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

Table des matières

Introduction

Conditions préalables

- Exigences
- Exigences supplémentaires
- Composants utilisés

Configurer

- Options de conception réseau

Configurations

- Haute disponibilité
- Paramètres avancés

Vérifier

Dépannage

À partir de Cisco IOS®Version IOS-XE 17.11+, a été migrée vers

Informations connexes

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 fait face 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. Ceci est important car si cela n'est pas résolu, les appels API et les vérifications d'intégrité de la couche 7 peuvent échouer. Et par défaut, utilisez ce serveur DNS
- Le protocole NTP (Network Time Protocol) doit s'assurer que l'heure du routeur de périphérie Cisco est exacte et que les appels API ne peuvent 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

Les différents types de déploiements de cette liste sont 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 active/active
- Paire de tunnels multiples actifs/en veille
- Paire de tunnels multiples actifs/actifs

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

Configurations

Procédez à la configuration de ces modèles :

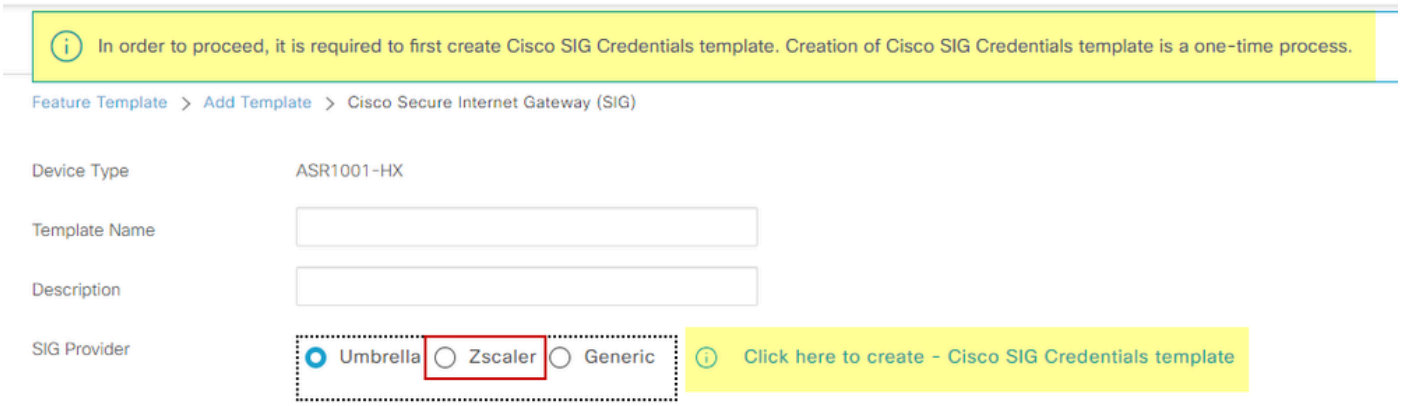
- Modèle de fonction d'informations d'identification de passerelle Internet de sécurité :
  - Vous en avez besoin pour tous les routeurs de périphérie Cisco. Les informations nécessaires pour remplir les champs du modèle doivent être créées sur le portail Zscaler.

- Modèle de fonction de passerelle Internet de sécurité (SIG) :
  - Dans ce modèle de fonctionnalité, vous configurez des tunnels IPsec, assurez le déploiement de la haute disponibilité (HA) en mode actif/actif ou actif/veille, et sélectionnez Zscaler Data-Center enter automatiquement ou manuellement.

1. Pour créer un modèle d'informations d'identification Zscaler, accédez à Configuration > Modèle > Modèle de fonction > Ajouter un modèle.

2. 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 l'exemple suivant :

3. Vous devez sélectionner Zscaler en tant que fournisseur SIG et cliquer sur le modèle Cliquez ici pour créer - Informations d'identification Cisco SIG.



