# Cisco Network-Based IPSec VPN Solution Release 1.5 Solution Overview and Planning Guide

May, 2003
Revised December 14, 2005

**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-3133-01

# About This Guide

This guide provides overview and provisioning information for the Cisco Network-Based IPSec VPN Release 1.5. This preface has the following main subjects:



## Document Objectives

This guide provides an overview of the Cisco network-based IPSec VPN solution Release 1.5 architectures as well as planning information. The guide references features described in Cisco IOS software configuration guides and command references. Consult those documents for additional information.

## Audience

This guide is meant for new and existing MPLS VPN service providers. It includes overview and configuration information designed to enable users to get their systems running as quickly as possible. However, it does not include extensive software configuration instructions. For more extensive software configuration information, refer to Cisco IOS configuration guides and command references. See also the documents listed under Related Documentation, page x, and For More Information, page xii.

This guide is intended primarily for the following audiences:

- Customers with technical networking background and experience
- Customers who support remote access users
- System administrators who are familiar with the fundamentals of router-based internet working, but who may not be familiar with Cisco IOS software
- System administrators who are responsible for installing and configuring internet working equipment, and who are familiar with Cisco IOS software

# Document Organization

This guide describes software installation and configuration procedures which are presented in the following chapters:

- Chapter 1, “Introduction,” describes the network-based IPSec VPN solution, solution components, and features.
- Chapter 2, “Deployment Models” describes the network-based IPSec VPN solution deployment models.
- Chapter 3, “Planning Issues and Decisions” provides general information to help you plan your implementation of the network-based IPSec VPN solution.
- Chapter 4, “Planning for IPSec Remote Access” provides information to help you plan for configuring remote access for the network-based IPSec VPN solution.
- Chapter 5, “Planning for IPSec Site-to-Site Access” provides information to help you plan for configuring site-to-site access for network-based IPSec VPN solution.
- Index

# Document Conventions

This publication uses the following conventions to display instructions and information.

Interactive examples showing prompts `AS5800(config-line)#` are used in procedures to show prompts for entering a command, and the result.

**Note** Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

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

**Tip** Means the following information will help you solve a problem.

## Safety Warnings

Safety warnings appear throughout this publication in procedures that, if performed incorrectly, may harm you. A warning symbol precedes each warning statement. To see translations of safety warnings, refer to the *Regulatory Compliance and Safety Information* document that shipped with your system.

**Warning** **This warning symbol means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

**Waarschuwing** Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het document Regulatory Compliance and Safety Information (Informatie over naleving van veiligheids- en andere voorschriften) raadplegen dat bij dit toestel is ingesloten.

**Varoitus** Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. Tässä julkaisussa esiintyvien varoitusten käännökset löydät laitteen mukana olevasta *Regulatory Compliance and Safety Information* -kirjasesta (määräysten noudattaminen ja tietoa turvallisuudesta).

**Attention** Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions d'avertissements figurant dans cette publication, consultez le document *Regulatory Compliance and Safety Information* (Conformité aux règlements et consignes de sécurité) qui aCisco.commpagne cet appareil.

**Warnung** Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Dokument *Regulatory Compliance and Safety Information* (Informationen zu behördlichen Vorschriften und Sicherheit), das zusammen mit diesem Gerät geliefert wurde.

**Avvertenza** Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, oCisco.comrre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nel documento *Regulatory Compliance and Safety Information* (Conformità alle norme e informazioni sulla sicurezza) che aCisco.commpagna questo dispositivo.

**Advarsel** Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du vare oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i dokumentet *Regulatory Compliance and Safety Information* (Overholdelse av forskrifter og sikkerhetsinformasjon) som ble levert med denne enheten.

**Aviso** Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. Para ver as traduções dos avisos que constam desta publicação, consulte o documento *Regulatory Compliance and Safety Information* (Informação de Segurança e Disposições Reguladoras) que acompanha este dispositivo.

**¡Advertencia!** Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. Para ver una traducción de las advertencias que aparecen en esta publicación, consultar el documento titulado *Regulatory Compliance and Safety Information* (Información sobre seguridad y conformidad con las disposiciones reglamentarias) que se acompaña con este dispositivo.

**Varning!** Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. Se förklaringar av de varningar som förkommer i denna publikation i dokumentet *Regulatory Compliance and Safety Information* (Efterrättelse av föreskrifter och säkerhetsinformation), vilket medföljer denna anordning.

# Related Documentation

## Cisco Network-Based IPSec VPN Solution 1.5 Documentation Set

In addition to this guide, the Cisco network-based IPSec VPN solution Release 1.5 documentation set includes:

- *Cisco Network-Based IPSec VPN Release 1.5Operation, Maintenance, and Troubleshooting Guide*
  http://www.cisco.com/univercd/cc/td/doc/product/vpn/solution/aswan15/omt/index.htm
- *Cisco Network-Based IPSec VPN Release 1.5 Solution Implementation Guide*
  http://www.cisco.com/univercd/cc/td/doc/product/vpn/solution/aswan15/sig/index.htm

- *Release Notes for the Cisco Network-Based IPSec VPN Release 1.5*

  http://www.cisco.com/univercd/cc/td/doc/product/vpn/solution/aswan15/aswnrn15.htm

# Reference Documentation

The following platform specific hardware component reference documentation is available on Cisco.com or the Cisco Universal CD.

## MPLS VPNSC References

The following Cisco MPLS VPN Solution Center reference documentation is available on Cisco.com or the Cisco Universal Documentation CD.

#### MPLS VPN Solution Center Documentation

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/vpnsc/mpls/index.htm

## Network Management References

Cisco network management reference documentation is available on Cisco.com or Cisco's Universal Documentation CD.

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

## Aggregation and PE Routers

#### Cisco 7200 Series Routers

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

## Customer Premises Equipment

For information on VPN 3002 Hardware Clients, go to the following url:

http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3002/index.htm

For information on Cisco PIX with EzVPN Client, go to the following url:

http://www.cisco.com/en/US/products/sw/cscowork/ps3992/index.html

For information on Cisco 8xx Series Routers, go to the following url:

http://www.cisco.com/en/US/products/hw/routers/ps380/index.html.

For information on Cisco 17xx Series Routers, go to the following url:

http://www.cisco.com/en/US/products/hw/routers/ps221/index.html.

For information on Cisco 26xx Series Routers, go to the following url:

http://www.cisco.com/en/US/products/hw/routers/ps259/index.html

For information on Cisco 36xx Series Routers, go to the following url:

http://www.cisco.com/en/US/products/hw/routers/ps274/index.html dial access, virtual private networks (VPNs), and multiprotocol data routing

For information on Cisco 72xx Series Routers, go to the following url:

http://www.cisco.com/en/US/products/hw/routers/ps341/index.html

## Cisco IOS Software

The following Cisco IOS reference documentation is available on Cisco.com or the Cisco Universal Documentation CD.

For information on Cisco IOS Software Configuration, go to the following url:

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

For information on MPLS VPN Overviews and Configurations, go to the following url:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/switch_c/xcprt4/index.htm

## Internetworking Technology Overviews

The following internetworking technology reference documentation is available on Cisco.com or the Cisco Universal Documentation CD.

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

For information on Virtual Private Networks Overview, go to the following url:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/vpn.htm

For information on Digital Subscriber Line Technology, go to the following url:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/adsl.htm

For information on Access VPDN Dial-in Using L2TP, go to the following url:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/l2tp/index.htm

For information on Access VPN Solutions Using Tunneling Technology, go to the following url:

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

For information on Tag Switching, go to the following url:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/tagswtch.htm

For information on Cisco Secure VPN Client Solutions Guide, go to the following url:, go to the following url:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csvpnc/csvpnsg/index.htm

For information on Introduction to WAN Technologies, go to the following url:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introwan.htm

For information on Internetwork Troubleshooting Guides, go to the following url:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/index.htm

For information on Internetworking Terms and Acronyms, go to the following url:

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

# For More Information

For information on MPLS, use the following resources:

- MPLS Resource Center (http://www.mplsrc.com/)

- *MPLS: Technologies and Applications* by Bruce S. Davie and Yakov Rekhter
- *Switching in IP Networks: IP Switching, Tag Switching, and Related Technologies* by Bruce S. Davie, Paul Dooley, and Yakov Rekhter
- *CSM Brochure,* Literature Number 953088
- *New World Operations Advertorial,* Literature Number 952807
- *CSM Advertorial,* Literature Number 952937
- *CSM Demo CD-ROM,* Literature Number 952319

# 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 calling, 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


# Introduction to the Cisco Network-Based IPSec VPN Solution Release 1.5

This chapter introduces the Cisco Network-Based IPSec VPN Solution Release 1.5 and includes the following sections:



## Network-Based IPSec VPN Solution Description

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 off-net locations to a customer's corporate VPN extranet or intranet.

The Cisco network-based IPSec VPN solution Release 1.5 leverages the Cisco 7200 series router as an IPSec aggregator/provider edge (PE) router to seamlessly integrate IPSec VPNs into MPLS-based VPNs or into VRFs to be sent out from other interfaces on the same VRFs.

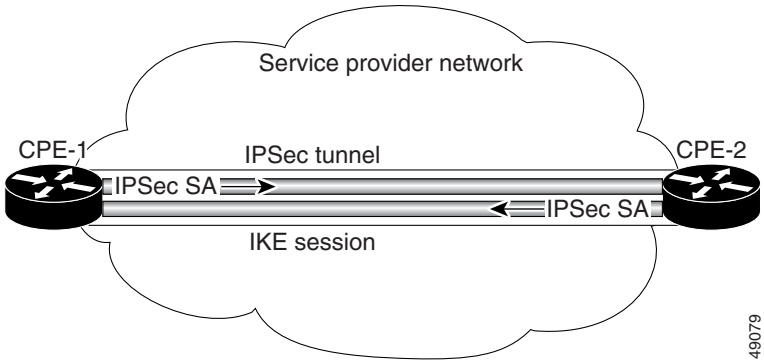
IPSec sessions can be terminated at the edge of the MPLS backbone and each of these can be mapped into their respective VPNs. The mapping configuration depends on the deployment model.

### Technology Overview: IPSec

For IPSec standards and specifications, as well as RFCs, see:
http://www.cisco.com/pcgi-bin/Support/browse/psp_view.pl?p=Internetworking:IPSec&s=Overview

IPSec provides secure tunnels between two peers, such as two routers. You define which packets are considered sensitive and should be sent through secure tunnels, and you define the parameters to use to protect these sensitive packets by specifying tunnel characteristics. When the IPSec peer encounters a sensitive packet, it sets up a secure tunnel and sends the packet through the tunnel to the remote peer. Figure 1-1 shows a high-level view of IPSec deployment across an IP network.

*Figure 1-1 IPSec Deployed Across a Public IP Network*




IPSec tunnels are sets of security associations (SAs) that are established between two IPSec peers. The security associations define which protocols and algorithms should be applied to sensitive packets, and also specify the keying material to be used by the two peers. Security associations are unidirectional and are established per security protocol [Authentication header (AH) or encapsulating security payload protocols (ESP)].

With IPSec, you define the traffic to be protected between two IPSec peers by configuring access lists and applying these access lists to interfaces by way of crypto map sets (a crypto map uses an access list to determine whether a packet needs to be passed through IPSec). Therefore, traffic can be selected based on source and destination address, and optionally Layer 4 protocol, and port. The access lists used for IPSec only determine which traffic should be protected by IPSec, not which traffic should be blocked or permitted through the interface. Separate access lists define blocking and permitting at the interface.

A crypto map set can contain multiple entries, each with a different access list. The crypto map entries are searched in order—the router attempts to match the packet to the access list specified in that entry. It is good practice to place the most important crypto map entries at the top of the list.

When a packet matches a permit entry in a particular access list, and the corresponding crypto map entry is tagged as cisco, then Cisco Encryption Technology (CET) is triggered, and connections are established if necessary. If the crypto map entry is tagged as ipsec-isakmp, IPSec is triggered.

If no security association that IPSec can use exists to protect this traffic to the peer, IPSec uses the Internet Key Exchange protocol (IKE) to negotiate with the remote peer to set up the necessary IPSec security associations on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry.

If the crypto map entry is tagged as ipsec-manual, IPSec is triggered. If no security association exists that IPSec can use to protect this traffic to the peer, the traffic is dropped. In this case, the security associations are installed through the configuration, without the intervention of IKE. If the security associations did not exist, IPSec does not have all of the necessary pieces configured.

When established, the set of security associations (outbound, to the peer) is then applied to the triggering packet as well as to subsequent applicable packets as those packets exit the router. Applicable packets are packets that match the same access list criteria that the original packet matched. For example, all applicable packets could be encrypted before being forwarded to the remote peer. The corresponding inbound security associations are used when processing the incoming traffic from that peer.

If IKE is used to establish the security associations, the security associations will have lifetimes set so that they periodically expire and require renegotiation, thus providing an additional level of security.

Multiple IPSec tunnels can exist between two peers to secure different data streams, with each tunnel using a separate set of security associations. For example, some data streams might be just authenticated while other data streams must both be encrypted and authenticated.

Access lists associated with IPSec crypto map entries also represent the traffic the router requires to be protected by IPSec. Inbound traffic is processed against the crypto map entries—if an unprotected packet matches a permit entry in a particular access list associated with an IPSec crypto map entry, that packet is dropped because it was not sent as an IPSec-protected packet.

Crypto map entries also include *transform sets*. A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPSec protected traffic. During the IPSec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

### Security

IPSec implements network layer encryption and authentication, embedding end-to-end security within the network architecture. The advantage to this is that individual applications do not need to be modified to take advantage of strong security. All packets routed through the network are automatically secured.

## IPSec Scope

IPSec provides three main facilities:

- An authentication-only function, referred to as Authentication Header (AH)
- A combined authentication and encryption function called Encapsulating Security Payload (ESP)
- A key exchange function. For virtual private networks, both authentication and encryption are generally desired, because it is important both to a) assure that unauthorized users do not penetrate the virtual private network, and b) assure that eavesdroppers on the Internet cannot read messages sent over the virtual private network.

Because both features are generally desirable, most implementations are likely to use ESP rather than AH. The key exchange function allows for manual exchange of keys as well as an automated scheme.

