administer a RADIUS system for customer-specific user information. The customer must provide you with the names of one or more administrators who are responsible for user administration, as well as their initial user-id/passwords. After you configure the administrators, the customer can add, delete, modify, and view users without your (service provider) intervention.

Proxy AAA Configuration

In a proxy AAA configuration, the service provider performs authorization while the customer controls user authentication. Proxy AAA is the only configuration that supports two-factor authentication (token card). When a customer manages an AAA system, one or more IP addresses must be associated with the customer AAA system. In addition to IP addresses, it is necessary to configure a shared secret on both ends of the proxy (service provider and customer). The shared secret should be a well-formed password and it must be communicated.

For information on configuring shared secrets, see
http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a008007fec3.html.

Per-VRF AAA

Using the Per VRF AAA feature, Internet Service Providers (ISPs) can partition authentication, authorization, and accounting (AAA) services based on Virtual Route Forwarding (VRF). This feature permits the IPSec aggregator to communicate directly with the customer's RADIUS server, which is associated with the customer's Virtual Private Network (VPN), without having to go through a RADIUS proxy. Thus, ISPs can scale their VPN offerings more efficiently because they no longer need to proxy AAA to provide their customers with the flexibility they demand.

For information on configuring per-VRF AAA, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftvrfaaa.htm#1015329.

IPSec VPN Accounting

The IPSec VPN Accounting feature allows for a session to be accounted for by indicating the times that the session starts and stops. Additionally, session-identifying information and session-usage information are passed to the Remote Authentication Dial-In User Service (RADIUS) server using RADIUS attributes and vendor-specific attributes (VSAs).

For information on configuring IPSec VPN accounting, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_evpna.htm.

Preprovisioning to Support Unity Client

This section deals with pre-provisioning on the IPSEC Aggregator and AAA server for Unity client support as well as the provisioning needed on the client.

Note Unlike the site-to-site model, much of the information configured at the head-end is VPN-specific, not tunnel endpoint-specific.

To support Unity clients, you must obtain information on IP address pools, DNS, WINS, and other policy when signing up customers for VPN service for remote access clients. You can store this information locally on the IPSec Aggregator or in your AAA server. You can store user-specific information (for example, username and passwords) as well as any user-specific policy information (for example, session time-outs) in your AAA server; however, for scaling reasons it may make more sense to store this information in the customer's AAA server.

Note In the absence of per-group AAA support, the service provider AAA server may proxy a request to the customer AAA server.

AAA Server Preprovisioning

An ISAKMP client configuration group (or VPN group) is a group of Unity clients that share the same authentication and configuration information. The shared group information consists of the following:

- Password (if preshared keys are used)

- IP address or name of IP address pool on IPSec aggregator from which an IP address is to be assigned to client
- IP addresses of primary and secondary DNS servers
- IP addresses of primary and secondary WINS servers
- Default domain name
- Name of access control list (ACL) to be applied at client when enabling split tunneling

IPSec Aggregator Preprovisioning

On the IPSec Aggregator, you need to pre-provision the following (assuming aggressive mode and pre-shared keys):

- How to reach SP-managed AAA server (global or management VPN) and customer-managed AAA servers (per customer VPN), if any.
- Indicate whether VPN group information is local or stored in a AAA server.
- If local, the above client group information is configured on the IPSEC aggregator.
- If remote, the name of the SP-managed AAA server to be used to fetch group configuration.
- Define the (overlapping) address pools referred to in the VPN group information, if any. Address range is provided by customer and assigned by SP.
- Define the ACLs referred to in the VPN group information which are used to enforce split tunneling at the Unity client is enabled.
- Define ISAKMP profile per VPN including:
  - Matching client configuration group.
  - VRF ID.
  - If XAUTH used, the name of the SP-managed or customer-managed AAA server to be used for user authentication.
- Define IPSec tunnel mode crypto policies per VPN.
- Define dynamic crypto map per VPN (same crypto map name, different policies) including ISAKMP profile, IPSEC policy.
- Crypto map applied to Internet-facing interfaces.

Cisco Unity Client Preprovisioning

We assume client has been assigned a global IP address from local ISP and sufficient configuration for Internet Access. We assume Unity client is pre-provisioned with:

- Public IP address or hostname of IPSEC aggregator
- Pre-shared group key with IPSEC aggregator
- XAUTH (username password or token)
- IKE authentication and encryption policy
- IPSEC authentication and encryption policy

Cisco Unity Client Operation

The Unity protocol operates based on the notion of a client group. A Unity client must identify and authenticate itself by group first, and if XAUTH enabled, by user later.

The Unity protocol supports either:

- Aggressive mode and pre-shared keys
- Main mode and certificates

In terms of AAA support, you can use RADIUS servers to store client group configuration information (including the pre-shared group password in case of aggressive mode and mode-config information) as well as to authenticate users (XAUTH). RADIUS servers can only be defined globally.

Assuming use of aggressive mode and pre-shared keys, as well as use of RADIUS servers for storing client group configuration information and for user authentication, the Unity protocol operates as follows:

1. If the IKE SA negotiates use of XAUTH, the client waits for a challenge and responds.
2. The server authenticates the user, typically using the customer's AAA server via a service provider AAA proxy. Any user-specific configuration information may be downloaded at this time or downloaded separately later.
3. The client requests mode-config parameters from the server. These include IP address, IP addresses of DNS and WINS servers, default domain name and ACLs to be applied if split tunneling is enabled.
4. If configured to do so, the server fetches the mode-config parameters from the your (service provider) AAA server based on group name. The server may also need to fetch user-specific information based on user name (for example, static IP address).
5. If configured to do so, the IPsec Aggregator allocates an IP address from the pre-defined IP address pool and sets up a route to the client in the appropriate routing table (global or VRF). The server returns the above information to the client.

For more information on Unity, see http://www.cisco.com/en/US/products/sw/voicesw/ps2237/.

For more information, see the Sequence of Operations for Remote Access, see Chapter 2, “Configuring the IPSec to MPLS Service Model” in the *Cisco Network-Based IPSec VPN Solution Release 1.5 Implementation Guide*.

User Authentication

Authentication verifies users before they are allowed access to the network and network services. See *http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfathen.htm*.

The Unity protocol operates based on the notion of a client group. A Unity client must identify and authenticate itself by group first, and if XAUTH enabled, by user later.

Note VPN clients should be authenticated by XAUTH to deny unauthorized access.

VPN group information consists of the following:

- Password if pre-shared keys are used
- Interface that VPN group allowed to come in on (from 12.2(9.4)T only)

- Name of IP address pool from which an IP address is to be assigned to client
- IP addresses of primary and secondary DNS servers
- IP addresses of primary and secondary WINS servers
- Default domain name
- Name of access control list to be applied at client when split tunneling enabled

AAA Authorization

AAA authorization enables you to limit the services available to a user. When AAA authorization is enabled, the network access server uses information retrieved from the user's profile, which is located either in the local user database or on the service provider AAA server, to configure the user's session. When this is done, the user is granted access to a requested service only if the information in the user profile allows it. See:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfathor.htm

The following IPSEC-related configuration information is available upon authorization:

- Pre-shared key per Unity group or per IPSec peer
- Unity group configuration per VPN (mode-config)
- IP address
- IP address pool
- ACL for split tunneling
- ISAKMP profile
- Virtual interface profiles for virtual IPSEC interfaces (if any)

IPSec Accounting

If IPSec accounting is configured for the session an accounting start record is generated after the IKE phases are complete.

