Configuration Guide

ISAKMP Profile Overview

The ISAKMP profile is an enhancement to Internet Security Association and Key Management Protocol (ISAKMP) configurations. It enables modularity of ISAKMP configuration for phase 1 negotiations. This modularity allows mapping different ISAKMP parameters to different IP Security (IPSec) tunnels, and mapping different IPSec tunnels to different VPN forwarding and routing (VRF) instances. ISAKMP profile enhancement was released as part of the VRF-aware IPSec feature in Cisco IOS® Software Release 12.2(15)T. Today, many applications and enhancements use the ISAKMP profile, including quality of service (QoS), router certificate management, and Multiprotocol Label Switching (MPLS) VPN configurations. This document provides an overview of the ISAKMP profile, and a description of the current applications that use the profile.

The ISAKMP profile is an enhancement to Internet Security Association and Key Management Protocol (ISAKMP) configurations. It enables modularity of ISAKMP configuration for phase 1 negotiations. This modularity allows mapping different ISAKMP parameters to different IP Security (IPSec) tunnels, and mapping different IPSec tunnels to different VPN forwarding and routing (VRF) instances. ISAKMP profile enhancement was released as part of the VRF-aware IPSec feature in Cisco IOS® Software Release 12.2(15)T. Today, many applications and enhancements use the ISAKMP profile, including quality of service (QoS), router certificate management, and Multiprotocol Label Switching (MPLS) VPN configurations. This document provides an overview of the ISAKMP profile, and a description of the current applications that use the profile.

