使用Zscaler配置和验证SD-WAN IPsec SIG隧道

目录

简介

先决条件

- 要求
- 其他要求
- 使用的组件

配置

- 网络设计选项

配置

- 高可用性
- 高级设置

验证

故障排除

从Cisco IOS®版本IOS-XE 17.11+, 已迁移至

相关信息

简介

本文档介绍使用Zscaler配置SD-WAN IPsec SIG隧道的配置步骤和验证。

先决条件

要求

Cisco 建议您了解以下主题：

- 安全互联网网关(SIG)。
- Cisco IOS®上的IPsec隧道的工作方式、第1阶段和第2阶段。

其他要求

- 必须在面向互联网的传输接口上启用NAT。

- 必须在VPN 0上创建DNS服务器，并且必须使用此DNS服务器解析Zscaler基本URL。这一点非常重要，因为如果不解决此问题，API调用和第7层运行状况检查可能会失败。默认情况下，使用此DNS服务器
- NTP（网络时间协议）必须确保Cisco Edge Router时间准确，并且API调用不能失败。
- 必须在服务VPN功能模板或CLI中配置指向SIG的服务路由：ip sdwan route vrf 1 0.0.0.0/0 service sig

使用的组件

本文档基于以下软件和硬件版本：

- 思科边缘路由器版本17.6.6a
- vManage版本20.9.4

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络设计选项

此列表中的各种部署类型是主用/备用组合设置。隧道封装可以与GRE或IPsec一起部署。

- 一个主用/备用隧道对
- 一个主用/主用隧道对
- 多个主用/备用隧道对
- 多个主用/主用隧道对

注意：在SD-WAN思科边缘路由器上，您可以使用一个或多个连接到Internet的传输接口，以使设置有效运行。

配置

继续配置以下模板：

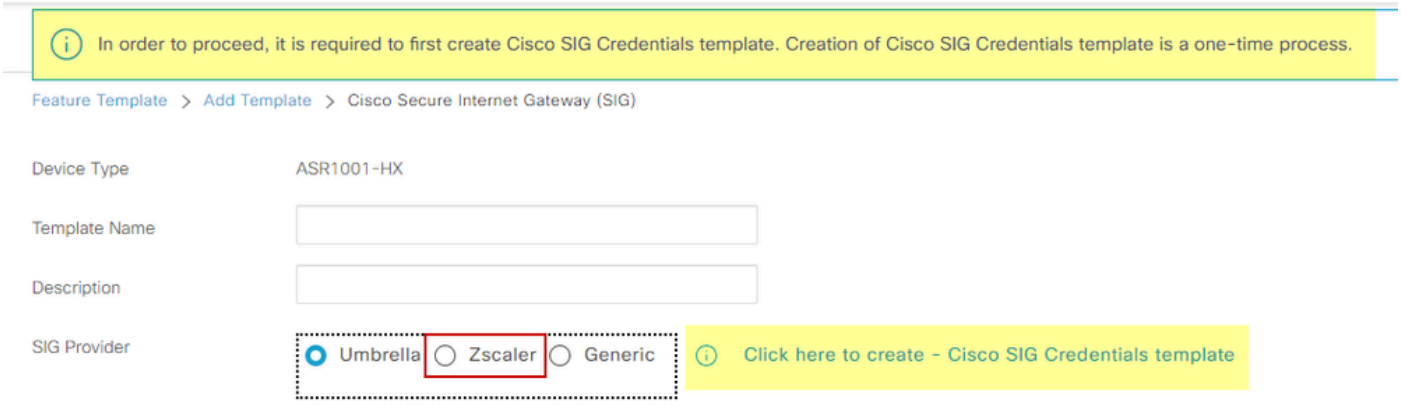
- 安全互联网网关(SIG)凭证功能模板：
  - 所有思科边缘路由器都需要一台。必须在Zscaler门户上创建用于填充模板必要字段的信息。

- 安全互联网网关(SIG)功能模板：
  - 在此功能模板下，您可以配置IPsec隧道，确保在主用/主用或主用/备用模式下部署高可用性(HA)，然后选择Zscaler Data-Center enter（自动或手动输入）。

1.要创建Zscaler凭证模板，请导航至配置 > 模板 > 功能模板 > 添加模板。

2.选择要用于此目的的设备型号，然后搜索SIG。首次创建时，系统显示必须先创建Zscaler凭证，如下例所示：

3.您必须选择Zscaler作为SIG Provider，然后单击Click here to create - Cisco SIG Credentials template。



签名凭证模板

4.系统会将您重定向至凭证模板。您必须为所有字段输入值：

- 模板名称
- 描述
- SIG提供程序（自动从上一步中选择）
- 组织
- 合作伙伴基础URL
- 用户名
- 密码
- 合作伙伴API密钥

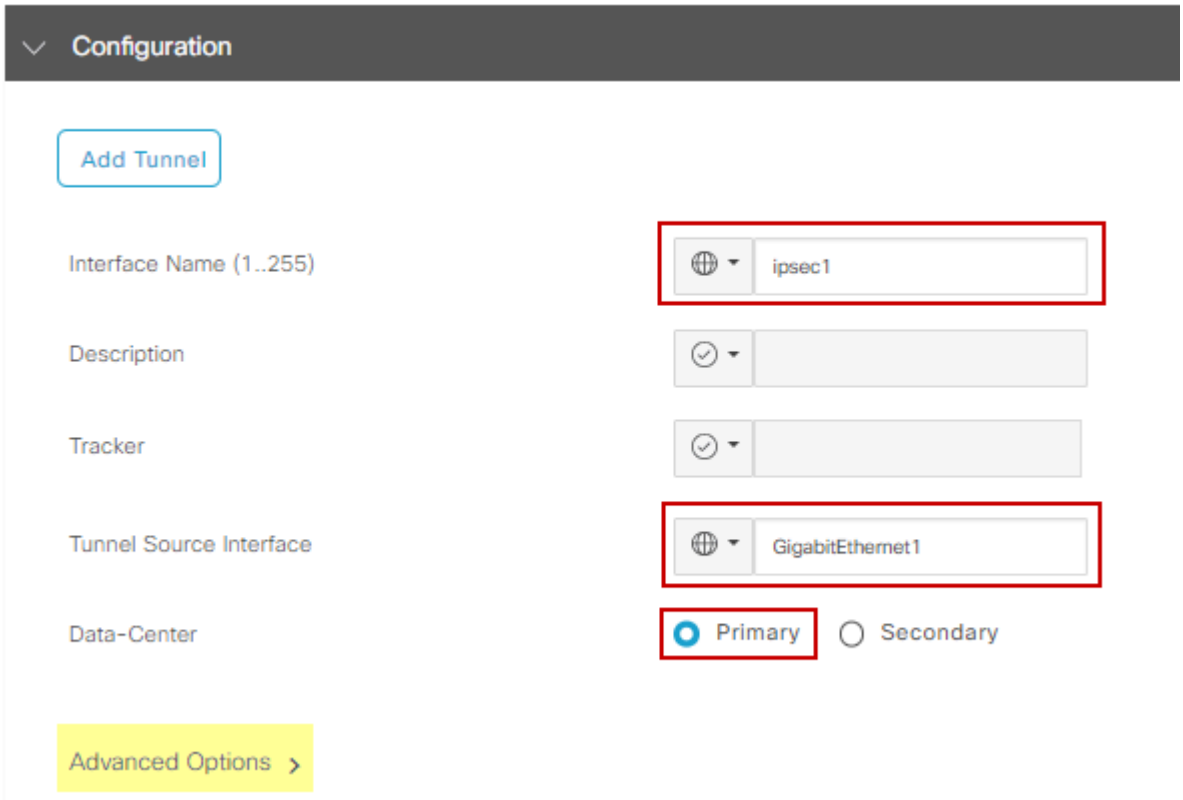
5.单击保存。

6.系统会将您重定向到安全互联网网关(SIG)模板。此模板允许您使用Zscaler配置SD-WAN IPsec SIG所需的项目。

在模板的第一部分，提供名称和说明。默认跟踪器会自动启用，并使用Zscaler Layer 7 Health Check的API URL。

7.在Cisco IOS XE中，必须为跟踪器设置IP地址。/32范围内的任何私有IP都是可接受的。Loopback 6530接口可以使用您设置的IP地址，该接口是自动创建的，用于执行Zscaler运行状况检查。

8.在Configuration部分下，您可以点击Add Tunnel创建IPsec隧道。在新弹出窗口中，根据要求进行选择。
9.在本示例中，已使用WAN接口GigabitEthernet1作为隧道源创建了接口IPsec1。它与主Zcaler数据中心建立连接。建议将Advanced Options值保留为默认值。

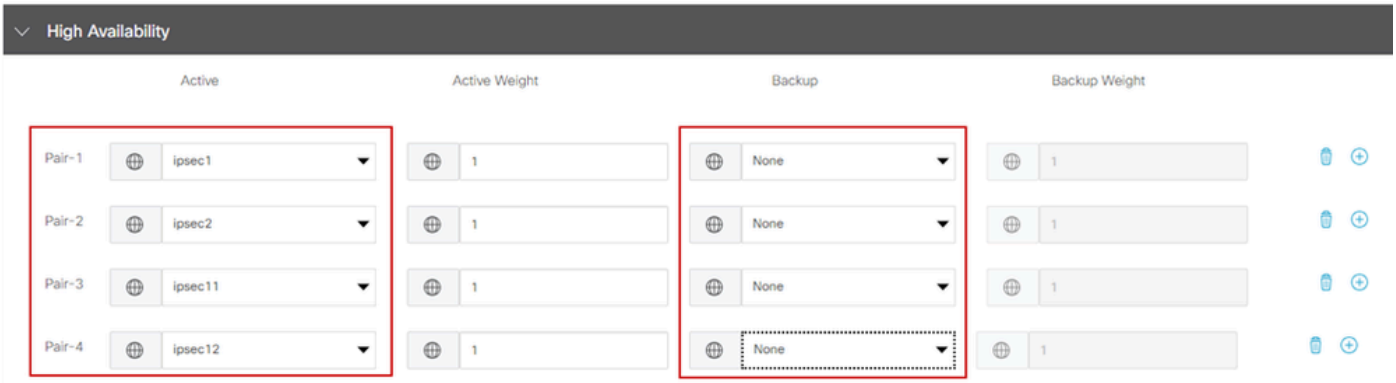


IPsec接口配置

高可用性

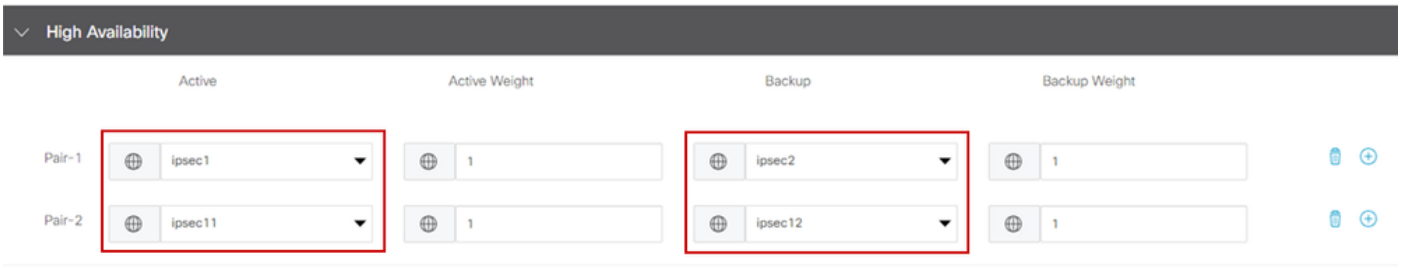
在本节中，选择设计是主用/主用还是主用/备用，并确定哪个IPsec接口处于主用状态。

