



CHAPTER 5

Configuring Security Features

This chapter provides an overview of authentication, authorization, and accounting (AAA), which is the primary Cisco framework for implementing selected security features that can be configured on the Cisco 860 and Cisco 880 series Integrated Services Routers (ISRs).

This chapter contains the following sections:

- [Authentication, Authorization, and Accounting, page 5-1](#)
- [Configuring AutoSecure, page 5-2](#)
- [Configuring Access Lists, page 5-2](#)
- [Configuring Cisco IOS Firewall, page 5-3](#)
- [Configuring Cisco IOS IPS, page 5-4](#)
- [URL Filtering, page 5-4](#)
- [Configuring VPN, page 5-4](#)

Authentication, Authorization, and Accounting

AAA network security services provide the primary framework through which you set up access control on your router. Authentication provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you choose, encryption. Authorization provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, Internetwork Packet Exchange (IPX), AppleTalk Remote Access (ARA), and Telnet. Accounting provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

AAA uses protocols such as RADIUS, TACACS+, or Kerberos to administer its security functions. If your router is acting as a network access server, AAA is the means through which you establish communication between your network access server and your RADIUS, TACACS+, or Kerberos security server.

For information about configuring AAA services and supported security protocols, see the following sections of the *Cisco IOS Release 12.4T Security Configuration Guide* at http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4t/sec_12_4t_book.html:

- [Configuring Authentication](#)
- [Configuring Authorization](#)
- [Configuring Accounting](#)
- [Configuring RADIUS](#)
- [Configuring TACACS+](#)
- [Configuring Kerberos](#)

Configuring AutoSecure

The AutoSecure feature disables common IP services that can be exploited for network attacks and enables IP services and features that can aid in the defense of a network when under attack. These IP services are all disabled and enabled simultaneously with a single command, greatly simplifying security configuration on your router. For a complete description of the AutoSecure feature, see the *AutoSecure* feature document at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123_1/ftatosec.htm.

Configuring Access Lists

Access lists permit or deny network traffic over an interface based on source IP address, destination IP address, or protocol. Access lists are configured as standard or extended. A standard access list either permits or denies passage of packets from a designated source. An extended access list allows designation of both the destination and the source, and it allows designation of individual protocols to be permitted or denied passage.

For more complete information on creating access lists, see the “[Access Control Lists: Overview and Guidelines](#)” section of the *Cisco IOS Release 12.4 Security Configuration Guide* at http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.html.

An access list is a series of commands with a common tag to bind them together. The tag is either a number or a name. [Table 5-1](#) lists the commands used to configure access lists.

Table 5-1 Access List Configuration Commands

| ACL Type | Configuration Commands |
|-----------------|---|
| Numbered | |
| Standard | access-list {1-99}{ permit deny } <i>source-addr</i> [<i>source-mask</i>] |
| Extended | access-list {100-199}{ permit deny } <i>protocol</i> <i>source-addr</i> [<i>source-mask</i>] <i>destination-addr</i> [<i>destination-mask</i>] |
| Named | |
| Standard | ip access-list standard <i>name</i> deny { <i>source</i> <i>source-wildcard</i> any } |
| Extended | ip access-list extended <i>name</i> { permit deny } <i>protocol</i> { <i>source-addr</i> [<i>source-mask</i>] any }{ <i>destination-addr</i> [<i>destination-mask</i>] any } |

To create, refine, and manage access lists, see the following sections of the “Traffic Filtering, Firewalls, and Virus Detection” part of the *Cisco IOS Release 12.4T Security Configuration Guide* at http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4t/sec_12_4t_book.html:

- [Creating an IP Access List and Applying It to an Interface](#)
- [Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values](#)
- [Refining an IP Access List](#)
- [Displaying and Clearing IP Access List Data Using ACL Manageability](#)

Access Groups

An access group is a sequence of access list definitions bound together with a common name or number. An access group is enabled for an interface during interface configuration. Use the following guidelines when creating access groups.