Note New accounting records are not generated during a re-key.

The accounting start record contains the following information:

- Group name
- User name
- Assigned IP address
- Interface for the connection
- Accounting list
- VRF ID
- AAA unique id
- ISAKMP Phase 1 ID information
- Status

- ACCT_REQUIRED
- START_REQUEST
- STARTED
- STOPPED
- NOT_REQUIRED

Below is an account start record generated on the router that goes to the defined AAA server.

```
*Aug 23 04:06:20.131: RADIUS(00000002): sending
*Aug 23 04:06:20.131: RADIUS(00000002): Send Accounting-Request to 100.1.1.4:1646 id 4,
len 220
*Aug 23 04:06:20.131: RADIUS:  authenticator 38 F5 EB 46 4D BE 4A 6F - 45 EB EF 7D B7 19
FB 3F
*Aug 23 04:06:20.135: RADIUS:  Acct-Session-Id     [44]  10  "00000001"
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  31
*Aug 23 04:06:20.135: RADIUS:   Cisco AVpair       [1]   25  "isakmp-group-id=cclient"
*Aug 23 04:06:20.135: RADIUS:  Framed-IP-Address   [8]   6   10.13.13.1
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  20
*Aug 23 04:06:20.135: RADIUS:   Cisco AVpair       [1]   14  "vrf-id=cisco"
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  35
*Aug 23 04:06:20.135: RADIUS:   Cisco AVpair       [1]   29  "isakmp-initator-ip=11.1.2.2"
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  36
*Aug 23 04:06:20.135: RADIUS:   Cisco AVpair       [1]   30  "connect-progress=No
Progress"
*Aug 23 04:06:20.135: RADIUS:  User-Name           [1]   13  "joe@cclient"
*Aug 23 04:06:20.135: RADIUS:  Acct-Status-Type    [40]  6   Start                     [1]
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  25
*Aug 23 04:06:20.135: RADIUS:   cisco-nas-port     [2]   19  "FastEthernet0/0.1"
*Aug 23 04:06:20.135: RADIUS:  NAS-Port            [5]   6   0
*Aug 23 04:06:20.135: RADIUS:  NAS-IP-Address      [4]   6   100.1.1.147
*Aug 23 04:06:20.135: RADIUS:  Acct-Delay-Time     [41]  6   0
*Aug 23 04:06:20.139: RADIUS: Received from id 21645/4 100.1.1.4:1646,
Accounting-response, len 20
*Aug 23 04:06:20.139: RADIUS:  authenticator B7 E3 D0 F5 61 9A 89 D8 - 99 A6 8A 8A 98 79
9D 5D
```

Accounting Stop

An accounting stop packet is generated when there are no flows (IPSec SA pairs) being protected to an IPSec Peer.

Accounting stop records contain the following information

- Packets out
- Packets in
- Octets out
- Octets in
- Gigawords in
- Gigawords out

Below is an account start record generated on the router that is sent to the defined AAA server.

```
*Aug 23 04:20:16.519: RADIUS(00000003): Using existing nas_port 0
*Aug 23 04:20:16.519: RADIUS(00000003): Config NAS IP: 100.1.1.147
```

```
*Aug 23 04:20:16.519: RADIUS(00000003): sending
*Aug 23 04:20:16.519: RADIUS(00000003): Send Accounting-Request to 100.1.1.4:1646 id 19,
len 238
*Aug 23 04:20:16.519: RADIUS:  authenticator 82 65 5B 42 F0 3F 17 C3 - 23 F3 4C 35 A2 8A
3E E6
*Aug 23 04:20:16.519: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco       [26]  20
*Aug 23 04:20:16.519: RADIUS:   Cisco AVpair       [1]   14  "vrf-id=cisco"
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco       [26]  35
*Aug 23 04:20:16.519: RADIUS:   Cisco AVpair       [1]   29  "isakmp-initator-ip=11.1.1.2"
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco       [26]  36
*Aug 23 04:20:16.519: RADIUS:   Cisco AVpair       [1]   30  "connect-progress=No
Progress"
*Aug 23 04:20:16.519: RADIUS:  Acct-Session-Time   [46]  6   709
*Aug 23 04:20:16.519: RADIUS:  Acct-Input-Octets   [42]  6   152608
*Aug 23 04:20:16.519: RADIUS:  Acct-Output-Octets  [43]  6   152608
*Aug 23 04:20:16.519: RADIUS:  Acct-Input-Packets  [47]  6   1004
*Aug 23 04:20:16.519: RADIUS:  Acct-Output-Packets [48]  6   1004
*Apr 23 04:20:16.519: RADIUS:  Acct-Input-Giga-Word[52]  6   0
*Apr 23 04:20:16.519: RADIUS:  Acct-Output-Giga-Wor[53]  6   0
*Aug 23 04:20:16.519: RADIUS:  Acct-Terminate-Cause[49]  6   none                        [0]
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco       [26]  32
*Aug 23 04:20:16.519: RADIUS:   Cisco AVpair       [1]   26  "disc-cause-ext=No Reason"
*Aug 23 04:20:16.519: RADIUS:  Acct-Status-Type    [40]  6   Stop                        [2]
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco       [26]  25
*Aug 23 04:20:16.519: RADIUS:   cisco-nas-port     [2]   19  "FastEthernet0/0.1"
*Aug 23 04:20:16.519: RADIUS:  NAS-Port            [5]   6   0
*Aug 23 04:20:16.519: RADIUS:  NAS-IP-Address      [4]   6   100.1.1.147
*Aug 23 04:20:16.519: RADIUS:  Acct-Delay-Time     [41]  6   0
*Aug 23 04:20:16.523: RADIUS: Received from id 21645/19 100.1.1.4:1646,
Accounting-response, len 20
*Aug 23 04:20:16.523: RADIUS:  authenticator F1 CA C1 28 CE A0 26 C9 - 3E 22 C9 DA EA B8
22 A0
```

Accounting Updates

You can enable periodic interim accounting records to be sent to the accounting server s using the **aaa accounting update** command. For more information on this command, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122tcr/122tsr/faaacr/sftacct.htm#1041103.

