GRE Over IPsec Tunnels

Table 1: Feature History

Feature Name	Release Information	Description
GRE Over IPsec Tunnels Between Cisco IOS XE Devices	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature allows you to set up GRE over IPsec tunnels with IKEv2 RSA-SIG authentication on Cisco IOS XE Catalyst SD-WAN devices in the controller mode to connect to Cisco IOS XE devices in the autonomous mode. This set up enables Cisco IOS XE Catalyst SD-WAN devices to use OSPFv3 as the dynamic routing protocol and multicast traffic across the WAN network. You can configure GRE over IPsec tunnels using the CLI device templates in Cisco SD-WAN Manager for Cisco IOS XE Catalyst SD-WAN devices.

GRE Over IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices

You can configure Generic Routing Encapsulation (GRE) over an Internet Protocol Security (IPsec) tunnels on Cisco IOS XE devices. GRE supports multicast and dynamic routing protocol, IPsec with IKEv2 protocol offers the enhanced security. GRE over IPsec tunnels are configured using the OSPFv3(dynamic routing protocol) and multicast(in sparse-mode), using the IPsec to encrypt the packets across the tunnels, and using the IKEv2 along with RSA-SIG authentication to perform authentication, establish and maintain security associations.

Prerequisites for GRE Over IPsec Tunnels Between Cisco IOS XE Devices

To configure GRE over IPsec tunnels, use Internet Key Exchange Version 2 (IKEv2) protocol, and RSA Signature as the authentication method.

Restrictions for GRE Over IPsec Tunnels Between Cisco IOS XE Devices

- IPv6 addresses for IPsec tunnel source are not supported.
- In IKEv2 Preshared Keys (PSK), the '\' character is not supported and should not be used.
- You cannot configure GRE Over IPsec tunnels between Cisco IOS XE devices using Cisco SD-WAN Manager GUI.

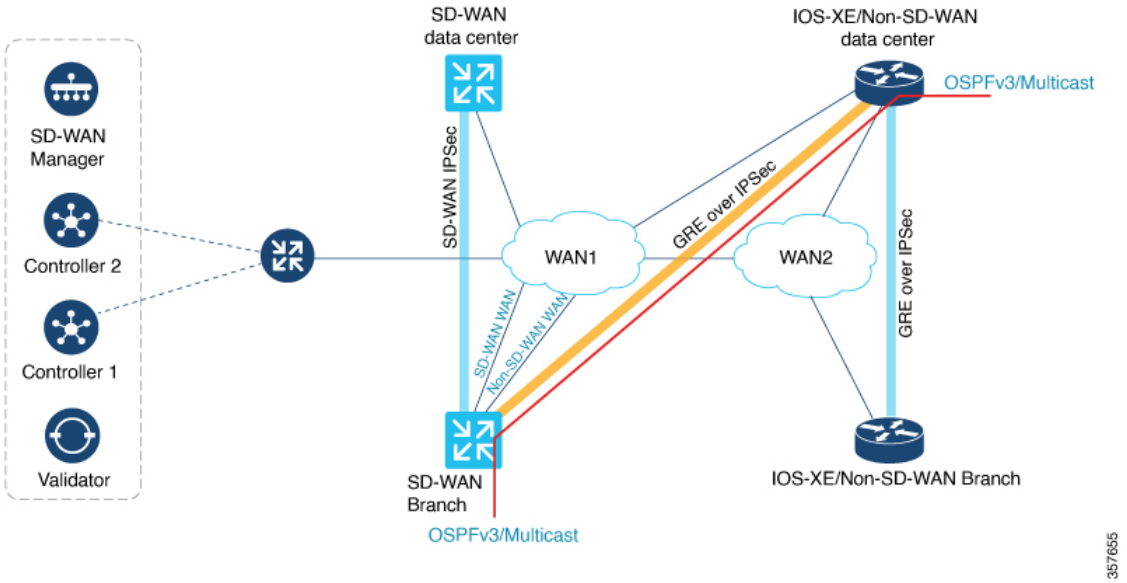
Benefits of GRE Over IPsec Tunnels Between Cisco IOS XE Devices

- Enables migration. You can either migrate to a Cisco Catalyst SD-WAN network or modify a device to support Cisco Catalyst SD-WAN.
- Provides a full mesh connection between a branch and data center, irrespective of whether the network is a Cisco Catalyst SD-WAN network or a non-SD-WAN network.
- Supports OSPFv3 and multicast traffic from a Cisco Catalyst SD-WAN enabled branch to a non-SD-WAN data center.

