Zscaler를 사용하여 SD-WAN IPsec SIG 터널 구성 및 확인

목차

소개

이 문서에서는 Zscaler를 사용한 SD-WAN IPsec SIG 터널의 컨피그레이션 단계 및 확인에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 보안 SIG(인터넷 게이트웨이).
- Cisco IOS®의 IPsec 터널 작동 방식, 1단계 및 2단계.

추가 요구 사항

- 인터넷에 연결할 전송 인터페이스에서 NAT를 활성화해야 합니다.
- VPN 0에서 DNS 서버를 만들고 이 DNS 서버로 Zscaler 기본 URL을 확인해야 합니다. 이렇게 해도 해결되지 않으면 API 호출이 실패하기 때문에 중요합니다. 레이어 7 상태 검사도 실패합니다. 기본적으로 URL은 http://gateway.<zscalercloud>.net/vpntest이기 때문입니다.
- NTP(Network Time Protocol)는 Cisco Edge Router 시간이 정확하고 API 호출이 실패하지 않

는지 확인해야 합니다.

- SIG를 가리키는 서비스 경로는 Service-VPN Feature Template(서비스 VPN 기능 템플릿) 또는 CLI에서 구성해야 합니다.
  ip sdwan route vrf 1 0.0.0.0/0 service sig

사용되는 구성 요소

이 문서는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Edge Router 버전 17.6.6a
- vManage 버전 20.9.4

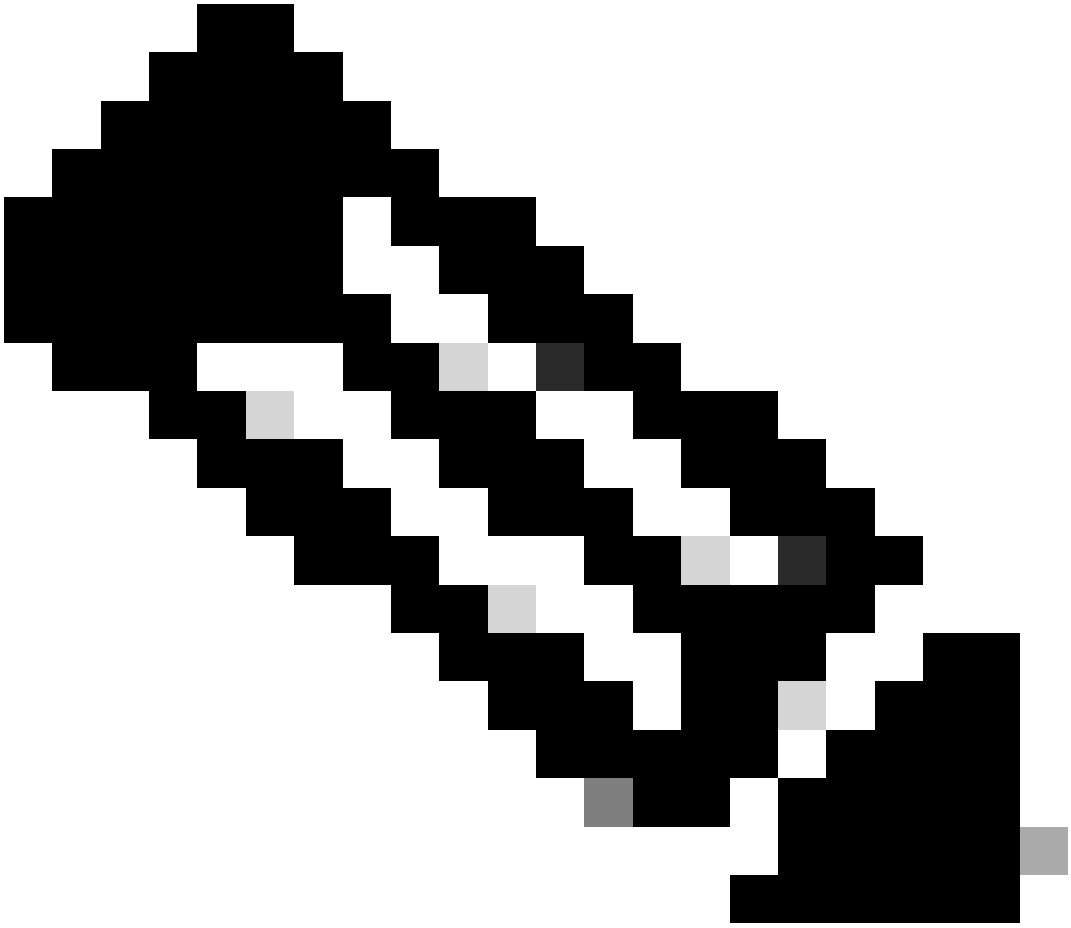
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

