Configuration et vérification du tunnel SD-WAN IPsec SIG avec Zscaler

Table des matières

Introduction

Ce document décrit les étapes de configuration et la vérification des tunnels SD-WAN IPsec SIG avec Zscaler.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Passerelle Internet de sécurité (SIG).
- Fonctionnement des tunnels IPsec, Phase1 et Phase2 sur Cisco IOS®.

Exigences supplémentaires

- La fonction NAT doit être activée sur l'interface de transport qui va être connectée à Internet.
- Un serveur DNS doit être créé sur le VPN 0, et l'URL de base Zscaler doit être résolue avec ce serveur DNS. C'est important car si cela ne résout pas le problème, les appels API vont échouer. Les vérifications d'intégrité de la couche 7 vont également échouer, car par défaut, l'URL est : http://gateway.<zscalercloud>.net/vpntest.

- Le protocole NTP (Network Time Protocol) doit s'assurer que l'heure du routeur de périphérie Cisco est exacte et que les appels d'API ne vont pas échouer.
- Une route de service pointant vers SIG doit être configurée dans le modèle de fonctionnalité Service-VPN ou CLI :
  ip sdwan route vrf 1.0.0.0.0/0 service sig

Composants utilisés

Ce document est basé sur les versions logicielles et matérielles suivantes :

- Routeur de périphérie Cisco version 17.6.6a
- vManage version 20.9.4

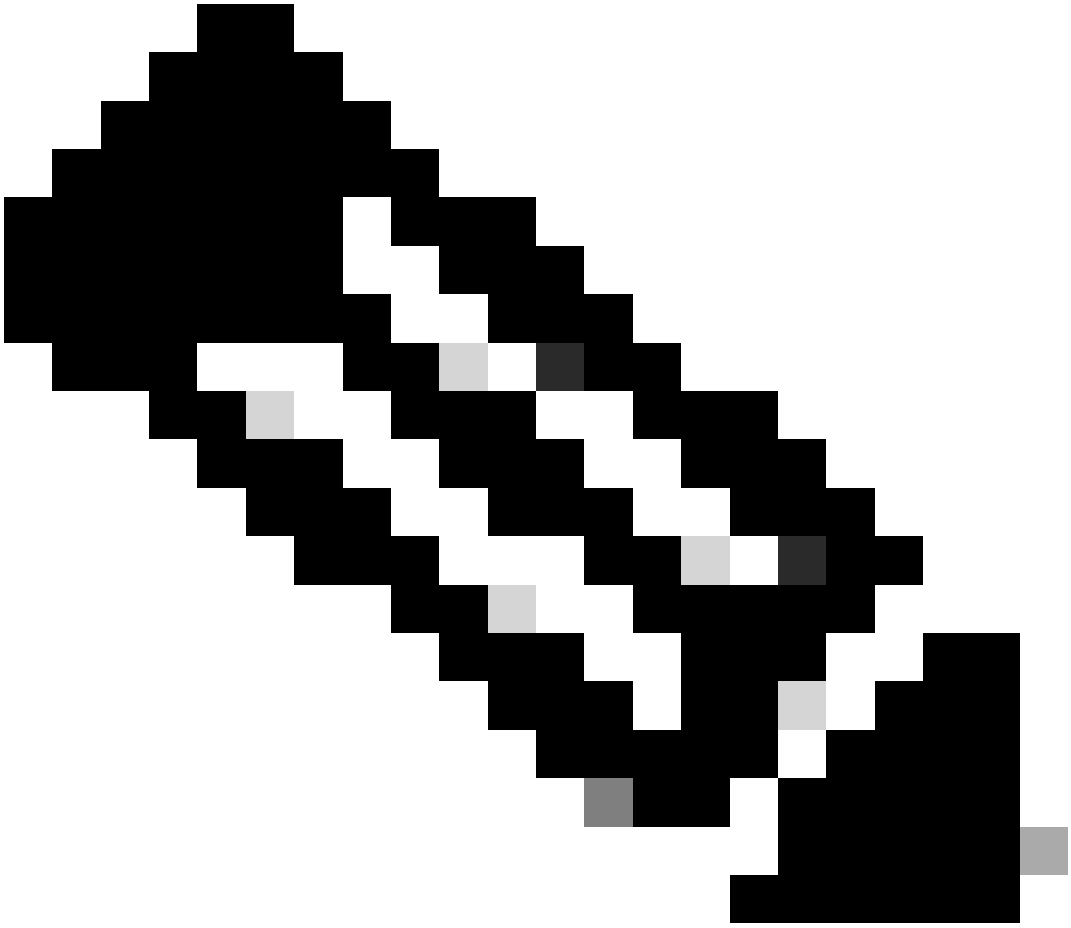
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configurer

