Deploying **IPsec** Virtual Private Networks

Introduction

Corporate networks connected to the Internet can enable flexible and secure VPN access with IPsec. Connecting remote sites over the Internet provides a great cost saving opportunity when compared to the traditional WAN access such as Frame Relay or ATM. With IPsec technology, customers now can build Virtual Private Networks (VPNs) over the Internet with the security of encryption protection against wire taping or intruding on the private communication.

This deployment guide provides multiple designs for the implementation of IPsec VPN configurations over public Internet infrastructure. The IPsec VPN configurations presented in this document are based on recommended customer configurations. These configurations were tested and verified in a lab environment and can be deployed in the field. This guide does not discuss alternate IPsec VPN implementation solutions.

This deployment document describes basic design and deployment of an IP VPN network on top of a public network infrastructure. It does not detail the general operation of the protocols associated with deployment, such as Internet Key Exchange (IKE), Digital Encryption Standard (DES), nor does it discuss the management and automation aspect for service provisioning.

This document contains the following IPsec designs:

- Site-to-Site VPN
  - Fully-meshed VPN
  - Hub-and-spoke VPN
  - Fully-meshed on-demand VPN with Tunnel Endpoint Discovery
  - Dynamic Multipoint VPN
- Remote Access VPN
  - Cisco Easy VPN

IPsec VPN Definition

IPsec VPN is an Enterprise Network deployed on a shared infrastructure using IPsec encryption technology. IPsec VPNs are used as an alternative to Wide Area Network (WAN) infrastructure that replace or augment existing private networks that utilize leased-line or Enterprise-owned Frame Relay and Asynchronous Transfer Mode (ATM) Networks. IPsec VPNs do not inherently change WAN requirements, such as support for multiple protocols, high reliability, and extensive scalability, but instead meet these requirements more cost-effectively and with greater flexibility.

An IPsec VPN utilizes the most pervasive transport technologies available today: the public Internet, SP Internet Protocol (IP) backbones, and also SP Frame Relay and ATM networks. IPsec. The equipment deployed at the edge of the Enterprise network and feature integration across the

WAN primarily define the functionality of an IPsec VPN, rather than definitions by the WAN transport protocol.

IPsec VPNs are deployed in order to ensure secure connectivity between the VPN sites. The VPN sites can be either a subnet or a host residing behind routers. Following are key components of this IPsec VPN designs:

- Cisco high-end VPN routers serving as VPN head-end termination devices at a central campus (head-end devices)
- Cisco VPN access routers serving as VPN branch-end termination devices at the branch office locations (branch-end devices)
- IPsec and GRE tunnels that interconnect the head-end and branch-end devices in the VPN
- Internet services procured from a third-party ISP serving as the WAN interconnection medium

Major Components

Internet Key Exchange (RFC 2409)

IPsec offers a standard way to establish authentication and encryption services between endpoints. This includes both standard algorithms and transforms, but also standard key negotiation and management mechanisms (via ISAKMP/Oakley) to promote interoperability between devices by allowing for the negotiation of services between these devices.

IKE is a key management protocol standard that is used in conjunction with the IPsec standard. It enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard. It enables automatic negotiation of IPsec security associations, enables IPsec secure communications without costly manual preconfiguration, and facilitates secure exchange of encryption keys.

Negotiation refers to the establishment of policies or Security Associations (SAs) between devices. An SA is a policy rule that maps to a specific peer, with each rule identified by a unique SPI (Security Parameter Index). A device may have many SAs stored in its Security Association Database (SADB), created in DRAM and indexed by SPI. As an IPsec datagram arrives, the device will use the enclosed SPI to reference the appropriate policy that needs to be applied to the datagram.

IKE is a form of ISAKMP (Internet Security Association Key Management Protocol)/Oakley specifically for IPsec. ISAKMP describes the phase of negotiation; Oakley defines the method to establish an authenticated key exchange. This method may take various modes of operation and is also used to derive keying material via algorithms such as Diffie-Hellman.

ISAKMP Phase 1 is used when two peers establish a secure, authenticated channel with which to communicate. Oakley main mode is generally used here. The result of main mode is the authenticated bi-directional IKE Security Association and its keying material. ISAKMP Phase 2 is required to establish SAs on behalf of other services, including IPsec. This uses Oakley Quick Mode to generate key material and/or parameter negotiation. The result of Quick Mode is two to four (depending on whether AH and/or ESP was used) uni-directional IPsec Security Associations and their keying material.

IPsec

IPsec combines the aforementioned security technologies into a complete system that provides confidentiality, integrity, and authenticity of IP datagrams. IPsec actually refers to several related protocols as defined in the new RFC 2401-2411 and 2451 (the original IPsec RFCs 1825-1829 are now obsolete). These standards include:

- IP Security Protocol proper, which defines the information to add to an IP packet to enable confidentiality, integrity, and authenticity controls as well as defining how to encrypt the packet data.
- Internet Key Exchange (IKE), which negotiates the security association between two entities and exchanges key material. IKE usage is not necessary, but it is difficult and labor-intensive to manually configure security associations. IKE should be used in most real-world applications to enable large-scale secure communications.

IPsec Modes

IPsec has two methods of forwarding data across a network: transport mode and tunnel mode. Each differs in their application as well as in the amount of overhead added to the passenger packet. These protocols are summarized briefly in the next two sections:

- Tunnel Mode
- Transport Mode

Tunnel Mode

Tunnel Mode encapsulates and protects an entire IP packet. Because tunnel mode encapsulates or hides the IP header of the packet, a new IP header must be added in order for the packet to be successfully forwarded. The encrypting routers themselves own the IP addresses used in these new headers. Tunnel mode may be employed with either or both ESP and AH. Using tunnel mode results in additional packet expansion of approximately 20 bytes associated with the new IP header. Tunnel mode expansion of the IP packet is depicted in Figure 1.

Figure 1
IPsec Tunnel Mode

IP HDR	Data

| New IP HDR	IPsec HDR	IP HDR	Data

To Be Protected
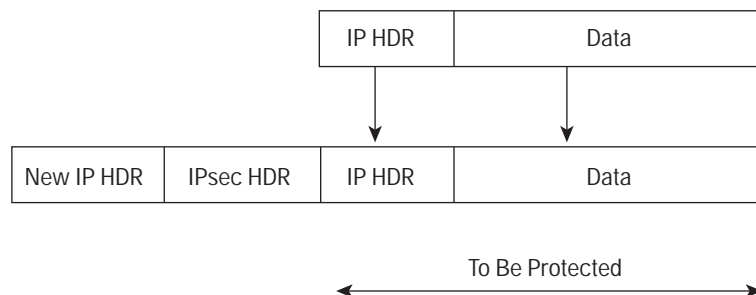
Transport Mode

Use transport mode only when using GRE tunnel for the VPN traffic.

IPsec transport mode inserts an IPsec header between the IP header and the GRE Header. In this case, transport mode saves an additional IP header, which results in less packet expansion. Transport mode can be deployed with either or both ESP and AH. Specifying transport mode allows the router to negotiate with the remote peer whether to use transport or tunnel mode. Transport mode expansion of the IP packet with GRE encapsulation is depicted in Figure 2.

Figure 2

IPsec Transport Mode with GRE

IP HDR	Data

New IP HDR	IPsec HDR	GRE	IP HDR	Data

To Be Protected
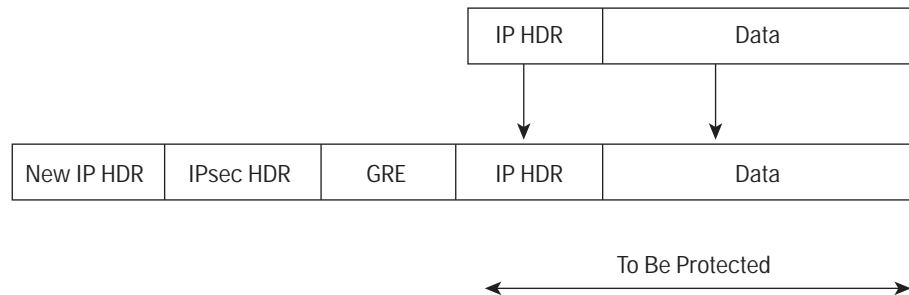
IPsec Headers

IPsec defines a new set of headers to be added to IP datagrams. These new headers are placed after the outer IP header. These new headers provide information for securing the payload of the IP packet as follows:

- *Authentication Header (AH)*—This header, when added to an IP datagram, ensures the integrity and authenticity of the data, including the invariant fields in the outer IP header. It does not provide confidentiality protection. AH uses a keyed-hash function rather than digital signatures, because digital signature technology is slow and would greatly reduce network throughput.

