Erstellung eines Umbrella SIG Manual Tunnels mit Cisco Edge-Geräten

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Überblick

Erstellung des manuellen Tunnels

Einleitung

In diesem Dokument wird die Einrichtung eines CDFW-Tunnels mithilfe eines Cisco Edge-Routers mit Version 16.12 in Umbrella SIG beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Das Gerät muss mithilfe der CLI-basierten Vorlagen vollständig konfiguriert und betriebsbereit sein, bevor die Umbrella SIG-relevanten, weiter unten in diesem Artikel erwähnten Teile konfiguriert werden können. Hier werden nur relevante Artikel für die Tunnelkonfiguration erfasst.
- NAT muss in einer oder mehreren Transport-VPN-Schnittstellen konfiguriert werden.
- Die aufgelistete Richtlinie ist eine Problemumgehung, bis "allow-service ipsec" in einer zukünftigen Version hinzugefügt wird.

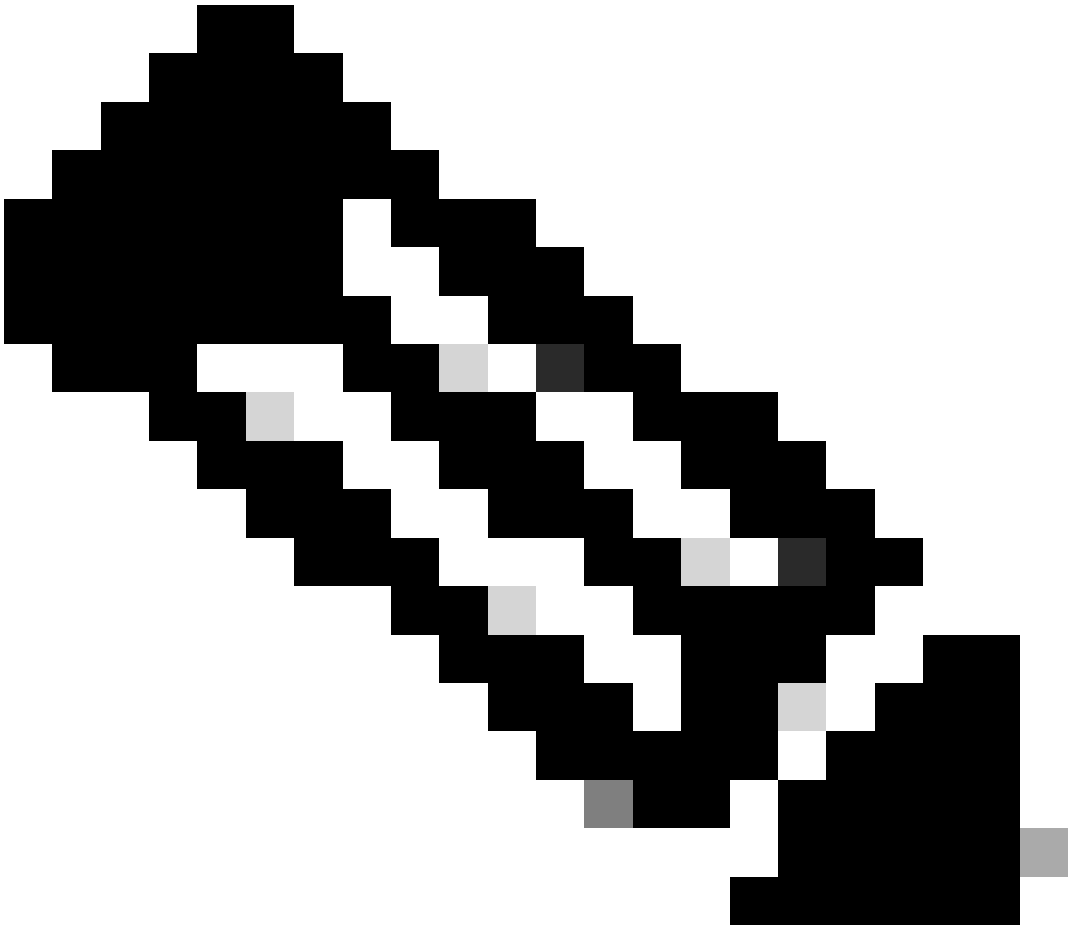
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella Secure Internet Gateway (SIG).

