# 使用Zscaler配置和验证SD-WAN IPsec SIG隧道

## 目录



## 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)。
- IPsec隧道的工作方式，Cisco IOS®上的第1阶段和第2阶段。

#### 其他要求

- 需要在面向互联网的传输接口上启用NAT。
- 需要在VPN 0上创建DNS服务器，并且需要用此DNS服务器解析Zscaler基本URL。这一点很重要，因为如果不解决此问题，API调用将失败。第7层运行状况检查也会失败，因为默认情况下，URL为：http://gateway.<zscalercloud>.net/vpntest。
- NTP（网络时间协议）必须确保Cisco Edge路由器时间准确，并且API调用不会失败。
- 需要在服务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

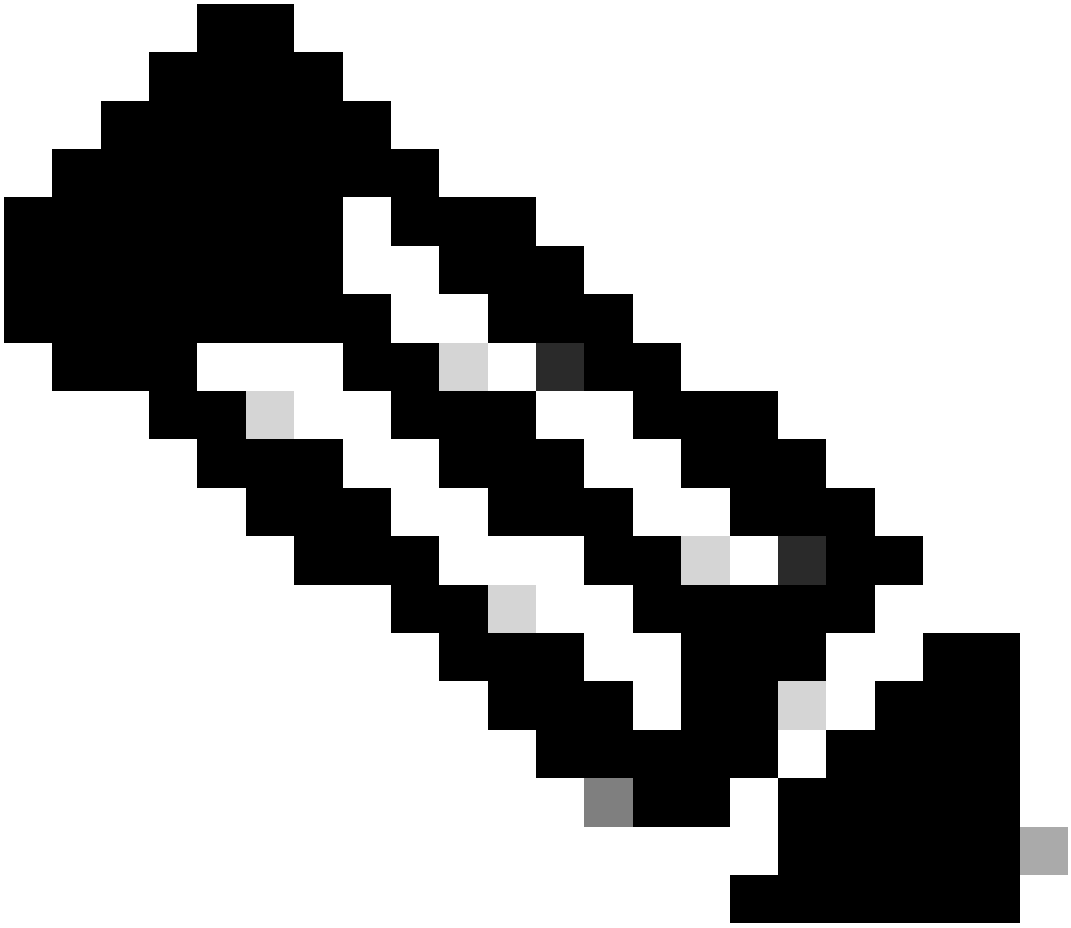
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 配置

