



Configuring VPNs Using an IPSec Tunnel and Generic Routing Encapsulation

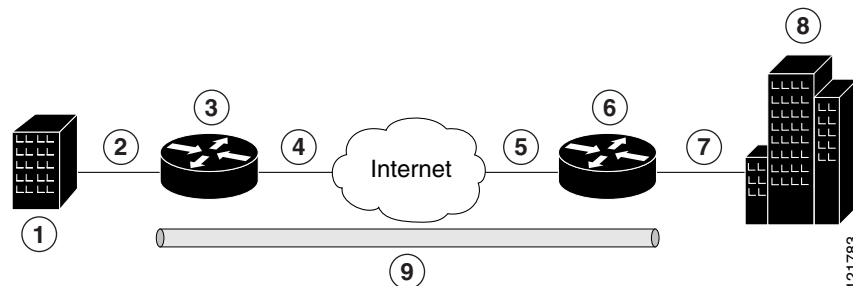
The Cisco 850 and Cisco 870 series routers support the creation of virtual private networks (VPNs).

Cisco routers and other broadband devices provide high-performance connections to the Internet, but many applications also require the security of VPN connections which perform a high level of authentication and which encrypt the data between two particular endpoints.

Two types of VPNs are supported—site-to-site and remote access. Site-to-site VPNs are used to connect branch offices to corporate offices, for example. Remote access VPNs are used by remote clients to log in to a corporate network.

The example in this chapter illustrates the configuration of a site-to-site VPN that uses IPSec and the generic routing encapsulation (GRE) protocol to secure the connection between the branch office and the corporate network. [Figure 7-1](#) shows a typical deployment scenario.

Figure 7-1 Site-to-Site VPN Using an IPSec Tunnel and GRE



1	Branch office containing multiple LANs and VLANs
2	Fast Ethernet LAN interface—With address 192.168.0.0/16 (also the inside interface for NAT)
3	VPN client—Cisco 850 or Cisco 870 series access router
4	Fast Ethernet or ATM interface—With address 200.1.1.1 (also the outside interface for NAT)
5	LAN interface—Connects to the Internet; with outside interface address of 210.110.101.1
6	VPN client—Another router, which controls access to the corporate network
7	LAN interface—Connects to the corporate network, with inside interface address of 10.1.1.1
8	Corporate office network
9	IPSec tunnel with GRE

GRE Tunnels

GRE tunnels are typically used to establish a VPN between the Cisco router and a remote device that controls access to a private network, such as a corporate network. Traffic forwarded through the GRE tunnel is encapsulated and routed out onto the physical interface of the router. When a GRE interface is used, the Cisco router and the router that controls access to the corporate network can support dynamic IP routing protocols to exchange routing updates over the tunnel, and to enable IP multicast traffic. Supported IP routing protocols include Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol (RIP), Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP).

**Note**

When IP Security (IPSec) is used with GRE, the access list for encrypting traffic does not list the desired end network and applications, but instead refers to the permitted source and destination of the GRE tunnel in the outbound direction. All packets forwarded to the GRE tunnel are encrypted if no further access control lists (ACLs) are applied to the tunnel interface.

VPNs

VPN configuration information must be configured on both endpoints; for example, on your Cisco router and at the remote user, or on your Cisco router and on another router. You must specify parameters, such as internal IP addresses, internal subnet masks, DHCP server addresses, and Network Address Translation (NAT).

Configuration Tasks

Perform the following tasks to configure this network scenario:

- [Configure a VPN](#)
- [Configure a GRE Tunnel](#)

A configuration example showing the results of these configuration tasks is provided in the “[Configuration Example](#)” section on page 7-9.

**Note**

The procedures in this chapter assume that you have already configured basic router features as well as PPPoE or PPPoA with NAT, DHCP, and VLANs. If you have not performed these configurations tasks, see [Chapter 1, “Basic Router Configuration,”](#) [Chapter 3, “Configuring PPP over Ethernet with NAT,”](#) [Chapter 4, “Configuring PPP over ATM with NAT,”](#) and [Chapter 5, “Configuring a LAN with DHCP and VLANs,”](#) as appropriate for your router.

