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

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

Table 1: Feature History

Feature Name	Release Information	Description
IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN and Third-Party Devices Over a Service VPN	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.x	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.
IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN and Third-Party Devices Over a Transport VPN	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	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 transport VPN.

Information About 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 or (from Cisco IOS XE Catalyst SD-WAN Release 17.14.1a) a transport VPN. The following types are supported for a tunnel in a service VPN:

- IPv6 GRE tunnel over IPv4 underlay
- IPv6 GRE tunnel over IPv6 underlay
- IPsec IPv6 tunnel over IPv4 underlay
- IPsec IPv6 tunnel over IPv6 underlay

The following types are supported for a tunnel in a transport VPN:

- 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

- Configuration methods:
  - Cisco IOS XE Catalyst SD-WAN Release 17.12.1a supports configuration in a service VPN by CLI template only.
  - Cisco IOS XE Catalyst SD-WAN Release 17.14.1a supports configuration in a service VPN by feature template and configuration groups.
  - Cisco IOS XE Catalyst SD-WAN Release 17.14.1a supports configuration in a transport VPN by CLI, feature template, and configuration groups.
- Dual stack:

  Dual stack is not supported for IPsec tunnels.
- Loopback interface:

  The interface name as loopback for tunnel source is not supported in the service VPN. 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.
- NAT traversal:

  NAT traversal is not supported for IPsec tunnels with IPv6 underlay.
- In IKEv2 Preshared Keys (PSK), the '\' character is not supported and should not be used.

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 17.14.1a and later	• Cisco Catalyst 8200 Series Edge Platforms

Release	Supported Devices
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and later	• Cisco Catalyst 8200 Series Edge Platforms • 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 in a Service VPN Using a CLI Template

Before You Begin

Configure a common source interface:

1. Enter interface configuration mode.

   ```
   interface GigabitEthernet1
   ```

2. Enable the interface.

   ```
   no shutdown
   ```

3. Set an IP address for the interface.

   ```
   ip address 209.165.200.225 255.255.255.0
   ```

4. Configure an IPv6 address.

   ```
   ipv6 address 2001:DB8:200::225/64
   ```

5. Exit the interface configuration mode.

   ```
   exit
   ```

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

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

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

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

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 devices and Third-Party Devices in Service VPN

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

```
Device#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.

```
Device#show adjacency tunnel164 internal
Protocol Interface                 Address
IPV6     Tunnel164                 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
718424FDE3D8
                                     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
Protocol Interface                 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
```

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

The following sections describe procedures for configuring IPv6 GRE or IPsec tunnels over IPv4 and IPv6 overlay networks and underlay networks. Each of the tunnel configuration procedures includes as a prerequisite the procedure for configuring a common source interface.

Configure a Common Source Interface Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates. By default, CLI templates execute commands in global config mode.

1. Enter interface configuration mode.

   ```
   interface GigabitEthernet1
   ```

2. Enable the interface.

   ```
   no shutdown
   ```

3. Set an IP address for the interface.

   ```
   ip address ip-address
   ```

4. Configure an IPv6 address.

   ```
   ipv6 address ip-address mask
   ```

5. Exit the interface configuration mode.

   ```
   exit
   ```

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

```
interface GigabitEthernet1
 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 an IPv4 Overlay Using a CLI Template

Before You Begin

- For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates. By default, CLI templates execute commands in global config mode.
- Configure a common source interface. For information, see Configure a Common Source Interface Using a CLI Template.

Configure an IPv6 GRE Tunnel Over an IPv4 Overlay

1. Create an interface tunnel.

   ```
   interface Tunnel64
   ```

2. Enable the interface.

   ```
   no shutdown
   ```

3. Configure the IPv6 address and enable IPv6 processing on an interface.

   ```
   ipv6 address ip-address
   ```

4. Set the source address for the tunnel interface.

   ```
   tunnel source tunnel-source-address
   ```

5. Set the destination address for the GRE tunnel interface.

   ```
   tunnel destination tunnel-destination-address
   ```

6. Specify the outgoing interface of the tunnel transport. If you use the **mandatory** keyword and if the route is not available, the traffic drops.

