Configurazione e verifica del tunnel SIG IPsec SD-WAN con Zscaler

Sommario

Introduzione

In questo documento vengono descritti i passaggi di configurazione e la verifica dei tunnel SIG IPsec SD-WAN con Zscaler.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Security Internet Gateway (SIG).
- Funzionamento dei tunnel IPsec, fase 1 e fase 2, su Cisco IOS®.

Requisiti aggiuntivi

- NAT deve essere abilitato sull'interfaccia di trasporto che sarà collegata a Internet.
- È necessario creare un server DNS sulla VPN 0 e risolvere l'URL di base Zscaler con questo server DNS. Questa operazione è importante perché, se non viene risolta, le chiamate API avranno esito negativo. Anche i controlli di integrità di layer 7 avranno esito negativo, poiché per impostazione predefinita l'URL è: http://gateway.<zscalercloud>.net/vpntest.

- Il protocollo NTP (Network Time Protocol) deve garantire che l'ora del Cisco Edge Router sia precisa e che le chiamate API non abbiano esito negativo.
- È necessario configurare un percorso di servizio che punta a SIG nel modello della funzionalità Service-VPN o nella CLI:
  ip sdwan route vrf 1.0.0.0.0/0 service sig

Componenti usati

Questo documento si basa sulle seguenti versioni software e hardware:

- Cisco Edge Router versione 17.6.6a
- vManage versione 20.9.4

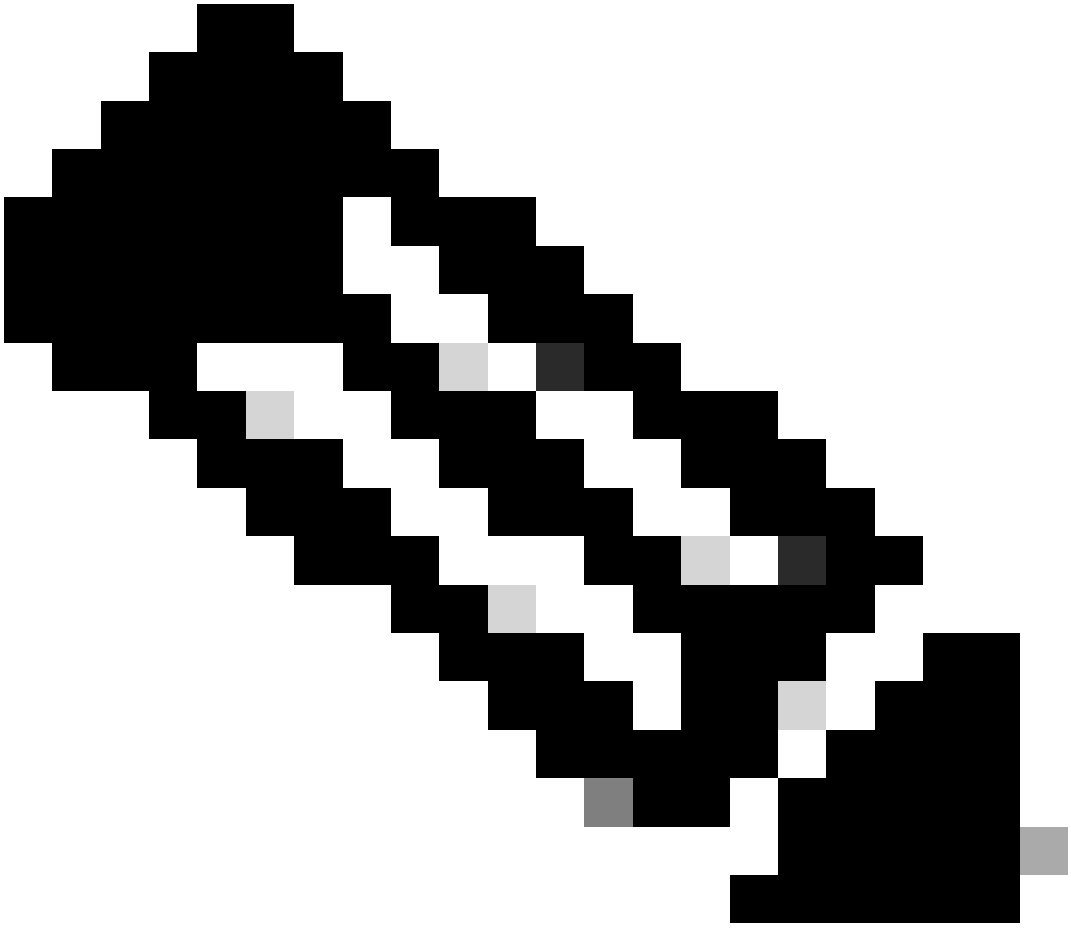
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Opzioni di progettazione della rete

