Zscalerを使用したSD-WAN IPsec SIGトンネルの設定と確認

内容

はじめに

このドキュメントでは、Zscalerを使用したSD-WAN IPsec SIGトンネルの設定手順と検証について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- セキュリティインターネットゲートウェイ(SIG)。
- IPSecトンネルの仕組み(Cisco IOS®でのフェーズ1とフェーズ2)

追加要件

- NATは、インターネットに面するトランスポートインターフェイスで有効にする必要があります。
- VPN 0でDNSサーバを作成し、ZscalerベースURLをこのDNSサーバで解決する必要があります。これが解決されない場合、API呼び出しは失敗するため、これは重要です。デフォルトではURLがhttp://gateway.<zscalercloud>.net/vpntestであるため、レイヤ7ヘルスチェック

も失敗します。

- NTP(Network Time Protocol)により、Ciscoエッジルータの時刻が正確であり、APIコールが失敗しないことを保証する必要があります。

- SIGを指すサービスルートをService-VPN機能テンプレートまたはCLIで設定する必要があります。
  ip sdwan route vrf 1 0.0.0.0/0 service sig

使用するコンポーネント

このドキュメントは、次のソフトウェアとハードウェアのバージョンに基づいています。

- Ciscoエッジルータバージョン17.6.6a
- vManageバージョン20.9.4

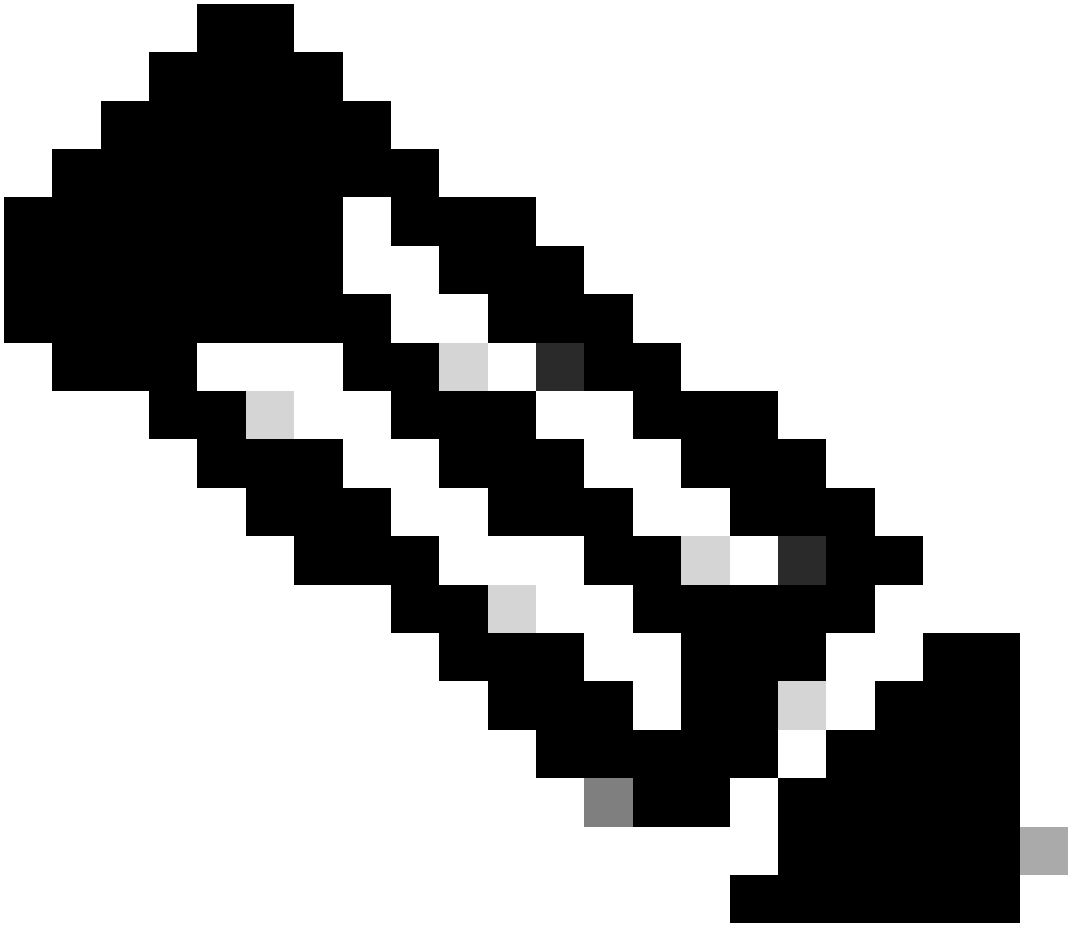
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク設計オプション

