Integrate Your Devices With Secure Internet Gateways

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	Release Information	Description
IPSEC/GRE Tunnel Routing and Load-Balancing Using ECMP	Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	This feature allows you to use the SIG template to steer application traffic to Cisco Umbrella or a Third party SIG Provider. The application traffic is steered to a SIG based on a defined data policy and other match criteria. This feature also allows you to configure weights for multiple GRE/IPSEC tunnels for distribution of traffic among multiple tunnels. The traffic distribution enables you to balance the load among the tunnels. You can also configure the weights to achieve Equal-cost multi-path (ECMP) routing.

Feature	Release Information	Description
Enable Layer 7 Health Check (Automatic Tunnels)	Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	This features integrates the Layer 7 Health Check feature with automatic tunnels to SIGs. When you create automatic IPsec tunnels using the Cisco Secure Internet Gateway (SIG) template to Zscaler or Cisco Umbrella, a tracker is also created to monitor and load balance or failover tunnels. You can customize the parameters based on which the tracker load balances or fails over tunnels.
Support for Zscaler Automatic IPSec Tunnel Provisioning	Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	This feature automates the provisioning of tunnels from Cisco Catalyst SD-WAN routers to Zscaler. Using your Zscaler partner API credentials, you can automatically provisions tunnels to Zscaler Internet Access (ZIA) Public Service Edges. You can choose **Zscaler** in the Cisco Security Internet Gateway (SIG) and SIG credentials feature templates to automate tunnel provisioning.
Layer 7 Health Check for Manual Tunnels	Cisco SD-WAN Release 20.8.1 Cisco vManage Release 20.8.1	You can create and attach trackers to manually created GRE or IPSec tunnels to a SIG endpoint. Trackers help failover traffic when a SIG tunnel is down.
Global SIG Credentials Template	Cisco SD-WAN Release 20.9.1 Cisco vManage Release 20.9.1	With this feature, create a single global SIG Credentials template for each SIG provider (Cisco Umbrella or Zscaler). When you attach a SIG template to a device template, Cisco SD-WAN Manager automatically attaches the applicable global SIG Credentials template to the device template.

Cisco Catalyst SD-WAN edge devices support SD-WAN, routing, security, and other LAN access features that can be managed centrally. On high-end devices, you can enable all these features while providing the scale and performance required by large enterprises. However, on lower-end devices, enabling all the security features simultaneously can degrade performance. To avoid the performance degradation, integrate lower-end devices with Secure Internet Gateways (SIG) that do most of the processing to secure enterprise traffic. When you integrate a Cisco Catalyst SD-WAN edge device with a SIG, all client internet traffic, based on routing or policy, is forwarded to the SIG. In addition, the SIG can also protect roaming users, mobile users, and BYOD users.

- Options to Integrate Your Devices with Secure Internet Gateways, on page 3
- Configure Tunnels, on page 7
- Monitor Tunnels, on page 32

Options to Integrate Your Devices with Secure Internet Gateways

To integrate Cisco Catalyst SD-WAN edge devices with a SIG, you can use:

- Automatic tunnels
- Manual tunnels

Automatic Tunnels

Using the Secure Internet Gateway (SIG) feature template, you can provision automatic IPSec tunnels to Cisco Umbrella SIGs, or automatic IPSec or GRE tunnels to Zscaler SIGs.

Provision an automatic tunnel as follows:

1. Complete the following prerequisites for the SIG:
2. Specify Cisco Umbrella or Zscaler credentials using the SIG Credentials feature template.
3. Specify the details for the tunnel to the SIGs using the Security Internet Gateway (SIG) feature template.

   In the template, define the parameters for the tunnels such as the interface name, the source interface, the SIG provider, and so on.
4. Edit the VPN feature template that provides the service route for the devices to the internet. Add a service route to the SIG in the VPN feature template.
5. Add feature templates to the device templates of the devices that should route traffic to the SIG.
6. Attach the device templates to the devices.

When you attach the device template, the device sets up tunnels to the SIGs and redirects traffic to it.

Cisco Umbrella Integration

From Cisco SD-WAN Release 20.1.1 and Cisco vManage Release 20.2.1, use Cisco Umbrella as a SIG by choosing Umbrella as the SIG provider in the Security Internet Gateway (SIG) feature template, and then define IPSec tunnels, and tunnel parameters. Use the SIG credentials feature template to specify the Umbrella Organization ID, Registration Key, and Secret. For information on configuring automatic tunnelling, see Configure Automatic Tunnels Using Cisco SD-WAN Manager, on page 7.

Cisco Umbrella Multi-Org Support

Minimum releases: Cisco IOS XE Release 17.11.1a and Cisco vManage Release 20.11.1

The Cisco Catalyst SD-WAN Umbrella for SIG support security policy requirements for different sub-regions of their SD-WAN network. This feature is supported for both DNS security policy and SIG templates.

Although Cisco Umbrella's individual dashboards can only support a single domain, the multi-org feature allows you to view and manage multiple domains or logically separate network segments from a particular dashboard. The multi-org setup is suitable for organizations that are highly distributed across different locations where networks are all connected, but where different regions require different security policies. The multi-org feature is also helpful for networks with more than one Active Directory (AD) domain, whether within an AD or logically separate domains.

Zscaler Integration

You can integrate Cisco Catalyst SD-WAN edge devices to Zscaler SIGs by provisioning automatic IPsec tunnels between the edge devices and the SIGs.

From Cisco SD-WAN Release 20.5.1 and Cisco vManage Release 20.5.1, you can provision automatic IPSec tunnels to Zscaler Internet Access (ZIA) Public Service Edges using the Security Internet Gateway (SIG) feature template. ZIA Public Service Edges are secure internet gateways that can inspect and secure traffic from Cisco Catalyst SD-WAN devices. The devices use Zscaler APIs to create IPSec tunnels by doing the following:

1. Establish an authenticated session with ZIA.
2. Based on the IP address of the device, obtain a list of nearby data centres.
3. Provision the VPN credentials and location using ZIA APIs.
4. Using the VPN credentials and location, create an IPSec tunnel between the ZIA Public Service Edges and the device.

For information on configuring automatic tunnelling, see Configure Automatic Tunnels Using Cisco SD-WAN Manager, on page 7.

Manual Tunnels

You can create a GRE or IPSec tunnel to a third-party SIG or a GRE tunnel to a Zscaler SIG by defining the tunnel properties in the Secure Internet Gateway (SIG) feature template.

Provision manual tunnels as follows:

1. Specify the details for the tunnel to the SIG by using the Security Internet Gateway (SIG) feature template.

   In the template, define the parameters for the tunnels such as the interface name, the source interface, the SIG provider, and so on.