- The order of access list definitions is significant. A packet is compared against the first access list in the sequence. If there is no match (that is, if neither a permit nor a deny occurs), the packet is compared with the next access list, and so on.
- All parameters must match the access list before the packet is permitted or denied.
- There is an implicit “deny all” at the end of all sequences.

For information on configuring and managing access groups, see the ““[Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values](#)” section of the *Cisco IOS Release 12.4T Security Configuration Guide* at

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4t/sec_12_4t_book.html.

Configuring Cisco IOS Firewall

The Cisco IOS Firewall lets you configure a stateful firewall where packets are inspected internally and the state of network connections is monitored. Stateful firewall is superior to static access lists, because access lists can only permit or deny traffic based on individual packets, not based on streams of packets. Also, because Cisco IOS Firewall inspects the packets, decisions to permit or deny traffic can be made by examining application layer data, which static access lists cannot examine.

To configure a Cisco IOS Firewall, specify which protocols to examine by using the following command in interface configuration mode:

```
ip inspect name inspection-name protocol timeout seconds
```

When inspection detects that the specified protocol is passing through the firewall, a dynamic access list is created to allow the passage of return traffic. The timeout parameter specifies the length of time the dynamic access list remains active without return traffic passing through the router. When the timeout value is reached, the dynamic access list is removed, and subsequent packets (possibly valid ones) are not permitted.

Use the same inspection name in multiple statements to group them into one set of rules. This set of rules can be activated elsewhere in the configuration by using the **ip inspect inspection-name in | out** command when you configure an interface at the firewall.

For additional information about configuring a Cisco IOS Firewall, see the “[Cisco IOS Firewall Overview](#)” section of the *Cisco IOS Release 12.4 Security Configuration Guide* at

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.html.

The Cisco IOS Firewall may also be configured to provide voice security in Session Initiated Protocol (SIP) applications. SIP inspection provides basic inspect functionality (SIP packet inspection and detection of pin-hole openings), as well protocol conformance and application security. For more information, see “[Cisco IOS Firewall: SIP Enhancements: ALG and AIC](http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_sip_alg_aic.html)” at http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_sip_alg_aic.html.

Configuring Cisco IOS IPS

Cisco IOS Intrusion Prevention System (IPS) technology is available on Cisco 880 series ISRs and enhances perimeter firewall protection by taking appropriate action on packets and flows that violate the security policy or represent malicious network activity.

Cisco IOS IPS identifies attacks using “signatures” to detect patterns of misuse in network traffic. Cisco IOS IPS acts as an in-line intrusion detection sensor, watching packets and sessions as they flow through the router, scanning each to match known IPS signatures. When Cisco IOS IPS detects suspicious activity, it responds before network security can be compromised, it logs the event, and, depending on configuration, it does one of the following:

- sends an alarm
- drops suspicious packets
- resets the connection
- denies traffic from the source IP address of the attacker for a specified amount of time
- denies traffic on the connection for which the signature was seen for a specified amount of time

For additional information about configuring Cisco IOS IPS, see the “[Configuring Cisco IOS Intrusion Prevention System \(IPS\)](http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4t/sec_12_4t_book.html)” section of the *Cisco IOS Release 12.4T Security Configuration Guide* at http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4t/sec_12_4t_book.html.

URL Filtering

Cisco 860 series and Cisco 880 series ISRs provide category based URL filtering. The user provisions URL filtering on the ISR by selecting categories of websites to be permitted or blocked. An external server, maintained by a 3rd party, will be used to check for URLs in each category. Permit and deny policies are maintained on the ISR. The service is subscription based, and the URLs in each category are maintained by the 3rd party vendor.

For additional information about configuring URL filtering, see [Subscription-based Cisco IOS Content Filtering](http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_url_filtering.html) at http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_url_filtering.html.