Below is a sample accounting update record:

```
7200-UUT#
*Aug 23 21:46:05.263: RADIUS(00000004): Using existing nas_port 0
*Aug 23 21:46:05.263: RADIUS(00000004): Config NAS IP: 100.1.1.147
*Aug 23 21:46:05.263: RADIUS(00000004): sending
*Aug 23 21:46:05.263: RADIUS(00000004): Send Accounting-Request to 100.1.1.4:1646 id 22,
len 200
*Aug 23 21:46:05.263: RADIUS:  authenticator 30 FA 48 86 8E 43 8E 4B - F9 09 71 04 4A F1
52 25
*Aug 23 21:46:05.263: RADIUS:  Acct-Session-Id     [44]  10  "00000003"
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco       [26]  20
*Aug 23 21:46:05.263: RADIUS:   Cisco AVpair       [1]   14  "vrf-id=cisco"
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco       [26]  35
*Aug 23 21:46:05.263: RADIUS:   Cisco AVpair       [1]   29  "isakmp-initator-ip=11.1.1.2"
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco       [26]  36
*Aug 23 21:46:05.263: RADIUS:   Cisco AVpair       [1]   30  "connect-progress=No
Progress"
*Aug 23 21:46:05.263: RADIUS:  Acct-Session-Time   [46]  6   109
*Aug 23 21:46:05.263: RADIUS:  Acct-Input-Octets   [42]  6   608
```

```
*Aug 23 21:46:05.263: RADIUS:  Acct-Output-Octets  [43]  6   608
*Aug 23 21:46:05.263: RADIUS:  Acct-Input-Packets  [47]  6   4
*Aug 23 21:46:05.263: RADIUS:  Acct-Output-Packets [48]  6   4
*Aug 23 21:46:05.263: RADIUS:  Acct-Status-Type    [40]  6   Watchdog                   [3]
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco       [26]  25
*Aug 23 21:46:05.263: RADIUS:   cisco-nas-port     [2]   19  "FastEthernet0/0.1"
*Aug 23 21:46:05.263: RADIUS:  NAS-Port            [5]   6   0
*Aug 23 21:46:05.263: RADIUS:  NAS-IP-Address      [4]   6   100.1.1.147
*Aug 23 21:46:05.263: RADIUS:  Acct-Delay-Time     [41]  6   0
*Aug 23 21:46:05.267: RADIUS: Received from id 21645/22 100.1.1.4:1646,
Accounting-response, len 20
*Aug 23 21:46:05.267: RADIUS:  authenticator 51 6B BB 27 A4 F5 D7 61 - A7 03 73 D3 0A AC
1C
```

Sample Accounting Configuration:

```
aaa new-model
!
!
aaa authentication login cisco-client group RADIUS
aaa authorization network cisco-client group RADIUS
aaa accounting network acc start-stop broadcast group RADIUS
aaa session-id common

crypto isakmp profile cisco
vrf cisco
match identity group cclient
client authentication list cisco-client
isakmp authorization list cisco-client
client configuration address respond
accounting acc
!
crypto dynamic-map dynamic 1
set transform-set aswan
 set isakmp-profile cisco
 reverse-route
!
RADIUS-server host 100.1.1.4 auth-port 1645 acct-port 1646
RADIUS-server key nsite
```

Using RADIUS for Network-Based IPSec

The Cisco network-based IPSec VPN solution release 1.5 supports RADIUS-based authentication and authorization for remote access clients.

During authorization of a remote access client, the following attributes can be downloaded from RADIUS:

```
cisco-avpair = "ipsec:key-exchange=ike"
cisco-avpair = "ipsec:tunnel-password=cisco123"
cisco-avpair = "ipsec:addr-pool=mypool"
cisco-avpair = "ipsec:default-domain=cisco.com"
cisco-avpair = "ipsec:dns-servers=1.1.1.9"
cisco-avpair = "ipsec:wins-servers=3.3.3.9"
cisco-avpair = "ipsec:access-restrict=ATM5/0.101"
```

RADIUS Configuration Sample

The following is a sample user and group configuration for remote VPN clients from Cisco Access Registrar.

User configuration (no attributes):

```
[ //localhost/RADIUS/UserLists/Default/joe-coke ]
 Name = joe-coke
 Description =
 Password = <encrypted>
 AllowNullPassword = FALSE
 Enabled = TRUE
 Group~ =
 BaseProfile~ =
 AuthenticationScript~ =
 AuthorizationScript~ =
 UserDefined1 =

[ //localhost/RADIUS/UserLists/Default/group1 ]
 Name = group1
 Description =
 Password = <encrypted>  (would be "cisco")
 AllowNullPassword = FALSE
 Enabled = TRUE
 Group~ =
 BaseProfile~ = group1profile
 AuthenticationScript~ =
 AuthorizationScript~ =
 UserDefined1 =

Define the group attributes such as pre-shared key, IP address pool name, etc. using Cisco
AV-pairs:
[ //localhost/RADIUS/Profiles/group1profile/Attributes ]
 cisco-avpair = ipsec:key-exchange=ike
 cisco-avpair = ipsec:tunnel-password=cisco123
 cisco-avpair = ipsec:addr-pool=pool1
 Service-Type = Outbound
```

Server Load Balancing for VPN Clients

The Cisco IOS server load balancing (SLB) feature is an IOS-based solution that provides IP server load balancing. Using the IOS SLB feature, you can define a virtual server that represents a group of real servers in a cluster of network servers known as a server farm. In this environment, the clients connect to the IP address of the virtual server. When a client initiates a connection to the virtual server, the IOS SLB function chooses a real server for the connection based on a configured load-balancing algorithm.

For more information on server load balancing, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e9/iosslb9e.htm#2711438.

In the Cisco network-based IPSec VPN solution release 1.5, server load balancing is necessary to distribute a large number of IPSec tunnels over multiple IOS devices.

A Cisco NPE-400 with VAM can accommodate up to 1500 clients or layer 2 tunnels. The Cisco network-based IPSec VPN solution release 1.5 can be scaled up using multiple Cisco 7200 routers stacked behind a load-balancer.

Below is a sample configuration for server load balancing that uses a Cisco Catalyst 6500 switch with the SLB feature to distribute the client tunnels. It also provides related configurations for two Cisco 7200 routers used in the configuration.

```
ip slb probe IPSEC ping << ping will be used to determine availability of 7200

address 220.1.1.1 << Loopback address on 7200; this address is the crypto endpoint
address.

interval 10

faildetect 30

!
ip slb serverfarm IPSEC

failaction purge
```

If any server (7200) fails, purge the connection from database.

```
probe IPSEC
```

This is a reference to probe method defined above.

```
!
real 192.168.1.1
```

The real server address.

```
weight 1
```

You can change the weight to divide IPSec tunnels unequally.

```
maxconns 4000
```

This is the maximum connections to this server.

```
faildetect numconns 255

inservice

!
real 192.168.2.1

weight 1

maxconns 3200

inservice

!

ip slb vserver ESP

virtual 220.1.1.1 esp
```

This is the virtual server address.

```
serverfarm IPSEC

sticky 3600 group 1
```

The sticky group is defined to connect IPSec, IKE, and NAT-transparency together.

```
inservice
!

ip slb vserver IKE

virtual 220.1.1.1 udp isakmp

serverfarm IPSEC

sticky 3600 group 1

inservice
!

ip slb vserver NAT-T

virtual 220.1.1.1 udp 4500

serverfarm IPSEC

sticky 3600 group 1

inservice

!
interface FastEthernet4/2
```

