Configure and Verify SD-WAN IPsec SIG Tunnel with Zscaler

Contents

Introduction

This document describes the configuration steps and verification of SD-WAN IPsec SIG tunnels with Zscaler.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Security Internet Gateway (SIG).
- How IPsec tunnels works, Phase1 and Phase2 on Cisco IOS®.

Additional Requirements

- NAT needs to be enabled on the transport interface that is going to face the internet.
- A DNS server needs to be created on VPN 0, and the Zscaler base URL needs to be resolved with this DNS server. This is important because if this does not resolve, API calls is going to fail. Layer 7 health checks is going to fail too, since by default, the URL is: http://gateway.<zscalercloud>.net/vpntest.
- NTP (Network Time Protocol) must ensure that the Cisco Edge Router time is accurate, and API calls are not going to not fail.

- A service route pointing to SIG needs to be configured in the Service-VPN Feature Template or CLI: ip sdwan route vrf 1 0.0.0.0/0 service sig

Components Used

This document is based on these software and hardware versions:

- Cisco Edge Router version 17.6.6a
- vManage version 20.9.4

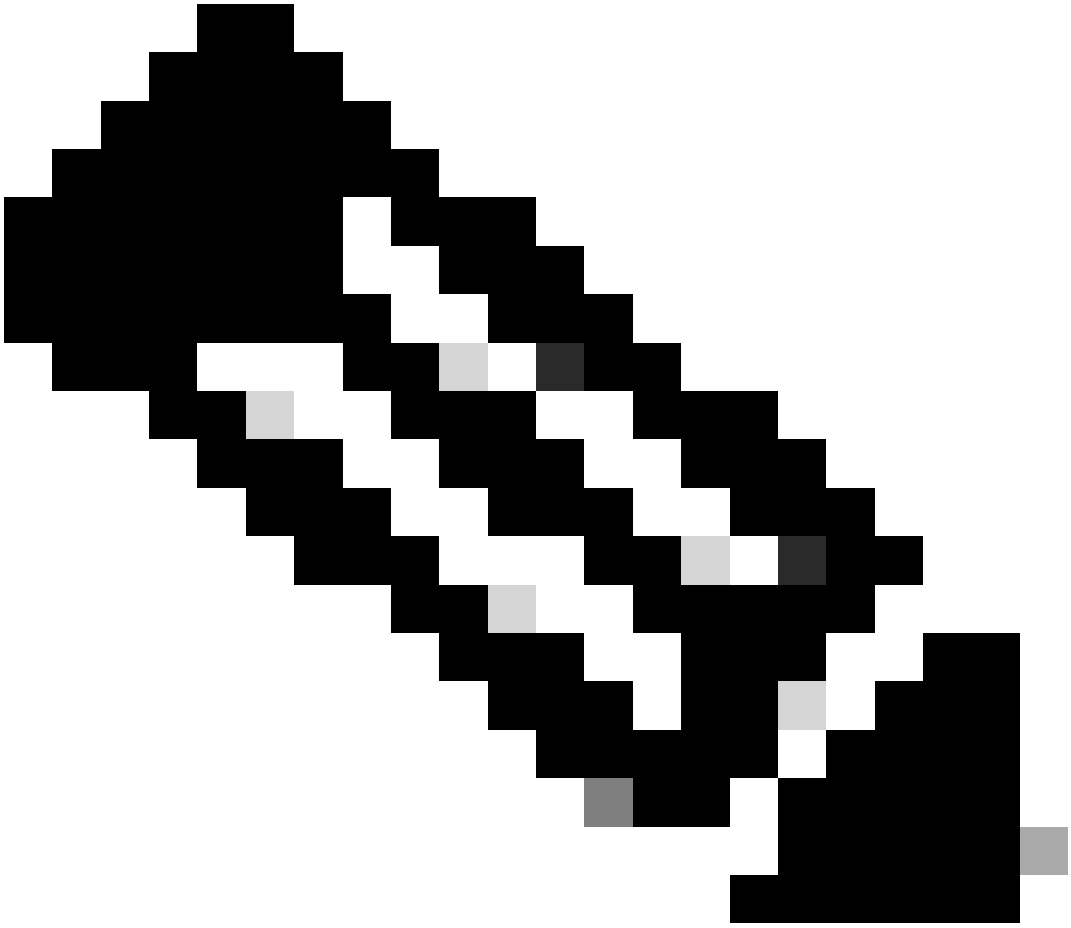
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Design Options

Here are the various types of deployments in an active/standby combination setup. Tunnel encapsulation can be deployed either GRE or IPsec.