네트워크 설계 옵션

다음은 활성/대기 조합 설정의 다양한 구축 유형입니다. 터널 캡슐화는 GRE 또는 IPsec으로 구축할 수 있습니다.

- 액티브/스탠바이 터널 쌍 1개
- 활성/활성 터널 쌍 1개
- 여러 활성/대기 터널 쌍
- 여러 활성/활성 터널 쌍



참고: SD-WAN Cisco Edge Router에서는 이러한 설정이 효과적으로 작동하기 위해 인터넷에 연결된 하나 이상의 전송 인터페이스를 사용할 수 있습니다.

설정

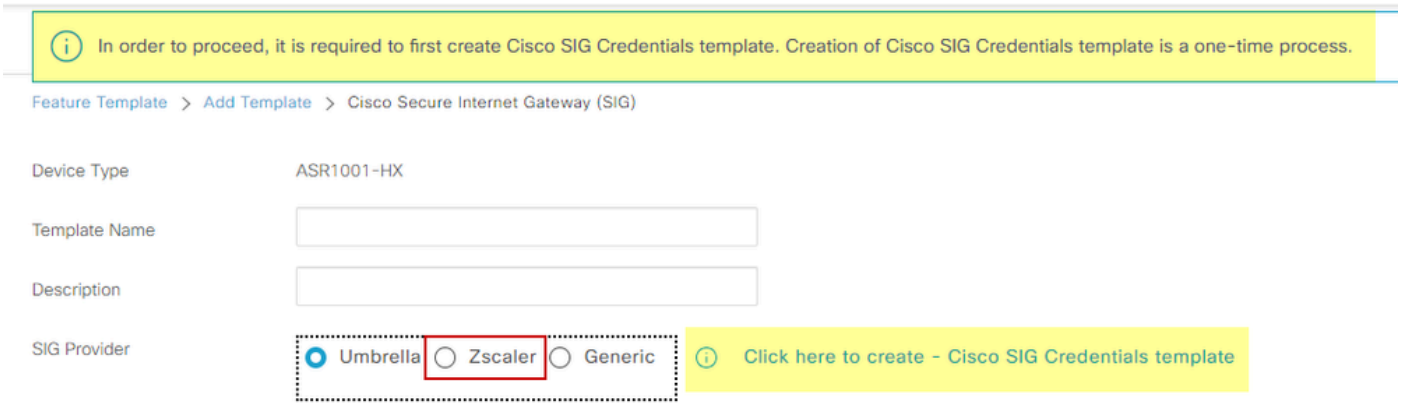
다음 템플릿 구성을 진행합니다.

- 보안 인터넷 게이트웨이(SIG) 자격 증명 기능 템플릿:
  - 모든 Cisco Edge Router에는 1개가 필요합니다. 템플릿의 필수 필드를 채우기 위한 정보를 Zscaler 포털에서 생성해야 합니다.
- 보안 인터넷 게이트웨이(SIG) 기능 템플릿:
  - 이 기능 템플릿에서 IPsec 터널을 구성하고 액티브/액티브 또는 액티브/스탠바이 모드에서 HA(High Availability)를 구축하며 Zscaler Datacenter를 자동 또는 수동으로 선택합니다.

Zscaler Credentials(Zscaler 자격 증명) 템플릿을 만들려면 Configuration(컨피그레이션) >

Template(템플릿) > Feature Template(기능 템플릿) > Add Template(템플릿 추가)으로 이동합니다
.

