使用Zscaler配置和驗證SD-WAN IPsec SIG隧道

目錄

簡介

本文檔介紹使用Zscaler對SD-WAN IPsec SIG隧道進行配置步驟和驗證。

必要條件

需求

思科建議您瞭解以下主題：

- 安全網際網路閘道(SIG)。
- Cisco IOS®上的Phase1和Phase2中IPsec隧道的工作方式。

其他要求

- 需要在將要面向Internet的傳輸介面上啟用NAT。
- 需要在VPN 0上建立DNS伺服器，並且需要用此DNS伺服器解析Zscaler基本URL。這一點很重要，因為如果不解決這個問題，API呼叫將會失敗。第7層運行狀況檢查也會失敗，因為預設情況下，URL為：http://gateway.<zscalercloud>.net/vpntest。
- NTP（網路時間協定）必須確保Cisco Edge路由器時間準確，並且API呼叫不會失敗。
- 需要在服務VPN功能模板或CLI中配置指向SIG的服務路由：
  ip sdwan route vrf 1 0.0.0.0/0服務簽名

採用元件

本檔案根據這些軟體和硬體版本：

- 思科邊緣路由器版本17.6.6a
- vManage 20.9.4版

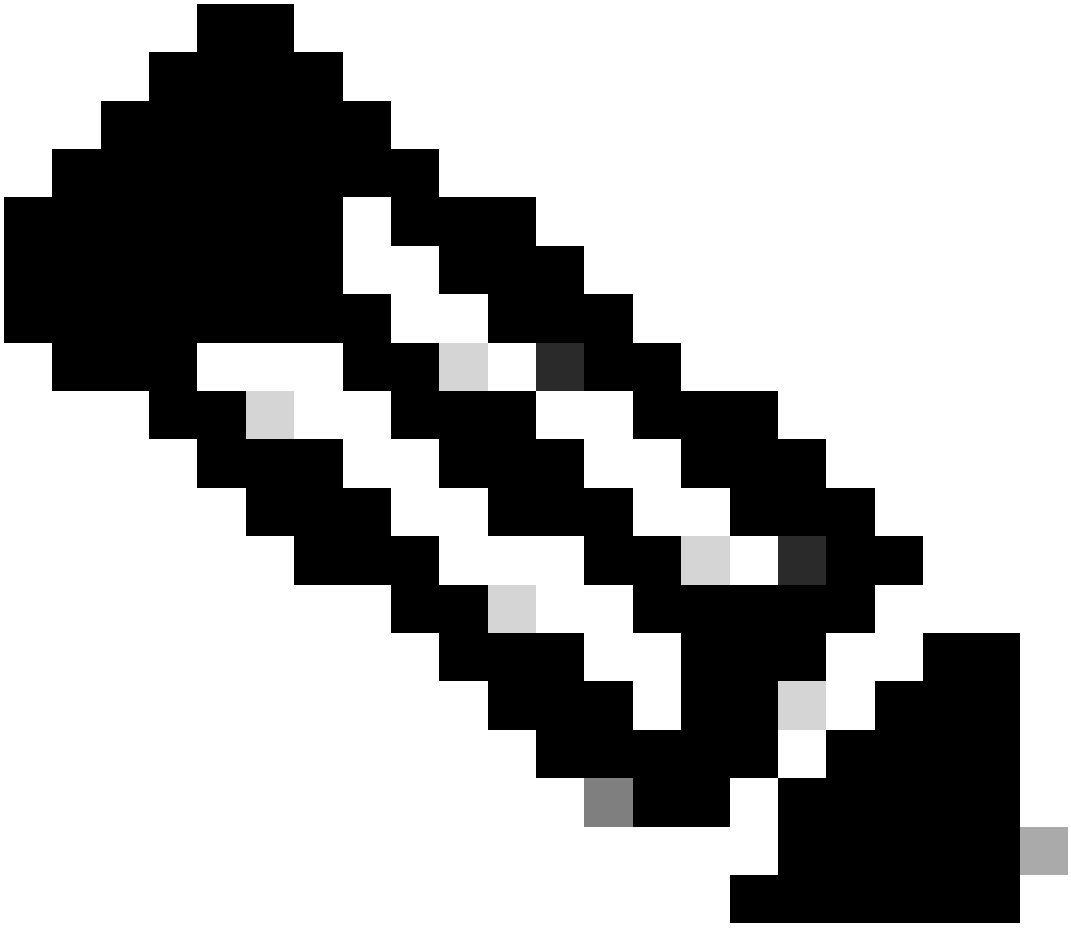
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

