Créer un tunnel manuel Umbrella SIG avec des périphériques Cisco Edge

Table des matières

Introduction

Ce document décrit comment construire un tunnel CDFW à l'aide d'un routeur de périphérie Cisco exécutant la version 16.12 dans Umbrella SIG.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Le périphérique doit être entièrement configuré et opérationnel à l'aide des modèles basés sur l'interface de ligne de commande (CLI) avant de configurer les parties concernées par Umbrella SIG mentionnées plus loin dans cet article. Seuls les éléments pertinents de la configuration du tunnel sont capturés ici.
- La fonction NAT doit être configurée dans une ou plusieurs interfaces VPN de transport.
- La stratégie répertoriée est une solution de contournement jusqu'à ce que « allow-service ipsec » soit ajouté dans une version ultérieure.

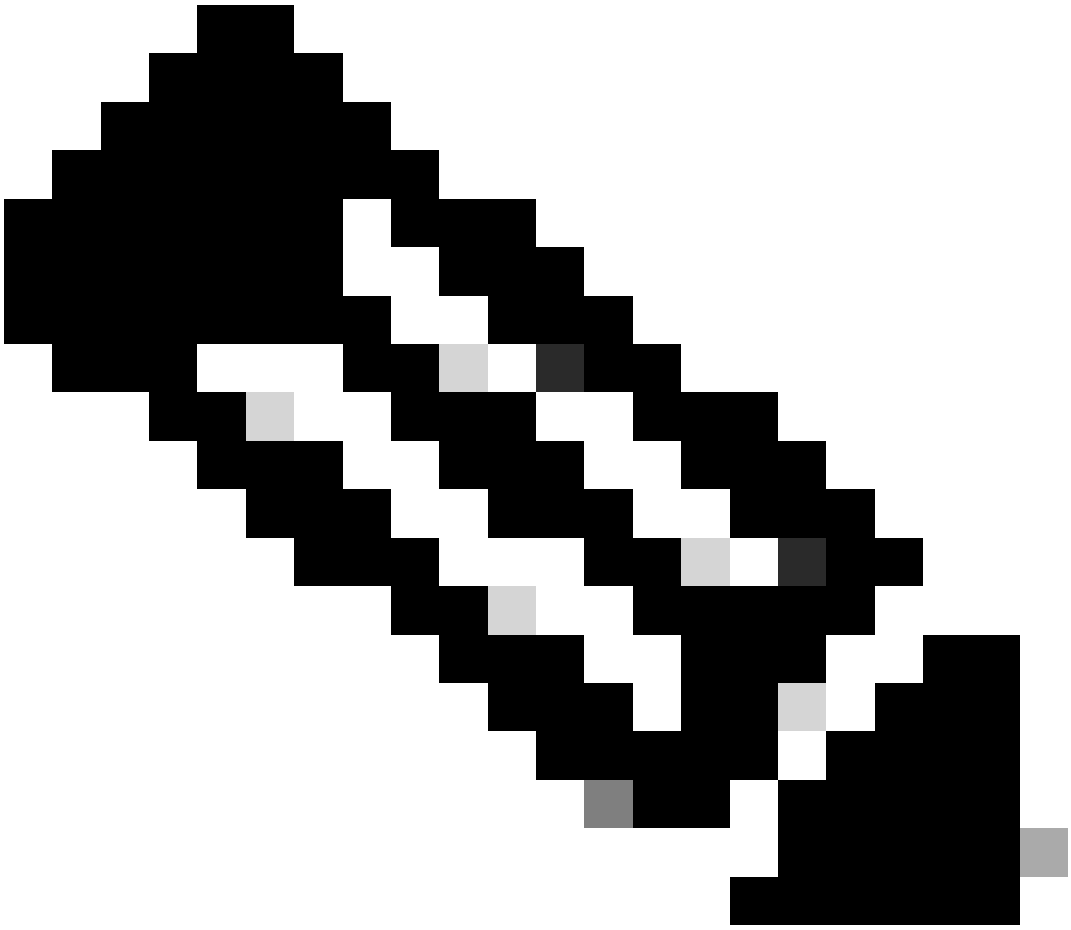
Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella Secure Internet Gateway (SIG).