### 网络设计选项

以下是主用/备用组合设置中的各种部署类型。隧道封装可以部署GRE或IPsec。

- 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。
- 多个活动/活动隧道对。



注意：在SD-WAN Cisco Edge路由器上，可以利用连接到互联网的一个或多个传输接口，以使这些设置有效运行。

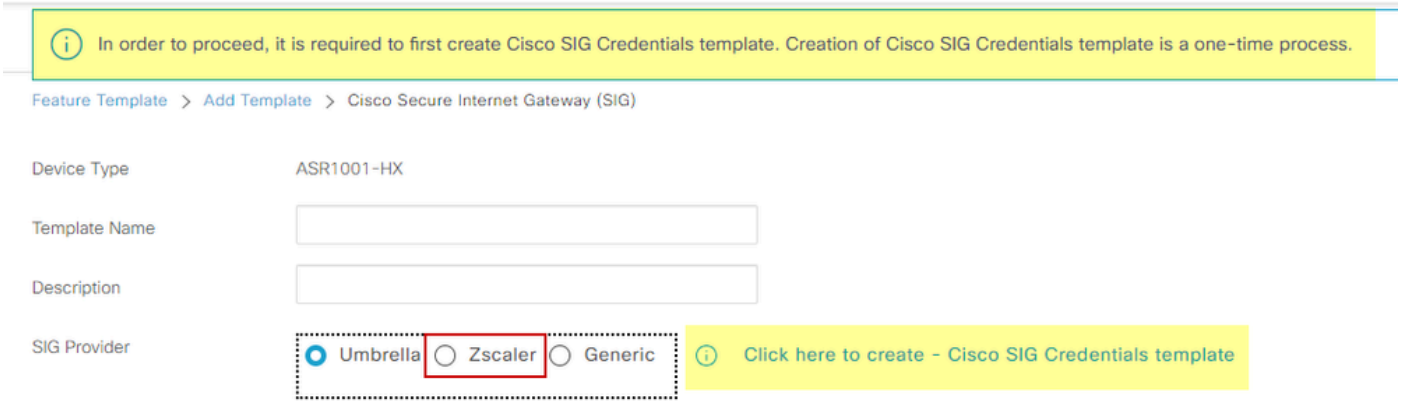
# 配置

继续配置这些模板：

- 安全互联网网关(SIG)凭证功能模板：
  - 所有云翼路由器均需要此配置。需要在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)，并自动或手动选择Zscaler Datacenter。

要创建Zscaler Credentials模板，请导航到配置>模板>功能模板>添加模板。

选择要用于此目的的设备型号并搜索SIG。首次创建时，系统显示需要首先创建Zscaler凭证，如下例所示：
您需要选择Zscaler作为SIG提供商，然后单击Click here to create - Cisco SIG Credentials template。




签名凭证模板

”

系统会将您重定向到“凭证”模板。在此模板上，必须输入所有字段的值：

- 模板名称
- 描述
- SIG提供程序（从上一步自动选择）
- 组织
- 合作伙伴基础URI
- 用户名
- 密码
- 合作伙伴API密钥

Click Save.

