



IPSec VPN Accounting

The IPSec VPN Accounting feature allows for a session to be accounted for by indicating when the session starts and when it stops.

A VPN session is defined as an Internet Key Exchange (IKE) security association (SA) and the one or more SA pairs that are created by the IKE SA. The session starts when the first IP Security (IPSec) pair is created and stops when all IPSec SAs are deleted.

Session identifying information and session usage information is passed to the Remote Authentication Dial-In User Service (RADIUS) server via standard RADIUS attributes and vendor-specific attributes (VSAs).

Feature Specifications for IPSec VPN Accounting

Feature History

Release	Modification
12.2(15)T	This feature was introduced.

Supported Platforms

Cisco 2610–2613, Cisco 2620–Cisco 2621, Cisco 2650–Cisco 2651, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 3725, Cisco 3745, Cisco 7100, Cisco 7200, Cisco 7400, Ciscoubr7100, Ciscoubr7200.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for IPSec VPN Accounting, page 2](#)
- [Information About IPSec VPN Accounting, page 2](#)
- [How to Configure IPSec VPN Accounting, page 6](#)
- [Configuration Examples for IPSec VPN Accounting, page 12](#)
- [Additional References, page 17](#)

- [Command Reference, page 18](#)
- [Glossary, page 37](#)

Prerequisites for IPSec VPN Accounting

You need to understand how to configure RADIUS and authentication, authorization, and accounting (AAA) accounting. For information about configuring RADIUS and AAA, refer to the following documents:

- [Configuring Basic AAA RADIUS for Dial-In Clients](#)
- [How Does RADIUS Work?](#)
- The chapter “[Configuring RADIUS](#)” in the *Cisco IOS Security Configuration Guide*
- The chapter “[RADIUS Commands](#)” in the *Cisco IOS Security Command Reference*, Release 12.2
- The chapter “[Configuring Accounting](#)” in the *Cisco IOS Security Configuration Guide*, Release 12.2

You also need to know how to configure IPSec accounting. For information about configuring IPSec accounting, refer to the chapter “[Configuring IPSec Network Security](#)” in the *Cisco IOS Security Configuration Guide*, Release 12.2.

Information About IPSec VPN Accounting

To configure IPSec VPN accounting, you must understand the following concepts:

- [RADIUS Accounting, page 2](#)
- [IKE and IPSec Subsystem Interaction, page 4](#)

RADIUS Accounting

For many large networks, it is required that user activity be recorded for auditing purposes. The method that is used most is RADIUS accounting.

RADIUS accounting allows for a session to be accounted for by indicating when the session starts and when it stops. Additionally, session identifying information and session usage information will be passed to the RADIUS server via RADIUS attributes and VSAs.

RADIUS Start Accounting

The RADIUS Start packet contains many attributes that generally identify who is requesting the service and of what the property of that service consists. [Table 1](#) represents the attributes required for the start.

Table 1 *RADIUS Accounting Start Packet Attributes*

RADIUS Attributes Value	Attribute	Description
1	user-name	Username used in extended authentication (XAUTH). The username may be NULL when XAUTH is not used.
4	nas-ip-address	Identifying IP address of the network access server (NAS) that serves the user. It should be unique to the NAS within the scope of the RADIUS server.
5	nas-port	Physical port number of the NAS that serves the user.
8	framed-ip-address	Private address allocated for the IP Security (IPSec) session.
40	acct-status-type	Status type. This attribute indicates whether this accounting request marks the beginning (start), the end (stop), or an update of the session.
41	acct-delay-time	Number of seconds the client has been trying to send a particular record.
44	acct-session-id	Unique accounting identifier that makes it easy to match start and stop records in a log file.
26	vrf-id	String that represents the name of the Virtual Route Forwarder (VRF).
26	isakmp-initiator-ip	Endpoint IP address of the remote Internet Key Exchange (IKE) initiator (V4).
26	isakmp-group-id	Name of the VPN group profile used for accounting.
26	isakmp-phase1-id	Phase 1 identification (ID) used by IKE (for example, domain name [DN], fully qualified domain name [FQDN], IP address) to help identify the session initiator.

RADIUS Stop Accounting

The RADIUS Stop packet contains many attributes that identify the usage of the session. Table 2 represents the additional attributes required for the RADIUS stop packet. It is possible that only the stop packet will be sent without the start if configured to do so. If only the stop packet is sent, this allows an easy way to reduce the number of records going to the AAA server.

Table 2 *RADIUS Accounting Stop Packet Attributes*

RADIUS Attributes Value	Attribute	Description
42	acct-input-octets	Number of octets that have been received from the Unity client over the course of the service that is being provided.
43	acct-output-octets	Number of octets that have been sent to the Unity client in the course of delivering this service.

Table 2 RADIUS Accounting Stop Packet Attributes (continued)

RADIUS Attributes Value	Attribute	Description
46	acct-session-time	Length of time (in seconds) that the Unity client has received service.
47	acct-input-packets	Quantity of packets that have been received from the Unity client in the course of delivering this service.
48	acct-output-packets	Quantity of packets that have been sent to the Unity client in the course of delivering this service.
49	acct-terminate-cause	For future use.
52	acct-input-gigawords	How many times the Acct-Input-Octets counter has wrapped around the 2^{32} (2 to the 32nd power) over the course of this service.
52	acct-output-gigawords	How many times the Acct-Input-Octets counter has wrapped around the 2^{32} (2 to the 32nd power) over the course of this service.

RADIUS Update Accounting

RADIUS accounting updates are supported. Packet and octet counts are shown in the updates. To learn more about AAA, refer to the following documents:

- [Configuring Basic AAA RADIUS for Dial-In Clients](#)
- The chapter “RADIUS Commands” in the *Cisco IOS Security Command Reference*, Release 12.2 T
- [How to Assign Privilege Levels with TACACS+ and RADIUS](#)
- Other AAA documentation at the [Cisco.com](#) website

IKE and IPSec Subsystem Interaction

Accounting Start

If IPSec accounting is configured, after IKE phases are complete, an accounting start record is generated for the session. New accounting records are not generated during a rekeying.