Di seguito sono elencati i vari tipi di distribuzione in un'installazione combinata attiva/standby. L'incapsulamento del tunnel può essere distribuito sia su GRE che su IPsec.

- Una Coppia Di Tunnel Attivo/Standby.
- Una coppia di tunnel attiva/attiva.
- Più coppie di tunnel attivo/standby.
- Più coppie di tunnel attive/attive.



Nota: sui router perimetrali Cisco SD-WAN, è possibile utilizzare una o più interfacce di trasporto connesse a Internet, per un funzionamento efficace della configurazione.

Configurazioni

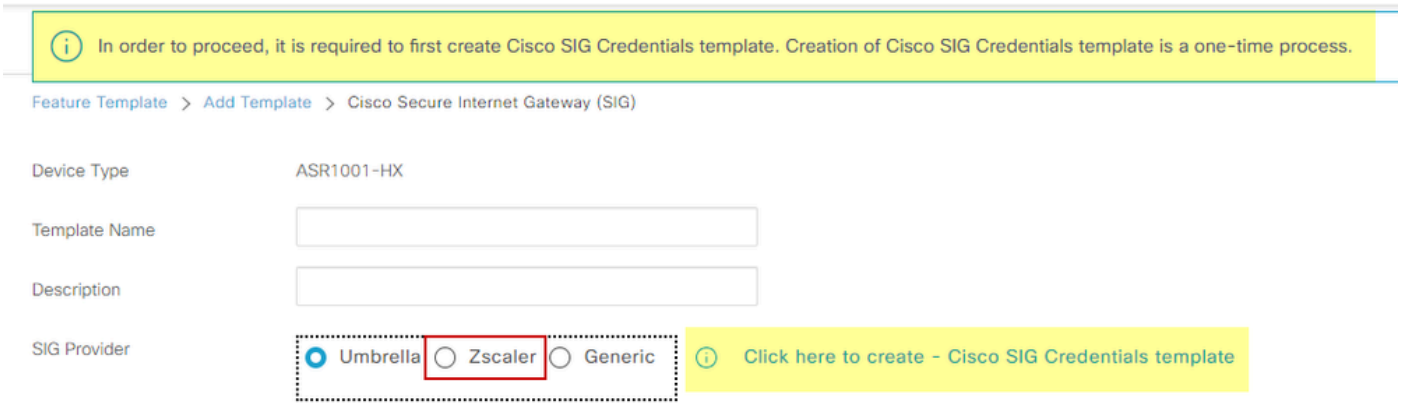
Procedere con la configurazione dei seguenti modelli:

- Modello funzionalità credenziali Security Internet Gateway (SIG):
  - Ne è necessario uno per tutti i router Cisco Edge. Le informazioni per compilare i campi necessari del modello devono essere create sul portale Zscaler.
- Modello di funzionalità Security Internet Gateway (SIG):
  - In questo modello di funzionalità è possibile configurare i tunnel IPSec, garantire l'elevata disponibilità (HA, Deployment High Availability) in modalità attiva/attiva o attiva/standby e selezionare Zscaler Datacenter automaticamente o manualmente.

