ASA VPN-Client-Verbindung über ein L2L-Tunnel-Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Cisco Adaptive Security Appliance (ASA) konfiguriert wird, um eine Remote-VPN-Client-Verbindung von einer LAN-to-LAN (L2L)-Peer-Adresse aus zuzulassen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco ASA
- VPNs für Remote-Zugriff
- LAN-zu-LAN-VPNs

Verwendete Komponenten

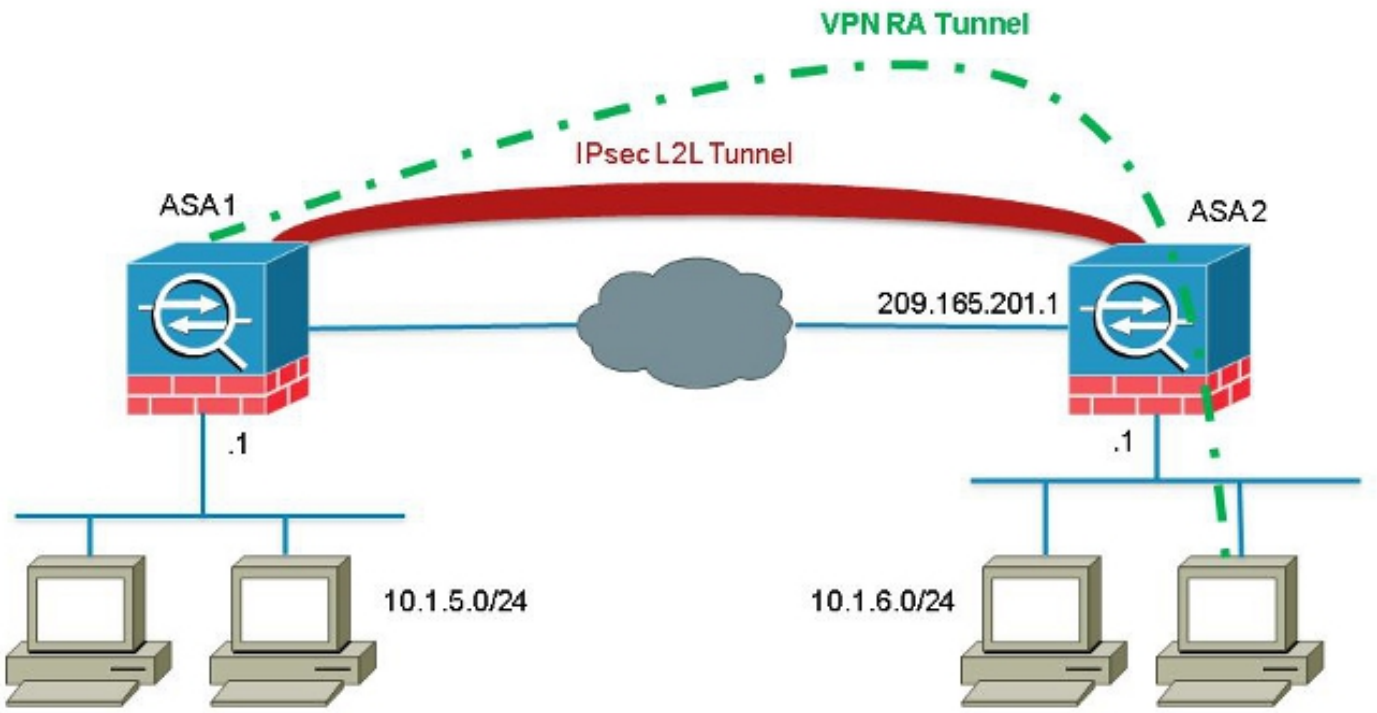
Die Informationen in diesem Dokument basieren auf der Cisco Serie ASA 5520, auf der Software Version 8.4(7) ausgeführt wird.

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. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Obwohl es nicht üblich ist, dass ein VPN-Client versucht, eine Verbindung über einen L2L-Tunnel herzustellen, können Administratoren bestimmten Remote-Benutzern bestimmte Berechtigungen oder Zugriffsbeschränkungen zuweisen und sie anweisen, den Software-Client zu verwenden, wenn Zugriff auf diese Ressourcen erforderlich ist.

> **Hinweis**: Dieses Szenario hat in der Vergangenheit funktioniert, aber nach einem Upgrade der Headend-ASA auf Version 8.4(6) oder höher kann der VPN-Client die Verbindung nicht mehr herstellen.



Cisco Bug ID CSCuc75090 führte eine Änderung des Verhaltens ein. Bei Private Internet Exchange (PIX), als der Internet Protocol Security (IPSec)-Proxy nicht mit einer Zugriffskontrollliste für die Crypto Map (ACL) übereinstimmte, überprüfte er die Einträge weiter unten in der Liste. Dies beinhaltet eine dynamische Crypto-Map ohne Peer-Angabe.

Dies galt als Schwachstelle, da Remote-Administratoren Zugriff auf Ressourcen erhalten konnten, die der Headend-Administrator bei der Konfiguration des statischen L2L nicht beabsichtigt hatte.

Es wurde eine Korrektur erstellt, die eine Prüfung hinzugefügt hat, um Übereinstimmungen mit einem Crypto-Map-Eintrag ohne Peer zu verhindern, wenn bereits ein Zuordnungseintrag überprüft wurde, der dem Peer entsprach. Dies betraf jedoch das Szenario, das in diesem Dokument behandelt wird. Insbesondere ein Remote-VPN-Client, der versucht, eine Verbindung über eine L2L-Peer-Adresse herzustellen, kann keine Verbindung zum Headend herstellen.

Konfigurieren

Verwenden Sie diesen Abschnitt, um die ASA so zu konfigurieren, dass eine Remote-VPN-Client-Verbindung von einer L2L-Peer-Adresse zugelassen wird.

Neuen dynamischen Eintrag hinzufügen

Um Remote-VPN-Verbindungen von L2L-Peer-Adressen zu ermöglichen, müssen Sie einen neuen dynamischen Eintrag hinzufügen, der dieselbe Peer-IP-Adresse enthält.

> **Hinweis**: Sie müssen auch einen anderen dynamischen Eintrag ohne Peer lassen, damit jeder Client aus dem Internet auch eine Verbindung herstellen kann.

Im Folgenden finden Sie ein Beispiel für die vorherige Konfiguration der dynamischen Crypto Map-Funktion:

```
crypto dynamic-map ra-dyn-map 10 set ikev1 transform-set ESP-AES-128-SHA

crypto map outside_map 1 match address outside_cryptomap_1
crypto map outside_map 1 set peer 209.165.201.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic ra-dyn-map
```

Nachfolgend finden Sie die Konfiguration der dynamischen Crypto Map mit dem neuen konfigurierten dynamischen Eintrag:

```
crypto dynamic-map ra-dyn-map 10 set ikev1 transform-set ESP-AES-128-SHA
crypto dynamic-map ra-dyn-map 10 set peer 209.165.201.1
crypto dynamic-map ra-dyn-map 20 set ikev1 transform-set ESP-AES-128-SHA

crypto map outside_map 1 match address outside_cryptomap_1
crypto map outside_map 1 set peer 209.165.201.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic ra-dyn-map
```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.