The following is an account start record that was generated on a router and that is to be sent to the AAA server that is defined:

```
*Aug 23 04:06:20.131: RADIUS(00000002): sending
*Aug 23 04:06:20.131: RADIUS(00000002): Send Accounting-Request to 10.1.1.4:1646 id 4, len 220
*Aug 23 04:06:20.131: RADIUS: authenticator 38 F5 EB 46 4D BE 4A 6F - 45 EB EF 7D B7 19 FB 3F
*Aug 23 04:06:20.135: RADIUS: Acct-Session-Id [44] 10 "00000001"
*Aug 23 04:06:20.135: RADIUS: Vendor, Cisco [26] 31
*Aug 23 04:06:20.135: RADIUS: Cisco AVpair [1] 25 "isakmp-group-id=cclient"
*Aug 23 04:06:20.135: RADIUS: Framed-IP-Address [8] 6 10.13.13.1
*Aug 23 04:06:20.135: RADIUS: Vendor, Cisco [26] 20
*Aug 23 04:06:20.135: RADIUS: Cisco AVpair [1] 14 "vrf-id=cisco"
*Aug 23 04:06:20.135: RADIUS: Vendor, Cisco [26] 35
```

```

*Aug 23 04:06:20.135: RADIUS: Cisco AVpair [1] 29 "isakmp-initator-ip=11.1.2.2"
*Aug 23 04:06:20.135: RADIUS: Vendor, Cisco [26] 36
*Aug 23 04:06:20.135: RADIUS: Cisco AVpair [1] 30 "connect-progress=No
Progress"
*Aug 23 04:06:20.135: RADIUS: User-Name [1] 13 "joe@cclient"
*Aug 23 04:06:20.135: RADIUS: Acct-Status-Type [40] 6 Start [1]
*Aug 23 04:06:20.135: RADIUS: Vendor, Cisco [26] 25
*Aug 23 04:06:20.135: RADIUS: cisco-nas-port [2] 19 "FastEthernet0/0.1"
*Aug 23 04:06:20.135: RADIUS: NAS-Port [5] 6 0
*Aug 23 04:06:20.135: RADIUS: NAS-IP-Address [4] 6 10.1.1.147
*Aug 23 04:06:20.135: RADIUS: Acct-Delay-Time [41] 6 0
*Aug 23 04:06:20.139: RADIUS: Received from id 21645/4 10.1.1.4:1646, Accounting-response,
len 20
*Aug 23 04:06:20.139: RADIUS: authenticator B7 E3 D0 F5 61 9A 89 D8 - 99 A6 8A 8A 98 79
9D 5D

```

Accounting Stop

An accounting stop packet is generated when there are no more flows (IPSec SA pairs) with the remote peer.

The accounting stop records contain the following information:

- Packets out
- Packets in
- Octets out
- Gigawords in
- Gigawords out

Below is an account start record that was generated on a router. The account start record is to be sent to the AAA server that is defined.

```

*Aug 23 04:20:16.519: RADIUS(00000003): Using existing nas_port 0
*Aug 23 04:20:16.519: RADIUS(00000003): Config NAS IP: 100.1.1.147
*Aug 23 04:20:16.519: RADIUS(00000003): sending
*Aug 23 04:20:16.519: RADIUS(00000003): Send Accounting-Request to 100.1.1.4:1646 id 19,
len 238
*Aug 23 04:20:16.519: RADIUS: authenticator 82 65 5B 42 F0 3F 17 C3 - 23 F3 4C 35 A2 8A
3E E6
*Aug 23 04:20:16.519: RADIUS: Acct-Session-Id [44] 10 "00000002"
*Aug 23 04:20:16.519: RADIUS: Vendor, Cisco [26] 20
*Aug 23 04:20:16.519: RADIUS: Cisco AVpair [1] 14 "vrf-id=cisco"
*Aug 23 04:20:16.519: RADIUS: Vendor, Cisco [26] 35
*Aug 23 04:20:16.519: RADIUS: Cisco AVpair [1] 29 "isakmp-initator-ip=11.1.1.2"
*Aug 23 04:20:16.519: RADIUS: Vendor, Cisco [26] 36
*Aug 23 04:20:16.519: RADIUS: Cisco AVpair [1] 30 "connect-progress=No
Progress"
*Aug 23 04:20:16.519: RADIUS: Acct-Session-Time [46] 6 709
*Aug 23 04:20:16.519: RADIUS: Acct-Input-Octets [42] 6 152608
*Aug 23 04:20:16.519: RADIUS: Acct-Output-Octets [43] 6 152608
*Aug 23 04:20:16.519: RADIUS: Acct-Input-Packets [47] 6 1004
*Aug 23 04:20:16.519: RADIUS: Acct-Output-Packets [48] 6 1004
*Apr 23 04:20:16.519: RADIUS: Acct-Input-Giga-Word[52] 6 0
*Apr 23 04:20:16.519: RADIUS: Acct-Output-Giga-Wor[53] 6 0
*Aug 23 04:20:16.519: RADIUS: Acct-Terminate-Cause[49] 6 none [0]
*Aug 23 04:20:16.519: RADIUS: Vendor, Cisco [26] 32
*Aug 23 04:20:16.519: RADIUS: Cisco AVpair [1] 26 "disc-cause-ext=No Reason"
*Aug 23 04:20:16.519: RADIUS: Acct-Status-Type [40] 6 Stop [2]
*Aug 23 04:20:16.519: RADIUS: Vendor, Cisco [26] 25
*Aug 23 04:20:16.519: RADIUS: cisco-nas-port [2] 19 "FastEthernet0/0.1"

```

```
*Aug 23 04:20:16.519: RADIUS: NAS-Port [5] 6 0
*Aug 23 04:20:16.519: RADIUS: NAS-IP-Address [4] 6 100.1.1.147
*Aug 23 04:20:16.519: RADIUS: Acct-Delay-Time [41] 6 0
*Aug 23 04:20:16.523: RADIUS: Received from id 21645/19 100.1.1.4:1646,
Accounting-response, len 20
*Aug 23 04:20:16.523: RADIUS: authenticator F1 CA C1 28 CE A0 26 C9 - 3E 22 C9 DA EA B8
22 A0
```

Accounting Updates

If accounting updates are enabled, accounting updates are sent while a session is “up.” The update interval is configurable. To enable the accounting updates, use the **aaa accounting update** command.

The following is an accounting update record that is being sent from the router:

```
Router#
*Aug 23 21:46:05.263: RADIUS(00000004): Using existing nas_port 0
*Aug 23 21:46:05.263: RADIUS(00000004): Config NAS IP: 100.1.1.147
*Aug 23 21:46:05.263: RADIUS(00000004): sending
*Aug 23 21:46:05.263: RADIUS(00000004): Send Accounting-Request to 100.1.1.4:1646 id 22,
len 200
*Aug 23 21:46:05.263: RADIUS: authenticator 30 FA 48 86 8E 43 8E 4B - F9 09 71 04 4A F1
52 25
*Aug 23 21:46:05.263: RADIUS: Acct-Session-Id [44] 10 "00000003"
*Aug 23 21:46:05.263: RADIUS: Vendor, Cisco [26] 20
*Aug 23 21:46:05.263: RADIUS: Cisco AVpair [1] 14 "vrf-id=cisco"
*Aug 23 21:46:05.263: RADIUS: Vendor, Cisco [26] 35
*Aug 23 21:46:05.263: RADIUS: Cisco AVpair [1] 29 "isakmp-initiator-ip=11.1.1.2"
*Aug 23 21:46:05.263: RADIUS: Vendor, Cisco [26] 36
*Aug 23 21:46:05.263: RADIUS: Cisco AVpair [1] 30 "connect-progress=No
Progress"
*Aug 23 21:46:05.263: RADIUS: Acct-Session-Time [46] 6 109
*Aug 23 21:46:05.263: RADIUS: Acct-Input-Octets [42] 6 608
*Aug 23 21:46:05.263: RADIUS: Acct-Output-Octets [43] 6 608
*Aug 23 21:46:05.263: RADIUS: Acct-Input-Packets [47] 6 4
*Aug 23 21:46:05.263: RADIUS: Acct-Output-Packets [48] 6 4
*Aug 23 21:46:05.263: RADIUS: Acct-Status-Type [40] 6 Watchdog [3]
*Aug 23 21:46:05.263: RADIUS: Vendor, Cisco [26] 25
*Aug 23 21:46:05.263: RADIUS: cisco-nas-port [2] 19 "FastEthernet0/0.1"
*Aug 23 21:46:05.263: RADIUS: NAS-Port [5] 6 0
*Aug 23 21:46:05.263: RADIUS: NAS-IP-Address [4] 6 100.1.1.147
*Aug 23 21:46:05.263: RADIUS: Acct-Delay-Time [41] 6 0
*Aug 23 21:46:05.267: RADIUS: Received from id 21645/22 100.1.1.4:1646,
Accounting-response, len 20
*Aug 23 21:46:05.267: RADIUS: authenticator 51 6B BB 27 A4 F5 D7 61 - A7 03 73 D3 0A AC
1C
```

