Ciscoエッジデバイスを使用したUmbrella SIG手動トンネルの作成

内容

はじめに

このドキュメントでは、Umbrella SIGの16.12リリースを実行するCiscoエッジルータを使用してCDFWトンネルを構築する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- デバイスは、CLIベースのテンプレートを使用して完全に設定され、動作している必要があります。その後、この記事で後述するUmbrella SIGの関連部分を設定します。ここでは、トンネル設定に関連する項目のみをキャプチャします。
- NATは、1つ以上のトランスポートVPNインターフェイスで設定する必要があります。
- リストされているポリシーは、将来のリリースで「allow-service ipsec」が追加されるまでの回避策です。

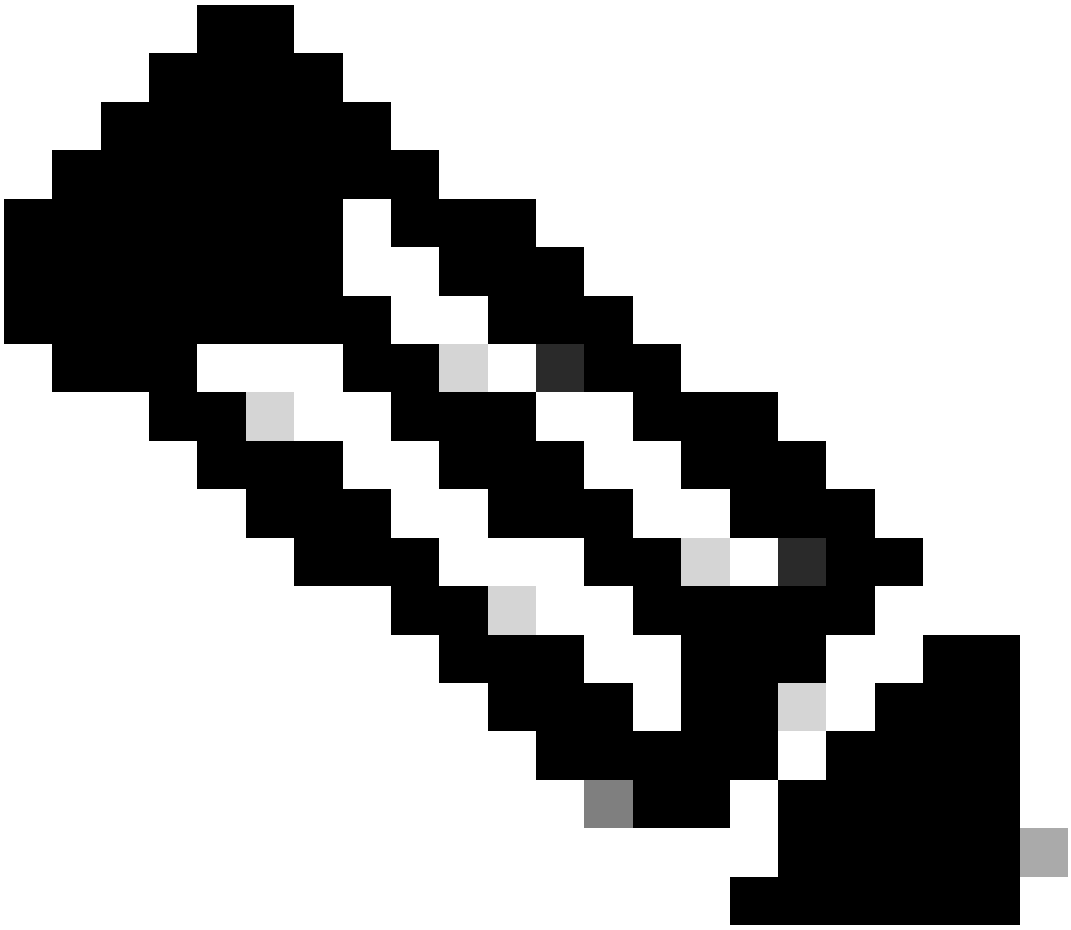
使用するコンポーネント

このドキュメントの情報は、Cisco Umbrellaセキュアインターネットゲートウェイ(SIG)に基づくものです。

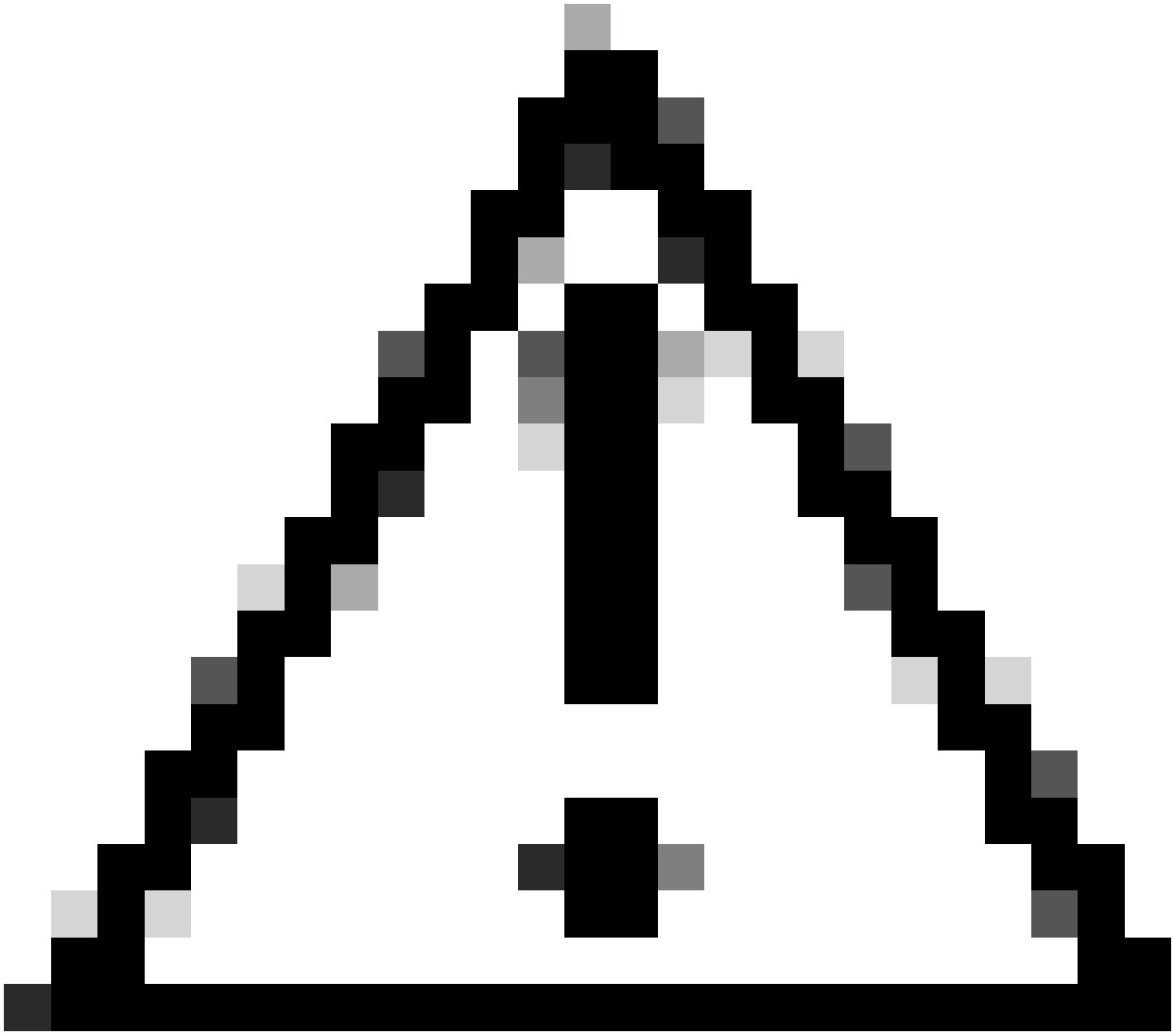
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

この記事では、16.12リリースを実行しているCiscoエッジルータ（旧称Viptela cEdge）を使用してCDFWトンネルを構築する方法について説明します。



注：次の設定テンプレートはINTENTベースの形式です。vManageでCLIベースのトンネルを作成するために必要です。INTENTベースのフォーマットはvEdge設定フォーマットに似ていますが、いくつかの違いがあります。機能テンプレートは、cEdge用の17.2.1まで効果的に使用できません。そのため、この例ではCLIベースのテンプレートを使用しています。



注意：この記事は、Cisco Umbrella SIGソリューションを介して企業ゲストトラフィックを送信する際の使用例を説明するために作成されました。この操作方法の記事では、CLIベースのテンプレートを使用して、vManageの機能ベースのテンプレートの制限を上書きします。

手動トンネルの構築

1. UmbrellaダッシュボードでCDFWトンネルを作成します。

2. Viptelaデバイステンプレートは、通常の環境に合わせて設定します。

3. SIGポリシーを設定して、UDP 500および4500ポートをトランスポートインターフェイスに許可します。A

