Configuring GRE over IPsec

Restrictions for GRE over IPsec

- GRE over IPsec doesn't support Virtual Routing and Forwarding (VRF).
- GRE over IPsec doesn't support Multipoint GRE (mGRE).
- GRE over IPSec doesn't support multiple sessions from the same tunnel source to the same tunnel destination.
- GRE over IPsec doesn't support concurrent Static Virtual Tunnel Interface (SVTI) and GRE over IPsec tunnel with the same tunnel source and tunnel destination.

Information about GRE Over IPsec

You can configure Generic Routing Encapsulation (GRE) over an Internet Protocol Security (IPsec) tunnel on Cisco IOS XE devices. GRE can encapsulate several types of traffic such as unicast, multicast, broadcast, and MPLS. However, GRE doesn't provide any type of protection for the transmitted payload.

Internet Protocol Security (IPsec) provides confidentiality, integrity, and authentication to the payloads transmitted through IPsec tunnels. However, IPsec can function only with IP packets.

The GRE over IPsec feature allows for the flexibility of using GRE along with the security of IPsec. GRE encapsulates the packets. IPsec encrypts the packets and transports them through an IPsec tunnel.

How to Configure GRE over IPsec

The following sections explain the procedures that you can perform to configure a GRE over IPsec tunnel interface.

Configuring the IKEv2 Keyring

Perform this task to configure the IKEv2 key ring if the local or remote authentication method is a preshared key.

IKEv2 key ring keys must be configured in the peer configuration submode that defines a peer subblock. An IKEv2 key ring can have multiple peer subblocks. A peer subblock contains a single symmetric or asymmetric key pair for a peer or peer group identified by any combination of the hostname, identity, and IP address.

IKEv2 key rings are independent of IKEv1 key rings. The key differences are as follows:

- IKEv2 key rings support symmetric and asymmetric preshared keys.
- IKEv2 key rings do not support Rivest, Shamir, and Adleman (RSA) public keys.
- IKEv2 key rings are specified in the IKEv2 profile and are not looked up, unlike IKEv1, where keys are looked up on receipt of MM1 to negotiate the preshared key authentication method. The authentication method is not negotiated in IKEv2.
- IKEv2 key rings are not associated with VPN routing and forwarding (VRF) during configuration. The VRF of an IKEv2 key ring is the VRF of the IKEv2 profile that refers to the key ring.
- A single key ring can be specified in an IKEv2 profile, unlike an IKEv1 profile, which can specify multiple key rings.
- A single key ring can be specified in more than one IKEv2 profile, if the same keys are shared across peers matching different profiles.
- An IKEv2 key ring is structured as one or more peer subblocks.

On an IKEv2 initiator, the IKEv2 key ring key lookup is performed using the peer's hostname or the address, in that order. On an IKEv2 responder, the key lookup is performed using the peer's IKEv2 identity or the address, in that order.

Note You cannot configure the same identity in more than one peer.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto ikev2 keyring** *keyring-name* **Example:** `Device(config)# crypto ikev2 keyring kyr1`	Defines an IKEv2 key ring and enters IKEv2 key ring configuration mode.

	Command or Action	Purpose
Step 4	**peer** *name* **Example:** `Device(config-ikev2-keyring)# peer peer1`	Defines the peer or peer group and enters IKEv2 key ring peer configuration mode.
Step 5	**description** *line-of-description* **Example:** `Device(config-ikev2-keyring-peer)# description this is the first peer`	(Optional) Describes the peer or peer group.
Step 6	**hostname** *name* **Example:** `Device(config-ikev2-keyring-peer)# hostname host1`	Specifies the peer using a hostname.
Step 7	**address** {*ipv4-address* [*mask*] | *ipv6-address prefix*} **Example:** `Device(config-ikev2-keyring-peer)# address 10.0.0.1 255.255.255.0`	Specifies an IPv4 or IPv6 address or range for the peer. **Note** This IP address is the IKE endpoint address and is independent of the identity address.

Step 8	**identity** {**address** {*ipv4-address* | *ipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *key-id*}
	Example:
	`Device(config-ikev2-keyring-peer)# identity address 10.0.0.5`
		Identifies the IKEv2 peer through the following identities:
		• E-mail
		• Fully qualified domain name (FQDN) .
		Note When FQDN is used to identify the peer in the keyring configuration, use the IP address of the peer along with the FQDN
		`crypto ikev2 keyring key1`
		`peer headend-1`
		`address 10.1.1.1 >>>>>>>>>`
		`identity fqdn`
		`NFVIS-headend-1.cisco.com`
		`pre-shared-key Cisco123`
		• IPv4 or IPv6 address
		• Key ID
		Note The identity is available for key lookup on the IKEv2 responder only.