2. Edit the VPN feature template that provides the service route for the devices to the internet. Add a service route to the SIG in the VPN feature template.
3. Add feature templates to the device templates of the devices that should route traffic to the SIG.
4. Attach the device templates to the devices.

When you attach the device template, the device sets up the defined IPSec or GRE tunnels to the SIG and redirects traffic to it.

High Availability and Load Balancing

When you connect a Cisco Catalyst SD-WAN edge device to Cisco Umbrella, Zscaler, or a third-party SIG, you can connect the device to a primary data center and a secondary data center. Also, you can provision more than one tunnel to each data center.

Active Tunnels: You can provision up to four IPSec tunnels to the primary data center. These tunnels serve as active tunnels, and when two or more active tunnels are provisioned, the traffic toward the SIG is distributed among these tunnels, increasing the available bandwidth toward the SIG. From Cisco SD-WAN Release 20.4.1 and Cisco vManage Release 20.4.1, you can distribute the traffic equally among the active tunnels to achieve an equal-cost multi-path (ECMP) distribution, or assign different weights to the active tunnels so that some tunnels carry more traffic toward the SIG than the others.

Back-up Tunnels: You can provision up to four IPSec tunnels to the secondary data center, one for each active tunnel that you have provisioned to the primary data center. These tunnels to the secondary data center serve as back-up tunnels. When an active tunnel fails, the traffic toward the SIG is sent through the corresponding back-up tunnel. When you provision two or more back-up tunnels, the traffic toward the SIG is distributed among these tunnels, increasing the available bandwidth toward the SIG. From Cisco SD-WAN Release 20.4.1 and Cisco vManage Release 20.4.1, you can distribute the traffic equally among the back-up tunnels to achieve an ECMP distribution, or assign different weights to the back-up tunnels so that some tunnels carry more traffic toward the SIG than the others.

By provisioning two or more active tunnels and distributing the traffic among them, while not provisioning any back-up tunnels, you can create an active-active setup. By provisioning a back-up tunnel for each active tunnel, you can create an active-back-up setup.

Support for Layer 7 Health Check

You can monitor the health of tunnels towards the SIG using trackers attached to the tunnels. These trackers are used to automatically fail over to backup tunnels based on the health of the tunnel.

While creating automatic tunnels, Cisco SD-WAN Manager creates and attaches a default tracker with default values for failover parameters. However, you can also create customized trackers with failover parameter values that suit your SLA requirements.

In the case of manually created tunnels, create and attach the tracker.

The following table summarizes tracker support for automatic and manual tunnels:

Tunnel Type	Default Tracker	Customized Tracker
Automatic	Yes	Yes Minimum releases: Cisco SD-WAN Release 20.5.1 and Cisco vManage Release 20.5.1
Manual	No	Yes Minimum releases: Cisco SD-WAN Release 20.8.1 and Cisco vManage Release 20.8.1

The tunnel health is monitored as follows:

1. Based on the configuration in the System feature template, Cisco SD-WAN Manager creates a tracker according to the default or customized failover parameters that you define in the SIG template. This tracker uses VPN 65530. Cisco SD-WAN Manager reserves VPN 65530 for tracker VPNs.

2. The tracker resolves the IP address of the SIG service using VPN 0.

   For automatic tunnels to Cisco Umbrella or Zscaler, the tracker uses the following URLs to connect to the SIG:

   - Cisco Umbrella: http://service.sig.umbrella.com
   - Zscaler: http://gateway.*zscaler-cloud-url*/vpntest

3. The device sets up tunnels to the SIG.
4. For each tunnel, the device creates a named TCP socket that it uses to identify the tunnels.
5. The tracker monitors the health of the tunnel using HTTP probes. The tracker calculates the round-trip time (RTT) and compares it to the configured SLA parameters.
6. If the tunnel does not meet the SLA parameters, the tracker marks the tunnel as down.
7. The device updates the routes for any service VPNs that are connected to the tunnel.

Tracker DNS Cache Timeout

Trackers attached to SIG tunnels monitor the corresponding SIG endpoints. A Cisco vEdge device resolves FQDNs of these SIG endpoints through DNS queries and caches the DNS resolved IP addresses. Trackers probe the SIG endpoint IP addresses to determine tunnel health.

The device refreshes the DNS cache containing SIG endpoint IP addresses as follows:

- Cisco SD-WAN Release 20.7.x and earlier, and Cisco vManage Release 20.7.x and earlier: Configure the DNS cache timeout using the **timer dns-cache-timeout** command on Cisco SD-WAN Manager in the system configuration mode. Cisco vEdge devices cache DNS resolved SIG endpoint IP addresses for the duration of this timeout. When the cache times out, Cisco vEdge devices refresh the cache through new DNS resolution queries. The default timeout is two minutes.

Note **timer dns-cache-timeout** also affects the caching of Cisco SD-WAN Validator IP addresses that the Cisco vEdge devices obtains by resolving FQDNs.

- Cisco SD-WAN Release 20.8.x and Cisco vManage Release 20.8.x: Cisco vEdge devices refresh cached SIG endpoint IP addresses every 2 hours. The DNS cache timeout is preconfigured and cannot be modified.
- From Cisco SD-WAN Release 20.9.1 and Cisco vManage Release 20.9.1: Configure the DNS cache timeout using the **timer tracker-dns-cache-timeout** command on Cisco SD-WAN Manager in the system configuration mode. Cisco vEdge devices cache DNS resolved SIG endpoint IP addresses for the duration of this timeout. When the cache times out, Cisco vEdge devices refresh the cache through new DNS resolution queries. The default timeout is two hours.

  When a Cisco vEdge device refreshes the cache, if a SIG endpoint FQDN is resolved to the IP address that was cached earlier, the device does not reset associated counters. In Cisco SD-WAN Release 20.8.x and earlier releases, and Cisco vManage Release 20.8.x and earlier releases, the device resets counters every time that it refreshes the cache. In some scenarios, this automatic resetting of the counters affects tracker behavior and the tracker fails to detect that the health of tunnel has degraded and it must not be used for routing traffic.

Related Topics

Create Automatic Tunnels Using a SIG Feature Template, on page 11
Create Manual Tunnels Using SIG Feature Template, on page 19
Configure Tracker DNS Cache Timeout Using a CLI Template, on page 29

Global SIG Credentials Template

Minimum supported release: Cisco vManage Release 20.9.1

In Cisco vManage Release 20.8.x and earlier releases, you must create a SIG Credentials template for a SIG provider (Cisco Umbrella or Zscaler) for each Cisco vEdge model that you wish to connect to the SIG.