網路設計選項

以下是主用/備用組合設定中的各種型別的部署。隧道封裝可以部署GRE或IPsec。

- 一個主用/備用隧道對。
- 一個主用/主用隧道對。
- 多個主用/備用隧道對。
- 多個主用/主用隧道對。



注意：在SD-WAN Cisco Edge路由器上，您可以使用連線到Internet的一個或多個傳輸介面，以便有效地執行這些設定。

組態

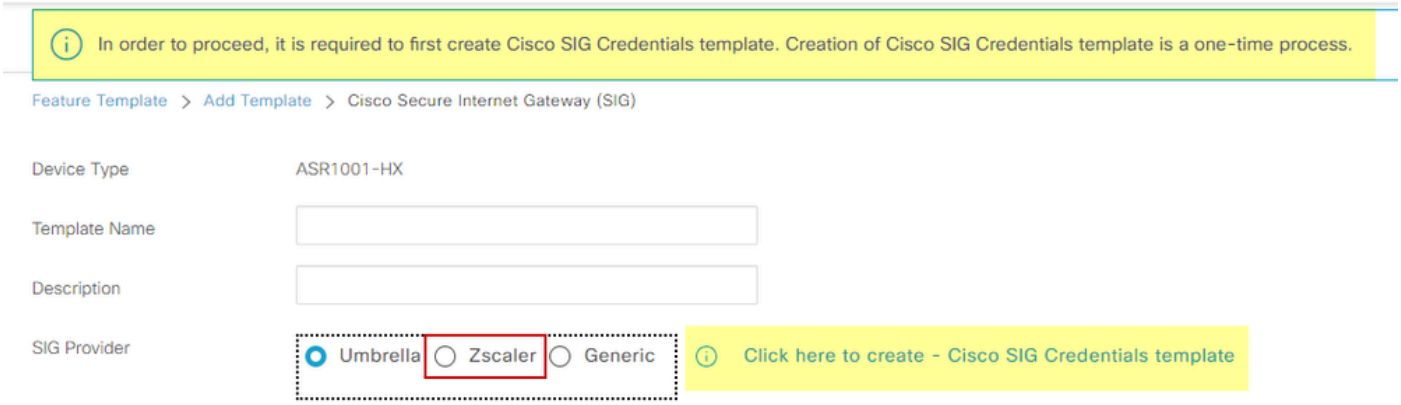
繼續配置以下模板：

- 安全網際網路閘道(SIG)認證功能範本：
  - 所有思科邊緣路由器都需要一台。需要在Zscaler門戶上建立填充模板必要欄位的資訊。
- 安全網際網路閘道(SIG)功能範本：
  - 在此功能模板下，您可以配置IPSec隧道，確保部署高可用性(HA)處於主用/主用或主用/備用模式，然後自動或手動選擇Zscaler Datacenter。

