Exemple de configuration de l'authentification ASA vers un ASA de secours lorsque le périphérique AAA est situé via une L2L

Contenu

Introduction

Ce document décrit comment contourner un scénario dans lequel l'administrateur ne peut pas s'authentifier auprès d'un dispositif de sécurité adaptatif (ASA) Cisco de secours dans une paire de basculement en raison du fait que le serveur AAA (Authentication, Authorization, and Accounting) est situé sur un site distant via un LAN à LAN (L2L).

Bien que la reprise de l'authentification LOCAL puisse être utilisée, l'authentification RADIUS pour les deux unités est préférée.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Basculement ASA
- VPN
- Traduction d'adresses réseau (NAT)

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

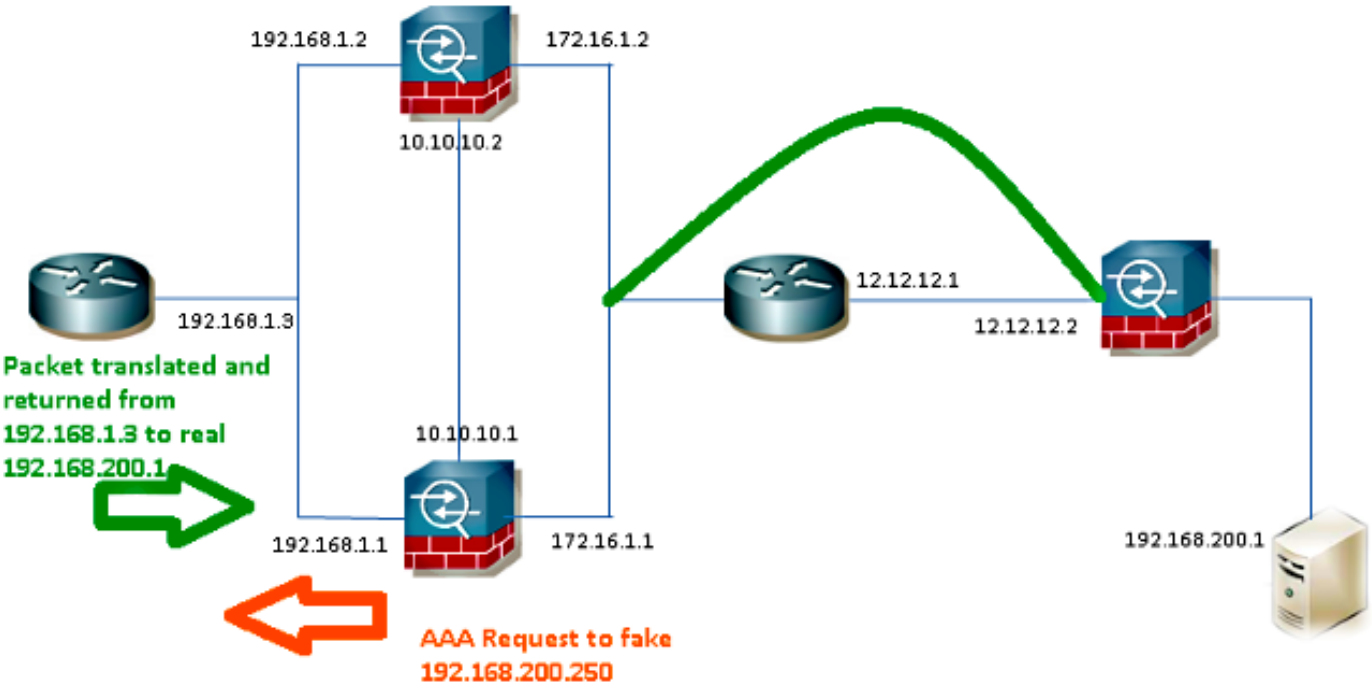
Configuration

> **Note**: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Le serveur RADIUS est situé à l'extérieur de la paire de basculement et il est accessible via un tunnel L2L vers 12.12.12.2. C'est ce qui cause le problème, car l'ASA de secours tente de l'atteindre via sa propre interface externe, mais il n'y a pas de tunnel sur elle à ce stade ; pour qu'il fonctionne, il doit envoyer la requête à l'interface active afin que le paquet puisse circuler sur le VPN mais que les routes soient répliquées à partir de l'unité active.

Une option consiste à utiliser une fausse adresse IP pour le serveur RADIUS sur les ASA et à la pointer vers l'intérieur. Par conséquent, les adresses IP source et de destination de ce paquet peuvent être traduites sur un périphérique interne.



Routeur 1

```
interface FastEthernet0/0
ip address 192.168.1.3 255.255.255.0
no ip redirects
no ip unreachables
ip nat enable
duplex auto
speed auto
```

```
ip access-list extended NAT
permit ip 192.168.1.0 0.0.0.255 host 192.168.200.250

ip nat source list NAT interface FastEthernet0/0 overload
ip nat source static 192.168.200.1 192.168.200.250

ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

ASA

```
aaa-server RADIUS protocol radius
aaa-server RADIUS (inside) host 192.168.200.250
timeout 3
key *****
authentication-port 1812
accounting-port 1813

aaa authentication serial console LOCAL
aaa authentication ssh console RADIUS LOCAL
aaa authentication telnet console RADIUS LOCAL
aaa authentication http console RADIUS LOCAL
aaa authentication enable console RADIUS LOCAL

route outside 0.0.0.0 0.0.0.0 172.16.1.3 1
route inside 192.168.200.250 255.255.255.255 192.168.1.3 1
```

> **Note**: L'adresse IP **192.168.200.250** a été utilisée dans l'exemple, mais toute adresse IP inutilisée fonctionne.

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Routeur

```
Router#   show ip nat nvi tra
Pro Source global Source local Destin local Destin global
udp 192.168.1.3:1025 192.168.1.1:1025 192.168.200.250:1812 192.168.200.1:1812
--- 192.168.200.1 192.168.2.1 --- ---
--- 192.168.200.250 192.168.200.1 --- ---
```

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.