次に、アクティブ/スタンバイの組み合わせ設定のさまざまなタイプの導入を示します。トンネルカプセル化は、GREまたはIPsecのどちらにも導入できます。

- アクティブ/スタンバイトンネルペア1つ
- 1つのアクティブ/アクティブトンネルペア。
- 複数のアクティブ/スタンバイトンネルペア。
- 複数のアクティブ/アクティブトンネルペア。



注:SD-WANシスコエッジルータでは、インターネットに接続された1つ以上のトランスポートインターフェイスを利用して、これらの設定を効果的に機能させることができます。

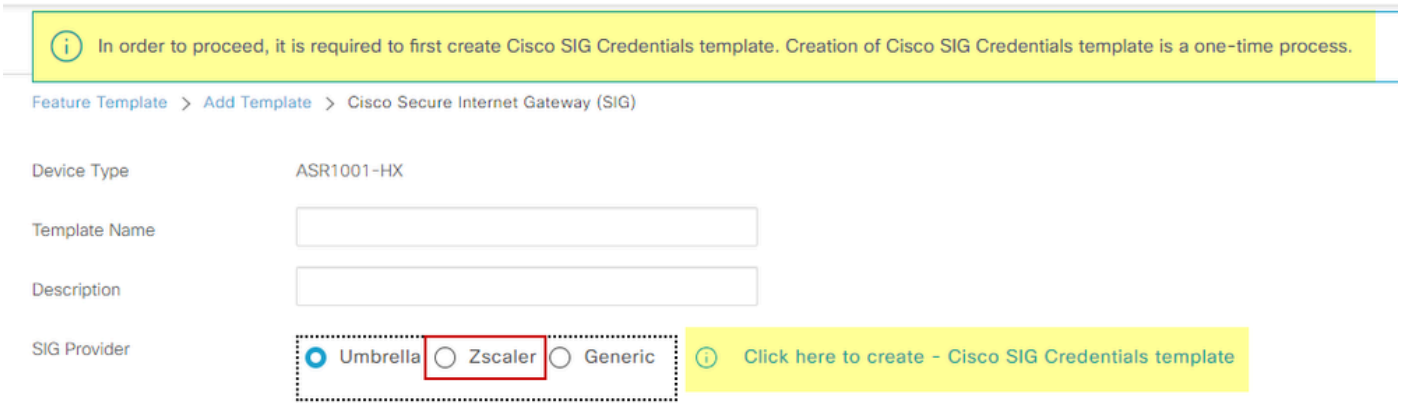
コンフィギュレーション

次のテンプレートの設定に進みます。

- セキュリティインターネットゲートウェイ(SIG)クレデンシャル機能テンプレート：
  - すべてのCisco工ッジルータに1つが必要です。テンプレートの必要なフィールドに入力する情報は、Zscalerポータルで作成する必要があります。
- セキュリティインターネットゲートウェイ(SIG)機能テンプレート：
  - この機能テンプレートでは、IPsecトンネルを設定し、アクティブ/アクティブまたはアクティブ/スタンバイモードで導入のハイアベイラビリティ(HA)を確保し、Zscaler Datacenterを自動または手動で選択します。