系统会将您重定向至安全互联网网关(SIG)模板。此模板允许您配置使用Zscaler的SD-WAN IPsec SIG所需的一切内容。

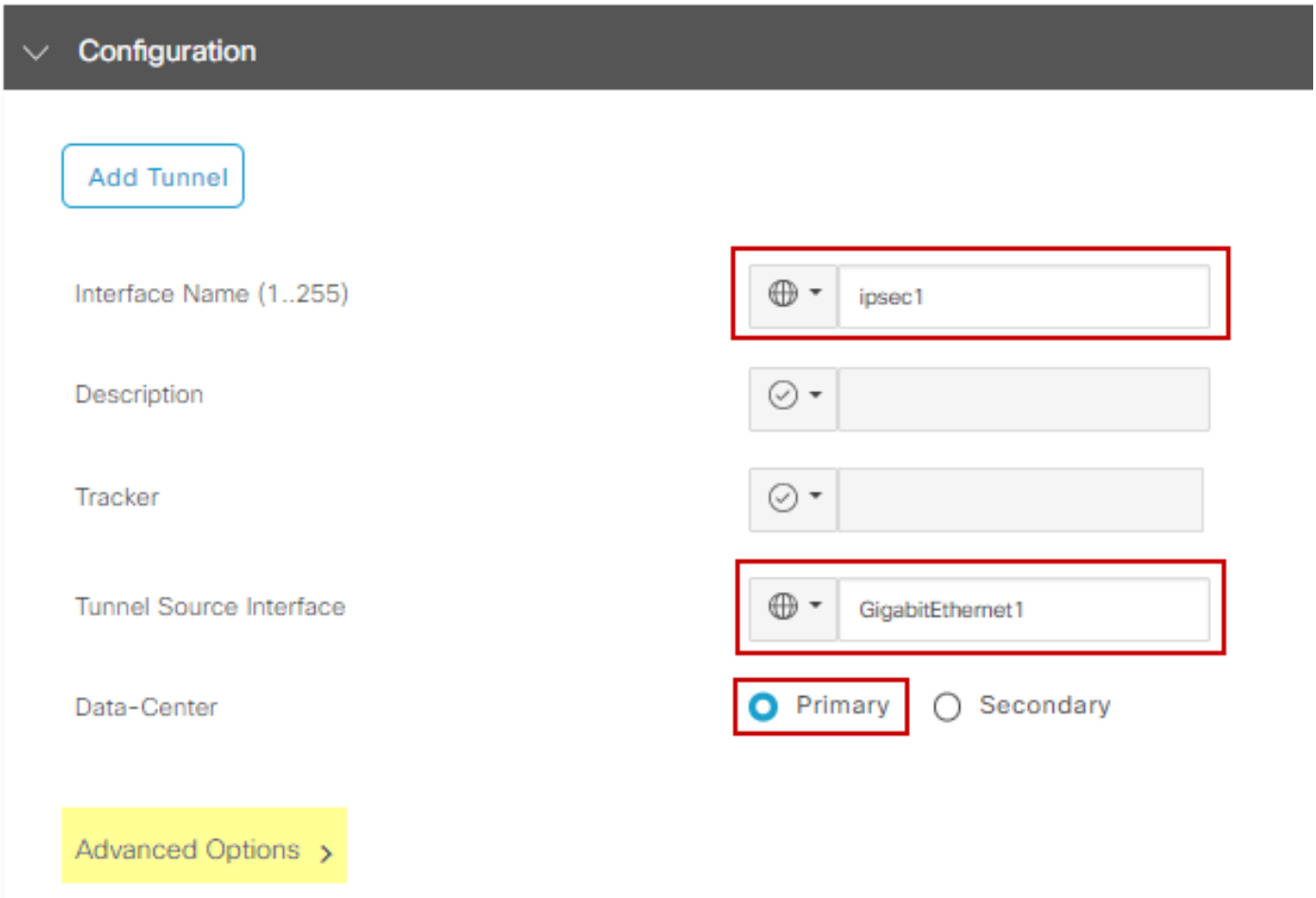
请在模板的第一部分提供名称和说明。默认跟踪器会自动启用。用于Zscaler第7层运行状况检查的API URL为：zscaler_L7_health_check) ishttp://gateway<zscalercloud>net/vpntest。

在Cisco IOS XE中，您需要为跟踪器设置IP地址。/32范围内的任何私有IP都是可以接受的。Loopback 65530接口可以使用您设置的IP地址，该接口会自动创建用于执行Zscaler运行状况检查。