4. Vous êtes redirigé vers le modèle d'informations d'identification. Vous devez également saisir les valeurs de tous les champs :

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

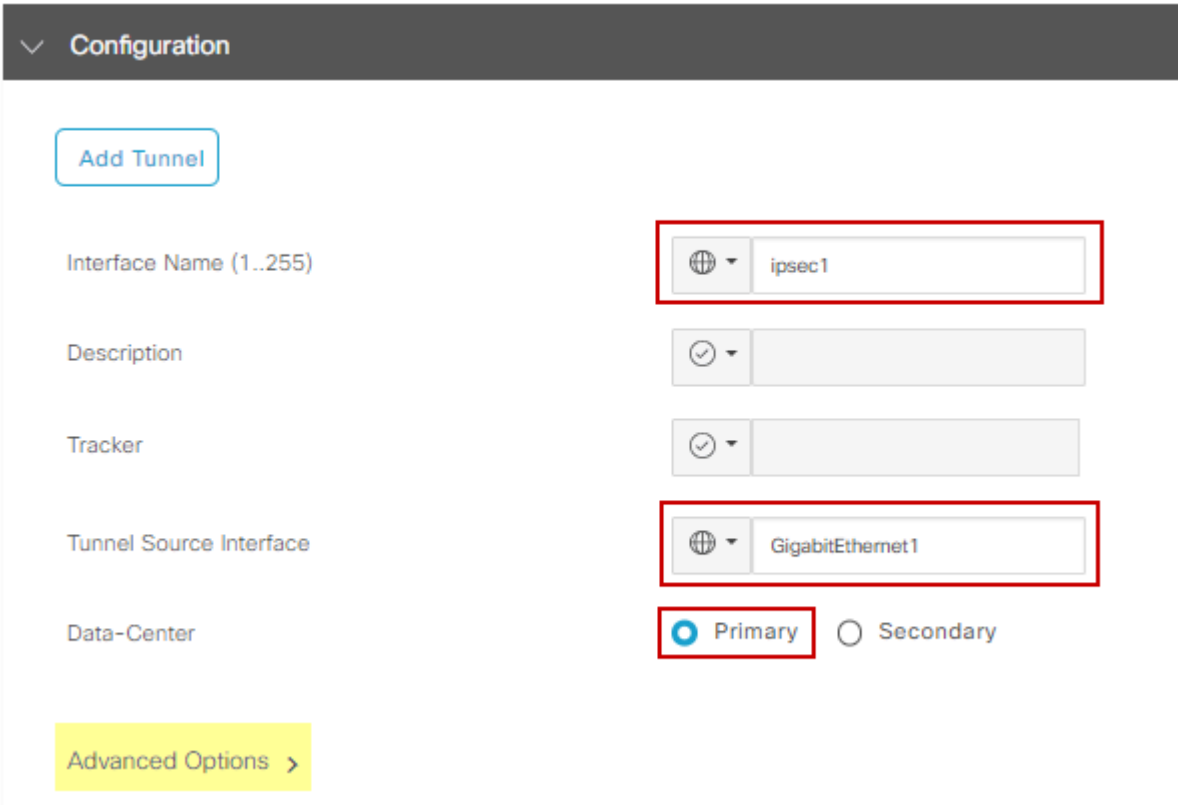
5. Cliquez sur Enregistrer.

6. Vous êtes redirigé vers le modèle Secure Internet Gateway (SIG). Ce modèle vous permet de configurer les éléments nécessaires pour SD-WAN IPsec SIG avec Zscaler.

Dans la première section du modèle, indiquez un nom et une description. Le tracker par défaut est automatiquement activé et utilise l'URL de l'API pour le contrôle d'état de la couche 7 de Zscaler.

7. 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.

8. Dans la section Configuration, vous pouvez créer les tunnels IPsec en cliquant sur Add Tunnel. Dans la nouvelle fenêtre contextuelle, effectuez vos sélections en fonction de vos besoins.
9. Dans cet exemple, l’interface IPsec1 a été créée en utilisant l’interface WAN GigabitEthernet1 comme source de tunnel. Il établit la connectivité avec le data center Zcaler principal. Il est recommandé de conserver les valeurs Options avancées par défaut.