Zscaler Credentialsテンプレートを作成するには、Configuration > Template > Feature Template > Add Templateの順に移動します。

この目的で使用するデバイスモデルを選択し、SIGを検索します。これを初めて作成すると、次の例のように、Zscalerクレデンシャルを最初に作成する必要があることが表示されます。SIGプロバイダーとしてZscalerを選択し、Click here to create - Cisco SIG Credentials templateをクリックする必要があります。



Sig Credentilaテンプレート

」

クレデンシャルテンプレートにリダイレクトされます。このテンプレートでは、すべてのフィールドに値を入力する必要があります。

- テンプレート名
- 説明
- SIGプロバイダー（前の手順から自動的に選択）
- 組織
- パートナーベースURI
- ユーザ名
- Password
- パートナーAPIキー

[Save] をクリックします。

セキュアインターネットゲートウェイ(SIG)テンプレートにリダイレクトされます。このテンプレートを使用すると、SD-WAN IPsec SIGに必要なすべてをZscalerで設定できます。

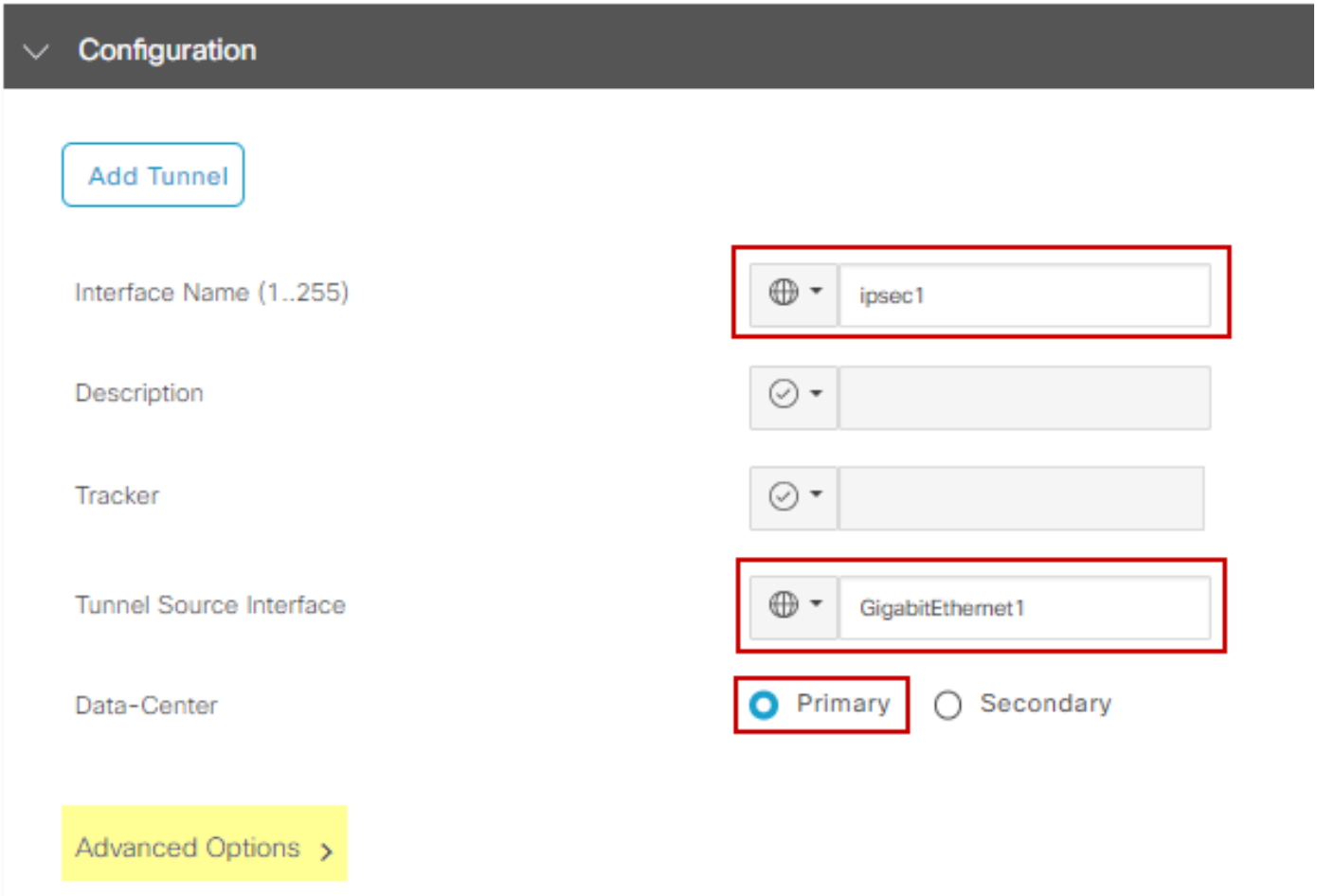
テンプレートの最初のセクションで、名前と説明を入力してください。デフォルトのトラッカーは自動的に有効になります。Zscaler Layer 7ヘルスチェックに使用されるAPI URLは zscaler_L7_health_check) ishttp://gateway<zscalercloud>net/vpntestです。

