



Configuring the VPN Acceleration Module

This chapter contains the information and procedures needed to configure the VPN Acceleration Module (VAM) in Cisco 7401ASR routers. This chapter contains the following sections:

- [Overview, page 4-1](#)
- [Configuration Tasks, page 4-1](#)

Overview

The VAM provides encryption services for Cisco 7401ASR routers. You must configure IPSec on the router for the VAM to provide encryption services.



Note

There are no interfaces to configure on the VAM.

This chapter contains basic configuration information for enabling encryption and IPSec tunneling services. Refer to the [Cisco Enterprise VPN Configuration Guide](#), the [VPN Acceleration Module Installation and Configuration Guide](#), the “IP Security and Encryption” part of the [Security Configuration Guide](#) and the [Security Command Reference](#) for detailed configuration information on IPSec, IKE, and CA.

Configuration Tasks

If the ENABLE LED is on on power up, the VAM is fully functional and does not require any configuration commands. However, for the VAM to provide encryption services, you must complete the steps in the following sections:

- [Configuring IKE, page 4-2](#) (required)
- [Configuring IPSec, page 4-3](#) (required)



Note

You can configure a static crypto map, create a dynamic crypto map, or add a dynamic crypto map into a static crypto map. Refer to Chapter 3, “[Site-to-Site and Extranet VPN Business Scenarios](#),” of the online publication [Cisco IOS Enterprise VPN Configuration Guide](#).

Optionally, you can configure Certification Authority (CA) interoperability (refer to the “[Configuring Certification Authority Interoperability](#)” chapter in the [Security Configuration Guide](#)).

Using the EXEC Command Interpreter

You modify the configuration of your router through the software command interpreter called the *EXEC* (also called enable mode). You must enter the privileged level of the EXEC command interpreter with the **enable** command before you can use the **configure** command to configure a new interface or change the existing configuration of an interface. The system prompts you for a password if one has been set.

The system prompt for the privileged level ends with a pound sign (#) instead of an angle bracket (>). At the console terminal, use the following procedure to enter the privileged level:

-
- Step 1** At the user-level EXEC prompt, enter the **enable** command. The EXEC prompts you for a privileged-level password as follows:
- ```
Router> enable

Password:
```
- Step 2** Enter the password (the password is case sensitive). For security purposes, the password is not displayed. When you enter the correct password, the system displays the privileged-level system prompt (#):
- ```
Router#
```
-

This completes the procedure for entering the privileged level of the EXEC command interpreter.

Configuring IKE

If you do not specify a value for a parameter, the default value is assigned. For information on default values, refer to the “IP Security and Encryption” chapter of the *Security Command Reference* publication.

To configure a policy, use the following commands, starting in global configuration mode:

	Command	Purpose
Step 1	crypto isakmp policy <i>priority</i>	Identifies the policy to create, and enters config-isakmp command mode.
Step 2	encryption {des 3des}	Specifies the encryption algorithm.
Step 3	group {1 2}	Specifies the Diffie-Hellman group identifier.

For detailed information on creating IKE policies, refer to the “Configuring Internet Key Exchange Security Protocol” chapter in the *Security Configuration Guide* publication.

Configuring IPsec

After you have completed IKE configuration, configure IPsec at each participating IPsec peer. This section contains basic steps to configure IPsec and includes the tasks discussed in the following sections:

- [Creating Crypto Access Lists, page 4-3](#)
- [Defining Transform Sets, page 4-4](#)
- [Creating Crypto Map Entries, page 4-5](#)
- [Verifying the Configuration, page 4-6](#)

For detailed information on configuring IPsec, refer to the “[Configuring IPsec Network Security](#)” chapter in the *Security Configuration Guide* publication.

Creating Crypto Access Lists

Crypto access lists define which IP traffic will be protected by encryption.



Note

IKE uses UDP port 500. The IPsec Encapsulation Security Protocol (ESP) and Authentication Header (AH) protocols use protocol numbers 50 and 51. Ensure that your interface access lists are configured so that protocol numbers 50, 51, and UDP port 500 traffic are not blocked at interfaces used by IPsec. In some cases you might need to add a statement to your access lists to explicitly permit this traffic.