Configure a VPN

Perform the following tasks to configure a VPN over an IPSec tunnel:

- [Configure the IKE Policy](#)
- [Configure Group Policy Information](#)
- [Enable Policy Lookup](#)
- [Configure IPSec Transforms and Protocols](#)
- [Configure the IPSec Crypto Method and Parameters](#)
- [Apply the Crypto Map to the Physical Interface](#)

Configure the IKE Policy

Perform these steps to configure the Internet Key Exchange (IKE) policy, beginning in global configuration mode:

	Command or Action	Purpose
Step 1	crypto isakmp policy <i>priority</i> Example: Router(config)# crypto isakmp policy 1 Router(config-isakmp)#	Creates an IKE policy that is used during IKE negotiation. The priority is a number from 1 to 10000, with 1 being the highest. Also enters Internet Security Association and Key Management Protocol (ISAKMP) policy configuration mode.
Step 2	encryption {des 3des aes aes 192 aes 256} Example: Router(config-isakmp)# encryption 3des Router(config-isakmp)#	Specifies the encryption algorithm used in the IKE policy. The example uses 168-bit Data Encryption Standard (DES).
Step 3	hash {md5 sha} Example: Router(config-isakmp)# hash md5 Router(config-isakmp)#	Specifies the hash algorithm used in the IKE policy. The example specifies the Message Digest 5 (MD5) algorithm. The default is Secure Hash standard (SHA-1).
Step 4	authentication {rsa-sig rsa-encr pre-share} Example: Router(config-isakmp)# authentication pre-share Router(config-isakmp)#	Specifies the authentication method used in the IKE policy. The example uses a pre-shared key.
Step 5	group {1 2 5} Example: Router(config-isakmp)# group 2 Router(config-isakmp)#	Specifies the Diffie-Hellman group to be used in the IKE policy.
Step 6	lifetime <i>seconds</i> Example: Router(config-isakmp)# lifetime 480 Router(config-isakmp)#	Specifies the lifetime, 60–86400 seconds, for an IKE security association (SA).
Step 7	exit Example: Router(config-isakmp)# exit Router(config)#	Exits IKE policy configuration mode, and enters global configuration mode.

Configure Group Policy Information

Perform these steps to configure the group policy, beginning in global configuration mode:

	Command or Action	Purpose
Step 1	<p>crypto isakmp client configuration group {group-name default}</p> <p>Example:</p> <pre>Router(config)# crypto isakmp client configuration group rtr-remote Router(config-isakmp-group)#</pre>	<p>Creates an IKE policy group that contains attributes to be downloaded to the remote client.</p> <p>Also enters Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode.</p>
Step 2	<p>key name</p> <p>Example:</p> <pre>Router(config-isakmp-group)# key secret-password Router(config-isakmp-group)#</pre>	<p>Specifies the IKE pre-shared key for the group policy.</p>
Step 3	<p>dns primary-server</p> <p>Example:</p> <pre>Router(config-isakmp-group)# dns 10.50.10.1 Router(config-isakmp-group)#</pre>	<p>Specifies the primary Domain Name Service (DNS) server for the group.</p> <p>Note You may also want to specify Windows Internet Naming Service (WINS) servers for the group by using the wins command.</p>
Step 4	<p>domain name</p> <p>Example:</p> <pre>Router(config-isakmp-group)# domain company.com Router(config-isakmp-group)#</pre>	<p>Specifies group domain membership.</p>
Step 5	<p>exit</p> <p>Example:</p> <pre>Router(config-isakmp-group)# exit Router(config)#</pre>	<p>Exits IKE group policy configuration mode, and enters global configuration mode.</p>
Step 6	<p>ip local pool {default poolname} [low-ip-address [high-ip-address]]</p> <p>Example:</p> <pre>Router(config)# ip local pool dynpool 30.30.30.20 30.30.30.30 Router(config)#</pre>	<p>Specifies a local address pool for the group.</p> <p>For details about this command and additional parameters that can be set, see the Cisco IOS Dial Technologies Command Reference.</p>

Enable Policy Lookup

Perform these steps to enable policy lookup through AAA, beginning in global configuration mode:

	Command or Action	Purpose
Step 1	aaa new-model Example: Router(config)# aaa new-model Router(config)#	Enables the AAA access control model.
Step 2	aaa authentication login {default list-name} method1 [method2...] Example: Router(config)# aaa authentication login rtr-remote local Router(config)#	Specifies AAA authentication of selected users at login, and specifies the method used. This example uses a local authentication database. You could also use a RADIUS server for this. See the Cisco IOS Security Configuration Guide and the Cisco IOS Security Command Reference for details.
Step 3	aaa authorization {network exec commands level reverse-access configuration} {default list-name} [method1 [method2...]] Example: Router(config)# aaa authorization network rtr-remote local Router(config)#	Specifies AAA authorization of all network-related service requests, including PPP, and the method used to do so. This example uses a local authorization database. You could also use a RADIUS server for this. See the Cisco IOS Security Configuration Guide and the Cisco IOS Security Command Reference for details.
Step 4	username name {nopassword password password password encryption-type encrypted-password} Example: Router(config)# username cisco password 0 cisco Router(config)#	Establishes a username-based authentication system. This example implements a username of <i>cisco</i> with an encrypted password of <i>cisco</i> .