이 용도로 사용할 디바이스 모델을 선택하고 SIG를 검색합니다. 처음 생성할 때 시스템은 다음 예제와 같이 Zscaler 자격 증명을 먼저 생성해야 함을 보여 줍니다.
Zscaler를 SIG 제공자로 선택하고 Click here to create - Cisco SIG Credentials(여기를 클릭하여 생성) 템플릿을 클릭해야 합니다.



Sig 인증서 템플릿

"

자격 증명 템플릿으로 리디렉션됩니다. 이 템플릿에서 모든 필드의 값을 입력해야 합니다.

- 템플릿 이름
- 설명
- SIG 제공자(이전 단계에서 자동으로 선택됨)
- 조직
- 파트너 기본 URI
- 사용자 이름
- 암호
- 파트너 API 키

저장을 클릭합니다.

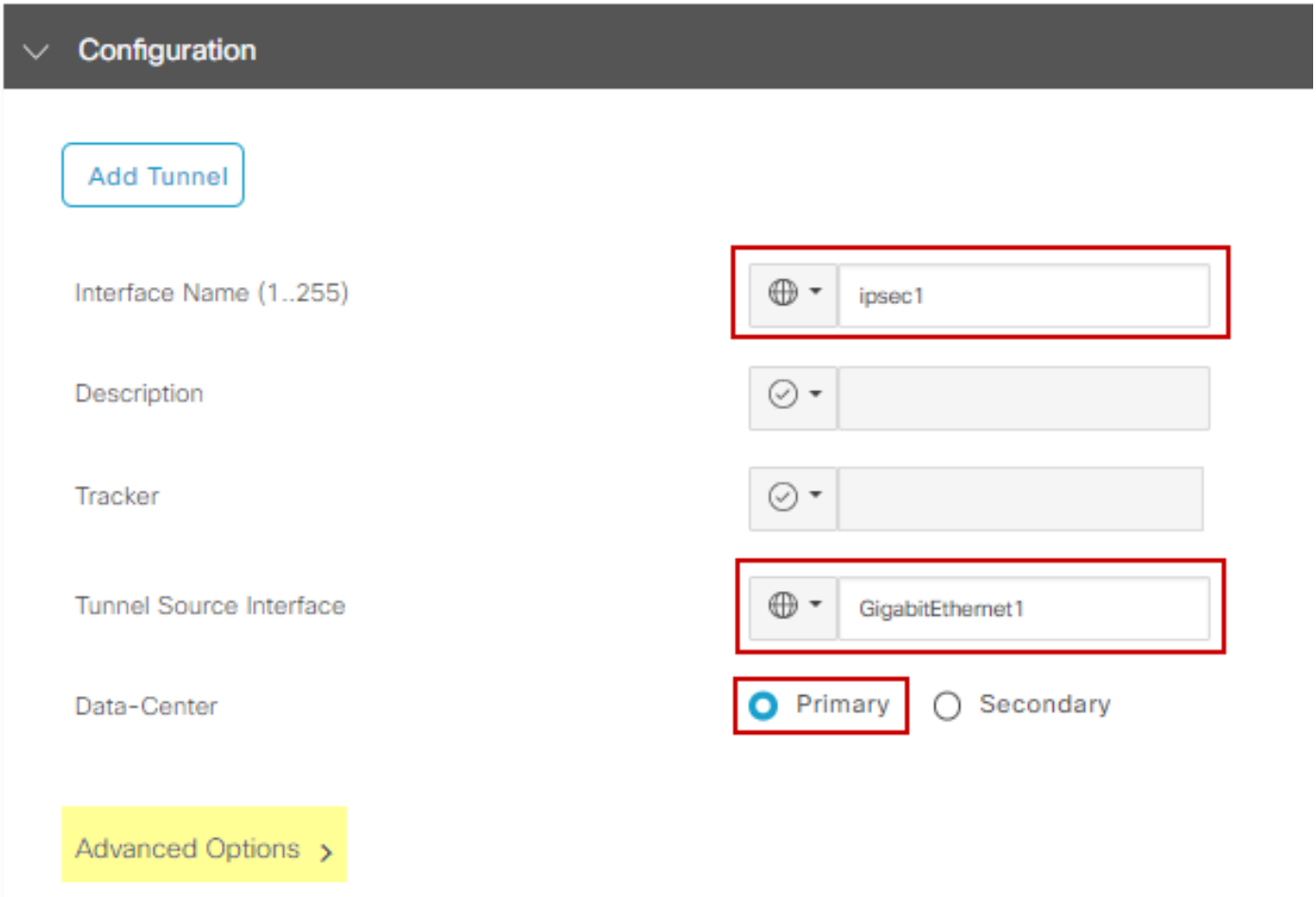
SIG(Secure Internet Gateway) 템플릿으로 리디렉션됩니다. 이 템플릿을 사용하여 SD-WAN IPsec SIG with Zscaler에 필요한 모든 것을 구성할 수 있습니다.