To create crypto access lists, use the following commands in global configuration mode:

Step	Command	Purpose
Step 1	<code>access-list access-list-number {deny permit} protocol source source-wildcard destination destination-wildcard [log]</code> or <code>ip access-list extended name</code>	Specifies conditions to determine which IP packets are protected. ¹ (Enable or disable encryption for traffic that matches these conditions.) We recommend that you configure “mirror image” crypto access lists for use by IPsec and that you avoid using the any keyword.
Step 2	Add permit and deny statements as appropriate.	Adds permit or deny statements to access lists.
Step 3	<code>end</code>	Exits the configuration command mode.

1. You specify conditions using an IP access list designated by either a number or a name. The **access-list** command designates a numbered extended access list; the **ip access-list extended** command designates a named access list.

For detailed information on configuring access lists, refer to the “[Configuring IPsec Network Security](#)” chapter in the *Security Configuration Guide* publication.

Defining Transform Sets

A transform set is a combination of security protocols and algorithms. During the IPsec security association negotiation, peers agree to use a specific transform set to protect a particular data flow.

To define a transform set, use the following commands, starting in global configuration mode:

	Command	Purpose
Step 1	crypto ipsec transform-set <i>transform-set-name transform1 [transform2 [transform3]]</i>	Defines a transform set and enters crypto transform configuration mode. Note Complex rules define which entries you can use for the transform arguments. These rules are explained in the command description for the crypto ipsec transform-set command, and Table 4-1 provides a list of allowed transform combinations.
Step 2	mode [tunnel transport]	Changes the mode associated with the transform set. The mode setting is applicable only to traffic whose source and destination addresses are the IPsec peer addresses; it is ignored for all other traffic. (All other traffic is in tunnel mode only.)
Step 3	end	Exits the crypto transform configuration mode to enabled mode.
Step 4	clear crypto sa or clear crypto sa peer { <i>ip-address</i> <i>peer-name</i> } or clear crypto sa map <i>map-name</i> or clear crypto sa spi <i>destination-address protocol spi</i>	Clears existing IPsec security associations so that any changes to a transform set take effect on subsequently established security associations (SAs). (Manually established SAs are reestablished immediately.) Using the clear crypto sa command without parameters clears out the full SA database, which clears out active security sessions. You may also specify the peer , map , or entry keywords to clear out only a subset of the SA database.

[Table 4-1](#) shows allowed transform combinations.

Table 4-1 Allowed Transform Combinations

AH Transform ¹		ESP Encryption Transform ¹		ESP Authentication Transform ²	
Transform	Description	Transform	Description	Transform	Description
ah-md5-hmac	AH with MD5 (HMAC variant) authentication algorithm	esp-3des	ESP with 168-bit Triple DES encryption algorithm	esp-md5-hmac	ESP with MD5 (HMAC variant) authentication algorithm

Table 4-1 Allowed Transform Combinations (continued)

AH Transform ¹		ESP Encryption Transform ¹		ESP Authentication Transform ²	
ah-sha-hmac	AH with SHA (HMAC variant) authentication algorithm	esp-des	ESP with 56-bit DES encryption algorithm	esp-sha-hmac	ESP with SHA (HMAC variant) authentication algorithm
		esp-null	ESP transform without cipher		

1. Pick one transform option.
2. Pick one transform option, but only if you selected **esp-null** or ESP encrypting transform.

Creating Crypto Map Entries

To create crypto map entries that use IKE to establish the security associations, use the following commands, starting in global configuration mode:

	Command	Purpose
Step 1	crypto map <i>map-name seq-num ipsec-isakmp</i>	Creates the crypto map and enters crypto map configuration mode.
Step 2	match address <i>access-list-id</i>	Specifies an extended access list. This access list determines which traffic is protected by IPsec and which is not.
Step 3	set peer { <i>hostname ip-address</i> }	Specifies a remote IPsec peer. This is the peer to which IPsec-protected traffic can be forwarded. Repeat for multiple remote peers.
Step 4	set transform-set <i>transform-set-name1 [transform-set-name2...transform-set-name6]</i>	Specifies which transform sets are allowed for this crypto map entry. Lists multiple transform sets in order of priority (highest priority first).
Step 5	end	Exits crypto map configuration mode.
Step 6	Repeat these steps to create additional crypto map entries as required.	

Verifying the Configuration

Some configuration changes take effect only after subsequent security associations are negotiated. For the new settings to take effect immediately, clear the existing security associations.