This is the uplink to the Internet gateway.

```
ip address 212.1.1.1 255.255.255.0

duplex full

speed 100
!
interface FastEthernet4/3
```

This is the connection to the first Cisco 7200 router.

```
ip address 192.168.1.2 255.255.255.0

duplex full

speed 100

!
```

Below is the connection to the second Cisco 7200 router.

```
interface FastEthernet4/4 << Connection to 2nd 7200

ip address 192.168.2.2 255.255.255.0

duplex full

speed 100

!
```

First Server is Cisco 7200 series router.

```
hostname EUROPA-7200

!
```

Make sure you define TDP ID.

```
tag-switching tdp router-id Loopback0 <<

!
```

Loopback 1 address is used.

```
crypto map crypmap local-address Loopback1 <<

interface Loopback0
```

Address is different on both Cisco 7200 routers.

```
ip address 101.1.1.9 255.255.255.255
!
interface Loopback1
```

Address is the same as virtual address defined on SLB.

```
ip address 220.1.1.1 255.255.255.255

!
interface FastEthernet0/0
```

Private or internal address.

```
ip address 192.168.1.1 255.255.255.0
```

```
no ip unreachables

duplex full

speed 100

crypto map crypmap
```

Second Server is Cisco 7200 series router.

```
hostname EUROPA-7200-2

!

tag-switching tdp router-id Loopback0

!
crypto map crypmap local-address Loopback1

!
interface Loopback0

ip address 101.1.1.44 255.255.255.255

!

interface Loopback1

ip address 220.1.1.1 255.255.255.255

!

interface FastEthernet0/0

ip address 192.168.2.1 255.255.255.0

no ip unreachables

duplex full

speed 100

crypto map crypmap
```

Upgrading to VRF-Aware IPSec

Cisco IOS Release 12.2(15)T introduces the VRF-Aware IPSec feature for IP Security (IPSec) tunnel mapping to Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). You can use this feature to map IPSec tunnels to Virtual Routing and Forwarding (VRF) instances using a single public-facing address.

For more information on VRF-Aware IPSec, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_vrfip.htm#wp1027129.

You must make minor configuration changes in order for the VRF-Aware IPSec feature to work in legacy IPSec configurations.

This appendix provides a sample legacy IPSec configuration and an upgraded IPSec configuration with VRF-Aware IPSec. Additionally, this appendix provides an appropriate debug session.

Sample Legacy Configuration

```
7200-UUT#show config
Using 5627 out of 129016 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 7200-UUT
!
boot system flash disk0:c7200-jk9o3s-mz.122-13.T1
logging queue-limit 100
enable password lab
!
aaa new-model
!
aaa authentication login cisco-client group radius
aaa authentication login juniper-client group radius
aaa authorization network cisco-client group radius
aaa authorization network juniper-client group radius
aaa accounting network acc start-stop broadcast group radius
aaa session-id common
ip subnet-zero
!
no ip domain lookup
!
```

```
ip vrf cisco
 rd 100:100
 route-target export 100:100
 route-target import 100:100
!
ip vrf juniper
 rd 200:200
 route-target export 200:200
 route-target import 200:200
!
ip cef
mpls label protocol ldp
mpls ldp logging neighbor-changes
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp policy 2
 authentication pre-share
crypto isakmp key bridge address 11.1.1.2 no-xauth
crypto isakmp key last address 12.1.1.2 no-xauth
crypto isakmp nat keepalive 200
crypto isakmp xauth timeout 90
!
crypto ipsec transform-set aswan esp-3des esp-sha-hmac
!
crypto dynamic-map dynamic 1
 set transform-set aswan
 reverse-route
crypto dynamic-map dynamic 2
 set transform-set aswan
 reverse-route
!
crypto map vpn client authentication list cisco-client
crypto map vpn isakmp authorization list cisco-client
crypto map vpn client configuration address respond
crypto map vpn 1 ipsec-isakmp dynamic dynamic
crypto map vpn 2 ipsec-isakmp
 set peer 11.1.1.2
 set transform-set aswan
 match address 100
 reverse-route
!
crypto map jvpn client authentication list juniper-client
crypto map jvpn isakmp authorization list juniper-client
crypto map jvpn client configuration address respond
crypto map jvpn 1 ipsec-isakmp
 set peer 12.1.1.2
 set transform-set aswan
 match address 110
 reverse-route
crypto map jvpn 2 ipsec-isakmp dynamic dynamic
!
xsm
xsm vdm
xsm edm
!
voice call carrier capacity active!
!
no voice hpi capture buffer
no voice hpi capture destination
!
```

```
mta receive maximum-recipients 0
!
controller ISA 1/1
!
interface Loopback0
 ip address 200.1.1.1 255.255.255.255
 no ip mroute-cache
!
interface Loopback12
 ip vrf forwarding cisco
 ip address 6.6.6.6 255.255.255.255
!
interface Loopback100
 no ip address
!
interface Loopback501
 ip vrf forwarding juniper
 ip address 3.3.3.3 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 duplex full
 no cdp enable
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding cisco
 ip address 20.1.1.1 255.255.255.0
 crypto map vpn
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip vrf forwarding juniper
 ip address 20.2.2.1 255.255.255.0
 crypto map jvpn
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip address 20.3.3.1 255.255.255.0
!
interface ATM4/0
 no ip address
 no atm ilmi-keepalive
!
interface ATM4/0.1 point-to-point
 ip address 172.16.100.1 255.255.255.0
 pvc 1/101
  broadcast
  encapsulation aal5snap
 !
 tag-switching ip
!
interface FastEthernet5/0
 ip address 100.1.1.147 255.255.255.0
 no ip mroute-cache
 duplex full
 no cdp enable
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex half
!
router bgp 100
```

```
 no synchronization
 bgp log-neighbor-changes
 neighbor 172.16.100.2 remote-as 200
 no auto-summary
 !
 address-family vpnv4
 neighbor 172.16.100.2 activate
 neighbor 172.16.100.2 send-community extended
 no auto-summary
 exit-address-family
 !
 address-family ipv4 vrf juniper
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf cisco
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
!
ip local pool pool1 10.13.13.1 10.13.13.13
ip local pool pool2 10.13.13.1 10.13.13.13 group jclient
ip classless
ip route 11.1.1.2 255.255.255.255 FastEthernet0/0.1
ip route 11.1.2.2 255.255.255.255 FastEthernet0/0.1
ip route 12.1.1.2 255.255.255.255 FastEthernet0/0.2
ip route 12.1.2.2 255.255.255.255 FastEthernet0/0.2
ip route vrf cisco 11.1.1.2 255.255.255.255 20.1.1.2
ip route vrf cisco 11.1.2.2 255.255.255.255 20.1.1.2
ip route vrf juniper 12.1.1.2 255.255.255.255 20.2.2.2
ip route vrf juniper 12.1.2.2 255.255.255.255 20.2.2.2
no ip http server
no ip http secure-server
!
!
ip radius source-interface FastEthernet5/0
!
access-list 100 permit ip 172.18.200.0 0.0.0.255 10.1.15.0 0.0.0.255
access-list 110 permit ip 195.1.1.0 0.0.0.255 10.1.1.0 0.0.0.255
!
!
radius-server attribute 44 include-in-access-req
radius-server host 100.1.1.4 auth-port 1645 acct-port 1646
radius-server key nsite
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
 shutdown
!
!
line con 0
```

```
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password lab
line vty 5 15
!
!
end
```

Upgraded Configuration with VRF-Aware IPSec

The upgraded configuration is shown below.