- *Encapsulating Security Payload (ESP)*—This header, when added to an IP datagram, protects the confidentiality, integrity, and authenticity of the data. If ESP is used to validate data integrity, it does not include the invariant fields in the IP header.

While AH and ESP can be used either independently or together; just one of them will suffice for most applications. For both of these protocols, IPsec does not define the specific security algorithms to use, but rather provides an open framework for implementing industry-standard algorithms. Initially, most implementations of IPsec will support MD5 from RSA Data Security or the Secure Hash Algorithm (SHA) as defined by the U.S. government for integrity and authentication. The Data Encryption Standard (DES) is currently the most commonly offered bulk encryption algorithm, although RFCs are available that define how to use many other encryption systems, including IDEA, Blowfish, and RC4.

Using these IKE and IPsec, this paper will provide a detailed guidelines for implementing the following scenarios:

- Fully meshed VPNs
- Hub and spoke VPN
- Fully-meshed on-demand VPN with Tunnel Endpoint Discovery
- Dynamic Multipoint VPN
- Cisco Easy VPN

1. Implementing Fully Meshed VPN

This section describes the implementation of IPsec configuration necessary to enable full mesh VPN connectivity across public IP infrastructure. It contains the following subsections:

- Strategy
- Network Topology
- Benefits
- Limitations
- Prerequisites
- Configuration Task List
- Summary

Fully Meshed VPN Configuration Strategy

The Site-to-Site design refers to a mesh of IPsec tunnels connecting between remote sites. For any to any connectivity, a full mesh of tunnels is required to provide path between all the sites. Site-to-Site VPNs are primarily deployed to connect branch office locations to the central site of an enterprise.

In this configuration, the IPsec peers utilize public IP addresses to establish the IPsec tunnels. The public IP addresses are specified in the IPsec peers configuration, and require that the public addresses of the VPN routers to be static addresses. The VPN site addresses however could be private or public addresses, since the site traffic is encrypted before entering the IPsec tunnels.

Fully Meshed VPN Network Topology

The IPsec VPN design used in this solution document is for an Enterprise network connecting many remote sites to the Internet with a range of link speeds. Figure 3 shows the IPsec tunnel between large and medium in which IPsec VPN connectivity is deployed.

Note: The solutions presented in this document are based on an example customer environment. All the IP addresses and configuration in this document are provided for illustrative purposes only.

Figure 3

Network Diagram: Fully Meshed VPN
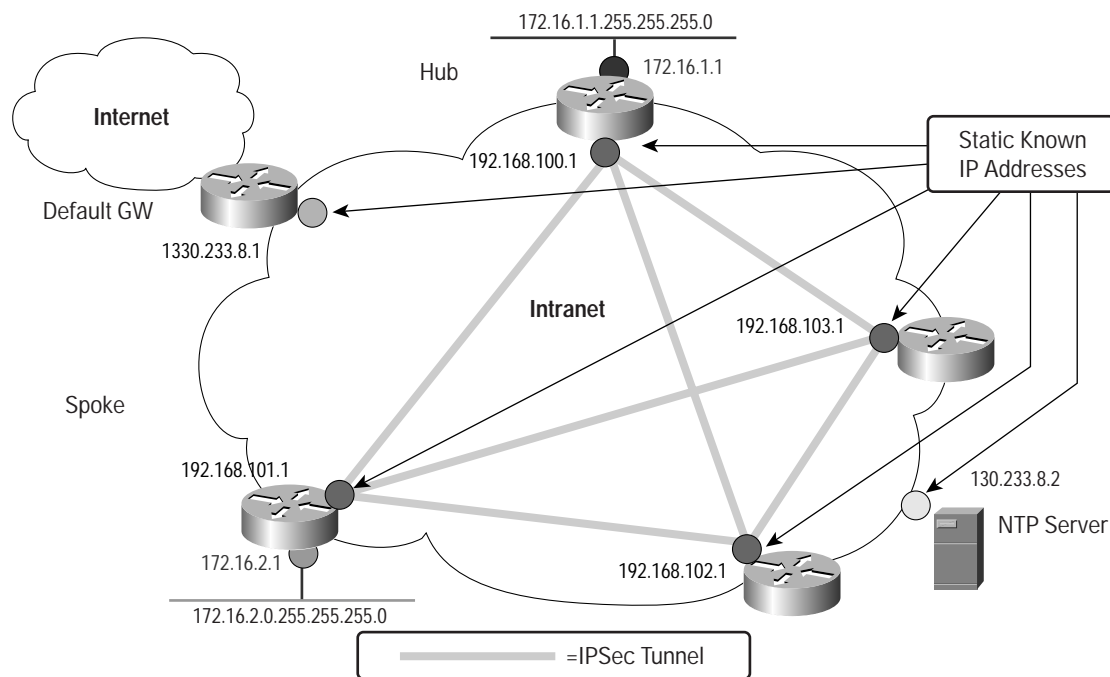
Fully Meshed VPN

- *Robust and simple* design/configuration procedure for adding new sites.
- *Simple to automate* with Cisco Network Management and Provisioning (NMP) system, using applications such as VPN Solution Center.
- *Reduce WAN Costs, Increase WAN Flexibility:* Using Internet transport, VPNs cut recurring WAN costs compared to traditional WAN technologies, including as Frame Relay. Unlike Frame Relay, VPNs can easily and quickly extend to new locations and "extranet" business partners.
- *Deliver New, Revenue-Enhancing Applications via VPNs:* VPNs enable secure use of cost-effective, high-speed links (i.e.: DSL) to deliver such revenue-generating applications as in-store online catalogs, ordering, and efficiency tools.
- *Increase Data and Network Security:* Traditional WANs use Frame Relay, leased lines, or ATM to provide traffic segregation, but they do not transport security. VPNs encrypt and authenticate traffic traversing the WAN to deliver true network security in an insecure, networked world.

Fully Meshed VPN

- All sites must have static IP addresses for IPsec peering
- When adding a new site, all other routers have to be re-configured in order to add the new site.

The scalability of this design is to the power of two.

Fully Meshed VPN Prerequisites

Before implementing Fully Meshed VPNs, the network must meet the following requirements:

- IP address allocation plan
- Using static global addresses for the connectivity to the Internet
- Cisco IOS Software Release 12.0 or later.

Fully Meshed VPN Configuration Task List

There are a number of configuration items that must be enabled to implement IPsec configuration. The general steps are as follows:

1. Configure IKE policy
2. Configure IPsec Transforms and protocol
3. Create Access Lists for Encryption
4. Configure Crypto Map
5. Apply Crypto Map on the interface

Step 1: Configure IKE policy

IKE is a protocol used to automatically negotiates the security parameters, authenticate identified, secure and establish an agreement between IPsec routers. Multiple IKE policies can be defined between two IPsec peers, however there must be at least one matching IKE policy between them to establish the IPsec tunnels.

To configure an IKE policy, use the following commands, beginning in global configuration mode:

```
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  crypto isakmp key bigsecret address 192.168.101.1 255.255.255.0
```

The preshared key is used to identify and authenticate the IPsec tunnel. The key can be any arbitrary alphanumeric key up to 128 characters long—the key is case-sensitive and must be entered identically on both routers. The previous configuration uses a unique preshared key that is tied to a specific IP address.

Alternatively, in the following section, a wild card preshared key is used to simplify the configuration. The wild card preshared key is not associated with any unique information to determine its peer's identity. When using a wild card preshared key, every member of a crypto policy uses the same key.