Use Case for GRE Over IPsec Tunnels Between Cisco IOS XE Devices

In this sample topology, there are Cisco IOS XE devices that are located in different data centers and branches. Two Cisco IOS XE devices in the controller mode are located in the Cisco Catalyst SD-WAN network, one in a data center and another in a branch. The other two Cisco IOS XE devices in the autonomous mode are located in a non-SD-WAN network. A GRE over IPsec tunnel is configured to connect the Cisco IOS XE devices from the branch on the Cisco Catalyst SD-WAN network to the data center located in the non-SD-WAN network.

Note Ensure that the tunnel source is configured with the global VPN for the WAN side and the tunnel VRF configured with the service VPN for the Service side.



Configure GRE Over IPsec Tunnels Between Cisco IOS XE Devices

Configuring GRE over IPsec tunnels using Cisco SD-WAN Manager is a two-step process:

1. Install Certification Authentication.

   Import the pkcs12 file on the Cisco IOS XE Catalyst SD-WAN device using the **pki import** command. For information, see the **Install Certification Authentication** section in Configure GRE Over IPsec Tunnels Between Cisco IOS XE Devices Using the CLI .

2. Prepare the GRE over IPsec tunnel configurations (GRE, IPsec, IKEv2, PKI, OSPFv3 and Multicast) via the Cisco SD-WAN Manager CLI Template, and push it to the Cisco IOS XE Catalyst SD-WAN device. For information about using a device template, see Device Configuration-Based CLI Templates for Cisco IOS XE Catalyst SD-WAN devices.

   See the **Configure GRE Over IPsec Tunnel** section in Configure GRE Over IPsec Tunnels Between Cisco IOS XE Devices Using the CLI for a sample configuration for use in the CLI template.

Note Note: Add the **crypto pki trustpoint** configuration command explicitly in the Cisco SD-WAN Manager CLI template.

Configure GRE Over IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices Using the CLI

This section provides example CLI configurations to configure GRE over IPsec tunnels for Cisco IOS XE Catalyst SD-WAN devices in the controller mode.

Install Certification Authentication

Import the pkcs12 file on the Cisco IOS XE Catalyst SD-WAN device using the **pki import** command.

```
Device# crypto pki import trustpoint_name pkcs12 bootflash:certificate_name
password cisco
```

Execute the **crypto pki trustpoint** command to reconfigure the Cisco IOS XE Catalyst SD-WAN device.

```
Device(config)# crypto pki trustpoint trustpoint_name
Device(ca-trustpoint)# enrollment pkcs12
Device(ca-trustpoint)# revocation-check none
Device(ca-trustpoint)# rsakeypair trustpoint_name
```

Configure GRE over IPsec Tunnel

The following is a sample configuration example for configuring GRE over IPsec tunnel.

```
interface Tunnel100
 no shutdown
 vrf forwarding 11
 ip address 10.10.100.1 255.255.255.0
 ipv6 address 2001:DB8:0:ABCD::1
 ipv6 enable
 ospfv3 100 ipv4 area 0
 ospfv3 100 ipv6 area 0
 tunnel source GigabitEthernet4
 tunnel destination 10.0.21.16
 tunnel path-mtu-discovery
 tunnel protection ipsec profile ikev2_TP
exit
!
crypto ikev2 policy policy1-global
 proposal p1-global
!
crypto ikev2 profile cisco
 authentication local rsa-sig
 authentication remote rsa-sig
 identity local dn
 match address local 10.0.20.15
 match fvrf any
 match identity remote any
 pki trustpoint TRUST_POINT_100
!
crypto ikev2 proposal p1-global
 encryption aes-cbc-128 aes-cbc-256
 group 14 15 16
 integrity sha1 sha256 sha384 sha512
!
crypto ipsec transform-set transform-set-v4 esp-gcm 256
 mode transport/tunnel
!
crypto ipsec profile ikev2_TP
 set ikev2-profile cisco
 set pfs group16
 set transform-set transform-set-v4
 set security-association lifetime kilobytes disable
 set security-association replay window-size 512
!
crypto pki trustpoint TRUST_POINT_100
 enrollment pkcs12
 revocation-check none
 rsakeypair TRUST_POINT_100
```