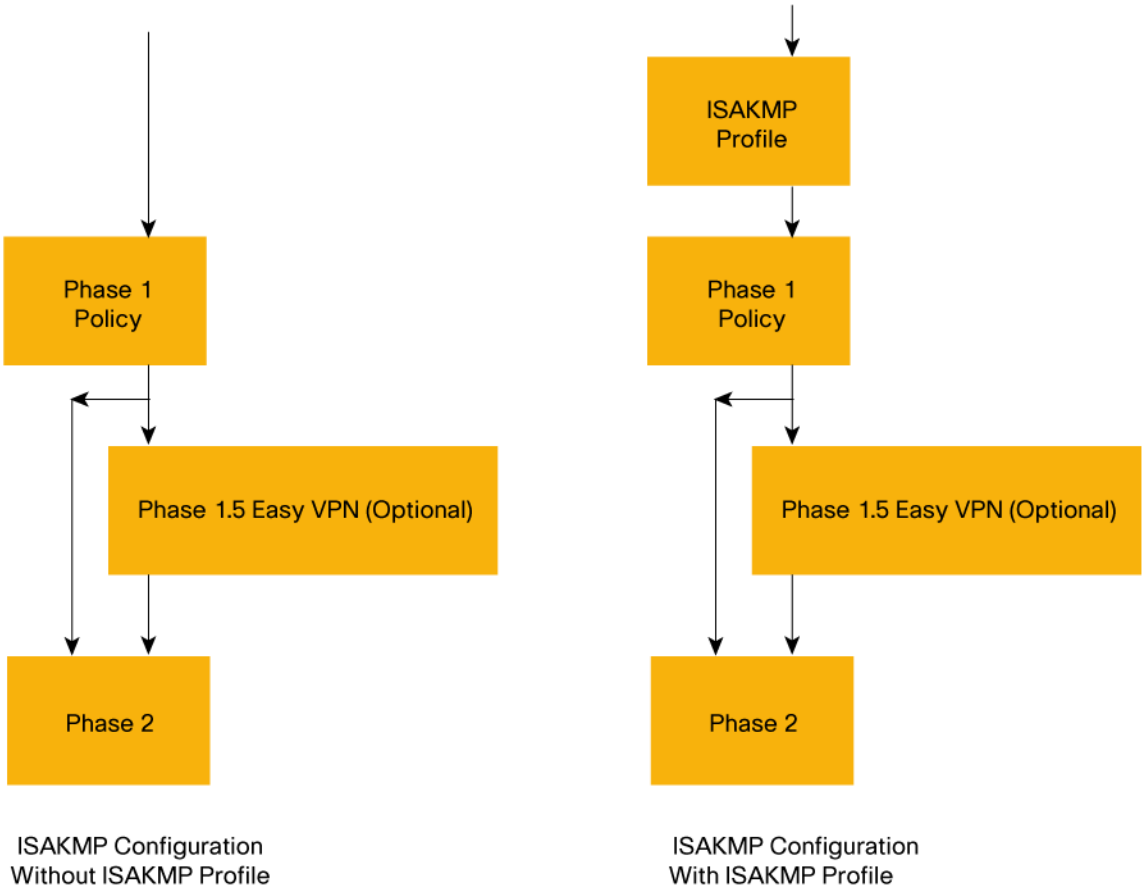
WHEN TO USE THE ISAKMP PROFILE

- Any router with two or more IPSec connections that requires different phase 1 parameters for different sites (for example, configuring site-to-site and remote access on the same router).
- It is recommended to use ISAKMP profile with Easy VPN Remote or Easy VPN Server configurations.
- If custom Internet Key Exchange (IKE) Phase 1 policies are needed for different peers. For example, whether XAUTH is to be applied a specific peer, rather than being applied on every connection.
- IPSec configuration using VRF-aware IPSec, which allows the use of single IP address to connect to different peers with different IKE Phase 1 parameters.

OVERVIEW OF THE ISAKMP PROFILE

An ISAKMP profile is a repository for IKE Phase 1 and IKE Phase 1.5 configuration for a set of peers (Figure 1). An ISAKMP profile applies parameters to an incoming IPSec connection identified uniquely through its concept of match identity criteria. These criteria are based on the IKE identity that is presented by incoming IKE connections and includes IP address, fully qualified domain name (FQDN), and group (the virtual private network [VPN] remote client grouping). The granularity of the match identity criteria will impose the granularity of applying the specified parameters. The ISAKMP profile applies parameters specific to each profile, such as trust points, peer identities, and XAUTH authentication, authorization, and accounting (AAA) list, keepalive, and others listed in the following sections.

Figure 1. IPSec Configuration With and Without ISAKMP Profile



ISAKMP Profile Parameters Configuration

There can be zero or more ISAKMP profiles on the Cisco IOS router. Following is a list of parameters that can be configured per profile:

1. `self-identity {`*`address`* `| fqdn | user-fqdn` *`user-fqdn`*`}`: Specifies the identity that the local IKE should use to identify itself to the remote peer.

- If not defined, IKE uses the global configured value.
- address—Uses the IP address of the egress interface.
- fqdn—Uses the FQDN of the router.
- user-fqdn—Uses the specified value.

2. `keyring` *`keyring-name`*: Specifies the keyring to use for Phase 1 authentication.

- If the keyring is not specified, the global key definitions are used.

3. `ca trust-point {`*`trustpoint-name`*`}`: Specifies a trustpoint to validate a Rivest, Shamir, and Adelman (RSA) certificate. If no trustpoint is specified in the ISAKMP profile, all the trustpoints that are configured on the Cisco IOS router are used to validate the certificate.

4. `client configuration address {initiate | respond}`: This command is used with Easy VPN Server; it specifies whether to initiate the mode configuration exchange or respond to mode configuration requests.

5. `client authentication list` *`list-name`*: AAA to use for authenticating the remote client during the extended authentication (XAUTH) exchange.
6. `isamkp authorization list` *`list-name`*: Network authorization server for receiving the Phase 1 preshared key and other attribute-value (AV) pairs.
7. `initiate mode aggressive`: Initiates aggressive mode exchange. If not specified, IKE always initiates Main Mode exchange.
8. `keepalive seconds retry retry-seconds`: Allows the gateway to send dead peer detection (DPD) messages to the peer. If not defined, the gateway uses the global configured value.