When connecting to another vendor's device, manual-keying configuration might be necessary to establish IPsec tunnel. If IKE is configurable on both devices, it is preferable to using manual keying. For a sample on configuring manual keying, please visit: http://www.cisco.com/warp/public/707/manual.shtml

Alternatively, IKE can be configured between the IPsec routers using digital certificates. The IKE policy can be configured with manually with RSA keys for the routers (Reference 9), or using Certificate Authority (CA) Server (Reference 10). Using preshared authentication keys works for networks of up to 10 or so nodes, but larger networks should use RSA public key signatures and digital certificates.

Reference9:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt4/scdike.htm#xtocid16

Reference10:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fipsenc/scfinter.htm

Step 2: Configure IPsec Transforms and Protocols

A transform set represents a certain combination of security protocols and algorithms. During IKE negotiation, the peers agree to use a particular transform set for protecting data flow.

During IKE negotiations, the peers search in multiple transform set for a transform that is the same at both peers. When such a transform set is found, it is selected and applied to the protected traffic as a part of both peers' configurations.

To configure an IKE policy, use the following commands, beginning in global configuration mode:

```
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
```

With manually established security associations, there is no negotiation with the peer and both sides must specify the same transform set.

Step 3: Create Access Lists for Encryption

Access lists define what IP traffic will be protected by crypto. Extended access list are used to specify further source and destination addresses and packet type.

The access list entries must mirror each other on the IPsec peers. If access list entries include ranges of ports, then a mirror image of those same ranges must be included on the remote peer access lists.

To create an access Lists, use the following commands, beginning in global configuration mode:

```
ip access-list extended vpn-static1
  permit 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
```

The address range in the access list represents the traffic on the local segment at each router. Any unprotected inbound traffic that matches a permit entry in the access list will be dropped, because it was expected that IPsec would protect this traffic.

Additionally, the default behavior allows the rest of the traffic to be forwarded with no encryption, and it is called split tunneling. Refer to additional configuration steps for configuring firewall protection with split tunneling. Alternatively, in order to provide the local segment with firewall protection, all traffic from the remote segment can be forwarded to a central site equipped with secure Internet access. To disable split tunneling and forward Internet traffic to a head end router, use a default access list as following:

```
ip access-list extended vpn-static1
  permit host 172.16.1.0 0.0.0.255.0 any
```

Step 4: Configure Crypto Map

The crypto map entry ties together the IPsec peers, the transform set used and the access list used to define the traffic to be encrypted. The crypto map entries are evaluated sequentially.

In the example below, the crypto map name static-map and crypto map numbers are locally significant. The first statement sets the IP address used by this peer to identify itself to other IPsec peers in this crypto map. This address must match the set peer statement in the remote IPsec peer crypto map entries. This address also needs to match the address used with any preshared keys the remote peers might have configured. The IPsec mode defaults to tunnel mode.

```
crypto map static-map local-address FastEthernet1/0
crypto map static-map 1 ipsec-isakmp
    set peer 192.168.101.1
    set transform-set vpn-test
    match address vpn-static1
```

A more complete description can be found at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/fipsencr/srfipsec.htm#xtocid5

Step 5: Apply Crypto Map on the interface

The crypto maps must be applied to each interface through which IPsec traffic will flow.

To apply crypto map on an interface, use the following sample commands, beginning in global configuration mode:

```
interface FastEthernet1/0
    ip address 192.168.100.1 255.255.255.0
     crypto map static-map
```

Applying the crypto map to the physical interface instructs the router to evaluate all the traffic against the Security Associations Database. With the default configurations, the router is providing secure connectivity by encrypting the traffic sent between the remote sites. However, the public interface still allows the rest of the traffic to pass and provide connectivity to the Internet. To create privacy of the remote sites or secure connectivity to the Internet, refer to the following Additional Configuration Steps section.

The address used on the outbound interface is configured manually in the router configuration and in the remote peers configuration for enable encryption configurations. This address cannot be changed dynamically without affecting the connectivity or the configurations in the peer routers.

Note: To create the full mesh configuration between multiple sites, repeat the previous steps between every router pairs.

Additional Configuration Steps

Using GRE Tunneling

Alternatively, traffic to be encrypted could be forwarded onto a GRE interface, which would be configured to use IPsec encryption. Packets forwarded by the GRE interface would be encapsulated and routed out onto the physical interface. Using GRE interface, the two routers can support dynamic IP routing protocol to exchange routing updates over the tunnel, and to enable IP multicast traffic. However, when using IPsec with GRE, the access list for encrypting

traffic does not list the desired end network and applications, but instead it refers to permit the source and destination of the GRE tunnel on the outbound direction. Without further ACL on the tunnel interface, this configuration will allows for all packets forwarded to the GRE tunnel to get encrypted.

To enable IPsec onto a GRE tunnel, use the following command, beginning in global configuration mode:

```
interface tunnel1
  ip address 10.62.1.193 255.255.255.252
  tunnel source FastEthernet1/0
  tunnel destination 192.168.101.1
  crypto map static-map
```

Notice that the crypto map statement is applied on both the physical interface and to the tunnel interface. In order to establish connectivity between VPN sites, dynamic routing or static routes to the tunnel interface must be configured to establish connectivity between the sites. Additional configuration for enabling dynamic IP routing and IP multicast is not shown here. Please refer to the Cisco IOS Software configuration guide for that information.

In addition to creating a tunnel interface, the access list used for the crypto map must be modified to only permit the GRE traffic on the outbound for both peers.

```
ip access-list extended vpn-static1
  permit gre host 192.168.100.1 host 192.168.101.1
```

Privacy Configuration

To enable the VPN sites privacy, the public interface need to be configured to deny all traffic that is not encrypted, or allow secure access to the Internet with FW feature set.

To create privacy for the VPN sites, enable inbound access list on the public interface to permit only the encrypted IPsec traffic and the addresses sent between the remote sites:

```
interface FastEthernet1/0
  ip access-group 120 in
```

Traffic received from the outside passes through the inbound access list twice. The first time it passes, it is encrypted, and permitted with the following ACLs:

```
access-list 120 permit esp any host 192.168.100.1
access-list 120 permit udp any eq isakmp host 192.168.100.1 eq isakmp
```

The second time the traffic passes through the inbound ACL, the traffic examined is unencrypted, allowing the examination of the original IP addresses. The following ACL, with original IP addresses, allows traffic from many VPN sites:

```
access-list 120 permit ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 120 permit ip 172.16.3.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 120 permit ip 172.16.3.0 0.0.0.255 172.16.1.0 0.0.0.255
```

Firewall Security Configuration

Configure the Cisco IOS Firewall feature set on the inside interfaces to allow protected outbound access to the Internet with split tunneling:

```
!
ip inspect name fwconf tcp
ip inspect name fwconf http
ip inspect name fwconf smtp
!
interface Ethernet0/0
  ip inspect fwconf in
```

This sample configuration will allow a secure outbound access to the Internet. Additional configuration options in Cisco IOS Firewall allow for additional access, including various protocols and for secure inbound access.

Refer to the configuration manual for full details on configuring Cisco IOS Firewall feature set.

Private Addresses and Network Address Translation

Private networks seldom use public IP addresses in the intranet. When remote sites use private addresses and access the Internet, Network Address Translation (NAT) is necessary at the Edge router to provide a translation to a public routable address.

To configure NAT to access the Internet follow the following three steps:

1. Create a global NAT configuration command. The following configuration is used to translate all inside addresses to the address assigned to the public interface on the router. It offers a convenience to users who wish to translate all the internal addresses in a simple step:

```
ip nat inside source list 150 interface FastEthernet0 over load
```

2. Create access list to specify what traffic will be translated. The following access list applies NAT on all traffic that is not sent between two sites within the same VPN.

```
access-list 150 deny ip 172.16.0.0 0.0.255.255 172.16.0.0 0.0.255.255
access-list 150 permit ip any any
```

3. Apply the NAT translation to the outbound and inside interfaces:

```
interface FastEthernet1/0
  ip nat outside
interface Ethernet0
  ip nat inside
```

This NAT configuration is used for illustration only. Please refer to reference (9) for additional NAT configuration options.