在Configuration部分下，您可以单击Add Tunnel创建IPSec隧道。在新弹出窗口中，根据需要进行选择。

在本示例中，已创建接口IPsec1，使用WAN接口GigabitEthernet1作为隧道源。然后，它可以与主Zcaler数据中心建立连接。

建议将Advanced Options值保留为默认值。

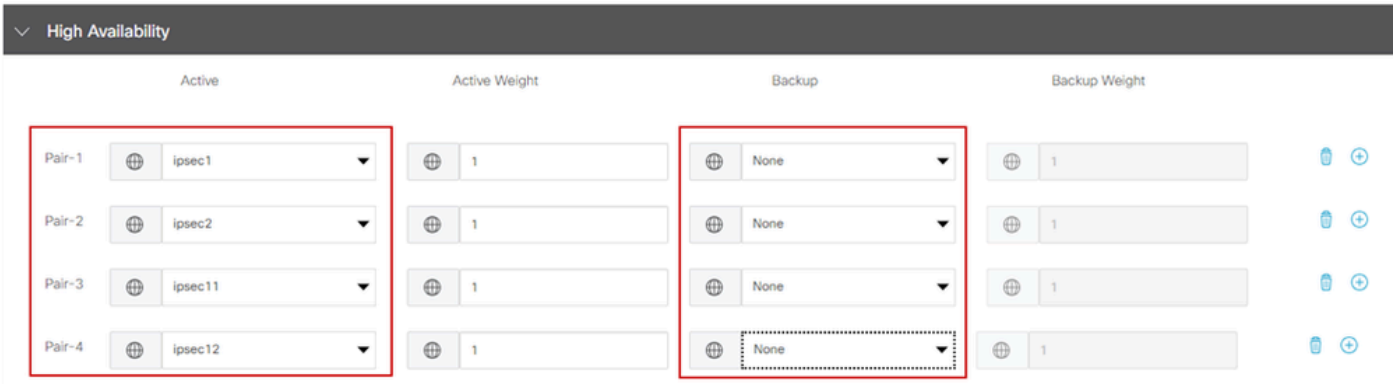



IPsec接口配置

## 高可用性

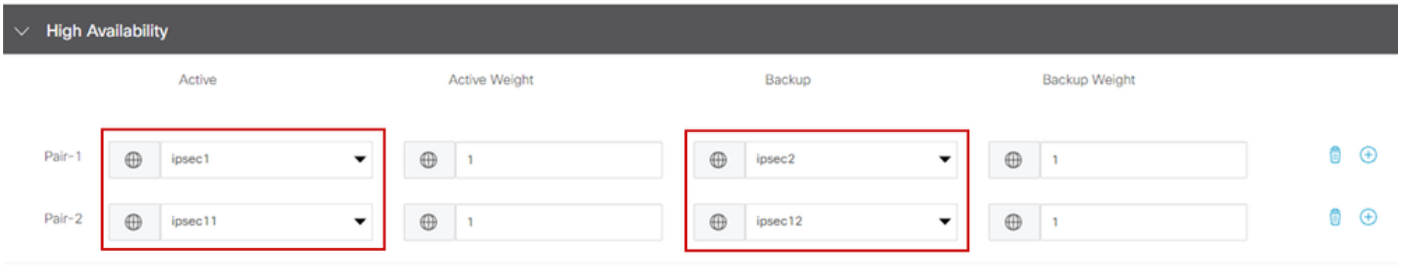
在本节中，您可以选择设计是主用/主用还是主用/备用，并确定哪个IPsec接口将处于主用状态。