How to Configure IPSec VPN Accounting

This section contains the following procedures:

- [Configuring IPSec VPN Accounting, page 7](#)
- [Configuring Accounting Updates, page 10](#)
- [Troubleshooting for IPSec VPN Accounting, page 11](#)

Configuring IPSec VPN Accounting

To enable IPSec VPN Accounting, you need to perform the following required task:

Prerequisites

Before configuring IPSec VPN accounting, you must first configure IPSec. To learn about configuring IPSec, refer to the following documents:

- The chapter “[Configuring IPSec Network Security](#)” in the *Cisco IOS Security Configuration Guide*, Release 12.2
- Other IPSec documentation at the [Cisco.com](#) website

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** *list-name method*
5. **aaa authorization network** *list-name method*
6. **aaa accounting network** *list-name start-stop [broadcast] group group-name*
7. **aaa session-id common**
8. **crypto isakmp profile** *profile-name*
9. **vrf** *ivrif*
10. **match identity group** *group-name*
11. **client authentication list** *list-name*
12. **isakmp authorization list** *list-name*
13. **client configuration address** [**initiate** | **respond**]
14. **accounting** *list-name*
15. **exit**
16. **crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
17. **set transform-set** *transform-set-name*
18. **set isakmp-profile** *profile-name*
19. **reverse-route** [**remote-peer**]
20. **exit**
21. **crypto map** *map-name ipsec-isakmp dynamic dynamic-template-name*
22. **radius-server host** *ip-address [auth-port port-number] [acct-port port-number]*
23. **radius-server key** *string*
24. **radius-server vsa send accounting**
25. **interface** *interface-id*
26. **crypto map** *map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Router (config)# aaa new-model	Enables periodic interim accounting records to be sent to the accounting server.
Step 4	aaa authentication login list-name method Example: Router (config)# aaa authentication login cisco-client group radius	Enforces authentication, authorization, and accounting (AAA) authentication for extended authorization (XAUTH) via RADIUS or local.
Step 5	aaa authorization network list-name method Example: Router (config)# aaa authorization network cisco-client group radius	Sets AAA authorization parameters on the remote client from RADIUS or local.
Step 6	aaa accounting network list-name start-stop [broadcast] group group-name Example: Router (config)# aaa accounting network acc start-stop broadcast group radius	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
Step 7	aaa session-id common Example: Router (config)# aaa session-id common	Specifies whether the same session ID will be used for each AAA accounting service type within a call or whether a different session ID will be assigned to each accounting service type.
Step 8	crypto isakmp profile profile-name Example: Route (config)# crypto isakmp profile cisco	Audits IP security (IPSec) user sessions and enters isakmp-profile submode.
Step 9	vrf ivrf Example: Router (conf-isa-prof)# vrf cisco	Associates the on-demand address pool with a Virtual Private Network (VPN) routing and forwarding (VRF) instance name.

	Command or Action	Purpose
Step 10	match identity group <i>group-name</i> Example: Router(conf-isa-prof)# match identity group cisco	Matches an identity from a peer in an ISAKMP profile.
Step 11	client authentication list <i>list-name</i> Example: Router(conf-isa-prof)# client authentication list cisco	Configures Internet Key Exchange (IKE) extended authentication (XAUTH) in an Internet Security Association and Key Management Protocol (ISAKMP) profile.
Step 12	isakmp authorization list <i>list-name</i> Example: Router(conf-isa-prof)# isakmp authorization list cisco-client	Configures an IKE shared secret and other parameters using the AAA server in an ISAKMP profile. The shared secret and other parameters are generally pushed to the remote peer via mode configuration (MODECFG).
Step 13	client configuration address [initiate respond] Example: Router(conf-isa-prof)# client configuration address respond	Configures IKE mode configuration (MODECFG) in the ISAKMP profile.
Step 14	accounting <i>list-name</i> Example: Router(conf-isa-prof)# accounting acc	Enables AAA accounting services for all peers that connect via this ISAKMP profile.
Step 15	exit Example: Router(conf-isa-prof)# exit	Exits isakmp-profile submode.
Step 16	crypto dynamic-map <i>dynamic-map-name</i> <i>dynamic-seq-num</i> Example: Router(config)# crypto dynamic-map mymap 10 ipsec-isakmp	Creates a dynamic crypto map template and enters the crypto map configuration command mode.
Step 17	set transform-set <i>transform-set-name</i> Example: Router(config-crypto-map)# set transform-set aswan	Specifies which transform sets can be used with the crypto map template.
Step 18	set isakmp-profile <i>profile-name</i> Example: Router(config-crypto-map)# set isakmp-profile cisco	Sets the ISAKMP profile name.

	Command or Action	Purpose
Step 19	reverse-route [remote-peer] Example: Router(config-crypto-map)# reverse-route	Allows routes (ip addresses) to be injected for destinations behind the VPN remote tunnel endpoint and may include a route to the tunnel endpoint itself (using the remote-peer keyword for the crypto map.
Step 20	exit Example: Router(config-crypto-map)# exit	Exits dynamic crypto map configuration mode.
Step 21	crypto map <i>map-name</i> ipsec-isakmp dynamic <i>dynamic-template-name</i> Example: Router(config)# crypto map mymap ipsec-isakmp dynamic dmap	Enters crypto map configuration mode
Step 22	radius-server host <i>ip-address</i> [auth-port <i>port-number</i>] [acct-port <i>port-number</i>] Example: Router(config)# radius-server host 172.16.1.4	Specifies a RADIUS server host.
Step 23	radius-server key <i>string</i> Example: Router(config)# radius-server key nsite	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
Step 24	radius-server vsa send accounting Example: Router(config)# radius-server vsa send accounting	Configures the network access server to recognize and use vendor-specific attributes.
Step 25	interface <i>type slot/port</i> Example: Router(config)# interface FastEthernet 1/0	Configures an interface type and enters interface configuration mode.
Step 26	crypto map <i>map-name</i> Example: Router(config-if)# crypto map mymap	Applies a previously defined crypto map set to an interface.

Configuring Accounting Updates

To send accounting updates while a session is “up,” perform the following optional task:

Prerequisites

Before you configure accounting updates, you must first configure IPSec VPN accounting. See the section “[Configuring IPSec VPN Accounting](#).”