## Cisco IPSec Technologies

Cisco IPSec includes the following technologies:

- IPSec—IPSec uses encryption technology to provide data confidentiality, integrity, and authenticity between participating peers in a private network. Cisco provides full Encapsulating Security Payload (ESP) and Authentication Header (AH) support.
- Internet Key Exchange (IKE)—The Internet Key Exchange (IKE) provides security association management. IKE authenticates each peer in an IPSec transaction, negotiates security policy, and handles the exchange of session keys. Cisco has been leading the standardization effort for IKE by writing IETF Internet drafts and by making a freeware version of IKE available on the Internet. For details, see the "Internet Key Exchange Security (IKE) Protocol" section.
- Certificate management—Cisco supports the X509.V3 certificates for device authentication during IKE negotiation. Certificate management includes the use of the Simple Certificate Enrollment Protocol (SCEP), a protocol for communicating with Certification Authorities (CA). This certificate solution supports hierarchical certificate structures and the cross-certification necessary for a public key infrastructure (PKI) solution.

The IPSec technologies include the following:

- Diffie-Hellman—Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecure communications channel. IKE uses Diffie-Hellman to establish session keys. VPN Solutions Center supports two Diffie-Hellman groups: Group 1—a MODP group with a 768-bit modulus; Group 2—a MODP group with a 1024-bit modulus.
- DES—The Data Encryption Standard (DES) encrypts packet data.
- MD5/SHA algorithms—The Message Digest 5/SHA hash algorithms authenticate packet data.

# Types of Security Attacks

IP-based data is vulnerable to hackers' tampering and eavesdropping. IP's strength is that it has small, manageable packets of electronic information that can be routed quickly and easily. These chunks of information create breaks in the data stream that allow them to be transmitted efficiently through the network. However, the way IP routes these packets causes large IP networks to be vulnerable to a number of security attacks, such as:

- Spoofing—An attack that involves one machine on a network masquerading as another.
- Sniffing—An attack that involves an eavesdropper listening in on communications between two other parties.
- Session hijacking—An attack in which a hacker uses both spoofing and sniffing to control an established communications session and pretends to be one of the parties involved.

In each of these forms of network attack, an unauthorized individual gains access to private company information. To remedy the problem, an international group organized under the Internet Engineering Task Force (IETF) created the IPSec protocol suite, a set of IP protocols that provide security services at the network level. IPSec is based on state-of-the-art cryptographic technology that makes secure data authentication and privacy on large networks a reality.

# IPSec Encryption Technologies

The IPSec protocol suite has a foundation of powerful encryption technologies. The suite adds security services to the IP layer in a way that is compatible with both the existing IPv4 standard and the emerging IPv6 standard.

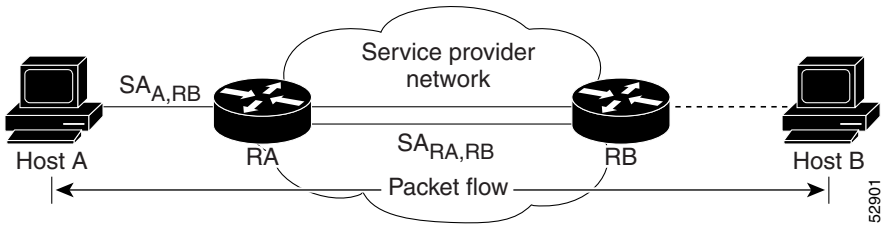
# Transport Mode and Tunnel Mode

IPSec supports two encryption modes:

- Transport mode—Encrypts only the data portion (payload) of each packet and leaves the packet header untouched. Transport mode is applicable to either gateway or host implementations, and provides protection for upper layer protocols as well as selected IP header fields.
- Tunnel mode—More secure than Transport mode because it encrypts both the payload and the header. IPSec in Tunnel mode is normally used when the ultimate destination of a packet is different than the security termination point. This mode is also used in cases when the security is provided by a device that did not originate packets, as in the case of VPNs.
  - Tunnel mode is often used in networks with unregistered IP addresses. The unregistered address can be tunneled from one gateway encryption device to another by hiding the unregistered addresses in the tunneled packet.

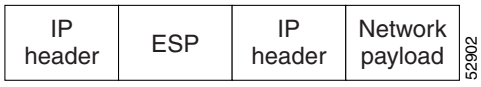
Figure 1-2 shows a typical network using IPSec in Tunnel mode:

*Figure 1-2 IPSec in Tunnel Mode*




In Tunnel mode, IPSec encapsulates an IP packet with IPSec headers and adds an outer IP header, as shown in Figure 1-3.

*Figure 1-3 IPSec Tunnel Mode Packet Format*




An IPSec Tunnel mode packet has two IP headers:

- The inner header—Is constructed by the host;
- The outer header—Is added by the device that is providing security services. IPSec defines Tunnel mode for both the Authentication Header (AH) and Encapsulating Security Payload (ESP).

IPSec standards define several new packet formats, such as an Authentication Header (AH) to provide data integrity and the Encapsulating Security Payload (ESP) to provide confidentiality. IPSec parameters between devices are negotiated with the Internet Key Exchange (IKE) protocol, formerly referred to as the Internet Security Association Key Management Protocol (ISAKMP/Oakley).

IKE can use digital certificates for device authentication. The Encapsulating Security Payload and the Authentication Header use cryptographic techniques to ensure data confidentiality and digital signatures that authenticate the data's source.

The IP packet is the fundamental unit of communications in IP networks. IPSec handles encryption at the packet level, and the protocol it uses is the ESP. ESP supports any type of symmetric encryption. The default standard built into ESP that assures basic interoperability is 56-bit DES.

# Using IPSec to Secure the IP Layer

IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides security for transmission of sensitive information over unprotected networks such as the Internet. It acts at the network level and implements the following standards:

- IPSec
- Internet Key Exchange (IKE)
- Data Encryption Standard (DES)
- MD5 (HMAC variant)
- SHA (HMAC variant)
- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

Essentially, if IPSec is used where IP is normally used (in the network layer), communications are secured for all applications and for all users more transparently than if any other approach was employed. With IPSec, a service provider can create a secure VPN as needed and with any other device that is using the IPSec standard. Because IPSec works with both existing and future IP standards, regular IP networks can still be used to carry data. The sending and receiving devices must be IPSec compliant, but the rest of the network between the sender and recipient does not have to be IPSec compliant.

The primary strength of the IPSec approach is that security works at a low network level. As a result, IP is transparent to the average user, and IPSec-based security services also function behind the scenes to ensure that all network communications are secure. IPSec meets a broad range of security needs and allows different networks around the world to interconnect and to communicate securely. In addition, IPSec offers almost infinite scalability with transparent and reliable service, no matter how demanding a company's security needs.

# Encapsulating Security Payload

The Encapsulating Security Payload (ESP) contains six parts as described below. The first two parts are not encrypted, but they are authenticated. Those parts are as follows:

- The Security Parameter Index (SPI) is an arbitrary 32-bit number that tells the device receiving the packet which group of security protocols the sender is using for communication. Those protocols include the particular algorithms and keys, and how long those keys are valid.
- The Sequence Number is a counter that is incremented by 1 each time a packet is sent to the same address and uses the same SPI. The sequence number indicates the identity of each packet, and how many packets have been sent with the same group of parameters. The sequence number also protects against replay attacks. Replay attacks involve an attacker who copies a packet and sends it out of sequence to confuse communicating devices.

The remaining four parts of the ESP are all encrypted during transmission across the network. Those parts are as follows:

- *Payload Data*—The actual data that is carried by the packet.
- *Padding*—(from 0 to 255 bytes of data) Allows certain types of encryption algorithms to require the data to be a multiple of a certain number of bytes. The padding also ensures that the text of a message terminates on a four-byte boundary (an architectural requirement within IP).
- *Pad Length* field—Specifies how much of the payload is padding rather than data.
- T *Next Header* field—(like a standard IP Next Header field) Identifies the type of data carried and the protocol.

The ESP is added after a standard IP header. Because the packet has a standard IP header, the network can route it with standard IP devices. As a result, IPSec is backward-compatible with IP routers and other equipment even if that equipment is not designed to use IPSec. ESP can support any number of encryption protocols. It is up to the user to decide which protocols to use. Different protocols can be employed for every person a user communicates with. However, IPSec specifies a basic DES-Cipher Block Chaining mode (CBC) cipher as the default to ensure minimal interoperability among IPSec networks. ESP's encryption capability is designed for symmetric encryption algorithms. IPSec employs asymmetric algorithms for such specialized purposes as negotiating keys for symmetric encryption.

### Tunneling with ESP

Tunneling encapsulates an original IP packet header within the ESP. Then, it adds a new IP header containing the address of a gateway device to the packet. Tunneling allows a user to send illegal IP addresses through a public network (like the Internet) that otherwise would not accept them. Tunneling with ESP offers the advantage of hiding original source and destination addresses from users on the public network. Hiding these addresses reduces the power of traffic analysis attacks. A traffic analysis attack employs network monitoring techniques to determine how much data and the type of data being communicated between two users.

### ESP Authentication Field

The ESP Authentication field contains an Integrity Check Value (ICV), which functions as a digital signature that is computed over the remaining part of the ESP. The ESP Authentication field varies in length depending on the authentication algorithm used. This field can be omitted entirely if authentication is not needed for the ESP. Authentication is calculated on the ESP packet after encryption is complete. The current IPSec standard requires HMAC (a symmetric signature scheme) with hashes SHA1 and MD5 as algorithms for IPSec-compliant hardware and software in the ESP packet's Authentication field.

The Integrity Check Value supports symmetric type authentication.

- The sending device encrypts a hash of the data payload and attaches it as the authentication field.
- The receiving device confirms that the data payload has not been tampered with and that the payload did come from the correct source device.

## Authentication Header

The IPSec suite's second protocol, the Authentication Header (AH), provides authentication services. The AH may be applied alone, together with the ESP, or in a nested fashion when tunnel mode is used. Authentication provided by the AH differs from what is provided in the ESP in that the ESP's authentication capabilities do not protect the IP header that lies in front of the ESP, although an encapsulated IP header in tunneling mode is protected. The AH services protect this external IP header, along with the entire contents of the ESP packet. The AH does not protect all of the fields in the external IP header because some change in transit, and the sender cannot predict how they might change. The AH protects everything that does not change in transit. In the packet, the AH is located after the IP header but before the ESP (if present) or other higher level protocol, such as TCP. Like the ESP, the AH can implement tunneling mode. Also, like the ESP, IPSec requires specific algorithms to be available for the AH to be implemented.

## Security Associations

The Authentication Header and Encapsulating Security Payload protocols are the building blocks of IPSec. The encryption services provided by the AH and ESP are powerful tools for keeping data secret, for verifying its origin, and for protecting it from undetected tampering. But these tools do not work unless there is a carefully designed infrastructure to work with them. VPN security succeeds or fails depending on the reliability and scalability of this infrastructure.

Secure communication with authentication and encryption requires negotiation, an exchange of keys, and a capability to keep track of the keys. The way that IPSec keeps track of the details, as well as which keys and algorithms to use, is by bundling everything together in a Security Association (SA). An

association is a 1-way relationship between a sender and a receiver that affords security services to the traffic carried on it. The SA groups together all of the elements needed for two parties to communicate securely.

If a peer relationship is needed for 2-way secure exchange, two security associations are required. Security services are afforded to an SA for the use of AH or ESP, but not both. A security association is uniquely identified by three parameters:

- Security Parameter Index (SPI)—The SPI assigns a bit string to this SA that has local significance only. The SPI is carried in the AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.
- IP destination address—Currently, only unicast addresses are allowed; this is the address of the destination endpoint of the SA, which may be an end-user system or a network system, such as a firewall or router.
- Security protocol identifier—This indicates whether the association is an AH or ESP security association. Hence, in any IP packet, the security association is uniquely identified by the destination address in the IPv4 or IPv6 header and the SPI in the enclosed extension header (AH or ESP).

An IPSec implementation includes a security association database that defines the parameters associated with each SA. A security association is defined by the following parameters:

- Sequence number counter

A 32-bit value used to generate the sequence number field in AH or ESP headers.

- Sequence counter overflow—A flag indicating whether or not overflow of the sequence number counter should generate an auditable event and prevent further transmission of packets on this SA.
- Antireplay window—Used to determine whether an inbound AH or ESP packet is a replay by defining a sliding window within which the sequence number must fall.
- AH information—Authentication algorithm, keys, key lifetimes, and related parameters being used with AH.
- ESP information

  Encryption and authentication algorithm, keys, initialization values, key lifetimes, and related parameters being used with ESP.
- Lifetime of this security association—A time interval or byte count after which an SA must be replaced with a new SA (and new SPI) or terminated, plus an indication of which of these actions should occur.
- IPSec protocol mode—Tunnel, transport, or wildcard (required for all implementations); these modes are discussed later in this chapter (XREF).
- Path MTU—Any observed path maximum transmission unit (maximum size of a packet that can be transmitted without fragmentation) and aging variables (required for all implementations).

The key management mechanism that is used to distribute keys is coupled to the authentication and privacy mechanisms only by way of the security parameters index. Hence, authentication and privacy are specified independent of any specific key management mechanism.

The SA is the secure channel through the public network. The SA also lets the system construct classes of security channels. If more secure safeguards are needed, more care can be taken, and the rules of the SA can be changed to specify stronger measures.

# Internet Key Exchange Security Protocol

Internet Key Exchange (IKE) is a protocol for protocol negotiation and key exchange through the Internet. IKE enables an agreement to be negotiated on which protocols, algorithms, and keys should be used. It ensures secure authentication services from the beginning of the exchange. It manages keys securely after they are agreed upon, and it exchanges those keys safely.

IKE provides four capabilities:

- Provides the means for parties to agree on which protocols, algorithms, and keys to use.
- Ensures from the beginning of the exchange that you are talking to the right person.
- Manages those keys after they have been agreed upon.
- Ensures that key exchanges are handled safely.

Key exchange is closely related to security association management. When a security association is created, keys must be exchanged. IKE wraps them together, and delivers them as an integrated package. IPSec specifies that compliant systems support manual keying as well. As a result, manual key exchange is possible in certain situations.

However, for most large enterprises, manual key exchange is impractical. Thus, IKE is expected to continue to negotiate SAs and exchange keys automatically through public networks. IKE functions in two phases:

- Phase 1—Two IKE peers establish a secure channel for performing ISAKMP operations.
- Phase 2—The two peers negotiate general purpose security associations.