Additional Configurations

Disable the following Cisco IOS features to reduce the security risks against attack from unsecured network:

```
interface FastEthernet1/0
  no ip redirects
  no ip directed-broadcast
  no ip unreachable
  no ip proxy-arp
  no cdp enable
!
no ip http server
no ip source-route
no ip finger
```

- Site-to-Site

2. Hub-and-spoke VPN

This section describes the implementation of Hub and Spoke IP connectivity. It contains the following subsections:

- Strategy
- Network Topology
- Benefits
- Limitations
- Configuration Task List
- Special Considerations

Hub-and-spoke VPN Strategy

In Hub and Spoke network configurations, the spokes sites connect with IPsec tunnels to a hub site to establish connectivity to the network. The hub site consists of high-end tunnel aggregation routers servicing multiple IPsec tunnels for a predefined maximum number of spoke locations.

In addition by terminating the VPN tunnels at the hub site, the head–end can act as the distribution point for all routing information and connectivity to and from spoke site devices. For resiliency and load distribution, the hub site could be made with multiple head-end devices.

The hub and spoke design is the most suitable configuration when the majority of traffic is targeted to the hub and the core of the network. Additional IPsec connections that form partial mesh connections can enable a direct IPsec path if some spokes sites require direct access.

In this hub and spoke configuration, the hub generally uses statically assigned IP addresses, while the spokes use dynamically assigned IP addresses. In an environment where the spoke sites are also using a static public addresses, a partial mesh of IPsec connections can create the VPN using Site-to-Site configurations.

The main feature for enabling this configuration is the Dynamic crypto maps, which ease IPsec configuration. They are used in the hub and spoke configuration to support the dynamic addresses at the spokes, and the peer addresses are not predetermined in the hub configuration and are dynamically assigned IP addresses. The spokes need to authenticate themselves to the hub in order to establish the IPsec tunnel to the hub. If pre-shared keys are used as the

authentication, then the hub needs to be configured with a wild-card pre-shared key because spoke IP addresses are not known before hand. All spokes that (1) know the pre-shared key and (2) whose IP address match the network mask for the wild-card pre-shared key are acceptable for connection to the hub.

Hub-and-spoke VPN Network Topology

The large site routers connect to multiple medium and large sites. Small site routers (spokes sites) typically connect to a set of larger large site routers (Hub sites).

The network topology used to illustrate this design is shown below in Figure 4:

Figure 4

Network Diagram: Hub-and-spoke VPN
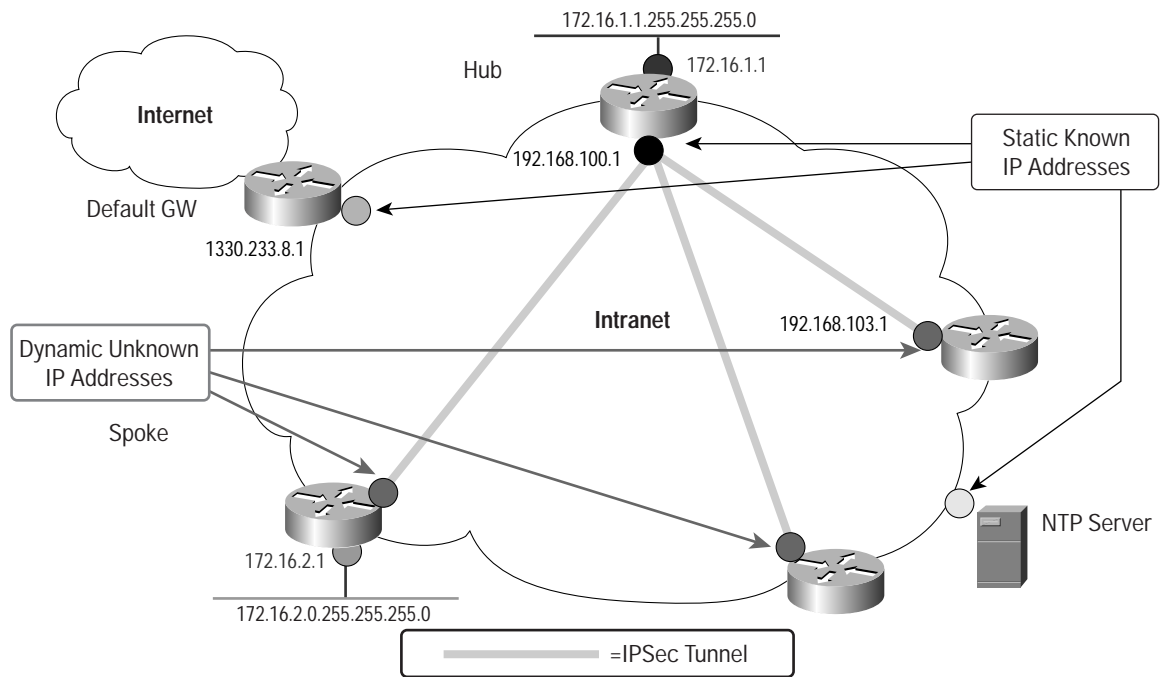
Hub-and-spoke VPN Benefits

- Provide support for small sites with small LAN and low-end routers as only one IPsec tunnel needed at the spoke routers.
- Reduces the hub router configuration size and complexity. The hub router no longer needs to maintain a separate static crypto map for each of the spoke sites, or maintain a list of IP addresses of the spoke sites, thus simplifying the add, delete and spoke sites.
- Scales the network through scaling of the network at specific hub point
- Only the hub needs to have a static and global IP address. All the spoke routers could have DHCP based dynamic IP address, with the hub configured with dynamic crypto map.
- Very easy to add a new site/router, as no changes to the existing spoke or hub routers are required.

Hub-and-spoke VPN Limitations

The Limitations of deploying Hub and spoke IPsec configurations are as follows:

- IPsec performance is aggregated at the hub.
- All spoke-spoke packets are decrypted and re-encrypted at the hub.
- When using hub and spoke with dynamic crypto maps, the IPsec encryption tunnel must be initiated by the spoke routers.

Hub-and-spoke VPN Configuration Task List

The following is a summary of the additional tasks to perform to configure the hub and spoke routers for hub and spoke IPsec VPNs configurations.

On the Hub

1. Use Dynamic Crypto map instead of static mapping for crypto map in step 4 of the main design. The dynamic crypto map policy is used to process negotiation requests for new security associations from remote IPsec peers, even if the router does not know all the crypto map parameters (i.e., IP address).

```
crypto dynamic-map test-map 1
  set transform-set vpn-test
!
crypto map static-map 1 ipsec-isakmp dynamic test-map
!
```

The vpn-test refers to the IPsec transforms defined in step 2 in the first design.

2. Use wildcard IP addresses with the pre-shared keys: this enables the negotiation with a peer without a preconfigured IP address. Any device that has the key may successfully authenticate. When using wildcard-preshared keys, every device in the network uses the same key.

```
crypto isakmp key secretkey address 0.0.0.0 0.0.0.0
```

On the Spokes

The spokes routers configurations follows the steps described in the main design. The spokes routers only establish IPsec peering with the hub. However when a significant amount of traffic is sent between two spokes, additional peering between the two spokes can be configured to send the traffic directly between the two spokes sites.

3. Fully-Meshed On-Demand VPN with Tunnel Endpoint Discovery

This section will provide an understanding of the application, benefits and configuration of fully-meshed on-demand VPN with Tunnel Endpoint Discover (TED):

- Introduction
- Strategy
- Software and Hardware Versions
- Network Topology

- Benefits
- Limitations
- Configuration Task List

Introduction

TED is a Cisco IOS Software feature that allows routers to discover IPsec end-points. TED enables IPsec configuration to scale in a large network by reducing multiple crypto maps and crypto policy configuration into a single step. It also allows for simpler configuration on participating peer routers.

Fully-Meshed On-Demand VPN with TED Strategy

TED was developed for use in large Enterprise IPsec deployments, particularly for an instance when there are many sites in a fully meshed topology and they need to establish security with each other. Initiating routers can use a dynamic crypto map to dynamically determine IPsec peers. With TED, the initiating router can dynamically discover the IPsec peer for secure IPsec communications.