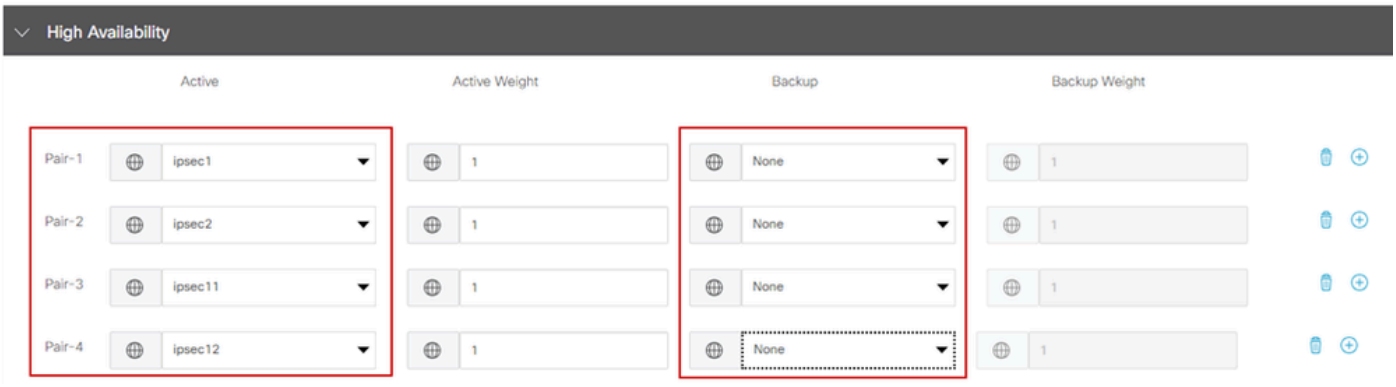


Configuration d'interface IPsec

Haute disponibilité

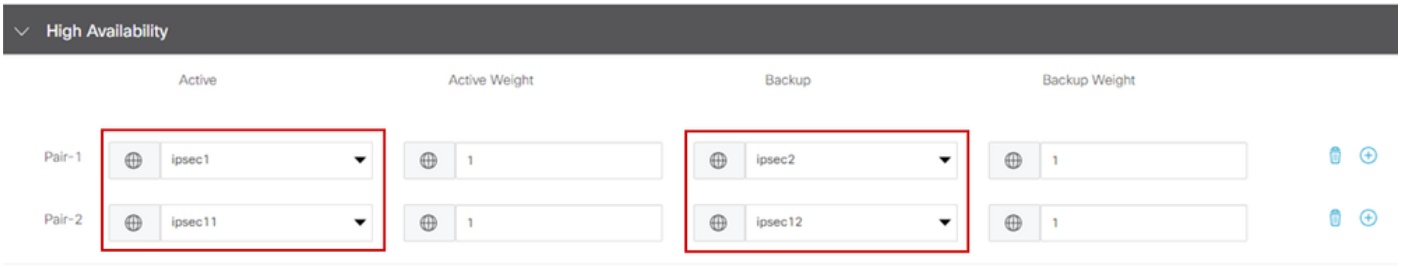
Dans cette section, choisissez si la conception est Active/Active ou Active/Standby, et déterminez quelle interface IPsec est active.

Il s'agit d'un exemple de conception Active/Active et toutes les interfaces sont sélectionnées sous Active, laissant Backup sans aucune interface.