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 sets 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.

Perform these steps to specify the IPSec transform set and protocols, beginning in global configuration mode:

	Command or Action	Purpose
Step 1	crypto ipsec transform-set <i>transform-set-name</i> <i>transform1</i> [<i>transform2</i>] [<i>transform3</i>] <i>transform4</i> Example: Router(config)# crypto ipsec transform-set <i>vpn1 esp-3des esp-sha-hmac</i> Router(config)#	Defines a transform set—An acceptable combination of IPSec security protocols and algorithms. See the Cisco IOS Security Command Reference for detail about the valid transforms and combinations.
Step 2	crypto ipsec security-association lifetime { seconds <i>seconds</i> kilobytes <i>kilobytes</i> } Example: Router(config)# crypto ipsec security-association lifetime seconds <i>86400</i> Router(config)#	Specifies global lifetime values used when negotiating IPSec security associations. See the Cisco IOS Security Command Reference for details.

**Note**

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

Configure the IPSec Crypto Method and Parameters

A dynamic crypto map policy processes negotiation requests for new security associations from remote IPSec peers, even if the router does not know all the crypto map parameters (for example, IP address).

Perform these steps to configure the IPSec crypto method, beginning in global configuration mode:

	Command or Action	Purpose
Step 1	crypto dynamic-map <i>dynamic-map-name</i> <i>dynamic-seq-num</i> Example: Router(config)# crypto dynamic-map <i>dynmap 1</i> Router(config-crypto-map)#	Creates a dynamic crypto map entry, and enters crypto map configuration mode. See the Cisco IOS Security Command Reference for more detail about this command.
Step 2	set transform-set <i>transform-set-name</i> [<i>transform-set-name2</i> ... <i>transform-set-name6</i>] Example: Router(config-crypto-map)# set transform-set <i>vpn1</i> Router(config-crypto-map)#	Specifies which transform sets can be used with the crypto map entry.

	Command or Action	Purpose
Step 3	reverse-route Example: Router(config-crypto-map)# reverse-route Router(config-crypto-map)#	Creates source proxy information for the crypto map entry. See the Cisco IOS Security Command Reference for details.
Step 4	exit Example: Router(config-crypto-map)# exit Router(config)#	Enters global configuration mode.
Step 5	crypto map <i>map-name seq-num [ipsec-isakmp]</i> <i>[dynamic dynamic-map-name] [discover]</i> <i>[profile profile-name]</i> Example: Router(config)# crypto map static-map 1 ipsec-isakmp dynamic dynmap Router(config)#	Creates a crypto map profile.

Apply the Crypto Map to the Physical Interface

The crypto maps must be applied to each interface through which IPsec traffic flows. 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 provides secure connectivity by encrypting the traffic sent between remote sites. However, the public interface still allows the rest of the traffic to pass and provides connectivity to the Internet.

Perform these steps to apply a crypto map to an interface, beginning in global configuration mode:

	Command or Action	Purpose
Step 1	interface <i>type number</i> Example: Router(config)# interface fastethernet 4 Router(config-if)#	Enters interface configuration mode for the interface to which you want to apply the crypto map.

	Command or Action	Purpose
Step 2	crypto map <i>map-name</i> Example: Router(config-if)# crypto map <i>static-map</i> Router(config-if)#	Applies the crypto map to the interface. See the Cisco IOS Security Command Reference for more detail about this command.
Step 3	exit Example: Router(config-if)# exit Router(config)#	Enters global configuration mode.

Configure a GRE Tunnel

Perform these steps to configure a GRE tunnel, beginning in global configuration mode:

	Command or Action	Purpose
Step 1	interface <i>type number</i> Example: Router(config)# interface <i>tunnel 1</i> Router(config-if)#	Creates a tunnel interface and enters interface configuration mode.
Step 2	ip address <i>subnet mask</i> Example: Router(config-if)# ip address <i>10.62.1.193</i> <i>255.255.255.255</i> Router(config-if)#	Assigns an address to the tunnel.
Step 3	tunnel source <i>interface-type number</i> Example: Router(config-if)# tunnel source <i>fastethernet 0</i> Router(config-if)#	Specifies the source endpoint of the router for the GRE tunnel.
Step 4	tunnel destination <i>default-gateway-ip-address</i> Example: Router(config-if)# tunnel destination <i>192.168.101.1</i> Router(config-if)#	Specifies the destination endpoint of the router for the GRE tunnel.