Note: The ISAKMP profile properties are applied as additional parameters to the ISAKMP policy configuration in the router. Details on the parameters configured under the ISAKMP policy are included in the ISAKMP policy configuration section below.

ISAKMP Profile Match Configuration

The ISAKMP parameters are applied at the ISAKMP profile level. The ISAKMP profile can uniquely identify devices through its concept of match identity criteria. These criteria are based on the IKE identity that is presented by incoming IKE connections and includes IP address, FQDN, and group (the VPN remote client grouping). The granularity of the match identity criteria will impose the granularity of the specified ISAKMP parameters, for example with Cisco QoS, to mark all traffic belonging to the VPN client group named "Engineering" as "TOS 5". Another example of having the granularity of a specified QoS policy imposed would be to allocate 30 percent of the bandwidth on an outbound WAN link to a specific group of remote VPN devices.

To match an identity from a peer in an ISAKMP profile, use the match identity command in isakmp profile configuration mode:

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

Specify the client IKE identity (ID) that is to be matched:

- group group-name—Matches the group-name with the ID type ID_KEY_ID. It also matches the group-name with the Organizational Unit (OU) field of the Distinguished Name (DN). Example: match identity group *`vpngroup`*
- address address [mask] fvrf—Matches the address with the ID type ID_IPV4_ADDR. The mask argument can be used to specify a range of addresses. The fvrf argument specifies that the address is in Front Door VRF (FVRF). Example: match identity address 10.53.11.1
- host hostname—Matches the hostname with the ID type ID_FQDN. Example: match identity host domain server1.vpn.com
- host domain domainname—Matches the domain name to the ID type ID_FQDN whose domain name is the same as the domainname. Use this command to match all the hosts in the domain. Example: match identity host domain vpn.com
- user username—Matches the username with the ID type ID_USER_FQDN. Example: match identity user username *`user1`*
- user domain domainname—Matches the ID type ID_USER_FQDN whose domain name matches the domainname. Example: match identity user domain vpn.com

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 identification [ID] payload of the IKE) 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
```

Crypto Keyring Configuration

A crypto keyring is a repository of preshared and RSA public keys. The keyring is configured in the router and assigned a key name. The keyring is then configured in the ISAKMP profile. There can be zero or more keyrings in the crypto ISAKMP profile. The following example shows the configuration of a crypto keyring:

```
crypto keyring KEYR1
 description The keys for VPN1
 pre-shared-key address 10.1.1.1 key cisco123
 pre-shared-key hostname host.lab.net key cisco123
 rsa-pubkey name host.vpn.com
   address 10.1.1.1
   serial-number 1000000
   key-string
   00302017 4A7D385B 1234EF29 335F
   Quit
!
crypto isakmp profile DMVPN
keyring KEYR1
```

Configuring an ISAKMP Profile on a Crypto Map

An ISAKMP profile must be applied to the crypto map. The VPN traffic classified as part of an ISAKMP profile is mapped as part of crypto map configurations for encryption. If the traffic is not part of any ISAKMP profile, the traffic will be part of the general IPSec configuration if it is configured. Perform this required task to configure an ISAKMP profile on a crypto map.

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

```
crypto map vpnmap 10 ipsec-isakmp
```

Configuration Example

The following example shows configuring ISAKMP profiles for Easy VPN client and DMVPN client on the same router:

```
aaa new-model
<   Commands omitted  >
!
!--- Keyring defining wildcard pre-shared key.
crypto keyring dmvpnspokes
pre-shared-key address 10.0.1.1 key cisco123
pre-shared-key address 10.0.1.2 key cisco123
!
!--- Create an ISAKMP policy for Phase 1 negotiations
!--- This policy is used by for the DMVPN spokes.
crypto isakmp policy 10
<   Commands omitted  >
!--- This policy is for Easy VPN Clients.
crypto isakmp policy 20
<   Commands omitted  >
!
!--- EasyVPN Client group configuration
crypto isakmp client config group hwc-group
<   Commands omitted  >
!
!--- ISAKMP Profile for EasyVPN Client
crypto isakmp profile VPNclient
match identity group hwc-group
client authentication list userauthen
isakmp authorization list hwc-group
client configuration address respond
!
!--- ISAKMP Profile for DMVPN Clients
crypto isakmp profile DMVPN
keyring dmvpnspokes
!--- Create an IPSec profile for the DMVPN GRE tunnel
crypto ipsec profile cisco
<   Commands omitted  >
match identity address 0.0.0.0
set isakmp-profile DMVPN
!
!--- This dynamic crypto map for
!---EasyVPN Client
crypto dynamic-map dynmap 10
set isakmp-profile VPNclient
```