   ```
   tunnel [route-via] GigabitEthernet-interface mandatory
   ```

7. Enable VRF multiplexing.

   ```
   tunnel vrf multiplexing
   ```

8. Enable tunnel protection.

   ```
   tunnel protection ipsec profile if-ipsec1-ipsec-profile64
   ```

Here's the complete configuration example for configuring an IPv6 GRE tunnel over an 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 GigabitEthernet1 mandatory
 tunnel vrf multiplexing
```

```
 tunnel protection ipsec profile if-ipsec1-ipsec-profile64
exit
```

Configure an IPv6 GRE Tunnel Over an IPv6 Overlay Using a CLI Template

Before You Begin

- For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates. By default, CLI templates execute commands in global config mode.
- Configure a common source interface. For information, see Configure a Common Source Interface Using a CLI Template.

Configure an IPv6 GRE Tunnel Over an IPv6 Overlay

1. Enter the tunnel interface mode.

   ```
   interface Tunnel66
   ```

2. Enable the interface.

   ```
   no shutdown
   ```

3. Configure the IPv6 address and enable IPv6 processing on an interface.

   ```
   ipv6 address ipv6-address
   ```

4. Set the source address for the tunnel interface.

   ```
   tunnel source tunnel-source-address
   ```

5. Set the destination address for the GRE tunnel interface.

   ```
   tunnel destination tunnel-destination-address
   ```

6. Set the encapsulation mode for the tunnel interface.

   ```
   tunnel mode gre ipv6
   ```

7. Specify the outgoing interface of the tunnel transport. If you use the **mandatory** keyword and if the route is not available, the traffic drops.

   ```
   tunnel route-via GigabitEthernet-interface mandatory
   ```

8. Enable VRF multiplexing.

   ```
   tunnel vrf multiplexing
   ```

9. Enable tunnel protection.

   ```
   tunnel protection ipsec profile if-ipsec1-ipsec-profile66
   ```

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

```
interface Tunnel66
 no shutdown
  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 GigabitEthernet1 mandatory
  tunnel vrf multiplexing
```

```
tunnel protection ipsec profile if-ipsec1-ipsec-profile66
exit
```

Configure an IPsec IPv6 Tunnel Over an IPv4 Underlay Using a CLI Template

Before You Begin

- For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates. By default, CLI templates execute commands in global config mode.
- Configure a common source interface. For information, see Configure a Common Source Interface Using a CLI Template.

Configure an IPsec IPv6 Tunnel Over an IPv4 Underlay

1. Enter the tunnel interface mode.

   ```
   interface Tunnel164
   ```

2. Enable the interface.

   ```
   no shutdown
   ```

3. Configure the IPv6 address and enable IPv6 processing on an interface.

   ```
   ipv6 address ipv6-address
   ```

4. Set the source address for the tunnel interface.

   ```
   tunnel source tunnel-source-address
   ```

5. Set the destination address for the IPsec tunnel interface.

   ```
   tunnel destination tunnel-destination-address
   ```

6. Set the encapsulation mode for the tunnel interface.

   ```
   tunnel mode ipsec ipv4 v6-overlay
   ```

7. Specify the outgoing interface of the tunnel transport. If you use the **mandatory** keyword and if the route is not available, the traffic drops.

   ```
   tunnel route-via GigabitEthernet-interface mandatory
   ```

8. Enable VRF multiplexing.

   ```
   tunnel vrf multiplexing
   ```

9. Associate the tunnel interface with an IPsec profile.

   ```
   tunnel protection ipsec profile if-ipsec1-ipsec-profile164
   ```

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

```
interface Tunnel164
no shutdown
 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 route-via GigabitEthernet1 mandatory
 tunnel vrf multiplexing
```