- One Active/Standby Tunnel Pair.
- One Active/Active Tunnel Pair.
- Multiple Active/Standby Tunnel Pair.
- Multiple Active/Active Tunnel Pair.



Note: On SD-WAN Cisco Edge Routers, you can utilize one or more transport interfaces connected to the Internet, for these setup to function effectively.

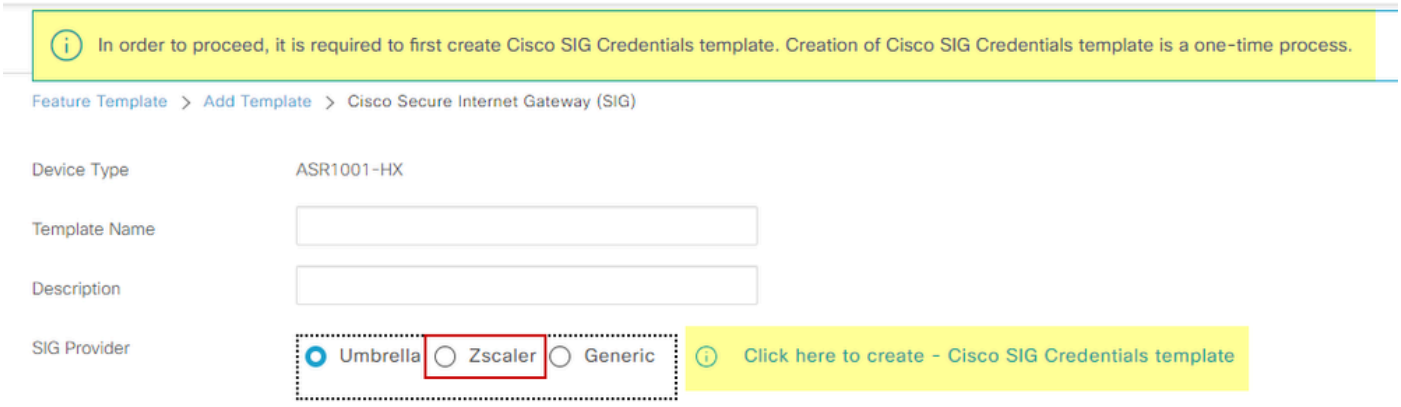
Configurations

Proceed with configuring these templates:

- Security Internet Gateway (SIG) Credential feature template:
  - You require one for all Cisco Edge Routers. Information to populate the necessary fields of the template needs to be created on the Zscaler portal.
- Security Internet Gateway (SIG) feature template:
  - Under this feature template, you configure IPsec tunnels, ensure deployment high availability (HA) in either active/active or active/standby mode, and select Zscaler Datacenter either automatically or manually.

To create a Zscaler Credentials template, navigate to **Configuration > Template > Feature Template > Add Template**.

Select the device model that you are going to use for this purpose and search for SIG. When you create it for the first time, the system shows that Zscaler Credentials need to be created first, as in this example:
You need to select **Zscaler** as a **SIG provider** and click on the **Click here to create - Cisco SIG Credentials template**.



Sig Credentila Template

"

You are redirected to the Credentials template. On this template, you must enter the values for all the fields:

- Template name
- Description
- SIG Provider (automatically selected from the previous step)
- Organization
- Partner Base URI
- Username
- Password
- Partner API Key

Click **Save**.