An IKE peer is an IPSec-compliant node capable of establishing IKE channels and negotiating SAs. IKE provides three modes for the exchange of keying information and setting up IKE security associations: *Main mode*, *Aggressive mode*, and *Quick mode*.

## Main Mode

Main mode provides a way to establish the first phase of an IKE SA, which is then used to negotiate future communications.

1. The first step, securing an IKE SA, occurs in three 2-way exchanges between the sender and the receiver. In the first exchange, the sender and receiver agree on basic algorithms and hashes.
2. In the second exchange, public keys are sent for a Diffie-Hellman exchange. Nonces (random numbers each party must sign and return to prove their identities) are then exchanged. In the third exchange, identities are verified, and each party is assured that the exchange has been completed.

## Aggressive Mode

Aggressive mode provides the same services as main mode. It establishes the phase one SA, and operates in much the same manner as main mode except that it is completed in two exchanges instead of three.

In aggressive mode, the sender generates a Diffie-Hellman pair at the beginning of the exchange, doing as much as is reasonable with the first packet (proposing an SA, passing the Diffie-Hellman public value, sending a nonce to the other party to sign, and so on). The recipient then sends back a consolidation of all three response steps that occur in Main mode.

The result is that aggressive mode accomplishes as much as main mode, with one exception. Aggressive mode does not provide identity protection for communicating parties. In other words, in aggressive mode, the sender and recipient exchange identification information before they establish a secure channel where the information is encrypted. As a result, a hacker monitoring an aggressive mode exchange can determine who has just formed a new SA. Aggressive mode's main value, though, is speed.

## Quick Mode

After two parties have established a secure channel using either aggressive mode or main mode, they can use Quick mode. Quick mode has two purposes—to negotiate general IPSec security services and to generate newly keyed material. Quick mode is much simpler than both Main and Aggressive modes. Quick mode packets are always encrypted under the secure channel (or an IKE SA established in phase 1) and start with a hash payload that is used to authenticate the rest of the packet. Quick mode determines which parts of the packet are included in the hash.

Key refreshing can be done in two different ways:

- If perfect forward secrecy is not needed, Quick mode can refresh the keying material already generated in main or aggressive mode with additional hashing. The sender and recipient can then exchange nonces through the secure channel, and use them to hash the existing keys.
- If perfect forward secrecy is desired, an additional Diffie-Hellman exchange is requested through the existing SA, and the keys can be changed that way. Basic quick mode is a three-packet exchange.

## Perfect Forward Secrecy

A method to generate a new key that does not depend on the current key is needed. The way that perfect forward secrecy is done through IKE is called "Diffie-Hellman."

A user can reduce the risk of hackers deciphering a message through the use of larger and larger keys. But, the larger the key, the slower encryption is accomplished, and network performance also decreases. Use of fairly large keys and frequent changes of them is a good compromise. However, the challenge is coming up with ways to generate these new keys.

Then, if a hacker knows the current key, he or she will know only a small amount of information. The hacker would have to find out an entirely unrelated key to get to the next part. This concept is called perfect forward secrecy.

A Diffie-Hellman exchange allows two users who wish to communicate with each other to randomly generate keys that are similar to a public/private key pair.

1. Each user sends a public key value to the other.
2. Each then combines the public key they receive with the private key they just generated using the Diffie-Hellman combination algorithm.
3. The resulting value is the same on both sides. No other users in the world can come up with the same key from the two public keys that traveled across the Internet, because the final key depends on each user's private key, which is secret.

The derived Diffie-Hellman key can be used either as a session key for subsequent exchanges or to encrypt another randomly generated key. Diffie-Hellman allows new shared keys, that are independent of older keys, to be generated for symmetric encryption, thus providing perfect forward secrecy. Because symmetric encryption operates quickly, Diffie-Hellman is valuable to network communications.

## Certification Authority

The IPSec-compliant secure VPN includes the Certification Authority (CA). Certification Authority interoperability:

- Is provided in support of the IPSec standard.
- Permits Cisco IOS devices and CAs to communicate so that your Cisco IOS device can obtain and use digital certificates from the CA. Although IPSec can be implemented in your network without the use of a CA, using a CA provides manageability and scalability for IPSec.

While not an integral part of IPSec, the CA is, nevertheless, a critical element in the public key infrastructure. A CA is a trusted third-party, an entity whose identity has already been established and proven. The CA's role is to vouch for the identities of people with whom a user is trying to communicate.

When verifying online communications, the CA software issues certificates tying together the following three elements:

- An individual's identity
- The public key the individual uses to "sign" online communications.
- The CA's public key (used to sign and authenticate communications).

The CA defends against the "middle-man" hacker who attempts to work his way into key exchanges. Each time an exchange is initiated:

1. Users sign their communications packages with their digital signatures.
2. Those signatures are checked against the ones on record with the CA; they must match.
3. Users then check the CA certificate's signature with the CA's signature. They must match too. Otherwise, an SA cannot be established and no communication can take place.

For a more information on IPSec, see the SAFE VPN White Paper at: http://www.cisco.com/go/safe.

For information on configuring IPSec, see http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/ipsec.htm.

For information about IPSec security, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm.

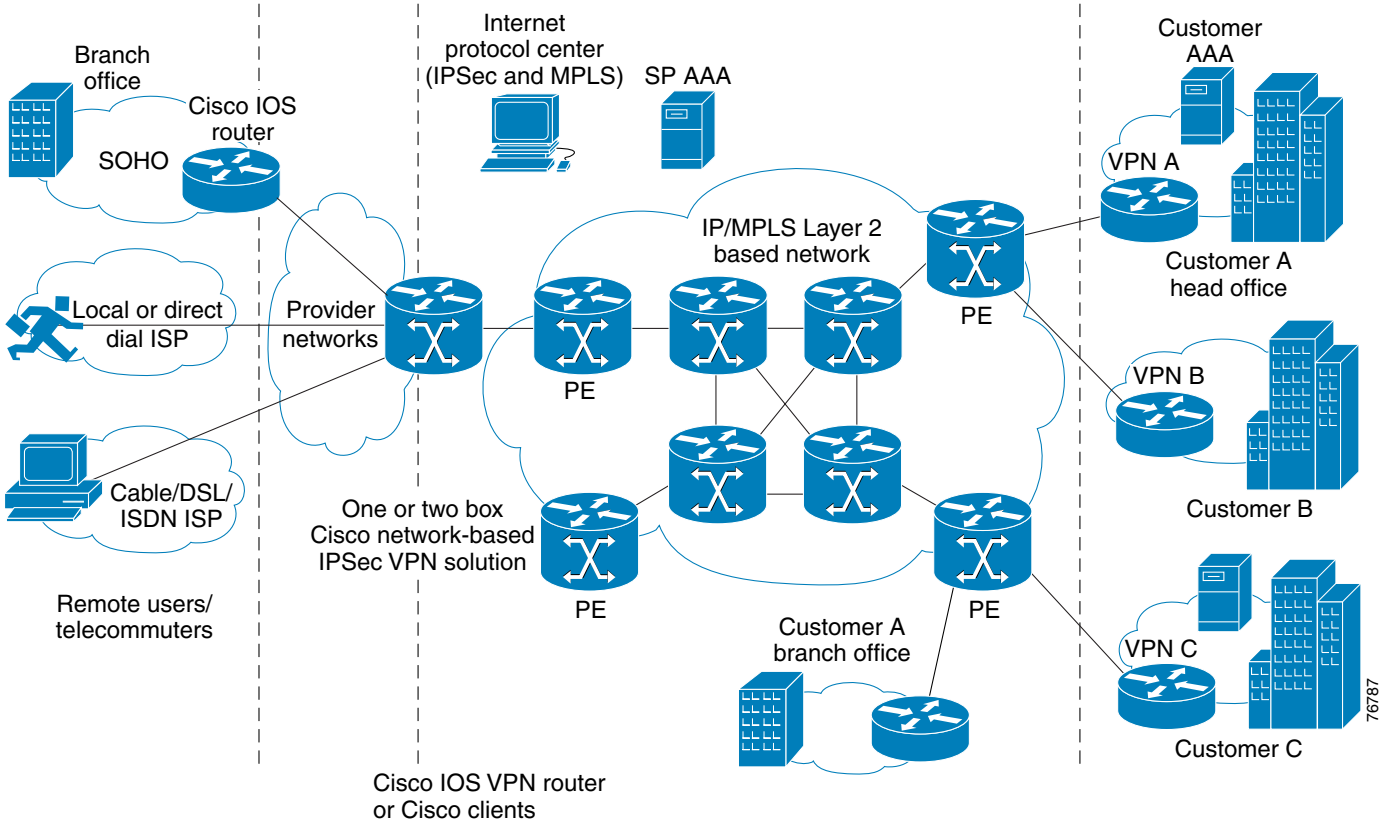
For information about configuring IPSec Network Security, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt4/scdipsec.htm.

For more information on Internet Key Exchange Security Protocol, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/isakmp.htm#xtocid1

# Architecture Overview

The Cisco network-based IPSec VPN solution Release 1.5 (Figure 1-4) maps off-net sites into a network-based Layer 3 VPN using IPSec tunnels. The network-based VPN is either a service provider MPLS VPN as described in RFC 2547bis or a service provider L2 network using Multi-VRF CE.

*Figure 1-4 IPSec to MPLS/VPN Architecture Overview*




There are three types of off-net sites:

- Remote users or telecommuters running a Cisco VPN client in a customer PC
- A SOHO site using the Cisco EZVPN client in a Cisco IOS router
- A SOHO or SMB site using the Cisco IPSEC peer functionality in a IOS router

IPSec off-net access is established through one of two ways:

- Traditional IPSec peer protocol (site-to-site) in tunnel mode or transport mode [in transport mode (m) GRE is used as the tunneling protocol].
- Unity client-server protocol (remote user) running in a PC (Cisco VPN client), in low-end Cisco routers (EZVPN), and in hardware (Cisco VPN 3002 series).

1. The off-net sites connect by way of an access technology [dial, digital subscriber line (DSL), or cable] to a customer edge (CE) device (typically a router). The CE connects over a data link to a provider edge (PE) router.
2. The CE establishes IPSec tunnels with the PE. After establishing the tunnel, the CE advertises the site's local VPN routes to the PE. The CE also learns remote VPN routes from the PE.
3. The PE exchanges routing information with the CE. The PE router also maintains VPN routing information for each VPN it connects to over the service provider network.
4. The PE router maintains a separate Virtual Routing and Forwarding (VRF) table for each off-net site that it connects to through the CE. It is this ability to support multiple VRFs permits per-VPN separation of routing information. Each off-net site connection maps to its specific VRF through a PE port.

**Note** You can associate multiple interfaces on a PE router with a single VRF if all the sites participate in the same VPN.

5. After learning routing information from the CE, the PE router advertises the site's local VPN routes over an MPLS or L2 network through provider core (P) routers (P router is out of the scope of this solution) to other PE routers, and then to other CE routers.

**Note** MPLS VPN supports a hub-and-spoke topology only if the spokes connect to two different PE routers, or the spokes are placed in different VRFs.

# Supported Topologies

The Cisco network-based IPSec VPN solution Release 1.5 supports the following four deployment modes:

- IPSec to MPLS VPN Configuration
- IPSec to L2VPN Using L3 Routing Configuration
- IPSec to IPSec Configuration
- IPSec to GRE Configuration

# Solution Hardware Components

Cisco network-based IPSec VPN solution Release 1.5 components include:

## IPSec Aggregator/PE

The Cisco 7204 and Cisco 7206 series routers serve as an IPSec aggregator/PE. The Integrated Service Adapter (ISA) and the VPN Acceleration Module (VAM) for Cisco 7200 and 7100 Series routers are supported as hardware encryption modules. All of the port adapters supported on the Cisco 7204 and Cisco 7206 series routers are supported by the Cisco network-based IPSec VPN solution Release 1.5 as interfaces.

### Cisco 7204 Series Router

For more information, see http://www.cisco.com/univercd/cc/td/doc/product/core/7202/index.htm.

### Cisco 7206 Series Router

For more information, see http://www.cisco.com/univercd/cc/td/doc/product/core/7206/index.htm.

## RADIUS Server

You can use any RADIUS server (for example, Cisco Access Registrar) that understands Cisco AV pairs to authenticate and authorize remote access clients. If a 2-factor secure-ID-based authentication is required, an RSA server must be installed on the SP management network for local AAA or on the customer premises for proxy authentication.

The service provider or the customer manages the RADIUS servers.

The service-provider managed RADIUS server:

- Can store all AAA and configuration information if the customer does not want to run a RADIUS server, or the information may be distributed across the two servers.
- Typically stores group-specific information (even information originally provided by the customer) because part of the group-specific information may refer to preprovisioned configured information on the IPSEC Aggregator (name of a preprovisioned address pool for router-assigned IP address and name of a preprovisioned access control list for split tunneling at CPE).

Customer-managed information is typically per-user information (for example, user authentication information).

**Note** It is important that you (the service provider) must manage IP address assignment for the VPN (using RADIUS or IPSEC Aggregator) because you know the network topology. The customer does not know the topology.

For more information about RADIUS servers, see http://www.cisco.com/en/US/tech/tk648/tk367/tk547/tech_protocol_home.html.

## Unity VPN Client

The Cisco network-based IPSec VPN solution Release 1.5 supports the Cisco Unity VPN client. The client has wide support on various operating systems including:

- Windows 95 (OSR2), 98, NT Version 4.0 (SP 3 or higher), 2000, XP, ME
- Linux (Red Hat Version 6.2)
- Solaris 2.6 or later
- Mac OS X Version 10.1.0 or later

# Customer Premise Equipment

Table 1-1 lists Cisco platforms can be used as customer premises equipment at remote locations for IPSec termination to the Cisco 7200 series router.

