Cisco 에지 디바이스로 Umbrella SIG 수동 터널 생성

목차

소개

이 문서에서는 Umbrella SIG에서 16.12 릴리스를 실행하는 Cisco Edge Router를 사용하여 CDFW 터널을 구축하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 이 문서의 뒷부분에 언급된 Umbrella SIG 관련 부품을 구성하기 전에 CLI 기반 템플릿을 사용하여 디바이스를 완전히 구성하고 작동해야 합니다. 여기서는 터널 컨피그레이션과 관련된 항목만 캡처합니다.
- NAT는 하나 이상의 전송 VPN 인터페이스에서 구성해야 합니다.
- 나열되는 정책은 향후 릴리스에서 "allow-service ipsec"을 추가할 때까지의 해결 방법입니다.

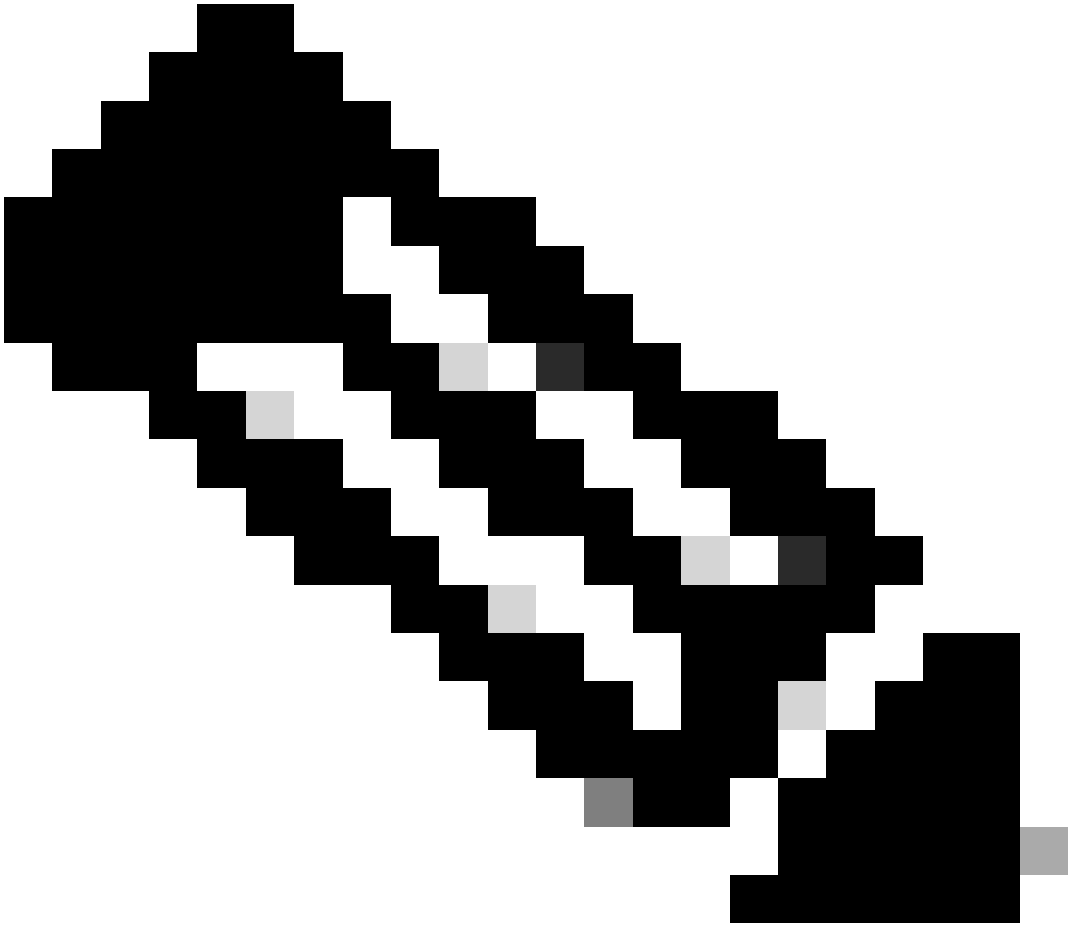
사용되는 구성 요소

이 문서의 정보는 Cisco Umbrella SIG(Secure Internet Gateway)를 기반으로 합니다.