要建立Zscaler Credentials模板，請導航到配置>模板>功能模板>增加模板。

選擇要用於此目的的裝置型號並搜尋SIG。當您首次建立時，系統顯示需要先建立Zscaler證明資料

，如以下範例所示：
您需要選擇Zscaler作為SIG提供商，並且點選點選此處建立- Cisco SIG憑證模板。



Sig Credentila Template

」

系統會將您重新導向至「身份證明」範本。在此範本上，您必須輸入所有欄位的值：

- 範本名稱
- 說明
- SIG提供者（自動從上一個步驟選取）
- 組織
- 合作夥伴基礎URI
- 使用者名稱
- 密碼
- 合作夥伴API金鑰

按一下Save。

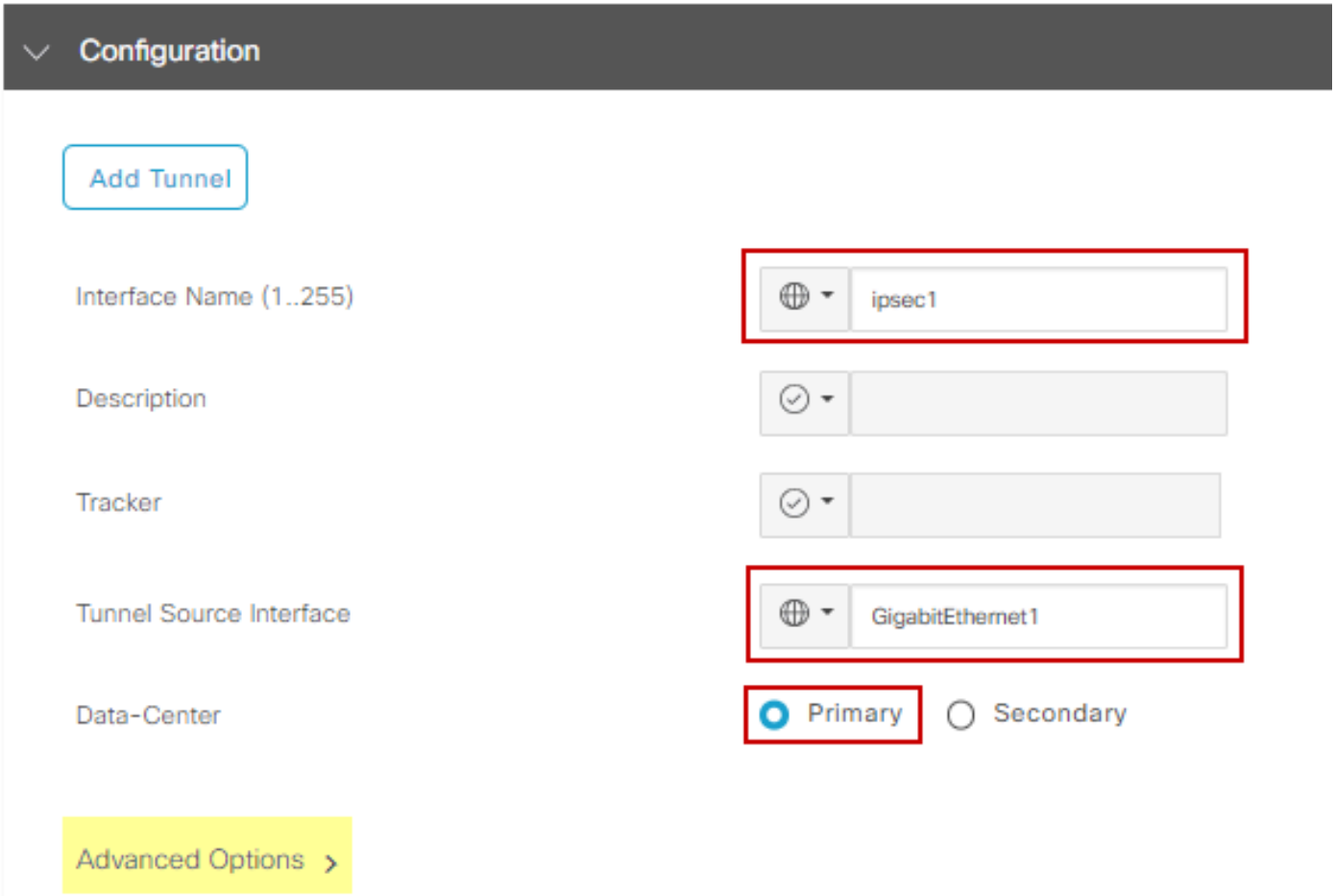
您將被重定向到安全網際網路網關(SIG)模板。此模板允許您配置使用Zscaler的SD-WAN IPsec SIG所需的一切。

在範本的第一部分，請提供名稱和說明。預設追蹤器會自動啟用。用於Zscaler第7層運行狀況檢查的API URL為：zscaler_L7_health_check) ishttp://gateway<zscalercloud>net/vpntest。

在Cisco IOS XE中，您需要為跟蹤器設定IP地址。/32範圍內的任何私有IP都是可接受的。Loopback 65530介面可以使用您設定的IP地址，該介面會自動建立以執行Zscaler運行狀況檢查。

在Configuration部分下，您可以按一下Add Tunnel建立IPSec隧道。在新快顯視窗中，根據您的需求進行選擇。

在本示例中，已使用WAN介面GigabitEthernet1作為隧道源建立介面IPsec1。然後，它可以與Primary Zcaler Data-Center建立連線。
建議將高級選項值保留為預設值。