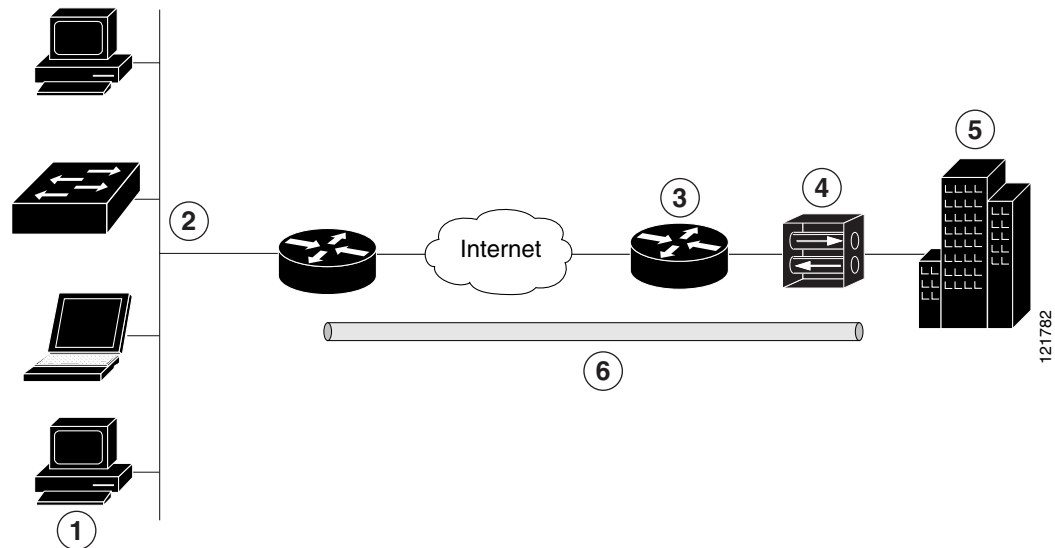
Configuring VPN

A virtual private network (VPN) connection provides a secure connection between two networks over a public network such as the Internet. Cisco 860 and Cisco 880 series ISRs support two types of VPNs—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. Two examples are given in this section: remote access VPN and site-to-site VPN.

Remote Access VPN

The configuration of a remote access VPN uses Cisco Easy VPN and an IP Security (IPSec) tunnel to configure and secure the connection between the remote client and the corporate network. Figure 5-1 shows a typical deployment scenario.

Figure 5-1 Remote Access VPN Using IPSec Tunnel



| | |
|---|---|
| 1 | Remote networked users |
| 2 | VPN client—Cisco 880 series access router |
| 3 | Router—Providing the corporate office network access |
| 4 | VPN server—Easy VPN server; for example, a Cisco VPN 3000 concentrator with outside interface address 210.110.101.1 |
| 5 | Corporate office with a network address of 10.1.1.1 |
| 6 | IPSec tunnel |

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, Windows Internet Naming Service (WINS) server addresses, and split-tunneling flags, to be defined at a VPN server, such as a Cisco VPN 3000 series concentrator that is acting as an IPSec server.

A Cisco 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. Cisco Easy VPN server-enabled devices allow remote routers to act as Cisco 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 (where the VPN 3000 series concentrator is located) 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 880 series ISR. 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**

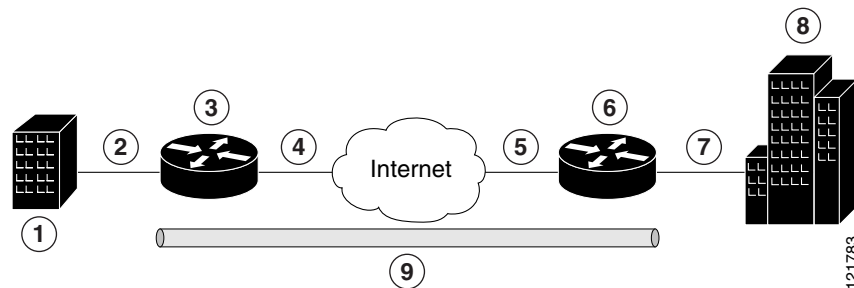
The Cisco Easy VPN client feature supports configuration of only one destination peer. If your application requires creation of multiple VPN tunnels, you must manually configure the IPsec VPN and Network Address Translation/Peer Address Translation (NAT/PAT) parameters on both the client and the server.

