Konfigurationsbeispiel für ASA Clientless-SSL-VPN-Datenverkehr über IPsec-LAN-to-LAN-Tunnel

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie eine Verbindung mit einem Clientless-SSL-VPN-Portal der Cisco Adaptive Security Appliance (ASA) herstellen und auf einen Server zugreifen, der sich an einem Remote-Standort befindet, der über einen IPsec-LAN-to-LAN-Tunnel verbunden ist.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Clientlose SSL VPN-Konfiguration.
- LAN-to-LAN-VPN-Konfiguration

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der ASA 5500-X-Serie, auf der Version 9.2(1) ausgeführt wird. Sie gelten jedoch für alle ASA-Versionen.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie Änderungen an einem Live-Netzwerk vornehmen.

Hintergrundinformationen

Wenn der Datenverkehr von einer Clientless-SSL-VPN-Sitzung einen LAN-zu-LAN-Tunnel passiert, beachten Sie, dass zwei Verbindungen vorhanden sind:

- Vom Client zur ASA
- Von der ASA zum Ziel-Host.

Für die ASA-zu-Ziel-Host-Verbindung wird die IP-Adresse der ASA-Schnittstelle verwendet, die dem Ziel-Host "am nächsten" ist. Daher muss der interessante LAN-zu-LAN-Datenverkehr eine Proxy-Identität von dieser Schnittstellenadresse zum Remote-Netzwerk enthalten.

> **Hinweis**: Wenn Smart-Tunnel für ein Lesezeichen verwendet wird, wird die IP-Adresse der ASA-Schnittstelle, die dem Ziel am nächsten liegt, weiterhin verwendet.

Konfigurieren

In diesem Diagramm gibt es einen LAN-zu-LAN-Tunnel zwischen zwei ASAs, der die Weiterleitung des Datenverkehrs von 192.168.10.x an 192.168.20.x ermöglicht.

Die Zugriffsliste, die den interessanten Datenverkehr für diesen Tunnel bestimmt:

ASA1

```
access-list l2l-list extended permit ip 192.168.10.0 255.255.255.0 192.168.20.0
255.255.255.0
```

ASA2

```
access-list l2l-list extended permit ip 192.168.20.0 255.255.255.0 192.168.10.0
255.255.255.0
```

Wenn der clientlose SSL VPN-Benutzer versucht, mit einem Host im Netzwerk 192.168.20.x zu kommunizieren, verwendet ASA1 die Adresse 209.165.200.225 als Quelle für diesen Datenverkehr. Da die ACL (LAN-to-LAN Access Control List) nicht die Proxy-Identität 209.168.200.225 enthält, wird der Datenverkehr nicht über den LAN-to-LAN-Tunnel gesendet.

Um Datenverkehr über den LAN-to-LAN-Tunnel zu senden, muss der interessanten Datenverkehr-ACL ein neuer Access Control Entry (ACE) hinzugefügt werden.

ASA1

```
access-list l2l-list extended permit ip host 209.165.200.225 192.168.20.0
255.255.255.0
```