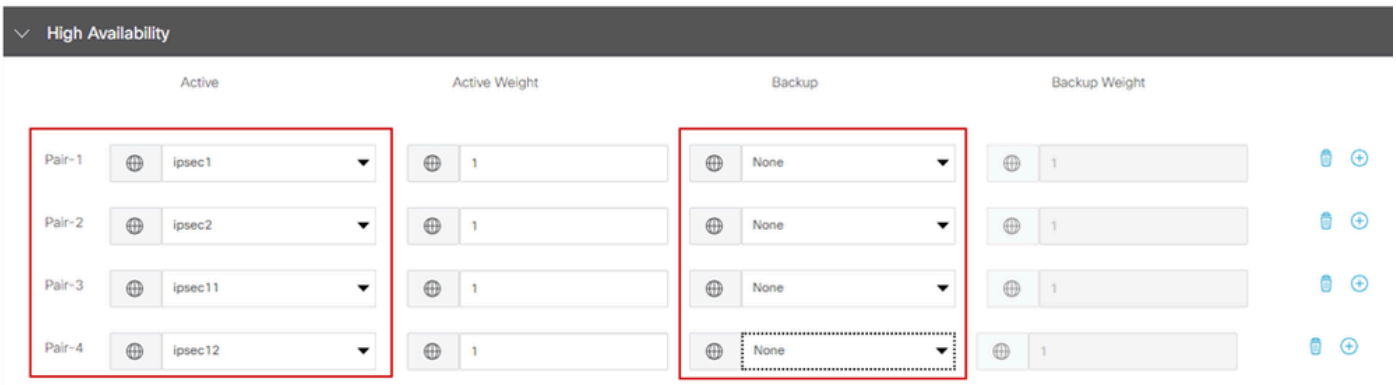


IPsec介面配置

高可用性

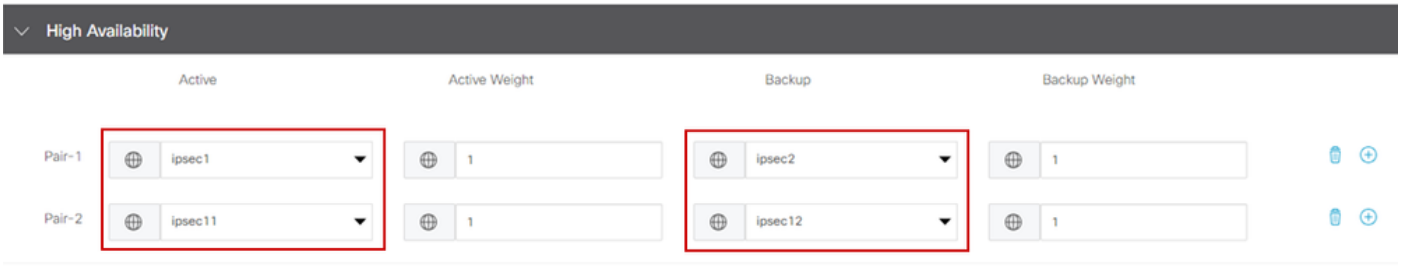
在本節中，您可以選擇設計是主用/主用還是主用/備用，並確定哪個IPSec介面將處於主用狀態。