Conception active/active

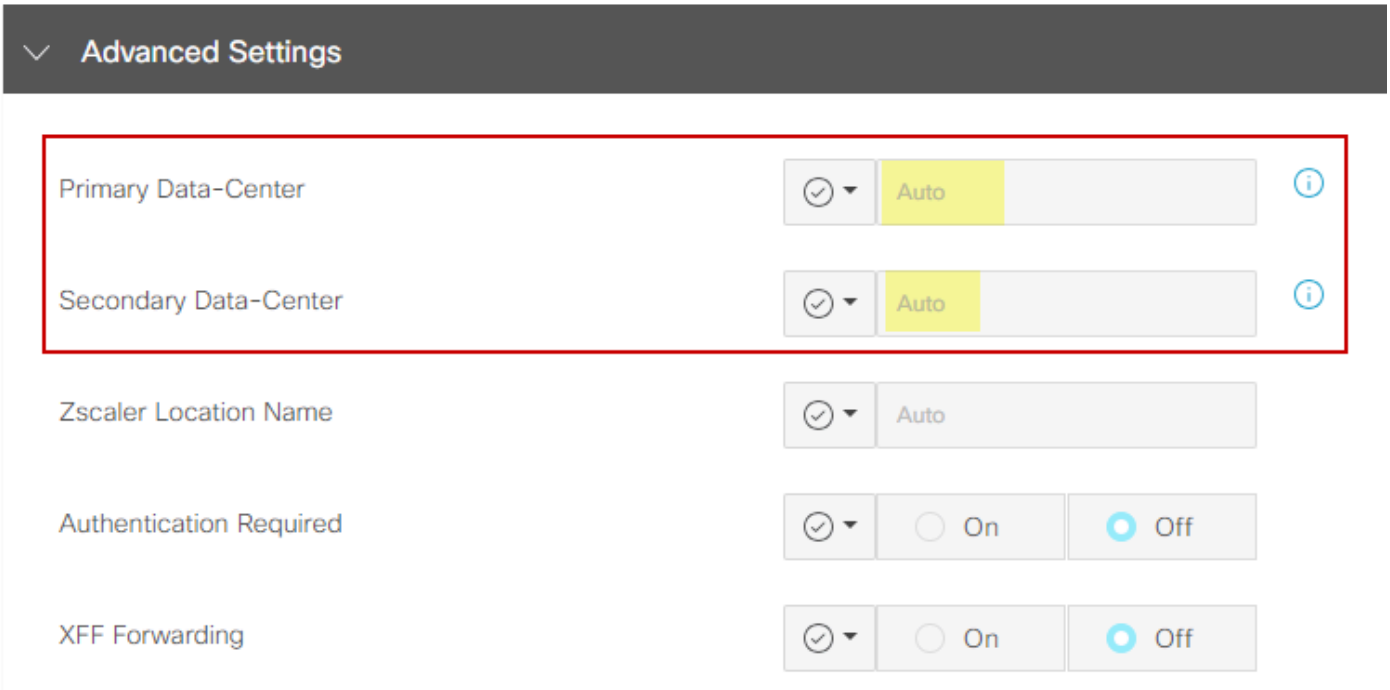
Cet exemple présente une conception active/veille et IPsec1 et IPsec11 sont sélectionnés en tant qu'interfaces actives, tandis que IPsec2 et IPsec12 sont désignés en tant qu'interfaces de veille.



Conception active/en veille

Paramètres avancés

1. 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 URL Partner Base.