Per creare un modello di credenziali Zscaler, selezionare Configurazione > Modello > Modello

funzionalità > Aggiungi modello.

Selezionare il modello di dispositivo che si desidera utilizzare per questo scopo e cercare SIG. Quando la create per la prima volta, il sistema mostra che è necessario creare prima le credenziali Zscaler, come nell'esempio seguente:
Selezionare Zscaler come provider SIG e fare clic sul modello Click here to create - Cisco SIG Credentials.



Firma modello di credenziali

"

L'utente viene reindirizzato al modello Credenziali. In questo modello è necessario immettere i valori per tutti i campi:

- Nome modello
- Descrizione
- Provider SIG (selezionato automaticamente dal passaggio precedente)
- Organizzazione
- URI di base partner
- Username
- Password
- Chiave API partner

Fare clic su Save (Salva).

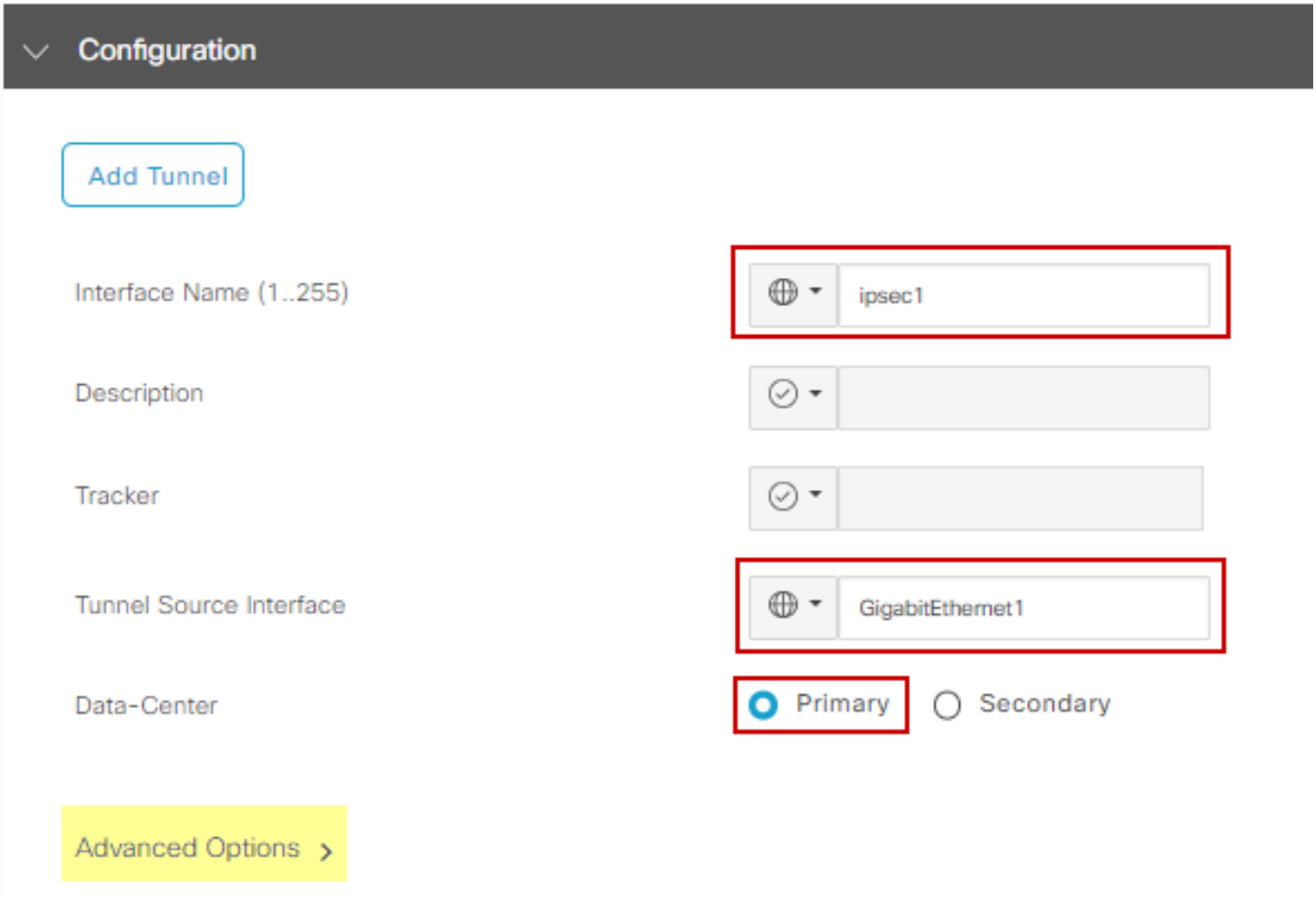
L'utente viene reindirizzato al modello SIG (Secure Internet Gateway). Questo modello consente di configurare tutto il necessario per SD-WAN IPsec SIG con Zscaler.