```
 tunnel protection ipsec profile if-ipsec1-ipsec-profile164
exit
```

Configure an IPsec IPv6 Tunnel Over an IPv6 Underlay Using a CLI Template

Before You Begin

- For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates. By default, CLI templates execute commands in global config mode.
- Configure a common source interface. For information, see Configure a Common Source Interface Using a CLI Template.

Configure an IPsec IPv6 Tunnel Over an IPv6 Underlay

1. Enter the tunnel interface mode.

   ```
   interface Tunnel166
   ```

2. Enable the interface.

   ```
   no shutdown
   ```

3. Configure the IPv6 address and enable IPv6 processing on an interface.

   ```
   ipv6 address ipv6-address
   ```

4. Set the source address for the tunnel interface.

   ```
   tunnel source tunnel-source-address
   ```

5. Set the destination address for the IPsec tunnel interface.

   ```
   tunnel destination tunnel-destination-address
   ```

6. Set the encapsulation mode for the tunnel interface.

   ```
   tunnel mode ipsec ipv6
   ```

7. Specify the outgoing interface of the tunnel transport. If you use the **mandatory** keyword and if the route is not available, the traffic drops.

   ```
   tunnel route-via GigabitEthernet-interface mandatory
   ```

8. Enable VRF multiplexing.

   ```
   tunnel vrf multiplexing
   ```

9. Associate the tunnel interface with an IPsec profile.

   ```
   tunnel protection ipsec profile if-ipsec1-ipsec-profile166
   ```

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

```
interface Tunnel166
no shutdown
 ipv6 address 2001:DB8:166::1/64
 tunnel source 2001:DB8:15::15
 tunnel destination 2001:DB8:15::16
 tunnel mode ipsec ipv6
 tunnel route-via GigabitEthernet1 mandatory
 tunnel vrf multiplexing
 tunnel protection ipsec profile if-ipsec1-ipsec-profile166
```

```
exit
```

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

Verify GRE Tunnel Protection

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

```
Device#show run interface tunnel 64
interface Tunnel64
 no ip address
 ipv6 address 2001:DB8:64::1/64
 tunnel source 209.165.202.129
 tunnel destination 209.165.202.158
 tunnel route-via GigabitEthernet1 mandatory
 tunnel vrf multiplexing
 tunnel protection ipsec profile if-ipsec-ipsec-profile64
end
```

The following is a sample output from the **show adjacency tunnel64 internal** command for a GRE tunnel.

```
Device#show adjacency tunnel64 internal
Protocol Interface                 Address
IPV6     Tunnel64                  point2point(11)
                                   14 packets, 1368 bytes
                                   epoch 0
                                   sourced in sev-epoch 1
                                   Encap length 24
                                   4500000000000000FF2F8363D1A5CA81
                                   D1A5CA9E000086DD
                                   P2P-ADJ
                                   Next chain element:
                                     IP adj out of GigabitEthernet1, addr 209.165.202.158
747CC8F3DD80
                                     parent oce 0x747CC8F3DE40
                                     frame originated locally (Null0)
                                   Fast adjacency enabled [OK]
                                   L3 mtu 1398
                                   Flags (0x5938CC)
                                   Fixup enabled (0x2)
                                         IP tunnel
                                   HWIDB/IDB pointers 0x747C5C618E90/0x747CC7B88190
                                   IP redirect enabled
Protocol Interface                 Address
                                   Switching vector: IPv6 midchain adjacency oce
                                Post encap features: IPSEC Post-encap output classification

                                   Next-hop cannot be inferred
                                   IOSXE-RP Inject sbublock:
                                     pak transmitted 14
                                     last inject at 00:00:44 ago
                                   IP Tunnel stack to 209.165.202.158 in Default (0x0)
                                    nh tracking enabled: 209.165.202.158/32
                                    route-via enabled: GigabitEthernet1 (mandatory)
                                    IP adj out of GigabitEthernet1, addr 209.165.202.158
                                   Platform adj-id: 0xF8000137, 0x0, tun_qos_dpidx:0
                                   Adjacency pointer 0x747CC8F3E870
                                   Next-hop unknown
```

The following is a sample output from the **show platform hardware qfp active feature tunnel datapath vrf-multiplexing ipv6 host** command.