Note Changes to the sample legacy configuration are noted within the configuration.

Note You must add a keyring for every remote peer within the VRF. Do not remove the existing crypto isakmp keys.

```
New Configuration:

Building configuration...

Current configuration : 5599 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 7200-UUT
!
```

Note the upgrade to Cisco IOS Release 12.2(15)T.

```
boot system flash disk0:c7200-jk9s-mz.122-15.T
logging queue-limit 100
enable password lab
!
aaa new-model
!
!
aaa authentication login cisco-client group radius
aaa authentication login juniper-client group radius
aaa authorization network cisco-client group radius
aaa authorization network juniper-client group radius
aaa accounting network acc start-stop broadcast group radius
aaa session-id common
ip subnet-zero
!
!
no ip domain lookup
!
ip vrf cisco
 rd 100:100
```

```
 route-target export 100:100
 route-target import 100:100
!
ip vrf juniper
 rd 200:200
 route-target export 200:200
 route-target import 200:200
!
ip cef
mpls label protocol ldp
mpls ldp logging neighbor-changes
!
!
```

Below are the necessary upgrade commands. The **crypto keyring** command defines a crypto keyring to be used during Internet Key Exchange (IKE) authentication. The **pre-shared-key** command defines a preshared key to be used for IKE authentication.

```
crypto keyring cisco-peer vrf cisco
  pre-shared-key address 11.1.1.2 key bridge
crypto keyring juniper-peer vrf juniper
  pre-shared-key address 12.1.1.2 key last
```

This ends the necessary upgrade commands.

```
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp policy 2
 authentication pre-share
crypto isakmp key bridge address 11.1.1.2 no-xauth
crypto isakmp key last address 12.1.1.2 no-xauth
crypto isakmp nat keepalive 200
crypto isakmp xauth timeout 90
!
!
crypto ipsec transform-set aswan esp-3des esp-sha-hmac
!
crypto dynamic-map dynamic 1
 set transform-set aswan
 reverse-route
crypto dynamic-map dynamic 2
 set transform-set aswan
 reverse-route
!
!
crypto map vpn client authentication list cisco-client
crypto map vpn isakmp authorization list cisco-client
crypto map vpn client configuration address respond
crypto map vpn 1 ipsec-isakmp dynamic dynamic
crypto map vpn 2 ipsec-isakmp
 set peer 11.1.1.2
 set transform-set aswan
 match address 100
 reverse-route
!
crypto map jvpn client authentication list juniper-client
crypto map jvpn isakmp authorization list juniper-client
crypto map jvpn client configuration address respond
crypto map jvpn 1 ipsec-isakmp
 set peer 12.1.1.2
 set transform-set aswan
```

```
 match address 110
 reverse-route
crypto map jvpn 2 ipsec-isakmp dynamic dynamic
!
!
xsm
xsm vdm
xsm edm
!
!
voice call carrier capacity active
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
mta receive maximum-recipients 0
!
!
controller ISA 1/1
!
!
interface Loopback0
 ip address 200.1.1.1 255.255.255.255
 no ip mroute-cache
!
interface Loopback12
 ip vrf forwarding cisco
 ip address 6.6.6.6 255.255.255.255
!
interface Loopback100
 no ip address
!
interface Loopback501
 ip vrf forwarding juniper
 ip address 3.3.3.3 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 duplex full
 no cdp enable
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding cisco
 ip address 20.1.1.1 255.255.255.0
 crypto map vpn
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip vrf forwarding juniper
 ip address 20.2.2.1 255.255.255.0
 crypto map jvpn
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip address 20.3.3.1 255.255.255.0
!
interface ATM4/0
 no ip address
 no atm ilmi-keepalive
!
interface ATM4/0.1 point-to-point
```

```
 ip address 172.16.100.1 255.255.255.0
 pvc 1/101
  broadcast
  encapsulation aal5snap
 !
 tag-switching ip
!
interface FastEthernet5/0
 ip address 100.1.1.147 255.255.255.0
 no ip mroute-cache
 duplex full
 no cdp enable
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex half
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 172.16.100.2 remote-as 200
 no auto-summary
 !
 address-family vpnv4
 neighbor 172.16.100.2 activate
 neighbor 172.16.100.2 send-community extended
 no auto-summary
 exit-address-family
 !
 address-family ipv4 vrf juniper
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf cisco
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
!
ip local pool pool1 10.13.13.1 10.13.13.13
ip local pool pool2 10.13.13.1 10.13.13.13 group jclient
ip classless
ip route 11.1.1.2 255.255.255.255 FastEthernet0/0.1
ip route 11.1.2.2 255.255.255.255 FastEthernet0/0.1
ip route 12.1.1.2 255.255.255.255 FastEthernet0/0.2
ip route 12.1.2.2 255.255.255.255 FastEthernet0/0.2
ip route vrf cisco 11.1.1.2 255.255.255.255 20.1.1.2
ip route vrf cisco 11.1.2.2 255.255.255.255 20.1.1.2
ip route vrf juniper 12.1.1.2 255.255.255.255 20.2.2.2
ip route vrf juniper 12.1.2.2 255.255.255.255 20.2.2.2
no ip http server
no ip http secure-server
!
!
ip radius source-interface FastEthernet5/0
!
access-list 100 permit ip 172.18.200.0 0.0.0.255 10.1.15.0 0.0.0.255
access-list 110 permit ip 195.1.1.0 0.0.0.255 10.1.1.0 0.0.0.255
!
```

```
!
radius-server attribute 44 include-in-access-req
radius-server host 100.1.1.4 auth-port 1645 acct-port 1646
radius-server key nsite
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password lab
line vty 5 15
!
!
end
```