```
!--- Crypto map only references
! -- the dynamic crypto map above.
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
interface Tunnel0
<   Commands omitted  >
tunnel protection ipsec profile cisco
!
interface FastEthernet0/0
<   Commands omitted  >
crypto map dynmap
```

For more information on this scenario, including complete configuration, please refer to the following document:
http://www.cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a00801eafcb.shtml

ISAKMP POLICY CONFIGURATION

The ISAKMP policy provides configuration of the security and encryption parameters used only for the security parameters of the ISAKMP communication channel, such as hashing, encryption, and key length. Following is a list of configuration parameters configured under the ISAKMP policy:

```
c3745-20(config)#crypto isakmp policy 1
c3745-20(config-isakmp)#?
ISAKMP commands:
  Authentication   Set authentication method for protection suite
  Default          Set a command to its defaults
  Encryption       Set encryption algorithm for protection suite
  Exit             Exit from ISAKMP protection suite configuration mode
  Group            Set the Diffie-Hellman group
  Hash             Set hash algorithm for protection suite
  Lifetime         Set lifetime for ISAKMP security association
  No               Negate a command or set its defaults
```

The ISAKMP profile affects only the negotiation phase of ISAKMP, and hence can be used in any subsequent phase of IPSec solutions, such as GRE, DMVPN, and Easy VPN.

ISAKMP PROFILES APPLICATIONS

Following are the current Cisco IOS features that are using and relying on the crypto ISAKMP profile feature:

1. VRF-Aware IPSec
2. IPSec and Quality of Service
3. SafeNet IPSec VPN Client Support
4. Certificate to ISAKMP Profile Mapping

1. VRF-Aware IPSec

The VRF-Aware IPSec feature was introduced in Cisco IOS Software Release 12.2(15)T. This feature provided the mapping of the crypto ISAKMP profile to a specific VRF. To map the IPSec tunnel to a VRF instance, use the vrf command in isakmp profile configuration mode. For example:

```
crypto isakmp profile vpn1
   vrf vpn1
   keyring vpn1
   match identity address 172.16.1.1 255.255.255.255
crypto map crypmap 1 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set vpn1
 set isakmp-profile vpn1
 match address 101
!
interface Ethernet1/2
 crypto map crypmap
```

2. IPSec and Quality of Service

The IPSec and Quality of Service feature allows Cisco IOS QoS policies to be applied to IPSec packet flows on the basis of a QoS group that can be added to the current ISAKMP profile. This feature was introduced in Cisco IOS Software Release 12.3(8)T.

The IPSec and Quality of Service feature allows you to apply QoS policies, such as traffic policing and shaping, to IPSec-protected packets by adding a QoS group to the ISAKMP profile. After the QoS group has been added, this group value will be mapped to the same QoS group as defined in QoS class maps. Any current QoS method that makes use of this QoS group tag can be applied to IPSec packet flows.

In the following example, a specific QoS policy is applied to two groups of remote users. Two ISAKMP profiles are configured so that upon initial connection via IKE, remote users are mapped to a specific profile. From that profile, all IPSec SAs that have been created for that remote user will be marked with the specific QoS group. As traffic leaves the outbound interface, the QoS service will map the IPSec-set QoS group with the QoS group that is specified in the class maps that comprise the service policy that is applied on that outbound interface.

Crypto Profile Configurations

