Konfigurieren des Hairpinning-Verfahrens für den Datenverkehr zwischen zwei Site-to-Site-Tunneln

Inhalt

Einleitung

In diesem Dokument wird die Weiterleitung des VPN-Datenverkehrs zwischen zwei VPN-Tunneln über eine einzige Schnittstelle beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:
- Grundlegendes Verständnis von richtlinienbasiertem Site-to-Site-VPN
- Erfahrung mit der ASA-Kommandozeile

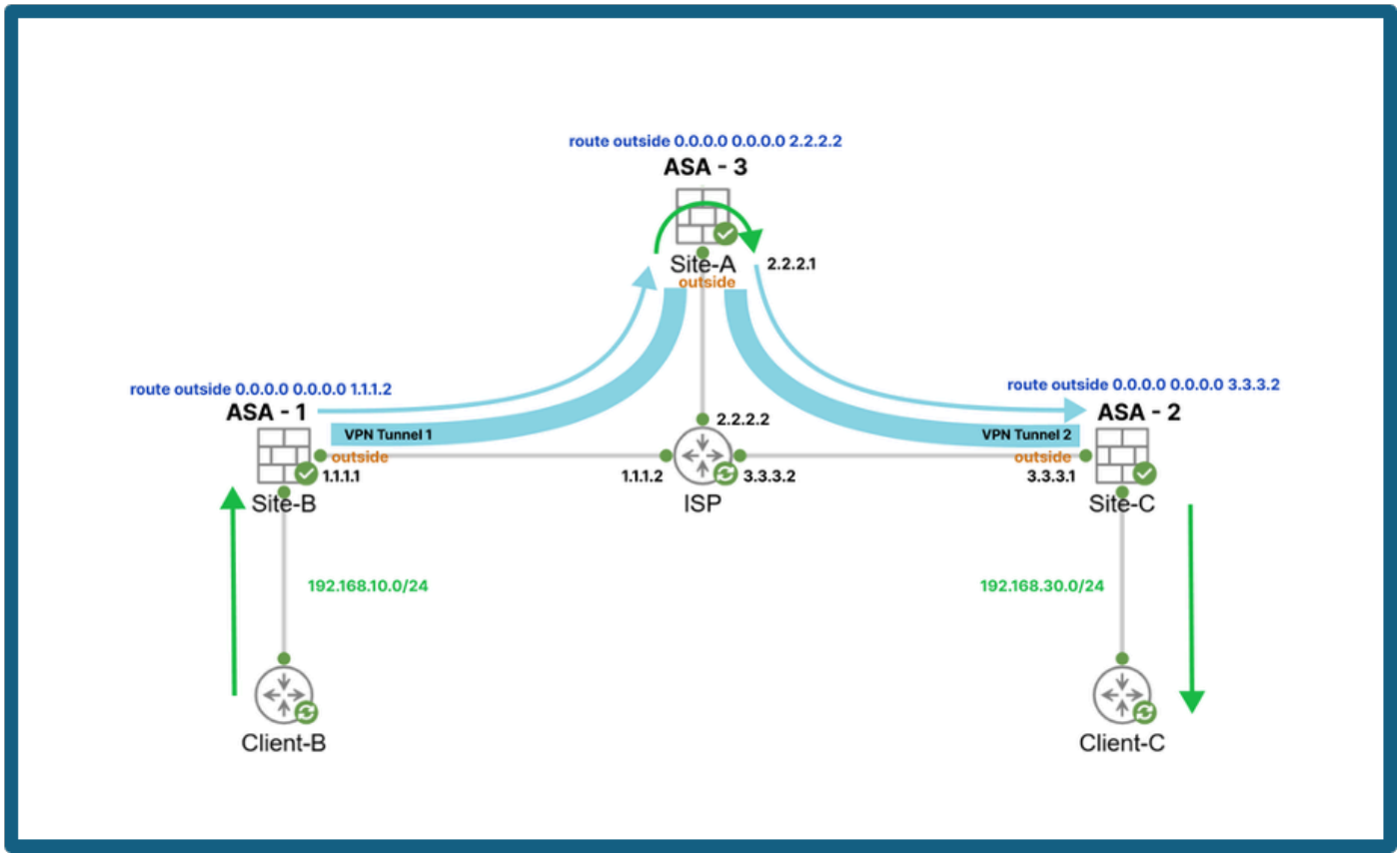
Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:
- Adaptive Security Appliance (ASA) Version 9.20

- IKEv1

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Topologie



Topologie

Hintergrundinformationen

Diese Konfiguration zeigt, wie Datenverkehr von einem Standort-zu-Standort-Tunnel zu einem anderen auf demselben Gerät umgeleitet wird. Zur Veranschaulichung dieser Konfiguration wurden drei ASAs für Standort A, Standort B und Standort C verwendet.

Konfiguration

In diesem Abschnitt wird die erforderliche Konfiguration beschrieben, um den Datenverkehr von ASA-1 (Standort B) zu ASA-2 (Standort C) über ASA-3 (Standort A) zuzulassen.