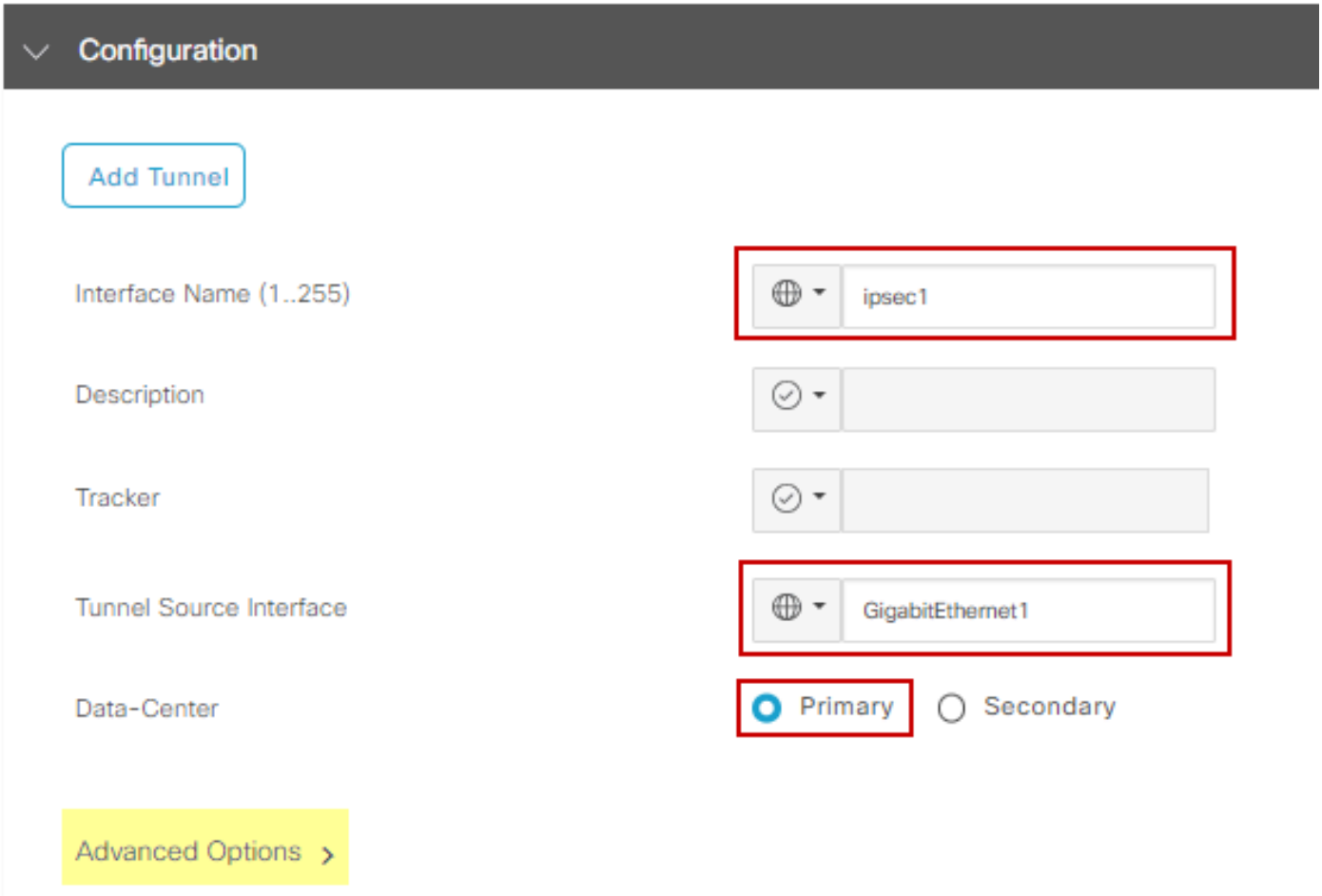
You are redirected to the Secure Internet Gateway (SIG) template. This template allows you to configure everything necessary for SD-WAN IPsec SIG with Zscaler.

In the first section of the template, please provide a name and a description. The default tracker is automatically enabled. The API URL used for the Zscaler Layer 7 health check is: zscaler_L7_health_check) ishttp://gateway<zscalercloud>net/vpntest.

In Cisco IOS XE, you need to set an IP address for the tracker. Any private IP within the /32 range is acceptable. The IP address you set can be utilized by the **Loopback 65530** interface, which is automatically created for performing Zscaler health inspections.

Under Configuration section you can create the IPsec tunnels by clicking **Add Tunnel**. On the new pop up window make selections based on your requirements.

In this example interface IPsec1 has been created, using WAN interface GigabitEthernet1 as Tunnel Source. Then it can form connectivity with the Primary Zcaler Data-Center.
It is recommended to keep the **Advanced Options** values as default.