To clear (and reinitialize) IPSec security associations, use one of the commands in [Table 4-2](#) in global configuration mode:

Table 4-2 Commands to Clear IPSec Security Associations

Command	Purpose
clear crypto sa or clear crypto sa peer {ip-address peer-name} or clear crypto sa map map-name or clear crypto sa spi destination-address protocol spi	Clear IPSec security associations (SAs). Using the clear crypto sa command without parameters clears out the full SA database, which clears out active security sessions. You may also specify the peer , map , or spi keywords to clear out only a subset of the SA database.

The following steps provide information on verifying your configurations:

Step 1 Enter the **show crypto ipsec transform-set** command to view your transform set configuration:

```
Router# show crypto ipsec transform-set
Transform set combined-des-md5: {esp-des esp-md5-hmac}
  will negotiate = {Tunnel,},
Transform set t1: {esp-des esp-md5-hmac}
  will negotiate = {Tunnel,},
Transform set t100: {ah-sha-hmac}
  will negotiate = {Transport,},
Transform set t2: {ah-sha-hmac}
  will negotiate = {Tunnel,},
  {esp-des}
  will negotiate = {Tunnel,},
```

Step 2 Enter the **show crypto map [interface interface | tag map-name]** command to view your crypto map configuration:

```
Router# show crypto map
Crypto Map: "router-alice" idb: Ethernet0 local address: 172.21.114.123
Crypto Map "router-alice" 10 ipsec-isakmp
  Peer = 172.21.114.67
  Extended IP access list 141
    access-list 141 permit ip
      source: addr = 172.21.114.123/0.0.0.0
      dest:   addr = 172.21.114.67/0.0.0.0
  Current peer: 172.21.114.67
  Security-association lifetime: 4608000 kilobytes/120 seconds
  PFS (Y/N): N
  Transform sets={t1,}
```

Step 3 Enter the **show crypto ipsec sa [map map-name | address | identity | detail | interface]** command to view information about IPSec security associations.

```
Router# show crypto ipsec sa
interface: Ethernet0
  Crypto map tag: router-alice, local addr. 172.21.114.123
  local ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
```

```

remote ident (addr/mask/prot/port): (172.21.114.67/255.255.255.255/0/0)
current_peer: 172.21.114.67
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10
#send errors 10, #recv errors 0
local crypto endpt.: 172.21.114.123, remote crypto endpt.: 172.21.114.67
path mtu 1500, media mtu 1500
current outbound spi: 20890A6F
inbound esp sas:
  spi: 0x257A1039(628756537)
    transform: esp-des esp-md5-hmac,
    in use settings ={Tunnel,}
    slot: 0, conn id: 26, crypto map: router-alice
    sa timing: remaining key lifetime (k/sec): (4607999/90)
    IV size: 8 bytes
    replay detection support: Y
inbound ah sas:
outbound esp sas:
  spi: 0x20890A6F(545852015)
    transform: esp-des esp-md5-hmac,
    in use settings ={Tunnel,}
    slot: 0, conn id: 27, crypto map: router-alice
    sa timing: remaining key lifetime (k/sec): (4607999/90)
    IV size: 8 bytes
    replay detection support: Y
outbound ah sas:
interface: Tunnel0
Crypto map tag: router-alice, local addr. 172.21.114.123
local ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.21.114.67/255.255.255.255/0/0)
current_peer: 172.21.114.67
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10
#send errors 10, #recv errors 0
local crypto endpt.: 172.21.114.123, remote crypto endpt.: 172.21.114.67
path mtu 1500, media mtu 1500
current outbound spi: 20890A6F
inbound esp sas:
  spi: 0x257A1039(628756537)
    transform: esp-des esp-md5-hmac,
    in use settings ={Tunnel,}
    slot: 0, conn id: 26, crypto map: router-alice
    sa timing: remaining key lifetime (k/sec): (4607999/90)
    IV size: 8 bytes
    replay detection support: Y
inbound ah sas:
outbound esp sas:
  spi: 0x20890A6F(545852015)
    OL-5419-01 B0transform: esp-des esp-md5-hmac,
    in use settings ={Tunnel,}
    slot: 0, conn id: 27, crypto map: router-alice
    sa timing: remaining key lifetime (k/sec): (4607999/90)
    IV size: 8 bytes
    replay detection support: Y
outbound ah sas:

```

For a detailed description of the information displayed by the **show** commands, refer to the “[IP Security and Encryption](#)” chapter of the *Security Command Reference* publication. For more information on the VAM, see the *VPN Acceleration Module Installation and Configuration Guide*.

