Umbrella SIG Manual Tunnel maken met Cisco Edge-apparaten

Inhoud

Inleiding

In dit document wordt beschreven hoe u een CDFW-tunnel kunt bouwen met behulp van een Cisco Edge-router waarop de release 10 .12 in Umbrella SIG wordt uitgevoerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Het apparaat moet volledig zijn geconfigureerd en operationeel zijn met behulp van de CLI-gebaseerde sjablonen voordat de relevante onderdelen van de SIG-paraplu worden geconfigureerd die verderop in dit artikel worden vermeld. Alleen relevante items voor de tunnelconfiguratie worden hier vastgelegd.
- NAT moet worden geconfigureerd in een of meer van de transport VPN-interfaces.
- Het vermelde beleid is een tijdelijke oplossing totdat "allow-service ipsec" wordt toegevoegd in een toekomstige release.

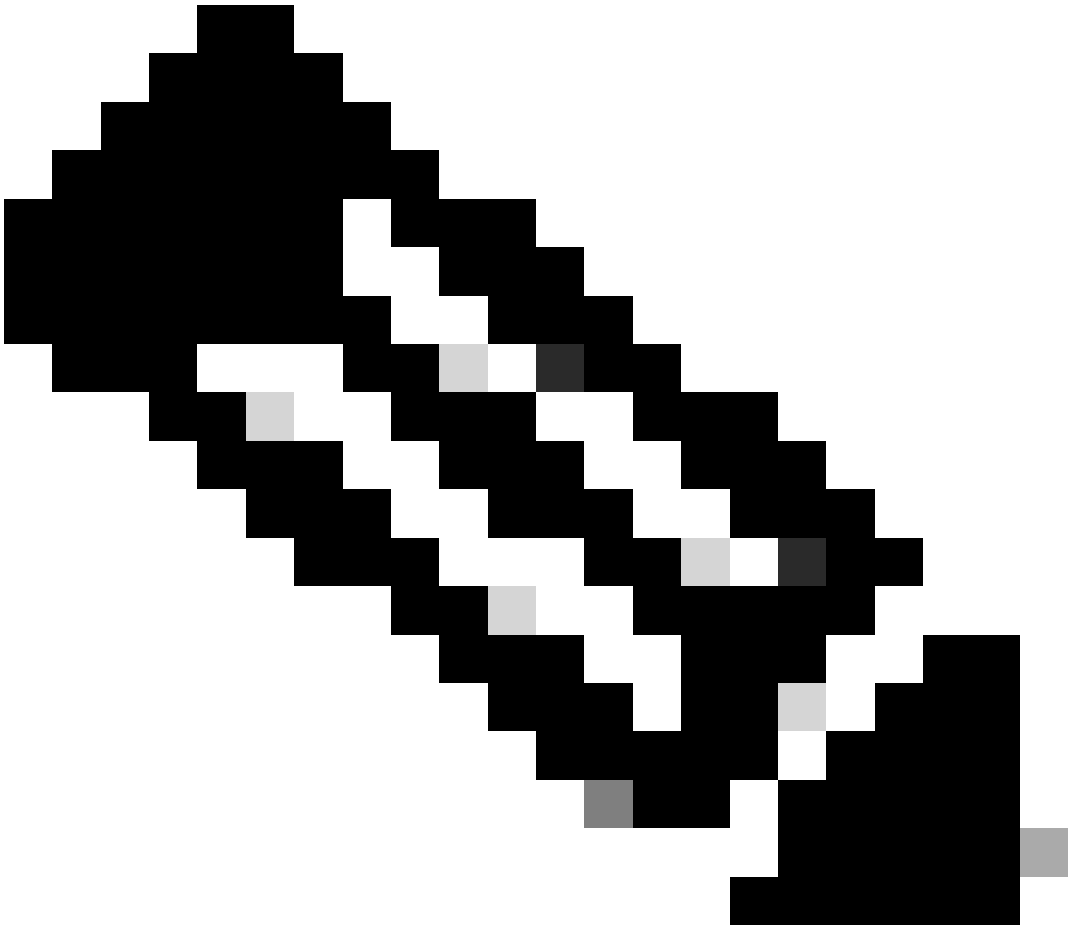
Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella Secure Internet Gateway (SIG).