From Cisco vManage Release 20.9.1, create a single global SIG Credentials template for a SIG provider (Cisco Umbrella or Zscaler) and attach the template to the required Cisco vEdges, irrespective of the device model. When you attach a SIG feature template that configures automatic SIG tunnels to a device template, Cisco SD-WAN Manager automatically attaches the applicable global SIG Credentials template to the device template.

The Cisco vEdges of your organization connect to Cisco Umbrella or Zscaler using a common organization account with the SIG provider. As such, it is beneficial to configure the organization account credentials on the devices through a global template. When you modify the Cisco Umbrella or Zscaler credentials, update only one global template for the modified credentials to take effect on the attached Cisco vEdges.

Note After you upgrade Cisco SD-WAN Manager software from Cisco vManage Release 20.8.x or earlier to Cisco vManage Release 20.9.1 or later, the device-model-specific SIG Credentials templates created in Cisco vManage Release 20.8.x or earlier become read-only. The read-only status allows you to only view the configured credentials. To update the credentials configured in Cisco vManage Release 20.8.x or an earlier release, create a SIG Credentials template for the SIG provider.

If you try to create or modify a SIG feature template, Cisco SD-WAN Manager prompts you to create a global SIG Credentials template for the SIG provider.

Related Topics

Create Cisco Umbrella SIG Credentials Template, on page 8
Create Zscaler SIG Credentials Template, on page 9

Configure Tunnels

Configure Automatic Tunnels Using Cisco SD-WAN Manager

Prerequisites

To configure automatic tunneling to a SIG, complete the following requisites:

- Cisco Umbrella: To configure automatic tunnels to Cisco Umbrella, you can do one of the following

- For Cisco SD-WAN Manager to fetch the API keys, specify Smart Account credentials here: **Administration** > **Settings** > **Smart Account Credentials**. Your Cisco Smart Account is the account that you use to log in to the Cisco Smart Software Manager (CSSM) portal.
- To manually specify the API keys, generate Umbrella Management API keys. See *Management and Provisioning* > *Getting Started* > *Overview* in the *Cloud Security API* documentation on the Cisco DevNet portal.

  Specify the generated keys in the SIG Credentials template.

- Zscaler Internet Access (ZIA): To configure automatic tunnels to Zscaler, do the following:

  1. Create partner API keys on the ZIA Partner Integrations page.
  2. Add the Partner Administrator role to the partner API keys.
  3. Create a Partner Administrator.
  4. Activate the changes.

  For more information, see *Managing SD-WAN Partner Keys* on the Zscaler Help Center.

  Specify the generated keys in the SIG Credentials template.

Create Cisco Umbrella SIG Credentials Template

Minimum supported release: Cisco vManage Release 20.9.1

When you Create Automatic Tunnels Using a SIG Feature Template, on page 11, on selecting Umbrella as the SIG provider, Cisco SD-WAN Manager prompts you to create the global SIG credentials template, if you haven't yet created the template. Click **Click here to create - SIG Credentials template** to create the Cisco Umbrella SIG credentials template.

Template Name and **Description** fields are prefilled:

Table 2: SIG Credentials Template Name and Description

Field	Description
Template Name	(Read only) Umbrella Global Credentials
Description	(Read only) Global credentials for Umbrella

Configure Cisco Umbrella Credentials

1. In the **Basic Details** section, do one of the following:

   - Enable Cisco SD-WAN Manager to fetch credentials from the Cisco Umbrella portal:

     a. Ensure that you have added your Cisco Smart Account credentials here: **Administration** > **Settings** > **Smart Account Credentials**.

        Cisco SD-WAN Manager uses the Cisco Smart Account credentials to connect to the Cisco Umbrella portal.

     b. Click **Get Keys**.

- Enter Cisco Umbrella credentials:

Field	Description
SIG Provider	(Read only) Umbrella
Organization ID	Enter the Cisco Umbrella parent organization ID for your organization. For more information, see *Find Your Organization ID* in the Cisco Umbrella SIG User Guide.
Registration Key	Enter the Umbrella Management API Key. It is part of DNS security policy under unified security policy. For more information, see *Management and Provisioning* > *Getting Started* > *Overview* in the Cloud Security API documentation on the Cisco DevNet portal.
Secret	Enter the Umbrella Management API Secret.

2. To save the template, click **Save**.

Create Zscaler SIG Credentials Template

Minimum release: Cisco vManage Release 20.9.1

When you Create Automatic Tunnels Using a SIG Feature Template, on page 11, on selecting Zscaler as the SIG provider, Cisco SD-WAN Manager prompts you to create the global SIG credentials template, if you haven't yet created the template. Click **Click here to create - SIG Credentials template** to create the Zscaler SIG credentials template.

Template Name and **Description** fields are prefilled:

Table 3: SIG Credentials Template Name and Description

Field	Description
Template Name	(Read only) Zscaler-Global-Credentials
Description	(Read only) Global credentials for Zscaler

1. In the **Basic Details** section, enter the Zscaler credentials:

Table 4: Zscaler Credentials

Field	Description
SIG Provider	(Read only) Zscaler
Organization	Name of the organization in Zscaler cloud. For more information, see *ZIA Help* > *Getting Started* > *Admin Portal* > *About the Company Profile*.

Field	Description
Partner base URI	This is the base URI that Cisco SD-WAN Manager uses in REST API calls. To find this information on the Zscaler portal, see *ZIA Help > ZIA API > API Developer & Reference Guide > Getting Started*.
Username	Username of the SD-WAN partner account.
Password	Password of the SD-WAN partner account.
Partner API key	Partner API key. To find the key in Zscaler, see *ZIA Help > Partner Integrations > Managing SD-WAN Partner Keys*.

2. To save the template, click **Save**.

Create SIG Credentials Template

Applicable releases: Cisco vManage Release 20.8.x and earlier releases.

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

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

3. Click **Add Template**.
4. Choose the device for which you are creating the template.
5. Under **Other Templates**, click **SIG Credentials**.
6. In the **Template Name** field, enter a name for the feature template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
7. In the **Description** field, enter a description for the feature template.
8. In **Basic Details** section, do the following:
   a. **SIG Provider**: Click **Umbrella** or **Zscaler**.
   b. For Cisco Umbrella, enter the following registration parameters or click **Get Keys** to have Cisco SD-WAN Manager fetch these parameters from the Cisco Umbrella portal.
      - **Organization ID**
      - **Child Org**
      - **Child Org List**
      - **Registration Key**

- **Secret**

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can select Child Org ID from the dropdown when a parent Org ID of a multi-org tenant is added to the SIG Credentials.

