

CISCO Catalyst SD-WAN Security Configuration User Guide

[Home](#) » [Cisco](#) » CISCO Catalyst SD-WAN Security Configuration User Guide 



GRE Over IPsec Tunnels

Contents

- [1 Catalyst SD-WAN Security Configuration](#)
- [2 GRE Over IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices](#)
- [3 IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices](#)
- [4 Documents / Resources](#)
 - [4.1 References](#)

Catalyst SD-WAN Security Configuration



Note

To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-

WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: Cisco vManage to Cisco Catalyst SD-WAN Manager, Cisco vAnalytics to Cisco Catalyst SD-WAN Analytics, Cisco vBond to Cisco Catalyst SD-WAN Validator, and Cisco vSmart to Cisco Catalyst SD-WAN Controller. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

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.
IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN and Third-Party Devices	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This feature allows you to configure an IPv6 GRE or IPSEC tunnel from a Cisco IOS XE Catalyst SD-WAN device to a third-party device over a service VPN.

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.
- 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.

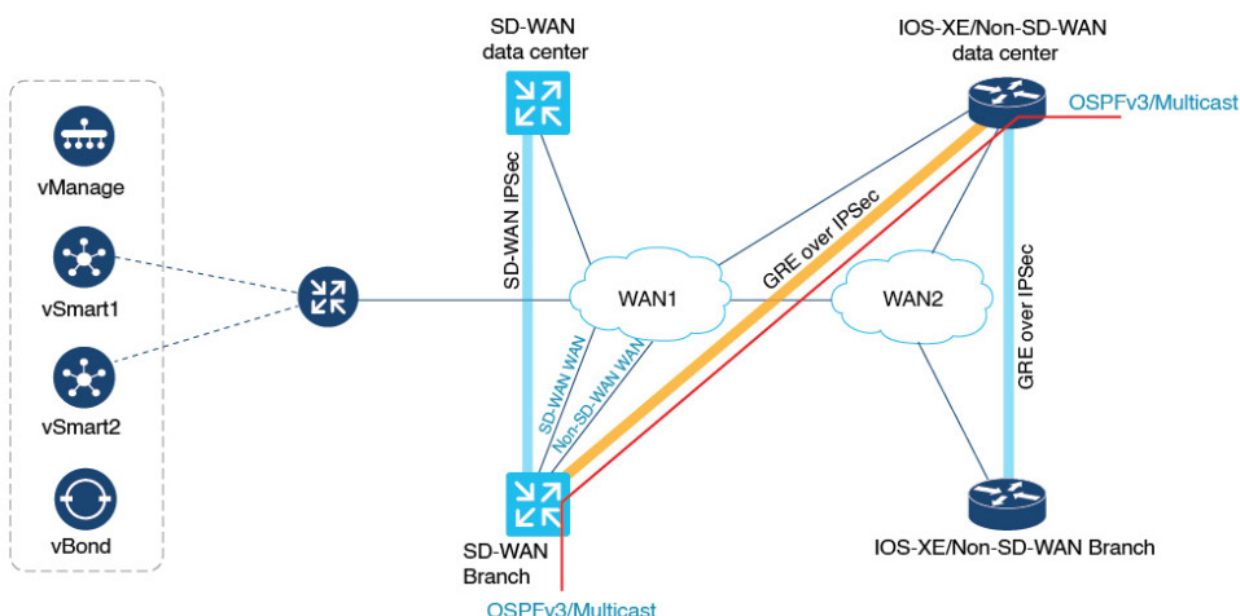
Use Case for GRE Over IPsec Tunnels Between Cisco IOS XE Devices

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.



357655

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 pcg 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 pcg 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 ABABE87DC 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
```

IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a

This feature allows you to configure an IPv6 GRE or IPSEC tunnel from Cisco IOS XE Catalyst SD-WAN devices to a third-party device over a service VPN. The following types are supported:

- IPv6 GRE tunnel over IPv4 Underlay
- IPv6 GRE tunnel over IPv6 Underlay

- IPsec IPv6 tunnel over IPv4 Underlay
- IPsec IPv6 tunnel over IPv6 Underlay

Restrictions for IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices

- This feature is configurable only through the device CLI template. Feature templates are not supported.
- Feature parcel is not supported.
- Dual stack is not supported for IPsec SVTI tunnels but supported for GRE tunnels.
- The interface name as loopback for tunnel source is not supported. When you use a loopback interface as a tunnel source, you must provide either an IPv4 or IPv6 address as the tunnel source field. You can provide an interface name as tunnel source field for the physical interface and sub-interface.

Supported Devices for IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices

Table 2: Supported Devices and Releases

Release	Supported Devices
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and later	<ul style="list-style-type: none"> • Cisco Catalyst 8300 Series Edge Platforms • Cisco Catalyst 8500 Series Edge Platforms • Cisco Catalyst 8500L Edge Platforms • Cisco Catalyst 8000V Edge Software • Cisco ASR 1001-HX Router • Cisco ASR 1002-HX Router • Cisco ISR1100 Series Routers • Cisco 4461 Integrated Services Router

Configure IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices Using a CLI Template

Configure a Common Source Interface

This section provides an example CLI configuration to configure a common source interface.

1. Enter the global configuration mode.

