使用思科邊緣裝置建立Umbrella SIG手動隧道

目錄

簡介

本檔案介紹如何在Umbrella SIG中使用執行16.12版的Cisco邊緣路由器建立CDFW通道。

必要條件

需求

思科建議您瞭解以下主題：

- 在配置本文後面提到的Umbrella SIG相關部件之前，必須使用基於CLI的模板對裝置進行完全配置和操作。此處只會擷取與通道組態相關的專案。
- 必須在一個或多個傳輸VPN介面中配置NAT。
- 在將來的版本中新增「allow-service ipsec」之前，列出的策略是一種解決方法。

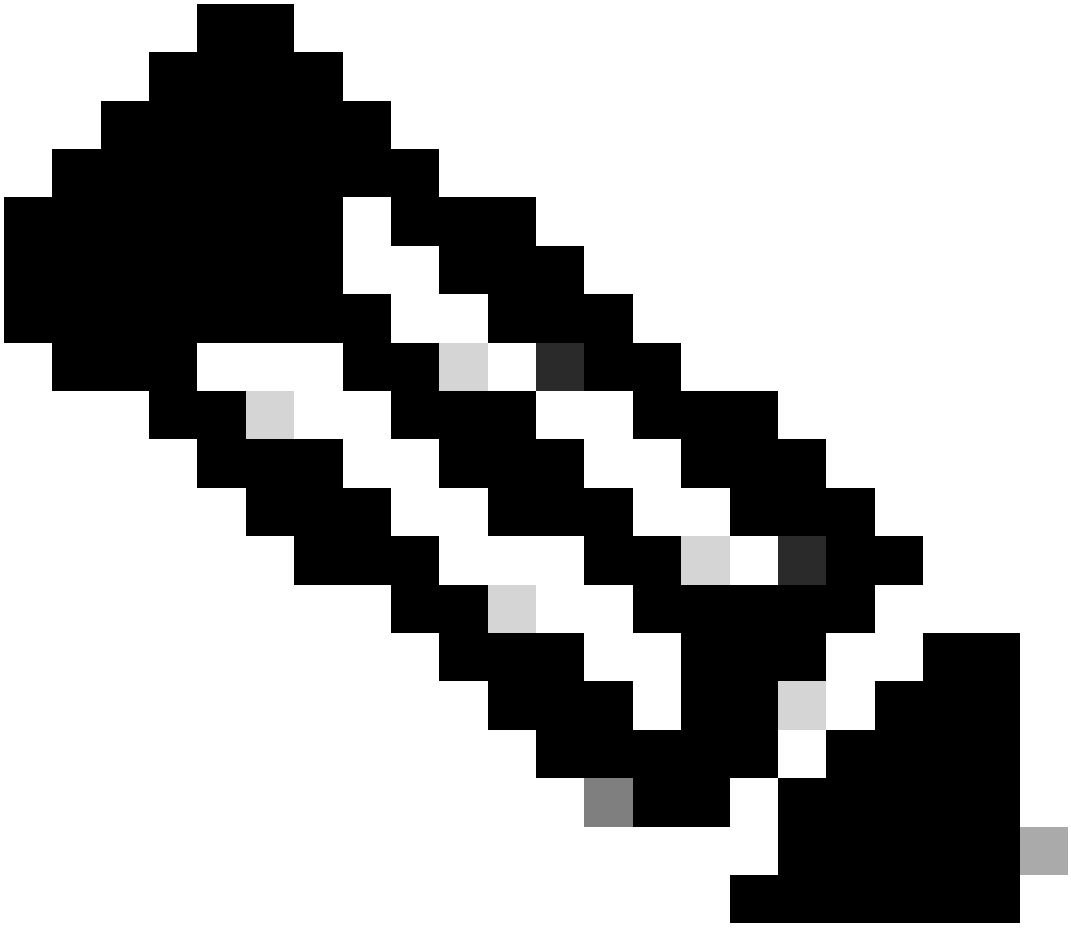
採用元件

本檔案中的資訊是根據Cisco Umbrella安全網際網路閘道(SIG)。

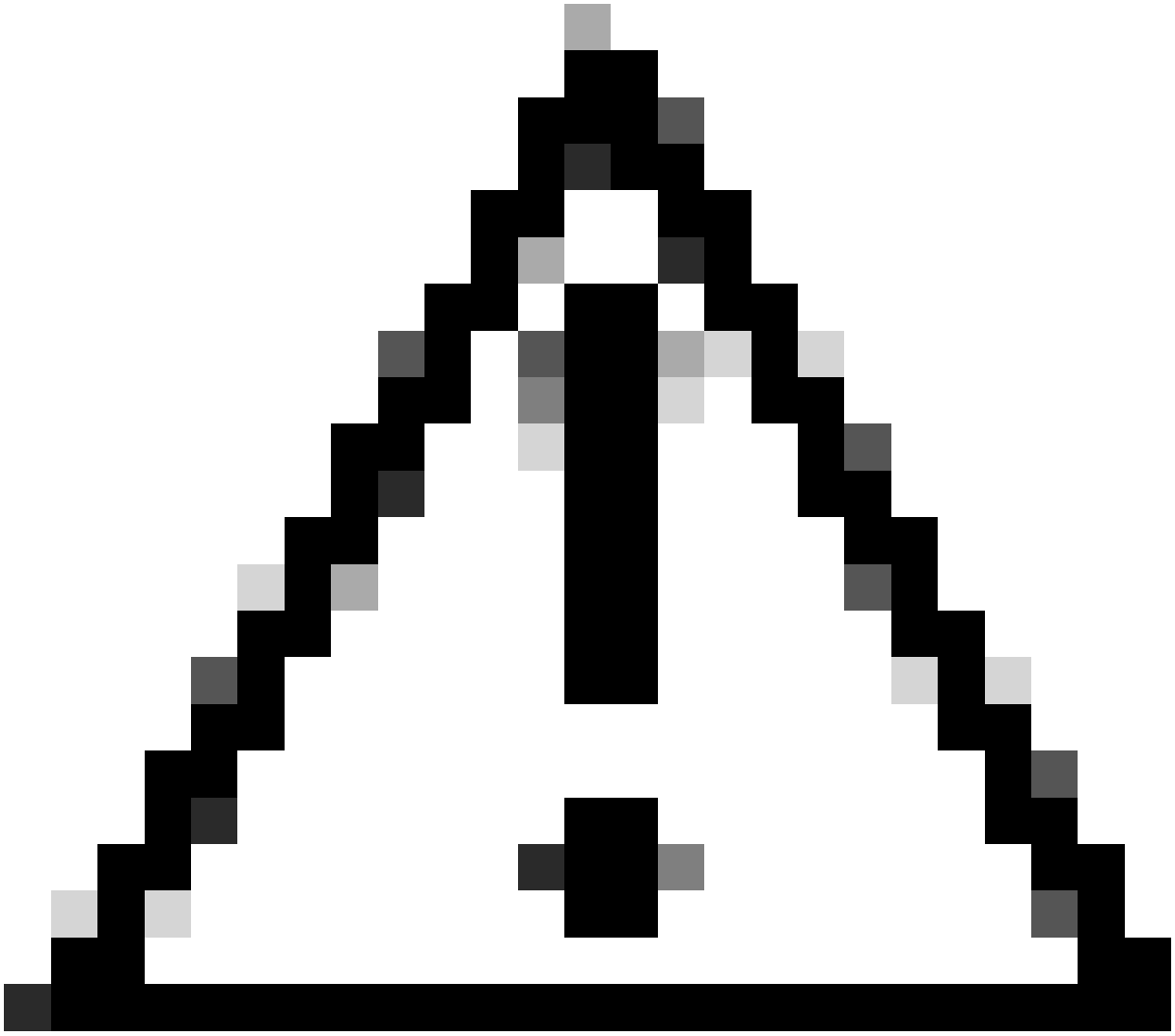
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

本文說明如何使用執行16.12版的Cisco Edge路由器（前身為Viptela cEdge）建立CDFW通道。



附註：下面的配置模板是基於INTENT的格式，在vManage中建立基於CLI的隧道時需要這種格式。基於INTENT的格式類似於vEdge配置格式，但存在一些差異。在cEdge的17.2.1之前，功能模板無法有效使用，因此本示例使用的是基於CLI的模板。



注意：本文旨在探討通過Cisco Umbrella SIG解決方案傳送企業訪客流量的使用案例。本操作說明文章使用基於CLI的模板覆蓋vManage中基於功能的模板的限制。

建立手動隧道

1.在Umbrella Dashboard中建立CDFW隧道。

2.按照通常為環境配置的方式配置Viptela裝置模板。

3.配置SIG策略以允許埠UDP 500和4500進入傳輸介面。A

- CL_for_IKE_IPSec_tunnel是允許IPSEC流量通過通道介面的ACL名稱