Nella prima sezione del modello, fornire un nome e una descrizione. Il tracciatore predefinito viene attivato automaticamente. L'URL dell'API utilizzato per il controllo dello stato di Zscaler Layer 7 è: zscaler_L7_health_check) ishttp://gateway<zscalercloud>net/vpntest.

In Cisco IOS XE, è necessario impostare un indirizzo IP per il tracker. Qualsiasi indirizzo IP privato compreso nell'intervallo /32 è accettabile. L'indirizzo IP impostato può essere utilizzato dall'interfaccia Loopback 65530, che viene creata automaticamente per l'esecuzione delle ispezioni di integrità Zscaler.

Nella sezione Configurazione è possibile creare i tunnel IPsec facendo clic su Aggiungi tunnel. Nella nuova finestra popup effettuare le selezioni in base alle proprie esigenze.

Nell'esempio, è stata creata l'interfaccia IPsec1, utilizzando l'interfaccia WAN Gigabit Ethernet1 come origine del tunnel. In questo modo è possibile creare la connettività con il data center Zcaler principale.
È consigliabile mantenere i valori delle opzioni avanzate come predefiniti.

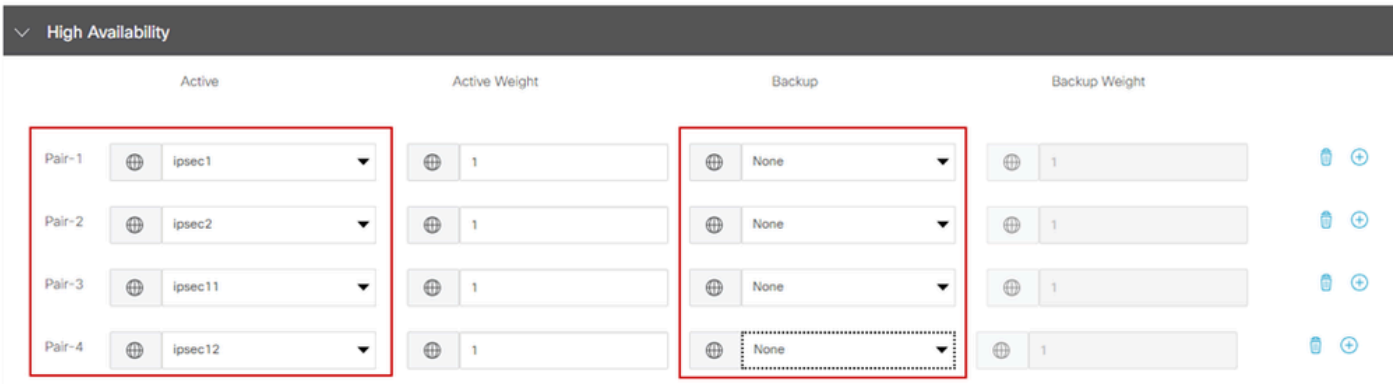


Configurazione interfaccia IPsec

Alta disponibilità

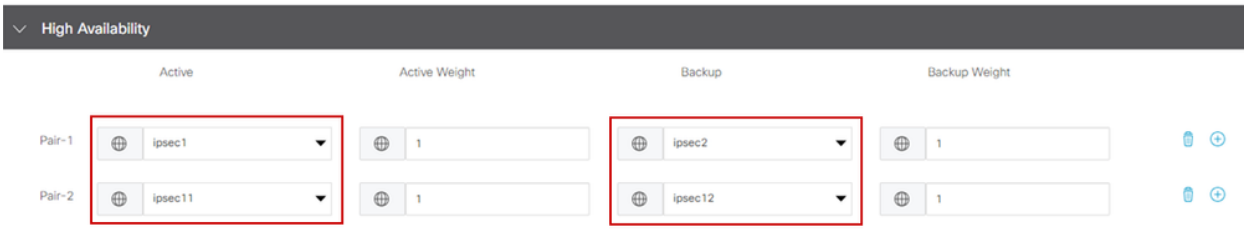
In questa sezione è possibile scegliere se il progetto sarà Attivo/Attivo o Attivo/Standby e determinare l'interfaccia IPSec da attivare.

Questo è un esempio di progettazione attiva/attiva. Tutte le interfacce sono selezionate in Attivo, lasciando Backup senza.



Progettazione attiva

In questo esempio viene illustrata una progettazione attiva/standby. IPsec1 e IPsec11 sono interfacce attive, mentre IPsec2 e IPsec12 sono interfacce in standby.