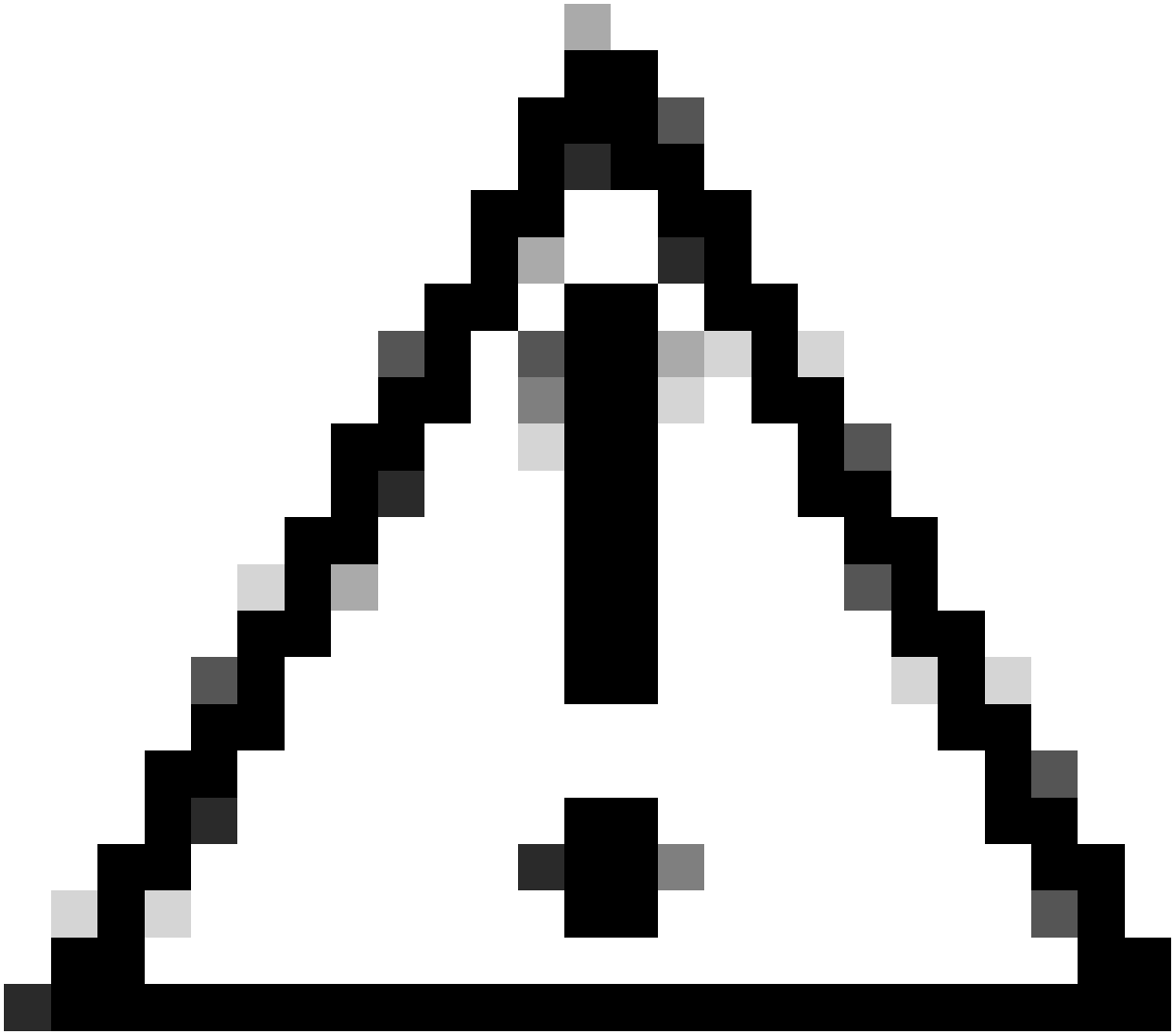
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

In diesem Artikel wird erläutert, wie ein CDFW-Tunnel mit einem Cisco Edge-Router (ehemals Viptela cEdge) erstellt wird, auf dem die Version 16.12 ausgeführt wird.



