Creazione tunnel manuale Umbrella SIG con dispositivi Cisco Edge

Sommario

Introduzione

Questo documento descrive come creare un tunnel CDFW con un Cisco Edge Router che esegue la versione 16.12 in Umbrella SIG.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Il dispositivo deve essere completamente configurato e operativo utilizzando i modelli basati sulla CLI prima di configurare le parti rilevanti di Umbrella SIG menzionate più avanti in questo articolo. In questa sezione vengono acquisiti solo gli elementi rilevanti per la configurazione del tunnel.
- NAT deve essere configurato in una o più interfacce VPN di trasporto.
- I criteri elencati costituiscono una soluzione alternativa fino a quando "allow-service ipsec" non viene aggiunto in una versione futura.

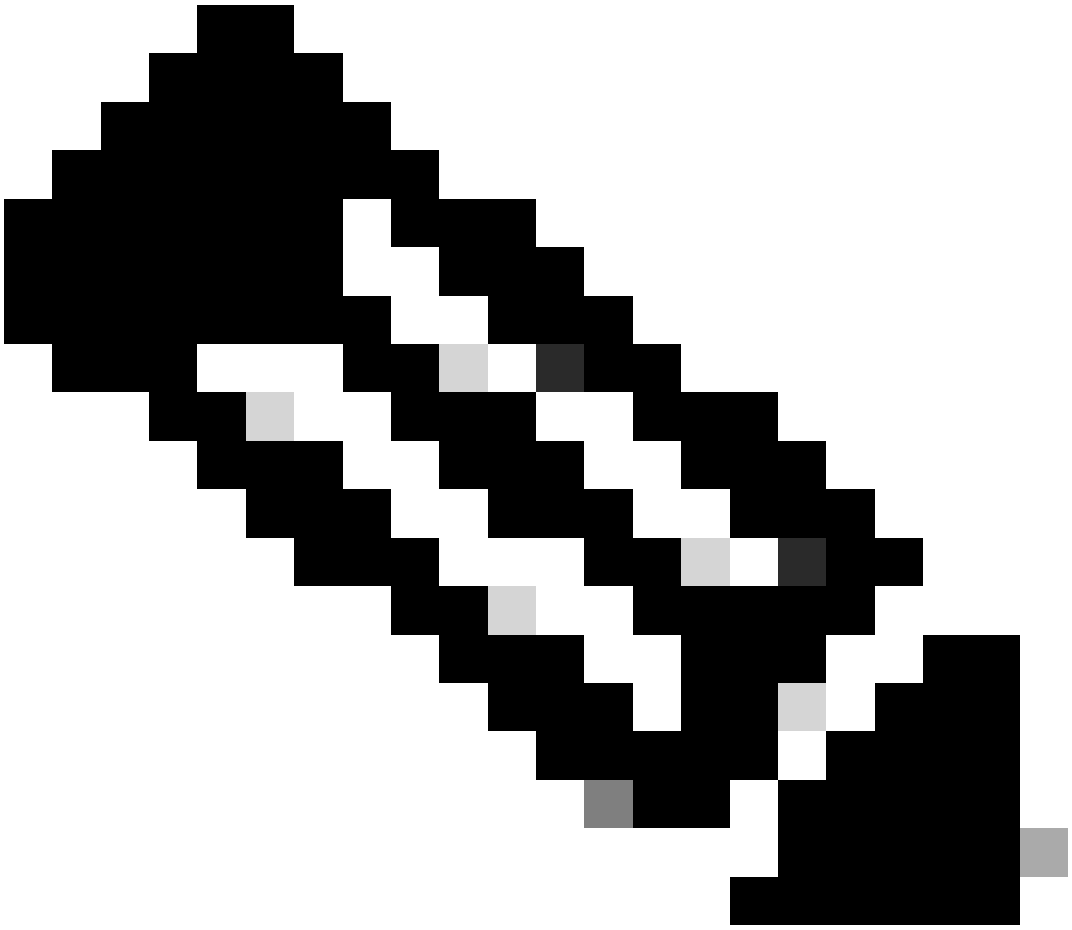
Componenti usati

Il riferimento delle informazioni contenute in questo documento è il SIG (Cisco Umbrella Secure Internet Gateway).