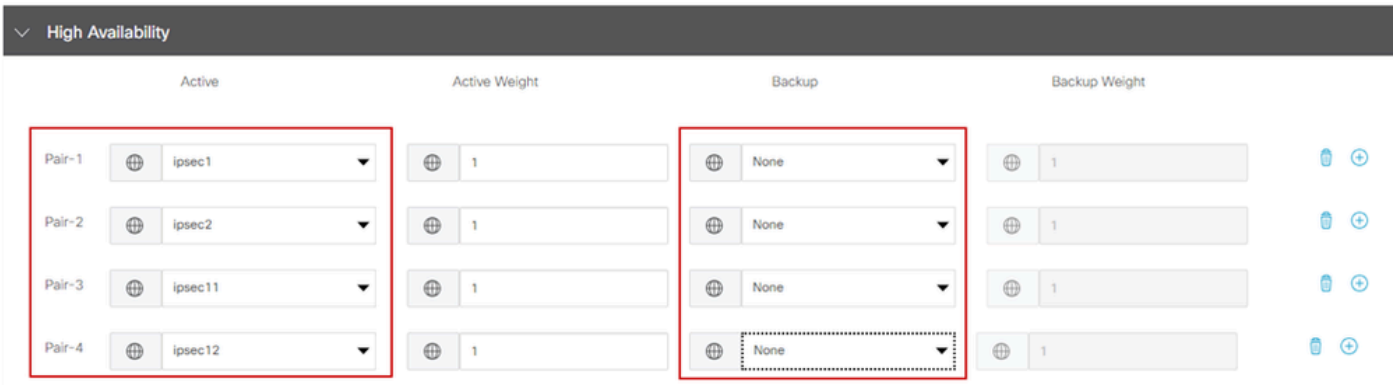


IPsec Interface Config

High Availability

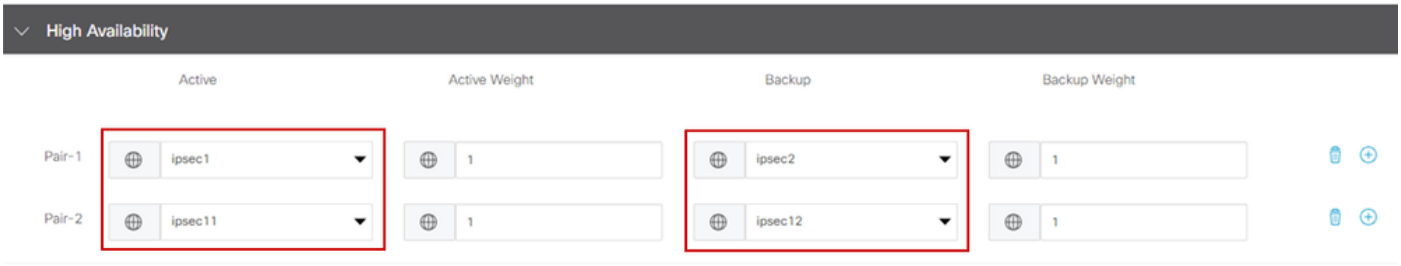
In this section, you choose whether the design is going to be Active/Active or Active/Standby, and determine which IPsec interface is going to be active.

This is an example of an Active/Active design. All the interfaces are selected under **Active**, leaving **Backup** with none.



Active/Active Design

This example showcases an Active/Standby design. IPsec1 and IPsec11 are selected to be active interfaces, while IPsec2 and IPsec12 are designated as standby interfaces.