To have a large, fully meshed network without TED, each peer needs to have static crypto maps to every other peer in the network. For example, if there are 100 peers in a large, fully meshed network, each router needs 99 static crypto maps for each of its peers. With TED enabled, only a single dynamic crypto map is needed because the peer is discovered dynamically. Thus, static crypto maps do not need to be configured for each peer.

TED uses a discovery probe, sent from the initiator, to determine which IPsec peer is responsible for a specific host or subnet. Once the address of that peer is learned, the initiator will proceed with IKE main mode in the normal way.

TED configuration can be used in conjunction with a hub-and-spoke model. TED can be used to add direct spoke-to-spoke tunnels establishment to the static hub-and-spoke configuration.

Fully-Meshed On-Demand VPN with TED Software and Hardware Versions

This configuration is supported using the software and hardware below:

- Cisco IOS Software Release 12.0T or later
- TED runs on all platforms that support Cisco IOS Software Release 12.0(5)T and later releases with IPsec
- It is supported on the following platforms (note: list is not inclusive): Cisco 1600 Series Routers, Cisco 1720 Router, Cisco 2500 Series Routers, Cisco 2600 Series Routers, Cisco 3600 Series Routers, Cisco 4000 Series Routers, Cisco 7200 Series Routers, Cisco 7500 Series Routers.

Fully-Meshed On-Demand VPN with TED Network Topology

Figure 5 show a network diagram of IPsec VPNs with TED IPsec.

Figure 5

Network Diagram: Fully-Meshed On-Demand VPN with TED
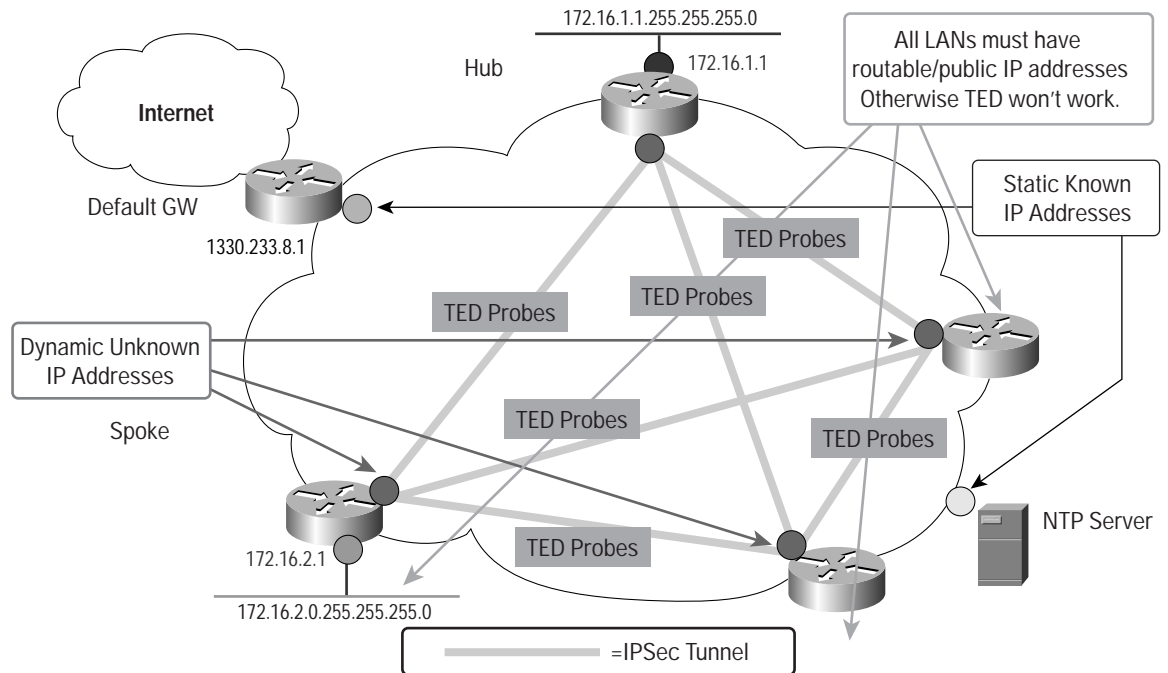
Fully-Meshed On-Demand VPN with TED Benefits

- All sites can have dynamic IP addresses
- Simplified configurations
- Simplifies the maintenance of preshared password, when used carefully and protectively
- No need for maintaining a full list of peer addresses in all the routers
- Fully-meshed On-demand VPN with TED Limitations
- TED probes use protected LAN addresses; therefore, all addresses must be routable. TED will not work if NAT is involved.
- Load balancing cannot be implemented when using TED at spokes sites
- All LANs must have a routable/public IP address

Fully-Meshed On-Demand VPN with TED Configuration Task List

To enable IPsec VPN configuration for VPN sites, refer to the earlier section of this document: "Implementing IPsec router to router configurations". Note the following necessary changes:

- Use Dynamic Crypto map for enabling probe discovery: Instead of using crypto static mapping in Step 4, use dynamic mapping to enable TED configurations:

```
crypto dynamic-map test-map 1
  set tranform vpn-test
  match address 101
!
crypto map static-map 1 ipsec-isakmp dynamic test-map discover
!
access-list 101 permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
```

The keyword discovery enables the IPsec peer discovery. It causes the router to intercept the first packet that matches the ACL, and instead sends a TED probe into the network. When the remote LAN router receives the TED probe message, it responds with a TED probe reply and includes its own IP address as the tunnel end for the dynamic IPsec session.

The access list identifies traffic that requires IPsec protection; additionally, it is a trigger mechanism for the TED discovery probe. The following example illustrates what happens when the packet arrives at the local router:

1. Packet arrives in the form of ping to 172.16.2.10

2. If this matches access-list 101, then the router will send the ping to 172.16.2.10 in the form of a probe, using its own address as the new source address of the packet

- Use wildcard ip addresses with the pre-shared keys: enables the negotiation with a peer without a preconfigured IP address. Any device that has the key may successfully authenticate. When using wildcard preshared keys, every device in the network uses the same key.

```
crypto isakmp key secretkey address 0.0.0.0 0.0.0.0
```

4. Dynamic Multipoint VPN

This section will provide an understanding of the application, benefits and configuration of Dynamic Multipoint VPN:

- Strategy
- Software and Hardware Versions
- Network Topology
- Benefits
- Limitations
- Configuration Task List

Dynamic Multipoint VPN Strategy

Companies may want to interconnect small sites together, while simultaneously connecting to a main site over the Internet. When small sites are interconnected, it is difficult to maintain the configurations for all the connections. It is also difficult to create, add, and change a large network configuration. Since the spokes do have direct access to each other over the Internet, it would be beneficial for the spoke-to-spoke traffic to go direct rather then via a hub site. This would be useful is when two spokes are in the same city and the hub is across the country. With the Dynamic Multipoint IPsec VPNs solution, the Spokes sites would be able to dynamically establish secure connectivity between them.

In this design, the IPsec connectivity is provided with a combination of static and dynamic on demand tunnels. The static VPN tunnels are connected to a hub site in a hub and spoke fashion. The hub and spoke design is the most suitable configuration when the majority of the traffic is targeted to the hub and the core of the network. When some spokes sites are requiring direct access between them, an additional IPsec connections forming a partial mesh connection will dynamically direct the IPsec path.

The Dynamic Multipoint IPsec VPN solution (DMVPN) solution uses Multipoint GRE/Next Hop Resolution Protocol (mGRE/NHRP) with both IPsec and NHRP to resolve the peer destination address, and automatic IPsec encryption initiation.

NHRP also provides the capability for the spoke routers to dynamically learn the exterior physical interface address of the routers in the VPN network. This means that the spoke routers would have enough information to dynamically build an IPsec+mGRE tunnel directly between spoke routers. This is important because if this spoke-to-spoke data traffic is sent via the hub router it must be encrypted/decrypted twice, thus increasing delay and the decryption and encryption of this through traffic increases the load on the hub router. In order to use this feature, the spoke routers need to learn, via the dynamic IP routing protocol running over the IPsec+mGRE tunnel with the hub, the sub networks that are available behind the other spokes with an IP next-hop of the tunnel IP address of other spoke router.