Note The configurations for GRE over IPsec tunnels for Cisco IOS XE devices in the autonomous mode are the same as in the controller mode shown above.

Furthermore, the steps to install certification authentication for Cisco IOS XE devices in the autonomous mode is the same as in Cisco IOS XE Catalyst SD-WAN devices, and there is no requirement for you to reconfigure **crypto pki trustpoint** explicitly on the Cisco IOS XE devices in the autonomous mode.

Monitor GRE Over IPsec Tunnels Between Cisco IOS XE Devices Using the CLI

Example 1

The following is sample output from the **show crypto pki certificates** command using the optional trustpoint-name argument and verbose keyword. The output shows the certificate of a device and the certificate of the CA. In this example, general-purpose RSA key pairs are previously generated, and a certificate is requested and received for the key pair.

```
Device# show crypto pki certificates verbose TRUST_POINT_100
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 31
  Certificate Usage: General Purpose
  Issuer:
    o=CRDC
    ou=CRDC-Lab
    cn=vCisco-CA
  Subject:
    Name: ROUTER1
    cn=ROUTER1
    o=Internet Widgits Pty Ltd
    st=Some-State
    c=AU
  Validity Date:
    start date: 12:57:14 UTC Jul 24 2021
    end   date: 12:57:14 UTC Jul 22 2031
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
  Signature Algorithm: SHA1 with RSA Encryption
  Fingerprint MD5: D0AD3252 586C0DB8 9F4EFC15 1D81AC5F
  Fingerprint SHA1: 6824ED1A C1405149 577CF210 C0BC83D1 8741F0D1
  X509v3 extensions:
    X509v3 Subject Key ID: E806DCF5 89698C43 97795999 4440D7F1 16F9827C
    X509v3 Authority Key ID: 91C2776C 651DF253 08FA9614 D2082F99 BEBF0B00
    Authority Info Access:
  Cert install time: 08:29:26 UTC Oct 21 2021
  Associated Trustpoints: TRUST_POINT_100
  Storage: nvram:CRDC#31.cer
  Key Label: TRUST_POINT_100
  Key storage device: private config

CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
```

```
  Issuer:
    o=CRDC
    ou=CRDC-Lab
    cn=vCisco-CA
  Subject:
    o=CRDC
    ou=CRDC-Lab
    cn=vCisco-CA
  Validity Date:
    start date: 13:41:14 UTC Feb 9 2018
    end   date: 13:41:14 UTC Feb 9 2038
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (4096 bit)
  Signature Algorithm: SHA1 with RSA Encryption
  Fingerprint MD5: 5ECA97DB 97FF1B95 DFEEB8FB DAB6656F
  Fingerprint SHA1: 73A7E91E 3AB12ABE 746348E4 A0E21BE3 8413130C
  X509v3 extensions:
    X509v3 Key Usage: 86000000
      Digital Signature
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 91C2776C 651DF253 08FA9614 D2082F99 BEBF0B00
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Authority Key ID: 91C2776C 651DF253 08FA9614 D2082F99 BEBF0B00
    Authority Info Access:
  Cert install time: 08:29:23 UTC Oct 21 2021
  Associated Trustpoints: TRUST_POINT_ex TRUST_POINT_100
  Storage: nvram:CRDC#1CA.cer
```