Options de conception réseau

Voici les différents types de déploiements dans une configuration combinée active/veille. L'encapsulation de tunnel peut être déployée avec GRE ou IPsec.

- Une Paire De Tunnels Actif/Veille.
- Une Paire De Tunnels Actif/Actif.
- Paire de tunnels multiples actif/veille.
- Paire de tunnels active/active multiple.



Remarque : sur les routeurs de périphérie Cisco SD-WAN, vous pouvez utiliser une ou plusieurs interfaces de transport connectées à Internet pour que ces configurations fonctionnent efficacement.

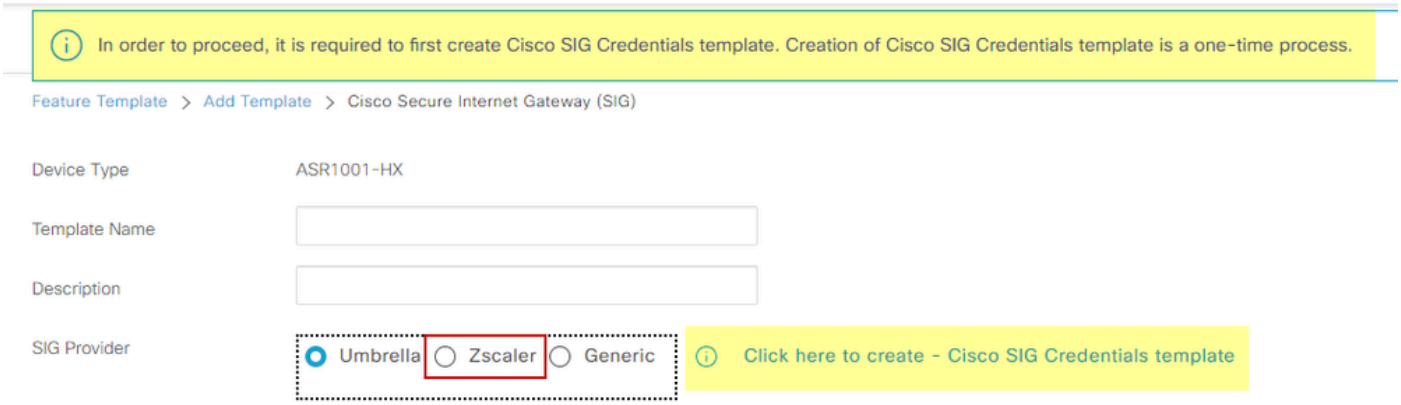
Configurations

Procédez à la configuration de ces modèles :

- Modèle de fonction d'informations d'identification de passerelle Internet de sécurité :
  - Vous en avez besoin pour tous les routeurs de périphérie Cisco. Les informations nécessaires pour remplir les champs du modèle doivent être créées sur le portail Zscaler.
- Modèle de fonction de passerelle Internet de sécurité (SIG) :
  - Dans ce modèle de fonctionnalité, vous configurez des tunnels IPsec, assurez la haute disponibilité (HA) du déploiement en mode actif/actif ou actif/veille, et sélectionnez Zscaler Datacenter automatiquement ou manuellement.

Pour créer un modèle d'informations d'identification Zscaler, accédez à Configuration > Template > Feature Template > Add Template.

Sélectionnez le modèle de périphérique que vous allez utiliser à cette fin et recherchez SIG. Lorsque vous le créez pour la première fois, le système indique que les informations d'identification Zscaler doivent être créées en premier, comme dans cet exemple :
Vous devez sélectionner Zscaler comme fournisseur SIG et cliquer sur le modèle Cliquez ici pour créer - Informations d'identification SIG Cisco.



Modèle de signature des informations d'identification

"

Vous êtes redirigé vers le modèle Informations d'identification. Dans ce modèle, vous devez entrer les valeurs de tous les champs :

- Nom du modèle
- Description
- SIG Provider (sélectionné automatiquement à l'étape précédente)
- Organisation
- URI de base du partenaire
- Nom d'utilisateur
- Mot de passe
- Clé API du partenaire

Cliquez sur Save.

Vous êtes redirigé vers le modèle Secure Internet Gateway (SIG). Ce modèle vous permet de configurer tout ce qui est nécessaire pour SD-WAN IPsec SIG avec Zscaler.

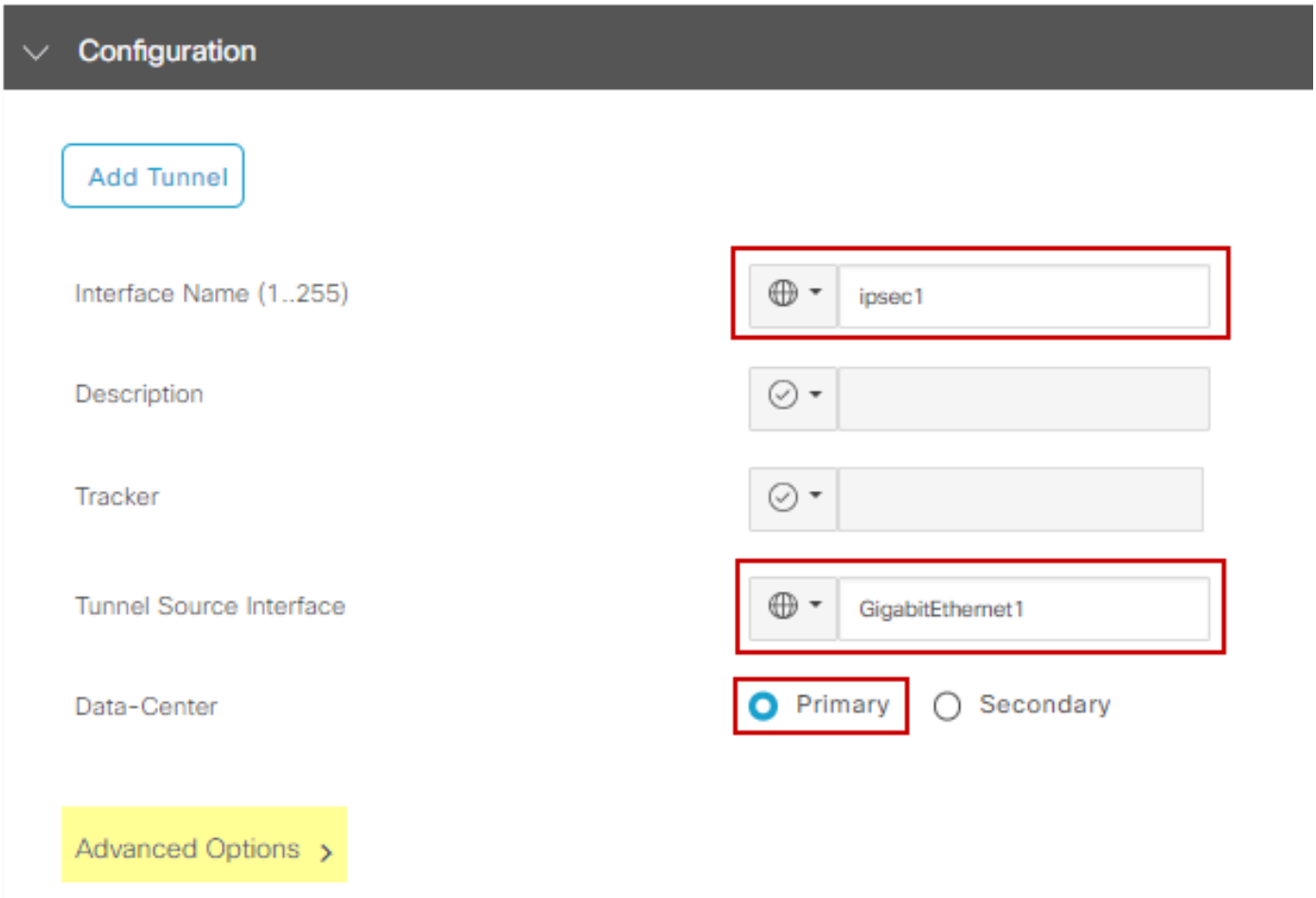
Dans la première section du modèle, veuillez fournir un nom et une description. Le tracker par défaut est automatiquement activé. L'URL de l'API utilisée pour le contrôle d'intégrité de la couche 7 de Zscaler est la suivante : zscaler_L7_health_check) ishttp://gateway<zscalercloud>net/vpntest.

Dans Cisco IOS XE, vous devez définir une adresse IP pour le traqueur. Toute adresse IP privée comprise dans la plage /32 est acceptable. L'adresse IP que vous définissez peut être utilisée par

l'interface de bouclage 6530, qui est automatiquement créée pour effectuer des inspections d'intégrité Zscaler.

Dans la section Configuration, vous pouvez créer les tunnels IPsec en cliquant sur Add Tunnel. Dans la nouvelle fenêtre contextuelle, effectuez des sélections en fonction de vos besoins.

Dans cet exemple, l'interface IPsec1 a été créée, en utilisant l'interface WAN GigabitEthernet1 comme source de tunnel. Il peut ensuite établir une connectivité avec le data center Zcaler principal.
Il est recommandé de conserver les valeurs Options avancées par défaut.

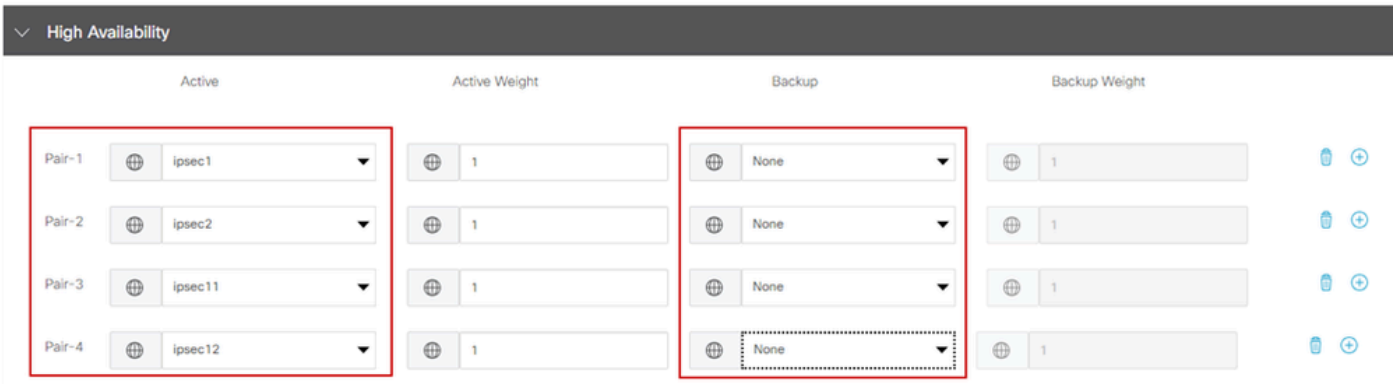


Configuration d'interface IPsec

Haute disponibilité

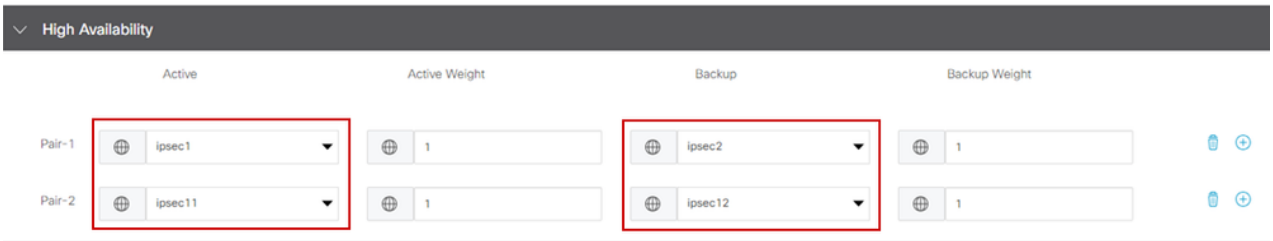
Dans cette section, vous choisissez si la conception sera Active/Active ou Active/Standby, et vous déterminez quelle interface IPsec sera active.

Voici un exemple de conception active/active. Toutes les interfaces sont sélectionnées sous Active, laissant Backup sans aucune.



Conception active/active

Cet exemple présente une conception active/veille. IPsec1 et IPsec11 sont sélectionnés pour être des interfaces actives, tandis que IPsec2 et IPsec12 sont désignés comme interfaces de secours.



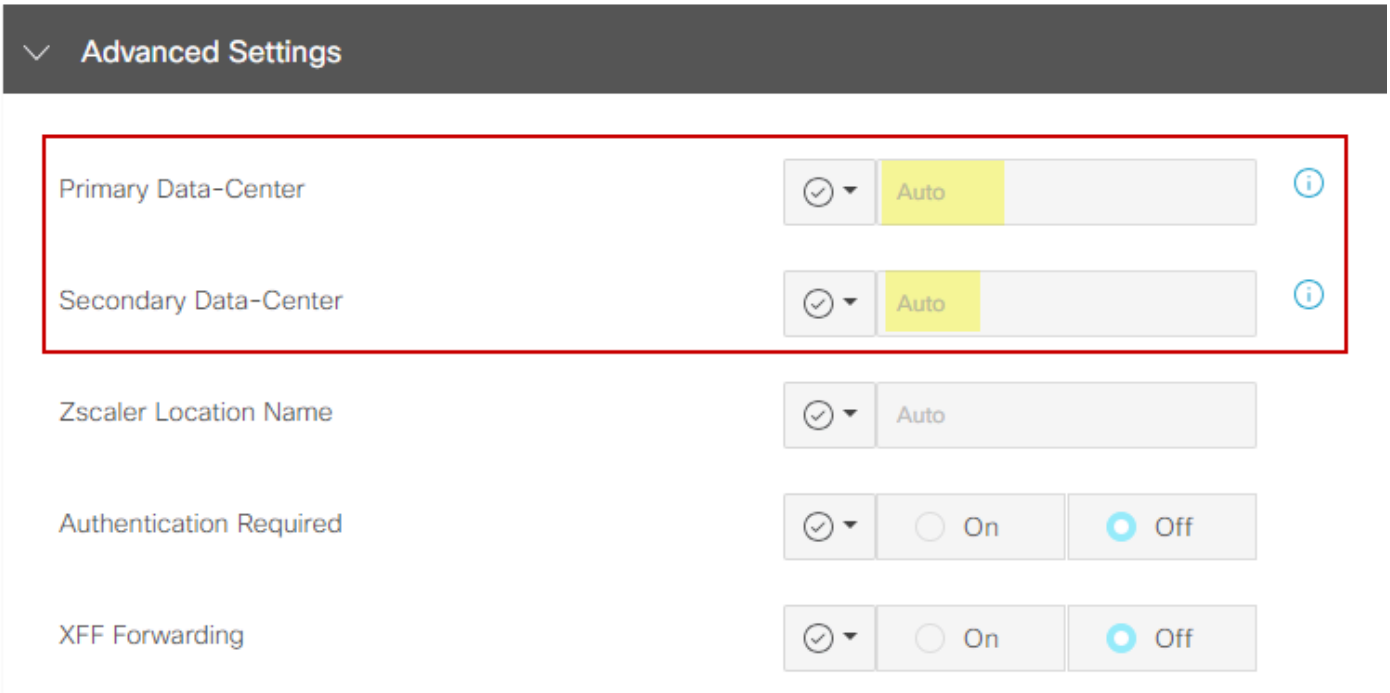
Conception active/veille

Paramètres avancés

Dans cette section, les configurations les plus importantes sont le data center principal et le data center secondaire.

Il est recommandé de configurer les deux en mode automatique ou manuel, mais il n'est pas recommandé de les configurer en mode mixte.

Si vous choisissez de les configurer manuellement, sélectionnez l'URL correcte sur le portail Zscaler, en fonction de votre URI de base partenaire



Data centers automatiques ou manuels

Cliquez sur Save lorsque vous avez terminé.

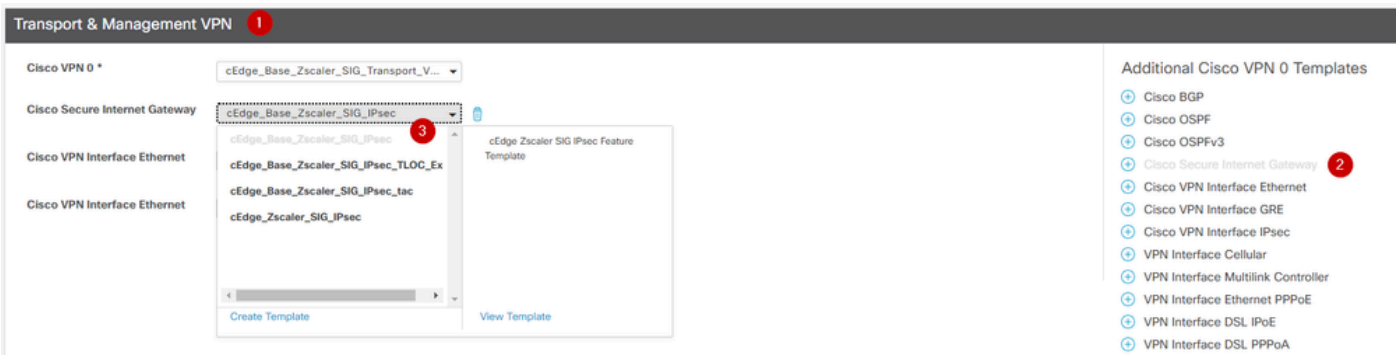
Une fois que vous avez terminé la configuration des modèles SIG, vous devez les appliquer sous le modèle de périphérique. De cette manière, la configuration est poussée sur les routeurs de périphérie Cisco.

Pour effectuer ces étapes, accédez à Configuration > Templates > Device Template, sur trois points cliquez sur Edit.

1. Sous Transport & Management VPN

2. Ajoutez un modèle de passerelle Internet sécurisée.

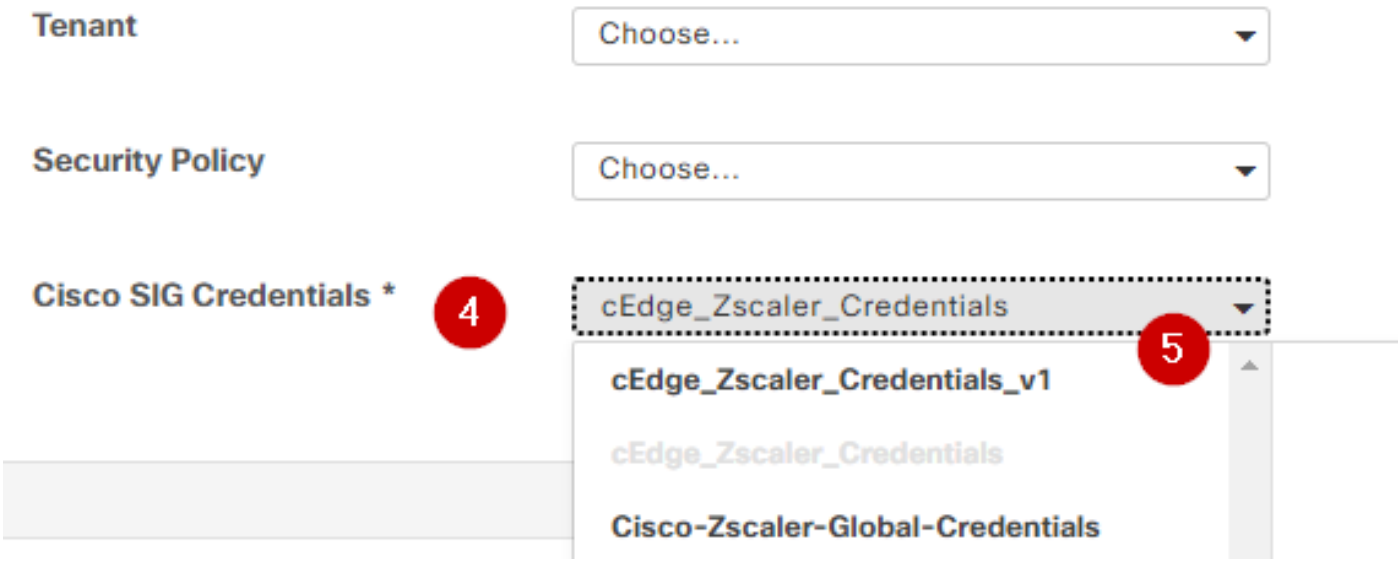
3. Sur Cisco Secure Internet Gateway, sélectionnez le modèle de fonction SIG approprié dans le menu déroulant.



Ajouter un modèle SIG au modèle de périphérique

Sous Modèles supplémentaires

4. Dans les identifiants Cisco SIG
5. Sélectionnez le modèle d'informations d'identification Cisco SIG approprié dans le menu déroulant :



Modèle Credential SIG

Cliquez sur Update, veuillez noter que si votre modèle de périphérique est un modèle actif, utilisez les étapes standard pour pousser les configurations sur un modèle actif.

Vérifier

La vérification peut être effectuée lors de l'aperçu de la configuration pendant que vous répercutez les modifications. Vous devez noter les points suivants :

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

Dans cet exemple, vous pouvez voir que la conception est active/en veille

<#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
```

Vous remarquerez que d'autres configurations sont ajoutées, comme les profils et les politiques crypto ikev2, plusieurs interfaces commençant par Tunnel1xxxxx, la définition vrf 65530, ip sdwan route vrf 1.0.0.0.0/0 service sig.

Toutes ces modifications font partie des tunnels IPSec SIG avec Zscaler.

Cet exemple montre comment se présente la configuration de l'interface du tunnel :

```
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
```

Une fois que les configurations ont été transmises avec succès aux routeurs de périphérie Cisco, vous pouvez utiliser des commandes pour vérifier si les tunnels sont actifs ou non.

<#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
```

Si vous ne voyez pas http resp code 200, cela signifie que vous êtes confronté à un problème concernant le mot de passe ou la clé partenaire.

Utilisez la commande pour vérifier l'état des interfaces.

<#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
```

Pour vérifier l'état du tracker, exécutez les commandes show endpoint-tracker et show endpoint-tracker records. Cela vous aide à confirmer l'URL que le traqueur utilise

```
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
```

Les autres validations que vous pouvez effectuer sont :
Pour vous assurer que les routes sur VRF pointent vers les tunnels IPsec, exécutez cette commande :

show ip route vrf 1

La passerelle de dernier recours est 0.0.0.0 vers le réseau 0.0.0.0

S* 0.0.0.0/0 [2/65535], Tunnel100002
[2/65535], Tunnel100001
10.0.0.0/8 est divisé en sous-réseaux variables, 4 sous-réseaux, 2 masques

Pour valider encore davantage, vous pouvez envoyer une requête ping vers Internet et effectuer une route de suivi pour vérifier les sauts que le trafic emprunte :

<#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>

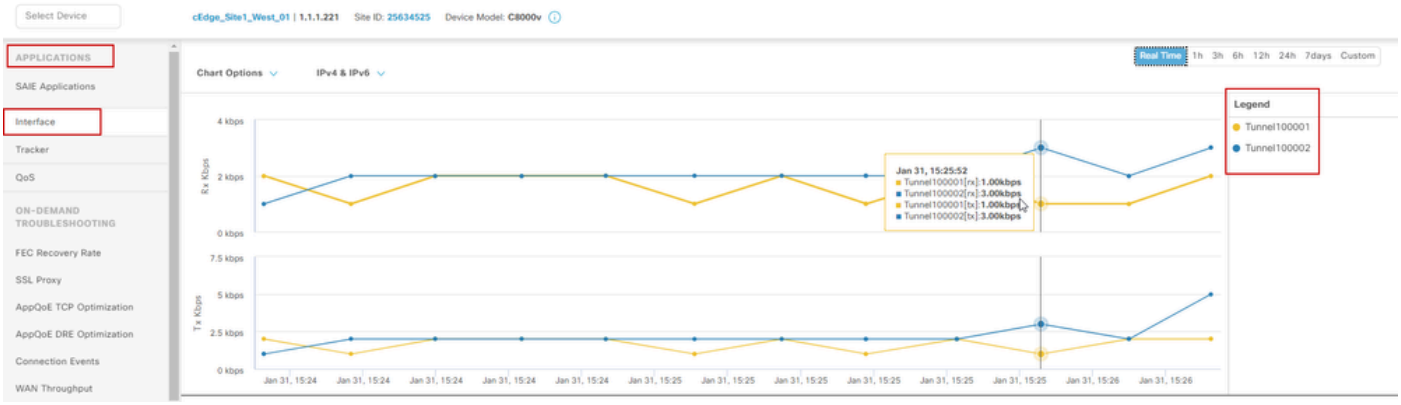
```
 200 msec
```

<The IP here need to be Zcaler IP>

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

Vous pouvez valider les interfaces IPsec à partir de l'interface graphique utilisateur de vManage en naviguant sur Monitor > Device ou Monitor > Network (pour les codes 20.6 et antérieurs).

- Sélectionnez votre routeur et accédez à Applications > Interfaces.
- Sélectionnez Tunnel100001 et Tunnel100002 pour afficher le trafic en temps réel ou le personnaliser selon la période requise :



Surveillance des tunnels IPsec

Dépannage

Si le tunnel SIG n'est pas en cours d'exécution, voici les quelques étapes à suivre pour résoudre le problème.

Étape 1 : Vérifiez les erreurs à l'aide de la commande show sdwan secure-internet-gateway zscaler tunnels. D'après le résultat, si vous remarquez le code RESP HTTP 401, il indique qu'il y a un problème avec l'authentification.

Vous pouvez vérifier les valeurs dans le modèle d'informations d'identification SIG pour voir si le mot de passe, ou la clé partenaire, est 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
```

Pour poursuivre le débogage, activez ces commandes et recherchez les messages de journal relatifs à SIG, HTTP ou tracker :

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

Voici un exemple des résultats des commandes debug :

<#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
```

Exécutez la commande show ip interface brief et vérifiez le protocole d'interface des tunnels si des messages s'affichent ou s'arrêtent.

<#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
```

Après avoir vérifié qu'il n'y a aucun problème avec les informations d'identification Zscaler, vous pouvez supprimer l'interface SIG du modèle de périphérique et la pousser vers le routeur.

Une fois la transmission terminée, appliquez le modèle SIG et repoussez-le sur le routeur. Cette méthode force la recréation des tunnels à partir de zéro.

Informations connexes

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.