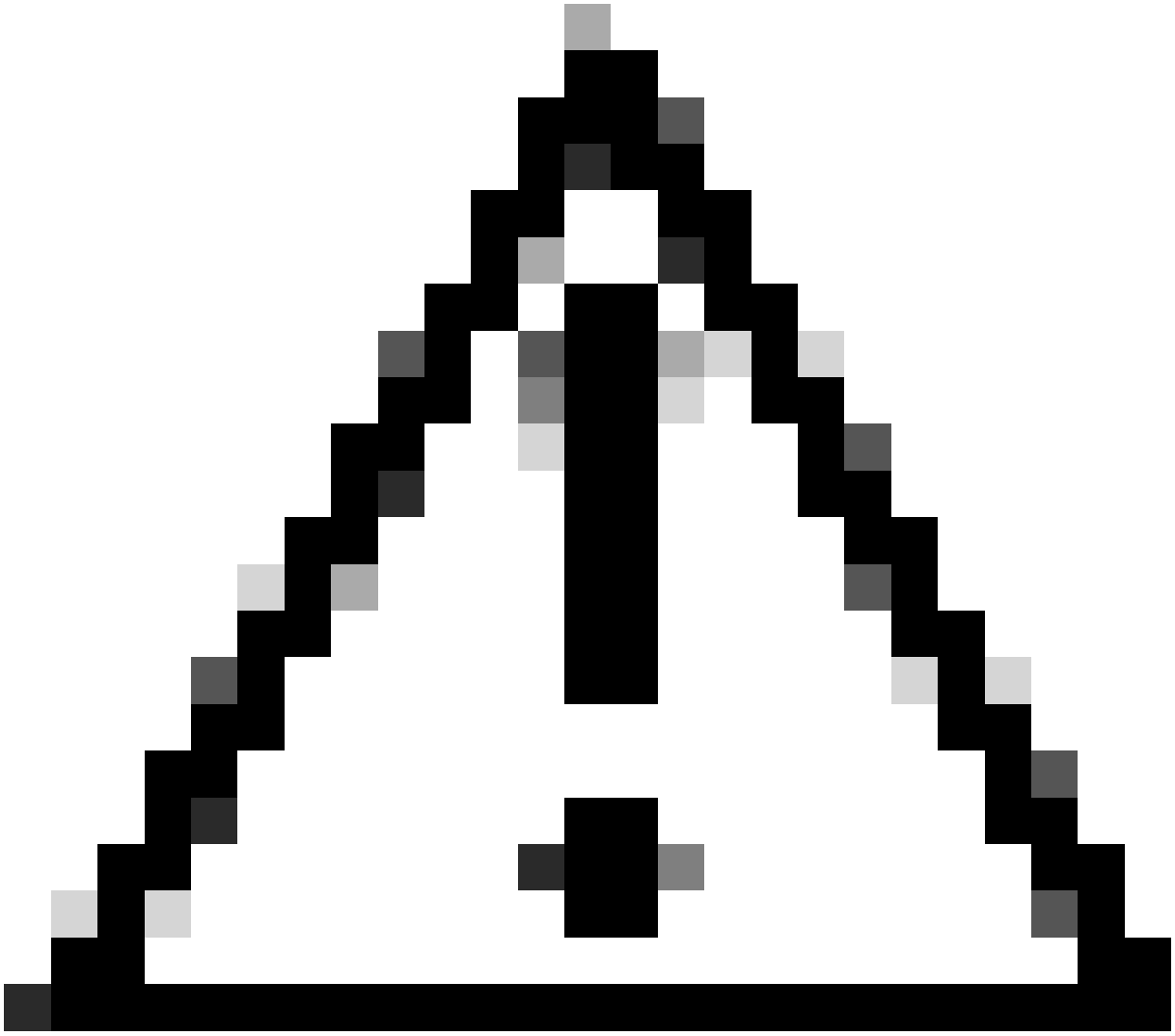
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

In questo articolo viene spiegato come creare un tunnel CDFW utilizzando un router Cisco Edge (in precedenza Viptela cEdge) con versione 16.12.



Nota: Il modello di configurazione riportato di seguito è in formato basato su INTENT, necessario per creare tunnel basati su CLI in vManage. Il formato basato su INTENT è simile al formato di configurazione vEdge, ma presenta alcune differenze. Un modello di funzionalità non può essere utilizzato efficacemente fino alla versione 17.2.1 per cEdge, pertanto questo esempio utilizza un modello basato sulla CLI.



Attenzione: Questo articolo è stato creato per risolvere il problema dell'invio di traffico guest aziendale tramite la soluzione Cisco Umbrella SIG. In questo articolo vengono utilizzati i modelli basati su CLI per ignorare una limitazione dei modelli basati su funzionalità in vManage.

Creazione del tunnel manuale

1. Creare un tunnel CDFW nel dashboard ombrello.

2. Configurare il modello di dispositivo Viptela come di solito si configura per il proprio ambiente.

3. Configurare una policy SIG per consentire le porte UDP 500 e 4500 nelle interfacce di trasporto. A

- CL_for_IKE_IPSec_tunnel è il nome ACL che consente il traffico IPSEC attraverso l'interfaccia del tunnel
- Facoltativo: È possibile limitare ulteriormente l'ACL ai soli controller di dominio Umbrella SIG.

Per ulteriori informazioni, consultare la documentazione di 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. Applicare l'ACL all'interfaccia del tunnel che si sta utilizzando.

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

5. Configurare le interfacce IPsec nella VPN di trasporto, incluse le route richieste.

Queste variabili sono definite nel modello di configurazione CLI dopo questo elenco:

- `{transport_vpn_1}` è l'interfaccia di rete (in genere l'interfaccia WAN) che stabilisce il tunnel IPSEC
- `{transport_vpn_ip_addr_prefix}` è la VPN di trasporto assegnata. (ad esempio, 1.1.1.0/24)
- `{ipsec_int_number}` è il numero dell'interfaccia del tunnel IPSEC (ad esempio, il numero 1 nell'interfaccia "IPSEC1")
- `{ipsec_ip_addr_prefix}` è l'indirizzo ip e la subnet definiti per l'interfaccia del tunnel IPSEC.
- `{transport_vpn_interface_1}` è l'interfaccia di rete (in genere l'interfaccia WAN) che stabilisce il tunnel IPSEC. Si tratta della stessa interfaccia utilizzata nella variabile transport_vpn_1.
- `{psk}` è il valore della chiave precondivisa del tunnel creato nella sezione tunnel di Umbrella Dashboard.
- `{sig_fqdn}` è l'ID IKE del tunnel creato nella sezione tunnel di Umbrella Dashboard.
- `{sig_tunnel_dest_ip}` è l'indirizzo IP del controller di dominio CDFW a cui è connesso il tunnel.

```
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}}
```

Per riferimento, di seguito è riportata una configurazione di esempio citata nei passaggi 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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).