Configuring a VPN Using Easy VPN and an IPSec Tunnel

This chapter provides an overview of the creation of Virtual Private Networks (VPNs) that can be configured on the Cisco 819, Cisco 860, and Cisco 880 series Integrated Services Routers (ISRs).

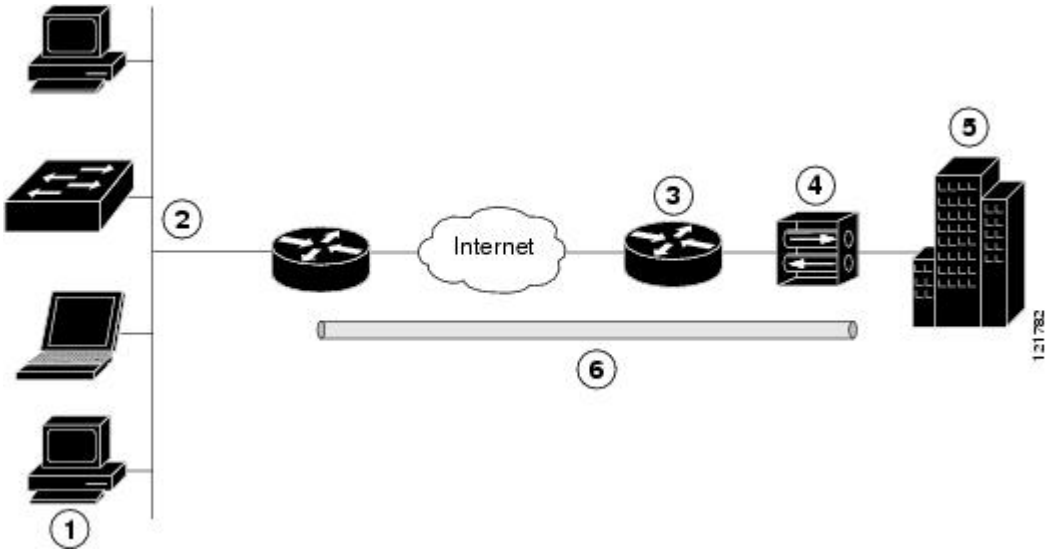
Configuring a VPN Using Easy VPN and an IPSec Tunnel

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 remote access VPN that uses the Cisco Easy VPN and an IP Security (IPSec) tunnel to configure and secure the connection between the remote client and the corporate network. The figure below shows a typical deployment scenario.

Figure 1: Remote Access VPN Using IPSec Tunnel



1	Remote, networked users
2	VPN client—Cisco 860 and Cisco 880 series ISRs
3	Router—Providing the corporate office network access
4	VPN server—Easy VPN server
5	Corporate office with a network address of 10.1.1.1
6	IPSec tunnel

Cisco Easy VPN

The Cisco Easy VPN client feature eliminates much of the tedious configuration work by implementing the Cisco Unity Client protocol. This protocol allows most VPN parameters, such as internal IP addresses, internal subnet masks, DHCP server addresses, WINS server addresses, and split-tunneling flags, to be defined at a VPN server that is acting as an IPSec server.

An Easy VPN server-enabled device can terminate VPN tunnels initiated by mobile and remote workers who are running Cisco Easy VPN Remote software on PCs. Easy VPN server-enabled devices allow remote routers to act as Easy VPN Remote nodes.

The Cisco Easy VPN client feature can be configured in one of two modes—client mode or network extension mode. Client mode is the default configuration and allows only devices at the client site to access resources

at the central site. Resources at the client site are unavailable to the central site. Network extension mode allows users at the central site to access network resources on the client site.

After the IPSec server has been configured, a VPN connection can be created with minimal configuration on an IPSec client, such as a supported Cisco 819, Cisco 860, and Cisco 880 series ISRs. When the IPSec client initiates the VPN tunnel connection, the IPSec server pushes the IPSec policies to the IPSec client and creates the corresponding VPN tunnel connection.

Note The Cisco Easy VPN client feature supports configuration of only one destination peer. If your application requires creation of multiple VPN tunnels, you must manually configure the IPSec VPN and Network Address Translation/Peer Address Translation (NAT/PAT) parameters on both the client and the server.