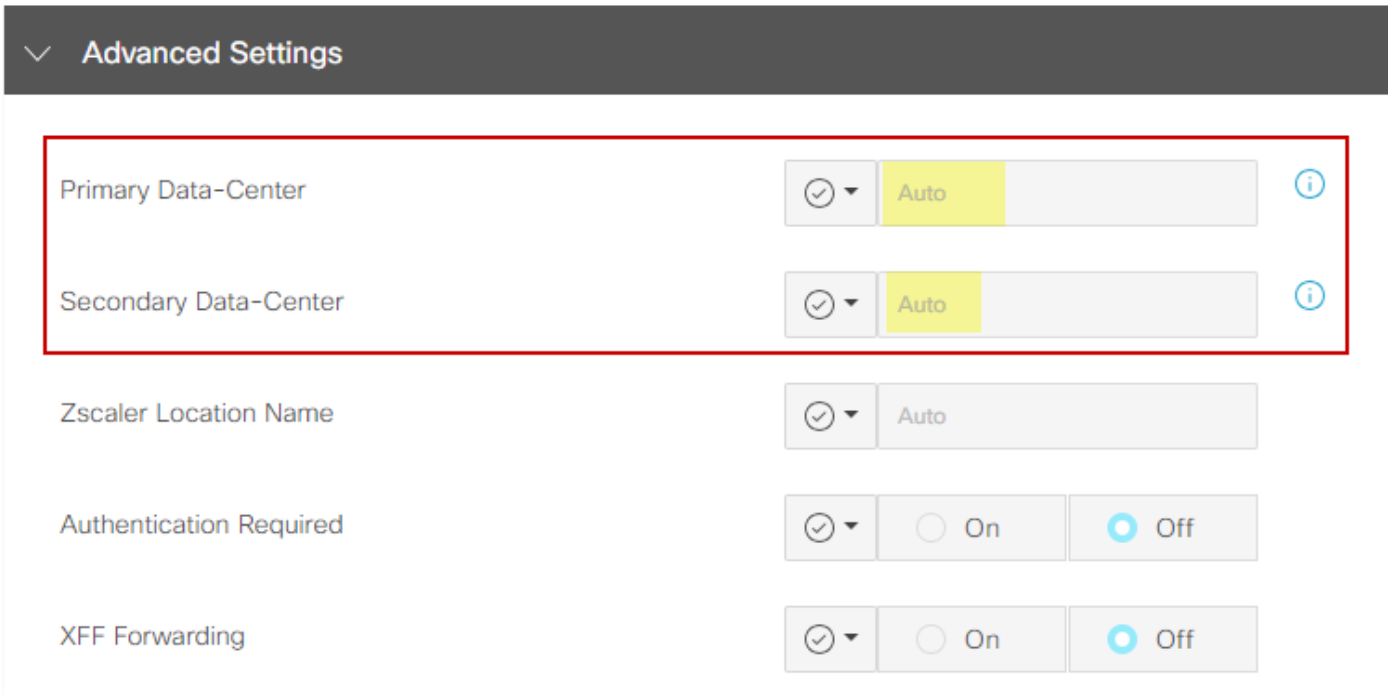
Progettazione attiva/standby

Impostazioni avanzate

In questa sezione, le configurazioni più importanti sono il centro dati principale e il centro dati secondario.

Si consiglia di configurare entrambe le opzioni come automatica o manuale, ma non è consigliabile configurarle come miste.

Se si sceglie di configurarli manualmente, selezionare l'URL corretto dal portale Zscaler, in base all'URI di base del partner