To fetch the parameters, Cisco SD-WAN Manager uses your Smart Account credentials to connect to the Cisco Umbrella portal. To manually enter the parameters, generate the values in your Umbrella account as described here.

c. For Zscaler, enter the following details:

Field	Description
Organization	The name of the organization in Zscaler cloud. To find this information in Zscaler, see **Administration** > **Company Profile**.
Child Org	Minimum releases: Cisco IOS XE Release 17.11.1a and Cisco vManage Release 20.11.1 Enter the child organization information in the SIG template.
Child Org List	Minimum releases: Cisco IOS XE Release 17.11.1a and Cisco vManage Release 20.11.1 Select the child org from the **Child Org List** drop-down list.
Partner base URI	This is the Zscaler Cloud API that Cisco SD-WAN Manager uses to connect to Zscaler. To find this information in Zscaler, see **Administration** > **API Key Management**.
Username	Username of the SD-WAN partner account.
Password	Password of the SD-WAN partner account.
Partner API key	The partner API key. To find the key in Zscaler, see **Zscaler Cloud Administration** > **Partner Integrations** > **SD-WAN**.

9. Click **Save**.

Create Automatic Tunnels Using a SIG Feature Template

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Click **Add Template**.
4. Choose the device for which you are creating the template.

5. Under **VPN**, click **Secure Internet Gateway (SIG)**.

6. In the **Template Name** field, enter a name for the feature template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 to 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

7. In the **Description** field, enter a description for the feature template.

8. (From Cisco vManage Release 20.9.1) **SIG Provider**: Click **Umbrella** or **Zscaler**.

   From Cisco vManage Release 20.9.1, on selecting **Umbrella** or **Zscaler** as the SIG provider, Cisco SD-WAN Manager prompts you to create the corresponding global SIG credentials template if you haven't yet created the template. Click **Click here to create - SIG Credentials template** to create the Cisco Umbrella or Zscaler SIG credentials template.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1, you can select Child Org ID from the dropdown when a parent Org ID of a multi-org tenant is added to the SIG Credentials.

9. To create one or more trackers to monitor tunnel health, do the following in the **Tracker** section:

Note From Cisco SD-WAN Release 20.5.1 and Cisco vManage Release 20.5.1 , you can create customized trackers to monitor the health of automatic tunnels. If you do not customize the SLA parameters, Cisco SD-WAN Manager creates a default tracker for the tunnel.

   a. Click **New Tracker**.

   b. Configure the following:

Table 5: Tracker Parameters

Field	Description
Name	Enter a name for the tracker. The name can be up to 128 alphanumeric characters.
Threshold	Enter the wait time for the probe to return a response before declaring that the configured endpoint is down. **Range**: 100 to 1000 milliseconds **Default**: 300 milliseconds.
Interval	Enter the time interval between probes to determine the status of the configured endpoint. **Range**: 20 to 600 seconds **Default**: 60 seconds

Field	Description
Multiplier	Enter the number of times the probes are resent before determining that a tunnel is down. **Note** When tunnel status changes continuously within a short period of time, the tunnel goes to the flapping state. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, to avoid flapping of tunnels, the tracker waits for the duration equal to the product of multiplier * interval to declare the status of the tunnel. **Range**: 1 to 10 **Default**: 3
API url of endpoint	Specify the API URL for the SIG endpoint of the tunnel.

Note Prior to Cisco vManage Release 20.8.1, SIG tracker monitor statistics were reset at every Domain Name System (DNS) cache timeout interval.

Beginning with Cisco vManage Release 20.8.1, SIG tracker monitor statistics are no longer reset at every DNS cache timeout interval. SIG tracker monitor statistics are reset every two hours. A SIG tracker allows you to track the health of your SIG tunnels.

c. Click **Add**.

d. To add more trackers, repeat sub-step **b** to sub-step **d**.

10. To create tunnels, do the following in the **Configuration** section:

a. (Cisco 20.8.x and earlier releases) **SIG Provider**: Click **Umbrella** or **Zscaler**.

b. Click **Add Tunnel**.

c. Under **Basic Settings**, configure the following:

Table 6: Basic Settings

Field	Description
Interface Name (0..255)	Enter the interface name. **Note** If you have attached the Cisco VPN Interface IPSec feature template to the same device, ensure that the interface number you enter is different from what you have entered in the IPSec template.
Description	Enter a description for the interface.

Field	Description
Tracker	By default, a tracker is attached to monitor the health of automatic tunnels to Cisco Umbrella or Zscaler. If you configured a customized tracker in step **8**, choose the tracker. **Note** From Cisco SD-WAN Release 20.5.1 and Cisco vManage Release 20.5.1, you can create customized trackers to monitor the health of automatic tunnels.
Tunnel Source Interface	Enter the name of the source interface of the tunnel. This interface should be the egress interface and is typically the internet-facing interface.
Data-Center	For a primary data center, click **Primary**, or for a secondary data center, click **Secondary**. Tunnels to the primary data center serve as active tunnels, and tunnels to the secondary data center serve as back-up tunnels.

d. (Optional) Under **Advanced Options**, configure the following:

Table 7: General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: **No**.
Track this interface for SIG	Enable or disable tracker for the tunnel. By default, Cisco SD-WAN Manager enables a tracker for automatic tunnels. **Default**: **On**.
IP MTU	Specify the maximum MTU size of packets on the interface. **Range**: 576 to 2000 bytes **Default**: 1400 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. **Range**: 500 to 1460 bytes **Default**: None
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. **Range**: 10 to 3600 seconds **Default**: 10

Field	Description
DPD Retries	Specify the number of seconds between DPD retry messages if the DPD retry message is missed by the peer. Once 1 DPD message is missed by the peer, the router moves to a more aggressive state and sends the DPD retry message at the faster retry interval, which is the number of seconds between DPD retries if the DPD message is missed by the peer. The default DPD retry message is sent every 2 seconds. Five aggressive DPD retry messages can be missed before the tunnel is marked as down. **Range**: 2 to 60 seconds **Default**: 3

Table 8: IKE

Field Name	Description
IKE Rekey Interval	Specify the interval for refreshing IKE keys. **Range:** 300 to 1209600 seconds (1 hour to 14 days) **Default**: 14400 seconds
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA2 • AES 128 CBC SHA1 • AES 128 CBC SHA2 **Default**: AES 256 CBC SHA1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. • 2 1024-bit modulus • 14 2048-bit modulus • 15 3072-bit modulus • 16 4096-bit modulus **Default**: 14 2048-bit modulus

Table 9: IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IPSec keys. **Range**: 300 to 1209600 seconds (1 hour to 14 days) **Default**: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. **Options**: 64, 128, 256, 512, 1024, 2048, 4096. **Default**: 512
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Options: • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM • NULL SHA1 • NULL SHA 384 • NULL SHA 256 • NULL SHA 512 **Default**: AES 256 GCM
Perfect Forward Secrecy	• Specify the PFS settings to use on the IPsec tunnel. • Choose one of the following Diffie-Hellman prime modulus groups: • Group-2 1024-bit modulus • Group-14 2048-bit modulus • Group-15 3072-bit modulus • Group-16 4096-bit modulus • None: disable PFS. **Default**: None

e. Click **Add**.

f. To create more tunnels, repeat sub-step **b** to sub-step **e**.

