使用思科边缘设备创建Umbrella SIG手动隧道

目录

简介

本文档介绍如何在Umbrella SIG中使用运行16.12版本的思科边缘路由器构建CDFW隧道。

先决条件

要求

Cisco 建议您了解以下主题：

- 在配置本文后面提到的Umbrella SIG相关部分之前，必须使用基于CLI的模板对设备进行完全配置并可操作。此处仅捕获与隧道配置相关的项目。
- 必须在一个或多个传输VPN接口中配置NAT。
- 在将来的版本中添加“allow-service ipsec”之前，列出的策略是一种解决方法。

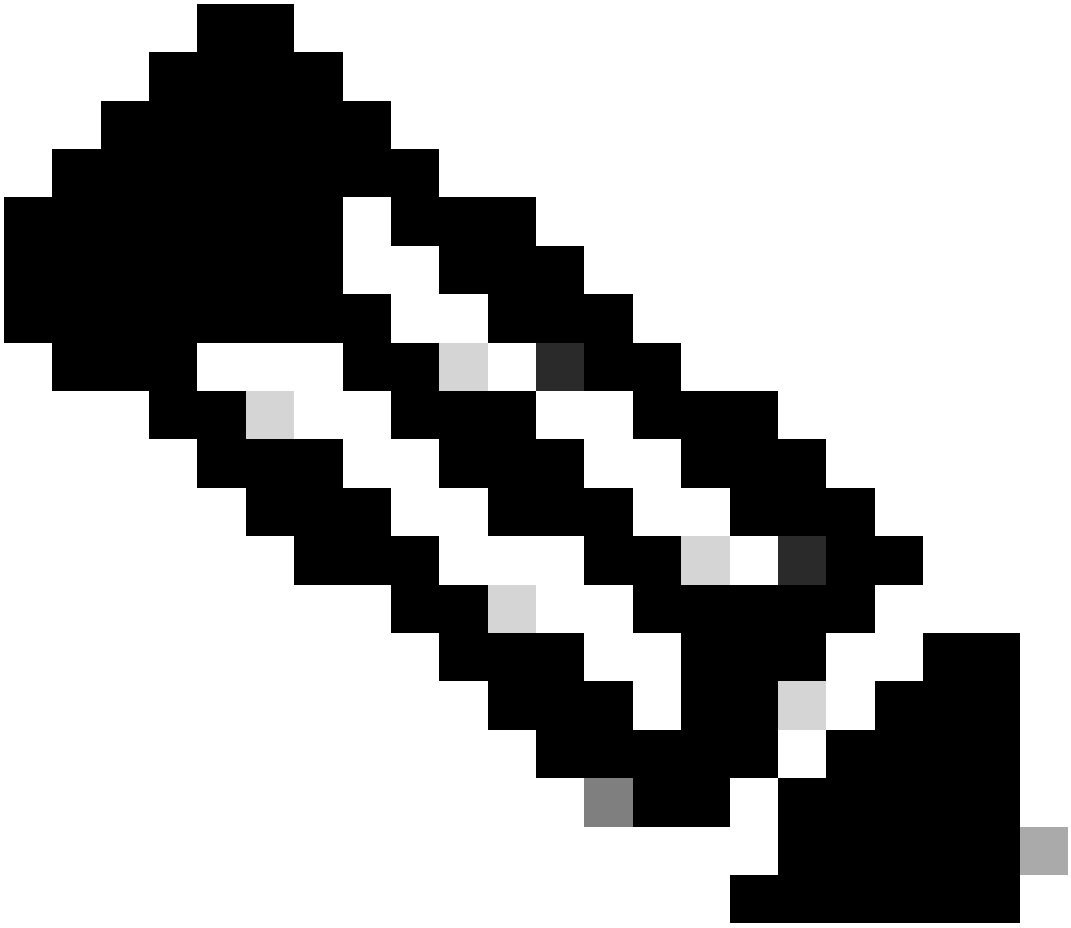
使用的组件

本文档中的信息基于Cisco Umbrella安全互联网网关(SIG)。

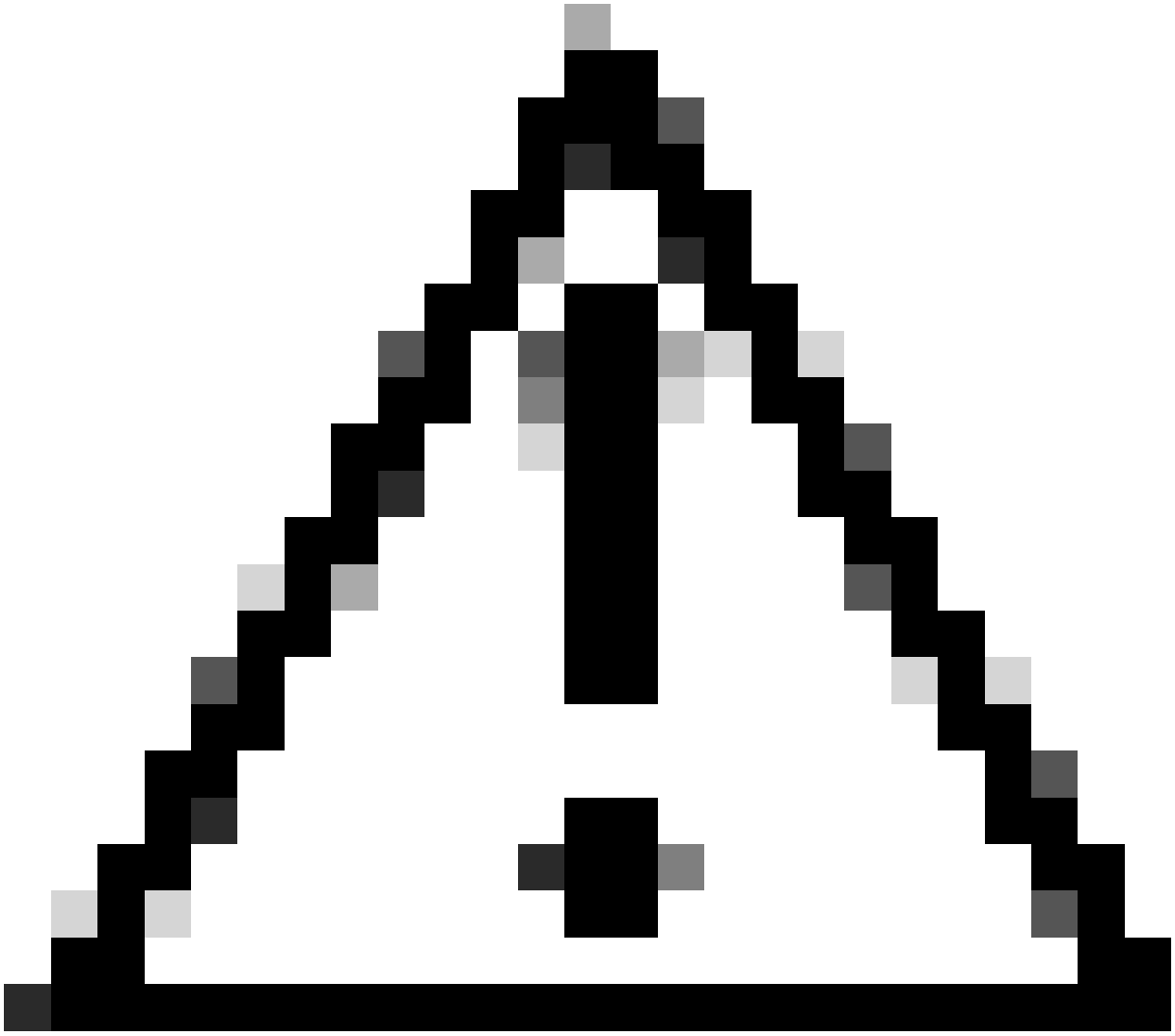
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

本文解释如何使用运行16.12版本的思科边缘路由器（以前称为Viptela cEdge）构建CDFW隧道。



注意：以下配置模板为基于INTENT的格式，在vManage中创建基于CLI的隧道时需要此格式。基于INTENT的格式类似于vEdge配置格式，但存在一些差异。在cEdge 17.2.1之前，功能模板无法有效使用，因此本示例使用的是基于CLI的模板。



警告：本文旨在解决通过Cisco Umbrella SIG解决方案发送企业访客流量的使用案例。本操作说明文章使用基于CLI的模板覆盖vManage中基于功能的模板的限制。

建立手动隧道

1.在Umbrella Dashboard中创建CDFW隧道。

2.按照通常为环境配置的方式配置Viptela设备模板。

3.配置SIG策略以允许端口UDP 500和4500进入传输接口。A

- CL_for_IKE_IPSec_tunnel是允许IPSEC流量通过隧道接口的ACL名称
- 可选：您可以进一步将ACL限制为Umbrella SIG DC。请阅读Umbrella文档中的更多内容。

```
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.将ACL应用到您使用的隧道接口。

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

5.在传输VPN中配置IPsec接口，包括所需的路由。

以下变量在此列表之后的CLI配置模板中定义：

- {transport_vpn_1}是建立IPSEC隧道的网络接口（通常为WAN接口）
- {transport_vpn_ip_addr_prefix}是分配的传输VPN。(例如，1.1.1.0/24)
- {ipsec__int_number}是IPSEC隧道接口编号（例如，接口“IPSEC1”中的编号1）
- {ipsec_ip_addr_prefix}是为IPSEC隧道接口定义的ip地址和子网。
- {transport_vpn_interface_1}是建立IPSEC隧道的网络接口（通常为WAN接口）。这是用于transport_vpn_1变量的接口。
- {psk}是在Umbrella Dashboard的tunnels部分创建的隧道预共享密钥值。
- {sig_fqdn}是在Umbrella Dashboard的tunnels部分中创建的隧道的IKE ID。
- {sig_tunnel_dest_ip}是隧道连接的CDFW DC的IP。

```
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}}
```

以下是步骤3-5中提到的配置示例，供您参考：

```
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
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。