Configuration Tasks

Perform the following tasks to configure your router for this network scenario:

- Configuring the IKE Policy, on page 3
- Configuring Group Policy Information, on page 5
- Applying Mode Configuration to the Crypto Map, on page 6
- Enabling Policy Lookup, on page 7
- Configuring IPSec Transforms and Protocols, on page 8
- Configuring the IPSec Crypto Method and Parameters, on page 9
- Applying the Crypto Map to the Physical Interface, on page 10
- Creating an Easy VPN Remote Configuration , on page 11

An example showing the results of these configuration tasks is provided in the Configuration Examples for VPN and IPSec, on page 13.

Note The procedures in this chapter assume that you have already configured basic router features as well as PPPoE or PPPoA with NAT, DCHP and VLANs. If you have not performed these configurations tasks, see Basic Router Configuration, Configuring PPP over Ethernet with NAT,Configuring PPP over ATM with NAT, and Configuring a LAN with DHCP and VLANs as appropriate for your router.

Note The examples shown in this chapter refer only to the endpoint configuration on the Cisco 819, 860 and 880 series routers. Any VPN connection requires both endpoints to be configured properly to function. See the software configuration documentation as needed to configure the VPN for other router models.

Configuring the IKE Policy

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

SUMMARY STEPS

1. **crypto isakmp policy** *priority*
2. **encryption {des | 3des | aes | aes 192 | aes 256}**
3. **hash {md5 | sha}**
4. **authentication** {**rsa-sig | rsa-encr | pre-share**}
5. **group** {**1 | 2 | 5**}
6. **lifetime** *seconds*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**crypto isakmp policy** *priority* **Example:** `Router(config)# crypto isakmp policy 1`	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 the Internet Security Association Key and Management Protocol (ISAKMP) policy configuration mode.
Step 2	**encryption {des | 3des | aes | aes 192 | aes 256}** **Example:** `Router(config-isakmp)# encryption 3des`	Specifies the encryption algorithm used in the IKE policy. The example specifies 168-bit data encryption standard (DES).
Step 3	**hash {md5 | sha}** **Example:** `Router(config-isakmp)# hash md5`	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`	Specifies the authentication method used in the IKE policy. The example specifies a pre-shared key.
Step 5	**group** {**1 | 2 | 5**} **Example:** `Router(config-isakmp)#group 2`	Specifies the Diffie-Hellman group to be used in an IKE policy.
Step 6	**lifetime** *seconds* **Example:** `Router(config-isakmp)# lifetime 480`	Specifies the lifetime, in seconds, for an IKE security association (SA). • Acceptable values are from 60 to 86400.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Router(config-isakmp)# exit`	Exits ISAKMP policy configuration mode and returns to global configuration mode.

Configuring Group Policy Information

To configure the group policy, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **crypto isakmp client configuration group** {**group-name** | **default**}
2. **key** *name*
3. dns *primary-server*
4. **domain** *name*
5. **exit**
6. **ip local pool** {**default** | *poolname*} [*low-ip-address [high-ip-address*]]

DETAILED STEPS

	Command or Action	Purpose

Step 1	**crypto isakmp client configuration group** {**group-name**	**default**}
		
		Example:
		
		`Router(config)# crypto isakmp client configuration group rtr-remote`
		
		`Router(config-isakmp-group)#`
			Creates an IKE policy group containing attributes to be downloaded to the remote client.
			
			Also enters the Internet Security Association Key and Management Protocol (ISAKMP) group policy configuration mode.

Step 2	**key** *name* **Example:** `Router(config-isakmp-group)# key secret-password`	Specifies the IKE pre-shared key for the group policy.
Step 3	dns *primary-server* **Example:** `Router(config-isakmp-group)# dns 10.50.10.1`	Specifies the primary Domain Name System (DNS) server for the group. **Note** To specify Windows Internet Naming Service (WINS) servers for the group, use the **wins** command.

	Command or Action	Purpose
Step 4	**domain** *name* **Example:** `Router(config-isakmp-group)# domain company.com`	Specifies group domain membership.

Step 5	**exit**
	
	Example:
	
	`Router(config-isakmp-group)# exit`
	
	`Router(config)#`
		Exits ISAKMP policy configuration mode and returns to global configuration mode.

