VPN Interface GRE

Configure VPN interface GRE

Use one of these methods to configure VPN interface GRE:

- Configuration group
- Feature template

Note Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

Configure VPN interface GRE on transport VPN using a configuration group

Follow these steps to configure VPN interface GRE on transport VPN using a configuration group.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure the GRE feature.

a) Configure GRE parameters.

Table 1: Basic Configuration

Field	Description
Interface Name (1..255)*	Enter the name of the GRE interface. Range: 1 through 255.
Interface Description	Enter a description of the GRE interface.
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.
Multiplexing	Choose **Yes** to enable multiplexing, in case of a tunnel in the transport VPN. Default: No
Preshared Key for IKE	Enter the preshared key (PSK) for authentication.

b) Configure Tunnel fields.

Table 2: Tunnel

Field	Description
Source	Enter the source of the GRE interface: • **IP Address**: Enter the source IP address of the GRE tunnel interface. Based on the option you selected in the **Tunnel Mode** drop-down list, enter an IPv4 or an IPv6 address. This address is on the local router. • **Interface**: Enter the egress interface name for the GRE tunnel. • **Tunnel Route Via***: Specify the tunnel route details to steer the GRE tunnel traffic through. **Note** If the Tunnel Source Interface type is a loopback interface, enter the interface for traffic to be routed to. You cannot use the tunnel route via option to configure IPSec tunnels on a cellular interface because cellular interfaces do not include a next hop IP address for the default route.
Destination	Enter the source of the GRE interface: • **GRE Destination IP Address***: Enter the destination IP address of the GRE tunnel interface. This address is on a remote device. • **IP Address**: Based on the option you selected in the **Tunnel Mode** drop-down list, enter an IPv4 or an IPv6 address for the GRE tunnel. • **Mask***: Enter the subnet mask. • **IPv6 Address**: Enter the destination IPv6 or address for the GRE tunnel.

c) Configure IKE fields.

Table 3: IKE

Field	Description
IKE Version	Enter 1 to choose IKEv1. Enter 2 to choose IKEv2. Default: IKEv1
IKE Integrity Protocol	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	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 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.

d) Configure IPSEC fields.

Table 4: IPSEC

Field	Description
IPsec Rekey Interval	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**
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
Application	Choose an application from the drop-down list: • None • Sig

e) Configure advanced fields.

Table 5: Advanced

Field	Description
Shutdown	Click **Off** to enable the interface.
IP MTU	Based on your choice in the **Tunnel Mode** option, specify the maximum MTU size of the IPv6 packets on the interface. Range: 576 through 9216 Default: 1500 bytes
TCP MSS	Based on your choice in the **Tunnel Mode** option, specify the maximum segment size (MSS) of 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: 552 through 1460 bytes Default: None
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.
Tunnel Protection	Choose **Yes** to enable tunnel protection. Default: No

What to do next

Also see Deploy a configuration group.

Configure GRE on service VPN using a configuration group

Follow these steps to configure GRE on service VPN using a configuration group.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure GRE in Service Profile.

a) Configure Basic Configuration fields.

Table 6: Basic Configuration

Field	Description
Interface Name (1..255)*	Enter the name of the GRE interface, in the format **grenumber**. The value for **number** can be from 1 through 255.
Interface Description	Enter a description of the GRE interface.
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.
Preshared Key for IKE	Enter the preshared key (PSK) for authentication.

b) Configure Tunnel Fields.

Table 7: Tunnel

Field	Description
Source	Enter the source of the GRE interface: • **IP Address**: Enter the source IP address of the GRE tunnel interface. Based on the option you selected in the **Tunnel Mode** drop-down list, enter an IPv4 or an IPv6 address. This address is on the local router. • **Interface**: Enter the egress interface name for the GRE tunnel. • **Tunnel Route Via***: Specify the tunnel route details to steer the GRE tunnel traffic through. **Note** If the Tunnel Source Interface type is a loopback interface, enter the interface for traffic to be routed to. You cannot use the tunnel route via option to configure IPSec tunnels on a cellular interface because cellular interfaces do not include a next hop IP address for the default route.
Destination	Enter the source of the GRE interface: • **GRE Destination IP Address***: Enter the destination IP address of the GRE tunnel interface. This address is on a remote device. • **IP Address**: Based on the option you selected in the **Tunnel Mode** drop-down list, enter an IPv4 or an IPv6 address for the GRE tunnel. • **Mask***: Enter the subnet mask. • **IPv6 Address**: Enter the destination IPv6 or address for the GRE tunnel.

c) Configure IKE fields.