Es sind zwei VPN-Tunnel konfiguriert:

- VPN-Tunnel 1: VPN-Tunnel zwischen Standort-B und Standort-A
- VPN-Tunnel 2: VPN-Tunnel zwischen Standort-C und Standort-A

Detaillierte Anleitungen zur Erstellung eines richtlinienbasierten VPN-Tunnels auf der ASA finden Sie im Abschnitt zur ASA-Konfiguration in der Cisco Dokumentation: Konfigurieren eines standortübergreifenden IPSec IKEv1-Tunnels zwischen ASA und Cisco IOS XE Router

ASA-Konfiguration (Standort B)

Wir müssen den Datenverkehr vom Standort-B-Netzwerk zum Standort-C-Netzwerk in der Krypto-Zugriffsliste von VPN Tunnel 1 an der externen Schnittstelle von ASA 1 zulassen.
In diesem Szenario ist dies von 192.168.10.0/24 bis 192.168.30.0/24

Krypto-Zugriffsliste:

```
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
```

NAT-Ausnahme:

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

Crypto Map für VPN-Tunnel 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
```

Verschlüsselungskonfiguration für ASA (Standort C)

Lassen Sie den Datenverkehr vom Standort-C-Netzwerk zum Standort-B-Netzwerk in der Krypto-Zugriffsliste von VPN Tunnel 2 an der externen Schnittstelle von ASA 2 zu.
In diesem Szenario ist dies von 192.168.30.0/24 bis 192.168.10.0/24

Krypto-Zugriffsliste:

```
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
```

NAT-Ausnahme:

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

Crypto Map für VPN Tunnel 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
```

Verschlüsselungskonfiguration für ASA (Standort A)

Lassen Sie den Datenverkehr vom Standort-C-Netzwerk zum Standort-B-Netzwerk in der Krypto-Zugriffsliste von VPN-Tunnel 1 und den Datenverkehr vom Standort-B-Netzwerk zum Standort-C-Netzwerk in der Krypto-Zugriffsliste von VPN-Tunnel 2 an der externen Schnittstelle von ASA an Standort A zu, was in umgekehrter Richtung zu dem ist, was wir auf _ ASAs konfiguriert haben.

In diesem Szenario ist für VPN-Tunnel 1 die Adresse 192.168.30.0/24 bis 192.168.10.0/24 und für VPN-Tunnel 2 die Adresse 192.168.10.0/24 bis 192.168.30.0/24

Krypto-Zugriffsliste:

```
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
```

Crypto Map-Konfiguration für VPN-Tunnel 1 und 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
```

Da der Datenverkehr außerdem von außen nach außen weitergeleitet werden muss, und zwar über dieselbe Schnittstelle mit derselben Sicherheitsstufe, muss folgender Befehl konfiguriert werden:

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

Datenverkehrsfluss von Standort B zu Standort C

Betrachten wir nun den Datenverkehr, der von Site-B zu Site-c initiiert wird, also von 192.168.10.0/24 zu 192.168.30.0/24.

Standort-B (Quelle)

1. Datenverkehr, der von der Adresse 192.168.10.0/24 network (Site-B) initiiert wurde und für die Adresse 192.168.30.0/24 network (Site-C) bestimmt ist, wird auf Basis der konfigurierten Routing-Tabelle an die externe Schnittstelle von ASA-1 weitergeleitet.

2. Sobald der Datenverkehr die ASA-1 erreicht, entspricht er der auf der ASA-1 konfigurierten Crypto-Zugriffsliste 110. Dies löst eine Verschlüsselung des Datenverkehrs über den VPN-Tunnel 1 aus, der die Daten sicher an den Standort A sendet.

Standort-A (Mittelstufe)

1. Der verschlüsselte Datenverkehr von 192.168.10.0/24 to 192.168.30.0/24 arrives an der externen Schnittstelle der ASA an Standort A.
2. Am Standort A wird der Datenverkehr durch den VPN-Tunnel 1 entschlüsselt, um die ursprüngliche Nutzlast wiederherzustellen.
3. Der entschlüsselte Datenverkehr wird dann mithilfe des VPN-Tunnels 2 an der externen Schnittstelle der ASA an Standort A erneut verschlüsselt.

Standort-C (Ziel)

1. Der verschlüsselte Datenverkehr von 192.168.10.0/24 to 192.168.30.0/24 reaches ist die externe Schnittstelle von ASA-2 am Standort C.
2. ASA-2 entschlüsselt den Datenverkehr mithilfe von VPN-Tunnel 2 und leitet die Pakete an die LAN-Seite von Standort C weiter. Dadurch werden sie an das gewünschte Ziel innerhalb von 192.168.30.0/24 network übermittelt.

Umgekehrter Datenverkehrsfluss von Standort C zu Standort B

Der umgekehrte Datenverkehrsfluss, der von Site-C (192.168.30.0/24) and) ausgeht und für Site-B (192.168.10.0/24) bestimmt ist, führt zum gleichen Prozess, jedoch in umgekehrter Richtung:
1. Am Standort C wird der Datenverkehr durch den VPN-Tunnel 2 verschlüsselt, bevor er an den Standort A gesendet wird.
2. Am Standort A wird der Datenverkehr durch den VPN-Tunnel 2 entschlüsselt und dann mithilfe des VPN-Tunnels 1 erneut verschlüsselt, bevor er an den Standort B weitergeleitet wird.
3. Am Standort B wird der Datenverkehr durch den VPN-Tunnel 1 entschlüsselt und an die Adresse 192.168.10.0/24 network übertragen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.