這是「主動/主動」設計的範例。所有介面都在Active下選擇，因此沒有Backup。



主動/主動設計

此示例顯示了主用/備用設計。IPsec1和IPsec11被選為活動介面，而IPsec2和IPsec12被指定為備用介面。



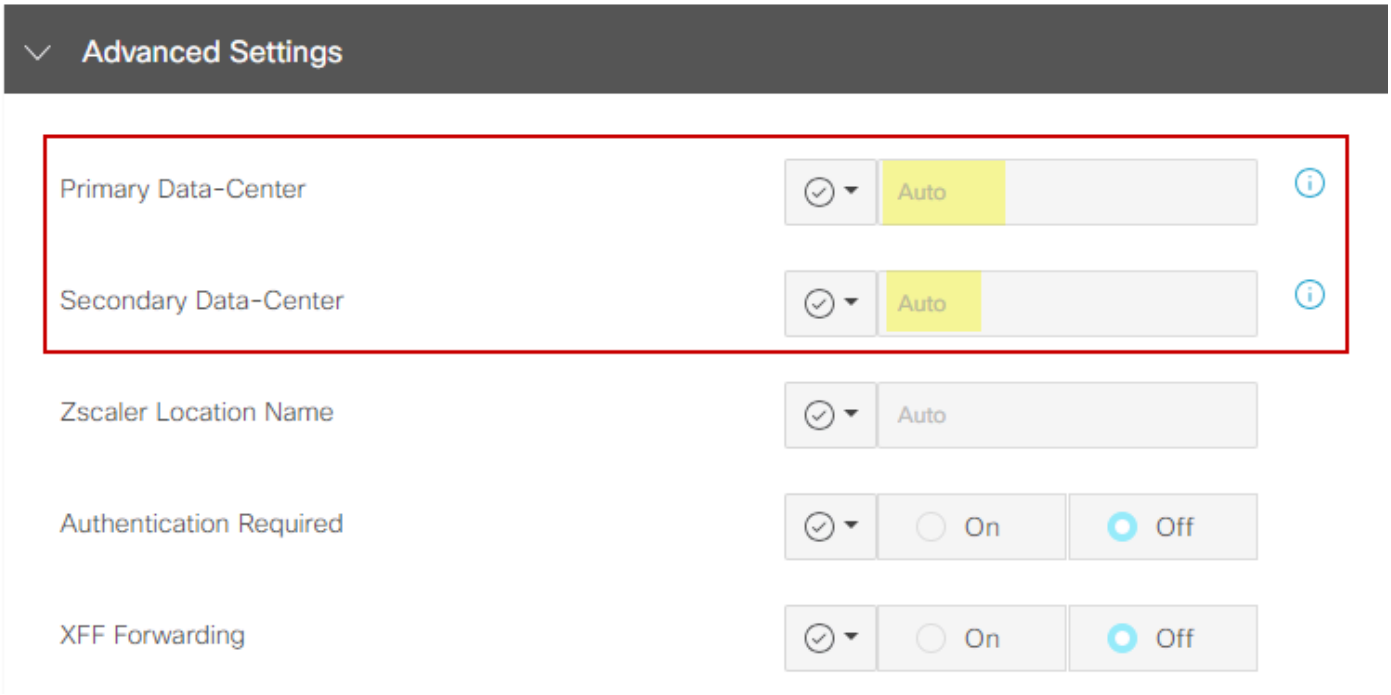
活動/備用設計

高級設定

在本部分中，最重要的配置是主資料中心和輔助資料中心。

建議將兩者配置為「自動」或「手動」，但不建議將其配置為「混合」。

如果您選擇手動配置，請根據您的合作夥伴基礎URI，從Zscaler門戶中選擇正確的URL



自動或手動資料中心

完成後，按一下Save。

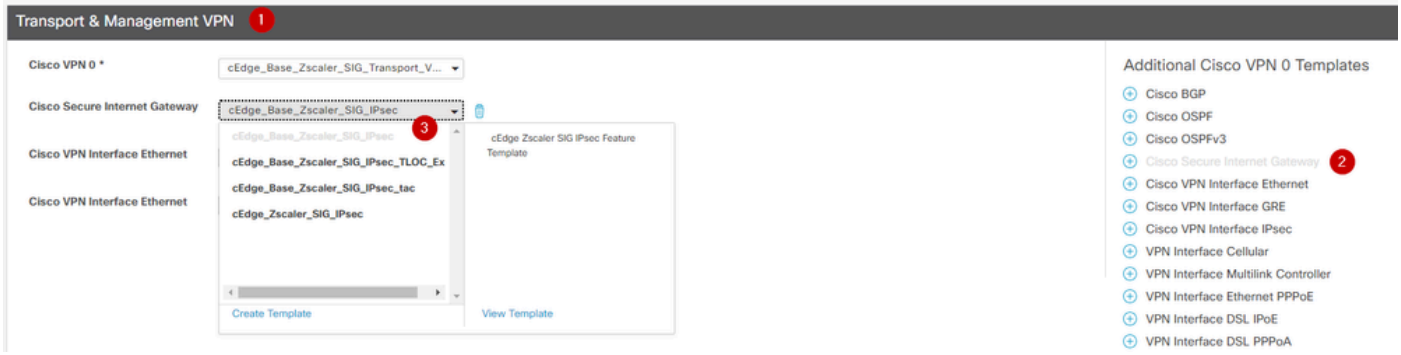
完成SIG模板配置後，必須在裝置模板下應用它們。透過這種方式，配置被推送到思科邊緣路由器上。