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa accounting update periodic *number***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa accounting update periodic <i>number</i> Example: Router (config)# aaa accounting update periodic 1-2147483647	(Optional) Enables periodic interim accounting records to be sent to the accounting server.

Troubleshooting for IPSec VPN Accounting

To display messages about IPSec accounting events, perform the following optional task:

SUMMARY STEPS

1. **enable**
2. **debug crypto isakmp aaa**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug crypto isakmp aaa Example: Router# debug crypto isakmp aaa	Displays messages about Internet Key Exchange (IKE) events. <ul style="list-style-type: none"> • The aaa keyword specifies accounting events.

Configuration Examples for IPSec VPN Accounting

- [Accounting and ISAKMP-Profile Example, page 12](#)
- [Accounting Without ISAKMP Profiles Example, page 14](#)

Accounting and ISAKMP-Profile Example

The following example shows a configuration for supporting remote access clients with accounting and ISAKMP profiles:

```

version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sheep
!
aaa new-model
!
!
aaa accounting network ipsecaaa start-stop group radius
aaa accounting update periodic 1
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
ip name-server 172.29.2.133
ip name-server 172.29.11.48
!
!
crypto isakmp policy 1
authentication pre-share
group 2
!
crypto isakmp policy 10
hash md5
authentication pre-share
lifetime 200
crypto isakmp key cisco address 172.31.100.2

crypto iakmp client configuration group cclient
key jegjegjhrj
pool addressA

crypto-isakmp profile groupA
vrf cisco
match identity group cclient
client authentication list cisco-client
isakmp authorization list cisco-client
client configuration address respond
accounting acc
!
!
crypto ipsec transform-set esp-des-md5 esp-des esp-md5-hmac
!
crypto dynamic-map remotes 1
set peer 172.31.100.2

```

```
set security-association lifetime seconds 120
set transform-set esp-des-md5
reverse-route

!
crypto map test 10 ipsec-isakmp dynamic remotes
!
voice call carrier capacity active
!
interface Loopback0
ip address 10.20.20.20 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface FastEthernet0/0
ip address 10.2.80.203 255.255.255.0
no ip mroute-cache
load-interval 30
duplex full
!
interface FastEthernet1/0
ip address 192.168.219.2 255.255.255.0
no ip mroute-cache
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 172.28.100.1 255.255.255.0
no ip mroute-cache
duplex auto
speed auto
crypto map test
!
no fair-queue
ip default-gateway 10.2.80.1
ip classless
ip route 10.0.0.0 0.0.0.0 10.2.80.1
ip route 10.20.0.0 255.0.0.0 10.2.80.56
ip route 10.10.10.0 255.255.255.0 172.31.100.2
ip route 10.0.0.2 255.255.255.255 10.2.80.73

ip local pool addressA 192.168.1.1 192.168.1.253
no ip http server
ip pim bidir-enable
!
!
ip access-list extended encrypt
permit ip host 10.0.0.1 host 10.5.0.1
!
access-list 101 permit ip host 10.20.20.20 host 10.10.10.10
!
!
radius-server host 172.27.162.206 auth-port 1645 acct-port 1646 key cisco123
radius-server retransmit 3
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
```

```

gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
exec prompt timestamp
line aux 0
line vty 5 15
  ntp server 172.31.150.52
end

```

Accounting Without ISAKMP Profiles Example

The following example shows a full Cisco IOS configuration that supports accounting remote access peers when ISAKMP profiles are not used:

```

version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sheep
!
aaa new-model
!
!
aaa accounting network ipsecaaa start-stop group radius
aaa accounting update periodic 1
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
ip name-server 172.29.2.133
ip name-server 172.29.11.48
!
!
crypto isakmp policy 1
  authentication pre-share
  group 2
!
crypto isakmp policy 10
  hash md5
  authentication pre-share
  lifetime 200
crypto isakmp key cisco address 172.31.100.2
!
!
crypto ipsec transform-set esp-des-md5 esp-des esp-md5-hmac
!
crypto map test client accounting list ipsecaaa
crypto map test 10 ipsec-isakmp
  set peer 172.31.100.2
  set security-association lifetime seconds 120
  set transform-set esp-des-md5
  match address 101
!
voice call carrier capacity active
!

```

```
interface Loopback0
 ip address 10.20.20.20 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 !
interface FastEthernet0/0
 ip address 10.2.80.203 255.255.255.0
 no ip mroute-cache
 load-interval 30
 duplex full
 !
interface FastEthernet1/0
 ip address 192.168.219.2 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
 !
interface FastEthernet1/1
 ip address 172.28.100.1 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
 crypto map test
 !
no fair-queue
 ip default-gateway 10.2.80.1
 ip classless
 ip route 10.0.0.0 0.0.0.0 10.2.80.1
 ip route 10.30.0.0 255.0.0.0 10.2.80.56
 ip route 10.10.10.0 255.255.255.0 172.31.100.2
 ip route 10.0.0.2 255.255.255.255 10.2.80.73
 no ip http server
 ip pim bidir-enable
 !
 !
 ip access-list extended encrypt
 permit ip host 10.0.0.1 host 10.5.0.1
 !
 access-list 101 permit ip host 10.20.20.20 host 10.10.10.10
 !
 !
 radius-server host 172.27.162.206 auth-port 1645 acct-port 1646 key cisco123
 radius-server retransmit 3
 radius-server authorization permit missing Service-Type
 radius-server vsa send accounting
 call rsvp-sync
 !
 !
 mgcp profile default
 !
 dial-peer cor custom
 !
 !
 gatekeeper
 shutdown
 !
 !
 line con 0
 exec-timeout 0 0
 exec prompt timestamp
 line aux 0
 line vty 5 15
 !
 exception core-file ioscrypto/core/sheep-core
```

```
exception dump 172.25.1.129
ntp clock-period 17208229
ntp server 172.71.150.52
!
end
```

Additional References

For additional information related to IPSec VPN accounting, refer to the following references:

Related Documents

Related Topic	Document Title
Configuring AAA accounting	<ul style="list-style-type: none"> The chapter “Configuring Accounting” in the <i>Cisco IOS Security Configuration Guide</i>, Release 12.2
Configuring IPSec VPN accounting	<ul style="list-style-type: none"> The chapter “Configuring IPSec Network Security” in the <i>Cisco IOS Security Configuration Guide</i>, Release 12.2
Configuring basic AAA RADIUS	<ul style="list-style-type: none"> Configuring Basic AAA RADIUS for Dial-In Clients How Does RADIUS Work? The chapter “Configuring RADIUS” in the <i>Cisco IOS Security Configuration Guide</i>, Release 12.2 The chapter “RADIUS Commands” in the <i>Security Command Reference</i>, Release 12.2 T
Configuring ISAKMP profiles	<i>VRF-Aware IPSec</i> , Cisco IOS Release 12.2(15)T feature module
Privilege levels with TACACS+ and RADIUS	How to Assign Privilege Levels with TACACS+ and RADIUS
IP security, RADIUS, and AAA commands	<i>Cisco IOS Security Command Reference</i> , Release 12.2 T

Standards

Standards	Title
None	

MIBs

MIBs	MIBs Link
None	<p>To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

RFCs	Title
None	

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 T command reference publications.