11. To designate active and back-up tunnels and distribute traffic among tunnels, configure the following in the **High Availability** section:

Table 10: High Availability

Field	Description
Active	Choose a tunnel that connects to the primary data center.
Active Weight	Enter a weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two active tunnels, where the first tunnel is configured with a weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.
Backup	To designate a back-up tunnel, choose a tunnel that connects to the secondary data center. To omit designating a back-up tunnel, choose **None**.
Backup Weight	Enter a weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two back-up tunnels, where the first tunnel is configured with a weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.

12. (Optional) Modify the default configuration in the **Advanced Settings** section:

Table 11: Umbrella

Field	Description
Umbrella Primary Data-Center	Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to a specific Cisco Umbrella data center, choose the data center from the drop-down list.
Umbrella Secondary Data-Center	Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to a specific Cisco Umbrella data center, choose the data center from the drop-down list.

Table 12: Zscaler

Field	Description
Primary Data-Center	Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to a specific Zscaler data center, choose the data center from the drop-down list.
Secondary Data-Center	Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to a specific Zscaler data center, choose the data center from the drop-down list.
Authentication Required	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
XFF Forwarding	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable Firewall	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable IPS Control	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable Caution	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable Surrogate IP	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Display Time Unit	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Minute
Idle Time to Disassociation	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: 0
Enforce Surrogate IP for known browsers	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off

Field	Description
Refresh Time Unit	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Minute
Refresh Time	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: 0
Enable AUP	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
First Time AUP Block Internet Access	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Force SSL Inspection	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
AUP Frequency	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: 0

13. Click **Save**.

Create Manual Tunnels Using SIG Feature Template

From Cisco SD-WAN Release 20.4.1 and Cisco vManage Release 20.4.1, all SIG related workflows for automatic and manual tunnels have been consolidated into the SIG template. If you are using Cisco SD-WAN Release 20.4.1 and Cisco vManage Release 20.4.1, or later, use the SIG template to configure GRE or IPSec tunnels to a third-party SIG, or GRE tunnels to a Zscaler SIG.

For a software release earlier than Cisco SD-WAN Release 20.4.1, Cisco vManage Release 20.4.1, see *Configuring a GRE Tunnel or IPsec Tunnel from Cisco SD-WAN Manager*.

Layer 7 Health Check: The option to create trackers and monitor the health of manually created tunnels is available from Cisco SD-WAN Release 20.8.1, Cisco vManage Relase 20.8.1. In earlier releases, the Layer 7 Health Check feature is only available if you use VPN Interface GRE/IPSEC templates, and not with SIG templates.

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

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Click **Add Template**.
4. Choose the device for which you are creating the template.
5. Under **VPN**, click **Secure Internet Gateway (SIG)**.
6. In the **Template Name** field, enter a name for the feature template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 to 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
7. In the **Description** field, enter a description for the feature template.
8. (Optional) To create one or more trackers to monitor tunnel health, do the following in the Tracker section:

Note The option to create trackers and monitor tunnel health is available from Cisco SD-WAN Release 20.8.1, Cisco vManage Relase 20.8.1.

a. Click **New Tracker**.

b. Configure the following:

Field	Description
Name	Enter a name for the tracker. The name can be up to 128 alphanumeric characters.
Threshold	Enter the wait time for the probe to return a response before declaring that the configured endpoint is down. **Range**: 100 to 1000 milliseconds **Default**: 300 milliseconds
Interval	Enter the time interval between probes to determine the status of the configured endpoint. **Range**: 20 to 600 seconds **Default**: 60 seconds
Multiplier	Enter the number of times to resend probes before determining that a tunnel is down. **Range**: 1 to 10 **Default**: 3
API url of endpoint	Specify the API URL for the SIG endpoint of the tunnel. **Note** Both HTTP and HTTPS API URLs are supported. SIG tunnel tracker configuration only supports HTTP even though the HTTPS option is available.

c. Click **Add**.

d. To add more trackers, repeat sub-step **b** to sub-step **d**.

9. To create tunnels, do the following in the **Configuration** section:

a. **SIG** Provider: Click **Generic**.

Cisco vManage Release 20.4.x and earlier: Click **Third Party**.

b. Click **Add Tunnel**.

c. Under **Basic Settings**, configure the following:

Field	Description
Tunnel Type	Based on the type of tunnel you wish to create, click **ipsec** or **gre**.
Interface Name (0..255)	Enter the interface name. **Note** If you have attached the Cisco VPN Interface IPSec feature template or the Cisco VPN Interface GRE feature template to the same device, ensure that the interface number you enter is different from what you have entered in the IPSec or GRE templates.
Description	(Optional) Enter a description for the interface.
Source Type	Click **INTERFACE** or **IP**.
Tracker	(Optional) Choose a tracker to monitor tunnel health. **Note** From Cisco SD-WAN Release 20.8.1 and Cisco vManage Relase 20.8.1, you can create trackers to monitor tunnel health.
Track this interface for SIG	Enable or disable tracker for the tunnel. By default, Cisco SD-WAN Manager enables a tracker for automatic tunnels. **Default**: **On**.
Tunnel Source Interface	This field is displayed only if you chose the **Source Type** as **INTERFACE.** Enter the name of the source interface of the tunnel. This interface should be an egress interface and is typically the internet-facing interface.
Tunnel Source IP Address	This field is displayed only if you chose the **Source Type** as **IP.** Enter the IP address of the tunnel source.
IPv4 address	This field is displayed only if you chose the **Source Type** as **IP.** (Optional) Enter the tunnel interface's IP address.
Tunnel Destination IP Address/FQDN	Enter the IP address of the SIG provider endpoint.