The dynamic IP routing protocol running on the hub router can be configured to reflect the routes learned from one spoke to all of the other spokes, but the IP next-hop on these routes will usually be the hub router not the spoke router from which the hub learned this route. Note, the dynamic routing protocol only runs on the hub and spoke links, it does not run on the dynamic spoke-to-to spoke links.

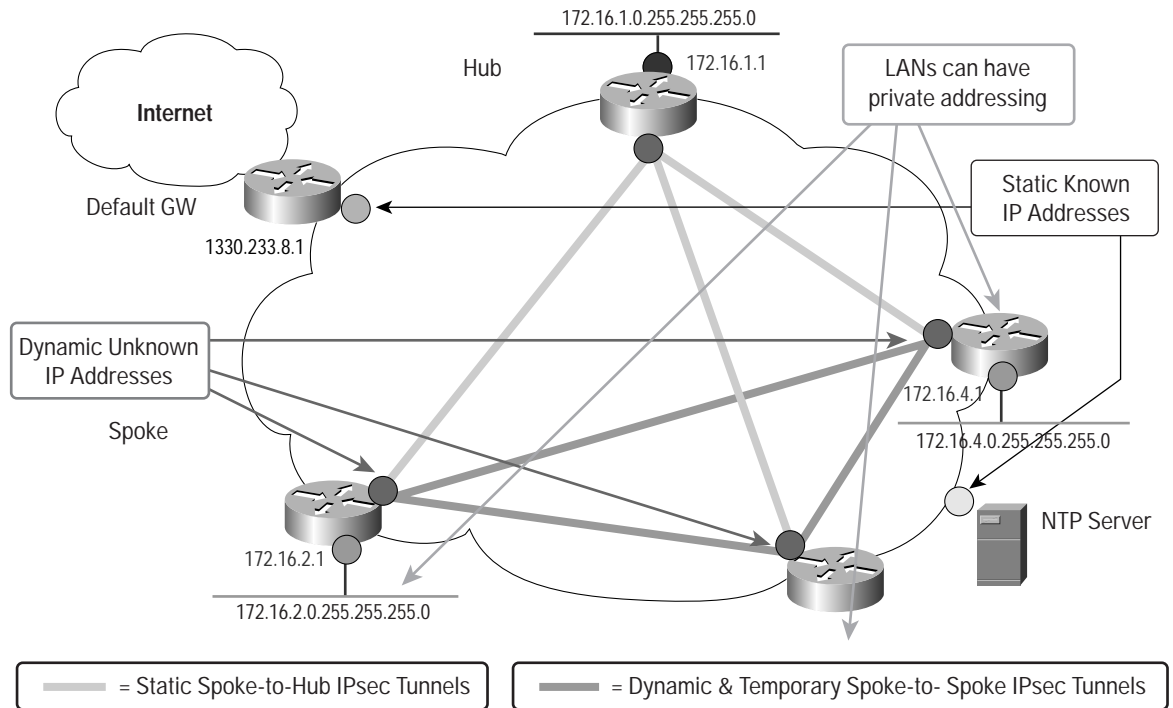### Dynamic Multipoint VPN Software and Hardware Versions

This feature is planned for release in Cisco IOS Software Release 12.2(11)T and the supported hardware platforms.

Dynamic Multipoint VPN IPsec VPNs Network Topology

Figure 6 shows the devices of the Dynamic Multipoint VPNs infrastructure.

Figure 6

Network Diagram: Dynamic Multipoint VPN

Dynamic Multipoint VPN with GRE Benefits

- Allows better scaling in full mesh and partial mesh IPsec VPNs
- Especially useful when configuration of spoke-to-spoke traffic is relatively complex to configure and maintain
- Reduces the hub router configuration size and complexity. The hub router no longer needs to maintain separate static crypto map for each of the spoke sites, or maintain a list of IP addresses of the spoke sites, simplifying the add, delete and spoke sites.
- Conserves router resources by establishing links on-demand and tear down after a pre-configured duration of inactivity. Enables low-end routers to participate in a large in large IPsec VPNs (1000 nodes).
- Provides optimum path between spoke site
- Supports dynamic IP addresses on the spokes
- Supports Private addressing in the Spokes LAN
- Split tunneling at the spokes is supported
- Creates a constant configuration size on the hub router, regardless of how many spoke routers are added to the VPN network

Dynamic Multipoint VPN with GRE Limitations

- The majority of the traffic should be passing the dedicated hub sites to minimize topology changes
- The initial packets will go through the Hub, until the spoke-to-spoke tunnel is established
- When using hub and spoke with dynamic crypto maps, the IPsec encryption tunnel must be initiated by the spoke routers

Dynamic Multipoint VPN with GRE Configuration Task List

To enable Dynamic Multipoint IPsec VPN configuration for VPN sites, refer to the earlier section of this document "Implementing IPsec router to router configurations". Note the following necessary changes:

On the Hub

In a traditional hub and spoke configuration, each spoke router has a separate block of configuration lines on the hub router to define the crypto map characteristics, the crypto access-list and the GRE tunnel interface for that spoke router. Typically, only the IP addresses vary between these configurations.

With Dynamic Multipoint IPsec VPN Solution, we can configure a single multiple GRE tunnel interface and a single IPsec profile on the hub router to handle all spoke routers. With this, the size of the configuration on the hub router is a constant, regardless of how many spoke routers are added to the VPN network.

Enable GRE configuration by using Steps 1–3 in the main configuration, followed by:

1. Use this step instead of Step 4. It is used similarly to a dynamic crypto map, and is designed specifically for tunnel interfaces.

   This command is defines the IPsec parameters for IPsec encryption between the hub router and the spoke routers. In general the only parameter that needs to be specified under the profile is the transform that will be used. The IPsec peer address and the 'match' clause for the IPsec proxy are automatically derived from the NHRP mapping for the GRE tunnel. Use the following commands:

   ```
   crypto IPsec profile vpnprof
     set transform-set vpn-test
   ```

2. Enable NHRP configurations on the tunnel interface:

   ```
   interface tunnel0
     ip address 10.0.0.1 255.255.255.0
     ip mtu 1436
     ip nhrp authentication test
     ip nhrp map multicast dynamic
     ip nhrp network-id 100000
     ip nhrp holdtime 600
   ```

Enable the following features on the tunnel interface:

```
interface tunnel0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection IPsec profile vpnprof
```

```
interface FastEthernet1/0
   ip address 192.168.100.1 255.255.255.0
```

Note that the 'tunnel protection IPsec profile <name>' command is configured under the GRE tunnel interface, and is used to associate the GRE tunnel interface with the IPsec profile. It specifies that the IPsec encryption will be completed after the GRE encapsulation has been added to the packet, and it replaces the 'crypto map' command on both the tunnel interface and on the physical interface.

On the Spoke

Follow Steps 1–5 in the main configuration and then enable the GRE configuration from the additional steps.

Enable NHRP configurations on the tunnel interface:

```
interface tunnel0
   ip address 10.0.0.n 255.255.255.0
   ip mtu 1436
   ip nhrp authentication test
   ip nhrp map 10.0.0.1 172.17.0.1
   ip nhrp network-id 100000
   ip nhrp holdtime 300
   ip nhrp nhs 192.168.100.1
   tunnel key 100000
```

The command 'ip nhrp map' is used to enable the spoke router when it comes up to initiate a tunnel connection with the hub. The spoke routers have to initiate the connection since it may have a dynamically assigned IP address, and the hub router isn't configured with any information about the spoke routers.

The spoke routers are also configured with the hub as their NHRP Next Hop Server (NHS). With this feature configured, the spoke router will send NHRP Registration packets through the mGRE+IPsec tunnel to the hub router at regular intervals. These registration packets provide the spoke NHRP mapping information that is needed by the hub router to tunnel packets back to the spoke routers.

Additional Configuration

The dynamic routing protocols (RIP, OSPF and EIGRP) need to be configured on the Hub router to advertise the routes back out the mGRE tunnel interface. This will also set the IP next-hop of the originating spoke router for routes learned

- RIP: Need to turn off split horizon on the mGRE tunnel interface on the hub, otherwise RIP will not advertise routers learned via the mGRE interface back out that interface.

```
no ip split-horizon
```

No other changes are necessary, as RIP will automatically use the original IP next-hop on routes that advertises back out the same interface where it learned these routes.