- CL_for_IKE_IPSec_tunnelは、トンネルインターフェイス経由でIPSECトラフィックを許可するACL名です
- オプション：さらに、ACLをUmbrella SIG DCのみに制限できます。詳細については、

Umbrellaのドキュメントを参照してください。

```
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. 使用しているトンネルインターフェイスにACLを適用します。

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

5. 必要なルートを含むトランスポートVPNでIPsecインターフェイスを設定します。

次の変数は、このリストの後のCLI設定テンプレートで定義されます。

- {transport_vpn_1}:IPSECトンネルを確立するネットワークインターフェイス（通常はWANインターフェイス）
- {transport_vpn_ip_addr_prefix}は、割り当てるトランスポートVPNです。(例：1.1.1.0/24)
- {ipsec__int_number}は、IPSECトンネルインターフェイス番号です（たとえば、インターフェイス「IPSEC1」の番号1）
- {ipsec_ip_addr_prefix}は、IPSECトンネルインターフェイスに定義されているIPアドレスとサブネットです。
- {transport_vpn_interface_1}:IPSECトンネルを確立するネットワークインターフェイス（通常はWANインターフェイス）です。これは、transport_vpn_1変数で使用されているものと同じインターフェイスです。
- {psk}は、Umbrellaダッシュボードのトンネルセクションで作成されたトンネルの事前共有キーの値です。
- {sig_fqdn}は、Umbrellaダッシュボードのトンネルセクションで作成されたトンネルのIKE IDです。
- {sig_tunnel_dest_ip}は、トンネルが接続されているCDFW DCのIPです。

```
 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}}
```

手順3 ~ 5で説明した設定例を参照してください。

```
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
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。