Field	Description
Preshared Key	This field is displayed only if you choose **ipsec** as the **Tunnel Type**. Enter the password to use with the preshared key.

d. (Optional) Under **Advanced Options**, configure the following:

Table 13: (Tunnel Type: gre) General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: No.
IP MTU	Specify the maximum MTU size of packets on the interface. **Range**: 576 to 2000 bytes **Default**: 1400 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. **Range**: 500 to 1460 bytes **Default**: None

Table 14: (Tunnel Type: gre) Keep Alive

Field	Description
Interval	Time duration between successive GRE keepalive messages. **Range**: 0 to 65535 seconds **Default**: 0
Retries	Number of times the keepalive messages are sent to the remote device when no response is received from the remote device. If no response is received after these many tries, the remote device is declared down. **Range**: 0 to 255 **Default**: 3

Table 15: (Tunnel Type: ipsec) General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: No.

Field	Description
IP MTU	Specify the maximum MTU size of packets on the interface. **Range**: 576 to 2000 bytes **Default**: 1400 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. **Range**: 500 to 1460 bytes **Default**: None
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. **Range**: 0 to 65535 seconds **Default**: 10
DPD Retries	Specify how many unacknowledged packets to send before declaring an IKE peer to be dead and then removing the tunnel to the peer. **Range**: 0 to 255 **Default**:3

Table 16: (Tunnel Type: ipsec) IKE

Field	Description
IKE Rekey Interval	Specify the interval for refreshing IKE keys **Range:** 300 to 1209600 seconds (1 hour to 14 days) **Default**: 14400 seconds
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA2 • AES 128 CBC SHA1 • AES 128 CBC SHA2 **Default**: AES 256 CBC SHA1

Field	Description
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. Choose one of the following: • 2 1024-bit modulus • 14 2048-bit modulus • 15 3072-bit modulus • 16 4096-bit modulus **Default**: 16 4096-bit modulus
IKE ID for Local Endpoint	If the remote IKE peer requires a local end point identifier, specify the same. **Range**: 1 to 64 characters **Default**: Tunnel's source IP address
IKE ID for Remote Endpoint	If the remote IKE peer requires a remote end point identifier, specify the same. **Range**: 1 to 64 characters **Default**: Tunnel's destination IP address

Table 17: (Tunnel Type: ipsec) IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IPSec keys. **Range**: 300 to 1209600 seconds (1 hour to 14 days) **Default**: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. **Options**: 64, 128, 256, 512, 1024, 2048, 4096. **Default**: 512

Field	Description
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM • NULL SHA 384 • NULL SHA 256 • NULL SHA 512 **Default**: NULL SHA 512
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel. Choose one of the following Diffie-Hellman prime modulus groups: • Group-2 1024-bit modulus • Group-14 2048-bit modulus • Group-15 3072-bit modulus • Group-16 4096-bit modulus • None: disable PFS. **Default**: Group-16 4096-bit modulus

e. Click **Add**.

f. To create more tunnels, repeat sub-step **b** to sub-step **e**.

10. To designate active and back-up tunnels and distribute traffic among tunnels, configure the following in the **High Availability** section:

Table 18: High Availability

Field	Description
Active	Choose a tunnel that connects to the primary data center.

Field	Description
Active Weight	Enter a weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two active tunnels, where the first tunnel is configured with a weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.
Backup	To designate a back-up tunnel, choose a tunnel that connects to the secondary data center. To omit designating a back-up tunnel, choose **None**.
Backup Weight	Enter a weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two back-up tunnels, where the first tunnel is configured with a weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.

11. Click **Save**.

Create Manual Tunnels Using the CLI

Minimum releases: Cisco SD-WAN Release 20.9.1 and Cisco vManage Release 20.9.1

This section provides example CLI configurations for creating manual SIG tunnels.

```
Device(config-vpn-0)# interface ipsec1
Device(config-interface-ipsec1)# description ZScaler-Primary-Account1-vpn1
Device(config-interface-ipsec1)# ip address 10.18.0.1/30
Device(config-interface-ipsec1)# tunnel-source-interface ge0/0
Device(config-interface-ipsec1)# tunnel-destination 10.225.200.20
Device(config-interface-ipsec1)# dead-peer-detection interval 5
Device(config-interface-ipsec1)# tunnel-set secure-internet-gateway-other
```

Redirect Traffic to a SIG

You can redirect traffic to a SIG in two ways:

- Using Data Policy. For more information, see Action Parameters in the Policies Configuration Guide.
- Using the Service route to SIG. For more information, see Modify Service VPN Template, on page 27

Modify Service VPN Template

To ensure that the device connects to the SIG, you must modify the VPN template to include a service route to the SIG.

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

   Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. For the VPN template of the device, click **Edit**.
4. Click **IPv4 Route**.
5. Click the delete icon on any existing IPv4 route to the internet.
6. Click **Service Route**.
7. Click **New Service Route**.
8. Enter a Prefix (for example, 10.0.0.0/8).
9. For the service route, ensure that **SIG** is chosen.
10. Click **Add**.
11. Click **Update**.

Create Device Template

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

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

3. Click **Create Template** and click **From Feature Template**.
4. From the **Device Model** drop-down list, choose the device model for which you are creating the template.

   Cisco SD-WAN Manager displays all the feature templates for that device type. The required feature templates are indicated with an asterisk (*), and the remaining templates are optional. The factory-default template for each feature is chosen by default.

5. From the **Device Role** drop-down list, choose **SDWAN Edge**.
6. In the **Template Name** field, enter a name for the device template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

7. In the **Description** field, enter a description for the device template.

This field is mandatory, and it can contain any characters and spaces.

8. Click **Transport & Management VPN**.

9. In the **Transport & Management VPN** section, under **Additional Cisco VPN 0 Templates**, click **Secure Internet Gateway**.

10. From the **Secure Internet Gateway** drop-down list, choose the SIG feature template that you created earlier.

11. Click **Additional Templates**.

12. In the **Additional Templates** section,

    a. Automatic tunneling:

    (Cisco vManage Release 20.8.x and earlier) From the **SIG Credentials** drop-down list, choose the relevant SIG Credentials feature template.

    (From Cisco vManage Release 20.9.1) Cisco SD-WAN Manager automatically chooses the applicable global SIG Credentials feature template based on the SIG feature template configuration.

Note If there are any changes to the SIG credentials, for these changes to take effect, you must first remove the SIG feature template from the device template and push the device template. Thereafter, re-attach the SIG feature template and then push the template to the device. For information on pushing the device template, see Attach the SIG Template to Devices.

    b. Manual tunneling: No need to attach a **SIG Credentials** template.

13. Click **Create**.

    The new configuration template is displayed in the **Device Template** table. The **Feature Templates** column shows the number of feature templates that are included in the device template, and the **Type** column shows **Feature** to indicate that the device template was created from a collection of feature templates.