```
Device#show platform hardware qfp active feature tunnel datapath vrf-multiplexing ipv6 host

VRF_IDX VRF_NAME Tbl_ID      Host_IP
   Flags   Tun_idx IFNAME         Tx_Pkts   Rx_Pkts
-------------------------------------------------------------------------------------------
3       1        503316481   2001::3800:102
   0x1     65519   Tunnel64            29         29
```

Verify IPsec Tunnel

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

```
Device#show run interface tunnel164
interface Tunnel164
 no ip address
 ipv6 address 2001:DB8:164::1/64
 tunnel source 209.165.202.129
 tunnel mode ipsec ipv4 v6-overlay
 tunnel destination 209.165.202.158
 tunnel route-via GigabitEthernet1 mandatory
 tunnel vrf multiplexing
 tunnel protection ipsec profile if-ipsec-ipsec-profile164
end
```

The following is a sample output from the **show adjacency tunnel164 internal** command for an IPsec tunnel.

```
Device#show adjacency tunnel164 internal
Protocol Interface                 Address
IPV6     Tunnel164                 point2point(11)
                                   14 packets, 1032 bytes
                                   epoch 0
                                   sourced in sev-epoch 3
                                   empty encap string
                                   P2P-ADJ
                                   Next chain element:
                                     IP adj out of GigabitEthernet1, addr 209.165.202.158
747CC8F3DD80
                                     parent oce 0x747CC8F3DE40
                                     frame originated locally (Null0)
                                   L3 mtu 1422
                                   Flags (0x5938C4)
                                   Fixup enabled (0x400000)
                                         IPSec tunnel
                                   HWIDB/IDB pointers 0x747CC265CEE0/0x747CC923AA98
                                   IP redirect enabled
                                   Switching vector: IPv6 midchain adjacency oce
                                Post encap features: IPSEC Post-encap output classification
Protocol Interface                 Address
                                   Next-hop cannot be inferred
                                   IOSXE-RP Inject sbublock:
                                     pak transmitted 14
                                     last inject at 00:01:32 ago
                                   IP Tunnel stack to 209.165.202.158 in Default (0x0)
                                    nh tracking enabled: 209.165.202.158/32
                                    route-via enabled: GigabitEthernet1 (mandatory)
                                    IP adj out of GigabitEthernet1, addr 209.165.202.158
                                   Platform adj-id: 0xF8000157, 0x0, tun_qos_dpidx:0
```

```
                                    Adjacency pointer 0x747CC91D9208
                                    Next-hop unknown
```

The following is a sample output from the **show platform hardware qfp active feature tunnel datapath vrf-multiplexing ipv6 host** command for an IPsec tunnel.

```
Device#show platform hardware qfp active feature tunnel datapath vrf-multiplexing ipv6 host

VRF_IDX VRF_NAME Tbl_ID      Host_IP
   Flags    Tun_idx IFNAME         Tx_Pkts   Rx_Pkts
------------------------------------------------------------------------------------------------------------------------