这是一个“主用/主用”设计的示例。所有接口都在Active下选择，因此将Backup保留为无。




主用/主用设计

本示例展示的是主用/备用设计。选择IPsec1和IPsec11作为主用接口，而选择IPsec2和IPsec12作为备用接口。



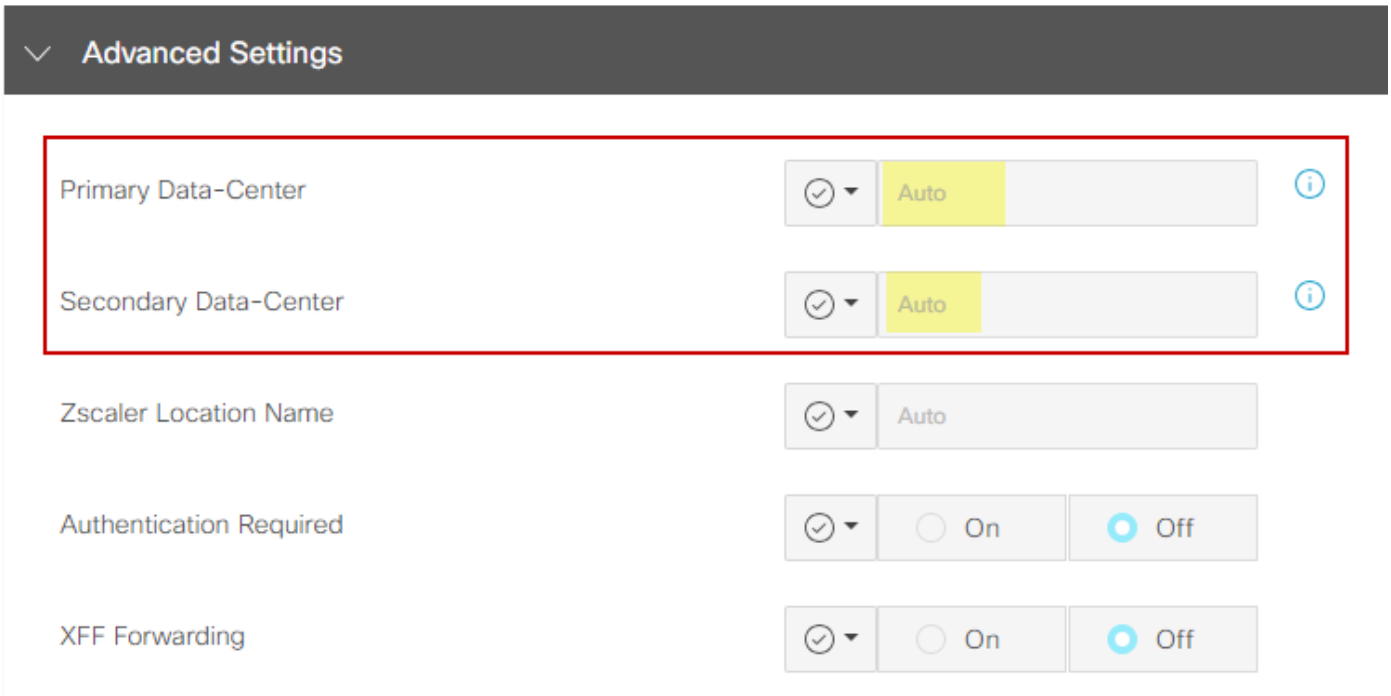

主用/备用设计

## 高级设置

在本部分中，最重要的配置是主数据中心和辅助数据中心。

建议将两者都配置为自动或手动，但不建议将它们配置为混合。

如果您选择手动配置，请根据您的合作伙伴基础URI，从Zscaler门户中选择正确的URL




自动或手动数据中心

完成后，单击Save。

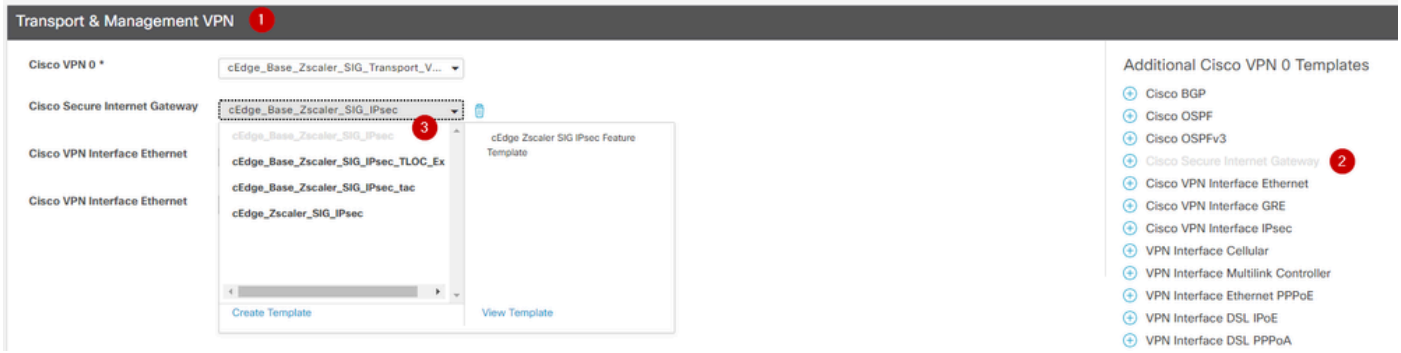
完成SIG模板配置后，必须在设备模板下应用它们。通过这种方式，配置会被推送到云翼路由器。