- EIGRP: Split horizon on the mGRE tunnel interface must be disabled; otherwise, EIGRP will not advertise routes learned via the mGRE interface back out that interface.

```
no ip split-horizon eigrp <as>
```

EIGRP will automatically set the IP next-hop to be the hub router for routes that it advertises, even when advertising those routes back out the same interface where it learned them. EIGRP must be instructed to use the original IP next-hop when advertising these routes via a new configuration command:

```
no ip next-hop-self eigrp <as>
```

- OSPF: Since ospf is a link-state routing protocol, there are not any split horizon issues. Configure the OSPF network type to be broadcast.

```
ip ospf network broadcast
```

Also, make sure that the hub router will be the designated router for the mGRE+IPsec network. This is done by setting the OSPF priority to be greater than 1 on the hub and 0 on the spokes.

```
Hub: ip ospf priority 2

Spoke: ip ospf priority 0
```

5. Cisco Easy VPN

This section describes the implementation of remote to server IPsec configuration:

- Introduction
- Software Requirements
- Network Topology
- Benefits
- Limitations
- Configuration Task List

Cisco Easy VPN Introduction

When deploying VPNs for teleworkers and small branch offices, ease of deployment increases in importance. It is now easier than ever to deploy VPNs as part of small/medium business or large enterprise networks with Cisco products. Cisco Easy VPN Remote and Cisco Easy VPN Server offer flexibility, scalability, and ease of use for site-to-site and remote-access VPNs.

An Easy VPN Server-enabled device can terminate VPN tunnels initiated by mobile and remote workers running Cisco Easy VPN Remote software on PCs. In addition, it allows remote routers to act as Easy VPN Remote nodes. The Cisco Easy VPN Remote feature eliminates much of this tedious work by implementing Cisco Unified Client protocol. It allows the VPN parameters, such as internal IP addresses, internal subnet masks, DHCP server addresses, WINS server addresses, and split-tunneling flags, to be pushed to the remote device. 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.

Cisco Easy VPN Software Requirements

On the Server

This feature was introduced in Cisco IOS Software Release 12.2(8)T and its supported platforms.
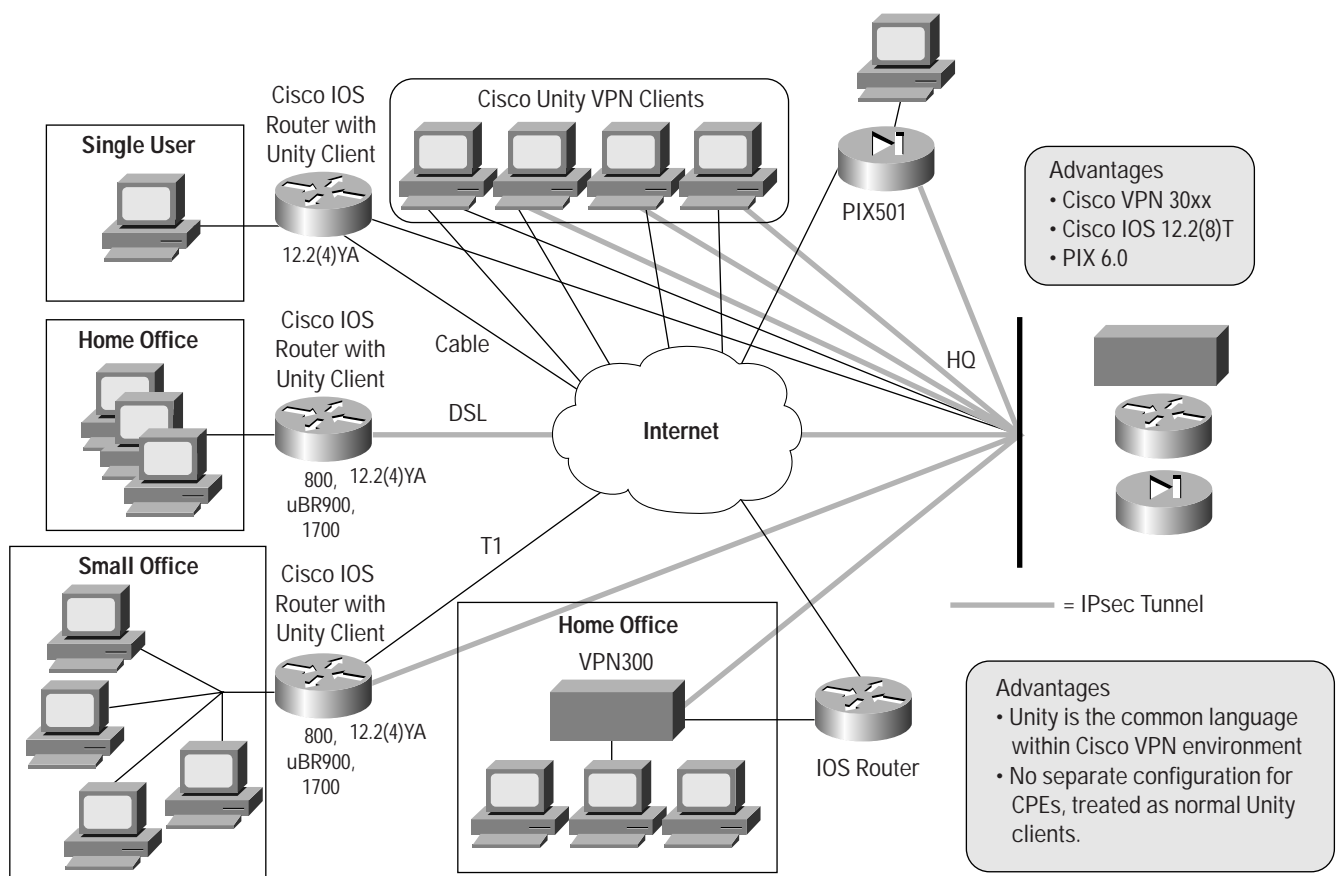
On the Remote Router

In 12.2(4)YA, this feature was introduced for the Cisco 806, 826, 827, and 828 Routers, Cisco 1700 Series Routers, and the Cisco uBR905 and Cisco uBR925 Cable Access Routers.

Remote to Server IPsec VPNs Network Topology

Figure 7 shows the devices of Cisco Easy VPN Remote/Server infrastructure.

Figure 7
Network Diagram: Cisco Easy VPN

Cisco Easy VPN Benefits

- The centrally stored configurations allow dynamic configuration of end-user policy and require less manual configuration by end-users and field technicians. This reduces errors and further service calls.
- The local VPN configuration is independent of the remote peer's IP address, allowing the provider to change equipment and network configurations as needed, with little or no reconfiguration of the end-user equipment.
- Provides for centralized security policy management
- Enables large-scale deployments with rapid user provisioning
- Removes the need for end-users to purchase and configure external VPN devices.

- Removes the need for end-users to install and configure VPN remote software on their PCs
- Offloads the creation and maintenance of the VPN connections from the PC to the router.
- Reduces interoperability problems between the different PC-based software VPN remotes, external hardware-based VPN solutions, and other VPN applications.

Cisco Easy VPN Limitations

- *No Manual NAT/PAT Configuration Allowed:* Cisco Easy VPN Remote automatically creates the appropriate NAT/PAT configuration for the VPN tunnel.
- *Only One Destination Peer Supported:* Cisco Easy VPN Remote supports the configuration of only one destination peer and tunnel connection. If an application requires the creation of multiple VPN tunnels, the IPsec VPN and NAT/PAT parameters on both the remote and server must be manually configured.
- *Required Destination Servers:* Cisco Easy VPN Remote requires that the destination peer be a VPN remote access server, or that VPN concentrator supports either the VPN Remote Access Server Enhancements feature or the Cisco Unity protocol.
- *Digital Certificates Not Supported:* Cisco IOS Easy VPN Remote does not support authentication using digital certificates at this time. Authentication is supported using pre-shared keys. Extended Authentication (Xauth) may also be used in addition to pre-shared keys in order to provide user level of authentication in addition to device level authentication.
- *Only ISAKMP Policy Group 2 Supported on IPsec Servers:* The Unity Protocol supports only ISAKMP policies that use group 2 (1024-bit Diffie-Hellman) IKE negotiation, so the IPsec server being used with the Cisco Easy VPN Remote must be configured for a group 2 isakmp policy. The IPsec server cannot be configured for ISAKMP group 1 or group 5 when being used with a Cisco Easy VPN Remote.
- *Transform Sets Supported:* To ensure a secure tunnel connection, the Cisco Easy VPN Remote feature does not support transform sets that provide encryption without authentication (ESP-DES and ESP-3DES) or transform sets that provide authentication without encryption (ESP-NULL ESP-SHA-HMAC and ESP-NULL ESP-MD5-HMAC).