Cisco IOS XEでは、トラッカーのIPアドレスを設定する必要があります。/32の範囲内のプライベートIPは許容されます。設定したIPアドレスは、Zscalerのヘルスインスペクションを実行するために自動的に作成されるLoopback 65530インターフェイスで使用できます。

ConfigurationセクションでAdd Tunnelをクリックすることにより、IPSecトンネルを作成できま

す。新しいポップアップウィンドウで、必要に応じて選択します。

この例では、トンネルソースとしてWANインターフェイスGigabitEthernet1を使用して、インターフェイスIPsec1が作成されています。その後、プライマリZcalerデータセンターとの接続を形成できます。
Advanced Optionsの値はデフォルトのままにしておくことをお勧めします。

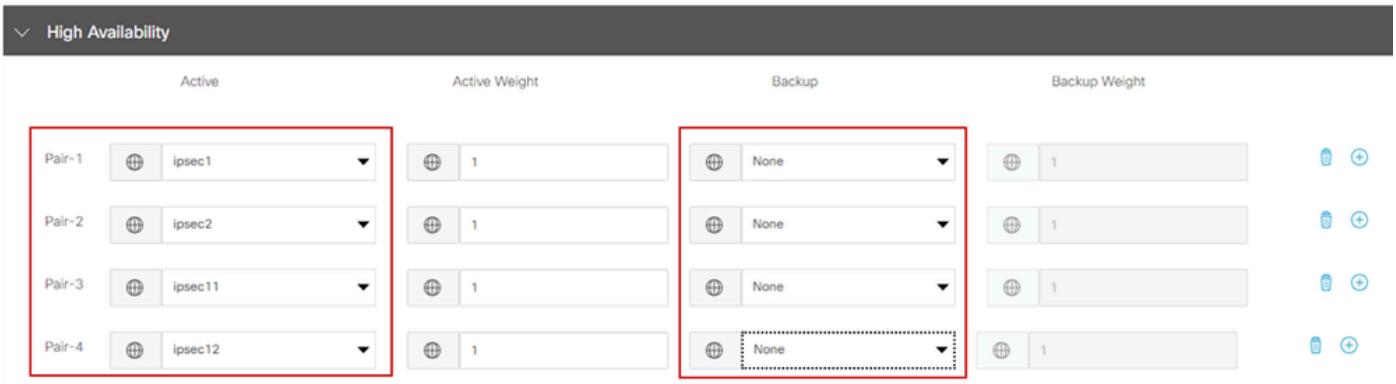


IPsecインターフェイスの設定

ハイ アベイラビリティ

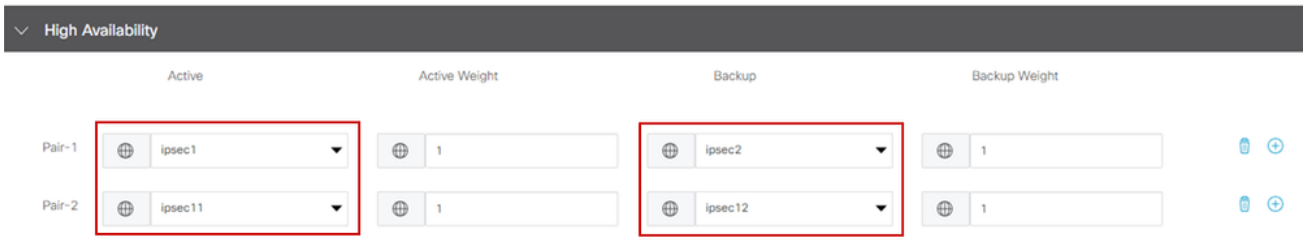
このセクションでは、設計をアクティブ/アクティブまたはアクティブ/スタンバイのどちらにするかを選択し、どのIPSecインターフェイスをアクティブにするかを決定します。

これは、アクティブ/アクティブ設計の例です。すべてのインターフェイスがActiveの下で選択され、Backupはそのままになります。



アクティブ/アクティブ設計

この例では、アクティブ/スタンバイ設計を示します。IPsec1とIPsec11はアクティブインターフェイスとして選択され、IPsec2とIPsec12はスタンバイインターフェイスとして指定されます。