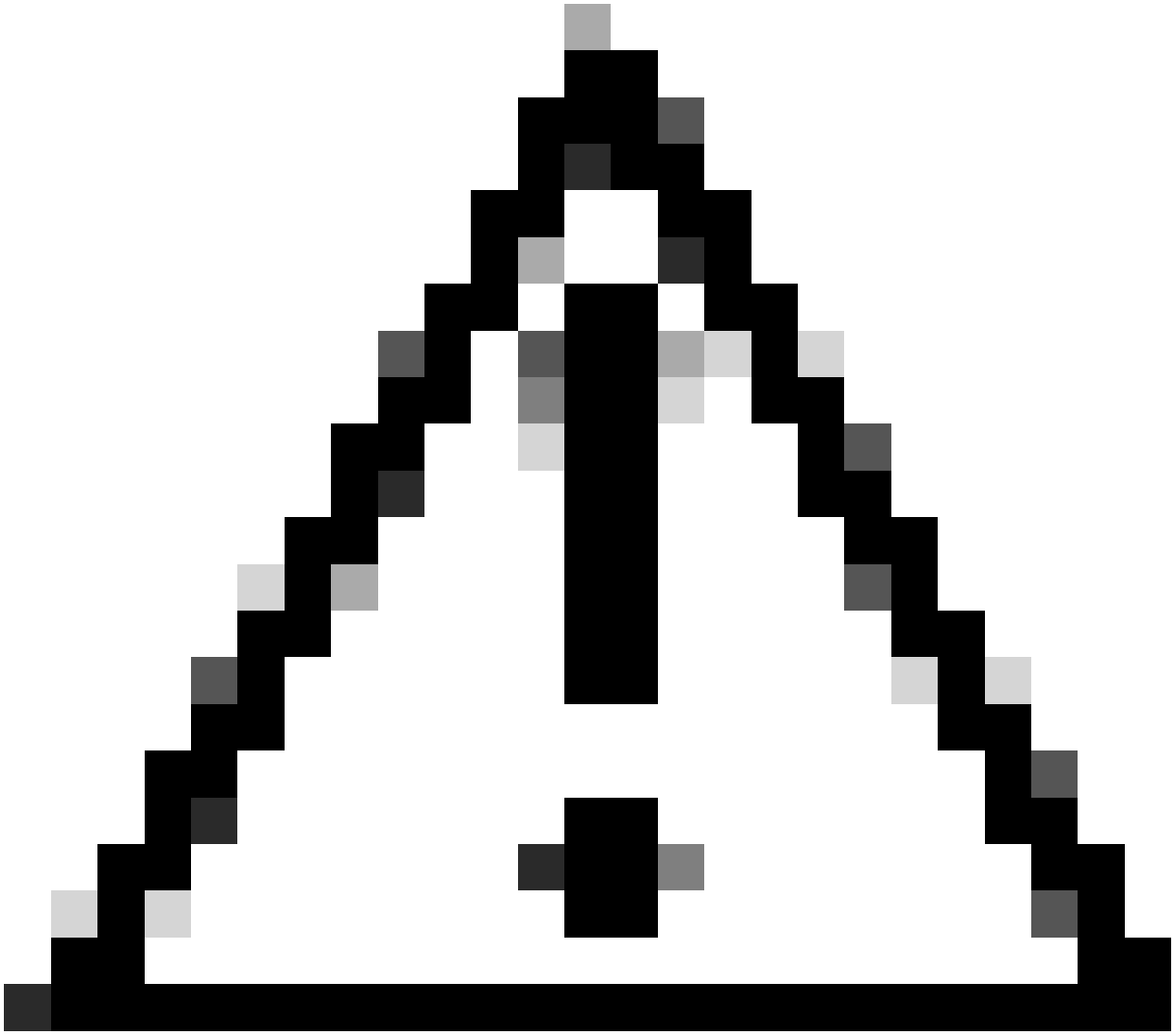
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

이 문서에서는 16.12 릴리스를 실행하는 Cisco Edge 라우터(이전의 Viptela cEdge)를 사용하여 CDFW 터널을 구축하는 방법에 대해 설명합니다.



참고: 아래 컨피그레이션 템플릿은 vManage에서 CLI 기반 터널을 생성하는 데 필요한 INTENT 기반 형식입니다. INTENT 기반 형식은 vEdge 구성 형식과 유사하지만 몇 가지 차이점이 있습니다. cEdge의 경우 17.2.1까지 기능 템플릿을 효과적으로 사용할 수 없으므로 이 예에서는 CLI 기반 템플릿을 사용합니다.



주의: 이 문서는 Cisco Umbrella SIG 솔루션을 통해 기업 게스트 트래픽을 전송하는 활용 사례를 다루기 위해 작성되었습니다. 이 How-To 문서에서는 CLI 기반 템플릿을 사용하여 vManage에서 기능 기반 템플릿의 제한을 재정의합니다.

수동 터널 구축

1. Umbrella 대시보드에서 CDFW 터널을 생성합니다.

2. 일반적으로 환경에 대해 구성하는 것처럼 Viptela 디바이스 템플릿을 구성합니다.