템플릿의 첫 번째 섹션에 이름과 설명을 입력하십시오. 기본 추적기는 자동으로 활성화됩니다. Zscaler Layer 7 상태 검사에 사용되는 API URL은 zscaler_L7_health_check) ishttp://gateway<zscalercloud>net/vpntest입니다.

Cisco IOS XE에서는 추적기의 IP 주소를 설정해야 합니다. /32 범위 내의 모든 개인 IP를 사용할 수 있습니다. 설정한 IP 주소는 Zscaler 상태 검사를 수행하기 위해 자동으로 만들어지는 루프백 65530 인터페이스에서 활용할 수 있습니다.

Configuration(컨피그레이션) 섹션에서 Add Tunnel(터널 추가)을 클릭하여 IPsec 터널을 생성할 수 있습니다. 새 팝업 창에서 요구 사항에 따라 선택합니다.

이 예에서는 WAN 인터페이스 GigabitEthernet1을 터널 소스로 사용하여 인터페이스 IPsec1을 생성했습니다. 그런 다음 Primary Zcaler Data-Center와의 연결을 형성할 수 있습니다.
고급 옵션 값을 기본값으로 유지하는 것이 좋습니다.

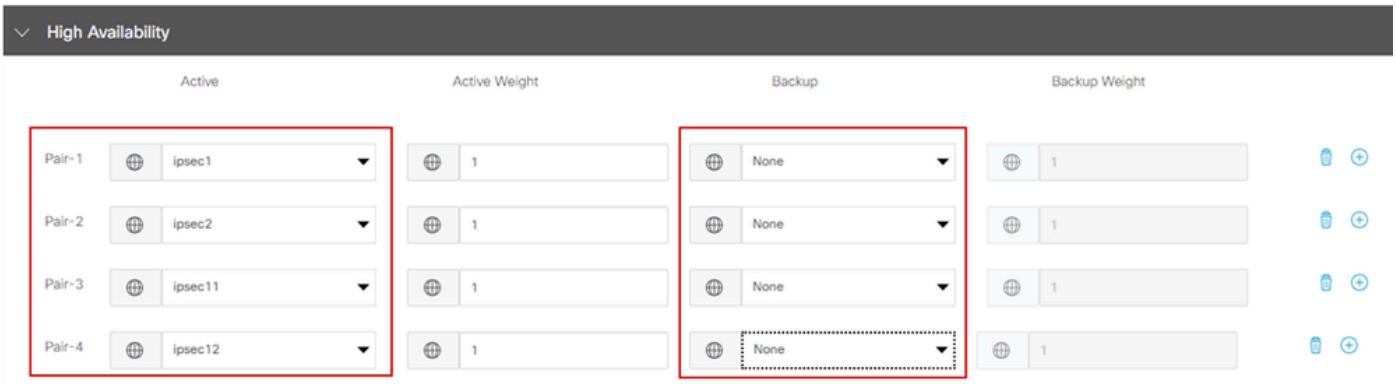


IPsec 인터페이스 컨피그레이션

고가용성

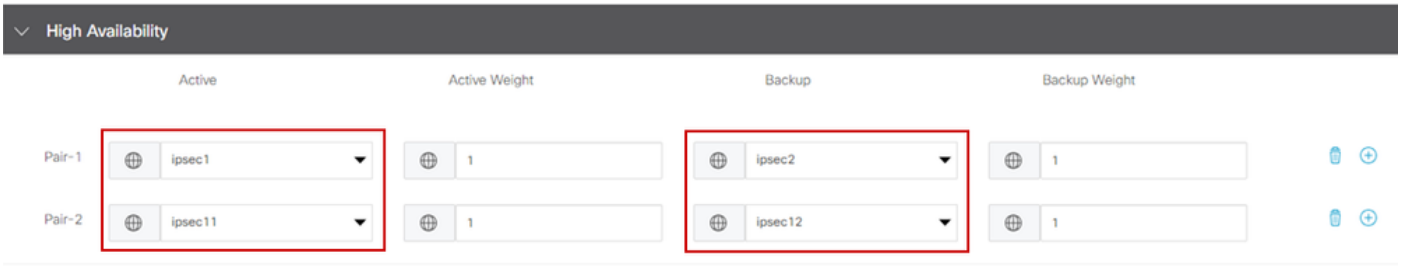
이 섹션에서는 설계가 액티브/액티브 또는 액티브/스탠바이 중 어떤 IPsec 인터페이스를 액티브 상태로 설정할지 선택합니다.

액티브/액티브 설계의 예입니다. 모든 인터페이스가 Active(활성)에서 선택되므로 Backup(백업)은 none(없음)으로 유지됩니다.



액티브/액티브 설계

이 예에서는 Active/Standby 설계를 보여 줍니다. IPsec1 및 IPsec11은 액티브 인터페이스로 선택되고 IPsec2 및 IPsec12는 스탠바이 인터페이스로 지정됩니다.



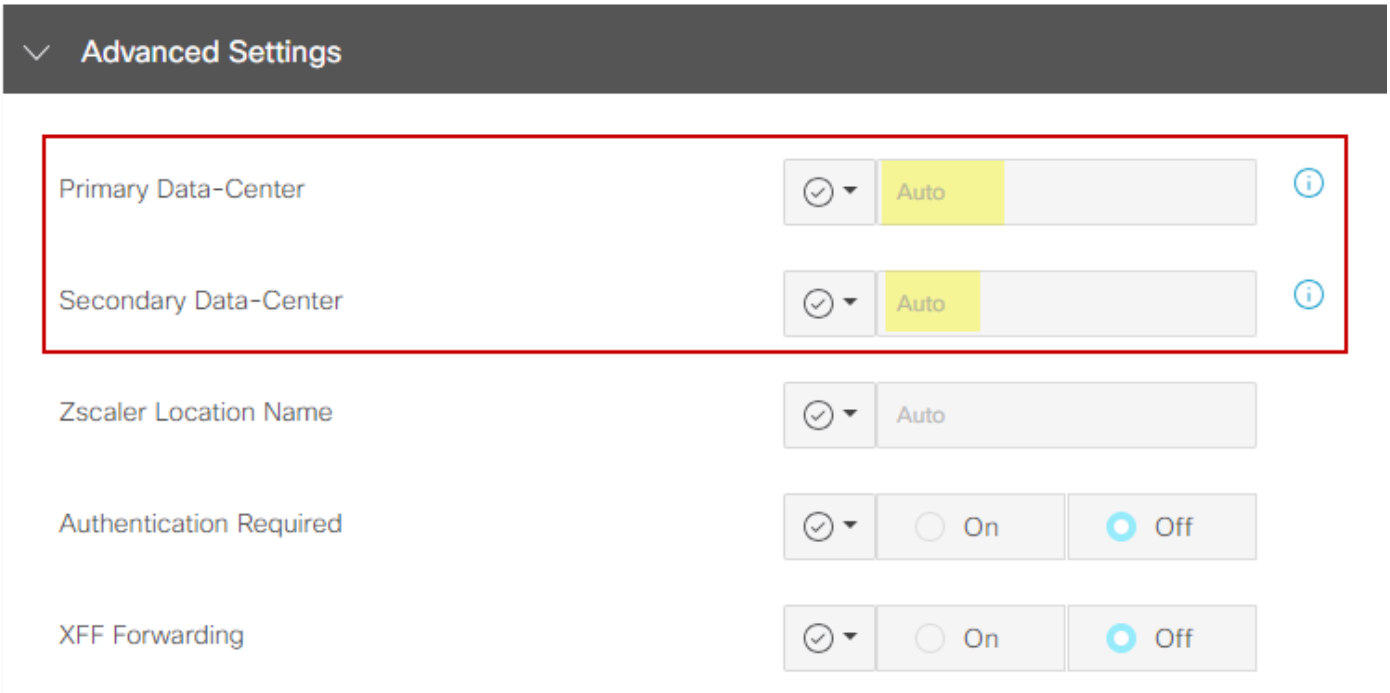
액티브/스탠바이 설계

고급 설정

이 섹션에서 가장 중요한 컨피그레이션은 기본 데이터 센터와 보조 데이터 센터입니다.

