
VPN-Interface-GRE

You can use the VPN-Interface-GRE template for all vEdge Cloud and vEdge router devices.

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 vEdge router 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 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.

To configure GRE interfaces using vManage templates:

1. Create a VPN-Interface-GRE feature template to configure a GRE interface, as described in this article.
2. Create a 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. See the Configuration ► Templates ► [VPN](#) help topic.
3. Create a device template that incorporates the VPN-Interface-GRE feature template and the VPN feature template. See the Configuration ► [Templates](#) help topic.
4. Create a data policy on the vSmart controller that applies to the service VPN, including a **set service service-name local** command. See the [Configuring Centralized Data Policy](#) article for your software release.
5. Activate the vSmart policy. See the Configuration ► Templates ► [Policy](#) help topic.

Navigate to the Template Screen

1. In vManage NMS, select the Configuration ► Templates screen.
2. From the Templates title bar, select Feature.
3. Click Add Template.
4. In the left pane, select one or more devices. The right pane displays the available templates for the selected devices.
5. Select the VPN-Interface-GRE template.

The right pane displays the VPN-Interface-GRE template form.

- The top of the form contains fields for naming the template.
- The bottom contains fields for defining parameters applicable to that template.
- A drop-down menu to the left of each parameter field defines the scope of the parameter. When you first open a feature template form, for each parameter that has a default value, the scope is set to Default. To edit a parameter field, change the scope to Global or Device Specific. Note that if a parameter's scope is Device Specific, you cannot enter a value for it in the feature template. Instead, you enter a value when you attach the template to a device.
- A plus sign (+) is displayed to the right when you can add multiple entries for the same parameter.



Minimum GRE Interface Configuration

The following parameters are required (unless otherwise indicated) to configure a GRE interface on a vEdge router:

Step	Parameter Field	Procedure
1.	Template Name	Enter a name for the template. It can be up to 128 characters and can contain only alphanumeric characters.
2.	Description (Template)	Enter a description for the template. It can be up to 2048 characters and can contain only alphanumeric characters.
3.	Shutdown	Click Off to enable the interface.
4.	GRE Source IP Address	Enter the source IP address of the GRE tunnel interface. This address is on the local router.
5.	GRE Destination IP Address	Enter the destination IP address of the GRE tunnel interface. This address is on a remote device
6.	Interface name	Enter the name of the GRE interface, in the format gre <i>number</i> . <i>number</i> can be from 1 through 255.
7.	Save	Click Save to save the feature template.

CLI equivalent:

```
vpn vpn-id
interface grenumber
[no] shutdown
tunnel-destination ip-address
tunnel-source ip-address
```

Configure Other Interface Properties

To configure other GRE interface properties:

Parameter Name	Description
Description (Interface)	Enter a description of the GRE interface.
IPv4 Address	Enter an IP address for the GRE tunnel itself.
Interval	Specify how often the GRE interface sends keepalive packets on the GRE tunnel. Because GRE tunnels are stateless, sending of keepalive packets is the only way to determine whether the remote end of the tunnel is up. The keepalive packets are looped back to the sender. Receipt of these packets by the sender indicates that the remote end of the GRE tunnel is up. <i>Range:</i> 0 through 65535 seconds <i>Default:</i> 10 seconds



Parameter Name	Description
Retries	Specify how many times the GRE interface tries to resend keepalive packets before declaring the remote end of the GRE tunnel to be down. <i>Range:</i> 0 through 255 <i>Default:</i> 3
IP MTU	Specify the maximum MTU size of packets on the interface. <i>Range:</i> 576 through 1804 <i>Default:</i> 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 TCP SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. <i>Range:</i> 552 to 1460 bytes <i>Default:</i> None
Rewrite rule	Click On, and specify the name of the rewrite rule to apply on the interface.
Ingress ACL	Click On, and specify the name of the access list to apply to packets being received on the interface.
Egress ACL	Click On, and specify the name of the access list to apply to packets being transmitted on the interface.
Ingress policer	Click On, and specify the name of the policer to apply to packets being received on the interface.
Egress policer	Click On, and specify the name of the policer to apply to packets being transmitted on the interface.

CLI equivalent:

```

vpn vpn-id
interface grenumber
  access-list acl-list (in | out)
  clear-dont-fragment
  description text
  mtu bytes
  policer policer-name (in | out)
  qos-map name
  rewrite-rule name
  shaping-rate name
  tcp-mss-adjust bytes

```

Release Information

Introduced in vManage NMS Release 15.4.1.