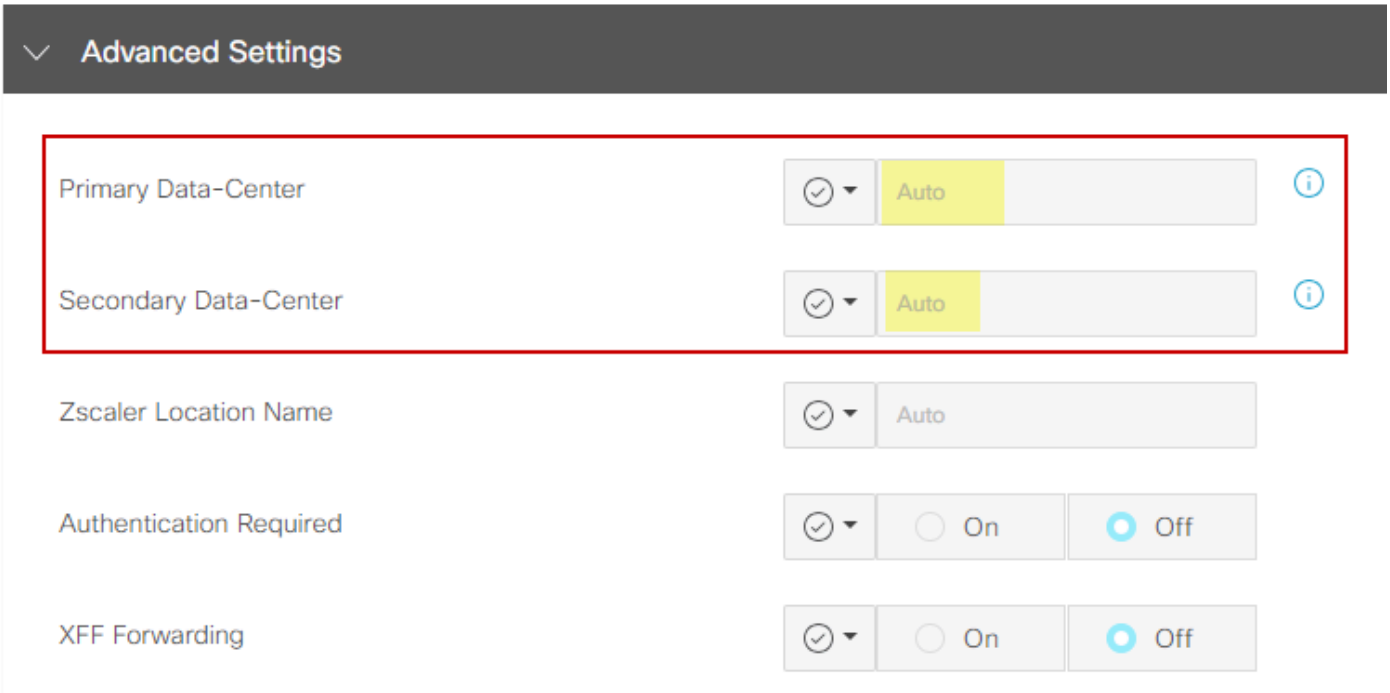
アクティブ/スタンバイ設計

詳細設定

このセクションでは、最も重要な設定はプライマリデータセンターとセカンダリデータセンターです。

両方を自動または手動で設定することをお勧めしますが、両方を混在として設定することはお勧めしません。

手動での設定を選択した場合は、パートナーベースURIに基づいて