Step 6	**ip local pool** {**default** | *poolname*} [*low-ip-address* *[high-ip-address*]] **Example:** `Router(config)# ip local pool dynpool 30.30.30.20 30.30.30.30`	Specifies a local address pool for the group. For details about this command and additional parameters that can be set, see Cisco IOS Dial Technologies Command Reference.

Applying Mode Configuration to the Crypto Map

To apply mode configuration to the crypto map, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **crypto map** *map-name* **isakmp authorization list** *list-name*
2. **crypto map** *tag* **client configuration address [initiate | respond]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**crypto map** *map-name* **isakmp authorization list** *list-name* **Example:** `Router(config)# crypto map dynmap isakmp authorization list rtr-remote`	Applies mode configuration to the crypto map and enables key lookup (IKE queries) for the group policy from an authentication, authorization, and accounting (AAA) server.

	Command or Action	Purpose
Step 2	**crypto map** *tag* **client configuration address [initiate | respond]** **Example:** `Router(config)# crypto map dynmap client configuration address respond`	Configures the router to reply to mode configuration requests from remote clients.

Enabling Policy Lookup

To enable policy lookup through AAA, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **aaa new-model**
2. **aaa authentication login {default |** *list-name***}** *method1* **[***method2...***]**
3. **aaa authorization {network | exec | commands** *level* **| reverse-access | configuration} {default |** *list-name***} [***method1* **[***method2...***]]**
4. **username** *name* **{nopassword | password** *password* **| password** *encryption-type encrypted-password***}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**aaa new-model** **Example:** `Router(config)# aaa new-model`	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`	Specifies AAA authentication of selected users at login, and specifies the method used. • This example uses a local authentication database. **Note** You could also use a RADIUS server for this. For details, see Cisco IOS Security Configuration Guide and Cisco IOS Security Command Reference.
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`	Specifies AAA authorization of all network-related service requests, including PPP, and specifies the method of authorization. • This example uses a local authorization database.

	Command or Action	Purpose
		Note You could also use a RADIUS server for this. For details, see the Cisco IOS Security Configuration Guide and Cisco IOS Security Command Reference.
Step 4	**username** *name* {**nopassword** | **password** *password* | **password** *encryption-type encrypted-password*} **Example:** `Router(config)# username Cisco password 0 Cisco`	Establishes a username-based authentication system.

Configuring 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 peer configurations.

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

SUMMARY STEPS

1. **crypto ipsec transform-set** *transform-set-name transform1 [transform2] [transform3] [transform4]*
2. **crypto ipsec security-association lifetime** *{***seconds** *seconds* | **kilobytes** *kilobytes}*

DETAILED STEPS

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

What to Do Next

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

Configuring 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).

To configure the IPSec crypto method, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
2. **set transform-set** *transform-set-name [transform-set-name2...transform-set-name6]*
3. **reverse-route**
4. **exit**
5. **crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]

DETAILED STEPS

	Command or Action	Purpose

Step 1	**crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
	
	Example:
	`Router(config)# crypto dynamic-map dynmap 1`
	`Router(config-crypto-map)#`
		Creates a dynamic crypto map entry and enters crypto map configuration mode.
		See Cisco IOS Security Command Reference for details about this command.

Step 2	**set transform-set** *transform-set-name [transform-set-name2...transform-set-name6]* **Example:** `Router(config-crypto-map)# set transform-set vpn1`	Specifies which transform sets can be used with the crypto map entry.
Step 3	**reverse-route** **Example:** `Router(config-crypto-map)# reverse-route`	Creates source proxy information for the crypto map entry.

	Command or Action	Purpose

Step 4	**exit**
	
	Example:
	`Router(config-crypto-map)# exit`
	`Router(config)#`
		Exits crypto map configuration mode and returns to global configuration mode.

Step 5	**crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*] **Example:** `Router(config)# crypto map static-map 1 ipsec-isakmp dynamic dynmap`	Creates a crypto map profile.

Applying the Crypto Map to the Physical Interface

The crypto maps must be applied to each interface through which IP Security (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.

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

SUMMARY STEPS

1. **interface** *type number*
2. **crypto map** *map-name*
3. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**interface** *type number*
	
	Example:
	`Router(config)# interface fastethernet 4`
	`Router(config-if)#`
		Enters the interface configuration mode for the interface to which the crypto map applies.

Step 2	**crypto map** *map-name*	Applies the crypto map to the interface.