Attach Template to Devices

To attach one or more devices to the device template:

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

2. Click **Device Templates**, and choose the template that you created.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is called **Device**.

3. For the desired template, click **...** and click **Attach Devices**.

   The Attach Devices dialog box displays.

4. In the **Available Devices** column, choose a group and search for one or more devices, choose a device from the list, or click **Select All**.

5. Click the arrow pointing right to move the device to the **Selected Devices** column.
6. Click **Attach**.
7. If the template contains variables, enter the missing variable values for each device in one of the following ways:
   - Enter the values manually for each device either in the table column or by clicking **...** in the row and clicking **Edit Device Template**. When you are using optional rows, if you do not want to include the parameter for the specific device, do not specify a value.
   - Click **Import File** to upload a CSV file that lists all the variables and defines each variable value for each device.
8. Click **Update**.

Configure Tracker DNS Cache Timeout Using a CLI Template

Minimum supported releases: Cisco SD-WAN Release 20.9.1 and Cisco vManage Release 20.9.1.

To configure tracker DNS cache timeout, add the CLI command sequence provided in this section to a device CLI template and attach the template to Cisco SD-WAN Manager. For more information about using a CLI template, see Create a Device CLI Template.

Note By default, CLI templates execute commands in the global configuration (config) mode.

1. Enter the system configuration mode.

   ```
   system
   ```

2. Configure tracker DNS cache timeout.

   ```
   timer tracker-dns-cache-timeout duration
   ```

The following example shows a sample configuration which defines the cache timeout as 15 minutes:

```
system
 timer tracker-dns-cache-timeout 15
```

Related Topics

Support for Layer 7 Health Check, on page 5

Configuring a GRE Tunnel or IPsec Tunnel from Cisco SD-WAN Manager

Table 19: Feature History

Feature Name	Release Information	Description
Manual Configuration for GRE Tunnels and IPsec Tunnels	Cisco SD-WAN Release 20.1.1	This feature lets you manually configure a GRE tunnel by using the VPN Interface GRE template or an IPSec tunnel by using the VPN Interface IPSec template. For example, use this feature to manually configure a tunnel to a SIG.

Note From Cisco SD-WAN Release 20.4.1, Cisco vManage Release 20.4.1, all SIG related workflows for Automatic and Manual Tunnels have been consolidated into the SIG template. If you are using Cisco SD-WAN Release 20.4.1, Cisco vManage Release 20.4.1, or later, configure GRE or IPSec tunnels to a generic SIG, or GRE tunnels to a Zscaler SIG, using the SIG template.

Configure a GRE Tunnel from Cisco SD-WAN Manager

This section describes how to manually create a GRE tunnel from Cisco SD-WAN Manager. This procedure lets you configure a GRE tunnel to a third-party vendor.

Note To configure a GRE tunnel from Cisco SD-WAN Manager, use the SIG Feature Template. For more information, see Create Manual Tunnels Using Cisco SIG Feature Template. The Cisco VPN Interface GRE template is no longer used to configure a tunnel to a SIG.

For releases prior to Cisco vManage Release 20.8.1, use the Cisco VPN Interface GRE template.

1. Perform these actions to create a GRE template:

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

   b. Click **Feature Templates**, and then click **Add Template**.

   Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

   c. Choose the type of device for which you are creating the template.

   d. Choose the VPN Interface GRE template from the group of VPN templates.

   e. In **Basic Configuration**, configure parameters as desired and then click **Save**. For more information on configuring the VPN GRE template, see VPN Interface GRE.

2. Perform these actions to create a GRE route:

   a. Click **Feature Templates**, and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

   b. Choose the type of device for which you are creating the template.
   c. Choose the Cisco VPN template in the group of VPN templates.
   d. Click **GRE Route**.
   e. Click **New GRE Route**.
   f. Configure parameters as desired, and then click **Add**.

3. Perform these actions to configure a device template for the GRE interface.
   a. Click **Device**, and then click **...**and click **Edit** for the device template that you want to configure.
   b. Click **Transport & Management VPN**.
   c. From the Additional Cisco VPN 0 Templates list, choose the VPN Interface GRE template.
   d. From the VPN Interface GRE drop-down menu, click **Create Template**.
   e. Configure the templates as desired, and then click **Save**.

Configure an IPsec Tunnel from Cisco SD-WAN Manager

This section describes how to manually create an IPsec tunnel from Cisco SD-WAN Manager. This procedure lets you configure an IPsec tunnel to a third-party vendor.

Note To configure a IPSec tunnel from Cisco SD-WAN Manager, use the SIG Feature Template. For more information, see Create Automatic Tunnels Using Cisco SIG Feature Template. The Cisco VPN Interface IPSec template is no longer used to configure a tunnel to a SIG.

For releases prior to Cisco vManage Release 20.8.1, use the Cisco VPN Interface IPsec template.

1. Perform these actions to create an IPsec template:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Feature Templates**, and click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

   c. Choose the type of device for which you are creating the template.
   d. Choose the VPN Interface IPsec template from the group of VPN templates.
   e. In **Basic Configuration**, configure parameters as desired,
   f. In **Advanced**, specify a name for your **Tracker**.

g. Click **Save**.

2. Perform these actions to create an IPSec route:

   a. Click **Feature Templates**, and, click **Add Template**.

   > **Note** In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

   b. Choose the type of device for which you are creating the template.

   c. Choose the Cisco VPN template in the group of VPN templates.

   d. Click **IPSEC Route**.

   e. Click **New IPSEC Route**.

   f. Configure parameters as desired, and then click **Add**.

3. Perform these actions to configure a device template for the IPsec interface.

   a. Click **Device**, and click **…** and choose **Edit** for the device template that you want to configure.

   b. Click **Transport & Management VPN**.

   c. From the Additional Cisco VPN 0 Templates list, choose the VPN Interface IPsec template.

   d. From the VPN Interface IPsec drop-down menu, click **Create Template**.

   e. Configure the templates as desired, and then click **Save**.