、Zscalerポータルから正しいURLを選択してください



自動または手動によるデータセンター

終了したら、Saveをクリックします。

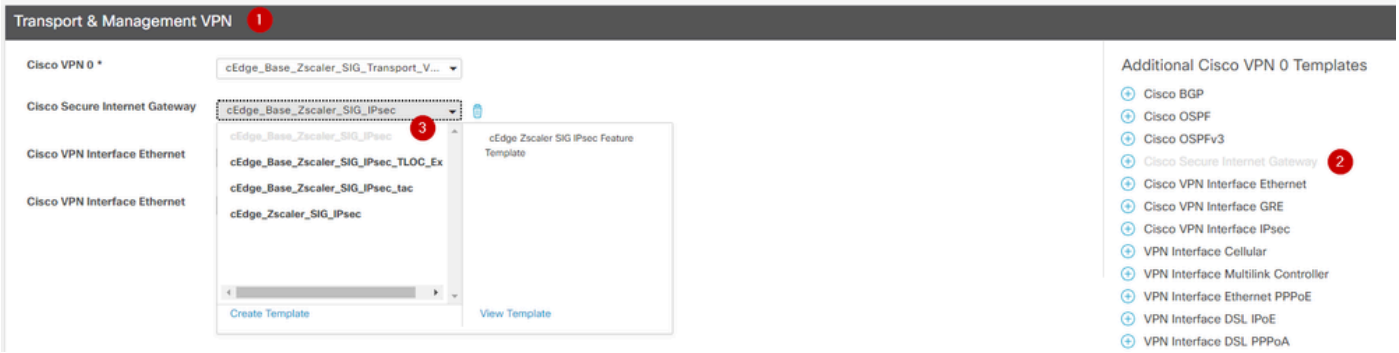
SIGテンプレートの設定が完了したら、それらをデバイステンプレートに適用する必要があります。このように、設定はCiscoエッジルータにプッシュされます。