Table 8: IKE

Field	Description
IKE Version	Enter 1 to choose IKEv1. Enter 2 to choose IKEv2. Default: IKEv1
IKE Integrity Protocol	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	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 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.

d) Configure IPSEC fields.

Table 9: 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**
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
Application	Choose an application from the drop-down list: • None • Sig

e) Configure advanced fields.

Table 10: Advanced

Field	Description
Shutdown	Click **Off** to enable the interface.
IP MTU	Based on your choice in the **Tunnel Mode** option, specify the maximum MTU size of the IPv4 or IPv6 packets on the interface. Range: 576 through 9216 Default: 1500 bytes
TCP MSS	Specify the maximum segment size (MSS) of the IPv4 TPC SYN packets passing through the Cisco vEdge device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
IPv6 TCP MSS	Specify the maximum segment size (MSS) of the IPv6 TPC SYN packets passing through the Cisco vEdge device. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 through 1460 bytes Default: None
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.
Tunnel Protection	Choose **Yes** to enable tunnel protection. Default: No

What to do next

Also see Deploy a configuration group.

Configure VPN Interface GRE using templates

Follow these steps to configure VPN interface GRE using a feature template.

To configure GRE interfaces using Cisco SD-WAN Manager templates:

1. Create a Cisco VPN Interface GRE feature template to configure a GRE interface.
2. Create a Cisco VPN feature template to advertise a service that is reachable via a GRE tunnel, to configure GRE-specific static routes, and to configure other VPN parameters.
3. Create a data policy on the Cisco SD-WAN Controller that applies to the service VPN, including a **set-service** *service-name* **local** command.

When a service, such as a firewall, is available on a device that supports only GRE tunnels, you can configure a GRE tunnel on the device to connect to the remote device by configuring a logical GRE interface. You then advertise that the service is available via a GRE tunnel, and you can create data policies to direct the appropriate traffic to the tunnel. GRE interfaces come up as soon as they are configured, and they stay up as long as the physical tunnel interface is up.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**.

In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

Step 3 From the **Create Template** drop-down list, select **From Feature Template**.

a) From the **Device Model** drop-down list, select the type of device for which you are creating the template.
b) Click **Transport & Management VPN** or scroll to the **Transport & Management VPN** section.
c) Under **Additional VPN 0 Templates**, click **VPN Interface GRE**.
d) From the **VPN Interface GRE** drop-down list, click **Create Template**. The VPN Interface GRE template form is displayed.
e) In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
f) In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 4 Configure the following VPN interface GRE parameters:

a) Configure a basic GRE interface.

Table 11:

Parameter Name	Description
Shutdown*	Click **Off** to enable the interface.
Interface Name*	Enter the name of the GRE interface, in the format **gre** *number*. *number* can be from 1 through 255.
Description	Enter a description of the GRE interface.
Source*	Enter the source of the GRE interface: • GRE Source IP Address—Enter the source IP address of the GRE tunnel interface. This address is on the local router. This address is on the local router. GRE keepalives can not be configured when source configured as IP address. • Tunnel Source Interface—Enter the physical interface that is the source of the GRE tunnel. GRE keepalives can not be configured when source configured as loopback interface. • 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.

Parameter Name	Description
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
IPv4 Address	Enter an IPv4 address for the GRE tunnel.
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500 bytes
Clear-Dont-Fragment	Click **On** to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface.
TCP MSS	Specify the maximum segment size (MSS) of 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: 552 to 1460 bytes Default: None

b) Configure access lists on a GRE interface.

Table 12:

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

c) Configure a tracker interface to track the status of a GRE interface.

Table 13:

Parameter Name	Description
Tracker	Enter the name of a tracker to track the status of GRE interfaces that connect to the Internet.