Anmerkung: Die nachfolgende Konfigurationsvorlage hat das Format INTENT, das zum Erstellen von CLI-basierten Tunneln in vManage erforderlich ist. Das ABSICHTSBEZOGENE Format ähnelt dem vEdge-Konfigurationsformat, es gibt jedoch einige Unterschiede. Eine Funktionsvorlage kann erst ab Version 17.2.1 für cEdge effektiv verwendet werden. Daher wird in diesem Beispiel eine CLI-basierte Vorlage verwendet.



Vorsicht: Dieser Artikel befasst sich mit dem Anwendungsfall, Gastdatenverkehr von Unternehmen über die Cisco Umbrella SIG-Lösung zu senden. In diesem Anleitungsartikel werden CLI-basierte Vorlagen verwendet, um eine Beschränkung der funktionsbasierten Vorlagen in vManage außer Kraft zu setzen.

Erstellung des manuellen Tunnels

1. Erstellen Sie einen CDFW-Tunnel im Umbrella Dashboard.

2. Konfigurieren Sie die Viptela-Gerätevorlage wie gewohnt für Ihre Umgebung.

3. Konfigurieren Sie eine SIG-Richtlinie, um die Ports UDP 500 und 4500 als Transportschnittstellen zuzulassen. A

- CL_for_IKE_IPSec_tunnel (CL_für_IKE_IPSec_tunnel) ist der ACL-Name, der IPSEC-Datenverkehr über die Tunnelschnittstelle zulässt.
- Optional: Sie können die ACL weiter auf Umbrella SIG-Rechenzentren beschränken. Lesen

Sie mehr in der Umbrella-Dokumentation.

```
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. Wenden Sie die ACL auf die verwendete Tunnelschnittstelle an.

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

5. Konfigurieren Sie die IPsec-Schnittstelle(n) im Transport-VPN einschließlich der erforderlichen Routen.

Diese Variablen werden in der CLI-Konfigurationsvorlage nach dieser Liste definiert:

- `{transport_vpn_1}` ist die Netzwerkschnittstelle (in der Regel die WAN-Schnittstelle), die den IPSEC-Tunnel erstellt.
- `{transport_vpn_ip_addr_prefix}` ist das Transport-VPN, das Sie zuweisen. (beispiel: 1.1.1.0/24)
- `{ipsec__int_number}` ist die IPSEC-Tunnelschnittstellennummer (z. B. die Nummer 1 in der Schnittstelle "IPSEC1").
- `{ipsec_ip_addr_prefix}` ist die IP-Adresse und das Subnetz, die für die IPSEC-Tunnelschnittstelle definiert sind.
- `{transport_vpn_interface_1}` ist die Netzwerkschnittstelle (in der Regel die WAN-Schnittstelle), die den IPSEC-Tunnel erstellt. Dies ist die gleiche Schnittstelle, die auch in der Variablen transport_vpn_1 verwendet wird.
- `{psk}` ist der vorinstallierte Schlüsselwert des Tunnels, der im Tunnelabschnitt des Umbrella Dashboards erstellt wird.
- `{sig_fqdn}` ist die IKE-ID des Tunnels, die im Tunnelabschnitt des Umbrella Dashboards erstellt wird.

- `{sig_tunnel_dest_ip}` ist die IP-Adresse des CDFW-Rechenzentrums, mit der der Tunnel verbunden ist.

```
 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}}
```

Es folgt eine Beispielkonfiguration, die in den Schritten 3-5 beschrieben wird:

```
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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.