3       1        503316481   2001::3800:102
   0x1      65517   Tunnel164            1         1
```

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

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, you can configure an IPv6 GRE or IPsec tunnel between Cisco IOS XE Catalyst SD-WAN devices and third-party devices in a service or transport VPN using a feature template.

The following sections describe the process of configuring the IPv6 GRE or IPsec tunnels between Cisco IOS XE Catalyst SD-WAN devices and third-party devices using a feature template.

Cisco VPN Interface GRE

Before you configure the GRE parameters, create the Cisco VPN Interface GRE template. To create the template using Cisco SD-WAN Manager feature templates, see "Navigate to the Template Screen and Name the Template" in Cisco VPN Interface GRE.

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, configure the following parameters:

Table 3: Basic Configuration

Field	Description
Shutdown*	Click **Off** to enable the interface.
Interface Name*	Enter the name of the GRE interface. Range: 1 through 255
Description	Enter a description of the GRE interface.
GRE Tunnel Mode	Choose from one of the following GRE tunnel modes: • **ipv4 underlay**: GRE tunnel with IPv4 underlay. IPv4 underlay is the default value. • **ipv6 underlay**: GRE tunnel with IPv6 underlay.
IPv4 Address	Enter an IPv4 address for the GRE tunnel.

Field	Description
IPv6 Address	Enter an IPv6 address for the GRE tunnel.
Source*	Enter the source of the GRE interface: • **IP Address**: Enter the source IP address of the GRE tunnel interface. This address is on the local router. • **Tunnel Route-via Interface**: Enter the physical interface name to steer the GRE traffic through. • **Interface**: Enter the name of the source interface. • **Tunnel Source Interface**: Enter the physical interface that is the source of the GRE tunnel.
Destination*	Enter the destination IP address of the GRE tunnel interface. This address is on a remote device. If this tunnel connects to a Secure Internet Gateway (SIG), specify the URL for the SIG.
GRE Destination IP Address*	Enter the destination IP address of the GRE tunnel interface. This address is on a remote device.
Multiplexing	Choose **Yes** to enable multiplexing, in case of a tunnel in the transport VPN. Default: No
IP MTU	Specify the maximum MTU size of the IPv4 packets on the interface. Range: 576 through 1804 Default: 1500 bytes
Clear-ike mode-Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.
IPv6 MTU	Specify the maximum MTU size of the IPv6 packets on the interface. Range: 1280 to 9976 bytes Default: 1500 bytes
IPv6 TCP MSS	Specify the maximum segment size (MSS) of IPv6 TPC SYN packets passing through the Cisco IOS XE Catalyst SD-WAN device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 40 to 1454 bytes Default: None

Table 4: DPD

Field	Description
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 through 3600 seconds (1 hour) Default: 10 seconds
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then removing the tunnel to the peer. Range: 2 through 60 Default: 3

Table 5: IKE

Field	Description
IKE Version	Enter 1 to choose IKEv1. Enter 2 to choose IKEv2. Default: IKEv1
IKE Mode	Choose one of the following modes for the exchange of keying information and setting up IKE security associations: • **Main**: Establishes an IKE SA session before starting IPsec negotiations. • **Aggressive**: Negotiation is quicker, and the initiator and responder ID pass in the clear. Aggressive mode does not provide identity protection for communicating parties. Default: Main mode
IKE Rekey Interval (Seconds)	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 14400 seconds (4 hours)
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Values: aes128-cbc-sha1, aes128-cbc-sha2, aes256-cbc-sha1, aes256-cbc-sha2 Default: aes256-cbc-sha1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchanges. Values: 2, 14, 15, 16, 19, 20, 21, 24 Default: 16
IKE Authentication	**Preshared Key**: Enter the preshared key (PSK) for authentication.

Field	Description
IKE ID for Local End Point	If the remote IKE peer requires a local endpoint identifier, specify it. Range: 1 through 64 characters Default: Source IP address of the tunnel
IKE ID for Remote End Point	If the remote IKE peer requires a remote end point identifier, specify it. Range: 1 through 64 characters Default: Destination IP address of the tunnel There is no default option if you have chosen IKEv2.

Table 6: IPsec

Field	Description
IPsec Rekey Interval (Seconds)	Specify the interval for refreshing IKE keys. Range: 3600 through 1209600 seconds (1 hour through 14 days) Default: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 bytes Default: 512 bytes