Step 9	**pre-shared-key** {**local** | **remote**} [**0** | **6**] *line* **hex** *hexadecimal-string*	Specifies the preshared key for the peer.

	Command or Action	Purpose
	Example: `Device(config-ikev2-keyring-peer)# pre-shared-key local key1`	
Step 10	**end** **Example:** `Device(config-ikev2-keyring-peer)# end`	Exits IKEv2 key ring peer configuration mode and returns to privileged EXEC mode.

IKEv2 Profile

An IKEv2 profile is a repository of nonnegotiable parameters of the IKE SA, such as local or remote identities and authentication methods and services that are available to authenticated peers that match the profile. An IKEv2 profile must be attached to either a crypto map or an IPsec profile on the initiator.

Note You must configure the responder-only configuration on the responder device because the IPsec process might fail without this configuration.

Attaching an IKEv2 profile to an IPsec profile

To attach an IKEv2 profile to an IPsec profile, perform the following procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto ipsec transform-set** *transform-set-name* **Example:** `Device(config)# crypto ipsec transform-set tfs`	Defines a transform set. Enters crypto transform configuration mode.
Step 4	**mode tunnel** **Example:** `Device(cfg-crypto-tran)# mode tunnel`	(Optional) Changes the mode associated with the transform set.

	Command or Action	Purpose
Step 5	**crypto IPsec profile** *profile-name* **Example:** `Device(cfg-crypto-tran)# crypto IPsec profile PROF`	Defines the IPsec parameters used for IPsec encryption between two IPsec devices. Enters IPsec profile configuration mode.
Step 6	**set transform-set** *transform-set-name* **Example:** `Device(ipsec-profile)# set transform-set tfs esp-gcm`	Specifies the transform sets used with the crypto map entry.
Step 7	**set ikev2-profile** *profile-name* **Example:** `Device(ipsec-profile)# set ikev2-profile ikev2_prof`	Attaches an IKEv2 profile to an IPSec profile.
Step 8	**exit** **Example:** `Device(ipsec-profile)# exit`	Exits IPsec profile configuration mode. Enters global configuration mode.

Configuring a GRE over IPsec Tunnel Interface

To create a GRE over IPsec tunnel and configure a tunnel source and tunnel destination under the tunnel interface, perform the following procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *tunnel number* **Example:** `Device(config)# interface tunnel 100`	Specifies the interface on which the tunnel will be configured. Enters interface configuration mode.

	Command or Action	Purpose
Step 4	**ip address** *address mask* **Example:** `Device(config-if)# ip address 128.1.1.1 255.255.255.0`	Specifies the IP address and mask.
Step 5	**tunnel source** *interface-type interface-number* **Example:** `Device(config-if)# tunnel source 120.1.1.1`	Specifies the tunnel source as a loopback interface.
Step 6	**tunnel destination** *ip-address* **Example:** `Device(config-if)# tunnel destination 120.1.1.2`	Identifies the IP address of the tunnel destination.
Step 7	**tunnel protection IPsec profile** *profile-name* **Example:** `Device(config-if)# tunnel protection IPsec profile ipsec-prof`	Associates a tunnel interface with an IPsec profile.
Step 8	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode. Returns to privileged EXEC mode.

Configuration Examples for GRE over IPsec

The following sections provide configuration examples for GRE over IPsec.

Example: Configuring GRE over IPsec

The following example shows how to configure an Internet Key Exchange Version 2 (IKEv2) key ring with symmetric preshared keys based on an IP address:

```
conf t
crypto ikev2 keyring ikev2_key
peer mypeer
address 0.0.0.0 0.0.0.0
pre-shared-key cisco123
```

The following example shows how to configure an IKEv2 profile:

```
conf t
```

```
crypto ikev2 profile ikev2_prof
 match identity remote address 120.1.1.2
 authentication remote pre-share
 authentication local pre-share
 keyring local ikev2_key
dpd 10 2 periodic
end
```

The following example shows how to attach an IKEv2 profile to an IPSec profile:

```
conf t
crypto ipsec transform-set tfs esp-aes esp-sha-hmac
esn
mode tunnel
end
conf t
crypto ipsec profile ipsec_prof
 set transform-set tfs
 set ikev2-profile ikev2_prof
end
```

The following example shows how to create a tunnel interface and configure a tunnel source and tunnel destination under the tunnel interface:

```
conf t
interface Tunnel100
ip address 128.1.1.1 255.255.255.0
tunnel source 120.1.1.1
tunnel destination 120.1.1.2
tunnel protection ipsec profile ipsec_prof
end
```

Feature Information for GRE over IPsec

This table provides release and related information for the features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Dublin 17.11.1	GRE over IPsec	The GRE over IPsec feature allows a payload to be GRE encapsulated and transferred securely over an IPsec tunnel.

Use the Cisco Feature Navigator to find information about platform and software image support. To access the Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.