```
configure terminal
```
2. Enter interface configuration mode.

```
interface GigabitEthernet1
```
3. Enable the interface.

```
no shutdown
```
4. Set an IP address for the interface.

```
ip address 209.165.200.225 255.255.255.0
```
5. Configure an IPv6 address.

```
ipv6 address 2001:DB8:200::225/64
```
6. Exit the interface configuration mode.

```
exit
```

This section provides an example CLI configuration to configure a loopback interface.

1. Configure a loopback interface.

```
interface Loopback 0
```

2. Set an IP address for the interface.

```
ip address 209.165.201.1 255.255.255.0
```

3. Configure an IPv6 address.

```
ipv6 address 2001:DB8:201::1/64
```

4. Exit the interface configuration mode.

```
exit
```

Here's the complete configuration example for configuring a common source interface.

```
interface GigabitEthernet5
no shutdown
ip address 209.165.202.129 255.255.255.0
ipv6 address 2001:DB8:202::129/64
exit
interface Loopback0
no shutdown
ip address 209.165.201.1 255.255.255.0
ipv6 address 2001:DB8:201::1/64
exit
```

Configure an IPv6 GRE Tunnel Over IPv4 Underlay

This section provides an example CLI configuration to configure an IPv6 GRE tunnel over IPv4 underlay.

1. Enter the global configuration mode.

```
configure terminal
```

2. Create an interface tunnel.

```
interface Tunnel64
```

3. Enable the interface.

```
no shutdown
```

4. Associate a VRF instance or a virtual network with an interface or subinterface in interface configuration mode.

```
vrf forwarding 1
```

5. Configure the IPv6 address and enable IPv6 processing on an interface in interface configuration mode.

```
ipv6 address 2001:DB8:64::1/64
```

6. Set the source address for the tunnel interface in interface configuration mode.

```
tunnel source 209.165.202.129
```

7. Set the destination address for the GRE tunnel interface in interface configuration mode.

```
tunnel destination 209.165.202.158
```

8. Specify the outgoing interface of the tunnel transport in interface configuration mode. If you use the mandatory keyword and if the route is not available, the traffic drops.

```
tunnel route-via GigabitEthernet5 mandatory
```

Here's the complete configuration example for configuring an IPv6 GRE tunnel over IPv4 underlay.

```
interface Tunnel64
no shutdown
vrf forwarding 1
ipv6 address 2001:DB8:64::1/64
tunnel source 209.165.202.129
tunnel destination 209.165.202.158
tunnel route-via GigabitEthernet5 mandatory
```

Configure an IPv6 GRE Tunnel Over IPv6 Underlay

This section provides an example CLI configuration to configure a IPv6 GRE tunnel over IPv6 underlay.

1. Enter the global configuration mode.

```
configure terminal
```

2. Enter the tunnel interface mode.

```
interface Tunnel66
```

3. Enable the interface.

```
no shutdown
```

4. Associate a VRF instance or a virtual network with an interface or subinterface in interface configuration mode.

```
vrf forwarding 1
```

5. Configure the IPv6 address and enable IPv6 processing on an interface in interface configuration mode.

```
ipv6 address 2001:DB8:166::1/64
```

6. Set the source address for the tunnel interface in interface configuration mode.

```
tunnel source 2001:DB8:15::15
```

7. Set the destination address for the GRE tunnel interface in interface configuration mode.

```
tunnel destination 2001:DB8:15::16
```

8. Set the encapsulation mode for the tunnel interface, in interface configuration mode.

```
tunnel mode gre ipv6
```

9. Specify the outgoing interface of the tunnel transport in interface configuration mode. If you use the mandatory keyword and if the route is not available, the traffic drops.

```
tunnel route-via GigabitEthernet5 mandatory
```

Here's the complete configuration example for configuring an IPv6 GRE tunnel over IPv6 underlay.

```
interface Tunnel66
no shutdown
vrf forwarding 1
ipv6 address 2001:DB8:66::1/64
tunnel source 2001:DB8:15::15
tunnel destination 2001:DB8:15::16
tunnel mode gre ipv6
tunnel route-via GigabitEthernet5 mandatory
```

Configure an IPsec IPv6 Tunnel Over IPv4 Underlay

This section provides an example CLI configuration to configure an IPsec IPv6 tunnel over IPv4 underlay.

1. Enter the global configuration mode.

```
configure terminal
```

2. Enter the tunnel interface mode.
`interface Tunnel164`
3. Enable the interface.
`no shutdown`
4. Associate a VRF instance or a virtual network with an interface or subinterface in interface configuration mode.
`vrf forwarding 1`
5. Configure the IPv6 address and enable IPv6 processing on an interface in interface configuration mode.
`ipv6 address 2001:DB8:164::1/64`
6. Set the source address for the tunnel interface in interface configuration mode.
`tunnel source 209.165.202.129`
7. Set the destination address for the IPsec tunnel interface in interface configuration mode.
`tunnel destination 209.165.202.158`
8. Set the encapsulation mode for the tunnel interface, in interface configuration mode.
`tunnel mode ipsec ipv4 v6-overlay`
9. Associate the tunnel interface with an IPsec profile.
`tunnel protection ipsec profile if-ipsec1-ipsec-profile164`
10. Specify the outgoing interface of the tunnel transport in interface configuration mode. If you use the mandatory keyword and if the route is not available, the traffic drops.
`tunnel route-via GigabitEthernet5 mandatory`

Here's the complete configuration example for configuring an IPsec IPv6 tunnel over IPv4 underlay.

