Creación del túnel manual SIG de Umbrella con los dispositivos periféricos de Cisco

Contenido

Introducción

Este documento describe cómo construir un túnel CDFW utilizando un router de borde de Cisco que ejecuta la versión 16.12 en Umbrella SIG.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- El dispositivo debe estar completamente configurado y operativo mediante las plantillas basadas en CLI antes de configurar las partes relevantes de Umbrella SIG que se mencionan más adelante en este artículo. Aquí solo se capturan los elementos relevantes para la configuración del túnel.
- NAT se debe configurar en una o más de las interfaces VPN de transporte.
- La política enumerada es una solución alternativa hasta que se agregue "allow-service ipsec" en una futura versión.

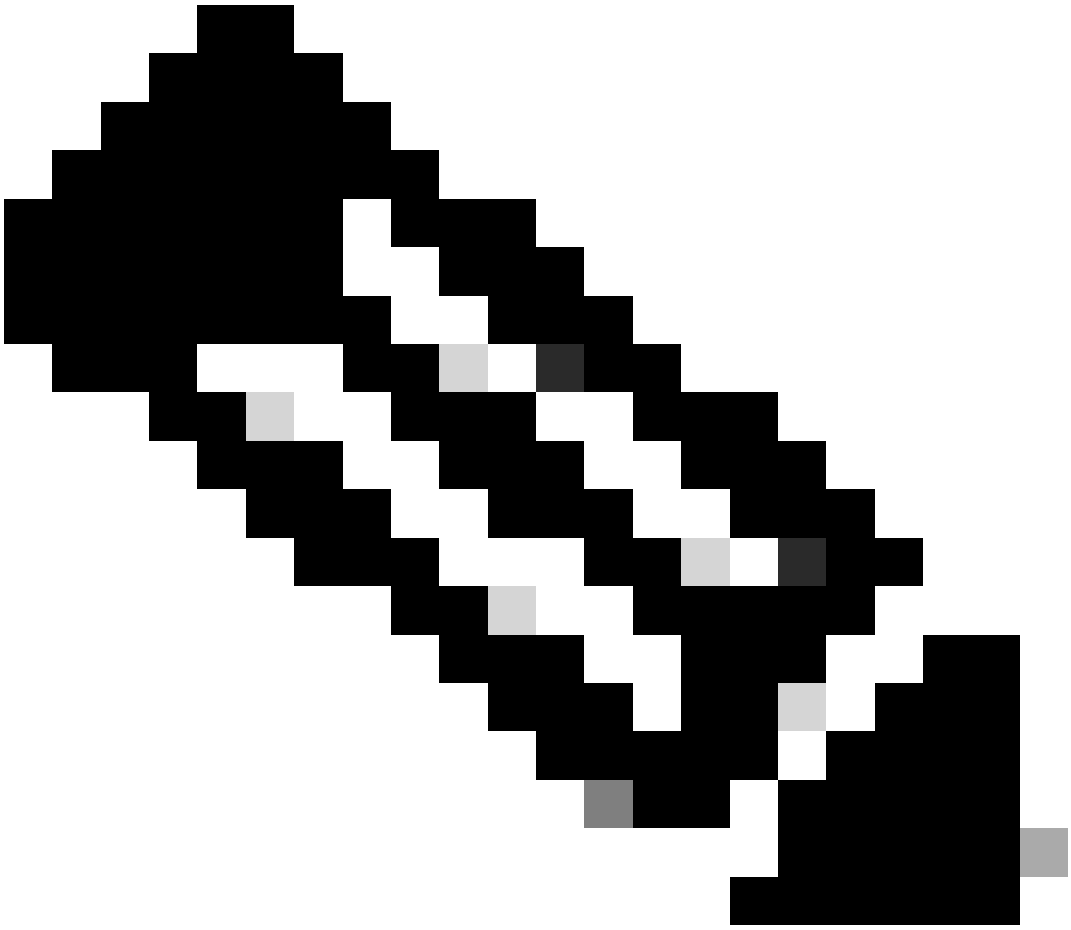
Componentes Utilizados

La información de este documento se basa en Cisco Umbrella Secure Internet Gateway (SIG).