*Table 1-1 Customer Premises Components of the Cisco Network-Based IPSec VPN Solution Release 1.5*

| Component | Description |
|---|---|
| Cisco PIX with EzVPN client | The CiscoWorks Management Center for PIX Firewalls features the look-and-feel of the PIX Device Manager (PDM) but offers centralized management scalability of up to 1,000 PIX firewalls. The management center for PIX firewalls provides entire SAFE coverage and features centralized management of access rules, network address translation, intrusion detection, and EZVPN on PIX firewalls. See http://www.cisco.com/en/US/products/sw/cscowork/ps3992/index.html |
| Cisco VPN 3002 hardware client | The Cisco VPN 3002 Hardware Client is a full-featured VPN client that supports 56-bit DES or 168-bit Triple DES (IPSec). Available in 2 modes (client and network extension mode) the Cisco VPN 3002 client can be configured to either emulate the operation of the software client, or to establish a secure site-to-site connection with the central site device. See http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3002/. |
| Cisco 800 series routers | Cisco 800 Series of Secure Routers are ideal for providing secure Internet and corporate network connectivity to small remote offices and teleworkers. The Cisco 800 series routers provide a wide range of rich integrated security services, advanced Quality of Service (QoS) features for high quality voice, video and data applications, and easy deployment and remote management features with Cisco IOS software. See http://www.cisco.com/en/US/products/hw/routers/ps380/index.html. |
| Cisco 1700 series routers | Cisco 1700 series modular access routers are designed to provide a cost-effective integrated e-business platform for small and medium-sized businesses and enterprise small branch offices. They provide flexibility and manageability to meet the most demanding and evolving e-business requirements, such as multiservice data/voice/video/fax integration, high-speed broadband Internet connection, and comprehensive security solutions. See http://www.cisco.com/en/US/products/hw/routers/ps221/index.html. |
| Cisco 2600 series routers | New Cisco 2600 series family of modular routers include the Cisco 2600XM routers and the Cisco 2691 router. These new models deliver extended performance, higher density, enhanced security performance and increased concurrent application support to meet the growing demands of branch offices today. See http://www.cisco.com/en/US/products/hw/routers/ps259/index.html. |
| Cisco 3600 series routers | The Cisco 3600 series is a family of modular, multiservice access platforms for medium and large-sized offices and smaller Internet service providers. With more than 70 modular interface options, the Cisco 3600 family provides solutions for data, voice video, and hybrid. See http://www.cisco.com/en/US/products/hw/routers/ps274/index.html dial access, virtual private networks (VPNs), and multiprotocol data routing. |
| Cisco 7200 series routers | Cisco 7200 routers combines exceptional performance and price with flexible connectivity options and unparalleled feature support. As the fastest single-processor router, it provides industry-leading serviceability and manageability features. See http://www.cisco.com/en/US/products/hw/routers/ps341/index.html. |
| Cisco IP Solution Center Version 3.0 | The Cisco IP Solution Center Version 3.0 provides MPLS VPN service providers a customizable network and service management solution. |

# Features

This section briefly describes the new features introduced in the Cisco network-based IPSec VPN solution Release 1.5.

For an overview of scalability and performance, system redundancy, and management, see subsequent sections of this document. For software requirements, refer to the *Release Notes for the Cisco Network-Based IPSec VPN Solution Release 1.5*.

## MPLS Virtual Private Networks

The IP virtual private network (VPN) feature for multiprotocol label switching (MPLS) allows a Cisco IOS network to deploy scalable IPv4 Layer 3 VPN backbone services. An IP VPN is the foundation companies use for deploying or administering value-added services including applications and data hosting network commerce, and telephony services to business customers.

For more information, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/vpn.htm.

## IPSec VPN High Availability

The IPSec VPN High Availability feature consists of two new features that work together to simplify network design for VPNs and reduce configuration complexity on remote peers with respect to defining gateway lists:

- Reverse Route Injection
- Hot Standby Router Protocol and IPSec

For more information, see http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide09186a00800ed370.html.

### Reverse Route Injection

Reverse Route Injection (RRI) simplifies network design for Virtual Private Network (VPNs) in which there is a requirement for redundancy or load balancing. RRI works with both dynamic and static crypto maps.

RRI allows dynamic installation of client routes in the routing table. This in conjunction with HSRP prevents asymmetrical routing problems.

For more information, see Reverse Route Injection at http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide09186a00800ed370.html#1024537.

### Hot Standby Router Protocol and IPSec

Hot Standby Router Protocol (HSRP) and IPSec provides high network availability by routing IP traffic from hosts on Ethernet networks without relying on the availability of any single router. HSRP is particularly useful for hosts that do not support a router discovery protocol, such as ICMP Router

Discovery Protocol (IRDP), and do not have the functionality to switch to a new router when their selected router reloads or loses power. Without this functionality, a router that loses its default gateway because of a router failure is unable to communicate with the network.

You can use HSRP to create a stateless failover mechanism. In case of a failure on the active router, the backup router can then assume IPSec aggregation functions.

For more information, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e9/ipsecha.htm#29050.

# Per VRF AAA

Using the Per VRF AAA feature on the IPSec Aggregator/PE, Internet Service Providers (ISPs) can partition authentication, authorization, and accounting (AAA) services based on Virtual Route Forwarding (VRF). This permits the IPSec Aggregator/PE to communicate directly with the customer RADIUS server associated with the customer 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 the flexibility demanded.

For more information, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftvrfaaa.htm.

# Cisco 7200 Series NPE-G1 Processor

The Cisco 7200 Series Network Processing Engine NPE-G1 (NPE-G1) addresses the demand for performance and flexibility by doubling its processing capacity and enabling unprecedented LAN performance.

For more information, see http://www.cisco.com/en/US/products/hw/routers/ps341/products_data_sheet09186a00800c6bd6.html.

# VRF Aware IPSec

The VRF Aware IPSec feature introduces full IP security (IPSec) tunnel mapping to VRF-aware core virtual private networks (VPNs) supporting Multiprotocol Label Switching (MPLS), ATM, and Frame Relay. Using the VRF Aware IPSec feature, you can map IPSec tunnels to VRFs based on IPSec authentication. Hard-configured interface-VRF bindings are not required.

For more information, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_vrfip.htm.

# IPSec VPN Accounting

The IPSec VPN Accounting feature allows for a session to be accounted for by indicating when the session starts and when it stops.

A VPN session is defined as an Internet Key Exchange (IKE) security association (SA) and the one or more SA pairs that are created by the IKE SA. The session

starts when the first IP Security (IPSec) pair is created and stops when all IPSec SAs are deleted.

For more information, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_evpna.htm#wp1027129.

# IPSec Security Association Idle Timers

This feature monitors SAs for activity and then removes idle SAs after some specified period of inactivity.

When a Cisco software-based IOS router creates an IPSec security association (SA) for a peer, it allocates a certain amount of resources to maintain the SA; the SA requires memory and several managed timers. For idle peers, these resources are wasted, and wasted resources could eventually prevent the router from creating new SAs with other peers.

For more information, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftsaidle.htm.

# Distinguished Name Based Crypto Maps

The Distinguished Name Based Crypto Maps feature allows you to configure the router to restrict access to selected encrypted interfaces for those peers with specific certificates, especially certificates with particular Distinguished Names (DNs).

Previously, if the router accepted a certificate or a shared secret from the encrypting peer, Cisco IOS software did not have a method of preventing the peer from communicating with any encrypted interface other than the restrictions on the IP address of the encrypting peer. This feature allows you to configure which crypto maps are usable to a peer based on the DN that a peer used to authenticate itself, thereby, enabling you to control which encrypted interfaces a peer with a specified DN can access.

For more information, see http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087b70.html#xtocid225341.

# Cisco Easy VPN Remote Feature

The Cisco Easy VPN Remote feature eliminates tedious work by implementing the Cisco Unity Client protocol, which allows most VPN parameters to be defined at a VPN remote access server. This server can be a dedicated VPN device such as a VPN 3000 concentrator or a Cisco PIX Firewall, or a Cisco IOS router that supports the Cisco Unity Client protocol.

Many applications require the security of VPN connections that perform a high level of authentication and that encrypt the data between two particular endpoints. However, establishing a VPN connection between two routers can be complicated, and typically requires tedious coordination between network administrators to configure the two routers' VPN parameters.

The Cisco Easy VPN Remote feature:

- Supports two modes of operation, client mode and network extension mode that, optionally, support split tunneling.
- Supports authentication using Extended Authentication (XAUTH).

For more information, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122y/122ya/122ya4/ftezvpcm.htm#xtocid0.

# Cisco Easy VPN Remote Phase II

The Cisco Easy VPN Remote feature provides enhancements and additional capabilities to Phase I features. In Phase II, the Cisco Easy VPN Remote feature provides:

- Manual Tunnel Control—Establishes and terminates the IPSec VPN tunnel on demand.
- NAT Interoperability Support—Automatically restores the NAT configuration when the IPSec VPN tunnel is disconnected.

For more information on these, as well as additional enhancements, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122y/122yj/ftezvp2.htm#xtocid3.

# Easy VPN Server

The Easy VPN Server feature introduces server support for the Cisco VPN client Release 3.x software clients and Cisco VPN hardware clients. It allows a remote end user to communicate using IP Security (IPSec) with any Cisco IOS Virtual Private Network (VPN) gateway. Centrally managed IPSec policies are "pushed" to the client by the server, minimizing configuration by the end user.

**Note** This feature also supports hardware VPN clients, such as the Cisco 800 device, Cisco 900 device, Cisco 1700 device, VPN 3002 device, and PIX 501 devices.

For more information, see

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087d1e.html#xtocid1.

# IPSec NAT Transparency

The IPSec NAT Transparency feature lets IPSec peers establish a connection through a NAT device. It does this by encapsulating IPSec traffic in UDP datagrams, using port 4500, thereby providing NAT devices with port information. NAT-T autodetects any NAT devices, and only encapsulates IPSec traffic when necessary.

For more information, see
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftipsnat.htm.

# VPN Acceleration Module

The VPN Acceleration Module (VAM) is a single-width acceleration module. It provides high-performance, hardware-assisted tunneling and encryption services suitable for virtual private network (VPN) remote access, site-to-site intranet, and extranet applications.

The VAM provides hardware-accelerated support for the following multiple encryption functions:

- 56-bit Data Encryption Standard (DES) standard mode: Cipher Block Chaining (CBC)
- 3-Key Triple DES (168-bit)
- Secure Hash Algorithm (SHA)-1 and Message Digest 5 (MD5)
- Rivest, Shamir, Adelman (RSA) public-key algorithm

- Diffie-Hellman key exchange RC4-40

For more information, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122y/122ye/1229ye/12ye_vam.htm.

## Prefragmentation for IPSec VPNs

This feature allows an encrypting router to predetermine the encapsulated packet size from information available in transform sets, which are configured as part of the IPSec security association (SA).

When a packet is nearly the size of the maximum transmission unit (MTU) of the outbound link of the encrypting router, and it is encapsulated with IPSec headers, it is likely to exceed the MTU of the outbound link. This causes packet fragmentation after encryption, which makes the decrypting router reassemble in the process path. Prefragmentation for IPSec VPNs increases the decrypting router's performance by enabling it to operate in the high performance CEF path instead of the process path.

If it is predetermined that the packet will exceed the MTU of the output interface, the packet is fragmented before encryption. This function avoids process level reassembly before decryption and helps improve decryption performance and overall IPSec traffic throughput.

For more information, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftprefrg.htm.

## Cisco IOS Server Load Balancing

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, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e9/iosslb9e.htm#2711438.

# Cisco IOS Software Fundamentals

Cisco IPSec VPN access provider, service provider, and customer CPE, CE, PE, concentrator, access server, aggregation, gateway, and headend hardware components use Cisco IOS software. Cisco IOS software provides the capability to configure Cisco routers and switches using command-line interface (CLI) commands.

Keep in mind the following when configuring your Cisco IOS software:

- Use the question mark (?) and arrow keys to help enter commands.
- Each command mode restricts you to a set of commands.
- Enter the keyword **no** before a command to disable a feature; for example, **no ip routing**.
- Save configuration changes to NVRAM so they are not lost in a system reload or power outage.
- Use the forward slash (/) command syntax to identify interface and port locations (*slot/port*). The slot identification number is the first number identified in the command syntax.

**Note** Cisco IOS software is feature specific and licensed on an "as is" basis without warranty of any kind, either expressed or implied. The version of Cisco IOS software used in this guide varies depending on configuration requisites for presentation purposes, and should not be construed as the Cisco IOS software version of choice for your system or internetwork environment. Consult your Cisco sales representative regarding your Cisco IOS requirements.

# User Interface Command Modes

Cisco routers/servers are configured from user interfaces, known as ports, which provide hardware connectivity. They are accessed from the console port on a router or Telnet into a router interface from another host. Typical interfaces are Serial 0 (S0), Serial 1 (S1), and Ethernet (E0). Token Ring interfaces are referenced as (T0) and FDDI interfaces use (F0).

# EXEC Command Modes

When you use the CLI, a command interpreter called EXEC is employed by the operating system to translate any command and execute its operation. This command interpreter has two access modes, user and privileged, which provide security to the respective command levels. Each command mode restricts you to a subset of mode-specific commands.

- User mode provides restricted access and limits router configuration or troubleshooting. At this level, miscellaneous functionality is performed, such as viewing system information, obtaining basic router status, changing terminal settings, or establishing remote device connectivity.
- Privileged mode includes user mode functionality and provides unrestricted access. It is used exclusively for router configuration, debugging, setting operating system (OS) parameters, and retrieving detailed router status information.

There are many modes of configuration within privileged mode that determine the type of configuration desired, such as interface configuration (`AS5800(config-if)#`), line configuration (`AS5800(config-line)#`), and controller configuration (`AS5800(config-controller)#`). Each configuration command mode restricts you to a subset of mode specific commands.

In the following command sequence, command prompts are automatically modified to reflect command mode changes. A manual carriage return is implied at the end of each line item.

```
AS5800> enable
AS5800# configure terminal
AS5800(config)# interface ethernet 0/0
AS5800(config-if)# line 0/0
AS5800(config-line)# controller e1 0/0
AS5800(config-controller)# exit
AS5800(config)# exit
AS5800#
%SYS-5-CONFIG_I: Configured from console by console
AS5800#
```

The last message is an example of a system response. Press **Enter** to get to the `AS5800#` prompt.

Table 1-2 lists common configuration modes. Configure global parameters in global configuration mode, interface parameters in interface configuration mode, and line parameters in line configuration mode.