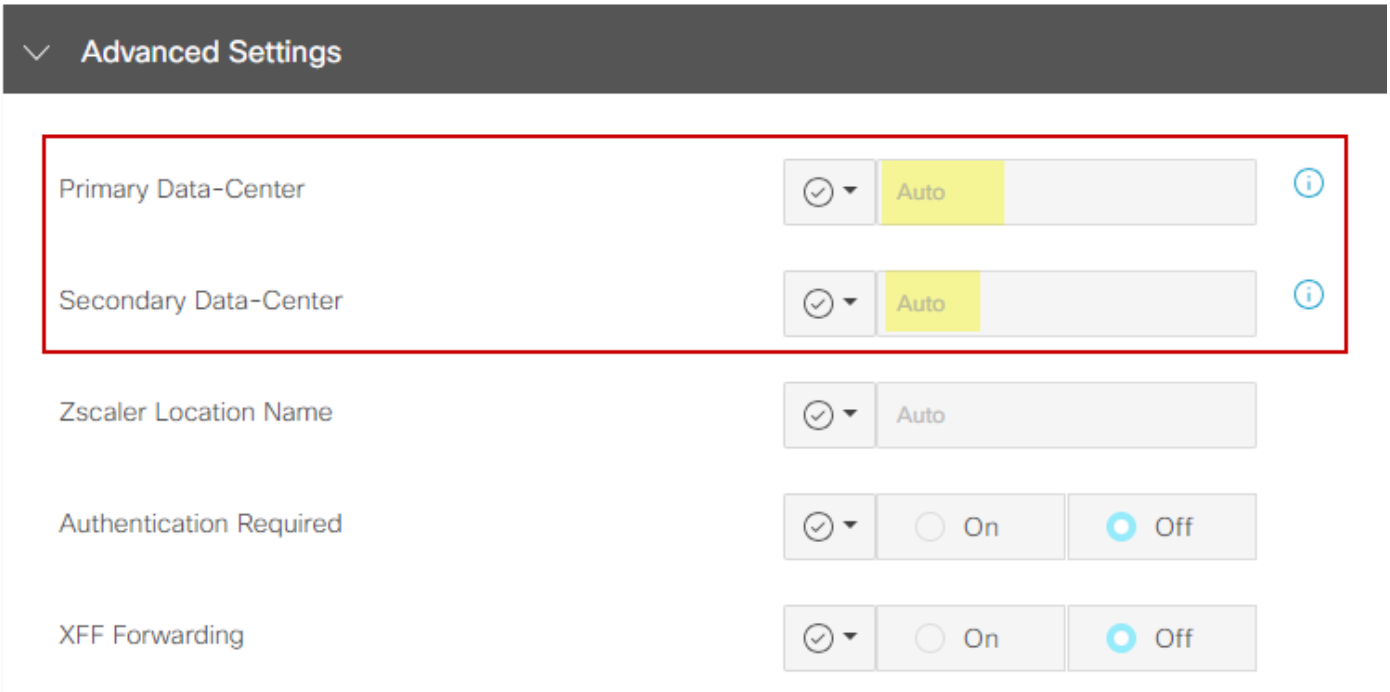
Active/Standby Design

Advance Settings

In this section, the most important configurations are the **Primary Data-Center** and **Secondary Data-Center**.

It is recommended to configure both as either automatic or manual, but it is not recommended to configure them as mixed.

If you choose to configure them manually, please select the correct URL from the Zscaler portal, based on your Partner Base URI



Auto or Manually Data Centers

Click **Save** when you have finished.

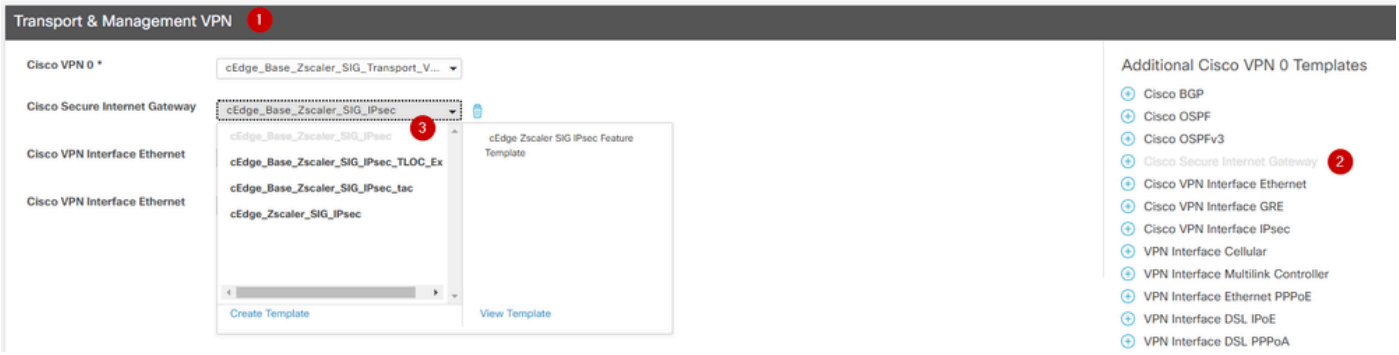
Once you are done with the SIG templates configuation you must apply them under the device template. In this way, the configuration is pushed onto the Cisco Edge Routers.

To complete these steps navigate to **Configuaration > Templates > Device Template**, on three dots click **Edit**.