3. 포트 UDP 500 및 4500을 전송 인터페이스로 허용하도록 SIG 정책을 구성합니다. A

- CL_for_IKE_IPSec_tunnel은 터널 인터페이스를 통한 IPSEC 트래픽을 허용하는 ACL 이름입니다
- 선택 사항: ACL을 Umbrella SIG DC로만 추가로 제한할 수 있습니다. Umbrella 문서에서 자세한 내용을 읽어 보십시오.

```
access-list ACL_for_IKE_IPSec_tunnel
sequence 10
match
protocol 50
!
action accept
!
!
sequence 20
match
destination-port 4500 500
!
action accept
!
!
default-action drop
!
```

4. 사용 중인 터널 인터페이스에 ACL을 적용합니다.

```
sdwan
interface GigabitEthernet1
tunnel-interface
access-list ACL_for_IKE_IPSec_tunnel in
```

5. 필요한 경로를 포함하여 전송 VPN에서 IPsec 인터페이스를 구성합니다.

이러한 변수는 이 목록 뒤에 있는 CLI 컨피그레이션 템플릿에서 정의됩니다.

- {transport_vpn_1}은 IPSEC 터널을 설정하는 네트워크 인터페이스(일반적으로 WAN 인터페이스)입니다
- {transport_vpn_ip_addr_prefix}는 사용자가 할당하는 전송 VPN입니다. (예: 1.1.1.0/24)
- {ipsec__int_number}는 IPSEC 터널 인터페이스 번호입니다(예: "IPSEC1" 인터페이스의 번호 1).
- {ipsec_ip_addr_prefix}는 IPSEC 터널 인터페이스에 대해 정의된 ip 주소 및 서브넷입니다.
- {transport_vpn_interface_1}은 IPSEC 터널을 설정하는 네트워크 인터페이스(일반적으로 WAN 인터페이스)입니다. 이는 transport_vpn_1 변수에 사용된 것과 동일한 인터페이스입니다.
- {psk}는 Umbrella Dashboard의 터널 섹션에서 생성된 터널의 사전 공유 키 값입니다.
- {sig_fqdn}은 Umbrella Dashboard의 터널 섹션에서 생성된 터널의 IKE ID입니다.
- {sig_tunnel_dest_ip}은 터널이 연결된 CDFW DC의 IP입니다.

```
vpn 0
  interface {{transport_vpn_1}}
   ip address {{transport_vpn_ip_addr_prefix}}
   nat
    refresh bi-directional
   !
  mtu      1360
```

```
    no shutdown
   !
   interface ipsec{{ipsec__int_number}}
    ip address {{ipsec_ip_addr_prefix}}
    tunnel-source-interface {{transport_vpn_interface_1}}
    tunnel-destination      {{sig_tunnel_dest_ip}}
    ike
     version      2
     rekey        14400
     cipher-suite aes256-cbc-sha1
     group        14
     authentication-type
      pre-shared-key
       pre-shared-secret {{psk}}
       local-id          {{sig_fqdn}}
       remote-id         {{sig_tunnel_dest_ip}}
      !
     !
    !
    ipsec
     rekey                    3600
     replay-window            512
     cipher-suite             aes256-gcm
     perfect-forward-secrecy none
    !
    no shutdown
   !

ip ipsec-route 0.0.0.0/0 vpn 0 interface ipsec{{ipsec__int_number}}
```

참고로 3-5단계에서 언급한 샘플 컨피그레이션은 다음과 같습니다.

```
access-list ACL_for_IKE_IPSec_tunnel
sequence 10
match
protocol 50
!
action accept
!
!
sequence 20
match
destination-port 4500 500
!
action accept
!
!
default-action drop
!
```

```
vpn 0
dns 208.67.222.222 primary
name VPN0
   interface GigabitEthernet4
    ip address 192.168.1.0/24
```

```
    nat
     refresh bi-directional
    !
   mtu      1360
    no shutdown
   !
   interface ipsec1
    ip address 10.10.10.1/30
    tunnel-source-interface GigabitEthernet4
    tunnel-destination      146.112.83.8
    ike
     version      2
     rekey        14400
     cipher-suite aes256-cbc-sha1
     group        14
     authentication-type
      pre-shared-key
       pre-shared-secret YourPreSharedKey
       local-id          YourTunnelID@umbrella.sig.cisco.com
       remote-id         146.112.83.8
      !
     !
    !
    ipsec
     rekey                    3600
     replay-window            512
     cipher-suite             aes256-gcm
     perfect-forward-secrecy none
    !
    no shutdown
   !
ip ipsec-route 0.0.0.0/0 vpn 0 interface ipsec1
```

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.