*Table 1-2 Common Cisco IOS Software Command Modes*

| Command Mode | Prompt | Access Method | Escape Method |
|---|---|---|---|
| User EXEC | `AS5800>` | Log in. | Use the **exit** or **logout** command to leave the command line interface. |
| Privileged EXEC | `AS5800#` | From user EXEC mode, enter the **enable** command. | Use the **disable** command to escape back to user EXEC mode. Use the **exit** or **logout** command to leave the command line interface. |
| Global configuration | `AS5800(config)#` | From privileged EXEC mode, enter the **configure terminal** command. | Use the **exit** or **end** (Ctrl-Z) command to escape to privileged EXEC mode. |
| Interface configuration | `AS5800(config-if)#` | Enter the **interface** type and number command, such as **interface ethernet 0/0/0**. | Use the **exit** command to escape to global configuration mode. Use the **end** (Ctrl-Z) command to escape directly to privileged EXEC mode. |
| Line configuration | `AS5800(config-line)#` | Enter the **line** start-number end-number command, such as **line 0/0/1 0/0/48**. | Use the **exit** command to escape to global configuration mode. Use the **end** (Ctrl-Z) command to escape directly to privileged EXEC mode. |
| Controller configuration | `AS5800(config-control)#` | Enter the **controller** name and number command, such as **controller t1 0/0/0**. | Use the **exit** command to escape to global configuration mode. Use the **end** (Ctrl-Z) command to escape directly to privileged EXEC mode. |

# Context-Sensitive Help

Context-sensitive help is available at any command prompt. Enter a question mark (?) for a list of complete command names, semantics, and command mode command syntax. Use arrow keys at command prompts to scroll through previous mode-specific commands for display.

**Note** Cycle through mode specific commands at a mode specific prompt.

- For a list of available commands, enter a question mark.

```
AS5800> ?
```

- To complete a command, enter known characters followed by a question mark (no space).

```
AS5800> s?
```

- For a list of command variables, enter the command followed by a space and a question mark.

```
AS5800> show ?
```

Refer to the chapter "Configuring the User Interface" in the *Configuration Fundamentals Configuration Guide* for more information about working with the user interface in the Cisco IOS software.

**Note** You can press **Ctrl-Z** in any mode to immediately return to enable mode (AS5800#), instead of entering **exit**, which returns you to the previous mode.

# Saving Configurations

To prevent losing the Cisco AS5800 configuration, save it to NVRAM using the following steps:

**Step 1** Enter the **enable** command and password. You are in privileged EXEC mode when the prompt changes to AS5800#.

```
AS5800> enable
Password: password
AS5800#
```

**Note** Press **Ctrl-Z** to return to privileged EXEC mode. Any subsequent system response message is normal and does not indicate an error.

**Step 2** Execute the **copy running-config startup-config** command to save configuration changes to nonvolatile random-access memory (NVRAM) so configuration data is not lost during a system reload, power cycle, or outage.

```
AS5800# copy running-config startup-config
Building configuration...
```

The following prompt appears after a successful configuration copy.

```
[OK]
AS5800#
```

# Undoing a Command

To undo a command or disable a feature, enter the keyword **no** before the command; for example, **no ip routing**.

# Passwords

Several passwords are used when configuring your Cisco IOS software. Passwords are used to identify user authorization and permission rights, virtual terminal configuration, and network management software initialization. Most passwords can use the same notation.

You need the following types of passwords when configuring Cisco IOS software:

- Enable password—A nonencrypted and, therefore, less secure password.
- Enable secret password—A very secure, encrypted password that is used in place of the enable password. Because many privileged-level EXEC commands are used to set operating parameters, we recommend that you use the enable secret password to prevent unauthorized use.

**Note** The enable password and enable secret password should be different. In both cases, a number cannot be the first character. Spaces are also valid password characters, but only when following valid characters; lead spaces are ignored.

- Virtual console password—A password that enables terminal emulation.


# Deployment Models

## Overview

This section describes deployment models for the Cisco network-based IPSec VPN solution Release 1.5:



## IPSec to MPLS VPN Configuration

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

This service model 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.

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

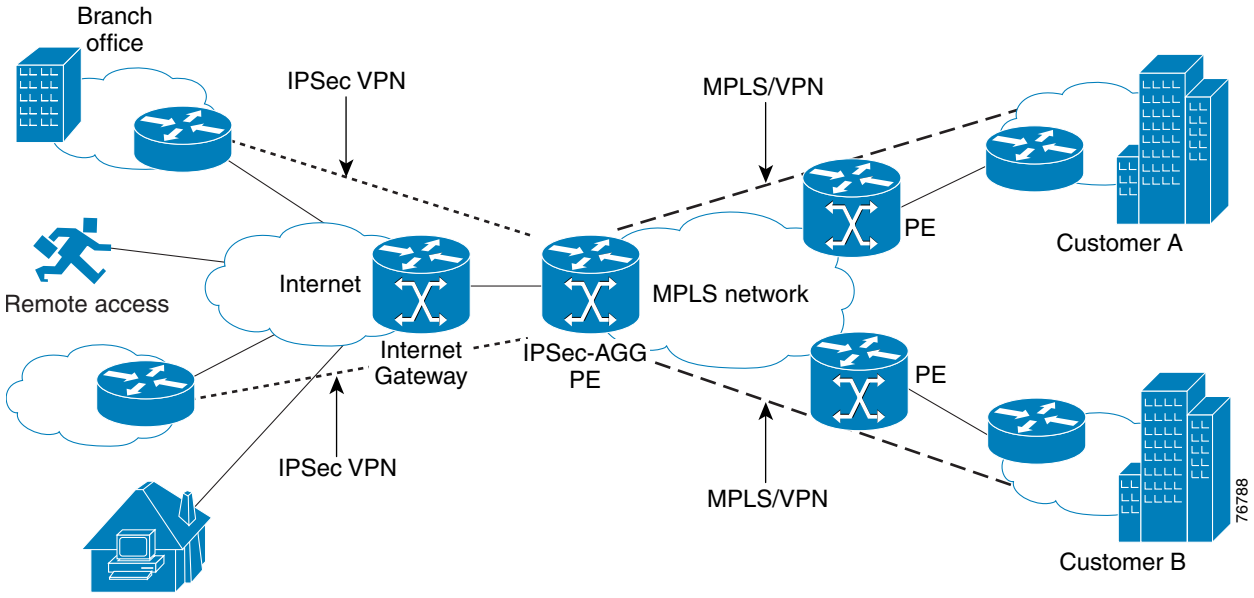
The service provider can either:

- Use the same router to function as an IPSec termination device and also as an MPLS PE.
- Segregate the two functions on separate routers (one router performing IPSec termination and the other router performing the MPLS PE function).

## IPSec MPLS PE Configuration

In this model a Cisco 7200 series router serves as an aggregating router and as a PE and uses VRFs to provide multiple routing instances with each instance independent of others (Figure 2-1).

***Figure 2-1 IPSec into MPLS VPN Configuration***




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. You can associate the VRF with one or more VPNs.

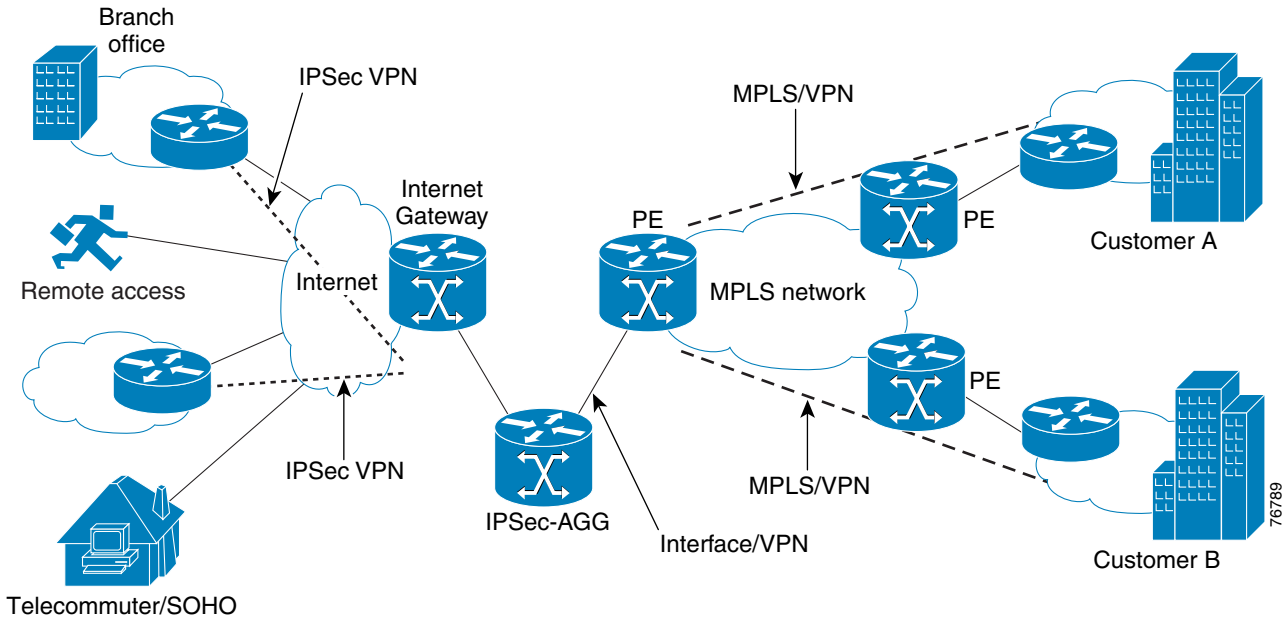
As a PE on the MPLS network, the Cisco 7200 advertises the connected routes to the remote PEs containing the same VPN.

For information on configuring IPSec to MPLS VPN, refer to Chapter 2 in the *Cisco Network-Based IPSec VPN Solution Release 1.5 Implementation Guide*.

## IPSec Aggregator Configuration

This setup uses the Multi-VRF on CE routers feature of Cisco IOS software (Figure 2-2).

***Figure 2-2 IPSec into MPLS VPN Configuration***




This feature brings PE functionality to the CE and uses VRF interfaces to form a VLAN-like setup on the customer side. Each VRF on the CE then maps to a VRF on the PE on separate logical or physical interfaces.

You can connect the IPSec aggregating router to the PE through various L2 technologies, including Frame Relay, ATM, or 802.1q interfaces. Each interface forwards remote sessions traffic belonging to a specific VPN.

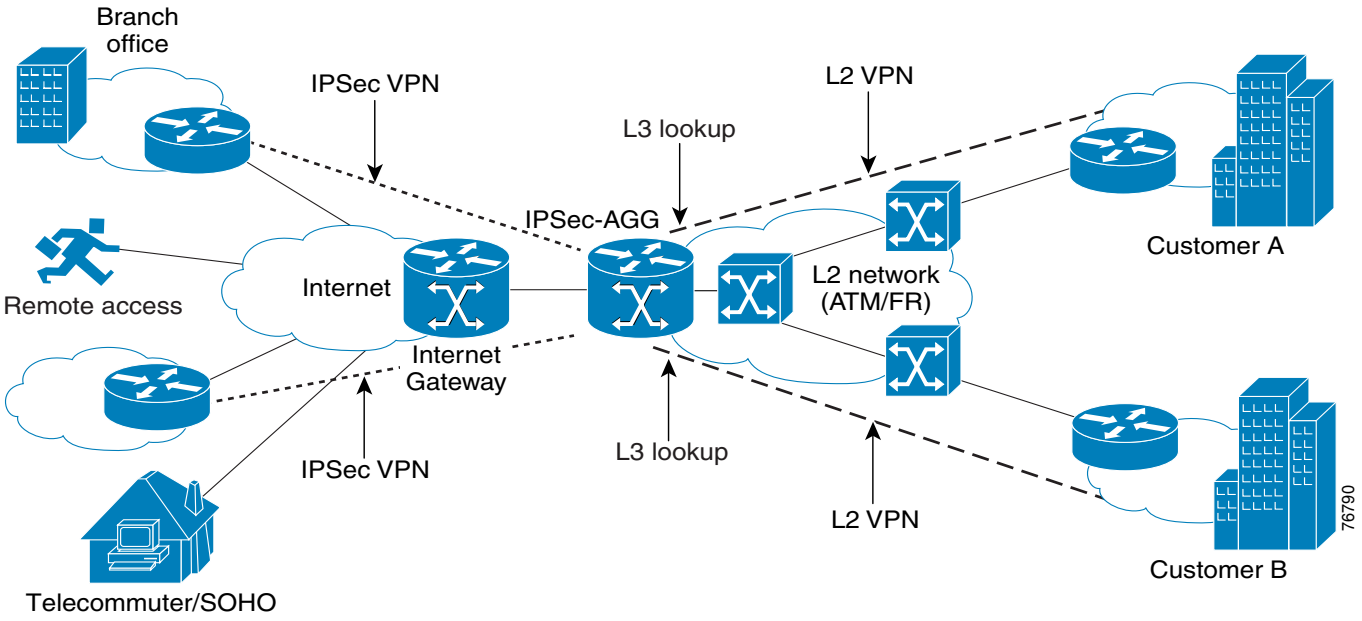
A typical scenario: You have a GSR as a PE but want to terminate IPSec too. Terminate IPSec on a Cisco 7200 router and map to the appropriate VRF. The Cisco 7200 router on the MPLS side connects to the GSR 802.1q interface with each 802.1q mapped to the appropriate VRF.

For information on configuring IPSec to MPLS VPN, refer to Chapter 2 in the *Cisco Network-Based IPSec VPN Solution Release 1.5 Implementation Guide*.

# IPSec to L2VPN Using L3 Routing Configuration

The IPSec to L2VPN model is very similar to the IPSec to MPLS topology described in the previous section, except the service provider has an L2 core instead of an MPLS core (Figure 2-3).

***Figure 2-3 IPSec to L2VPN Configuration***




The L2 core can be Frame Relay, ATM, 802.1q, or wireless.

This topology enables an L2 service provider to extend secured access service beyond its core into the Internet. Sessions terminate on the aggregator platform, similarly to the IPSec to MPLS model.You can then perform an L3 lookup in the routing table and send it out of the appropriate L2VPN VRF interface (Frame Relay, ATM, or 802.1q).