Centri dati automatici o manuali

Al termine, fare clic su Save (Salva).

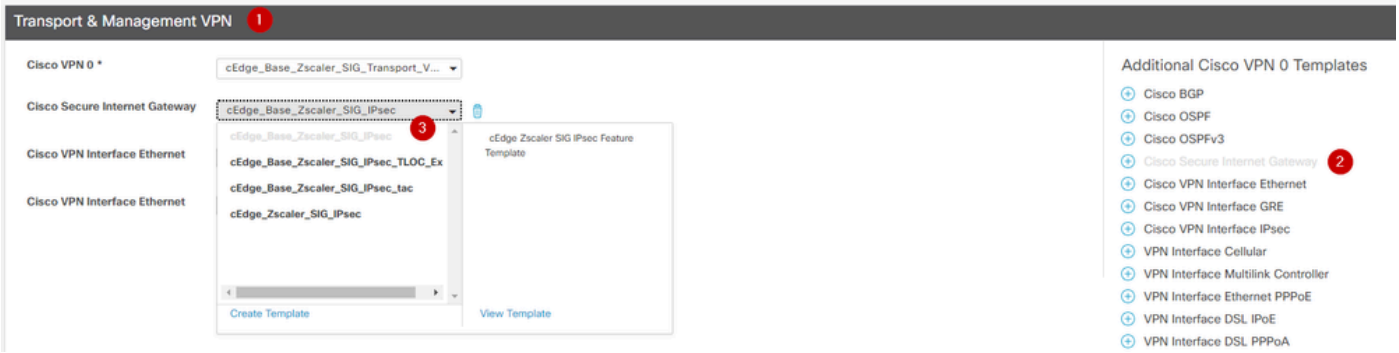
Al termine della configurazione dei modelli SIG, è necessario applicarli nel modello del dispositivo. In questo modo, la configurazione viene trasferita sui router perimetrali Cisco.

Per completare la procedura descritta, selezionare Configurazione > Modelli > Modello dispositivo, fare clic su Modifica in tre punti.