Cisco Easy VPN Configuration Task List

The following are the tasks required to configure Easy VPN Server and Easy VPN Remote running Cisco IOS Software:

On the Server

Step 1. Configure IKE policy

To configure the IKE policy, use the following commands, beginning in global configuration mode:

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

Step 2.   Configure Group Policy Information

Define the group policy information to enable download IPsec configurations to the remote. To define the policy attributes that are pushed to the remote via Mode Configuration, use the following commands beginning in global configuration mode:

Use the following command to specify a group named rtr-remote policy, that will be defined and will enters to the Internet Security Association Key Management Protocol (ISAKMP) group configuration mode:

```
crypto isakmp client configuration group rtr-remote
```

Specify the IKE preshared key for group policy attribute definition in the isakmp group configuration mode:

```
key secret-password
```

Define the optional configurations, as needed, for DNS servers, WINS servers, DNS domain name to which the group belongs:

```
dns 10.50.10.1 10.60.10.1
wins 10.50.20.1 10.60.20.1
domain company.com
```

Define a local pool address in the isakmp group configuration mode. This command refers to a valid IP local pool address

```
pool  dyn-pool
!
ip local pool dyn-pool 30.30.30.20 30.30.30.30
```

Step 3.   Apply Mode configuration to crypto map

To apply mode configuration to the crypto map, configure the router to reply to Mode Configuration requests from the remote sites, using the respond keyword, and enable IKE query for group policy for remote site requests.

Use the following sample commands in global configuration mode:

```
crypto map dynmap isakmp authorization list rtr-remote
crypto map dynmap client configuration address respond
```

Step 4.   Enable Policy Lookup via AAA model

Use the following commands to enable policy lookup via AAA, beginning in global configuration mode:

```
aaa new-model
aaa authentication login rtr-remote local
aaa authorization network rtr-remote local
!
username cisco password 0 cisco
```

This configurations uses local database for authentication and authorization, alternatively a Radius server can be used in this step. For details on configuring Radius, please refer to:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt2/scdrad.htm

Step 5. Configure IPsec transforms and protocols

Refer to Step 2 in the site-to-site design for configuration description

Step 6. Configure the IPsec Crypto method and parameters

Follow Step 1 in the hub and spoke design to create a dynamic crypto map for IPsec sessions. In additional, configure Reverse Route Injection (RRI) to ensure that a static route is created dynamically on the Hub router for each remote router's internal IP address. To enable RRI, use the following command under the crypto-map configuration mode:

```
(config-crypto-map)# reverse-route
```

Step 7. Apply Crypto Map on the physical interface

Follow Step 5 in the site-to-site design for applying the Crypto Map on the physical interface.

On the Spokes

The router acting as the IPsec remote router must create an Easy VPN remote configuration and assign it to the outgoing interface. To do so, use the following steps:

Step 1. Create an Easy VPN remote configuration

Create an Easy VPN remote configuration named hw-remote and enters Easy VPN remote configuration mode.

```
Crypto ipsec client ezvpn hw-remote
```

Step 2. Specify the VPN peer and key information

Specify the IPsec group, IPsec key value, the IP address for the destination peer to be associated with this configuration:

```
(config-crypto-ezvpn)# group hw-remote-groupname key secret-password
(config-crypto-ezvpn)# peer 192.168.100.1
(config-crypto-ezvpn)# mode client
```

Step 3. Assign the Cisco Easy VPN Remote configuration to the WAN interface

To assign the Cisco Easy VPN remote configuration to the interface, use the following commands:

```
interface Ethernet1
crypto ipsec client ezvpn hw-remote
```

Configuration Options

Modes of Operations

The Cisco Easy VPN Remote feature supports two modes of operation, client mode and network extension mode:

- *Client*—Specifies that NAT/PAT are essential, so that the PCs and other hosts at the client end of the VPN tunnel form a private network that does not use any IP addresses in the destination server's IP address space.

In client mode, Cisco Easy VPN Remote automatically creates and deletes the NAT/PAT translation and access lists that are needed to implement the VPN tunnel. In these configurations, the IP NAT outside command is applied to the interface that is configured with the Cisco Easy VPN Remote configuration, and these NAT/PAT configurations are dynamic and can only be displayed using the show ip nat statistics and show access-list commands.

To configure Client mode on the VPN client, configure the following commands:

```
crypto ipsec client ezvpn hw-client
      (config-crypto-ezvpn)# mode client
```

In a typical VPN connection, the PCs connected to the remote router's LAN interface are assigned an IP address in a private address space. The router then uses NAT/PAT to translate those IP addresses into a single IP address that is transmitted across the VPN tunnel connection. The following is an example for configuring DHCP server:

```
ip dhcp pool CLIENT
import all
network 10.10.10.0 255.255.255.0
default-router 10.10.10.1
option 150 ip 30.30.30.200
!
ip dhcp excluded-address 10.10.10.1
```

- *Network Extension*—Specifies that the PCs and other hosts at the client end of the VPN tunnel should be given IP addresses that are fully routable and reachable by the destination network over the tunneled network, so that they form one logical network. PAT is not used, which allows the client PCs and hosts to have direct access to the hosts at the destination network.

    To configure network extension mode on the VPN client, configure the following commands:

```
crypto ipsec client ezvpn hw-client
      (config-crypto-ezvpn)# mode network
```

In order to reach the routable segment at the remote router, an additional static route is required at the hub router to forward the traffic to the public interface with the IPsec connections, such as:

```
ip route 10.10.10.0 255.255.255.0 Ethernet0/0
```

Split Tunneling with Cisco Easy VPN

Cisco Easy VPN supports split tunneling, which allows Internet-destined traffic to be sent unencrypted directly to the Internet. Without split tunneling all traffic is sent to the head-end device and then routed to destination resources, eliminating the corporate network from the path for web access. This functionality provides a more efficient use of corporate IT resources, freeing bandwidth for those who access mission-critical data and applications from remote locations.

Split tunneling is disabled with the default configurations. The ACL is used to specify the traffic to be encrypted with IPsec. The rest of the traffic is forwarded without encryption. To enable split tunneling use the following commands on the hub router:

```
Crypto isakmp client configuration group hw-client-groupname
(isakmp-group)# acl 150
!
access-list 150 permit ip 30.30.30.0 0.0.0.255 any
```

Both Client and Network modes of operation optionally support split tunneling. When enabling split tunneling, additional security and firewall configurations is required to ensure the security of the remote site. Refer to the security configuration in the site-to-site design for a sample configuration.

Extended Authentication (Xauth)

After the IKE SA is successfully established, and if the Cisco IOS VPN device is configured for Xauth, the client waits for a "username/password" challenge, and then responds to the peer's challenge. The information that is entered is checked against authentication entities using authentication, authorization, and accounting (AAA) protocols such as RADIUS and TACACS+. Token cards may also be used via AAA proxy.

To set AAA authentication at login with Xauth, local and radius server may be used together and will be tried in order. The following commands must be enabled to enforce Xauth with local authentication:

aaa authentication login userlist local

crypto map dynmap client authentication list userlist

Related Documents

- Cisco Easy VPN Remote Feature:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122y/122ya/122ya4/ftezvpcm.htm#xtocid11

- Cisco Easy VPN Application Note:

  http://www.cisco.com/warp/public/cc/so/neso/vpn/ns171/ns27/prodlit/evpnc_qa.htm

- Easy VPN Server:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftunity.htm

- IPsec Virtual Private Networks in Depth:

  http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.pdf

CISCO SYSTEMS

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe