Configurazione dell'hairpinning del traffico tra due tunnel da sito a sito

Sommario

Introduzione

Questo documento descrive come inoltrare il traffico VPN tra due tunnel VPN su una singola interfaccia.

Prerequisiti

Requisiti

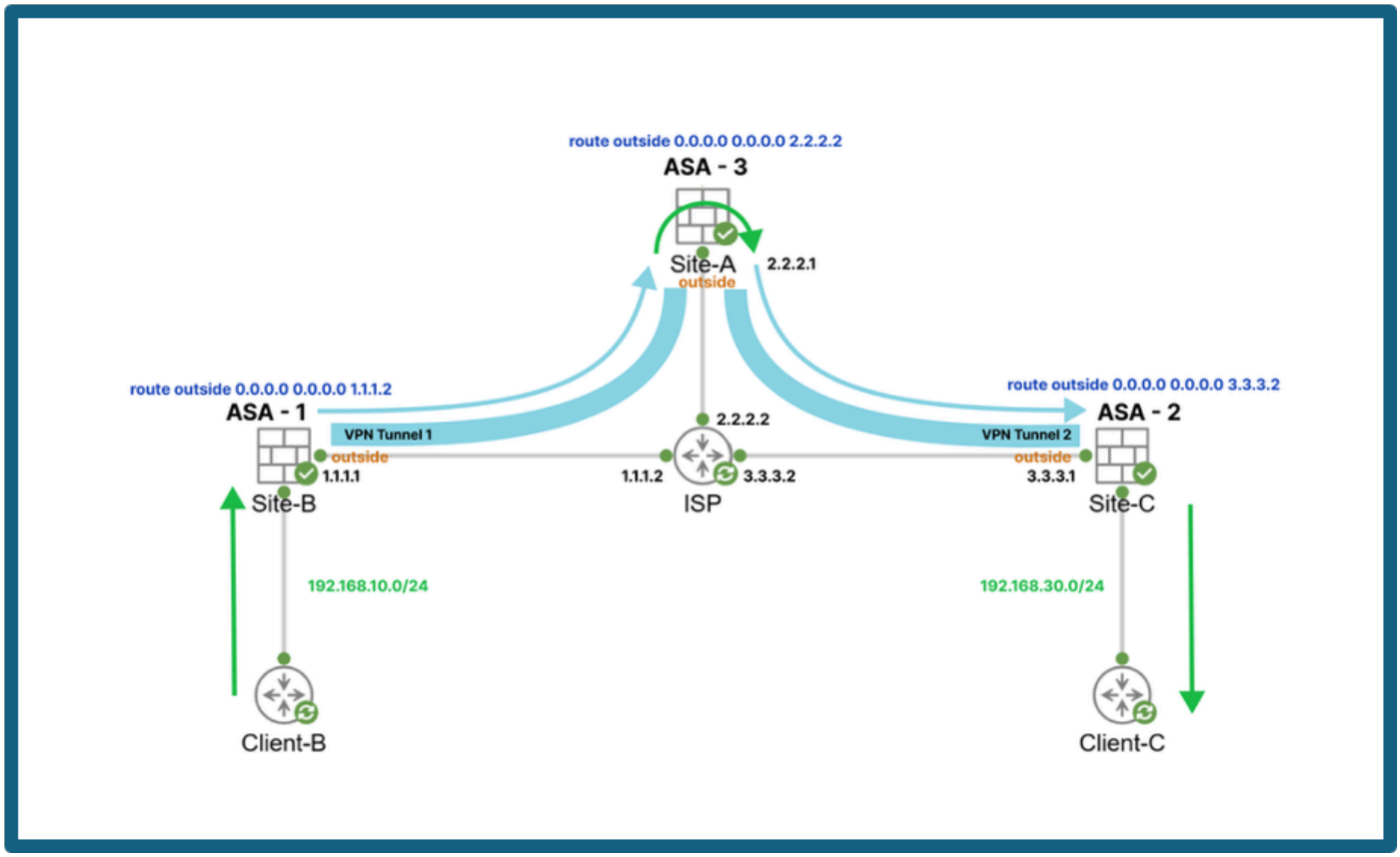
Cisco raccomanda la conoscenza dei seguenti argomenti:
· Conoscenza di base della VPN da sito a sito basata su policy
· Esperienza con la riga di comando ASA

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:
· Adaptive Security Appliance (ASA) versione 9.20
IKEv1

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.

Topologia



Topologia

Premesse

In questa configurazione viene illustrato come reindirizzare il traffico da un tunnel da sito a sito a un altro sullo stesso dispositivo. Per illustrare questa configurazione, sono state usate tre appliance ASA che rappresentano il sito A, il sito B e il sito C.

Configurazione

In questa sezione viene descritta la configurazione necessaria per autorizzare il traffico tra l'appliance ASA-1 (sito B) e l'appliance ASA-2 (sito C) e l'appliance ASA-3 (sito A).