Cisco 860 and Cisco 880 series ISRs can be also configured to act as Cisco Easy VPN servers, letting authorized Cisco Easy VPN clients establish dynamic VPN tunnels to the connected network. For information on the configuration of Cisco Easy VPN servers see the *Easy VPN Server* feature document at http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ftunity.html.

Site-to-Site VPN

The configuration of a site-to-site VPN uses IPsec and the generic routing encapsulation (GRE) protocol to secure the connection between the branch office and the corporate network. [Figure 5-2](#) shows a typical deployment scenario.

Figure 5-2 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 192.165.0.0/16 (also the inside interface for NAT) |
| 3 | VPN client—Cisco 860 or Cisco 880 series ISR |
| 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 |

For more information about IPsec and GRE configuration, see the “Configuring Security for VPNs with IPsec” chapter of the *Cisco IOS Release 12.4T Security Configuration Guide* at http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4t/sec_12_4t_book.html.

Configuration Examples

Each example configures a VPN over an IPsec tunnel, using the procedure given in the “[Configure a VPN over an IPsec Tunnel](#)” section on page 5-7. Then, the specific procedure for a remote access configuration is given, followed by the specific procedure for a site-to-site configuration.

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

VPN configuration information must be configured on both endpoints. You must specify parameters, such as internal IP addresses, internal subnet masks, DHCP server addresses, and Network Address Translation (NAT).

- [Configure a VPN over an IPsec Tunnel](#), page 5-7
- [Create a Cisco Easy VPN Remote Configuration](#), page 5-13
- [Configure a Site-to-Site GRE Tunnel](#), page 5-16

Configure a VPN over an IPsec Tunnel

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

- [Configure the IKE Policy](#), page 5-7
- [Configure Group Policy Information](#), page 5-8
- [Apply Mode Configuration to the Crypto Map](#), page 5-9
- [Enable Policy Lookup](#), page 5-10
- [Configure IPsec Transforms and Protocols](#), page 5-11
- [Configure the IPsec Crypto Method and Parameters](#), page 5-11
- [Apply the Crypto Map to the Physical Interface](#), page 5-12
- [Where to Go Next](#), page 5-13

Configure the IKE Policy

To configure the Internet Key Exchange (IKE) policy, perform these steps, 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 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 Router(config-isakmp)# | Specifies the encryption algorithm used in the IKE policy. The example specifies 168-bit data encryption standard (DES). |

| | Command or Action | Purpose |
|--------|--|--|
| Step 3 | hash {md5 sha} Example: <pre>Router(config-isakmp)# hash md5 Router(config-isakmp)#</pre> | 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: <pre>Router(config-isakmp)# authentication pre-share Router(config-isakmp)#</pre> | Specifies the authentication method used in the IKE policy. The example specifies a pre-shared key. |
| Step 5 | group {1 2 5} Example: <pre>Router(config-isakmp)# group 2 Router(config-isakmp)#</pre> | Specifies the Diffie-Hellman group to be used in an IKE policy. |
| Step 6 | lifetime <i>seconds</i> Example: <pre>Router(config-isakmp)# lifetime 480 Router(config-isakmp)#</pre> | Specifies the lifetime, from 60 to 86400 seconds, for an IKE security association (SA). |
| Step 7 | exit Example: <pre>Router(config-isakmp)# exit Router(config)#</pre> | Exits IKE policy configuration mode, and enters global configuration mode. |