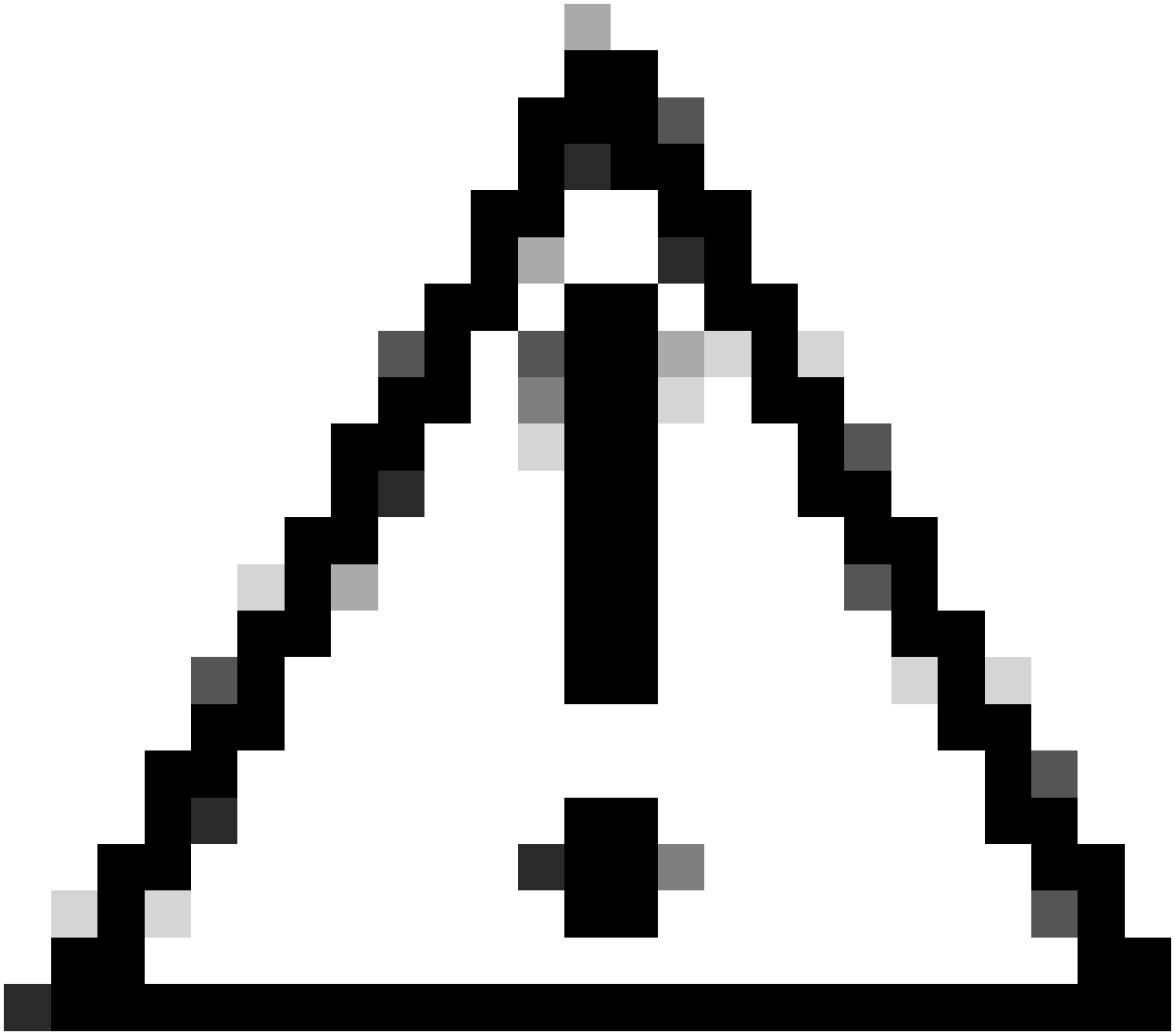
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

Cet article explique comment créer un tunnel CDFW à l'aide d'un routeur Cisco Edge (anciennement Viptela cEdge) exécutant la version 16.12.



Remarque : Le modèle de configuration ci-dessous est au format basé sur l'INTENTION, qui est nécessaire pour créer des tunnels basés sur l'interface de ligne de commande dans vManage. Le format basé sur l'INTENTION est similaire au format de configuration vEdge, mais il existe certaines différences. Un modèle de fonctionnalité ne peut pas être utilisé efficacement avant la version 17.2.1 pour cEdge. Cet exemple utilise donc un modèle basé sur l'interface de ligne de commande.



Mise en garde : Cet article a été créé pour traiter l'exemple d'utilisation de l'envoi de trafic invité d'entreprise via la solution Cisco Umbrella SIG. Cet article de procédure utilise des modèles basés sur l'interface de ligne de commande pour remplacer une limitation des modèles basés sur les fonctionnalités dans vManage.

Création du tunnel manuel

1. Créez un tunnel CDFW dans le tableau de bord Umbrella.

2. Configurez le modèle de périphérique Viptela comme vous le feriez normalement pour votre environnement.

3. Configurez une stratégie SIG pour autoriser les ports UDP 500 et 4500 dans les interfaces de transport. A

- CL_for_IKE_IPSec_tunnel est le nom de la liste de contrôle d'accès qui autorise le trafic IPSEC via l'interface du tunnel

- Facultatif: Vous pouvez limiter la liste de contrôle d’accès aux seuls contrôleurs de domaine Umbrella SIG. Pour en savoir plus, consultez la documentation 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. Appliquez la liste de contrôle d’accès à l’interface de tunnel que vous utilisez.

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

5. Configurez la ou les interfaces IPsec dans le VPN de transport, y compris les routes requises.

Ces variables sont définies dans le modèle de configuration CLI après cette liste :

- `{transport_vpn_1}` est l'interface réseau (généralement l'interface WAN) qui établit le tunnel IPSEC
- `{transport_vpn_ip_addr_prefix}` est le VPN de transport que vous attribuez. (par exemple, 1.1.1.0/24)
- `{ipsec__int_number}` est le numéro d'interface du tunnel IPSEC (par exemple, le numéro 1 dans l'interface « IPSEC1 »)
- `{ipsec_ip_addr_prefix}` est l'adresse IP et le sous-réseau définis pour l'interface du tunnel IPSEC.
- `{transport_vpn_interface_1}` est l'interface réseau (généralement l'interface WAN) qui établit le tunnel IPSEC. Il s'agit de la même interface utilisée dans la variable transport_vpn_1.
- `{psk}` est la valeur de clé pré-partagée du tunnel créée dans la section tunnels du tableau de bord Umbrella.
- `{sig_fqdn}` est l'ID IKE du tunnel créé dans la section tunnels du tableau de bord Umbrella.
- `{sig_tunnel_dest_ip}` est l'adresse IP du contrôleur de domaine CDFW auquel le tunnel est connecté.

```
 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}}
```

Pour référence, voici un exemple de configuration mentionné aux étapes 3 à 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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.