这是一个“活动/活动”设计的示例，所有接口都在活动下选择，并使Backup保留为无。



主用/主用设计

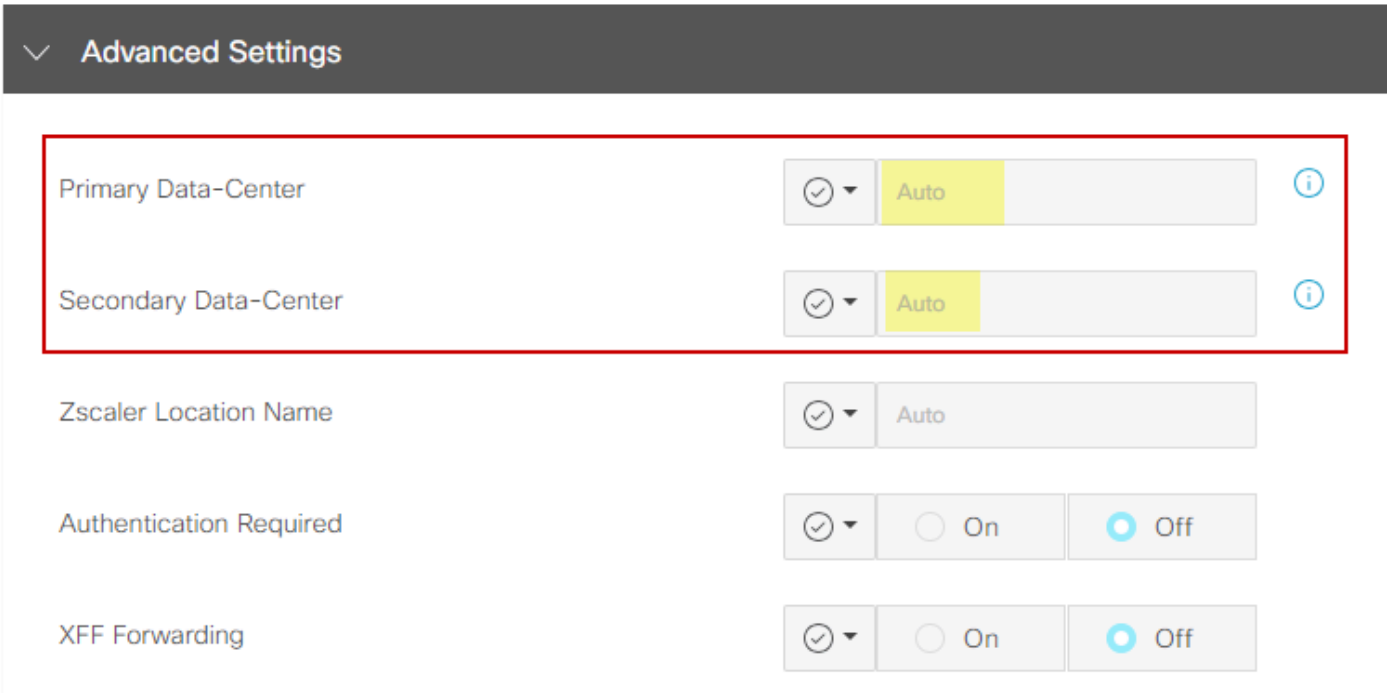
本示例显示主用/备用设计，IPsec1和IPsec11被选为主用接口，而IPsec2和IPsec12被指定为备用接口。



主用/备用设计

高级设置

1.在本节中，最重要的配置是主数据中心和辅助数据中心。建议将这两个配置配置为自动或手动，但不建议将它们配置为混合。如果您选择手动配置它们，请根据您的合作伙伴基础URL从Zscaler门户中选择正确的URL。