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Values: **aes256-cbc-sha1**, **aes256-gcm**, **null-sha1** Default: **aes256-gcm**
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel by choosing one of the following values: • **group-2**: Use the 1024-bit Diffie-Hellman prime modulus group • **group-14**: Use the 2048-bit Diffie-Hellman prime modulus group • **group-15**: Use the 3072-bit Diffie-Hellman prime modulus group • **group-16**: Use the 4096-bit Diffie-Hellman prime modulus group • **none**: Disable PFS Default: **group-16**

Table 7: ACL

Field	Description
Rewrite Rule	Click **On** and specify the name of the rewrite rule to apply on the interface.

Field	Description
Ingress ACL – IPv4	Click **On** and specify the name of the access list to apply to IPv4 packets being received on the interface.
Egress ACL – IPv4	Click **On** and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.

Table 8: ADVANCED

Field	Description
Tracker	Enter the name of a tracker to track the status of GRE interfaces that connect to the internet.
Application	Specify that this tunnel connects to a SIG.
Tunnel Protection	Choose **Yes** to enable tunnel protection. Default: No

Cisco VPN Interface IPsec

Before you configure the IPsec parameters, create the Cisco VPN Interface IPsec template. To create the template using Cisco SD-WAN Manager feature templates, see Create VPN IPsec Interface Template.

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, configure the parameters in the following section.

Table 9: Basic Configuration

Field	Options/Format	Description
Shutdown*	**Yes** / **No**	Click **No** to enable the interface; click **Yes** to disable.
Interface Name*	**ipsec** *number* (1…255)	Enter the name of the IPsec interface. *Number* can be from 1 through 255.
Description	Enter a description of the IPsec interface.	
IPsec Tunnel Mode	Choose from one of the following IPsec tunnel modes: • **4o4**: IPsec tunnel with IPv4 overlay and IPv4 underlay. • **6o4**: IPsec tunnel with IPv6 overlay and IPv4 underlay. • **6o6**: IPsec tunnel with IPv6 overlay and IPv6 underlay.	
IPv4 Address*	*ipv4 prefix/length*	Enter the IPv4 address of the IPsec interface.

Field	Options/Format	Description
Source *	Set the source of the IPsec tunnel that is being used for IKE key exchange:	
	IP Address	Based on the option you chose from the **IPsec Tunnel Mode** option, enter the IPv4 or IPv6 address for the overlay tunnel. Configure this address in **VPN 0**.
	Interface	Click and enter the name of the physical interface that is the source of the IPsec tunnel. Configure this interface in **VPN 0**. • If you selected the Source as **Interface**, enter the name of the source interface. If you enter a loopback interface, an additional field **Tunnel Route-via Interface** displays where you enter the egress interface name.

Field	Options/Format	Description
Destination*	Set the destination of the IPsec tunnel that is being used for IKE key exchange.	
	IPsec Destination IP Address/FQDN	Enter an IPv4 or IPv6 address that points to the destination.
	TCP MSS	Based on the IPv4 or IPv6 option you chose from the **IPsec Tunnel Mode** option, enter the maximum segment size (MSS) of the TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range for IPv4 TCP MSS: 500 to 1460 bytes Range for IPv6 TCP MSS: 40 to 1454 bytes Default: None
	Multiplexing	Choose **Yes** to enable multiplexing, in case of a tunnel in the transport mode. Default: No
	IP MTU	Based on the option you chose from the **IPsec Tunnel Mode** option, enter the maximum transmission unit (MTU) size of the IPv4 MTU or IPv6 MTU packets on the interface. Range for IPv4 MTU: 68 through 9914 bytes Range for IPv6 MTU: 1280 to 9976 bytes Default: 1500 bytes
	Clear-Dont-Fragment	Configure **Clear-Dont-Fragment** for packets that arrive at an interface that has Don't Fragment configured. If these packets are larger than what MTU allows, they are dropped. If you clear the Don't Fragment bit, the packets are fragmented and sent. Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out of the interface. When the Don't Fragment bit is cleared, packets larger than the MTU of the interface are fragmented before being sent. **Note** **Clear-Dont-Fragment** clears the Don't Fragment bit and the Don't Fragment bit is set. For packets not requiring fragmentation, the Don't Fragment bit is not affected.

Table 10: DPD

Field	Description
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 through 3600 seconds Default: Disabled
DPD Retries	Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then tearing down the tunnel to the peer. Range: 2 through 60 Default: 3

Table 11: IKE

Field	Description
IKE Version	Enter **1** to choose IKEv1. Enter **2** to choose IKEv2. Default: IKEv1