New Commands

- **client authentication list**
- **client configuration address**
- **crypto isakmp profile**
- **isakmp authorization list**
- **match identity**
- **set isakmp-profile**
- **vrf**

Modified Commands

- **crypto map (global IPSec)**
- **debug crypto isakmp**

client authentication list

To configure Internet Key Exchange (IKE) extended authentication (XAUTH) in an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **client authentication list** command in isakmp profile configuration mode. To restore the default behavior, which is that XAUTH is not enabled, use the **no** form of this command.

client authentication list *list-name*

no client authentication list *list-name*

Syntax Description

<i>list-name</i>	Character string used to name the list of authentication methods activated when a user logs in. The list name must match the list name that was defined during the authentication, authorization, and accounting (AAA) configuration.
------------------	---

Defaults

No default behaviors or values

Command Modes

Isakmp profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Before configuring XAUTH, you must set up an authentication list using AAA commands.

Examples

The following example shows that user authentication is configured. User authentication is a list of authentication methods called “xauthlist” in an ISAKMP profile called “vpnprofile.”

```
crypto isakmp profile vpnprofile
  client authentication list xauthlist
```

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.

client configuration address

To configure Internet Key Exchange (IKE) configuration mode in the Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **client configuration address** command in isakmp profile configuration mode. To disable IKE configuraton mode, use the **no** form of this command.

client configuration address {initiate | respond}

no client configuration address {initiate | respond}

Syntax Description

initiate	Router will attempt to set IP addresses for each peer.
respond	Router will accept requests for IP addresses from any requesting peer.

Defaults

IKE configuration is not enabled.

Command Modes

Isakmp profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Before you can use this command, you must enter the **crypto isakmp profile** command.

Examples

The following example shows that IKE mode is configured to either initiate or respond in an ISAKMP profile called “vpnprofile”:

```
crypto isakmp profile vpnprofile
client configuration address initiate
client configuration address respond
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile.

crypto isakmp profile

To define an Internet Security Association and Key Management Protocol (ISAKMP) profile and to audit IP Security (IPSec) user sessions, use the **crypto isakmp profile** command in global configuration mode. To delete a crypto ISAKMP profile, use the **no** form of this command.

```
crypto isakmp profile profile-name [accounting aaalist]
```

```
no crypto isakmp profile profile-name [accounting aaalist]
```

Syntax Description	
<i>profile-name</i>	Name of the user profile. To associate a user profile with the RADIUS server, the user profile name must be identified.
accounting <i>aaalist</i>	(Optional) Name of a client accounting list.

Defaults No default behaviors or values

Command Modes Global configuration

Command History	Release	Modification
	12.2(15)T	This command was introduced.

Usage Guidelines

Defining an ISAKMP Profile

An ISAKMP profile can be viewed as a repository of Phase 1 and Phase 1.5 commands for a set of peers. The Phase 1 configuration includes commands to configure such things as keepalive, identity matching, and the authorization list. The Phase 1.5 configuration includes commands to configure such things as extended authentication (XAUTH) and mode configuration.

The peers are mapped to an ISAKMP profile when their identities are matched (as given in the identification [ID] payload of the Internet Key Exchange [IKE]) against the identities defined in the ISAKMP profile. To uniquely map to an ISAKMP profile, no two ISAKMP profiles should match the same identity. If the peer identity is matched in two ISAKMP profiles, the configuration is invalid. Also, there must be at least one **match identity** command defined in the ISAKMP profile for it to be complete.

Auditing IPSec User Sessions

Use this command to audit multiple user sessions that are terminating on the IPSec gateway.



Note

The **crypto isakmp profile** command and the **crypto map** (global IPSec) command are mutually exclusive. If a profile is present (the **crypto isakmp profile** command has been used), with no accounting configured but with the global command present (the **crypto isakmp profile** command without the **accounting** keyword), accounting will occur using the attributes in the global command.

Examples

The following example shows how to define an ISAKMP profile and match the peer identities:

```
crypto isakmp profile vpnprofile
 match identity address 10.76.11.53
```

The following accounting example shows that an ISAKMP profile is configured:

```
aaa new-model
!
!
aaa authentication login cisco-client group radius
aaa authorization network cisco-client group radius
aaa accounting network acc start-stop broadcast group radius
aaa session-id common
!
crypto isakmp profile cisco
vrf cisco
match identity group cclient
  client authentication list cisco-client
  isakmp authorization list cisco-client
  client configuration address respond
  accounting acc
!
crypto dynamic-map dynamic 1
  set transform-set aswan
  set isakmp-profile cisco
  reverse-route
!
!
radius-server host 172.1.1.4 auth-port 1645 acct-port 1646
radius-server key nsite
```

Related Commands

Command	Description
crypto map (global IPsec)	Enters crypto map configuration mode and creates or modifies a crypto map entry, creates a crypto profile that provides a template for configuration of dynamically created crypto maps, or configures a client accounting list.
debug crypto isakmp	Displays messages about IKE events.
match identity	Matches an identity from a peer in an ISAKMP profile.

crypto map (global IPSec)

To enter crypto map configuration mode and create or modify a crypto map entry, to create a crypto profile that provides a template for configuration of dynamically created crypto maps, or to configure a client accounting list, use the **crypto map** command in global configuration mode. To delete a crypto map entry, profile, or set, use the **no** form of this command.

crypto map *map-name seq-num [ipsec-manual]*

crypto map *map-name seq-num [ipsec-isakmp] [dynamic dynamic-map-name] [discover] [profile profile-name]*

crypto map *map-name [client-accounting-list aaalist]*

no crypto map *map-name seq-num*



Note

Issue the **crypto map** *map-name seq-num* command without a keyword to modify an existing crypto map entry.

Syntax Description

<i>map-name</i>	Name that identifies the crypto map set. This is the name assigned when the crypto map was created.
<i>seq-num</i>	Sequence number you assign to the crypto map entry. See additional explanation for using this argument in the “Usage Guidelines” section.
ipsec-manual	(Optional) Indicates that Internet Key Exchange (IKE) will not be used to establish the IP Security (IPSec) security associations (SAs) for protecting the traffic specified by this crypto map entry.
ipsec-isakmp	(Optional) Indicates that IKE will be used to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.
dynamic	(Optional) Specifies that this crypto map entry is to reference a preexisting dynamic crypto map. Dynamic crypto maps are policy templates used in processing negotiation requests from a peer IPSec device. If you use this keyword, none of the crypto map configuration commands will be available.
<i>dynamic-map-name</i>	(Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template.
discover	(Optional) Enables peer discovery. By default, peer discovery is not enabled.
profile	(Optional) Designates a crypto map as a configuration template. The security configurations of this crypto map will be cloned as new crypto maps are created dynamically on demand.
<i>profile-name</i>	(Optional) Name of the crypto profile being created.
client-accounting-list	(Optional) Designates a client accounting list.
<i>aaalist</i>	(Optional) List name.

Defaults

No crypto maps exist.

Peer discovery is not enabled.

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.
	11.3 T	The following keywords and arguments were added: <ul style="list-style-type: none"> • ipsec-manual • ipsec-isakmp • dynamic • <i>dynamic-map-name</i>
	12.0(5)T	The discover keyword was added to support Tunnel Endpoint Discovery (TED).
	12.2(4)T	The profile <i>profile-name</i> keyword and argument combination was introduced to allow the generation of a crypto map profile that is cloned to create dynamically created crypto maps on demand.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
	12.2(15)T	The client-accounting-list keyword and <i>aaalist</i> argument were added.

Usage Guidelines

Use this command to create a new crypto map entry, to create a crypto map profile, or to modify an existing crypto map entry or profile.

After a crypto map entry has been created, you cannot change the parameters specified at the global configuration level because these parameters determine which of the configuration commands are valid at the crypto map level. For example, after a map entry has been created using the **ipsec-isakmp** keyword, you cannot change it to the option specified by the **ipsec-manual** keyword; you must delete and reenter the map entry.

After you define crypto map entries, you can assign the crypto map set to interfaces using the **crypto map** (interface IPSec) command.

Crypto Map Functions

Crypto maps provide two functions: filtering and classifying traffic to be protected and defining the policy to be applied to that traffic. The first use affects the flow of traffic on an interface; the second affects the negotiation performed (via IKE) on behalf of that traffic.

IPSec crypto maps define the following:

- What traffic should be protected
- To which IPSec peers the protected traffic can be forwarded—these are the peers with which an SA can be established
- Which transform sets are acceptable for use with the protected traffic
- How keys and security associations should be used or managed (or what the keys are, if IKE is not used)

Multiple Crypto Map Entries with the Same Map Name Form a Crypto Map Set

A crypto map set is a collection of crypto map entries, each with a different *seq-num* argument but the same *map-name* argument. Therefore, for a given interface, you could have certain traffic forwarded to one IPSec peer with specified security applied to that traffic and other traffic forwarded to the same or a different IPSec peer with different IPSec security applied. To accomplish differential forwarding you would create two crypto maps, each with the same *map-name* argument, but each with a different *seq-num* argument. Crypto profiles must have unique names within a crypto map set.

Sequence Numbers

The number you assign to the *seq-num* argument should not be arbitrary. This number is used to rank multiple crypto map entries within a crypto map set. Within a crypto map set, a crypto map entry with a lower *seq-num* is evaluated before a map entry with a higher *seq-num*; that is, the map entry with the lower number has a higher priority.

For example, consider a crypto map set that contains three crypto map entries: mymap 10, mymap 20, and mymap 30. The crypto map set named “mymap” is applied to serial interface 0. When traffic passes through serial interface 0, the traffic is evaluated first for mymap 10. If the traffic matches any access list permit statement entry in the extended access list in mymap 10, the traffic will be processed according to the information defined in mymap 10 (including establishing IPSec SAs when necessary). If the traffic does not match the mymap 10 access list, the traffic will be evaluated for mymap 20, and then mymap 30, until the traffic matches a permit entry in a map entry. (If the traffic does not match a permit entry in any crypto map entry, it will be forwarded without any IPSec security.)

Dynamic Crypto Maps

Refer to the “Usage Guidelines” section of the **crypto dynamic-map** command for a discussion on dynamic crypto maps.

Crypto map entries that reference dynamic map sets should be the lowest priority map entries, allowing inbound SA negotiation requests to try to match the static maps first. Only after the request does not match any of the static maps, do you want it to be evaluated against the dynamic map set.

To make a crypto map entry referencing a dynamic crypto map set the lowest priority map entry, give the map entry the highest *seq-num* of all the map entries in a crypto map set.

Create dynamic crypto map entries using the **crypto dynamic-map** command. After you create a dynamic crypto map set, add the dynamic crypto map set to a static crypto map set with the **crypto map** (global IPSec) command using the **dynamic** keyword.

TED

TED is an enhancement to the IPSec feature. Defining a dynamic crypto map allows you to dynamically determine an IPSec peer; however, only the receiving router has this ability. With TED, the initiating router can dynamically determine an IPSec peer for secure IPSec communications.

Dynamic TED helps to simplify IPSec configuration on the individual routers within a large network. Each node has a simple configuration that defines the local network that the router is protecting and the IPSec transforms that are required.



Note

TED helps only in discovering peers; otherwise, TED does not function any differently from normal IPSec. Thus, TED does not improve the scalability of IPSec (in terms of performance or the number of peers or tunnels).

Crypto Map Profiles

Crypto map profiles are created using the **profile** *profile-name* keyword and argument combination. Crypto map profiles are used as configuration templates for dynamically creating crypto maps on demand for use with the Layer 2 Transport Protocol (L2TP) Security feature. The relevant SAs the crypto map profile will be cloned and used to protect IP traffic on the L2TP tunnel.



Note

The **set peer** and **match address** commands are ignored by crypto profiles and should not be configured in the crypto map definition.

Examples

The following example shows the minimum required crypto map configuration when IKE will be used to establish the SAs:

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
```

The following example shows the minimum required crypto map configuration when the SAs are manually established:

```
crypto transform-set someset ah-md5-hmac esp-des
crypto map mymap 10 ipsec-manual
 match address 102
 set transform-set someset
 set peer 10.0.0.5
 set session-key inbound ah 256 98765432109876549876543210987654
 set session-key outbound ah 256 fedcbafedcbafedcfedcbafedcbafedc
 set session-key inbound esp 256 cipher 0123456789012345
 set session-key outbound esp 256 cipher abcdefabcdefabcd
```

The following example configures an IPSec crypto map set that includes a reference to a dynamic crypto map set.

Crypto map “mymap 10” allows SAs to be established between the router and either (or both) of two remote IPSec peers for traffic matching access list 101. Crypto map “mymap 20” allows either of two transform sets to be negotiated with the remote peer for traffic matching access list 102.

Crypto map entry “mymap 30” references the dynamic crypto map set “mydynamicmap,” which can be used to process inbound SA negotiation requests that do not match “mymap” entries 10 or 20. In this case, if the peer specifies a transform set that matches one of the transform sets specified in “mydynamicmap,” for a flow permitted by the access list 103, IPSec will accept the request and set up SAs with the remote peer without previously knowing about the remote peer. If the request is accepted, the resulting SAs (and temporary crypto map entry) are established according to the settings specified by the remote peer.

The access list associated with “mydynamicmap 10” is also used as a filter. Inbound packets that match any access list permit statement in this list are dropped for not being IPSec protected. (The same is true for access lists associated with static crypto maps entries.) Outbound packets that match a permit statement without an existing corresponding IPSec SA are also dropped.