1. Alla voce Trasporti e gestione VPN

2. Aggiungere il modello Secure Internet Gateway.

3. Su Cisco Secure Internet Gateway, selezionare il modello di funzionalità SIG corretto dal menu a discesa.

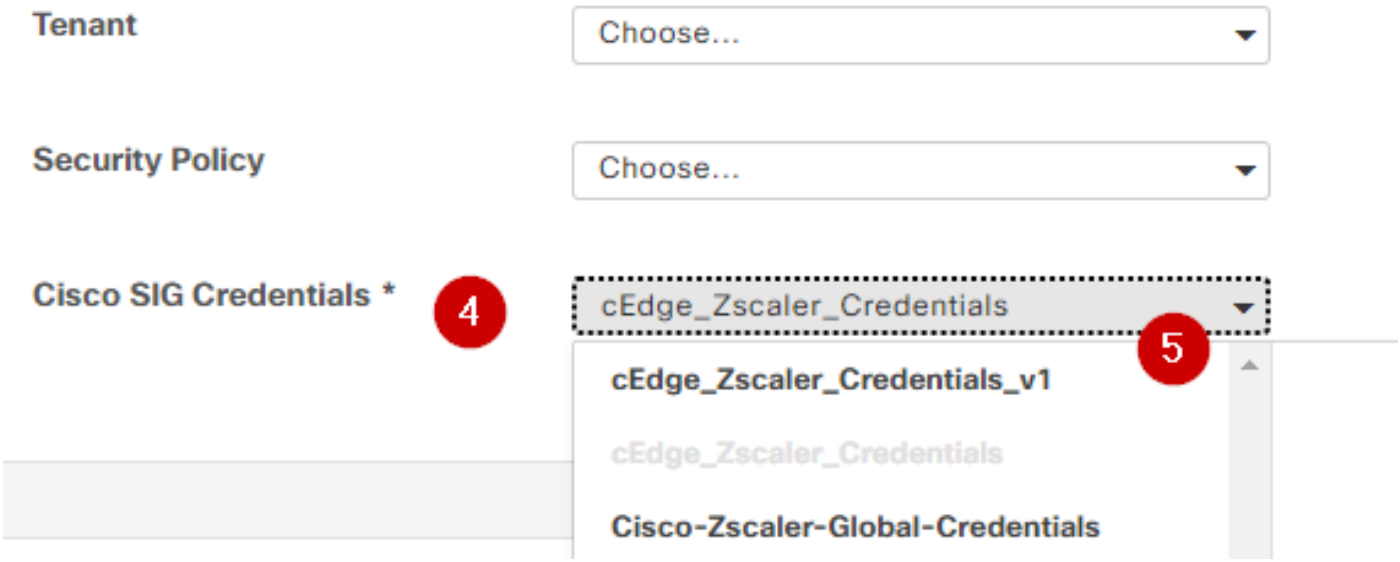


Aggiungi modello SIG su modello dispositivo

In Modelli aggiuntivi

4. Nelle credenziali Cisco SIG

5. Selezionare il modello di credenziali Cisco SIG corretto dal menu a discesa:



Modello SIG credenziali

Fare clic su Aggiorna. Se il modello di dispositivo è attivo, attenersi alla procedura standard per eseguire il push delle configurazioni su un modello attivo.

Verifica

La verifica può essere eseguita durante l'anteprima della configurazione mentre si esegue il push delle modifiche. È necessario notare quanto segue:

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

Da questo esempio si può vedere che il progetto è attivo/in standby

<#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
```

Si noterà che vengono aggiunte altre configurazioni come i profili e le policy crypto ikev2, più interfacce a partire da Tunnel1xxxxx, vrf definizione 65530, ip sdwan route vrf 1 0.0.0.0/0 service sig.

Tutte queste modifiche fanno parte dei tunnel IPsec SIG con Zscaler.

Nell'esempio viene mostrato come appare la configurazione dell'interfaccia del 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
```

Dopo aver eseguito correttamente il push delle configurazioni sui router perimetrali Cisco, è possibile utilizzare i comandi per verificare se i tunnel sono in corso o meno.

<#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
```

Se http resp code 200 non è visibile, significa che si è verificato un problema relativo alla password o alla chiave del partner.

Per verificare lo stato delle interfacce, usare il comando.

<#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
```

Per verificare lo stato del tracker, eseguire i comandi show endpoint-tracker e show endpoint-tracker records. Ciò consente di confermare l'URL utilizzato dal tracker

```
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
```

Altre convalide che è possibile eseguire sono:
Per verificare che le route sul VRF puntino ai tunnel IPsec, eseguire questo comando:

show ip route vrf 1

Il gateway di ultima istanza è 0.0.0.0 alla rete 0.0.0.0

S* 0.0.0.0/0 [2/65535], Tunnel100002
[2/65535], Tunnel100001
10.0.0.0/8 è subnet in modo variabile, 4 subnet, 2 maschere