要完成这些步骤，请导航到配置>模板>设备模板，点击三点编辑。

1. 在传输和管理VPN下

2. 添加安全Internet网关模板。

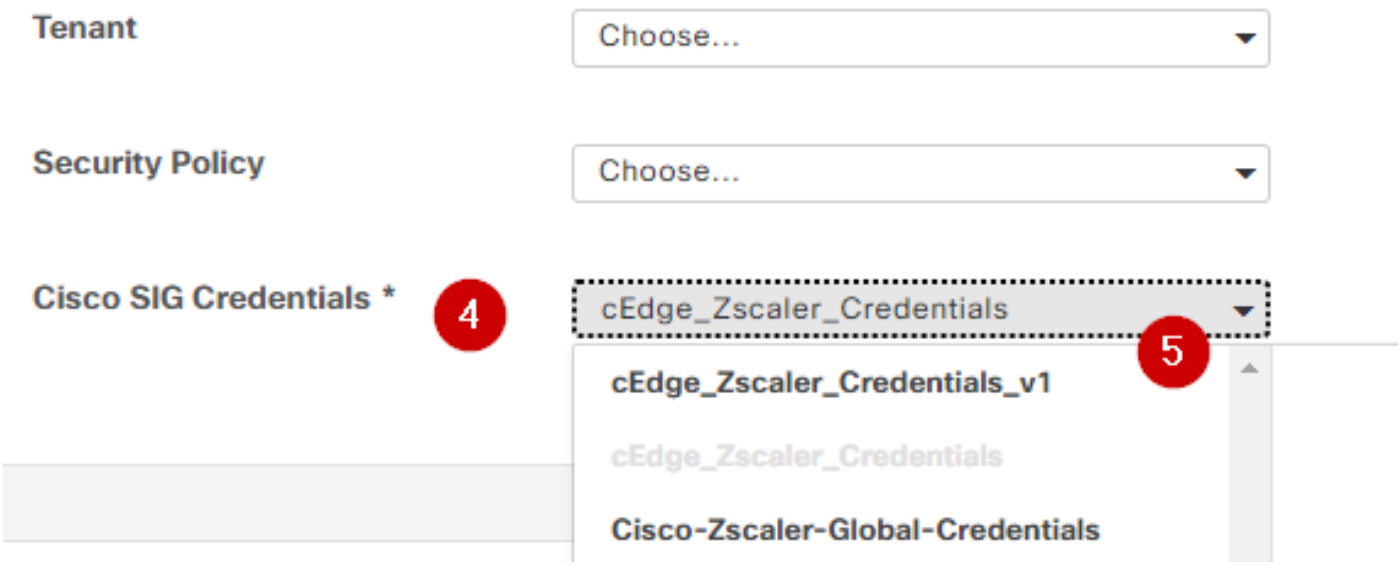
3. 在Cisco安全Internet网关上，从下拉菜单中选择正确的SIG功能模板。




在设备模板上添加SIG模板

在Additional Templates下

4. 在Cisco SIG凭证中
5.从下拉菜单中选择正确的Cisco SIG Credentials模板：




凭证SIG模板

单击Update，请注意您的设备模板是否为活动模板，请使用标准步骤在活动模板上推送配置。

# 验证

在推送更改时，可以在配置预览期间进行验证，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>
    !
```

从本示例中可以看到，设计为主用/备用

<#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
```