- 可選：您可以進一步將ACL限製為僅使用Umbrella SIG DC。閱讀Umbrella文檔中的更多內容。

```
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.將ACL套用到您使用的通道介面。

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

5.在傳輸VPN中配置IPsec介面，包括所需的路由。

以下變數是在此清單之後的CLI配置模板中定義的：

- {transport_vpn_1}是用於建立IPSEC隧道的網路介面（通常為WAN介面）
- {transport_vpn_ip_addr_prefix}是您分配的傳輸VPN。(例如，1.1.1.0/24)
- {ipsec__int_number}是IPSEC隧道介面編號（例如，介面「IPSEC1」中的編號1）
- {ipsec_ip_addr_prefix}是為IPSEC隧道介面定義的ip地址和子網。
- {transport_vpn_interface_1}是建立IPSEC隧道的網路介面（通常是WAN介面）。此介面與transport_vpn_1變數中使用的介面相同。
- {psk}是在Umbrella Dashboard的tunnels部分中建立的隧道的預共用金鑰值。
- {sig_fqdn}是在Umbrella Dashboard的tunnels部分中建立的隧道的IKE ID。
- {sig_tunnel_dest_ip}是通道所連線的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}}
```

以下是步驟3-5中提到的組態範例，供您參考：

```
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
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。