Data centers automatiques ou manuels

2. Cliquez sur Enregistrer lorsque vous avez terminé.

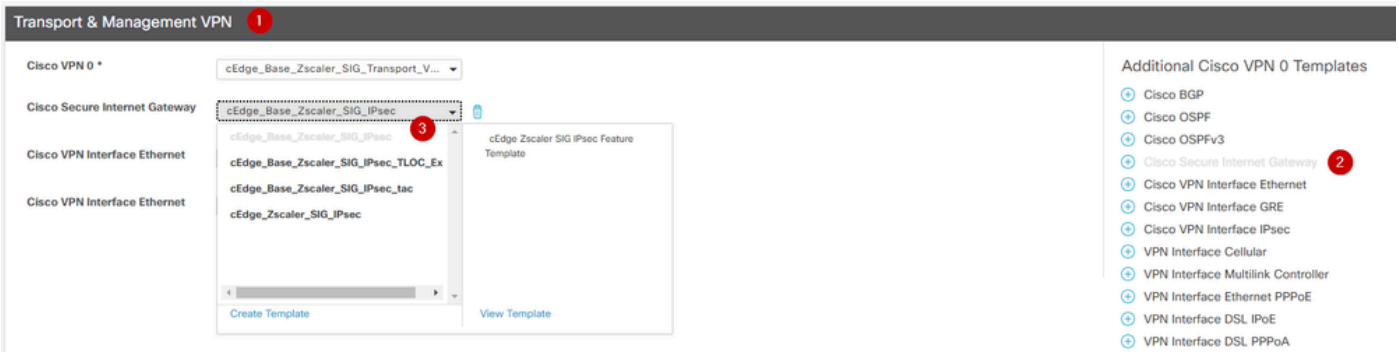
3. Une fois la configuration des modèles SIG terminée, vous devez les appliquer sous le modèle

de périphérique. De cette façon, la configuration est poussée sur les routeurs de périphérie Cisco.

4. Étapes suivantes, naviguez à Configuration > Modèles > Modèle de périphérique, sur les trois points cliquez sur Modifier.

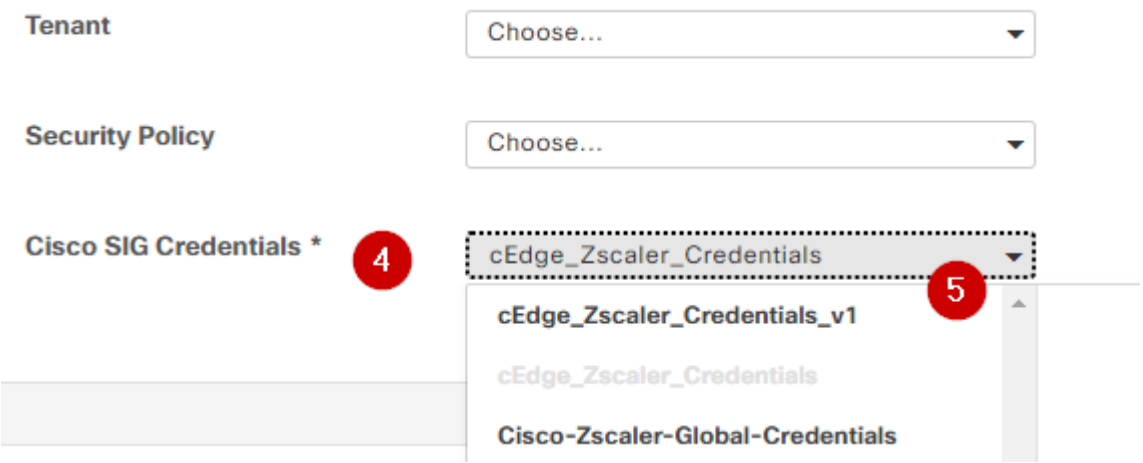
5. Sous Transport & Management VPN, ajoutez le modèle Secure Internet Gateway.

6. Sur la passerelle Internet sécurisée Cisco, sélectionnez le modèle de fonction SIG approprié dans le menu déroulant.



Ajouter un modèle SIG au modèle de périphérique

7. Sous Additional Templates in Cisco SIG Credentials, sélectionnez le modèle Cisco SIG Credentials approprié dans le menu déroulant :



Modèle Credential SIG

8. Cliquez sur Mettre à jour (si votre modèle de périphérique est un modèle actif, suivez les étapes standard pour appliquer les configurations sur un modèle actif).