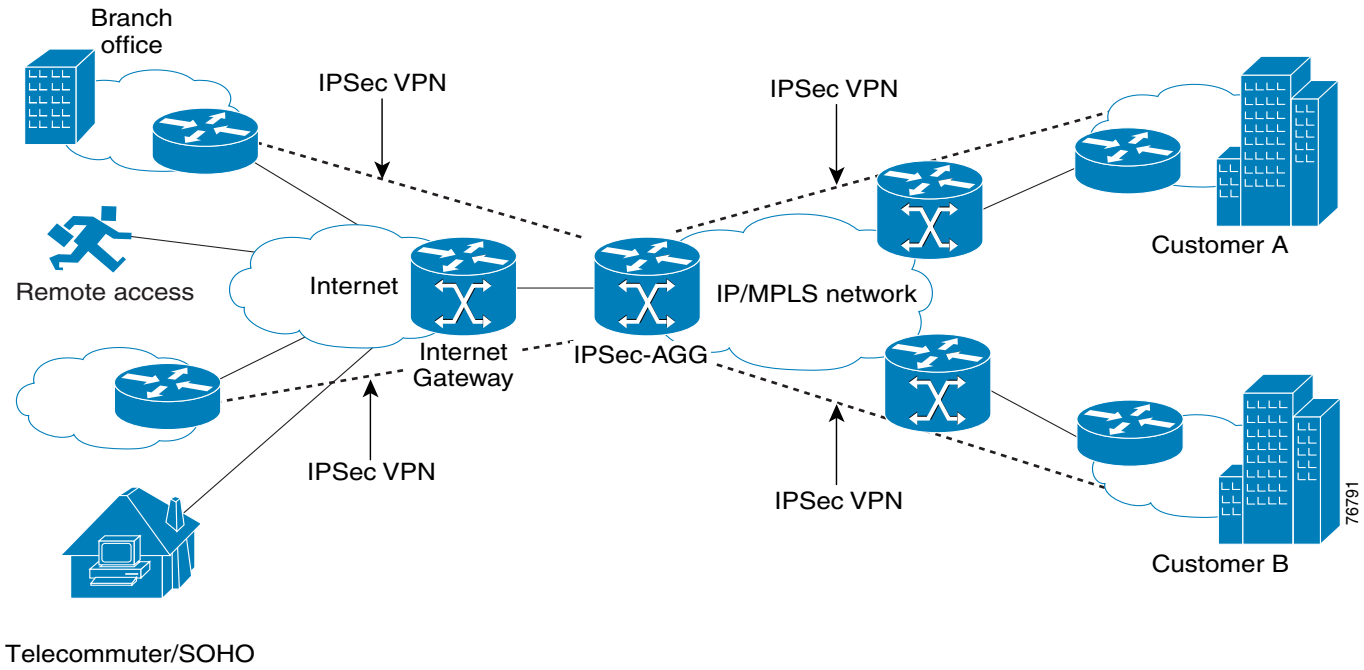
At an L3 level, the IPSec aggregator connects directly to the customer site that has L2 service. The service provider does not need to address the customer routing issue in its core. The IPSec aggregator and the L2 customer site can use either static routes or a dynamic routing protocol to establish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

For information on configuring IPSec to L2VPN, refer to Chapter 3 in the *Cisco Network-Based IPSec VPN Solution Release 1.5 Implementation Guide*.

# IPSec to IPSec Configuration

In this model, the IPSec aggregator aggregates any remote sites/clients and then forwards the information to a headend enterprise VPN device (Figure 2-4).

***Figure 2-4 IPSec to IPSec Configuration***



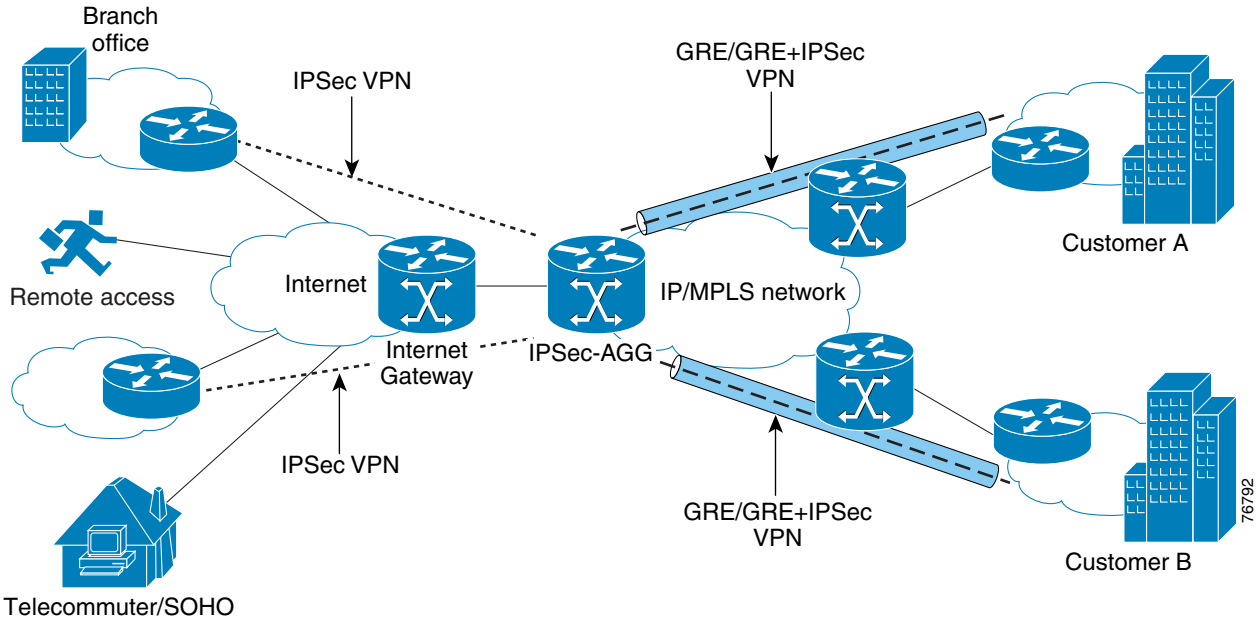

Because traffic is going over an open IP network, IPSec provides the necessary encryption over the IP backbone. This also permits private overlapping IP addressing schemes between enterprises.

For information on configuring IPSec to IPSec, refer to Chapter 4 in the *Cisco Network-Based IPSec VPN Solution Release 1.5 Implementation Guide*.

# IPSec to GRE Configuration

The IPSec to GRE model is useful when the service provider has a IP backbone but still wants to provide VPN-like functionality (Figure 2-5).

***Figure 2-5 IPSec to GRE Configuration***




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.

Using 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.

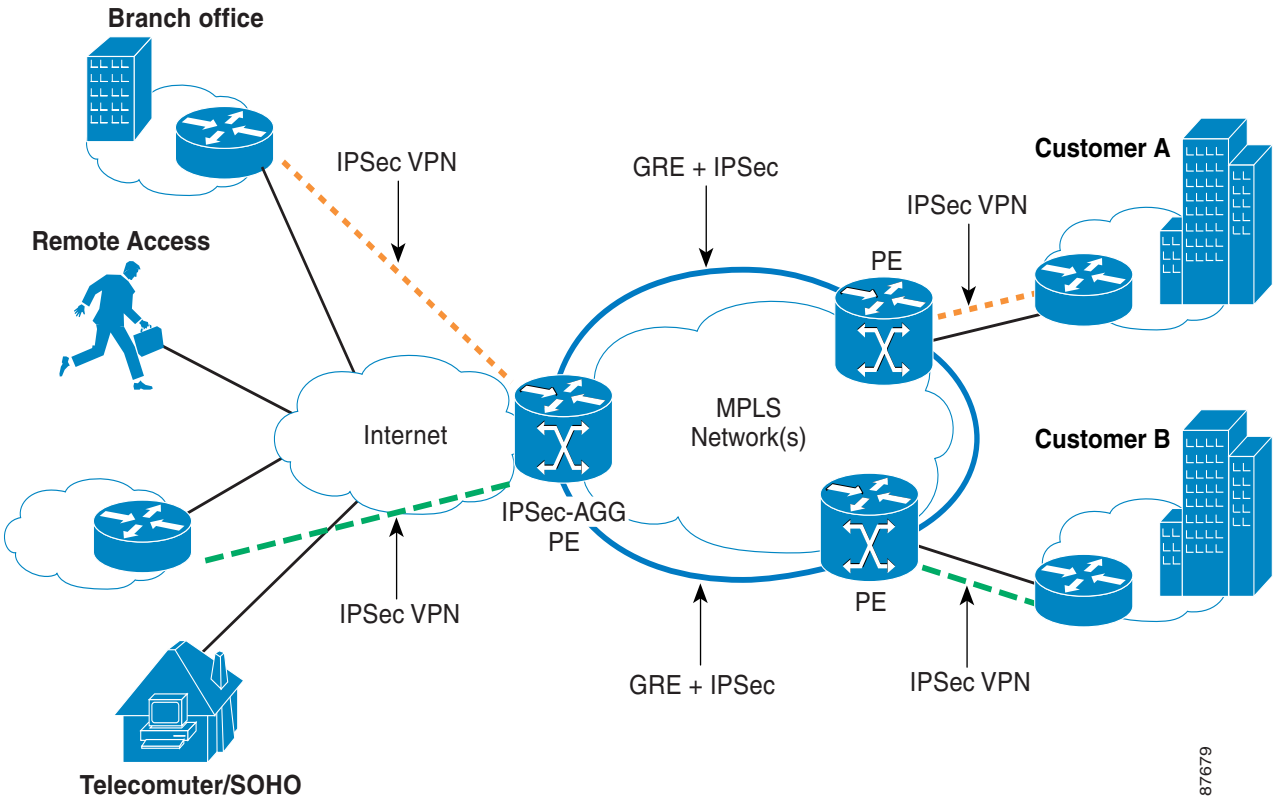
The packets traveling from remote clients and sites are decrypted, routed to the GRE tunnel interface where they are encapsulated with the GRE header. The GRE packet is then encrypted by IPSec to provide secure connectivity across the IP backbone.

For information on configuring IPSec to GRE, refer to Chapter 5 in the *Cisco Network-Based IPSec VPN Solution Release 1.5 Implementation Guide*.

# PE to PE Encryption Configuration

The PE to PE encryption configuration is useful when the service provider wants to encrypt the traffic between the PE devices and an MPLS network (Figure 2-6).

*Figure 2-6 PE to PE Encryption Configuration*




A service provider may want to use this configuration because:

- The service agreement with the end customer requires encryption in the core.
- The MPLS network is spread across several networks and serviced by one or more transport providers.

This model allows a service provider to encrypt the traffic between PE devices while continuing to maintain the traffic separation that MPLS provides.

In this configuration, the service provider creates a network of GRE tunnels between all PE devices. Because the VPN tag is maintained across the MPLS network, only a single GRE tunnel is required between two PEs to service all the VPNs.

The MPLS PE is configured to route all traffic to the IPSec PE through a GRE tunnel which that is encrypted. Similarly, the IPSec PE is configured to route all traffic to the MPLS PE through the same encrypted GRE tunnel. Tag switching is configured on the tunnel endpoints.

For information on configuring PE to PE Encryption, refer to Chapter 5 in the *Cisco Network-Based IPSec VPN Solution Release 1.5 Implementation Guide*.

# IPSec Off-Net Access

off-net access is typically required for:

- A SOHO or SMB site using the Cisco IPSec peer functionality in a Cisco IOS router to connect from its site to another site or to a headquarter's site. This is typically accomplished using traditional IPSec peer protocol (site-to-site) in tunnel mode or GRE in transport mode (in transport mode GRE is used as the tunneling protocol).
- Remote users or telecommuters running a Cisco VPN client in a customer PC to connect from their remote location to another site or to a headquarter's site. This is typically accomplished using Unity protocol (remote user) running in a PC (Cisco VPN client) and in low-end Cisco routers supporting EZVPN.

## Site-to-Site Considerations

IPSec site-to-site access is for use by remote sites that require access to a specific VPN. It requires that you preconfigure each remote site (with IPSec access configuration) to communicate with the edge of the VPN. Because each site is a remote location requiring dynamic routing, you must configure a GRE tunnel for each site.

IPSec operates in:

- Transport mode—where security is provided by using extension to IP header.
- Tunnel mode—where the IP packet is tunneled inside another IP packet and outer IP header has extensions to support authentication and encryption headers.

off-net sites using the peer-to-peer IPSec model access network-based VPN through:

- IPSec in tunnel mode
- GRE tunnel protected by IPSec in transport mode

In the Cisco network-based IPSec VPN solution Release 1.5, IPSec in tunnel mode is used in each possible instance (because VPNs require tunnels).

You must use GRE tunnels to enable dynamic routing between off-net sites and the network-based VPN.

off-net sites typically connect to the network-based VPN in a pre-provisioned hub-and-spoke topology using IPSec tunnel mode and IPSec-protected GRE.

### Operational Considerations

In an off-net site, the IPSec VPN may begin in the customer edge router (the router with the WAN interface to the Internet) or in a device behind the WAN.

If the IPSec VPN originates in the customer edge router, you must provision the router for both Internet access as well as IPSec VPN. You (service provider) and the ISP may both manage this configuration (the customer may also manage parts of the configuration that you and the ISP are not responsible for).

Joint management is not necessary (except that the customer may choose to jointly manage the device) when the IPSec VPN is in a device separate from the WAN router. For the purposes of this document, the following assumptions are made:

- The CE router at the off-net site implements both IPSec VPN and Internet access,
- You (the service provider) are responsible for managing the device and

- You (the service provider) have an agreement with the ISP to receive all provisioning information from the ISP (for example, IP address and routing information for Internet access)

You (the service provider) are responsible for configuring:

- PE routers that connect to on-net customer sites and off-net sites
- IPSec aggregator (which may be in a PE linked to the Internet gateway)
- On-net CE routers and the off-net CE routers that comprise the customer VPN

When an on-net customer subscribes for service, the customer typically provides the location of the headquarter site, and on-net and off-net branch sites. This information identifies the set of PE routers necessary to service the customer.

The customer also provides the following information:

- VPN configuration topology (typically hub and spoke)
- CE-specific information (for example, the VPN address pool for provisioning the CE routers at each site and possibly hosts behind the CE router
- NAT disabled/enabled at CE routers
- Split tunneling disabled/enabled
- Static or dynamic routing required across the VPN
- IP addresses of VPN DNS servers
- Customer domain name

You (the service provider) can use this information to configure all necessary PEs router to provide VPN access over the MPLS backbone in a specified topology. For each on-net or off-net CE router that is brought online, you (the service provider) must configure PE-CE connectivity.

For the peer-to-peer IPSec model, there are no mechanisms for a device to autoconfigure. You must pre-provision configuration information on a peer by peer basis, one end at a CE router and one end at a PE router.