您将看到添加了更多配置，例如crypto ikev2 pofiles and policies、多个以Tunnel1xxxxx开头的接口、vrf definition 65530、ip sdwan route vrf 1 0.0.0.0/0 service sig。

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如下所示：

```
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
```

配置成功推送到云翼路由器后，您可以使用命令验证隧道是否打开。

<#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
```

如果未看到http resp code 200，则意味着您面临着与密码或合作伙伴密钥有关的问题。

使用命令检验接口状态。

```
<#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
```

要验证跟踪器的状态，请执行show endpoint-tracker和show endpoint-tracker records命令。这有助于您确认跟踪器正在使用的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.<removed>.net/vpnt API_URL         1000             2
```

您可以执行的其他验证包括：
要确保VRF上的路由指向IPsec隧道，请运行此命令：

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

要进一步验证，可以向internet发出ping命令，并执行跟踪路由以检查流量所采用的跳数：

<#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
```

**<The IP here need to be Zcaler IP>**

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

**<The IP here need to be Zcaler IP>**

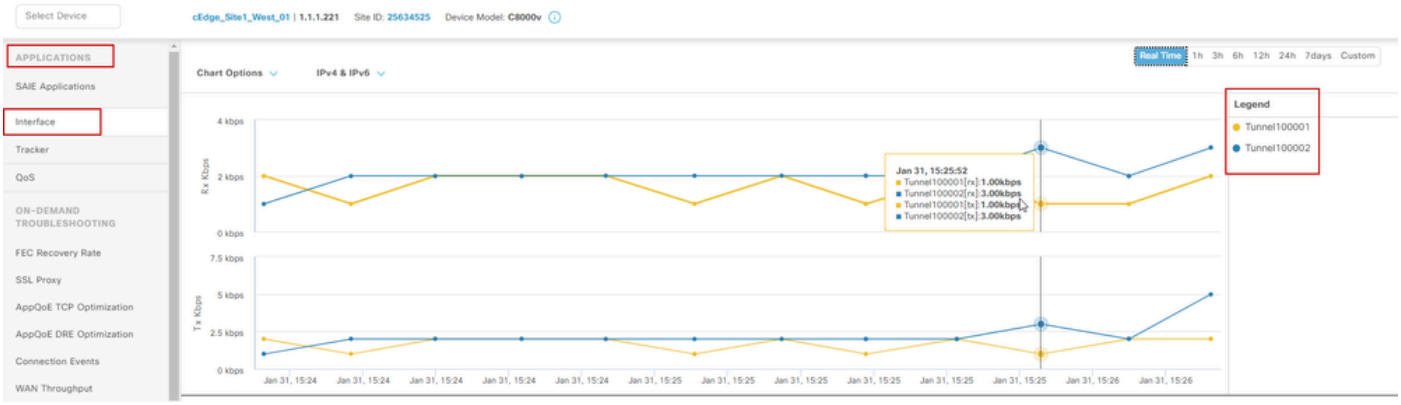
200 msec

**<The IP here need to be Zcaler IP>**

199 msec *
.....

您可以导航到Monitor > Device或Monitor > Network（针对代码20.6及更早版本）来从vManage GUI验证IPsec接口。

- 选择路由器并导航Applications > Interfaces。
- 选择Tunnel100001和Tunnel100002以查看实时流量或根据所需时间范围进行自定义：



监控IPsec隧道

# 故障排除

如果SIG隧道未运行，以下是几个故障排除步骤。

第1步：使用命令show sdwan secure-internet-gateway zscaler tunnels检查错误。从输出中，如果您注意到HTTP响应代码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 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
```

为了进一步调试，请启用以下命令，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
- debug platform software sdwan tracker
- 调试平台软件sdwan ftm rtm-events

下面是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
```

运行命令show ip interface brief，并检查隧道接口协议（如果显示）是打开还是关闭。

<#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** |

在确认Zscaler凭证没有问题之后，您可以从设备模板中删除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。此方法强制从头开始重新创建隧道。

# 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）。