1. Under **Transport & Management VPN**

2. Add **Secure Internet Gateway** template.

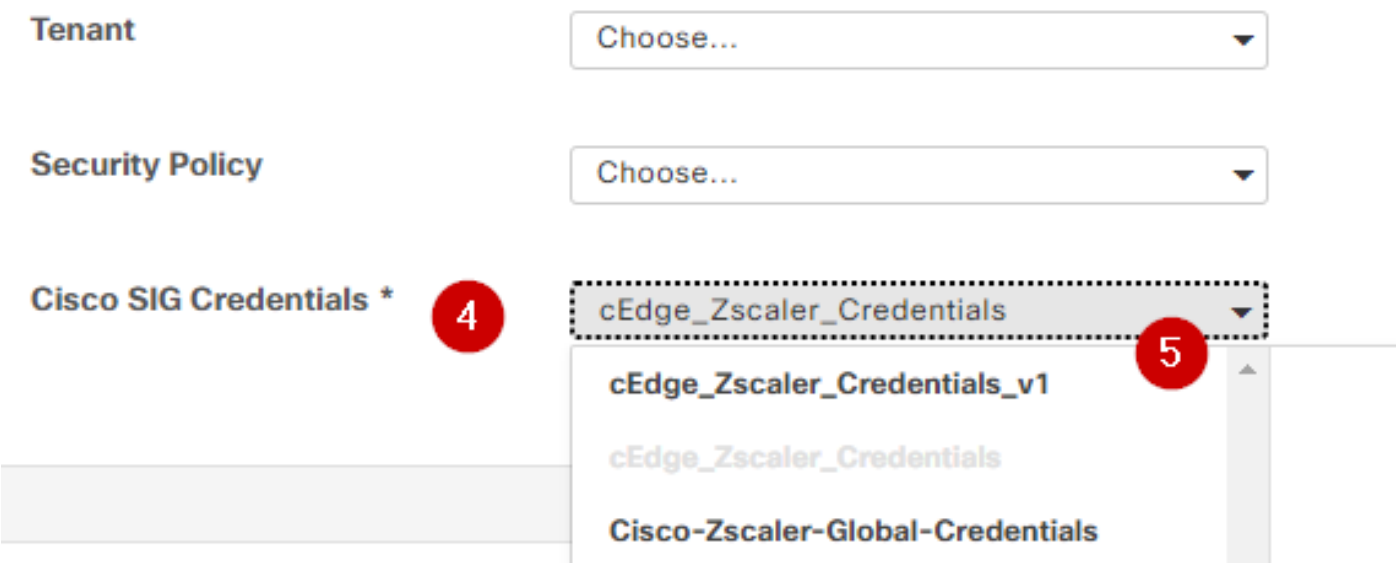
3. On **Cisco Secure Internet Gateway** select the correct SIG feature template from the drop down menu.



Add SIG Template on Device Template

Under **Additional Templates**

4. In **Cisco SIG Credentials**
5. Select the correct **Cisco SIG Credentials** template from the drop down menu:



Credential SIG template

Click **Update**, please note if your device template is a active template use the standard steps to push configurations on an active template.

Verify

Verification can be done during config preview while you are pushing the changes, what you must notice are:

```
secure-internet-gateway
     zscaler organization <removed>
     zscaler partner-base-uri <removed>
     zscaler partner-key <removed>
```

```
     zscaler username <removed>
     zscaler password <removed>
    !
```

From this example you can see that the design it is active/standby

<#root>

```
ha-pairs
  interface-pair
Tunnel100001 active
-interface-weight 1
Tunnel100002 backup
-interface-weight 1
  interface-pair
Tunnel100011 active
-interface-weight 1
Tunnel100012 backup
-interface-weight 1
```

You are going to notice more configurations are added like crypto ikev2 pofiles and policies, multiple interface starting with Tunnel1xxxxx, vrf defination 65530, ip sdwan route vrf 1 0.0.0.0/0 service sig.

All of these changes are part of the IPsec SIG tunnels with Zscaler.

This example shows how the configuration for the Tunnel interface looks:

```
interface Tunnel100001
     no shutdown
     ip unnumbered       GigabitEthernet1
     no ip clear-dont-fragment
     ip mtu              1400
     tunnel source GigabitEthernet1
     tunnel destination dynamic
     tunnel mode ipsec ipv4
     tunnel protection ipsec profile if-ipsec1-ipsec-profile
     tunnel vrf multiplexing
```

After configurations are pushed successfully onto the Cisco Edge Routers you can use commads to verify whether the tunnels are comming up or not.