	Command or Action	Purpose
	Example: `Router(config-if)# crypto map static-map`	See Cisco IOS Security Command Reference for details about this command.

Step 3	**exit**
	Example:
	`Router(config-crypto-map)# exit`
	`Router(config)#`
		Exits interface configuration mode and returns to global configuration mode.

Creating an Easy VPN Remote Configuration

The router acting as the IPSec remote router must create an Easy VPN remote configuration and assign it to the outgoing interface.

To create the remote configuration, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **crypto ipsec client ezvpn** *name*
2. **group** *group-name* **key** *group-key*
3. **peer** {*ipaddress* | *hostname*}
4. **mode** {**client** | **network-extension** | **network extension plus**}
5. **exit**
6. **interface** *type number*
7. **crypto ipsec client ezvpn** *name* [**outside** | **inside**]
8. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**crypto ipsec client ezvpn** *name*
	Example:
	`Router(config)# crypto ipsec client ezvpn ezvpnclient`
	`Router(config-crypto-ezvpn)#`
		Creates a Cisco Easy VPN remote configuration, and enters Cisco Easy VPN remote configuration mode.

	Command or Action	Purpose

Step 2	**group** *group-name* **key** *group-key*
	
	Example:
	`Router(config-crypto-ezvpn)# group ezvpnclient key secret-password`
	`Router(config-crypto-ezvpn)#`
		Specifies the IPSec group and IPSec key value for the VPN connection.

Step 3	**peer** {*ipaddress* | *hostname*}
	
	Example:
	`Router(config-crypto-ezvpn)# peer 192.168.100.1`
	`Router(config-crypto-ezvpn)#`
		Specifies the peer IP address or hostname for the VPN connection.
		Note A hostname can be specified only when the router has a DNS server available for hostname resolution.

Step 4	**mode** {**client** | **network-extension** | **network extension plus**}
	
	Example:
	`Router(config-crypto-ezvpn)# mode client`
	`Router(config-crypto-ezvpn)#`
		Specifies the VPN mode of operation.

Step 5	**exit**
	
	Example:
	`Router(config-crypto-ezvpn)# exit`
	`Router(config)#`
		Exits Cisco Easy VPN remote configuration mode and returns to global configuration mode.

Step 6	**interface** *type number*
	
	Example:
	`Router(config)# interface fastethernet 4`
	`Router(config-if)#`
		Enters the interface configuration mode for the interface to which the Cisco Easy VPN remote configuration applies.
		Note For routers with an ATM WAN interface, this command would be **interface atm 0**.

Step 7	**crypto ipsec client ezvpn** *name* [**outside** | **inside**]
	
	Example:
	`Router(config-if)# crypto ipsec client ezvpn ezvpnclient outside`
	`Router(config-if)#`
		Assigns the Cisco Easy VPN remote configuration to the WAN interface.
		This command causes the router to automatically create the NAT or port address translation (PAT) and access list configuration needed for the VPN connection.

Step 8	**exit**
	
	Example:
	`Router(config-crypto-ezvpn)# exit`
	`Router(config)#`
		Exits interface configuration mode and returns to global configuration mode.

Verifying Your Easy VPN Configuration

```
Router# show crypto ipsec client ezvpn
Tunnel name :ezvpnclient
Inside interface list:vlan 1
Outside interface:fastethernet 4
Current State:IPSEC_ACTIVE
Last Event:SOCKET_UP
Address:8.0.0.5
Mask:255.255.255.255
Default Domain:cisco.com
```

Configuration Examples for VPN and IPSec

The following configuration example shows a portion of the configuration file for the VPN and IPSec tunnel described in this chapter.

```
!
aaa new-model
!
aaa authentication login rtr-remote local
aaa authorization network rtr-remote local
aaa session-id common
!
username Cisco password 0 Cisco
!
crypto isakmp policy 1
 encryption 3des
 authentication pre-share
 group 2
 lifetime 480
!
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
crypto ipsec client ezvpn ezvpnclient
 connect auto
 group 2 key secret-password
 mode client
 peer 192.168.100.1
!
interface fastethernet 4
 crypto ipsec client ezvpn ezvpnclient outside
 crypto map static-map
!
interface vlan 1
```

```
 crypto ipsec client ezvpn ezvpnclient inside
!
```