Crie um túnel manual do Umbrella SIG com dispositivos Cisco Edge

Contents

[Introdução](#)

[Pré-requisitos](#)

- [Requisitos](#)
- [Componentes Utilizados](#)

[Overview](#)

[Construir o túnel manual](#)

Introdução

Este documento descreve como construir um túnel CDFW usando um Cisco Edge Router executando a versão 16.12 no Umbrella SIG.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- O dispositivo deve estar totalmente configurado e operacional usando os modelos baseados em CLI antes de configurar as peças relevantes do Umbrella SIG mencionadas mais adiante neste artigo. Somente itens relevantes para a configuração do túnel são capturados aqui.
- O NAT deve ser configurado em uma ou mais interfaces VPN de transporte.
- A política listada é uma solução até que "allow-service ipsec" seja adicionado em uma versão futura.

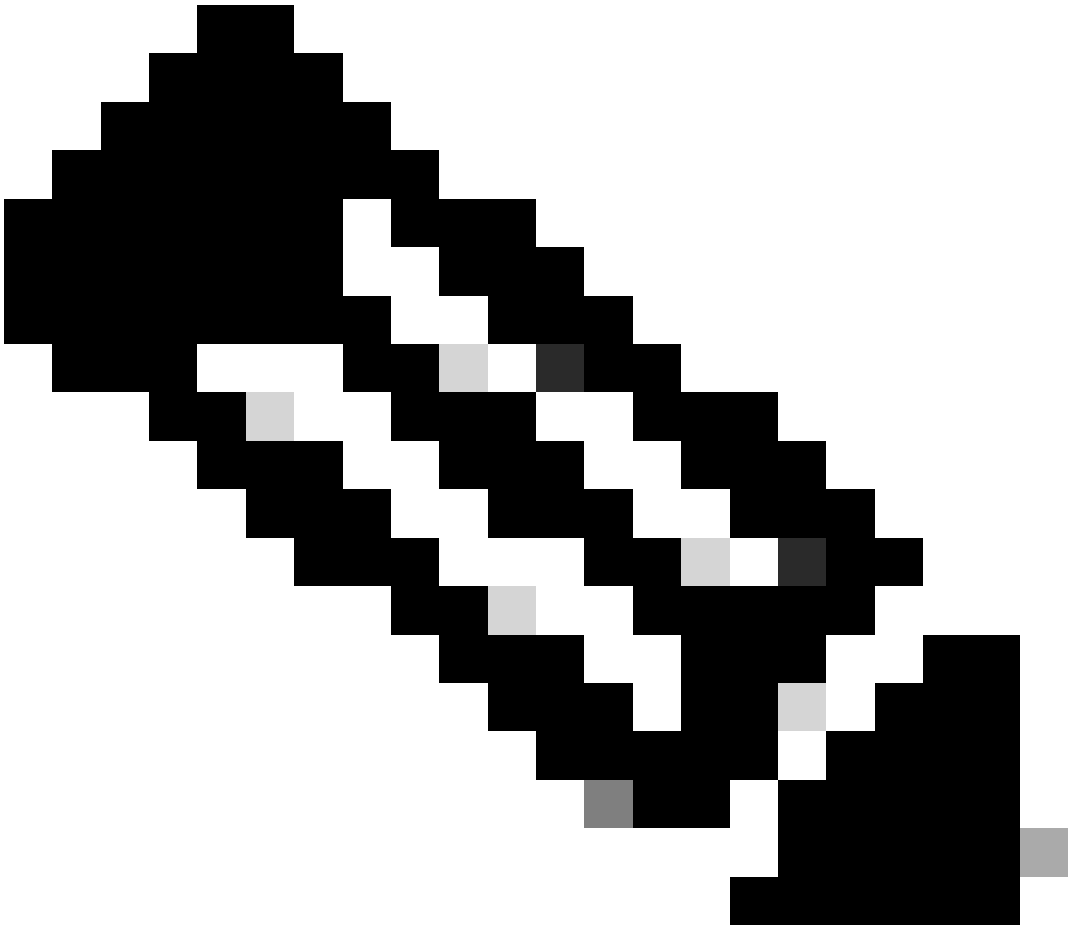
Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella Secure Internet Gateway (SIG).