<#root>

```
Router#show sdwan secure-internet-gateway zscaler tunnels
```

```
HTTP

TUNNEL IF                                                TUNNEL

RESP

NAME          TUNNEL NAME                                ID        FQDN           TUNNEL FSM STATE

CODE

-------------------------------------------------------------------------------------------------------------
Tunnel100001  site<removed>Tunnel100001             <removed>   <removed>     add-vpn-credential-info  +

200

Tunnel100002  site<removed>Tunnel100002              <removed>  <removed>     add-vpn-credential-info  +

200
```

If you do not see **http resp code 200**, it means that you are facing an issue concerned with password or the partner key.

To verify the interfaces status use the command.

```
<#root>

Router#

show ip interface brief

Interface              IP-Address      OK? Method Status    Protocol
GigabitEthernet1       10.2.234.146    YES DHCP   up            up
GigabitEthernet2       10.2.58.221     YES other  up            up
GigabitEthernet3       10.2.20.77      YES other  up            up
GigabitEthernet4       10.2.248.43     YES other  up            up
Sdwan-system-intf      10.10.10.221    YES unset  up            up
Loopback65528          192.168.1.1     YES other  up            up

Loopback65530          192.168.0.2     YES other  up            up   <<< This is the IP that you used or

NVI0                   unassigned      YES unset  up            up
Tunnel2                10.2.58.221     YES TFTP   up            up
Tunnel3                10.2.20.77      YES TFTP   up            up

Tunnel100001           10.2.58.221     YES TFTP   up            up


Tunnel100002           10.2.58.221     YES TFTP   up            up
```

To verify the status of the tracker, execute the commands **show endpoint-tracker** and **show endpoint-**

tracker records. This helps you confirm the URL that the tracker is utilizing

```
Router#show endpoint-tracker
Interface              Record Name            Status          RTT in msecs    Probe ID        Next Hop
Tunnel100001           #SIGL7#AUTO#TRACKER    Up              194             44              None
Tunnel100002           #SIGL7#AUTO#TRACKER    Up              80              48              None
```

```
Router#show endpoint-tracker records
Record Name            Endpoint                              EndPoint Type   Threshold(ms)    Multiplier
#SIGL7#AUTO#TRACKER    http://gateway.<removed>.net/vpnt API_URL         1000             2
```

Other validations you can do are:
To ensure that routes on VRF are pointing to IPsec tunnels, run this command:

show ip route vrf 1

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 [2/65535], Tunnel100002
[2/65535], Tunnel100001
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

To valiate even further, you can ping towards internet and do a trace route to check the hops that traffic is taking:

<#root>

```
Router#
```

ping vrf 1 cisco.com

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to <removed>, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 406/411/417 ms
```

<#root>

```
Router1#
```

traceroute vrf 1 cisco.com

```
Type escape sequence to abort.
Tracing the route to redirect-ns.cisco.com (<removed>)
VRF info: (vrf in name/id, vrf out name/id)
1 * * *
2
```

<The IP here need to be Zcaler IP>

```
 195 msec 193 msec 199 msec
3
```

<The IP here need to be Zcaler IP>

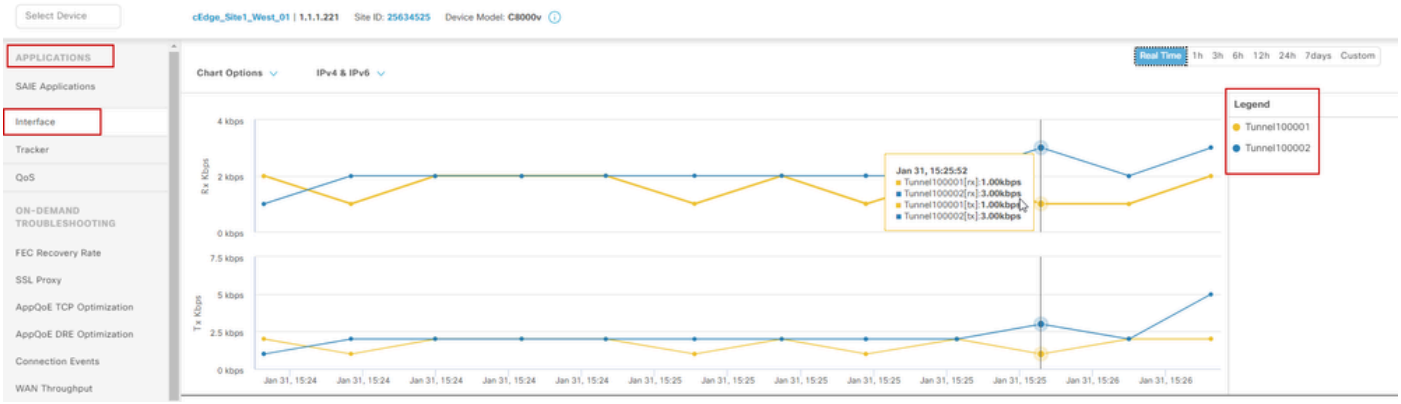
```
 200 msec
```

<The IP here need to be Zcaler IP>