IPSec Debug Session

```
*Oct  9 03:50:17.727: ISAKMP (0:0): received packet from 11.1.1.2 dport 500 sport 500
cisco (N) NEW SA
*Oct  9 03:50:17.727: ISAKMP: Created a peer struct for 11.1.1.2, peer port 500
*Oct  9 03:50:17.727: ISAKMP: Locking peer struct 0x64890C84, IKE refcount 1 for
crypto_ikmp_config_initialize_sa
*Oct  9 03:50:17.727: ISAKMP (0:0): Setting client config settings 649167D0
*Oct  9 03:50:17.727: ISAKMP: local port 500, remote port 500
*Oct  9 03:50:17.727: ISAKMP: insert sa successfully sa = 64916174
*Oct  9 03:50:17.727: ISAKMP (0:5): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Oct  9 03:50:17.727: ISAKMP (0:5): Old State = IKE_READY  New State = IKE_R_MM1

*Oct  9 03:50:17.727: ISAKMP (0:5): processing SA payload. message ID = 0
*Oct  9 03:50:17.727: ISAKMP (0:5): processing vendor id payload
*Oct  9 03:50:17.727: ISAKMP (0:5): vendor ID seems Unity/DPD but major 157 mismatch
*Oct  9 03:50:17.727: ISAKMP (0:5): vendor ID is NAT-T v3
*Oct  9 03:50:17.727: ISAKMP (0:5): processing vendor id payload
*Oct  9 03:50:17.727: ISAKMP (0:5): vendor ID seems Unity/DPD but major 123 mismatch
*Oct  9 03:50:17.727: ISAKMP (0:5): vendor ID is NAT-T v2
*Oct  9 03:50:17.727: ISAKMP: Looking for a matching key for 11.1.1.2 in cisco-peer :
success
*Oct  9 03:50:17.727: ISAKMP (0:5): found peer pre-shared key matching 11.1.1.2
*Oct  9 03:50:17.727: ISAKMP (0:5) local preshared key found
*Oct  9 03:50:17.727: ISAKMP : Scanning profiles for xauth ...
*Oct  9 03:50:17.727: ISAKMP (0:5): Checking ISAKMP transform 1 against priority 1 policy
*Oct  9 03:50:17.727: ISAKMP:      encryption DES-CBC
*Oct  9 03:50:17.727: ISAKMP:      hash SHA
*Oct  9 03:50:17.727: ISAKMP:      default group 1
*Oct  9 03:50:17.727: ISAKMP:      auth pre-share
```

```
*Oct  9 03:50:17.727: ISAKMP:      life type in seconds
*Oct  9 03:50:17.727: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
*Oct  9 03:50:17.727: ISAKMP (0:5): Encryption algorithm offered does not match policy!
*Oct  9 03:50:17.727: ISAKMP (0:5): atts are not acceptable. Next payload is 0
*Oct  9 03:50:17.727: ISAKMP (0:5): Checking ISAKMP transform 1 against priority 2 policy
*Oct  9 03:50:17.727: ISAKMP:      encryption DES-CBC
*Oct  9 03:50:17.727: ISAKMP:      hash SHA
*Oct  9 03:50:17.727: ISAKMP:      default group 1
*Oct  9 03:50:17.727: ISAKMP:      auth pre-share
*Oct  9 03:50:17.727: ISAKMP:      life type in seconds
*Oct  9 03:50:17.727: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
*Oct  9 03:50:17.727: ISAKMP (0:5): atts are acceptable. Next payload is 0
*Oct  9 03:50:17.735: ISAKMP (0:5): processing vendor id payload
*Oct  9 03:50:17.735: ISAKMP (0:5): vendor ID seems Unity/DPD but major 157 mismatch
*Oct  9 03:50:17.735: ISAKMP (0:5): vendor ID is NAT-T v3
*Oct  9 03:50:17.735: ISAKMP (0:5): processing vendor id payload
*Oct  9 03:50:17.735: ISAKMP (0:5): vendor ID seems Unity/DPD but major 123 mismatch
*Oct  9 03:50:17.735: ISAKMP (0:5): vendor ID is NAT-T v2
*Oct  9 03:50:17.735: ISAKMP (0:5): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
*Oct  9 03:50:17.735: ISAKMP (0:5): Old State = IKE_R_MM1  New State = IKE_R_MM1

*Oct  9 03:50:17.735: ISAKMP (0:5): constructed NAT-T vendor-03 ID
*Oct  9 03:50:17.735: ISAKMP (0:5): sending packet to 11.1.1.2 my_port 500 peer_port 500
(R) MM_SA_SETUP
*Oct  9 03:50:17.735: ISAKMP (0:5): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
*Oct  9 03:50:17.735: ISAKMP (0:5): Old State = IKE_R_MM1  New State = IKE_R_MM2

*Oct  9 03:50:17.787: ISAKMP (0:5): received packet from 11.1.1.2 dport 500 sport 500
cisco (R) MM_SA_SETUP
*Oct  9 03:50:17.787: ISAKMP (0:5): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Oct  9 03:50:17.787: ISAKMP (0:5): Old State = IKE_R_MM2  New State = IKE_R_MM3

*Oct  9 03:50:17.787: ISAKMP (0:5): processing KE payload. message ID = 0
*Oct  9 03:50:17.795: ISAKMP (0:5): processing NONCE payload. message ID = 0
*Oct  9 03:50:17.795: ISAKMP: Looking for a matching key for 11.1.1.2 in cisco-peer :
success
*Oct  9 03:50:17.795: ISAKMP (0:5): found peer pre-shared key matching 11.1.1.2
*Oct  9 03:50:17.795: ISAKMP: Looking for a matching key for 11.1.1.2 in cisco-peer :
success
*Oct  9 03:50:17.795: ISAKMP (0:5): found peer pre-shared key matching 11.1.1.2
*Oct  9 03:50:17.795: ISAKMP (0:5): SKEYID state generated
*Oct  9 03:50:17.795: ISAKMP (0:5): processing vendor id payload
*Oct  9 03:50:17.795: ISAKMP (0:5): vendor ID is Unity
*Oct  9 03:50:17.795: ISAKMP (0:5): processing vendor id payload
*Oct  9 03:50:17.795: ISAKMP (0:5): vendor ID is DPD
*Oct  9 03:50:17.795: ISAKMP (0:5): processing vendor id payload
*Oct  9 03:50:17.795: ISAKMP (0:5): speaking to another IOS box!
*Oct  9 03:50:17.795: ISAKMP:received payload type 17
*Oct  9 03:50:17.795: ISAKMP (0:5): Detected NAT-D payload
*Oct  9 03:50:17.795: ISAKMP (0:5): NAT match MINE hash
*Oct  9 03:50:17.795: ISAKMP:received payload type 17
*Oct  9 03:50:17.795: ISAKMP (0:5): Detected NAT-D payload
*Oct  9 03:50:17.795: ISAKMP (0:5): NAT match HIS hash
*Oct  9 03:50:17.795: ISAKMP (0:5): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
*Oct  9 03:50:17.795: ISAKMP (0:5): Old State = IKE_R_MM3  New State = IKE_R_MM3

*Oct  9 03:50:17.795: ISAKMP (0:5): constructed HIS NAT-D
*Oct  9 03:50:17.795: ISAKMP (0:5): constructed MINE NAT-D
*Oct  9 03:50:17.795: ISAKMP (0:5): sending packet to 11.1.1.2 my_port 500 peer_port 500
(R) MM_KEY_EXCH
*Oct  9 03:50:17.795: ISAKMP (0:5): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
*Oct  9 03:50:17.795: ISAKMP (0:5): Old State = IKE_R_MM3  New State = IKE_R_MM4
```

```
*Oct  9 03:50:17.895: ISAKMP (0:5): received packet from 11.1.1.2 dport 500 sport 500
cisco (R) MM_KEY_EXCH
*Oct  9 03:50:17.895: ISAKMP (0:5): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Oct  9 03:50:17.895: ISAKMP (0:5): Old State = IKE_R_MM4  New State = IKE_R_MM5

*Oct  9 03:50:17.895: ISAKMP (0:5): processing ID payload. message ID = 0
*Oct  9 03:50:17.895: ISAKMP (0:5): peer matches *none* of the profiles
*Oct  9 03:50:17.895: ISAKMP (0:5): processing HASH payload. message ID = 0
*Oct  9 03:50:17.895: ISAKMP:received payload type 14
*Oct  9 03:50:17.895: ISAKMP (0:5): processing NOTIFY INITIAL_CONTACT protocol 1
        spi 0, message ID = 0, sa = 64916174
*Oct  9 03:50:17.895: ISAKMP (0:5): Process initial contact,
bring down existing phase 1 and 2 SA's with local 20.1.1.1 remote 11.1.1.2 remote port 500