Configure Group Policy Information

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

| | Command or Action | Purpose |
|--------|--|---|
| Step 1 | crypto isakmp client configuration group {group-name default} Example: <pre>Router(config)# crypto isakmp client configuration group rtr-remote Router(config-isakmp-group)#</pre> | 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. |

| | Command or Action | Purpose |
|--------|---|---|
| Step 2 | <p>key name</p> <p>Example:</p> <pre>Router(config-isakmp-group)# key secret-password Router(config-isakmp-group)#</pre> | Specifies the IKE pre-shared key for the group policy. |
| 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> | Specifies the primary Domain Name System (DNS) server for the group. You may also want to specify Windows Internet Naming Service (WINS) servers for the group by using the wins command. |
| Step 4 | <p>domain name</p> <p>Example:</p> <pre>Router(config-isakmp-group)# domain company.com Router(config-isakmp-group)#</pre> | Specifies group domain membership. |
| Step 5 | <p>exit</p> <p>Example:</p> <pre>Router(config-isakmp-group)# exit Router(config)#</pre> | Exits IKE group policy configuration mode, and enters global configuration mode. |
| 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> | Specifies a local address pool for the group. For details about this command and additional parameters that can be set, see the Cisco IOS Dial Technologies Command Reference . |

Apply Mode Configuration to the Crypto Map

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

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | <p>crypto map map-name isakmp authorization list list-name</p> <p>Example:</p> <pre>Router(config)# crypto map dynmap isakmp authorization list rtr-remote Router(config)#</pre> | 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: <pre>Router(config)# crypto map dynmap client configuration address respond Router(config)#</pre> | Configures the router to reply to mode configuration requests from remote clients. |

Enable Policy Lookup

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

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

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 a transform set is found that contains such a transform, it is selected and applied to the protected traffic as a part of both peers' configurations.

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

| | Command or Action | Purpose |
|--------|--|---|
| Step 1 | crypto ipsec profile <i>profile-name</i> Example: Router(config)# crypto ipsec profile pro1 Router(config)# | Configures IPSec profile to apply protection on the tunnel for encryption. |
| Step 2 | 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 vpn1 esp-3des esp-sha-hmac 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 3 | crypto ipsec security-association lifetime { seconds <i>seconds</i> kilobytes <i>kilobytes</i> } Example: Router(config)# crypto ipsec security-association lifetime seconds 86400 Router(config)# | Specifies global lifetime values used when IPSec security associations are negotiated. See the Cisco IOS Security Command Reference for details. |

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).

To configure the IPSec crypto method, perform these steps, 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 dynmap 1 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. |

| | Command or Action | Purpose |
|--------|--|---|
| Step 2 | <p>set transform-set <i>transform-set-name</i> [<i>transform-set-name2...transform-set-name6</i>]</p> <p>Example:</p> <pre>Router(config-crypto-map)# set transform-set vpn1 Router(config-crypto-map)#</pre> | Specifies which transform sets can be used with the crypto map entry. |
| Step 3 | <p>reverse-route</p> <p>Example:</p> <pre>Router(config-crypto-map)# reverse-route Router(config-crypto-map)#</pre> | Creates source proxy information for the crypto map entry. See the Cisco IOS Security Command Reference for details. |
| Step 4 | <p>exit</p> <p>Example:</p> <pre>Router(config-crypto-map)# exit Router(config)#</pre> | Returns to global configuration mode. |
| Step 5 | <p>crypto map <i>map-name seq-num</i> [ipsec-isakmp] [dynamic <i>dynamic-map-name</i>] [discover] [profile <i>profile-name</i>]</p> <p>Example:</p> <pre>Router(config)# crypto map static-map 1 ipsec-isakmp dynamic dynmap Router(config)#</pre> | 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.

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

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

| | Command or Action | Purpose |
|--------|--|--|
| Step 2 | crypto map <i>map-name</i> Example: Router(config-if)# crypto map static-map 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-crypto-map)# exit Router(config)# | Returns to global configuration mode. |

Where to Go Next

If you are creating a Cisco Easy VPN remote configuration, go to the [“Create a Cisco Easy VPN Remote Configuration”](#) section on page 5-13.