Per eseguire una convalida ancora maggiore, è possibile eseguire il ping verso Internet e seguire una traccia degli hop attraversati dal traffico:

<#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>

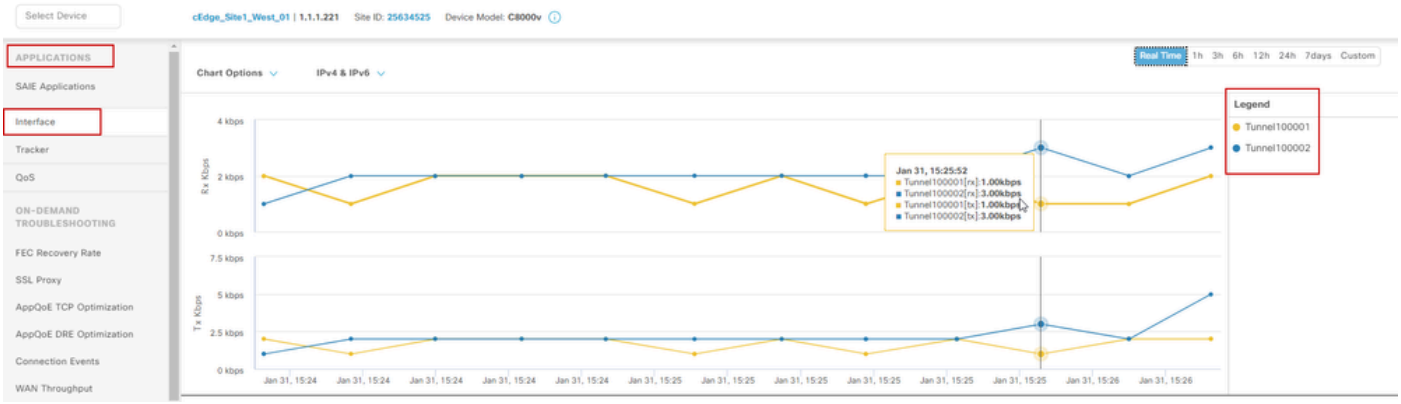
```
 200 msec
```

<The IP here need to be Zcaler IP>

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

È possibile convalidare le interfacce IPsec dalla GUI di vManage selezionando Monitor > Dispositivo o Monitor > Rete (per i codici 20.6 e precedenti).

- Selezionare il router e selezionare Applicazioni > Interfacce.
- Selezionare Tunnel100001 e Tunnel100002 per visualizzare il traffico in tempo reale o personalizzare in base all'intervallo di tempo richiesto:



Monitoraggio dei tunnel IPsec

Risoluzione dei problemi

Se il tunnel SIG non è in esecuzione, procedere come segue per risolvere il problema.

Passaggio 1: controllare gli errori utilizzando il comando show sdwan secure-internet-gateway zscaler tunnel. Dall'output, se si nota il codice RESP HTTP 401, si è verificato un problema di autenticazione.

È possibile verificare i valori nel modello di credenziali SIG per verificare se la password o la chiave del partner è corretta.

<#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 F

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
```

Per ulteriori operazioni di debug, abilitare questi comandi e cercare i messaggi di log relativi a SIG, HTTP o tracker:

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

Questo è un esempio di output dei comandi di 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
```

Eseguire il comando show ip interface brief e controllare il protocollo dell'interfaccia dei tunnel se

sono visualizzati.

<#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
```

Dopo aver verificato che non vi siano problemi con le credenziali Zscaler, è possibile rimuovere l'interfaccia SIG dal modello del dispositivo e spingerla sul router.

Una volta completato il push, applicare il modello SIG e spostarlo nuovamente sul router. Questo metodo forza la ricreazione da zero dei tunnel.

Informazioni correlate

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).