*Oct  9 03:50:17.895: ISAKMP (0:5): returning IP addr to the address pool
*Oct  9 03:50:17.895: ISAKMP (0:5): SA has been authenticated with 11.1.1.2
*Oct  9 03:50:17.895: ISAKMP: Trying to insert a peer 11.1.1.2/500/cisco,  and inserted
successfully.
*Oct  9 03:50:17.895: ISAKMP (0:5): peer matches *none* of the profiles
*Oct  9 03:50:17.895: ISAKMP (0:5): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
*Oct  9 03:50:17.895: ISAKMP (0:5): Old State = IKE_R_MM5  New State = IKE_R_MM5

*Oct  9 03:50:17.895: IPSEC(key_engine): got a queue event...
*Oct  9 03:50:17.895: ISAKMP (0:5): SA is doing pre-shared key authentication using id
type ID_IPV4_ADDR
*Oct  9 03:50:17.895: ISAKMP (5): ID payload
        next-payload : 8
        type         : 1
        addr         : 20.1.1.1
        protocol     : 17
        port         : 0
        length       : 8
*Oct  9 03:50:17.895: ISAKMP (5): Total payload length: 12
*Oct  9 03:50:17.895: ISAKMP (0:5): sending packet to 11.1.1.2 my_port 500 peer_port 500
(R) MM_KEY_EXCH
*Oct  9 03:50:17.895: ISAKMP (0:5): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
*Oct  9 03:50:17.895: ISAKMP (0:5): Old State = IKE_R_MM5  New State = IKE_P1_COMPLETE

*Oct  9 03:50:17.895: ISAKMP (0:5): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
*Oct  9 03:50:17.895: ISAKMP (0:5): Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE

*Oct  9 03:50:17.939: ISAKMP (0:5): received packet from 11.1.1.2 dport 500 sport 500
cisco (R) QM_IDLE
*Oct  9 03:50:17.939: ISAKMP: set new node 792995152 to QM_IDLE
*Oct  9 03:50:17.943: ISAKMP (0:5): processing HASH payload. message ID = 792995152
*Oct  9 03:50:17.943: ISAKMP (0:5): processing SA payload. message ID = 792995152
*Oct  9 03:50:17.943: ISAKMP (0:5): Checking IPSec proposal 1
*Oct  9 03:50:17.943: ISAKMP: transform 1, ESP_3DES
*Oct  9 03:50:17.943: ISAKMP:   attributes in transform:
*Oct  9 03:50:17.943: ISAKMP:      encaps is 1
*Oct  9 03:50:17.943: ISAKMP:      SA life type in seconds
*Oct  9 03:50:17.943: ISAKMP:      SA life duration (basic) of 3600
*Oct  9 03:50:17.943: ISAKMP:      SA life type in kilobytes
*Oct  9 03:50:17.943: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
*Oct  9 03:50:17.943: ISAKMP:      authenticator is HMAC-SHA
*Oct  9 03:50:17.943: ISAKMP (0:5): atts are acceptable.
*Oct  9 03:50:17.943: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 20.1.1.1, remote= 11.1.1.2,
    local_proxy= 60.1.1.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 10.1.15.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Oct  9 03:50:17.943: IPSEC(kei_proxy): head = vpn, map->ivrf = cisco, kei->ivrf = cisco
```

```
*Oct  9 03:50:17.943: ISAKMP (0:5): processing NONCE payload. message ID = 792995152
*Oct  9 03:50:17.943: ISAKMP (0:5): processing ID payload. message ID = 792995152
*Oct  9 03:50:17.943: ISAKMP (0:5): processing ID payload. message ID = 792995152
*Oct  9 03:50:17.943: ISAKMP (0:5): asking for 1 spis from ipsec
*Oct  9 03:50:17.943: ISAKMP (0:5): Node 792995152, Input = IKE_MESG_FROM_PEER,
IKE_QM_EXCH
*Oct  9 03:50:17.943: ISAKMP (0:5): Old State = IKE_QM_READY  New State =
IKE_QM_SPI_STARVE
*Oct  9 03:50:17.943: IPSEC(key_engine): got a queue event...
*Oct  9 03:50:17.943: IPSEC(spi_response): getting spi 2126455568 for SA
        from 20.1.1.1        to 11.1.1.2        for prot 3
*Oct  9 03:50:17.943: ISAKMP: received ke message (2/1)
*Oct  9 03:50:18.195: ISAKMP (0:5): sending packet to 11.1.1.2 my_port 500 peer_port 500
(R) QM_IDLE
*Oct  9 03:50:18.195: ISAKMP (0:5): Node 792995152, Input = IKE_MESG_FROM_IPSEC,
IKE_SPI_REPLY
*Oct  9 03:50:18.195: ISAKMP (0:5): Old State = IKE_QM_SPI_STARVE  New State =
IKE_QM_R_QM2
*Oct  9 03:50:18.311: ISAKMP (0:5): received packet from 11.1.1.2 dport 500 sport 500
cisco (R) QM_IDLE
*Oct  9 03:50:18.311: ISAKMP: Locking peer struct 0x64890C84, IPSEC refcount 1 for for
stuff_ke
*Oct  9 03:50:18.311: ISAKMP (0:5): Creating IPSec SAs
*Oct  9 03:50:18.315:         inbound SA from 11.1.1.2 to 20.1.1.1 (f/i)  1/ 1
        (proxy 10.1.15.0 to 60.1.1.0)
*Oct  9 03:50:18.315:         has spi 0x7EBF2310 and conn_id 5123 and flags 2
*Oct  9 03:50:18.315:         lifetime of 3600 seconds
*Oct  9 03:50:18.315:         lifetime of 4608000 kilobytes
*Oct  9 03:50:18.315:         has client flags 0x0
*Oct  9 03:50:18.315:         outbound SA from 20.1.1.1        to 11.1.1.2        (f/i)
1/ 1 (proxy 60.1.1.0        to 10.1.15.0      )
*Oct  9 03:50:18.315:         has spi 1940656993 and conn_id 5124 and flags A
*Oct  9 03:50:18.315:         lifetime of 3600 seconds
*Oct  9 03:50:18.315:         lifetime of 4608000 kilobytes
*Oct  9 03:50:18.315:         has client flags 0x0
*Oct  9 03:50:18.315: ISAKMP (0:5): deleting node 792995152 error FALSE reason "quick mode
done (await)"
*Oct  9 03:50:18.315: ISAKMP (0:5): Node 792995152, Input = IKE_MESG_FROM_PEER,
IKE_QM_EXCH
*Oct  9 03:50:18.315: ISAKMP (0:5): Old State = IKE_QM_R_QM2  New State =
IKE_QM_PHASE2_COMPLETE
*Oct  9 03:50:18.315: IPSEC(key_engine): got a queue event...
*Oct  9 03:50:18.315: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 20.1.1.1, remote= 11.1.1.2,
    local_proxy= 60.1.1.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 10.1.15.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x7EBF2310(2126455568), conn_id= 5123, keysize= 0, flags= 0x2
*Oct  9 03:50:18.315: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 20.1.1.1, remote= 11.1.1.2,
    local_proxy= 60.1.1.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 10.1.15.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x73AC1361(1940656993), conn_id= 5124, keysize= 0, flags= 0xA
*Oct  9 03:50:18.315: IPSEC(kei_proxy): head = vpn, map->ivrf = cisco, kei->ivrf = cisco
*Oct  9 03:50:18.315: IPSEC(add mtree): src 60.1.1.0, dest 10.1.15.0, dest_port 0

*Oct  9 03:50:18.315: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.1.1.1, sa_prot= 50,
    sa_spi= 0x7EBF2310(2126455568),
    sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 5123
*Oct  9 03:50:18.315: IPSEC(create_sa): sa created,
```

```
  (sa) sa_dest= 11.1.1.2, sa_prot= 50,
    sa_spi= 0x73AC1361(1940656993),
    sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 5124
7200-UUT#


7200-UUT#sh cry isa sa
  f_vrf/i_vrf   dst             src             state       conn-id slot
  cisco/cisco   20.1.1.1        11.1.1.2        QM_IDLE           5    0
```