If you are creating a site-to-site VPN using IPsec tunnels and GRE, go to the [“Configure a Site-to-Site GRE Tunnel”](#) section on page 5-16.

Create a Cisco Easy VPN Remote Configuration

The router acting as the Cisco Easy VPN client must create a Cisco Easy VPN remote configuration and assign it to the outgoing interface.

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

| | Command or Action | Purpose |
|--------|--|---|
| Step 1 | crypto ipsec client ezvpn <i>name</i> 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. |
| Step 2 | group <i>group-name</i> key <i>group-key</i> 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. |

| | Command or Action | Purpose |
|--------|---|--|
| Step 3 | <p>peer {<i>ipaddress</i> <i>hostname</i>}</p> <p>Example:</p> <pre>Router(config-crypto-ezvpn)# peer 192.168.100.1 Router(config-crypto-ezvpn)#</pre> | <p>Specifies the peer IP address or hostname for the VPN connection.</p> <p>Note A hostname can be specified only when the router has a DNS server available for hostname resolution.</p> <p>Note Use this command to configure multiple peers for use as backup. If one peer goes down, the Easy VPN tunnel is established with the second available peer. When the primary peer comes up again, the tunnel is reestablished with the primary peer.</p> |
| Step 4 | <p>mode {<i>client</i> network-extension network extension plus}</p> <p>Example:</p> <pre>Router(config-crypto-ezvpn)# mode client Router(config-crypto-ezvpn)#</pre> | <p>Specifies the VPN mode of operation.</p> |
| Step 5 | <p>exit</p> <p>Example:</p> <pre>Router(config-crypto-ezvpn)# exit Router(config)#</pre> | <p>Returns to global configuration mode.</p> |
| Step 6 | <p>crypto isakmp keepalive <i>seconds</i></p> <p>Example:</p> <pre>Router(config-crypto-ezvpn)# crypto isakmp keepalive 10 Router(config)#</pre> | <p>Enables dead peer detection messages. Time between messages is given by <i>seconds</i>, with a range of 10 to 3600.</p> |
| Step 7 | <p>interface <i>type number</i></p> <p>Example:</p> <pre>Router(config)# interface fastethernet 4 Router(config-if)#</pre> | <p>Enters the interface configuration mode for the interface to which you want the Cisco Easy VPN remote configuration applied.</p> <p>Note For routers with an ATM WAN interface, this command would be interface atm 0.</p> |

| | Command or Action | Purpose |
|--------|---|---|
| Step 8 | crypto ipsec client ezvpn <i>name</i> [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, causing the router to automatically create the NAT or port address translation (PAT) and access list configuration needed for the VPN connection. |
| Step 9 | exit Example: Router(config-crypto-ezvpn)# exit Router(config)# | Returns to global configuration mode. |

Configuration Example

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
!

```

Configure a Site-to-Site GRE Tunnel

To configure a GRE tunnel, perform these steps, beginning in global configuration mode:

| | Command or Action | Purpose |
|--------|--|---|
| Step 1 | interface <i>type number</i> Example: Router(config)# interface tunnel 1 Router(config-if)# | Creates a tunnel interface and enters interface configuration mode. |
| Step 2 | ip address <i>ip-address mask</i> Example: Router(config-if)# 10.62.1.193 255.255.255.252 Router(config-if)# | Assigns an address to the tunnel. |
| Step 3 | tunnel source <i>interface-type number</i> Example: Router(config-if)# tunnel source fastethernet 0 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 192.168.101.1 Router(config-if)# | Specifies the destination endpoint of the router for the GRE tunnel. |
| Step 5 | crypto map <i>map-name</i> Example: Router(config-if)# crypto map static-map 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. |

| | Command or Action | Purpose |
|--------|--|---|
| 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} access-list-name Example: Router(config)# ip access-list extended vpnstatic1 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 destination destination-wildcard Example: Router(config-acl)# permit gre host 192.168.100.1 host 192.168.101.1 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 home network.
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
```