```
 199 msec *
.....
```

You can validate IPsec interfaces from vManage GUI by navigating on **Monitor > Device** or **Monitor > Network** (for codes 20.6 and early).

- Select your router and navigate **Applications > Interfaces.**
- Select **Tunnel100001** and **Tunnel100002** to see the real time traffic or customize per required time frame:



Monitoring IPsec Tunnels

Troubleshoot

If the SIG tunnel are not running, here are the few steps to troubleshoot the problem.

Step 1: Check the errors using the command **show sdwan secure-internet-gateway zscaler tunnels**. From the output, if you notice **HTTP RESP Code 401**, it indicates that there is an issue with authentication.

You can verify the values in the SIG Credentials template to see if the password, or Partner Key, is correct.

<#root>

```
Router#
```

show sdwan secure-internet-gateway zscaler tunnels

HTTP

```
TUNNEL IF                                TUNNEL                                LOCATION
RESP

NAME TUNNEL             NAME                ID        FQDN   TUNNEL FSM STATE      ID        LOCATION FS
LAST HTTP REQ

CODE

-------------------------------------------------------------------------------------------------------------
Tunnel100001   site<removed>Tunnel100001   0                tunnel-st-invalid  <removed>  location-init
req-auth-session      401

Tunnel100002   site<removed>Tunnel100002   0                tunnel-st-invalid  <removed>  location-init
req-auth-session      401

Tunnel100011   site<removed>Tunnel100011   0                tunnel-st-invalid  <removed>  location-init
req-auth-session      401

Tunnel100012   site<removed>Tunnel100012   0                tunnel-st-invalid  <removed>  location-init
req-auth-session      401
```

For further debugging, enable these commands, and search for log messages related to SIG, HTTP, or tracker:

- **debug platform software sdwan ftm sig**
- **debug platform software sdwan sig**
- **debug platform software sdwan tracker**
- **debug platform software sdwan ftm rtm-events**

This is an example of output from debug commands:

<#root>

```
Router#
show logging | inc SIG

Jan 31 19:39:38.666: ENDPOINT TRACKER: endpoint tracker SLA already unconfigured: #SIGL7#AUTO#TRACKER
Jan 31 19:39:38.669: ENDPOINT TRACKER: endpoint tracker SLA already unconfigured: #SIGL7#AUTO#TRACKER
Jan 31 19:59:18.240: SDWAN INFO:
 Tracker entry Tunnel100001/#SIGL7#AUTO#TRACKER state => DOWN

Jan 31 19:59:18.263: SDWAN INFO: Tracker entry Tunnel100002/#SIGL7#AUTO#TRACKER state => DOWN
```

```
Jan 31 19:59:18.274: SDWAN INFO: Tracker entry Tunnel100011/#SIGL7#AUTO#TRACKER state => DOWN
Jan 31 19:59:18.291: SDWAN INFO: Tracker entry Tunnel100012/#SIGL7#AUTO#TRACKER state => DOWN
```

Run the command **show ip interface brief** and check the tunnels interface **Protocol** if there are showing up or down.

<#root>

```
Router#
```

```
show ip interface brief
```

```
Interface              IP-Address      OK? Method Status    Protocol
GigabitEthernet1       10.2.234.146    YES DHCP   up            up
GigabitEthernet2       10.2.58.221     YES other  up            up
Tunnel100001           10.2.58.221     YES TFTP   up            down


Tunnel100002           10.2.58.221     YES TFTP   up            down
```

After confirming that there are no issues with the Zscaler credentials, you can remove the SIG interface from the device template and push it to the router.

Once the push is completed, apply the SIG template and push it back to the router. This method forces the tunnels to be recreated from scratch.

Related Information

- Cisco Technical Support & Downloads