Vérifier

1. 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>
    !
```

2. 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
```

3. Des configurations supplémentaires sont ajoutées, telles que des profils et des politiques crypto ikev2, plusieurs interfaces commencent par Tunnel1xxxxx, vrf definition 65530 et 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
```

4. Une fois que les configurations ont été transmises avec succès aux routeurs de périphérie Cisco, vous pouvez exécuter des commandes pour vérifier si les tunnels sont disponibles :

<#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. Si vous ne voyez pas le code resp http 200, cela signifie que vous êtes confronté à un problème avec le mot de passe ou la clé partenaire.
6. Pour vérifier l'état de l'interface, utilisez cette commande :

<#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. Pour vérifier l'état du dispositif de suivi, exécutez les commandes show endpoint-tracker et show endpoint-tracker records. Cela vous aide à confirmer l'URL utilisée par le traqueur :

```
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. Les autres validations que vous pouvez utiliser sont les suivantes :

- Assurez-vous que les routes sur VRF pointent vers les tunnels IPsec et 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
```

9. Pour valider davantage, vous pouvez envoyer une requête ping vers Internet et effectuer une route de suivi pour valider les sauts du trafic :

<#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







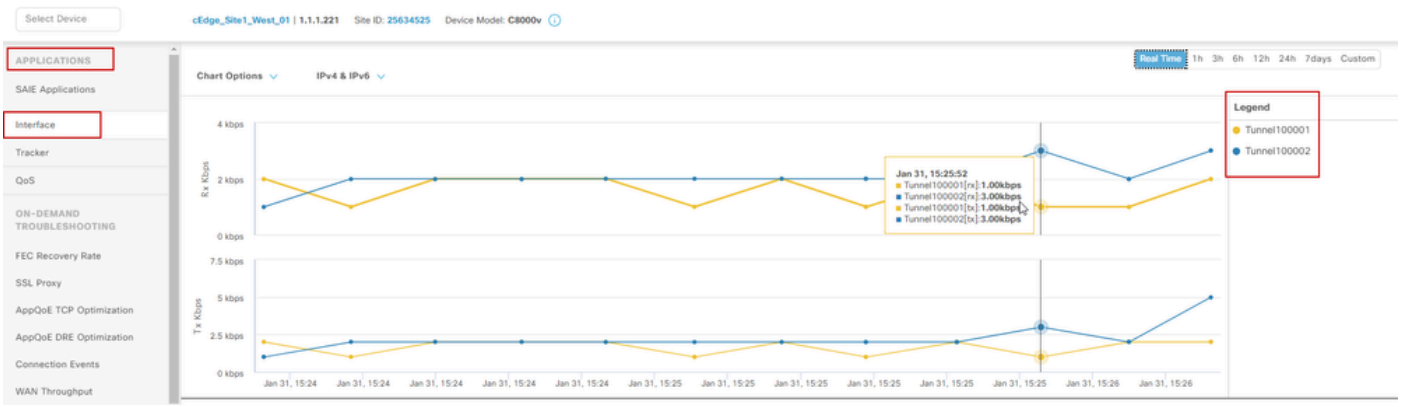


 199 msec *
.....
```

10. Vous pouvez valider les interfaces IPsec à partir de l'interface utilisateur graphique de

vManage en naviguant vers Monitor > Device ou Monitor > Network (pour les codes 20.6 et antérieurs).

- Sélectionnez votre routeur et accédez à Applications > Interfaces.
- Sélectionnez Tunnel10001 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, passez en revue ces étapes pour résoudre les problèmes suivants :

Étape 1: Vérifiez les erreurs en exécutant 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 du 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-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
```

Étape 2. 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

À partir de Cisco IOS® Version IOS-XE 17.11+, <debug platform> a été migré vers <set platform trace>

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

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 | verbeux]

1. Voici un exemple du résultat 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
```

2. Exécutez la commande show ip interface brief et vérifiez le protocole d'interface des tunnels et vérifiez si ceux-ci sont activés ou désactivés.

<#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. Après avoir vérifié qu'il n'y a aucun problème avec les informations d'identification Zscaler, supprimez l'interface SIG du modèle de périphérique et poussez-la 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.