要完成這些步驟，請導航到Configuration > Templates > Device Template，在三個點上按一下Edit。

1. 在傳輸和管理VPN下

2. 增加安全Internet網關模板。

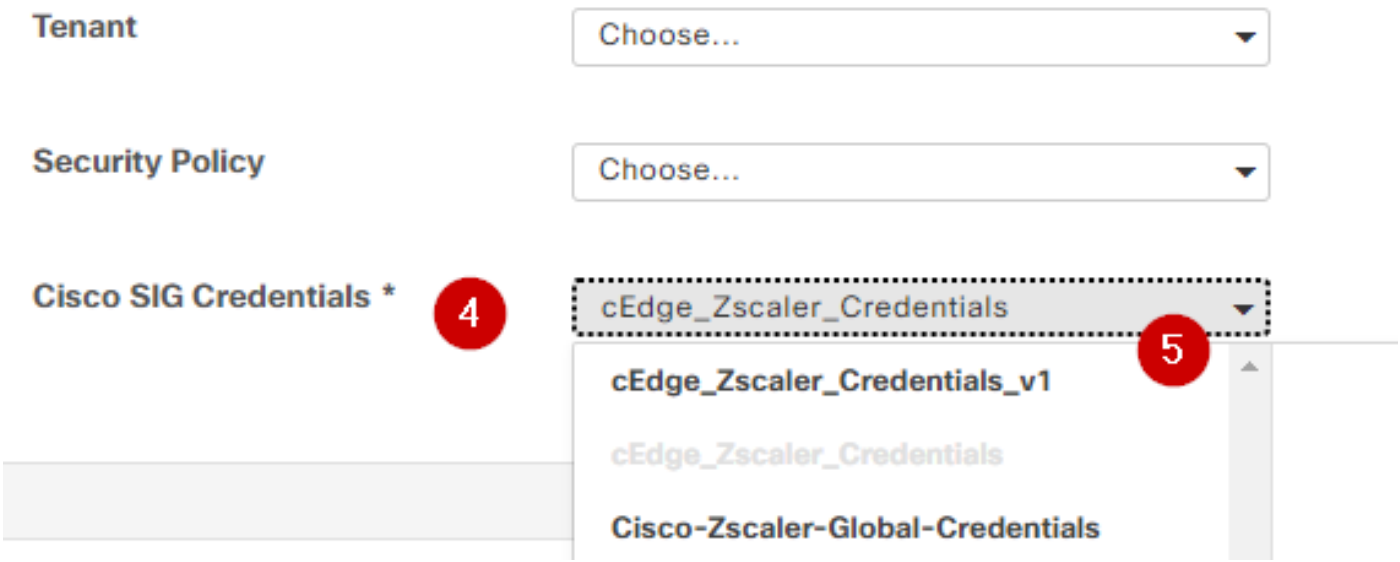
3. 在Cisco Secure Internet Gateway 上，從下拉選單中選擇正確的SIG功能模板。



在裝置模板上增加SIG模板

在Additional Templates下

4. 在Cisco SIG憑證中
5. 從下拉選單中選擇正確的Cisco SIG Credentials模板：



憑據SIG模板

點選更新，請注意，如果您的裝置模板是活動模板，請使用標準步驟在活動模板上推送配置。

驗證

在推送更改時，可以在配置預覽期間進行驗證，您必須注意以下事項：

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

```
    !
```

在此示例中，您可以看到設計為活動/備用

```
<#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
```

您會注意到增加了更多配置，例如crypto ikev2 pofiles和策略、多個以Tunnel1xxxxx開頭的介面、vrf定義65530、ip sdwan route vrf 1 0.0.0.0/0服務簽名。