둘 다 자동 또는 수동으로 구성하는 것이 좋지만 혼합으로 구성하는 것은 좋지 않습니다.

수동으로 구성하도록 선택하는 경우 Partner Base URI에 따라 Zscaler 포털에서 올바른 URL을 선택하십시오.



자동 또는 수동 데이터 센터

완료되면 Save(저장)를 클릭합니다.

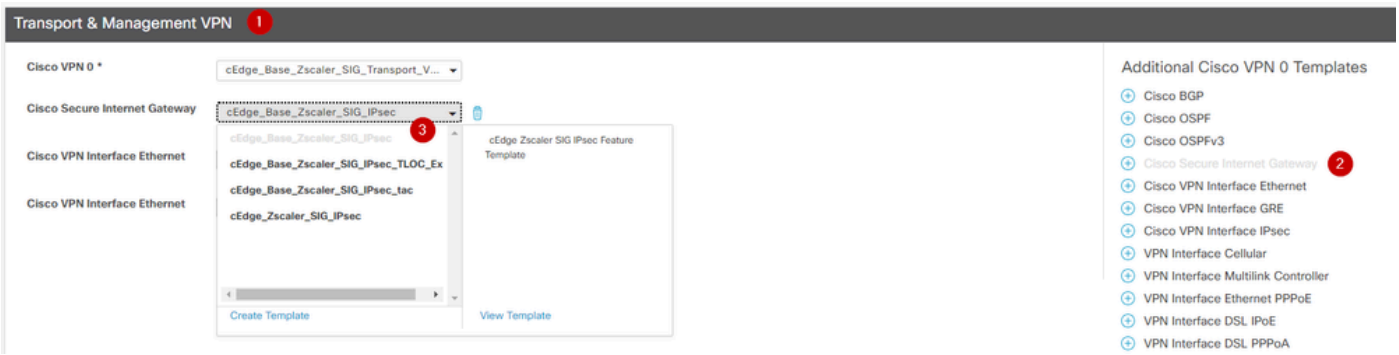
SIG 템플릿 컨피그레이션을 완료했으면 디바이스 템플릿 아래에 적용해야 합니다. 이렇게 하면 컨피그레이션이 Cisco Edge 라우터에 푸시됩니다.

이 단계를 완료하려면 Configuration(컨피그레이션) > Templates(템플릿) > Device Template(디바이스 템플릿)으로 이동하고 세 개의 점에서 Edit(수정)를 클릭합니다.

1. Transport & Management VPN

2. 보안 인터넷 게이트웨이 템플릿을 추가합니다.