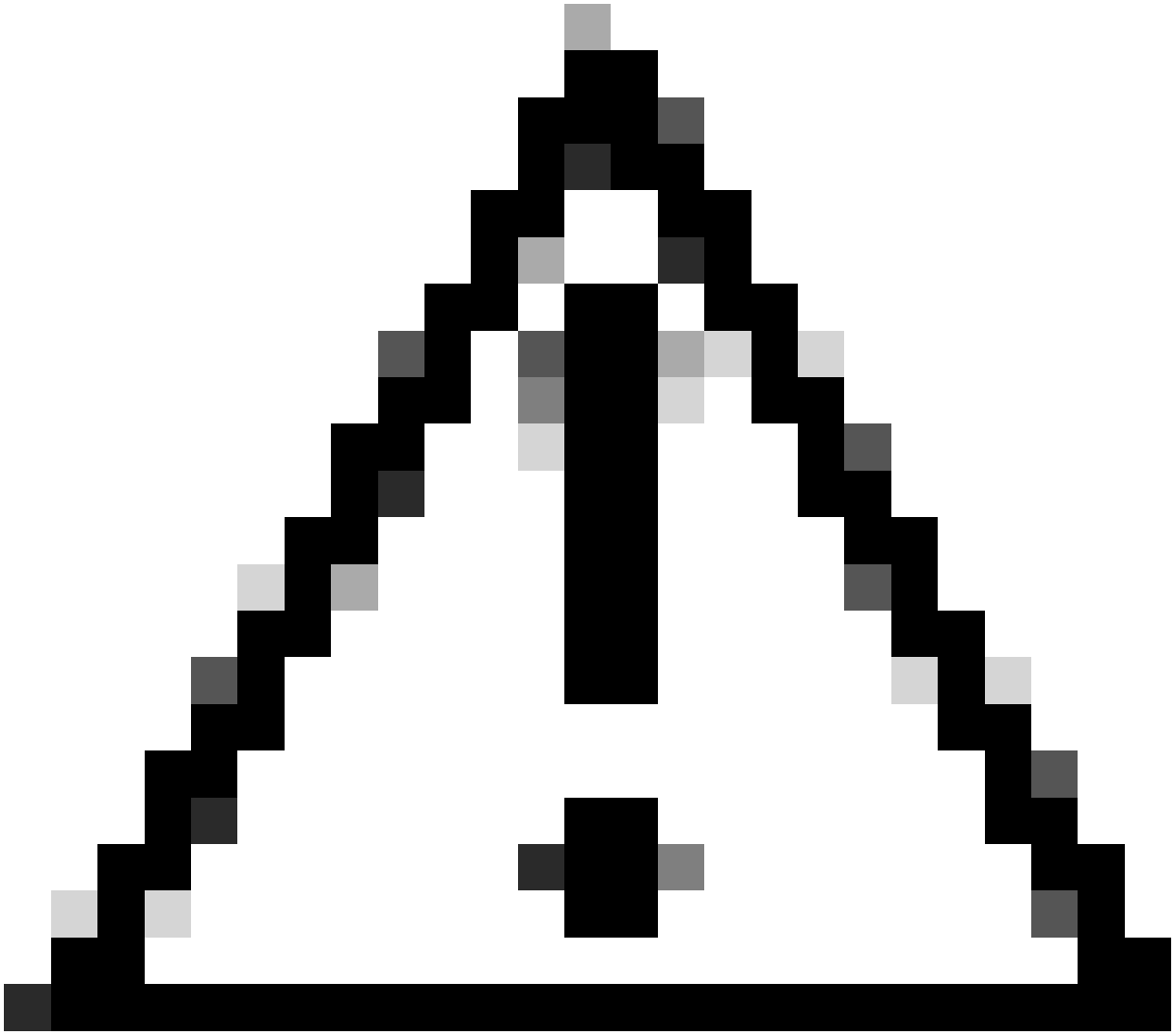
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

In dit artikel wordt uitgelegd hoe u een CDFW-tunnel kunt bouwen met behulp van een Cisco Edge-router (voorheen Viptela cEdge) waarop de release van 10 .12 wordt uitgevoerd.



Opmerking: de onderstaande configuratiesjabloon is in een op INTENTIE gebaseerde indeling, die nodig is om CLI-gebaseerde tunnels in vManage te maken. Het op INTENT gebaseerde formaat is vergelijkbaar met het vEdge-configuratieformaat, maar er zijn enkele verschillen. Een functiesjabloon kan niet effectief worden gebruikt tot 17.2.1 voor cEdge, dus dit voorbeeld gebruikt een CLI-gebaseerde sjabloon.



Waarschuwing: dit artikel is gemaakt om het gebruik van het verzenden van zakelijk gastverkeer via de Cisco Umbrella SIG-oplossing aan te pakken. In dit instructieartikel worden op CLI gebaseerde sjablonen gebruikt om een beperking van op functies gebaseerde sjablonen in vManage te negeren.

Bouw de manuele tunnel

1. Maak een CDFW-tunnel in het Umbrella Dashboard.

2. Configureer Viptela-apparaatsjabloon zoals u normaal zou configureren voor uw omgeving.

3. Configureer een SIG-beleid zodat de poorten UDP 500 en 4500 in de transportinterfaces kunnen worden opgenomen. A

- CL_for_IKE_IPSec_tunnel is de ACL-naam die IPSEC-verkeer door de tunnelinterface mogelijk maakt
- Optioneel: u kunt de ACL verder beperken tot alleen SIG-DC's met paraplu. Lees meer in de

overkoepelende documentatie.

```
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. Pas de ACL toe op de tunnelinterface die u gebruikt.

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

5. Configureer de IPsec-interface(s) in de VPN-transportroute, inclusief de vereiste routes.

Deze variabelen worden gedefinieerd in de CLI-configuratiesjabloon na deze lijst:

- `{transport_vpn_1}` is de netwerkinterface (meestal de WAN-interface) die de IPSEC-tunnel tot stand brengt
- `{transport_vpn_ip_addr_prefix}` is de transport-VPN die u toewijst. (bijvoorbeeld 1.1.1.0/24)
- `{ipsec__int_number}` is het IPSEC-tunnelinterfacenummer (bijvoorbeeld het nummer 1 in interface "IPSEC1")
- `{ipsec_ip_addr_prefix}` is het IP-adres en subnet dat is gedefinieerd voor de IPSEC-tunnelinterface.
- `{transport_vpn_interface_1}` is de netwerkinterface (meestal de WAN-interface) die de IPSEC-tunnel tot stand brengt. Dit is dezelfde interface die wordt gebruikt in de variabele transport_vpn_1.
- `{psk}` is de vooraf gedeelde sleutelwaarde van de tunnel die is gemaakt in de tunnelsectie van het Umbrella Dashboard.
- `{sig_fqdn}` is de IKE-ID van de tunnel die is gemaakt in de tunnelsectie van het Umbrella Dashboard.
- `{sig_tunnel_dest_ip}` is het IP van de CDFW DC waarmee de tunnel is verbonden.

```
 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}}
```

Ter referentie, hier is een voorbeeldconfiguratie vermeld in stap 3-5:

```
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
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.