```
crypto isakmp client configuration group yellow
   <Snip>
!
crypto isakmp profile blue
   match identity group sales
   qos-group 2
crypto isakmp profile yellow
   match identity group support
   match identity address 10.0.0.11
   qos-group 3
!
crypto dynamic-map mode 1
 set isakmp-profile blue
```

```
crypto dynamic-map mode 2
 set isakmp-profile yellow
!
crypto map mode 1 ipsec-isakmp dynamic mode
```

QoS Configurations

```
class-map match-all yellow
 match qos-group 3
class-map match-all blue
 match qos-group 2
!
policy-map clients
 class blue
  set precedence 5
 class yellow
  set precedence 7
!
interface FastEthernet0/0
 crypto map mode
 service-policy out clients
```

3. SafeNet IPSec VPN Client Support

The SafeNet IPSec VPN Client Support feature allows you to limit the scope of an ISAKMP profile or ISAKMP keyring configuration to a local termination address or interface. The benefit of this feature is that different customers can use the same peer identities and ISAKMP keys by using different local termination addresses.

Prior to Cisco IOS Software Release 12.3(14)T, ISAKMP profile and ISAKMP keyring configurations could be only global, meaning that the scope of these configurations could not be limited by any locally defined parameters (VRF instances were an exception). For example, if an ISAKMP keyring contained a preshared key for address 10.11.12.13, the same key would be used if the peer had the address 10.11.12.13, regardless of the interface or local address to which the peer was connected. There are situations, however, in which users prefer that associate keyrings be bound not only with VRF instances but also to a particular interface.

1. Limiting an ISAKMP profile to a local termination address or interface:

```
crypto isakmp profile profile1
  keyring keyring1
  match identity address 10.0.0.0 255.0.0.0
  local-address serial2/0
```

2. Limiting a keyring to a local termination address or interface:

```
crypto keyring keyring1
  local-address serial2/0
  pre-shared-key address 10.0.0.1
```

4. Certificate to ISAKMP Profile Mapping

The Certificate to ISAKMP Profile Mapping feature enables you to assign an ISAKMP profile to a peer on the basis of the contents of arbitrary fields in the certificate. This feature also allows you to assign a group name to peers that are assigned an ISAKMP profile.

Prior to Cisco IOS Software Release 12.3(8)T, the only way to map a peer to an ISAKMP profile was to use the ISAKMP identity field in the ISAKMP exchange. When certificates were used for authentication, the ISAKMP identity payload contained the subject name from the certificate. If a certificate authority (CA) did not provide the required group value in the first Organizational Unit (OU) field of a certificate, an ISAKMP profile could not be assigned to a peer.

Effective with Cisco IOS Software Release 12.3(8)T, a peer can still be mapped as explained above. However, the Certificate to ISAKMP Profile Mapping feature enables you to assign an ISAKMP profile to a peer on the basis of the contents of arbitrary fields in the certificate. You are no longer limited to assigning an ISAKMP profile on the basis of the subject name of the certificate. In addition, this feature allows you to assign a group to a peer to which an ISAKMP profile has been assigned.

To associate a group with the peer that has been assigned an ISAKMP profile, use the client configuration command in crypto ISAKMP profile configuration mode:

```
client configuration group group-name
```

To assign an ISAKMP profile to a peer on the basis of the contents of arbitrary fields in the certificate, use the match certificate command in crypto ISAKMP profile configuration mode:

```
match certificate certificate-map
```

For more information on configuring this feature, please check the following documentation:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a0080225d2a.html

RELATED INFORMATION

- IPsec Support Page
- DMVPN and Easy VPN Server with ISAKMP Profile Configuration Example (IPSec Negotiation/IKE Protocols)
- Certificate to ISAKMP Profile Mapping
- SafeNet IPSec VPN Client Support
- An Introduction to IPSec Encryption
- Configuring IPSec Network Security
- Configuring Internet Key Exchange Security Protocol
- Technical Support—Cisco Systems

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

205233.BQ_ETMG_KL_10.05

Printed in the USA