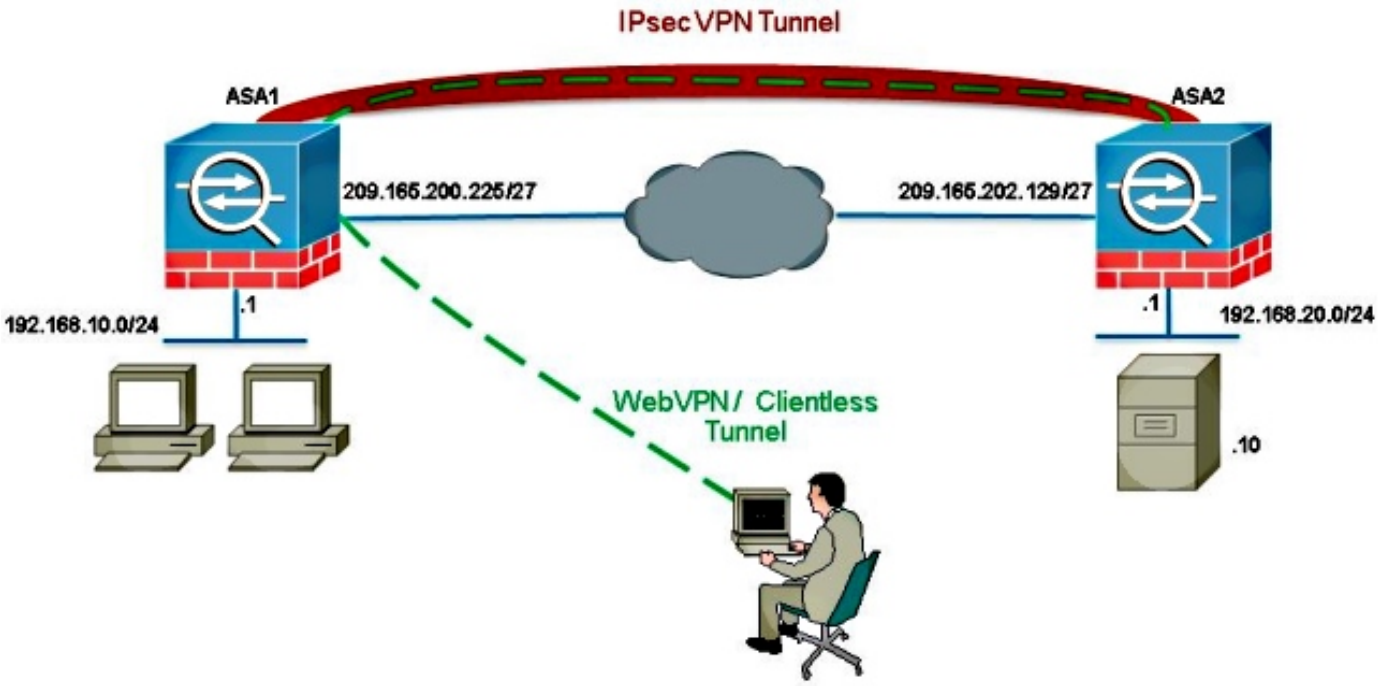
ASA2

```
access-list l2l-list extended permit ip 192.168.20.0 255.255.255.0 host
209.165.200.225
```

Das gleiche Prinzip gilt für Konfigurationen, bei denen der clientlose SSL VPN-Datenverkehr dieselbe Schnittstelle **ausblenden** muss, die auch eingeschaltet wurde, selbst wenn der Datenverkehr nicht über einen LAN-zu-LAN-Tunnel geleitet werden soll.

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm



In der Regel führt ASA2 Port Address Translation (PAT) für die Adresse 192.168.20.0/24 durch, um einen Internetzugang bereitzustellen. In diesem Fall sollte der Datenverkehr von 192.168.20.0/24 auf ASA 2 vom PAT-Prozess ausgeschlossen werden, wenn er auf 209.165.200.225 steigt. Andernfalls würde die Antwort nicht durch den LAN-zu-LAN-Tunnel geleitet. Beispiel:

ASA2

```
nat (inside,outside) source static obj-192.168.20.0 obj-
192.168.20.0 destination
static obj-209.165.200.225 obj-209.165.200.225
!
object network obj-192.168.20.0
nat (inside,outside) dynamic interface
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

- **show crypto ipsec sa**-Verify with this command that a Security Association (SA) between the ASA1 Proxy IP address and the remote network has been created. Überprüfen Sie, ob die verschlüsselten und entschlüsselten Zähler größer werden, wenn der Clientless-SSL VPN-Benutzer auf diesen Server zugreift.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Wenn die Sicherheitszuordnung nicht erstellt wird, können Sie das IPsec-Debuggen für die Fehlerursache verwenden:

- **debuggen crypto ipsec <level>**

  Hinweis: Weitere Informationen zu Debug-Befehlen vor der Verwendung von **Debug-**Befehlen finden Sie unter Wichtige Informationen.