これらの手順を完了するには、Configuration > Templates > Device Templateの3つのドットでEditをクリックします。

1. Transport & Management VPNの下

2.セキュアインターネットゲートウェイテンプレートを追加します。

3. Cisco Secure Internet Gatewayで、ドロップダウンメニューから正しいSIG機能テンプレートを選択します。

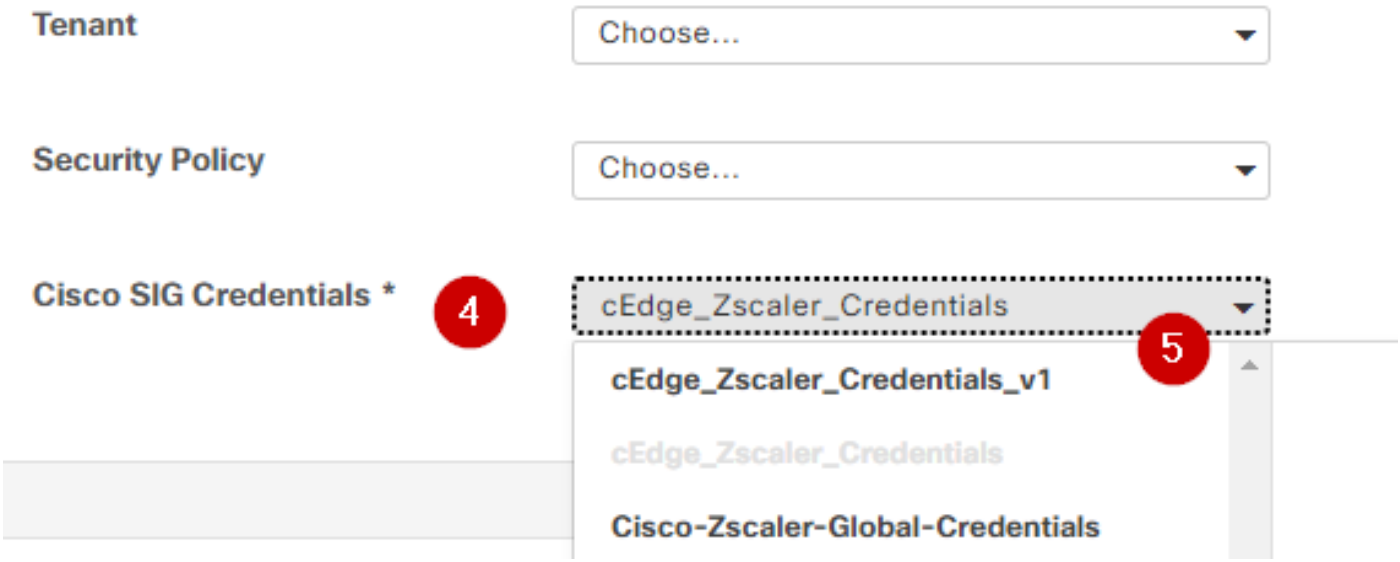


デバイステンプレートへのSIGテンプレートの追加

追加テンプレートの下

4. Cisco SIGクレデンシャル

5. ドロップダウンメニューから、適切なCisco SIG Credentialsテンプレートを選択します。



クレデンシャルSIGテンプレート

Updateをクリックします。デバイステンプレートがアクティブなテンプレートである場合は、標準的な手順を使用してアクティブなテンプレートに設定をプッシュします。

確認

変更をプッシュする間、設定のプレビュー中に検証を実行できます。次の点に注意してください。

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

この例から、設計がアクティブ/スタンバイであることがわかります

<#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
```

crypto ikev2プロファイルとポリシー、Tunnel1xxxxxで始まる複数のインターフェイス、vrf defination 65530、ip sdwan route vrf 1 0.0.0.0/0 service sigなど、さらに多くの設定が追加されています。

これらの変更はすべて、Zscalerを使用したIPSec SIGトンネルの一部です。

次の例は、トンネルインターフェイスの設定がどのように表示されるかを示しています。

```
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
```

設定がCiscoエッジルータに正常にプッシュされたら、コマンドを使用してトンネルが起動しているかどうかを確認できます。

<#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
```

http resp code 200が表示されない場合は、パスワードまたはパートナーキーに関する問題に直面していることを意味します。

インターフェイスのステータスを確認するには、コマンドを使用します。

<#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
```

トラッカーのステータスを確認するには、show endpoint-trackerコマンドおよびshow endpoint-tracker recordsコマンドを実行します。これは、トラッカーが利用しているURLを確認するのに役立ちます