```
interface Tunnel164
no shutdown
vrf forwarding 1
ipv6 address 2001:DB8:164::1/64
tunnel source 209.165.202.129
tunnel destination 209.165.202.158
tunnel mode ipsec ipv4 v6-overlay
tunnel protection ipsec profile if-ipsec1-ipsec-profile164
tunnel route-via GigabitEthernet5 mandatory
```

Configure an IPsec IPv6 Tunnel Over IPv6 Underlay

This section provides an example CLI configuration to configure an IPsec IPv6 tunnel over IPv6 underlay.

1. Enter the global configuration mode.
`configure terminal`
2. Enter the tunnel interface mode.
`interface Tunnel166`
3. Enable the interface.
`no shutdown`
4. Associate a VRF instance or a virtual network with an interface or subinterface in interface configuration mode.
`vrf forwarding 1`
5. Configure the IPv6 address and enable IPv6 processing on an interface in interface configuration mode.
`ipv6 address 2001:DB8:166::1/64`

6. Set the source address for the tunnel interface in interface configuration mode.
`tunnel source 2001:DB8:15::15`
7. Set the destination address for the IPsec tunnel interface in interface configuration mode.
`tunnel destination 2001:DB8:15::16`
8. Set the encapsulation mode for the tunnel interface, in interface configuration mode.
`tunnel mode ipsec ipv6`
9. Associate the tunnel interface with an IPsec profile.
`tunnel protection ipsec profile if-ipsec1-ipsec-profile166`
10. Specify the outgoing interface of the tunnel transport in interface configuration mode. If you use the mandatory keyword and if the route is not available, the traffic drops.
`tunnel route-via GigabitEthernet5 mandatory`

Here's the complete configuration example for configuring an IPsec IPv6 tunnel over IPv6 underlay.

```
interface Tunnel166
no shutdown
vrf forwarding 1
ipv6 address 2001:DB8:166::1/64
tunnel source 2001:DB8:15::15
tunnel destination 2001:DB8:15::16
tunnel mode ipsec ipv6
tunnel protection ipsec profile if-ipsec1-ipsec-profile166
tunnel route-via GigabitEthernet5 mandatory
```

Verify IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN Device Devices and Third-Party Devices

The following is a sample output from the show run interface type/number command.

```
show run interface tunnel 164
interface Tunnel164
no shutdown
vrf forwarding 1
ipv6 address 2001:DB8:164::1/64
tunnel source 209.165.202.129
tunnel destination 209.165.202.158
tunnel mode ipsec ipv4 v6-overlay
tunnel protection ipsec profile if-ipsec1-ipsec-profile164
tunnel route-via GigabitEthernet5 mandatory
```

The following is a sample output from the show adjacency tunnel164 internal command.

show adjacency tunnel164 internal

```

Protocol Interface
IPV6      Tunnel164
718424FDE3D8

Address
point2point(7)
0 packets, 0 bytes
epoch 0
sourced in sev-epoch 14
empty encap string
P2P-ADJ
Next chain element:
    IP adj out of GigabitEthernet5, addr 209.165.202.158


    parent oce 0x718424FDE498
    frame originated locally (Null0)
L3 mtu 1500
Flags (0x5938C4)
Fixup enabled (0x400000)
    IPsec tunnel
HWIDB/IDB pointers 0x71842EA25C50/0x71842EA30E90
IP redirect enabled
Switching vector: IPv6 midchain adjacency oce
Post encap features: IPSEC Post-encap output classification
Address
Next-hop cannot be inferred
IOSXE-RP Inject sbublock:
    pak transmitted 14
    last inject at 00:00:02 ago
IP Tunnel stack to 209.165.202.158 in Default (0x0)
nh tracking enabled: 209.165.202.158/32
route-via enabled: GigabitEthernet5 (mandatory)
IP adj out of GigabitEthernet5, addr 209.165.202.158
Platform adj-id: 0xF80001D7, 0x0, tun_qos_dpidx:0

Adjacency pointer 0x718424FDD8E8
Next-hop unknown

```



Documents / Resources

	<p>CISCO Catalyst SD-WAN Security Configuration [pdf] User Guide Catalyst SD-WAN Security Configuration, Catalyst SD-WAN, Security Configuration, Configuration</p>
---	---

References

- [Cisco Catalyst SD-WAN Security Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x - GRE Over IPsec Tunnels \[Cisco SD-WAN\] - Cisco](#)
- [Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x - CLI Templates for Cisco IOS XE Catalyst SD-WAN Devices \[Cisco SD-WAN\] - Cisco](#)
- [User Manual](#)

Manuals+. Privacy Policy

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.