IKE Mode	For IKEv1 only, specify one of the following modes: • Aggressive mode: Negotiation is quicker, and the initiator and responder ID pass in the clear. • Main mode: Establishes an IKE SA session before starting IPsec negotiations. **Note** For IKEv2, there is no mode. **Note** We do not recommend using IKE aggressive mode with pre-shared keys. If it is necessary to use this mode, use a strong pre-shared key. Default: Main mode
IPsec Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 to 1209600 seconds (1 hour to 14 days) Default: 14400 seconds (4 hours)
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Default: 256-AES

Field	Description
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. • 1024-bit modulus • 2048-bit modulus • 3072-bit modulus • 4096-bit modulus Default: 4096-bit modulus
IKE Authentication	Enter the password to use with the preshared key.
	If the remote IKE peer requires a local end point identifier, specify it. Range: 1 through 64 characters Default: Tunnel's source IP address
	If the remote IKE peer requires a remote end point identifier, specify it. Range: 1 through 64 characters Default: Tunnel destination IP address

Table 12: IPsec

Parameter Name	Options	Description
IPsec Rekey Interval	3600 to 1209600 seconds	Specify the interval for refreshing IKE keys. Range: 1 hour through 14 days Default: 3600 seconds
IKE Replay Window	64, 128, 256, 512, 1024, 2048, 4096, 8192	Specify the replay window size for the IPsec tunnel. Default: 512
IPsec Cipher Suite	aes256-cbc-sha1 aes256-gcm null-sha1	Specify the authentication and encryption to use on the IPsec tunnel Default: aes256-gcm

Parameter Name	Options	Description
Perfect Forward Secrecy	**2** 1024-bit modulus **14** 2048-bit modulus **15** 3072-bit modulus **16** 4096-bit modulus **none**	Specify the PFS settings to use on the IPsec tunnel. From the drop-down list, choose one of the following Diffie-Hellman prime modulus groups: • 1024-bit – group-2 • 2048-bit – group-14 • 3072-bit – group-15 • 4096-bit – group-16 • none – disable PFS Default: group-16

Table 13: Advanced

Parameter Name	Description
Tracker	Tracking the interface status is useful when you enable NAT on a transport interface in VPN 0 to allow data traffic from the router to exit directly to the internet.
Application	Specify that this tunnel connects to a SIG.

Configure IPv6 GRE or IPsec Tunnel Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices in a Service VPN Using Configuration Groups

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, you can configure an IPv6 GRE tunnel between Cisco IOS XE Catalyst SD-WAN devices and third-party devices in a service VPN using configuration groups.

Before You Begin

Add the GRE or IPsec subfeature:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **…** adjacent to a configuration group name and choose **Edit**.
3. Click **Service Profile** to open it.
4. Click **…** adjacent to the **VPN** feature and choose **Add Sub-Feature**.
5. From the drop-down list, choose **GRE** or **IPsec**.
6. In the **Name** field, enter a name for the feature.
7. In the **Description** field, enter a description of the feature.

8. Configure the options described in the following section, as needed, and click **Save**.

After adding the subfeature, see the following sections to configure the IPv6 GRE or IPsec parameters for tunnels between Cisco IOS XE Catalyst SD-WAN devices and third-party devices using a feature template.

GRE

To configure the GRE parameters for a service VPN, see the GRE section in Service Profile.

IPsec

To configure the IPsec parameters for a service VPN, see the IPsec section in Service Profile.

Configure IPv6 IPsec Tunnel Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices in a Transport VPN Using Configuration Groups

Before You Begin

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, you can configure an IPv6 IPsec tunnel between Cisco IOS XE Catalyst SD-WAN devices and third-party devices in a transport VPN using configuration groups.

Configure IPv6 IPsec Tunnel Between Cisco IOS XE Catalyst SD-WAN Devices and Third-Party Devices in a Transport VPN

1. Add the GRE or IPsec subfeature.
    a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
    b. Click **…** adjacent to a configuration group name and choose **Edit**.
    c. Click **Transport & Management Profile** to open it.
    d. Click **…** adjacent to the **VPN0** feature and choose **Add Sub-Feature**.
    e. From the drop-down list, choose **GRE** or **IPsec**.
2. In the **Name** field, enter a name for the feature.
3. In the **Description** field, enter a description of the feature.
4. Configure the GRE or IPsec parameters as follows:
    - GRE: To configure the GRE parameters for a transport VPN, see the GRE section in Transport and Management Profile.
    - IPsec: To configure the IPsec parameters for a transport VPN, see the IPsec section in Transport and Management Profile.
5. Click **Save**.