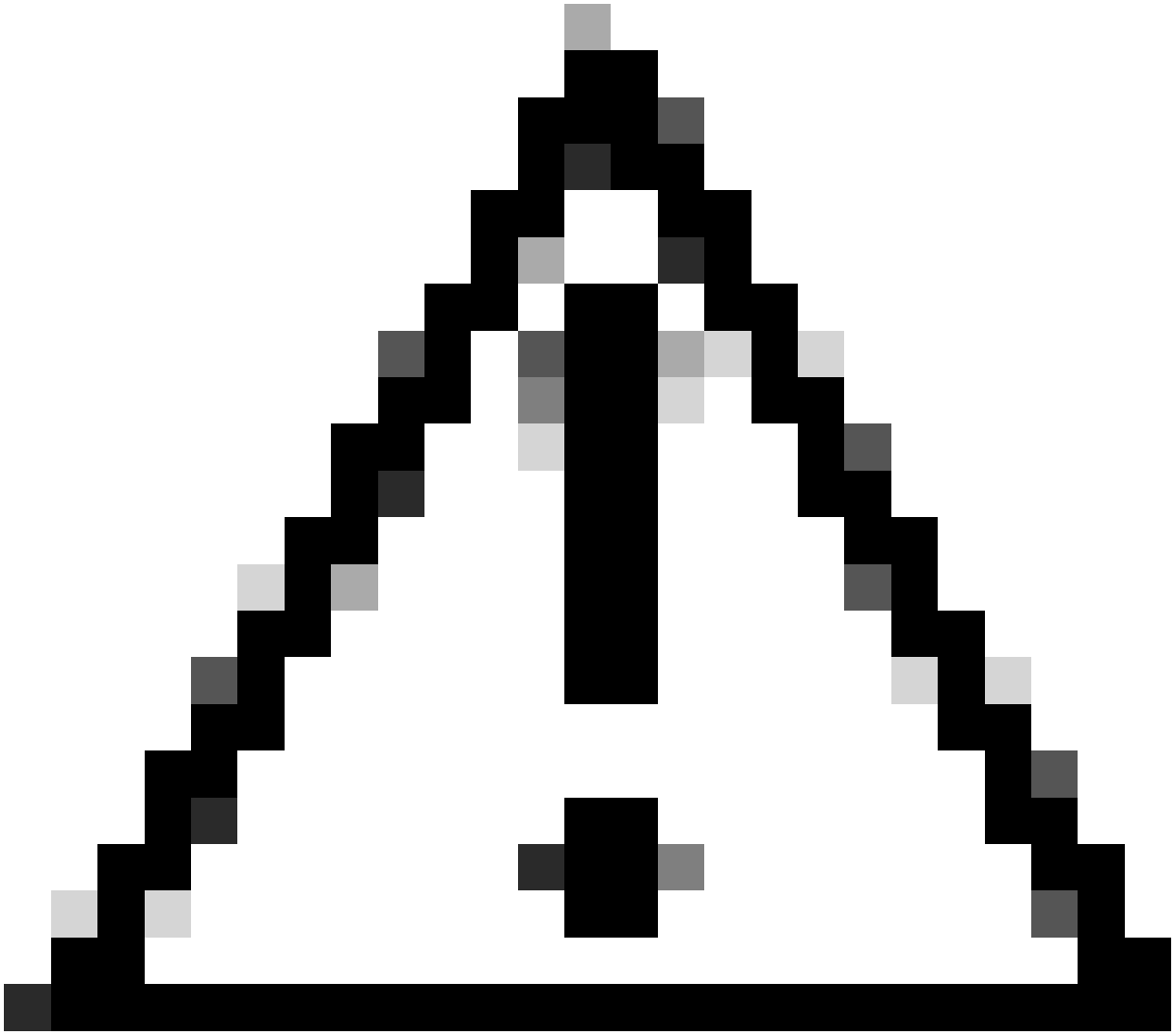
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

En este artículo se explica cómo crear un túnel CDFW mediante un router Cisco Edge (anteriormente Viptela cEdge) que ejecuta la versión 16.12.



Nota: La plantilla de configuración siguiente está en formato basado en INTENT, que es necesario para crear túneles basados en CLI en vManage. El formato basado en INTENT es similar al formato de configuración de vEdge, pero hay algunas diferencias. Una plantilla de función no se puede utilizar eficazmente hasta 17.2.1 para cEdge, por lo que este ejemplo utiliza una plantilla basada en CLI.



Precaución: Este artículo se ha creado para abordar el caso práctico del envío de tráfico de invitados corporativo a través de la solución Cisco Umbrella SIG. Este artículo de procedimientos utiliza plantillas basadas en CLI para anular una limitación de plantillas basadas en funciones en vManage.

Creación del túnel manual

1. Cree un túnel CDFW en el panel de control general.

2. Configure la plantilla del dispositivo Viptela como lo haría normalmente para su entorno.

3. Configure una política SIG para permitir los puertos UDP 500 y 4500 en las interfaces de transporte. R

- CL_for_IKE_IPSec_tunnel es el nombre de ACL que permite el tráfico IPSEC a través de la interfaz de túnel
- Opcional: Puede restringir aún más la ACL a solo los DC de Umbrella SIG. Lea más en la

documentación de Umbrella.

```
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. Aplique la ACL a la interfaz de túnel que está utilizando.

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

5. Configure las interfaces IPsec en la VPN de transporte, incluidas las rutas necesarias.

Estas variables se definen en la plantilla de configuración de CLI después de esta lista:

- `{transport_vpn_1}` es la interfaz de red (normalmente la interfaz WAN) que establece el túnel IPSEC
- `{transport_vpn_ip_addr_prefix}` es la VPN de transporte que asigna. (por ejemplo: 1.1.1.0/24)
- `{ipsec__int_number}` es el número de interfaz de túnel IPSEC (por ejemplo, el número 1 en la interfaz "IPSEC1")
- `{ipsec_ip_addr_prefix}` es la dirección IP y la subred definidas para la interfaz de túnel IPSEC.
- `{transport_vpn_interface_1}` es la interfaz de red (normalmente la interfaz WAN) que establece el túnel IPSEC. Ésta es la misma interfaz utilizada en la variable transport_vpn_1.
- `{psk}` es el valor de clave previamente compartida del túnel creado en la sección de túneles del panel de Umbrella.
- `{sig_fqdn}` es la ID de IKE del túnel creada en la sección de túneles del panel de Umbrella.
- `{sig_tunnel_dest_ip}` es la IP del DC de CDFW al que está conectado el túnel.

```
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}}
```

Para su información, a continuación se incluye una configuración de ejemplo mencionada en los pasos 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
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).