Monitor Tunnels

To monitor the status of tunnels running the layer 7 health check tracker, run the **show interface** or **show support tracker interface monitors** commands.

```
Device# show interface

IF IF IF TCP
AF ADMIN OPER TRACKER ENCAP SPEED MSS RX TX
VPN INTERFACE TYPE IP ADDRESS STATUS STATUS STATUS TYPE PORT TYPE MTU HWADDR MBPS DUPLEX
ADJUST UPTIME PACKETS PACKETS
--------------------------------------------------------------------------------------------
0 ge0/0 ipv4 10.1.16.16/24Up Up NA null transport 1500 52:54:00:93:04:c6 1000 full 1416
0:03:01:39 10405 11377
0 ge0/1 ipv4 10.0.21.16/24Up Up NA null transport 1500 52:54:00:c4:e3:6f 1000 full 1416
0:03:01:37 6214 6112
0 ge0/2 ipv4 - Up Up NA null service 1500 52:54:00:7b:e1:3f 1000 full 1416 0:03:01:37 0 0
0 ge0/3 ipv4 10.0.100.16/24Up Up NA null service 1500 52:54:00:1a:ec:8c 1000 full 1416
0:03:01:37 114 57
0 ge0/4 ipv4 10.0.14.16/24Up Up NA null service 1500 52:54:00:77:15:59 1000 full 1416
0:03:01:37 0 0
0 ipsec1 ipv4 - Up Up Up vlan service 1400 00:00:00:00:00:01 1000 full 1316 0:00:10:16 1587
 2776
0 ipsec2 ipv4 - Up Up Down vlan service 1400 00:00:00:00:00:01 1000 full 1316 0:00:10:01
41 0
```

```
0 system ipv4 172.16.255.16/32Up Up NA null loopback 1500 00:00:00:00:00:00 1000 full 1416
 0:03:01:49 0 0
1 ge0/2.101 ipv4 172.16.21.2/24Up Up NA vlan service 1496 52:54:00:7b:e1:3f 1000 full 1412
 0:03:01:37 2752 1553
2 ge0/2.102 ipv4 172.16.22.2/24Up Up NA vlan service 1496 52:54:00:7b:e1:3f 1000 full 1412
 0:03:01:39 63 56
3 ge0/2.103 ipv4 172.16.23.2/24Up Up NA vlan service 1496 52:54:00:7b:e1:3f 1000 full 1412
 0:03:01:39 59 59
512 eth0 ipv4 10.0.1.16/24Up Up NA null service 1500 00:50:56:00:01:10 1000 full 1416
0:03:01:39 2005 1196
65528 loopback65528 ipv4 192.168.0.2/24Up Up NA null service 1500 00:00:00:00:00:00 1000
full 1416 0:03:01:39 0 0
65530 loopback65530 ipv4 192.168.0.2/24Up Up NA null service 1500 00:00:00:00:00:00 1000
full 1416 0:03:01:39 0 0
0 1000 full 1416 0:03:01:39 0 0
65530 loopback65530 ipv4 192.168.0.2/24 Up Up NA null service 1500 00:00:00:00:00:00 1000
full 1416 0:03:01:39 0 0
```

In the following example, the tracker is up:

```
Device#show support tracker interface monitors
  Interface: ipsec1/#SIGL7#AUTO#TRA#ZIA
Monitor: 65530/http://gateway.zscalerthree.net/vpntest/80 via ipsec1
   Monitor state     : UP (flapped 1 times)
   Ref count         : 1
   Monitor type      : httping
   Num of probes     : 1
   Max Re-transmit   : 2
   First Probe       : 0 secs
   Probe interval    : 30 secs
   Probe timeout     : 1000 msecs
   DNS TTL           : 33935 secs
   DNS query/ok/fail : 1/1/0

   Peer: 104.129.198.175 (UP - flapped 1 times, Re-Transmit 0)
     Total requests  : 1           Total responses : 1
     Total Tx errors : 0           Total Rx errors : 0
     Total Tx skipped: 0           Total Rx ignored: 0
     Total timeout   : 0           Connect errors  : 0
     RTT min/avg/max : 24.90/24.90/24.90 ms
     TCP min/avg/max : 11.70/11.70/11.70 ms

Interface: ipsec2/#SIGL7#AUTO#TRA#ZIA
Monitor: 65530/http://gateway.zscalerthree.net/vpntest/80 via ipsec2
   Monitor state     : UP (flapped 0 times)
   Ref count         : 1
   Monitor type      : httping
   Num of probes     : 1
   Max Re-transmit   : 2
   First Probe       : 0 secs
   Probe interval    : 30 secs
   Probe timeout     : 1000 msecs
   DNS TTL           : 33935 secs
   DNS query/ok/fail : 1/1/0

   Peer: 104.129.198.175 (UP - flapped 0 times, Re-Transmit 0)
     Total requests  : 6           Total responses : 6
     Total Tx errors : 0           Total Rx errors : 0
     Total Tx skipped: 0           Total Rx ignored: 0
     Total timeout   : 0           Connect errors  : 0
     RTT min/avg/max : 297.32/333.95/472.63 ms
     TCP min/avg/max : 150.47/181.04/320.78 ms
```

In the following example, the tracker is down:

```
vm6# show support tracker interface monitors
Interface: ipsec1/#SIGL7#AUTO#TRA#ZIA
Monitor: 65530/http://gateway.zscalerthree.net/vpntest/80 via ipsec1
   Monitor state : UP (flapped 0 times)
   Ref count : 1
   Monitor type : httping
   Num of probes : 1
   Max Re-transmit : 2
   First Probe : 0 secs
   Probe interval : 30 secs
   Probe timeout : 1000 msecs
   DNS TTL : 47453 secs
   DNS query/ok/fail : 1/1/0

   Peer: 192.0.2.1 (UP - flapped 0 times, Re-Transmit 0)
     Total requests : 34 Total responses : 34
     Total Tx errors : 0 Total Rx errors : 0
     Total Tx skipped: 0 Total Rx ignored: 0
     Total timeout : 0 Connect errors : 0
     RTT min/avg/max : 25.16/35.62/111.92 ms
     TCP min/avg/max : 12.45/17.71/69.28 ms

Interface: ipsec2/#SIGL7#AUTO#TRA#ZIA
Monitor: 65530/http://gateway.zscalerthree.net/vpntest/80 via ipsec2
   Monitor state : DOWN (flapped 1 times)
   Ref count : 1
   Monitor type : httping
   Num of probes : 1
   Max Re-transmit : 2
   First Probe : 0 secs
   Probe interval : 30 secs
   Probe timeout : 1000 msecs
   DNS TTL : 47453 secs
   DNS query/ok/fail : 1/1/0

   Peer: 192.0.2.1 (DOWN - flapped 1 times, Re-Transmit 0)
     Total requests : 33 Total responses : 0
     Total Tx errors : 0 Total Rx errors : 0
     Total Tx skipped: 0 Total Rx ignored: 0
     Total timeout : 33 Connect errors : 0
     RTT min/avg/max : 0.00/0.00/0.00 ms
     TCP min/avg/max : 0.00/0.00/0.00 ms
```