**Note** ISC assumes IP connectivity to the CE routers and that the IP address of the CE router is known.

# Remote VPN Access Considerations

## IPSec Unity Client

The Unity protocol operates:

- Based on the concept of a client group. An ISAKMP client configuration group is a group of Unity clients that share the same identity, authentication material, and configuration (policy) information. A Unity client must identify and authenticate itself by group first, and if XAUTH enabled, by user later.
- In a client/server mode where the client always initiates and implements IKE continuous channel mode. The Unity protocol supports use of either aggressive mode and pre-shared keys, or main mode and certificates.

RADIUS servers can be used to:

- Store client group configuration information (including preshared group password in case of aggressive mode and MODE-CONFIG information).

- Authenticate users (XAUTH). RADIUS servers can only be defined globally.

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

## Unity Client Operation

If the IKE SA negotiates use of XAUTH:

1. The client waits for a challenge and responds.
2. The server authenticates the user, typically using AAA.
3. The client requests MODE-CONFIG parameters from the server. These include:
   - IP address
   - IP addresses of DNS and WINS servers
   - Default domain name
   - ACLs to be applied if split tunneling is enabled

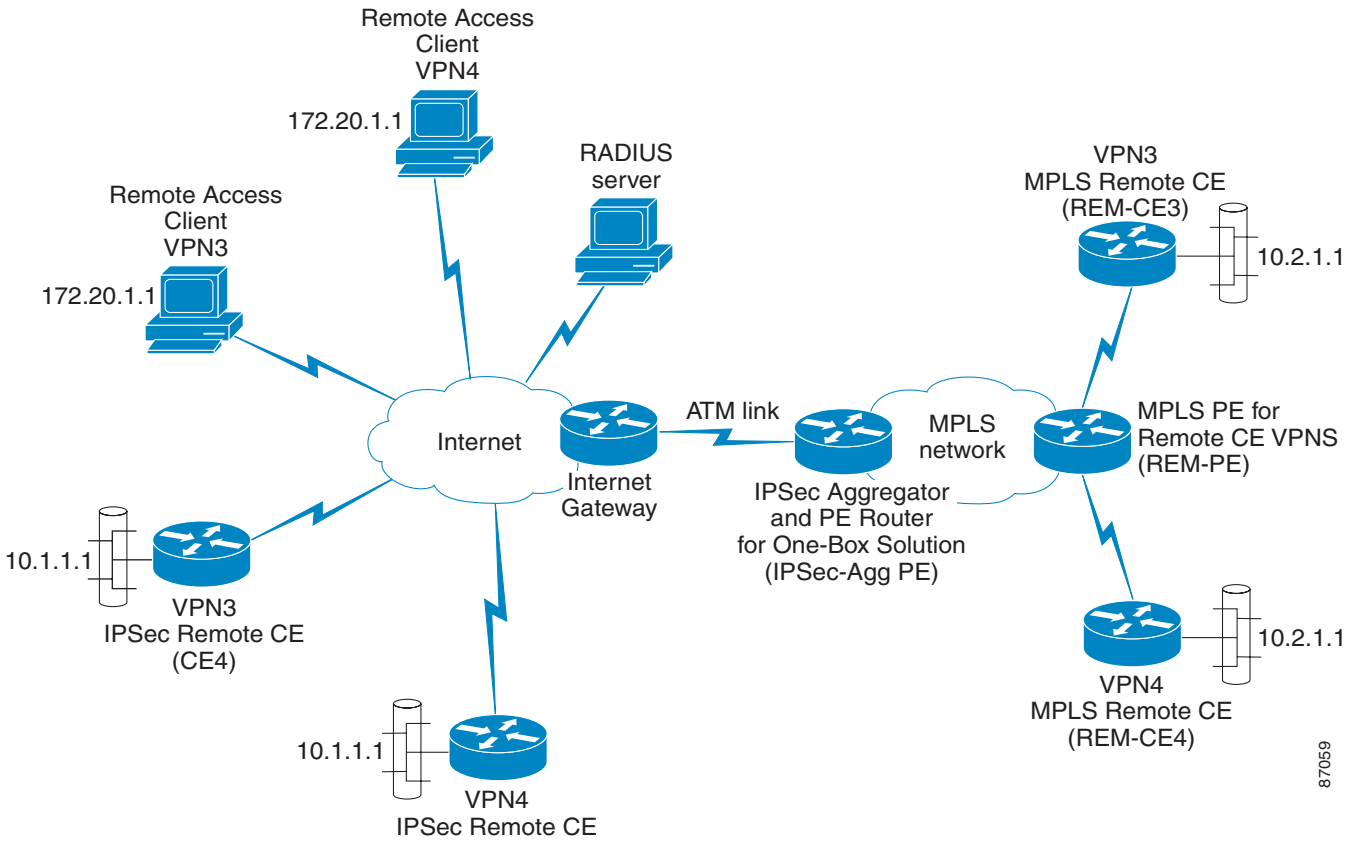
For more information on the Unity client, see http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_software_versions_home.html.

## Mapping Unity Client into VRF

The Unity protocol maps to a VRF in the same way as the peer-to-peer model described in the section titled "Mapping Unity Client into VRF" section on page 2-10. The Unity client must be configured with the IP address (or FQDN) of the appropriate tunnel-end point address. The group name that you configure on the Unity client for preshared key authentication is also used as the identity. You can also use RSA digital signature authentication where the DN name serves as the identify.

Figure 2-7 shows a typical connection sequence for remote sites.

*Figure 2-7 Connection Sequence*




# Sequence of Operations—Site-to-Site Connection

The following provides typical connection sequences for remote sites (see Figure 2-7).

1. At the remote site CE4, 10.1.1.1 initiates a FTP file transfer to 10.2.1.1 on the corporate side of a network behind REM-CE3. CE4 connects to the Internet gateway by way of an access technology (dial, digital subscriber line [DSL], or cable).
2. When the packet reaches CE4, CE4 performs a route lookup for the destination address and then determines the outbound interface through which to send the packet.
3. After determining the outbound interface, CE4 checks for all the features defined on the outbound interface; this includes a crypto map check.
4. CE4 determines crypto map is configured on the egress interface and identifies the Security Policy Database (SPD) for the crypto entry.
5. CE4 determines from SPD that this traffic is interesting (meaning that it should be protected).
6. CE4 determines if existing SA in the SADB covers this policy.

**Note** If there is no Security Association, CE4 initiate an IKE exchange to the IPSec-Agg PE to negotiate transforms and their corresponding proposals.

7. CE4 sends IKE SA offer (des, sha, D-H Group, lifetime). ISKAMP Phase 1, Main mode begins.

8. IPSec-Agg PE returns policy match accepting offer.
9. CE4 initiates D-H and Nonce (i) exchange to IPSec-Agg PE.
10. IPSec-Agg PE responds to CE4 with D-H and Nonce (r) exchange.
11. CE4 authenticates D-H Apply sha hash (bidirectional IKE SA established).
12. IPSec-Agg PE authenticates D-H Apply sha hash (bidirectional IKE SA is established. ISKAMP Phase 1, Main mode ends.

**Note** After  is established (that is, IKE SAs are established), the IPSec session maps to the VRF.

13. CE4 sends IPSec offer (transform, mode, lifetime, authen). ISKAMP Phase 2, Quick Mode begins.
14. IPSec-Agg PE identifies policy match and accepts offer.
15. If PFS (perfect forward secrecy) is enabled, CE4 initiates a new D-H exchange to generate new Keying Material (KEYMAT).
16. IPSec-Agg PE initiates D-H exchange or refresh key for IPSec. Unidirectional SA is established; ISKAMP Phase 2, Quick mode ends.

**Note** Routing updates can be exchanged with the CE4 if GRE tunnels are configured for that purpose. Otherwise, static routes corresponding to the remote LAN must be defined in the VRF.

17. IPSec SAs are associated with the VRF in the SADB table; CE4 transmits packets using SA associated with the egress interface.
18. IPSec-Agg PE checks incoming encrypted packets for decryption and the encryption SA is found. IPSec-Agg PE decrypts the packet and places it in the VRF associated with the SA.
19. IPSec-Agg PE selects an MPLS label for the address of the remote site (10.1.1.1).
20. IPSec-AGG PE advertises the route to REM-PE.
21. CE3 receives the route advertisement and installs the route to 10.1.1.1.
22. IPSec-AGG PE sends the data to CE3 through MPLS using previously learned label for 10.2.1.1.

# Sequence of Operations—Remote Access Connection

The client connection is very similar, however the Unity client negotiates SAs differently. The following provides typical connection sequences for remote access (see Figure 2-7).

1. For remote access, a user/client (for example, 170.20.1.1) sends packets (for transfer to main office or to another site) by way of an access technology [dial, digital subscriber line (DSL), or cable].
2. User/client launches custom-installed VPN client and uses a predefined server profile for IPSec-VPN connectivity.
3. DNS resolves server name to a public IP address.
4. Client sends IKE SA offer (des, sha, D-H Group, lifetime). ISKAMP Phase 1, Main mode begins.
5. IPSec-Agg PE returns policy match.
6. Client initiates D-H exchange to IPSec-Agg PE.
7. IPSec-Agg PE responds to client with D-H exchange.

8. Client authenticates D-H Apply sha hash (bidirectional IKE SA established).
9. IPSec-Agg PE authenticates D-H Apply sha hash. The bidirectional IKE SA is established; ISKAMP Phase 1, Main mode ends. IPSec-Agg PE associates IKE SA with the VRF defined in the profile.
10. At user/client, XAUTH prompts for user name and password and forwards to IPSec-Agg PE.
11. IPSec-Agg PE sends authentication request to RADIUS server.
12. RADIUS server accepts (or rejects) request and notifies IPSec-Agg PE.
13. Client requests Mode-Config from IPSec-Agg PE.
14. IPSec-Agg PE sends authorization request to RADIUS server (or provides requested info to client).
15. RADIUS server (or IPSec-Agg PE) provides Mode-Config info to client.
16. Client sends IPSec offer (transform, mode, lifetime, authen). ISKAMP Phase 2, Quick Mode begins.
17. IPSec-Agg PE identifies policy match and accepts offer.
18. Client initiates D-H exchange or refresh key for IPSec.
19. IPSec-Agg PE initiates D-H exchange or refresh key for IPSec. Unidirectional SA established; ISKAMP Phase 2, Quick Mode ends.
20. CE4 transmits packets using SA associated with the egress interface.
21. IPSec-Agg PE checks incoming encrypted packets for decryption and locates the encryption SA. The IPSec-Agg PE decrypts the packet and places it in the VRF associated with the SA.
22. IPSec-Agg PE selects an MPLS label for the address of the remote site (10.1.1.1).
23. IPSec-AGG PE advertises the route to REM-PE.
24. CE3 receives the route advertisement and installs the route to 10.1.1.1.
25. IPSec-AGG PE sends the data to CE3 through MPLS using a previously learned label for 10.2.1.1.


# Planning Issues and Decisions

## IPSec Overview

For general information about IPSec, see http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/vpnsc/ipsec/2_0/prov_gd/ipsecpg1.htm.

## Deployment Information

For information on deploying IPSec VPNs, see http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/depip_wp.htm.

## Standards and Specifications

For information on standards and specifications, see http://www.cisco.com/pcgi-bin/Support/browse/psp_view.pl?p=Internetworking:IPSec&s=Overview#Standards_and_Specifications.

## Network-Based IPSec VPN Solution Planning

Keep the following issues in mind when planning the solution:

- Use of domain name—Use a domain name in the IPSec endpoint definition on the VPN clients instead of IP addresses. You can then use DNS to resolve the domain names into IP address before IPSec session creation.

  Using domain names allows flexibility in deployments because no changes are required on the clients if any changes are made on the server side (server IP address, additional server added that must be resolved to different IP addresses, and load balancing among servers based on DNS resolution).

- AAA setup—You (service provider) can set up RADIUS so that it conforms to your own and to your enterprise customers' existing AAA structure. We recommend two ways to implement AAA:
  - Proxy AAA—Your AAA can perform the user authentication while the authorization request can be proxied to the customer AAA server.

**Note** The customer AAA server must be reachable through the global routing table.

  - VRF aware AAA—Send the authorization and the authentication requests directly to the customer AAA server on a per VRF basis.

- Route summarization—RRI installs a route to the IP address assigned to the client in the VRF routing table. The route would usually be in the customer address range, but it must be advertised to the other PEs that are part of the VPN. It is advisable to define the address pools along summarizable boundaries. Instead of advertising each and every individual RRI installed route, only advertise a summary route into the VPN (this reduces the routing protocol overhead and the routes that a VRF handles).
- Split tunneling—The VPN clients normally connect to the server over the Internet; after connecting, you have the option to:
  - restrict their Internet access by forcing all the traffic over the IPSec tunnel or
  - allowing it to continue using its existing Internet connection for non-VPN related traffic (split tunneling)

  You can send the access-list to separate the VPN traffic to the client during Mode-Config. The decision to enable/disable split tunneling is usually based on the policies and service agreements of the service provider and customer.

**Note** Most enterprise customers would like to disable split tunneling, thereby forcing all traffic, even non-VPN related, to the central site. This allows the enterprise to have greater control over client communication and to force all Internet traffic through a firewall to protect the enterprise's internal network.

- If split tunneling is enabled, the enterprise customer can potentially open up its networks to external attacks. If the customer has a service agreement with you (the service provider) to provide direct Internet services, then the split tunneling would be disabled and you (the service provider) would provide Internet services.
- Default route—For IKE/IPSec completion, the tunnel endpoint reachability needs to be available in the global or the VRF routing table.