The following **show crypto isakmp sa** detail shows four IPSec sessions up, one remote EZVPN session and one lan-to-lan session for each VRF:

```
7200-UUT#sh cry isa sa de
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

Conn-id Local           Remote          I-VRF      Encr Hash Auth DH Lifetime Capabilities
1       20.2.2.1        12.1.1.2        juniper    des  sha  psk  1  23:46:25
2       20.1.1.1        11.1.1.2        cisco      des  sha  psk  1  23:46:35
10      20.1.1.1        11.1.2.4        cisco      3des sha       2  23:59:03 CX
5       20.2.2.1        12.1.2.2        juniper    3des sha       2  18:02:41 CX
```

A

Access VPN Provides remote access to a corporate intranet or extranet over a shared infrastructure with the same policies as a private network. Access VPNs enable users to access corporate resources whenever, wherever, and however they require. Access VPNs encompass analog, dial, ISDN, Digital Subscriber Line (DSL), mobile IP, and cable technologies to securely connect mobile users, telecommuters, or branch offices.

ACL Access Control List.

ADSL Asymmetric Digital Subscriber Line. A type of DSL supporting upstream and downstream speeds that are different.

AH Authentication Header. A security protocol that provides authentication and optional replay-detection services. AH is embedded in the data to be protected (a full IP datagram, for example). AH can be used either by itself or with Encryption Security Payload (ESP).

ATM Asynchronous Transfer Mode.

C

CAC Call Admission Control.

CE Customer Edge router. This device is typically located at the customer site and connects to the service provider network. Same as CPE.

CIC Cisco InfoCenter.

CLEC Competitive Local Exchange Carrier.

CO Central Office.

COS Class of Service. Classification of traffic that allows differentiated processing using prioritization and QOS features.

CPE Customer Premises Equipment. Same as CE, more widely used in IPsec VPNs.

CSRC Cisco Subscriber Registration Center.

D

DES Data Encryption Standard. The DES was published in 1977 by the National Bureau of Standards and is a secret key encryption scheme based on the Lucifer algorithm from IBM. The contrast of DES is public-key. Cisco uses DES in classic crypto (40-bit and 56-bit key lengths), IPsec crypto (56-bit key), and on the PIX Firewall (56-bit key).

E

Extranet VPN Links customers, suppliers, partners, or communities of interest to a corporate intranet over a shared infrastructure using dedicated connections. Businesses enjoy the same policies as a private network, including security, QoS, manageability, and reliability.

G

GRE Generic Routing Encapsulation. Tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling using GRE allows network expansion across a single-protocol backbone environment.

I

IDS Intrusion Detection System.

IKE Internet Key Exchange. A hybrid protocol that uses part Oakley and part of another protocol suite called SKEME inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. IKE is used to establish a shared security policy and authenticated keys for services (such as IPsec) that require keys. Before any IPsec traffic can be passed, each router/firewall/host must be able to verify the identity of its peer. This can be done by manually entering pre-shared keys into both hosts, by a CA service, or the forthcoming secure DNS (DNSSec). This is the protocol formerly known as ISAKMP/Oakley, and is defined in The Internet Key Exchange (IKE). A potential point of confusion is that the acronyms "ISAKMP" and "IKE" are both used in Cisco IOS software to refer to the same thing. These two items are somewhat different, as you will see in the next definition.

Intranet VPN Links corporate headquarters, remote offices, and branch offices over a shared infrastructure using dedicated connections. Businesses enjoy the same policies as a private network, including security, quality of service (QoS), manageability, and reliability.

IPAM IP Address Management.

ISAKMP Internet Security Association and Key Management Protocol. A protocol framework that defines the mechanics of implementing a key exchange protocol and negotiation of a security policy.

ISC 3.0 IP Solution Center 3.0

M

MD5 Message Digest 5. A one way hashing algorithm that produces a 128-bit hash. Both MD5 and Secure Hash Alogorithm (SHA) are variations on MD4, which is designed to strengthen the security of this hashing algorithm. SHA is more secure than MD4 and MD5. Cisco uses hashes for authentication within the IPsec framework.

O

OSS Operations Support Systems.

OSM Outsource Security/VPN Management provider.

P

PE Provider router. This device connects to one or more customer sites in the service provider network.

POP Point Of Presence or service provider center.

Q

QOS Quality of Service. Features providing prioritization, policing, congestion management and shaping of the traffic based on its classification.

S

SLA Service Level Agreement. Set of parameter values (e.g., availability) that the service provider agrees to provide to customers.

SOC Security Operations Center.

Stateful Firewall A secure method of analyzing packets that places extensive information about a data packet in a table. In order for a session to be established, information about the connection must match information stored in the table.

V

A

C

G

I

P

R

U

V

W