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
 set peer 10.0.0.2
crypto map mymap 20 ipsec-isakmp
 match address 102
 set transform-set my_t_set1 my_t_set2
 set peer 10.0.0.3
crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
!
crypto dynamic-map mydynamicmap 10
 match address 103
 set transform-set my_t_set1 my_t_set2 my_t_set3
```

The following example configures TED on a Cisco router:

```
crypto map testtag 10 ipsec-isakmp dynamic dmap discover
```

The following example configures a crypto profile to be used as a template for dynamically created crypto maps when IPSec is used to protect an L2TP tunnel:

```
crypto map l2tpsec 10 ipsec-isakmp profile l2tp
```

Related Commands*

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto isakmp profile	Audits IPSec user sessions.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
debug crypto isakmp	Applies a previously defined crypto map set to an interface.
match address (IPSec)	Specifies an extended access list for a crypto map entry.
set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.
set pfs	Specifies that IPSec should ask for PFS when requesting new SAs for this crypto map entry, or that IPSec requires PFS when receiving requests for new SAs.
set security-association level per-host	Specifies that separate IPSec SAs should be requested for each source/destination host pair.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec SAs.
set session-key	Specifies the IPSec session keys within a crypto map entry.

Command	Description
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

debug crypto isakmp

To display messages about Internet Key Exchange (IKE) events, use the **debug crypto isakmp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug crypto isakmp aaa

no debug crypto isakmp aaa

Syntax Description	aaa	Specifies accounting events.
--------------------	-----	------------------------------

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modifications
	11.3 T	This command was introduced.
	12.2(15)T	The aaa keyword was added.

Examples

The following is sample output from the **debug crypto isakmp** command for an IKE peer that initiates an IKE negotiation.

First, IKE negotiates its own security association (SA), checking for a matching IKE policy.

```
Router# debug crypto isakmp
```

```
20:26:58: ISAKMP (8): beginning Main Mode exchange
20:26:58: ISAKMP (8): processing SA payload. message ID = 0
20:26:58: ISAKMP (8): Checking ISAKMP transform 1 against priority 10 policy
20:26:58: ISAKMP: encryption DES-CBC
20:26:58: ISAKMP: hash SHA
20:26:58: ISAKMP: default group 1
20:26:58: ISAKMP: auth pre-share
20:26:58: ISAKMP (8): atts are acceptable. Next payload is 0
```

IKE has found a matching policy. Next, the IKE SA is used by each peer to authenticate the other peer.

```
20:26:58: ISAKMP (8): SA is doing pre-shared key authentication
20:26:59: ISAKMP (8): processing KE payload. message ID = 0
20:26:59: ISAKMP (8): processing NONCE payload. message ID = 0
20:26:59: ISAKMP (8): SKEYID state generated
20:26:59: ISAKMP (8): processing ID payload. message ID = 0
20:26:59: ISAKMP (8): processing HASH payload. message ID = 0
20:26:59: ISAKMP (8): SA has been authenticated
```

Next, IKE negotiates to set up the IP Security (IPSec) SA by searching for a matching transform set.

```
20:26:59: ISAKMP (8): beginning Quick Mode exchange, M-ID of 767162845
20:26:59: ISAKMP (8): processing SA payload. message ID = 767162845
20:26:59: ISAKMP (8): Checking IPSec proposal 1
20:26:59: ISAKMP: transform 1, ESP_DES
20:26:59: ISAKMP: attributes in transform:
20:26:59: ISAKMP: encaps is 1
20:26:59: ISAKMP: SA life type in seconds
20:26:59: ISAKMP: SA life duration (basic) of 600
```

debug crypto isakmp

```

20:26:59: ISAKMP:      SA life type in kilobytes
20:26:59: ISAKMP:      SA life duration (VPI) of
                0x0 0x46 0x50 0x0
20:26:59: ISAKMP:      authenticator is HMAC-MD5
20:26:59: ISAKMP (8): atts are acceptable.

```

A matching IPSec transform set has been found at the two peers. Now the IPSec SA can be created (one SA is created for each direction).

```

20:26:59: ISAKMP (8): processing NONCE payload. message ID = 767162845
20:26:59: ISAKMP (8): processing ID payload. message ID = 767162845
20:26:59: ISAKMP (8): processing ID payload. message ID = 767162845
20:26:59: ISAKMP (8): Creating IPSec SAs
20:26:59:      inbound SA from 155.0.0.2 to 155.0.0.1 (proxy 155.0.0.2 to 155.0.0.1
)
20:26:59:      has spi 454886490 and conn_id 9 and flags 4
20:26:59:      lifetime of 600 seconds
20:26:59:      lifetime of 4608000 kilobytes
20:26:59:      outbound SA from 155.0.0.1      to 155.0.0.2      (proxy 155.0.0.1
to 155.0.0.2      )
20:26:59:      has spi 75506225 and conn_id 10 and flags 4
20:26:59:      lifetime of 600 seconds
20:26:59:      lifetime of 4608000 kilobytes

```

The following is sample output from the **debug crypto isakmp** command using the **aaa** keyword:

```
Router# debug crypto isakmp aaa
```

```
Start Example
```

```

01:38:55: ISAKMP AAA: Sent Accounting Message
01:38:55: ISAKMP AAA: Accounting message successful
01:38:55: ISAKMP AAA: Rx Accounting Message
01:38:55: ISAKMP AAA: Adding Client Attributes to Accounting Record
01:38:55: ISAKMP AAA: Accounting Started

```

```
Update Example
```

```

01:09:55: ISAKMP AAA: Accounting received kei with flags 0x1042
01:09:55: ISAKMP AAA: Updating Stats
01:09:55:      Previous in acc (PKTS) IN: 10 OUT: 10
01:09:55:      Traffic on sa (PKTS) IN: 176 OUT: 176

```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile and audits IPSec user sessions.
crypto map (global IPSec)	Enters crypto map configuration mode and creates or modifies a crypto map entry, creates a crypto profile that provides a template for configuration of a dynamically created crypto map, or configures a client accounting list.

isakmp authorization list

To configure an Internet Key Exchange (IKE) shared secret using the authentication, authorization, and accounting (AAA) server in an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **isakmp authorization list** command in isakmp profile configuration mode. To disable the shared secret, use the **no** form of this command.

isakmp authorization list *list-name*

no isakmp authorization list *list-name*

Syntax Description	<i>list-name</i>	AAA authorization list used for configuration mode attributes or preshared keys for aggressive mode.
---------------------------	------------------	--

Defaults	No default behaviors or values
-----------------	--------------------------------

Command Modes	Isakmp profile configuration
----------------------	------------------------------

Command History	Release	Modification
	12.2(15)T	This command was introduced.

Usage Guidelines	This command allows you to retrieve a shared secret from an AAA server.
-------------------------	---

Examples	The following example shows that an IKE shared secret is configured using an AAA server on a router: <pre>crypto isakmp profile vpnprofile isakmp authorization list ikessaaalist</pre>
-----------------	---

Related Commands	Command	Description
	aaa authorization	Sets parameters that restrict user access to a network.

match identity

To match an identity from a peer in an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **match identity** command in isakmp profile configuration mode. To remove the identity, use the **no** form of this command.