	Command or Action	Purpose
Step 5	crypto map <i>map-name</i> Example: Router(config-if)# crypto map <i>static-map</i> Router(config-if)#	Assigns a crypto map to the tunnel. Note Dynamic routing or static routes to the tunnel interface must be configured to establish connectivity between the sites. See the Cisco IOS Security Configuration Guide for details.
Step 6	exit Example: Router(config-if)# exit Router(config)#	Exits interface configuration mode, and returns to global configuration mode.
Step 7	ip access-list {standard extended} <i>access-list-name</i> Example: Router(config)# ip access-list extended <i>vpnstatic1</i> Router(config-acl)#	Enters ACL configuration mode for the named ACL that is used by the crypto map.
Step 8	permit protocol source source-wildcard <i>destination destination-wildcard</i> Example: Router(config-acl)# permit gre host <i>192.168.100.1 host 192.168.101.1</i> Router(config-acl)#	Specifies that only GRE traffic is permitted on the outbound interface.
Step 9	exit Example: Router(config-acl)# exit Router(config)#	Returns to global configuration mode.

Configuration Example

The following configuration example shows a portion of the configuration file for a VPN using a GRE tunnel scenario described in the preceding sections.

```

!
aaa new-model
!
aaa authentication login rtr-remote local
aaa authorization network rtr-remote local
aaa session-id common
!
username cisco password 0 cisco
!
interface tunnel 1
 ip address 10.62.1.193 255.255.255.252

```

```

tunnel source fastethernet 0

tunnel destination interface 192.168.101.1

ip route 20.20.20.0 255.255.255.0 tunnel 1

crypto isakmp policy 1
  encryption 3des
  authentication pre-share
  group 2
!
crypto isakmp client configuration group rtr-remote
  key secret-password
  dns 10.50.10.1 10.60.10.1
  domain company.com
  pool dynpool
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto ipsec security-association lifetime seconds 86400
!
crypto dynamic-map dynmap 1
  set transform-set vpn1
  reverse-route
!
crypto map static-map 1 ipsec-isakmp dynamic dynmap
crypto map dynmap isakmp authorization list rtr-remote
crypto map dynmap client configuration address respond
!
! Defines the key association and authentication for IPSec tunnel.
crypto isakmp policy 1
  hash md5
  authentication pre-share
  crypto isakmp key cisco123 address 200.1.1.1
!
! Defines encryption and transform set for the IPSec tunnel.
crypto ipsec transform-set set1 esp-3des esp-md5-hmac
!
! Associates all crypto values and peering address for the IPSec tunnel.
crypto map to_corporate 1 ipsec-isakmp
  set peer 200.1.1.1
  set transform-set set1
  match address 105
!
!
! VLAN 1 is the internal interface
interface vlan 1
  ip address 10.1.1.1 255.255.255.0
  ip nat inside
  ip inspect firewall in ! Inspection examines outbound traffic.
  crypto map static-map
  no cdp enable
!
! FE4 is the outside or Internet-exposed interface
interface fastethernet 4
  ip address 210.110.101.21 255.255.255.0
  ! acl 103 permits IPSec traffic from the corp. router as well as
  ! denies Internet-initiated traffic inbound.
  ip access-group 103 in
  ip nat outside
  no cdp enable
  crypto map to_corporate ! Applies the IPSec tunnel to the outside interface.

```

```
!  
! Utilize NAT overload in order to make best use of the  
! single address provided by the ISP.  
ip nat inside source list 102 interface Ethernet1 overload  
ip classless  
ip route 0.0.0.0 0.0.0.0 210.110.101.1  
no ip http server  
!  
!  
! acl 102 associated addresses used for NAT.  
access-list 102 permit ip 10.1.1.0 0.0.0.255 any  
! acl 103 defines traffic allowed from the peer for the IPSec tunnel.  
access-list 103 permit udp host 200.1.1.1 any eq isakmp  
access-list 103 permit udp host 200.1.1.1 eq isakmp any  
access-list 103 permit esp host 200.1.1.1 any  
! Allow ICMP for debugging but should be disabled because of security implications.  
access-list 103 permit icmp any any  
access-list 103 deny ip any any ! Prevents Internet-initiated traffic inbound.  
! acl 105 matches addresses for the IPSec tunnel to or from the corporate network.  
access-list 105 permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.255.255  
no cdp run
```

■ Configuration Example