```
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
```

実行できるその他の検証は次のとおりです。
VRFのルートがIPSecトンネルをポイントしていることを確認するには、次のコマンドを実行します。

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

さらに詳しく検証するには、インターネットに向けてpingを実行し、トラフィックが通過するホップを確認するトレースルートを実行します。

<#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>

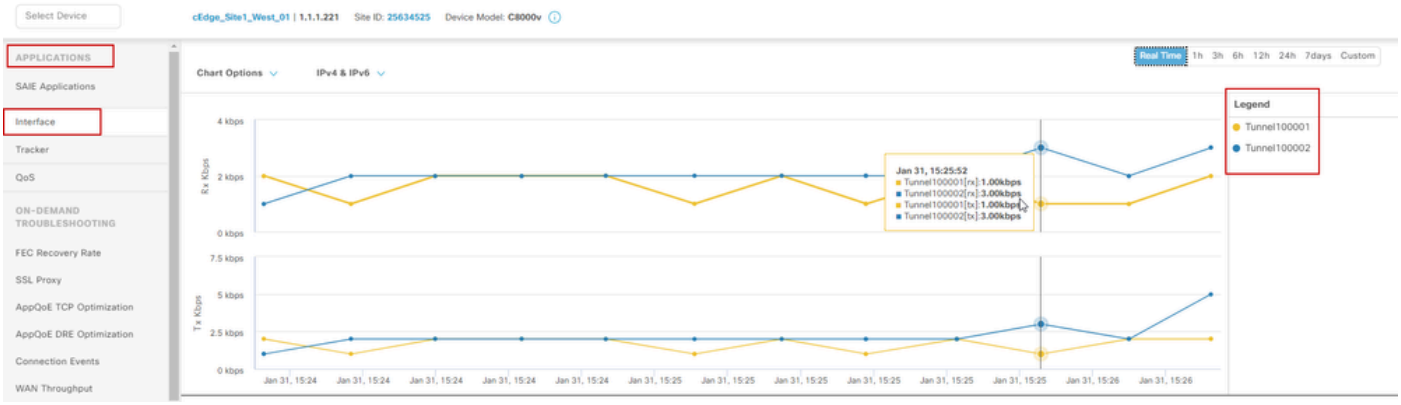
```
 200 msec
```

<The IP here need to be Zcaler IP>

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

IPsecインターフェイスをvManage GUIから検証するには、Monitor > Device（コード20.6以前）またはMonitor > Network（コード20.6以前）に移動します。

- ルータを選択し、Applications > Interfacesの順に選択します。
- リアルタイムトラフィックを表示したり、必要な時間枠ごとにカスタマイズするには、Tunnel100001およびTunnel100002を選択します。



IPSecトンネルのモニタリング

トラブルシュート

SIGトンネルが稼働していない場合は、問題のトラブルシューティング手順を次に示します。

手順1:show sdwan secure-internet-gateway zscaler tunnelsコマンドを使用してエラーを確認します。出力から、HTTP RESP Code 401に気付いた場合、認証に問題があることを示しています。

SIG Credentialsテンプレートの値を確認して、パスワードまたはパートナーキーが正しいかどうかを確認できます。

<#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-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
```

さらにデバッグを行うには、次のコマンドを有効にし、SIG、HTTP、またはトラッカーに関連するログメッセージを検索します。

- debug platform software sdwan ftm sig
- debug platform software sdwan sig
- debug platform software sdwan tracker（登録ユーザ専用）
- debug platform software sdwan ftm rtm-events（登録ユーザ専用）

次にdebugコマンドの出力例を示します。

```
<#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
```

コマンドshow ip interface briefを実行して、トンネルインターフェイスProtocol（upまたはdown）が表示されているかどうかを確認します。

<#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**

Zscalerクレデンシャルに問題がないことを確認したら、デバイステンプレートからSIGインターフェイスを削除し、ルータにプッシュします。

プッシュが完了したら、SIGテンプレートを適用し、ルータにプッシュします。この方法では、トンネルが最初から再作成されます。

関連情報

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。