自动或手动数据中心

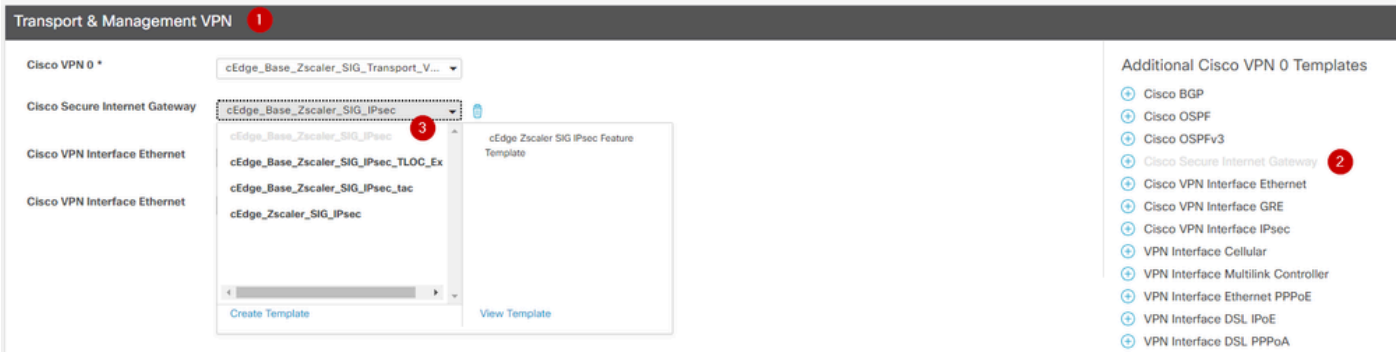
2.完成后，单击Save。

3.完成SIG模板配置后，必须在设备模板下应用它们。这样，配置就会被推送到思科边缘路由器上。

4.后续步骤，导航到配置>模板>设备模板，在三个点上单击编辑。

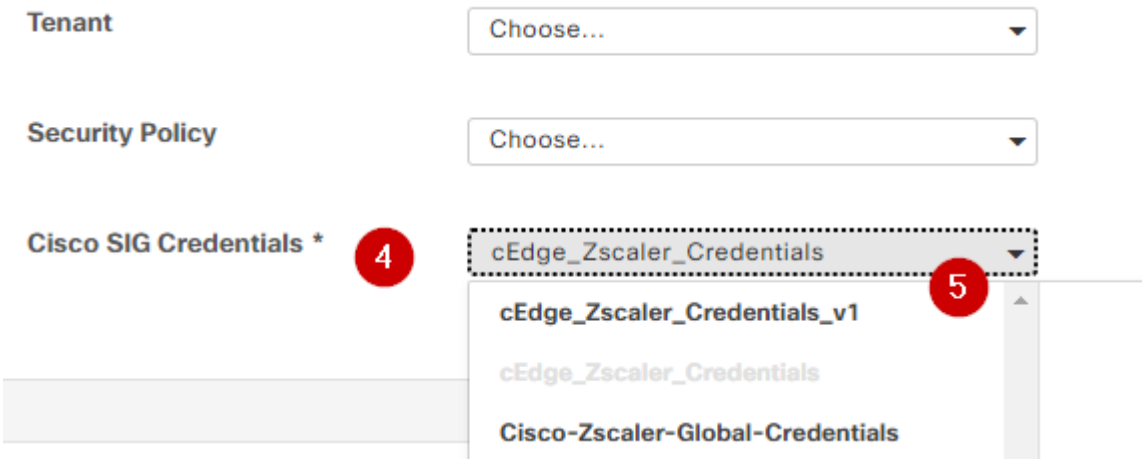
5.在Transport & Management VPN下，添加Secure Internet Gateway模板。

6.在Cisco Secure Internet Gateway上，从下拉菜单中选择正确的SIG功能模板。



在设备模板上添加SIG模板

7.在Cisco SIG凭证中的其他模板下，从下拉菜单中选择正确的Cisco SIG凭证模板：



凭证SIG模板

8.单击更新（如果您的设备模板是活动模板，请使用标准步骤在活动模板上推送配置）。

验证

1.在推送更改时，可以在配置预览期间完成验证，您必须注意以下事项：

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

2.在本例中，您可以看到设计是主用/备用的：

<#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
```

3.添加其他配置，例如crypto ikev2 pofiles and policies，多个接口以Tunnel1xxxxx、vrf definition 65530和ip sdwan route vrf 1 0.0.0.0/0 service sig开头。所有这些更改都是使用Zscaler的IPsec SIG隧道的一部分。

此示例显示隧道接口的配置外观：

```
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
```

4.将配置成功推送到思科边缘路由器后，您可以运行命令来验证隧道是否可用：

<#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
```

5.如果未看到http响应代码200，则意味着您面临密码或合作伙伴密钥的问题。

6.要验证接口状态，请使用以下命令：

<#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
```

7.要验证跟踪器的状态，请运行show endpoint-tracker和show endpoint-tracker records命令。这有助于您确认跟踪器正在使用哪个URL:

```
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.