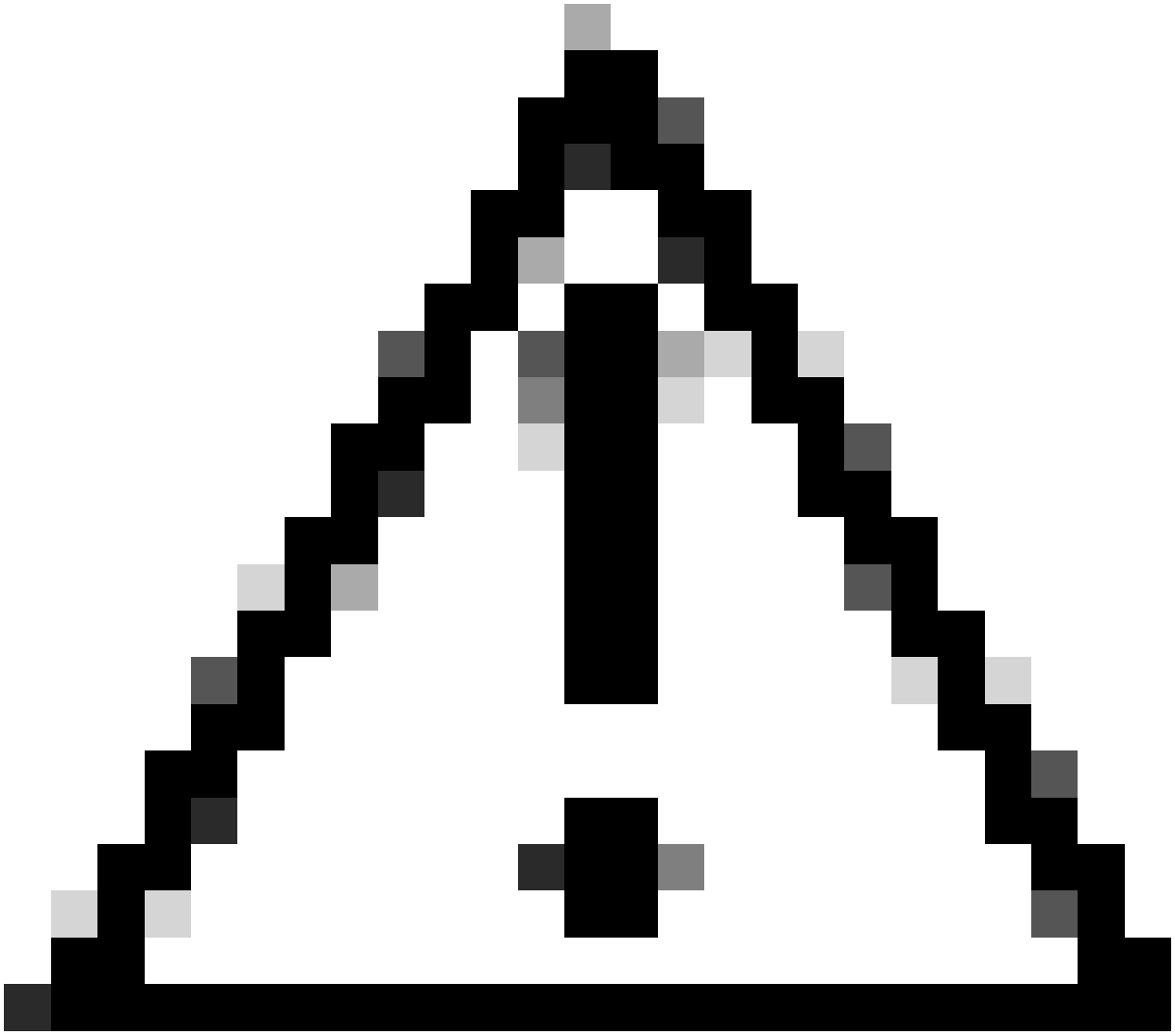
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

Este artigo explica como construir um túnel CDFW usando um roteador Cisco Edge (anteriormente Viptela cEdge) executando a versão 16.12.



Note: O modelo de configuração abaixo está no formato baseado em INTENT, que é necessário para criar túneis baseados em CLI no vManage. O formato baseado em INTENT é semelhante ao formato de configuração do vEdge, mas há algumas diferenças. Um modelo de recurso não pode ser usado efetivamente até 17.2.1 para o cEdge, portanto, este exemplo está usando um modelo baseado em CLI.



Caution: Este artigo foi criado para tratar do caso de uso de envio de tráfego de convidados corporativos através da solução Cisco Umbrella SIG. Este artigo "como fazer" usa modelos baseados em CLI para substituir uma limitação de modelos baseados em recursos no vManage.

Construir o túnel manual

1. Crie um túnel CDFW no Painel do Umbrella.

2. Configure o modelo de dispositivo Viptela como você normalmente configuraria para o seu ambiente.

3. Configure uma política SIG para permitir as portas UDP 500 e 4500 nas interfaces de transporte. R

- CL_for_IKE_IPSec_tunnel é o nome da ACL que permite o tráfego IPSEC através da interface do túnel

- Opcional: Você pode restringir ainda mais a ACL somente aos DCs do Umbrella SIG. Leia mais na documentação do 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 a ACL à interface de túnel que você está usando.

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

5. Configure as interfaces IPsec na VPN de transporte, incluindo as rotas necessárias.

Estas variáveis são definidas no modelo de configuração da CLI após esta lista:

- `{transport_vpn_1}` é a interface da rede (geralmente a interface da WAN) que estabelece o túnel IPSEC
- `{transport_vpn_ip_addr_prefix}` é a VPN de transporte que você atribui. (por exemplo, 1.1.1.0/24)
- `{ipsec__int_number}` é o número da interface de túnel IPSEC (por exemplo, o número 1 na interface "IPSEC1")
- `{ipsec_ip_addr_prefix}` é o endereço ip e a sub-rede definidos para a interface de túnel IPSEC.
- `{transport_vpn_interface_1}` é a interface da rede (geralmente a interface da WAN) que estabelece o túnel IPSEC. Esta é a mesma interface usada na variável transport_vpn_1.
- `{psk}` é o valor de chave pré-compartilhada do túnel criado na seção de túneis do Umbrella Dashboard.
- `{sig_fqdn}` é a ID de IKE do túnel criada na seção de túneis do Umbrella Dashboard.
- `{sig_tunnel_dest_ip}` é o IP do DC do CDFW ao qual o túnel está conectado.

```
 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 sua referência, aqui está um exemplo de configuração mencionado nas etapas 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
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.