Sono stati configurati due tunnel VPN:

- Tunnel VPN 1: Tunnel VPN tra il sito B e il sito A
- Tunnel VPN 2 : Tunnel VPN tra il sito C e il sito A

Per istruzioni dettagliate su come creare un tunnel VPN basato su criteri su ASA, fare riferimento alla sezione sulla configurazione dell'ASA nella documentazione di Cisco: Configurazione di un tunnel IPSec IKEv1 da sito a sito tra ASA e router Cisco IOS XE

Configurazione di ASA (sito B)

È necessario autorizzare il traffico dalla rete del sito B alla rete del sito C nell'elenco degli accessi crittografici del tunnel VPN 1 sull'interfaccia esterna di ASA 1.
In questo scenario, è compreso tra 192.168.10.0/24 e 192.168.30.0/24

Crypto Access-list:

```
object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

access-list 110 extended permit ip object 192.168.10.0_24 object 192.168.30.0_24
```

Eccezione Nat:

```
nat (inside,outside) source static192.168.10.0_24192.168.10.0_24 destination static192.168.30.0_24192.1
```

Mappa crittografica per tunnel VPN 1:

```
crypto map outside_map 10 match address 110
crypto map outside_map 10 set pfs
crypto map outside_map 10 set peer 2.2.2.1
crypto map outside_map 10 set ikev1 transform-set myset

crypto map outside_map interface outside
```

Configurazione della crittografia ASA (sito C)

Consentire il traffico dalla rete del sito C alla rete del sito B nell'elenco degli accessi crittografici del tunnel VPN 2 sull'interfaccia esterna di ASA 2.
In questo scenario, è compreso tra 192.168.30.0/24 e 192.168.10.0/24

Crypto Access-list:

```
object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

access-list 110 extended permit ip object 192.168.30.0_24 object 192.168.10.0_24
```

Eccezione Nat:

```
nat (inside,outside) source static 192.168.30.0_24 192.168.30.0_24 destination static 192.168.10.0_24 1
```

Mappa crittografica per tunnel VPN 2:

```
crypto map outside_map 20 match address 120
crypto map outside_map 20 set pfs
crypto map outside_map 20 set peer 2.2.2.1
crypto map outside_map 20 set ikev1 transform-set myset

crypto map outside_map interface outside
```

Configurazione della crittografia ASA (sito A)

Consentire il traffico tra la rete del Sito C e la rete del Sito B nell'elenco degli accessi crittografici del tunnel VPN 1 e il traffico tra la rete del Sito B e la rete del Sito C nell'elenco degli accessi crittografici del tunnel VPN 2 sull'interfaccia esterna dell'ASA sul Sito A, in direzione inversa rispetto a quella configurata sulle appliance ASA.

In questo scenario, il valore è compreso tra 192.168.30.0/24 e 192.168.10.0/24 per il tunnel VPN 1 e tra 192.168.10.0/24 e 192.168.30.0/24 per il tunnel VPN 2

Crypto Access-list:

```
object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

access-list 110 extended permit ip object 192.168.30.0_24 object 192.168.10.0_24
access-list 120 extended permit ip object 192.168.10.0_24 object 192.168.30.0_24
```

Configurazione mappa crittografica per il tunnel VPN 1 e 2:

```
crypto map outside_map 10 match address 110
crypto map outside_map 10 set pfs
crypto map outside_map 10 set peer 1.1.1.1
crypto map outside_map 10 set ikev1 transform-set myset

crypto map outside_map 20 match address 120
crypto map outside_map 20 set pfs
crypto map outside_map 20 set peer 3.3.3.1
crypto map outside_map 20 set ikev1 transform-set myset

crypto map outside_map interface outside
```

Inoltre, poiché il traffico deve essere indirizzato dall'esterno verso l'esterno della stessa interfaccia con lo stesso livello di sicurezza, è necessario configurare il comando:

```
same-security-traffic permit intra-interface
```

Flusso di traffico dal sito B al sito C

Si consideri che il traffico viene avviato dal Sito B al Sito c tra il 192.168.10.0/24 e il 192.168.30.0/24.

Sito-B (origine)

1. Il traffico iniziato dalla porta 192.168.10.0/24 network (sito-B) e destinato alla porta 192.168.30.0/24 network (sito-C) viene indirizzato all'interfaccia esterna di ASA-1 in base alla tabella di routing configurata.

2. Una volta raggiunto l'ASA-1, il traffico corrisponde al crypto access-list 110 configurato sull'ASA-1. Ciò attiva la crittografia del traffico tramite il tunnel VPN 1, che invia in modo sicuro i

dati al sito A.

Sito-A (intermedio)

1. Il traffico crittografato proveniente da 192.168.10.0/24 to 192.168.30.0/24 arrives sull'interfaccia esterna dell'ASA sul sito-A.
2. Nel sito A, il traffico viene decrittografato dal tunnel VPN 1 per ripristinare il payload originale.
3. Il traffico decrittografato viene quindi ricrittografato utilizzando il tunnel VPN 2 sull'interfaccia esterna dell'ASA sul sito A.

Sito-C (destinazione)

1. Il traffico crittografato da 192.168.10.0/24 to 192.168.30.0/24 reaches è l'interfaccia esterna di ASA-2 sul sito C.
2. ASA-2 decrittografa il traffico utilizzando il tunnel VPN 2 e inoltra i pacchetti alla LAN del sito C, consegnandoli alla destinazione prevista nel percorso 192.168.30.0/24 network.

Flusso di traffico inverso dal sito C al sito B

Il flusso del traffico inverso, proveniente dal sito C (192.168.30.0/24) and) e destinato al sito B (192.168.10.0/24), determina lo stesso processo, ma in direzione inversa:
1. Nel sito C, il traffico viene crittografato dal tunnel VPN 2 prima dell'invio al sito A.
2. Nel sito A, il traffico viene decrittografato dal tunnel VPN 2, quindi nuovamente crittografato utilizzando il tunnel VPN 1 prima di essere inoltrato al sito B.
3. Nel sito B, il traffico viene decrittografato dal tunnel VPN 1 e consegnato al sito 192.168.10.0/24 network.

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).