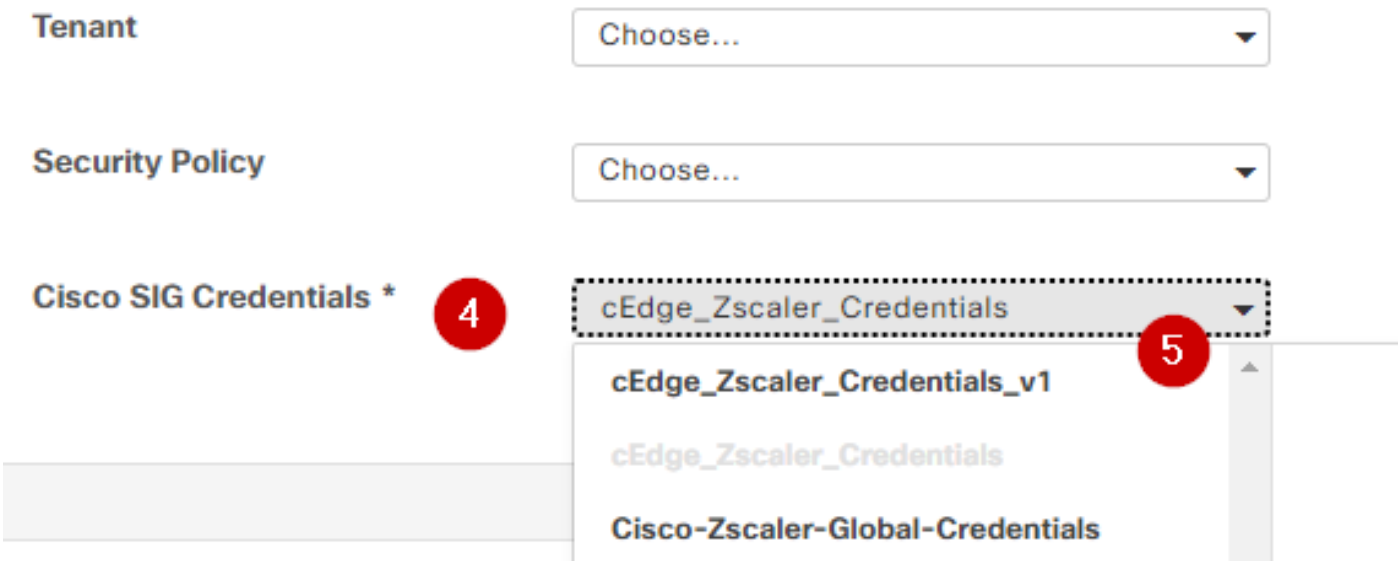
3. Cisco Secure Internet Gateway의 드롭다운 메뉴에서 올바른 SIG 기능 템플릿을 선택합니다.



디바이스 템플릿에 SIG 템플릿 추가

추가 템플릿 아래

4. Cisco SIG 자격 증명
5. 드롭다운 메뉴에서 올바른 Cisco SIG 인증서 템플릿을 선택합니다.



자격 증명 SIG 템플릿

업데이트를 클릭합니다. 디바이스 템플릿이 활성 템플릿인 경우 표준 단계를 사용하여 활성 템플릿에 컨피그레이션을 푸시합니다.

다음을 확인합니다.

컨피그레이션 미리 보기 중에 확인 작업을 수행하여 변경 사항을 푸시할 수 있습니다. 다음 사항을 확인해야 합니다.

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

이 예에서는 설계가 액티브/스탠바이임을 확인할 수 있습니다

<#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 pofiles 및 policy, Tunnel1xxxxx로 시작하는 다중 인터페이스, vrf 정의 65530, ip sdwan route vrf 1 0.0.0.0/0 service sig와 같이 더 많은 컨피그레이션이 추가된 것을 확인할 수 있습니다.

이러한 모든 변경 사항은 Zscaler를 사용하는 IPsec SIG 터널의 일부입니다.

다음 예에서는 터널 인터페이스의 컨피그레이션이 어떻게 표시되는지 보여줍니다.

```
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
```

컨피그레이션이 Cisco Edge Router에 성공적으로 푸시되면 명령을 사용하여 터널이 시작되는지 여부를 확인할 수 있습니다.

<#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 코드 200이 표시되지 않으면 비밀번호 또는 파트너 키와 관련된 문제에 직면한 것입니다.

인터페이스 상태를 확인하려면 명령을 사용합니다.

<#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
```

추적기의 상태를 확인하려면 show endpoint-tracker 및 show endpoint-tracker records 명령을 실행합니다. 이렇게 하면 추적기에서 사용 중인 URL을 확인할 수 있습니다