Example 2

The following is sample output from the **show crypto ipsec sa** command to display the settings used by IPsec security associations.

```
Device# show crypto ipsec sa
interface: Tunnel100
    Crypto map tag: Tunnel100-head-0, local addr 10.0.20.15

   protected vrf: 11
   local  ident (addr/mask/prot/port): (10.0.20.15/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.0.21.16/255.255.255.255/47/0)
   current_peer 10.0.21.16 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 2674, #pkts encrypt: 2674, #pkts digest: 2674
    #pkts decaps: 2677, #pkts decrypt: 2677, #pkts verify: 2677
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.0.20.15, remote crypto endpt.: 10.0.21.16
     plaintext mtu 1446, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet4
     current outbound spi: 0xDEFA0160(3740926304)
     PFS (Y/N): Y, DH group: group16

     inbound esp sas:
      spi: 0x32A84C67(849890407)
        transform: esp-gcm 256 ,
        in use settings ={Tunnel, }
        conn id: 2057, flow_id: CSR:57, sibling_flags FFFFFFFF80000048, crypto map:
Tunnel100-head-0
        sa timing: remaining key lifetime (sec): 2217
        Kilobyte Volume Rekey has been disabled
```

```
        IV size: 8 bytes
        replay detection support: Y  replay window size: 512
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xDEFA0160(3740926304)
        transform: esp-gcm 256 ,
        in use settings ={Tunnel, }
        conn id: 2058, flow_id: CSR:58, sibling_flags FFFFFFFF80000048, crypto map:
Tunnel100-head-0
        sa timing: remaining key lifetime (sec): 2217
        Kilobyte Volume Rekey has been disabled
        IV size: 8 bytes
        replay detection support: Y  replay window size: 512
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

Example 3

The following example shows the **show crypto session detail** command output that displays the status information for active crypto sessions.

```
Device# show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP VPN

Interface: Tunnel100
Profile: cisco
Uptime: 03:59:01
Session status: UP-ACTIVE
Peer: 10.0.21.16 port 500 fvrf: (none) ivrf: 11
      Phase1_id: cn=ROUTER2,o=Internet Widgits Pty Ltd,st=Some-State,c=AU
      Desc: (none)
  Session ID: 1780
  IKEv2 SA: local 10.0.20.15/500 remote 10.0.21.16/500 Active
          Capabilities:U connid:1 lifetime:20:00:59
  IPSEC FLOW: permit 47 host 10.0.20.15 host 10.0.21.16
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 1668 drop 0 life (KB/Sec) KB Vol Rekey Disabled/2294
        Outbound: #pkts enc'ed 1665 drop 0 life (KB/Sec) KB Vol Rekey Disabled/2294
```

Example 4

The following is sample output from the **show crypto key mypubkey rsa** command that displays the RSA public keys of your device.

```
Device# show crypto key mypubkey rsa
Key name: TRUST_POINT_100
Key type: RSA KEYS
 Storage Device: private-config
 Usage: General Purpose Key
 Key is not exportable. Redundancy enabled.
 Key Data:
```

```
  30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
  00B4E83F ABAE87DC DB7ACBB2 844F5FD6 FF2E9E02 DE49A302 D3D7884F 0B26EE6A
  D3D56275 4D733A4F 5D974061 CE8FB520 54276D6D 3B132C82 EB8A3C24 115F77F5
  C38740CE 1BBD89DB 3F766728 649B63FC 2C40C3AD 251656A1 BAF8341E 1736F03D
  0A0D15AF 0E9D3E94 4E2074C7 BA572CA3 95B3D664 916ADA74 281CDE07 B3DD0B42
  13289610 32E611AB 2B3B4EB6 0A3573B1 F097AC2A 3720961C 97597201 3CE8171C
  F02B99B4 3B7B718F 83E221E1 E172554D C2BEA127 93882766 A28C5E8C 4B83BDC5
  A161597D 2C3D8E13 3BE00D8F 02D0AD55 962DF402 599580A6 F049DBF4 045D751B
  A8932156 10B29D9F 037AB33F C1FC463D E59E014C 27660223 546A8B3A E6997713
  CF020301 0001
% Key pair was generated at: 00:22:51 UTC Oct 27 2021
```