```
match identity { group group-name | address address [mask] [fvr] | host host-name | host domain
domain-name | user user-fqdn | user domain domain-name }
```

```
no match identity { group group-name | address address [mask] [fvr] | host host-name | host
domain domain-name | user user-fqdn | user domain domain-name }
```

Syntax Description

group <i>group-name</i>	A Unity group that matches identification (ID) type ID_KEY_ID. If Unity and main mode Rivest, Shamir, and Adelman (RSA) signatures are used, the <i>group-name</i> argument matches the Organizational Unit (OU) field of the Distinguished Name (DN).
address <i>address</i> [<i>mask</i>] [<i>fvr</i>]	An identity that matches the identity of type ID_IPV4_ADDR. <ul style="list-style-type: none"> <i>mask</i>—Use to match the range of the address. <i>fvr</i>—Use to match the address in the front door Virtual Route Forwarding (FVRF) Virtual Private Network (VPN) space.
host <i>host-name</i>	Identity that matches an identity of the type ID_FQDN.
host domain <i>domain-name</i>	Identity that matches an identity of the type ID_FQDN, whose fully qualified domain name (FQDN) ends with the domain name.
user <i>user-fqdn</i>	Identity that matches the FQDN.
user domain <i>domain-name</i>	Identity that matches the identities of the type ID_USER_FQDN. When the user domain keyword is present, all users having identities of the type ID_USER_FQDN and ending with “ <i>domain-name</i> ” will be matched.

Defaults

No default behavior or values

Command Modes

Isakmp profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

There must be at least one **match identity** command in an ISAKMP profile configuration. The peers are mapped to an ISAKMP profile when their identities are matched (as given in the ID payload of the Internet Key Exchange [IKE] exchange) against the identities that are defined in the ISAKMP profile. To uniquely map to an ISAKMP profile, no two ISAKMP profiles should match the same identity. If the peer identity is matched in two ISAKMP profiles, the configuration is invalid.

Examples

The following example shows that the **match identity** command is configured:

```
crypto isakmp profile vpnprofile
  match identity group vpngroup
  match identity address 10.53.11.1
  match identity host domain vpn.com
  match identity host server.vpn.com
```

set isakmp-profile

To set the Internet Security Association and Key Management Protocol (ISAKMP) profile name, use the **set isakmp-profile** command in crypto map configuration mode. To remove the ISAKMP profile name, use the **no** form of this command.

set isakmp-profile *profile-name*

no set isakmp-profile *profile-name*

Syntax Description

<i>profile-name</i>	Name of the ISAKMP profile.
---------------------	-----------------------------

Defaults

If the ISAKMP profile is not specified in the crypto map entry, the default is to the ISAKMP profile that is on the head. If there is no ISAKMP profile on the head, the default is “none.”

Command Modes

Crypto map configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

This command describes the ISAKMP profile to use when you start the Internet Key Exchange (IKE) exchange.

Before configuring an ISAKMP profile on a crypto map, you should set up the ISAKMP profile.

Examples

The following example shows that an ISAKMP profile has been configured on a crypto map:

```
crypto map vpnmap 10 ipsec-isakmp
 set isakmp-profile vpnprofile
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines a transform set, which is an acceptable combination of security protocols and algorithms.
crypto map (global)	Creates or modifies a crypto map entry.

vrf

To define the virtual routing and forwarding (VRF) value to which the IP Security (IPSec) tunnel will be mapped, use the **vrf** command in isakmp profile configuration mode. To disable the VRF that was defined, use the **no** form of this command.

```
vrf ivrf
```

```
no vrf ivrf
```

Syntax Description

<i>ivrf</i>	VRF to which the IPSec tunnel will be mapped.
-------------	---

Defaults

The VRF will be the same as the front door VRF (FVRF).

Command Modes

Isakmp profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use this command to map IPSec tunnels that terminate on a global interface to a specific Virtual Private Network (VPN).

If traffic from the router to a certification authority (CA) (for authentication, enrollment, or for obtaining a certificate revocation list [CRL]) or to a Lightweight Directory Access Protocol (LDAP) server (for obtaining a CRL) needs to be routed via a VRF, the **vrf** command must be added to the trustpoint. Otherwise, such traffic will use the default routing table.

If a profile does not specify one or more trustpoints, all trustpoints in the router will be used to attempt to validate the certificate of the peer (Internet Key Exchange [IKE] main mode or signature authentication). If one or more trustpoints are specified, only those trustpoints will be used.

Examples

The following example shows that two IPSec tunnels to VPN 1 and VPN 2 are terminated:

```
crypto isakmp profile vpn1
  vrf vpn1
  keyring vpn1
  match identity address 172.16.1.1 255.255.255.255
crypto isakmp profile vpn2
  vrf vpn2
  keyring vpn2
  match identity address 10.1.1.1 255.255.255.255
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
crypto ipsec transform-set vpn2 esp-3des esp-md5-hmac
!
crypto map crypmap 1 ipsec-isakmp
  set peer 172.16.1.1
  set transform-set vpn1
```

```
    set isakmp-profile vpn1
    match address 101
crypto map crypmap 3 ipsec-isakmp
    set peer 10.1.1.1
    set transform-set vpn2
    set isakmp-profile vpn2
    match address 102
!
!
interface Ethernet1/2
    ip address 172.26.1.1 255.255.255.0
    duplex half
    no keepalive
    no cdp enable
    crypto map crypmap
!
```

Glossary

IKE—Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IP security [IPSec]) that require keys. Before any IPSec traffic can be passed, each router, firewall, and host must verify the identity of its peer. This can be done by manually entering preshared keys into both hosts or by a certification authority (CA) service.

IPSec—IP security. IPSec is A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

ISAKMP—Internet Security Association and Key Management Protocol. ISAKMP is an Internet IPSec protocol (RFC 2408) that negotiates, establishes, modifies, and deletes security associations. It also exchanges key generation and authentication data (independent of the details of any specific key generation technique), key establishment protocol, encryption algorithm, or authentication mechanism.

L2TP session—Layer 2 Transport Protocol. L2TP are communications transactions between the L2TP access concentrator (LAC) and the L2TP network server (LNS) that support tunneling of a single PPP connection. There is a one-to-one relationship among the PPP connection, L2TP session, and L2TP call.

NAS—network access server. A NAS is a Cisco platform (or collection of platforms, such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the public switched telephone network [PSTN]).

PFS—perfect forward secrecy. PFS is a cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not compromised because subsequent keys are not derived from previous keys.

QM—Queue Manager. The Cisco IP Queue Manager (IP QM) is an intelligent, IP-based, call-treatment and routing solution that provides powerful call-treatment options as part of the Cisco IP Contact Center (IPCC) solution.

RADIUS—Remote Authentication Dial-In User Service. RADIUS is a database for authenticating modem and ISDN connections and for tracking connection time.

RSA—Rivest, Shamir, and Adelman. Rivest, Shamir, and Adelman are the inventors of the Public-key cryptographic system that can be used for encryption and authentication.

SA—security association. A SA is an instance of security policy and keying material that is applied to a data flow.

TACACS+—Terminal Access Controller Access Control System Plus. TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server.

TED—Tunnel Endpoint Discovery. TED is a Cisco IOS software feature that allows routers to discover IPSec endpoints.

VPN—Virtual Private Network. A VPN enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

VRF—A VPN routing/forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

VSA—vendor-specific attribute. A VSA is an attribute that has been implemented by a particular vendor. It uses the attribute Vendor-Specific to encapsulate the resulting AV pair: essentially, Vendor-Specific = protocol:attribute = value.

XAUTH—Extended authentication. XAUTH is an optional exchange between IKE Phase 1 and IKE Phase 2, in which the router demands additional authentication information in an attempt to authenticate the actual user (as opposed to authenticating the peer).

**Note**

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary.