```
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
```

다음과 같은 다른 검증을 수행할 수 있습니다.
VRF의 경로가 IPsec 터널을 가리키도록 하려면 다음 명령을 실행합니다.

show ip route vrf 1

마지막 방법의 게이트웨이는 0.0.0.0에서 네트워크 0.0.0.0으로

S* 0.0.0.0/0 [2/65535], 터널100002
[2/65535], 터널100001
10.0.0.0/8은 가변 서브넷입니다. 서브넷 4개, 마스크 2개

더 자세히 검증하려면 인터넷을 향해 ping을 수행하고 추적 경로를 수행하여 트래픽이 취하는 홉을 확인할 수 있습니다.

<#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>

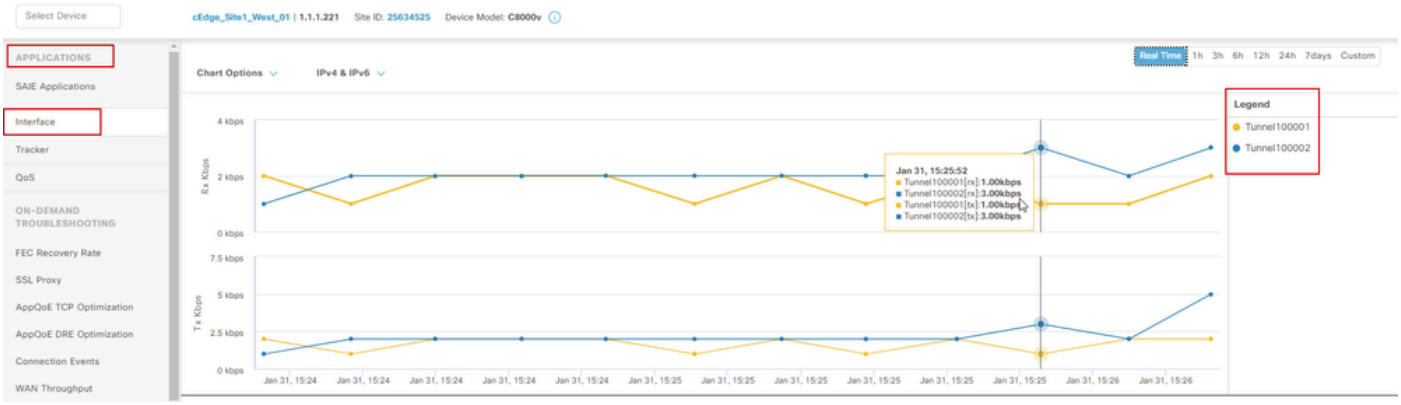
```
 200 msec
```

<The IP here need to be Zcaler IP>

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

Monitor(모니터) > Device(디바이스) 또는 Monitor(모니터) > Network(네트워크)(코드 20.6 이하)에서 탐색하여 vManage GUI에서 IPsec 인터페이스를 검증할 수 있습니다.

- 라우터를 선택하고 Applications(애플리케이션) > Interfaces(인터페이스)로 이동합니다.
- 실시간 트래픽을 보거나 필요한 시간 프레임당 사용자 지정하려면 Tunnel10001 및 Tunnel100002를 선택합니다.



IPsec 터널 모니터링

문제 해결

SIG 터널이 실행되고 있지 않은 경우 문제를 해결하기 위한 몇 가지 단계는 다음과 같습니다.

1단계: show sdwan secure-internet-gateway zscaler tunnels 명령을 사용하여 오류를 확인합니다. 출력에서 HTTP RESP 코드 401을 발견하면 인증에 문제가 있음을 나타냅니다.

SIG Credentials(SIG 자격 증명) 템플릿의 값을 확인하여 비밀번호 또는 Partner Key(파트너 키)가 올바른지 확인할 수 있습니다.

```
<#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
```

추가 디버깅을 위해 다음 명령을 활성화하고 SIG, HTTP 또는 추적기와 관련된 로그 메시지를 검색합니다.

- 디버그 플랫폼 소프트웨어 sdwan ftm sig
- 디버그 플랫폼 소프트웨어 sdwan sig
- 디버그 플랫폼 소프트웨어 sdwan 추적기
- 디버그 플랫폼 소프트웨어 sdwan ftm rtm-events

다음은 debug 명령의 출력 예입니다.

<#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
```

show ip interface brief 명령을 실행하고 tunnels interface Protocol(up 또는 down이 표시되는 경우)을 확인합니다.

<#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 자격 증명에 문제가 없음을 확인한 후 디바이스 템플릿에서 SIG 인터페이스를 제거하고 라우터로 푸시할 수 있습니다.

푸시가 완료되면 SIG 템플릿을 적용하고 라우터로 다시 푸시합니다. 이 방법은 터널을 처음부터 다시 만들도록 강제합니다.

관련 정보

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.