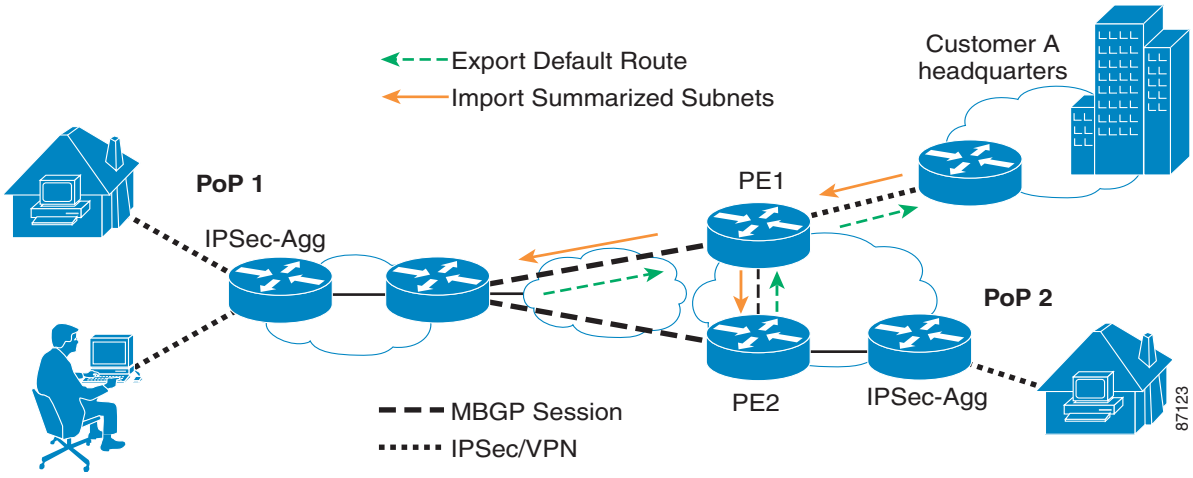
**Note** For almost all deployment models in the network-based IPSec VPN solution the outbound interface is global. However, if you choose to, you can place the outbound interface in a VRF.

  - For global reachability, a default route in the global routing table needs to be injected; this should not be a issue in most deployments as the server would need some form of Internet connectivity for the clients and the sites to connect to it.
  - The endpoint reachability in the VRF table can pose challenges. The easiest implementation is to have a default route in each of the VRFs pointing out the interface on which the clients connect. This may not be possible or desirable in many situations.

- If split tunneling is disabled, then all the traffic needs to be forwarded to the enterprise hub site. The easiest way to accomplish this would be for the hub site to distribute a default route to its PE which would then be propagated to the rest of the PEs in the VPN network.

Figure 3-1 shows one possible implementation that manipulates the VRF route export/import policies in BGP.

*Figure 3-1 Possible Default Route Implementation*




If customer A belongs to a certain VPN and if split tunneling is disabled on the clients, then all the traffic going to the Internet is forwarded to the company hub site. Customer A's hub router advertises a default route to the PE1. The MBGP route export policies on PE1 are defined in such a way that only the default route is advertised to the other PEs (PE2 and PE3 in this case). The route targets on PE2 and PE3 are set in such a way that they import PE1 routes only (default route). PE2 and PE3 in turn export aggregate subnets to the PE1 only. These subnets are in turn advertised into the IGP running between the Company A hub router and PE1. In effect, all the traffic is forwarded to the company hub site which can control user policies and apply services such as firewall.

# Scalability, Capacity Planning, and Performance

The Cisco 7204 and 7206 routers are the only supported platforms in Cisco network-based IPSec VPN solution Release 1.5. Keep in mind the following factors when deploying the solution:

- Total number of tunnels; distinguish between site-to-site and client tunnels.
- Peak number of tunnels that will be serviced.
- Number of VRFs.
- Number of routes per VRF from remote PEs and from remote sites (if performing dynamic routing).
- Whether you will load balance or provide redundancy.

  Load balancing can be accomplished by:

  - Manually distributing the VRFs across multiple boxes.
  - Using multiple HSRP groups, which will also provide redundancy.
  - Using fully-qualified domain names to resolve domain names into IP addresses. The DNS server can load balance the incoming request across different boxes.

# Security Policies

When defining and installing security policies for the Cisco network-based IPSec VPN solution Release 1.5, consider the following:

- Firewalls—Although not part of the solution, it is assumed that firewalls are installed and used on both your own (service provider) network and the customer network. You should have a firewall at the Internet entry/exit point to protect your network and the customers it services. In most cases you should disable split tunneling on the clients so that all traffic, including non-VPN traffic, is forwarded to the customer hub site. This allows the customer firewall to process all incoming traffic thereby protect the customer network from external attacks.
- Access lists—To further protect the IPSec server, define access lists on the outgoing interfaces of the router connected to the server (towards the Internet) to restrict the traffic to IKE and IPSec.
- AAA—To deny unauthorized access, use XAUTH to authenticate the VPN clients. We also recommend that you use advanced password generation methods such as secure ID during authentication.

**Note** When using the proxy AAA method for user authorization, the customer AAA server needs to be accessible through the global routing table for proxy function successfully.

- Route import/export policy—In the MPLS VPN scenario, PEs exchange VPN routes based on the route export/import policies configured under each VRF. Potential configuration errors (for example, incorrect route descriptors) could lead to cross-VRF route export/import that can compromise the VPNs.

**Note** Be sure to verify the configuration before applying any changes to the network.


# Planning for IPSec Remote Access

Revised December 14, 2005

## IPSec Remote Access Overview

With IPSec remote access, mobile workers and single client locations can connect to a specific VPN using a software client by referring to a fully qualified domain name or FQDN that is associated with a single or set of IPSec PEs serving that specific VPN. Remote access requires a software bundle (or client) to communicate with the edge of the VPN.

The Cisco network-based IPSec VPN solution Release 1.5 uses RADIUS to support IPSec remote access to network-based VPNs and to provide the information necessary to establish the IKE connection as well as the session with the remote access user.

**Note** IPSec remote access requires one access-request for IKE (authorization) and another for XAUTH+MODE-CFG (authentication).

The infrastructure supporting IPSec remote access is allocated to a distinct set of resources called the IPSec service module. Each IPSec service module supports a distinct set of VPNs and their associated users. For new customers, you must invoke assignment logic to associate customers with a specific IPSec service module.

Assignments are followed by reduction in inventory for a given IPSec service module, configuration of customer specific VRF, establishment of RADIUS infrastructure, and finally documentation of VPN topology/engineering information.

# Required Information for Implementing Remote Access

The following information is necessary to successfully implement IPSec remote access for the Cisco network-based IPSec VPN solution Release 1.5:

- Forecast of subscribers in month 0, 6, 12, and 24.
- Percentage of subscribers active at peak.
- The average IPSec tunnel speed (initially, the speeds will be unconstrained).
- Number of routes in the customer's network (information should encompass all routes for a given customer network).

Consider this information algorithmically (against IPSec server module capacity) to assign the customer to the appropriate service module and to reduce the capacity of the selected service module by the appropriate amount of resources the customer is expected to consume.

## VPN Topology

Remote access users must identify the desired VPN topology type. In the case of hub and spoke, the remote access user must identify the sites designated as a hub.

## AAA Management

Remote access users need to identify the following AAA configuration options:

### Managed AAA

In a managed AAA configuration, a service provider hosts a RADIUS system that administers user information specific to a remote access user. The remote access user must designate one or more administrators that will be responsible for user administration. The remote access user must provide contact information and initial user-id/password for each administrator. After administrators are configured, the remote access user can add, delete, modify, and view users without the intervention of service provider.

### Proxy AAA

The service provider performs authorization while the remote access user controls user authentication. Proxy AAA is the only configuration that supports two-factor authentication (also called token card). In the case where a remote access user is managing his own AAA system, the remote access user must identify one or more IP addresses associated with the remote access user’s AAA system. In addition to IP addresses:

- A shared secret must be configured on both ends of the proxy (service provider and remote access user).
- The shared secret must be communicated.
- The shared secret should be a well-formed password.

### 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 Virtual Home Gateway (VHG) 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 do not need to proxy AAA to provide their customers with the flexibility they demand.

## Preshared Key

A preshared key is used for the client PE IKE security association (SA). There is one preshared key for each group name. The group name is the IKE ID that binds it to the preshared key. The preshared key is loaded into RADIUS for device authentication and integrated with software clients. Software client distribution must be addressed along with key generation.

We recommend that client software along with patches/upgrades for customer be distributed from a web page maintained by the service provider. After preshared key assignment, the software for each remote access user has the preshared key bundled with the software when the software is downloaded. This process must be validated by security.

## User Password Options

Authentication of users can be implemented using simple user passwords or RSA SecurID based two-factor authentication passwords. Remote access users that require two-factor authentication passwords must use Proxy AAA.

**Note** SecurID is supported only in proxy mode and not in native mode.

## Address Pools

The remote access user must provide addresses to use as address pools for dynamic assignment to clients. The remote access user must also provide address space for use by the service provider to assign addresses to connecting clients. An algorithm or policy is necessary so that the number of peak users over time is considered along with the IPSec service module configuration to generate the appropriate address space requirement for a specific remote access user.

## Internet Access Method

To support troubleshooting, the remote access user should provide information describing the Internet access methods that clients use to access the IPSec service module.

## Domain Name

Consistent with the format user%service@domain, the remote access user must specify a unique domain name used to make certain that clients are unique. This domain name determines the domain of authority relative to user authentication (proxy or service provider hosted). If you are defining multiple users in multiple groups on the VPN 3000 series concentrator, you must enable group lock to prevent users in one group from logging in with another group's parameters. For information on group lock, see http://www.cisco.com/warp/public/471/altigagroup.html.

# IPSec Infrastructure Provisioning

In addition to the required information, router configuration information is necessary to provision the infrastructure for a specific customer (this assumes basic infrastructure provisioning is complete):

- VRF name
- Route distinguisher (should be generated by an algorithm)
- Route targets for import/export
- Routing policy—Required to assure address pools are exposed.
- IPSec policy—All customers have the same policy. Configuration arguments must be loaded into the new customer VRF.

# Remote Access IPSec Configuration Example

The following configuration example shows relevant service-related configuration required for remote access users activation on an ITR. Customer 'Coke' is used for example purposes only. Customer-specific routing is not shown.

For information on the Cisco IOS software commands used below, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm.

**Note** Download group parameters from RADIUS during device authorization. The parameters are not configured on the router.

**Step 1** Configure the AAA group list for the new customer pointing to RADIUS for authentication as well as authorization.

```
aaa authentication login coke-ra radius
aaa authorization network coke-ra radius
```

**Step 2** Configure the VRF including route descriptor and the export/import route targets.

```
ip vrf coke
 rd 1:101
 route-target export 1:101
 route-target import 1:101
```

**Step 3** Configure ISAKMP policy for Phase 1 if it is different from the existing policies or does not exist.

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

**Step 4** Configure the remote access profile.

```
crypto isakmp profile coke-ra
   vrf coke
   match identity group coker-ra
   client authentication list coke-ra
   isakmp authorization list coke-ra
   client configuration address respond
```

**Step 5** Configure the transform set if it is different than the existing ones or does not exist.

```
crypto ipsec transform-set tset esp-des esp-md5-hmac
```

**Step 6** Configure the dynamic map for remote access clients

```
crypto dynamic-map coke-ra 1
 set transform-set tset
 reverse-route
set isakmp-profile-coke-ra
```

**Step 7** Apply the dynamic map as well as the isakmp profile to the crypto map.

```
crypto map vpn 1 ipsec-isakmp dynamic coke-ra
```

**Step 8** Configure the address pool corresponding to the customer.

```
ip local pool coke-ra 192.168.1.1 192.168.1.254
```

**Step 9** Assuming that the BGP PE configuration is already configured, add the customer-specific address-family configuration. Optional route maps can be applied to filter any routes.

```
address-family ipv4 vrf coke
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 aggregate-address 192.168.1.0 255.255.255.0 summary-only
 exit-address-family
```


# Planning for IPSec Site-to-Site Access

## IPSec Site-to-Site Access Overview

With IPSec site-to-site access, single sites that require access to a specific VPN use a Cisco IOS software peer protocol to connect to a specific VPN. Each remote site must be preconfigured with IPSec access configuration information to communicate with the edge of the VPN.

Sites refer to remote locations that must perform dynamic routing; you need to configure a GRE tunnel for each site.

The infrastructure supporting IPSec remote access is allocated to a distinct set of resources called the IPSec service module. Each IPSec service module supports a distinct set of VPNs and their associated users. For new customers, you must invoke assignment logic to associate the customers with a specific IPSec service module.

Assignments are followed by reduction in inventory for a given IPSec service module, configuration of customer specific VRF, establishment of RADIUS infrastructure, and finally documentation of VPN topology/engineering information.

Because the site-to-site model has a different set of requirements in terms of routing, bidirectional tunnel initiation, and the ability to shape/police the individual tunnels, we recommend having separate clusters

In most cases these would be nailed-up connections that should be provisioned for redundancy. One way to accomplish redundancy is to create two GRE tunnels per remote site to different clusters.

## Required Information for Implementing Remote Access

The following information is necessary to successfully implement IPSec remote access for the Cisco network-based IPSec VPN solution Release 1.5:

- Forecast of subscribers in month 0, 6, 12, and 24.
- Percentage of subscribers active at peak.
- The average IPSec tunnel speed (initially, speeds are unconstrained).
- Number of routes in the customer's network (information should encompass all routes for a given customer network).

Consider this information algorithmically (against IPSec server module capacity) in order to assign the customer to the appropriate service module and to reduce the capacity of the selected service module by the appropriate amount of resources the customer is expected to consume.

This section describes information that you must consider:

- VPN Topology—Users must identify the desired VPN topology type (fully meshed or hub and spoke). In the case of hub and spoke, the remote access user must identify the site(s) designated as a hub.
- Preshared Key—A preshared key is used for the client PE IKE security association (SA). There is one preshared key for each site.
- GRE Parameters and Routing Protocol—You must determine and supply GRE tunnel addressing as well as the tunnel destination (from the perspective of the PE). You must run a routing protocol between the sites and the PE. You (service provider) should select the routing protocol to maintain consistency within the network and to allow for easier management.
- Bandwidth Per Site—You can use traffic policing [Modular QoS Command-line interface (MQC) and committed access rate (CAR)] on a per site basis to restrict bandwidth. This may not be part of current service offering.

# IPSec Infrastructure Provisioning

The following information is necessary to provision the infrastructure for a specific customer (this assumes basic infrastructure provisioning is complete):

- VRF name
- Route distinguisher (should be generated by an algorithm)
- Route targets for import/export
- Routing policy—Required to assure address pools are exposed.

IPSec policy—All customers have the same policy. Configuration arguments must be loaded into the new customer's VRF.

**Note** The configuration for site-to-site clusters should be made in tandem with the remote access client clusters to maintain connectivity within the VPN.

# Site-to-Site IPSec PE Configuration

See the *Cisco Network-Based IPSec VPN Solution Release 1.5 Implementation Guide* for examples of GRE tunnel configurations.


## A



## C



## D



## E



## H

## I



## M



## N



## O



## P



## Q



## R

## S



## T



## U



## V