所有這些更改都是使用Zscaler的IPSec SIG隧道的一部分。

此範例顯示通道介面的組態外觀：

```
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
```

配置成功推送到思科邊緣路由器後，您可以使用命令來驗證隧道是否打開。

```
<#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，則意味著您面臨著與密碼或合作夥伴金鑰有關的問題。

要檢驗介面狀態，請使用命令。

<#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
```

要驗證跟蹤器的狀態，請執行show endpoint-tracker和show endpoint-tracker records命令。這可協

助您確認追蹤器正在使用的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
```

您可以進行的其他驗證包括：
要確保VRF上的路由指向IPSec隧道，請運行此命令：

show ip route vrf 1

最後選用網關是0.0.0.0到網路0.0.0.0

S* 0.0.0.0/0 [2/65535]，通道100002
[2/65535]，隧道100001
10.0.0.0/8進行了可變子網劃分，4個子網，2個掩碼

要進一步驗證，您可以向internet執行ping操作並執行跟蹤路由以檢查流量所花費的跳數：

<#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#
```

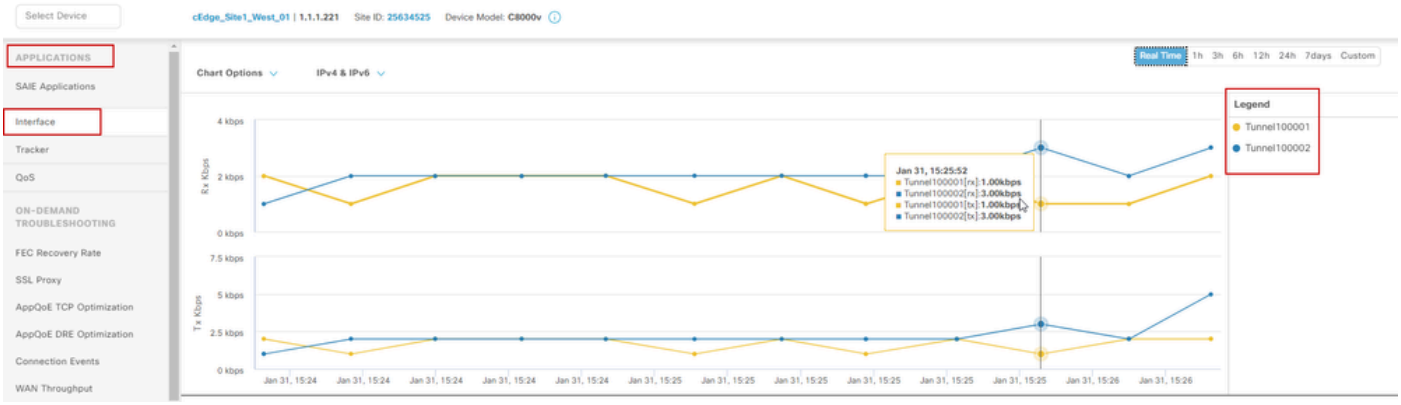
traceroute vrf 1 cisco.com

```
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 *
.....
```

您可以導航到Monitor > Device或Monitor > Network（針對代碼20.6及更早版本），從vManage GUI驗證IPsec介面。

- 選擇路由器並導航至應用>介面。
- 選擇Tunnel100001和Tunnel100002以檢視即時流量或根據所需時間段進行自定義：



監控IPSec隧道

疑難排解

如果SIG隧道未運行，下面是排除此問題的幾個步驟。

第1步：使用命令show sdwan secure-internet-gateway zscaler tunnels檢查錯誤。從輸出中，如果您發現HTTP RESP代碼401，則表明存在身份驗證問題。

您可以驗證SIG憑證模板中的值以檢視密碼或合作夥伴金鑰是否正確。

<#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
```

要進一步調試，請啟用以下命令，並搜尋與SIG、HTTP或跟蹤器相關的日誌消息：

- debug platform software sdwan ftm sig
- debug platform software sdwan sig
- debug platform software sdwan tracker
- 調試平台軟體sdwan ftm rtm-events

以下是debug命令的輸出示例：

<#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
```

運行命令show ip interface brief，並檢查隧道介面Protocol（如果顯示up或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
```

在確認Zscaler憑證沒有問題之後，您可以從裝置模板中刪除SIG介面並將其推送到路由器。

推送完成後，應用SIG模板並將其推迴路由器。此方法強制從零開始重新建立隧道。

相關資訊

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。