      .net/vpnt API_URL         1000            2            30              interface
```

8.您可以使用的其他验证包括：

- 确保VRF上的路由指向IPsec隧道并运行以下命令：

  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]，隧道100002
[2/65535]，隧道100001
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

9.要进一步验证，您可以向Internet发出ping命令，并完成跟踪路由以验证流量的跳数：

<#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
```

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

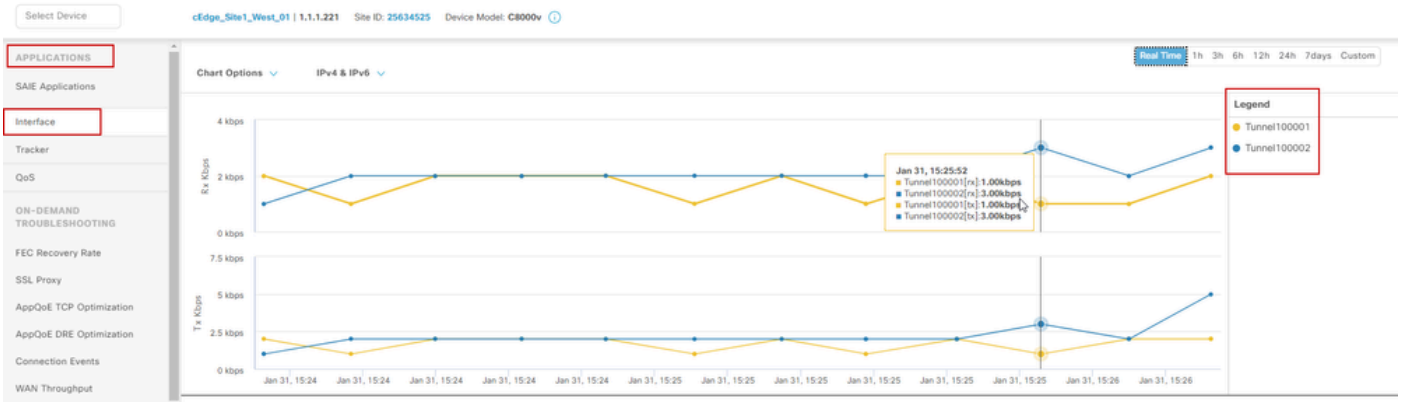
```
 200 msec



 199 msec *
.....
```

10.通过导航到Monitor > Device或Monitor > Network（用于代码20.6及早期版本），可以从vManage GUI验证IPsec接口。

- 选择路由器并导航到应用>接口。
- 选择Tunnel10001和Tunnel10002以查看实时流量或按所需时间帧自定义实时流量：



监控IPsec隧道

故障排除

如果SIG隧道未运行，请查看以下步骤进行故障排除：

步骤 1：通过运行命令show sdwan secure-internet-gateway zscaler tunnels检查错误。从输出中，如果您注意到HTTP RESP代码401，则表明存在身份验证问题。您可以验证SIG凭证模板中的值，以查看密码或合作伙伴密钥是否正确。

<#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 F

LAST HTTP REQ

CODE

Tunnel100001 site<removed>Tunnel100001 0 tunnel-st-invalid <removed> location-ini

req-auth-session 401

Tunnel100002 site<removed>Tunnel100002 0 tunnel-st-invalid <removed> location-ini

req-auth-session 401

Tunnel100011 site<removed>Tunnel100011 0 tunnel-st-invalid <removed> location-ini

req-auth-session 401

Tunnel100012 site<removed>Tunnel100012 0 tunnel-st-invalid <removed> location-ini

req-auth-session 401

步骤2.要进一步调试，请启用这些命令并搜索与SIG、HTTP或跟踪器相关的日志消息：

- debug platform software sdwan ftm sig
- debug platform software sdwan sig
- 调试平台软件sdwan跟踪器
- 调试平台软件sdwan ftm rtm-events

从Cisco IOS®版本IOS-XE 17.11+,<debug platform>已迁移到<set platform trace>

set platform software trace ftmd R0 ftmd-sig [debug | verbose]

set platform software trace ios R0 sdwanrp-sig debug

set platform software trace ios R0 sdwanrp-tracker debug

set platform software trace ftmd R0 ftmd-rtm [debug | verbose]

1.以下是debug命令的输出示例：

<#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
```

2.运行命令show ip interface brief，检查隧道接口Protocol，并检查这些隧道是否显示或关闭。

<#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
```

3.确认Zscaler凭证不存在问题后，从设备模板中删除SIG接口并将其推送到路由器。推送完成后，应用SIG模板并将其推回路由器。此方法强制从零开始重新创建隧道。

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。