Configuration de la connexion épinglée sur ASA

Table des matières

Introduction

Ce document décrit les étapes nécessaires pour configurer correctement Hairpin sur un dispositif de sécurité adaptatif Cisco (ASA)

Conditions préalables

Exigences

Cisco vous recommande de connaître les sujets suivants :

- Configuration NAT sur ASA
- Configuration ACL sur ASA

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel Cisco Adaptive Security Appliance Version 9.18(4)22

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configurer

La traduction d'adresses réseau (NAT) en épingle à cheveux, également appelée bouclage NAT ou réflexion NAT, est une technique utilisée dans le routage réseau, par laquelle un périphérique sur un réseau privé peut accéder à un autre périphérique sur le même réseau privé via une adresse IP publique.

Cette option est utilisée lorsqu'un serveur est hébergé derrière un routeur et que vous souhaitez autoriser des périphériques sur le même réseau local que le serveur à y accéder à l'aide de l'adresse IP publique (celle attribuée au routeur par le fournisseur d'accès Internet), comme le ferait un périphérique externe.

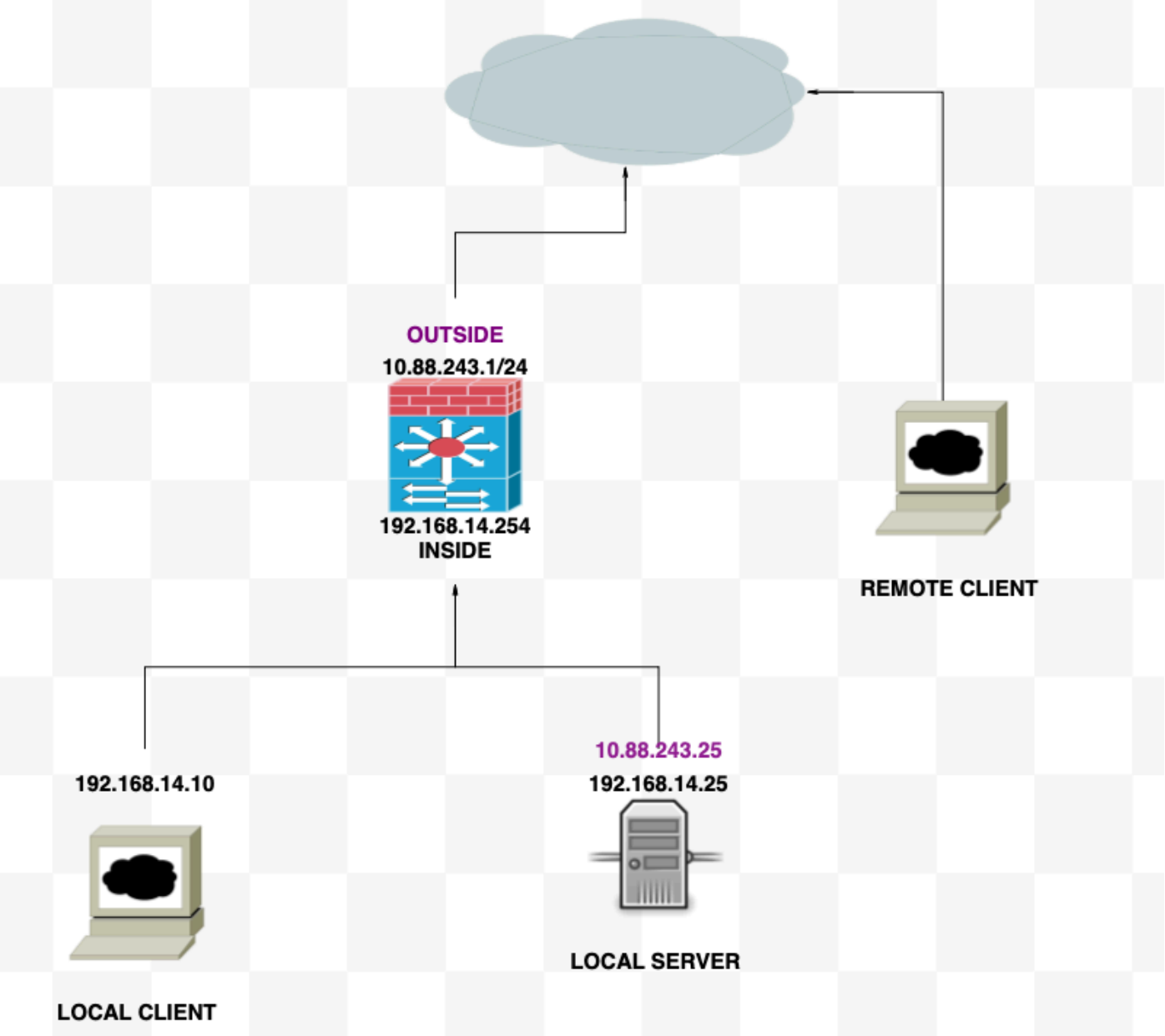
Le terme « hairpin » est utilisé parce que le trafic du client arrive au routeur (ou au pare-feu implémentant la NAT) et est ensuite « renvoyé » comme une épingle au réseau interne après traduction pour accéder à l'adresse IP privée du serveur.

Par exemple, vous avez un serveur Web sur votre réseau local avec une adresse IP privée. Vous souhaitez accéder à ce serveur à l'aide de son adresse IP publique ou d'un nom de domaine qui correspond à l'adresse IP publique, même lorsque vous êtes sur le même réseau local.

Sans la fonction NAT Hairpin, votre routeur ne comprendrait pas cette requête, car il s'attend à ce que les requêtes d'adresse IP publique proviennent de l'extérieur du réseau.

La NAT en épingle à cheveux résout ce problème en permettant au routeur de reconnaître que, bien que la requête soit effectuée vers une adresse IP publique, elle doit être routée vers un périphérique sur le réseau local.

Diagramme du réseau



Configurations

Étape 1. Création des objets

- Réseau interne:192.168.14.10
- Serveur Web : 192.168.14.25
- Serveur Web public : 10.88.243.25
- Port : 80

<#root>

```
ciscoasa(config)#
 object network Local_Client
ciscoasa(config-network-object)#
 host 192.168.14.10
```

```
ciscoasa(config)#
 object network Web_Server
ciscoasa(config-network-object)#
 host 192.168.14.25
ciscoasa(config)#
 object network P_Web_Server
ciscoasa(config-network-object)#
 host 10.88.243.25
ciscoasa(config)#
 object service HTTP
ciscoasa(config-service-object)#
 service tcp destination eq 80
```

Étape 2. Création de la NAT

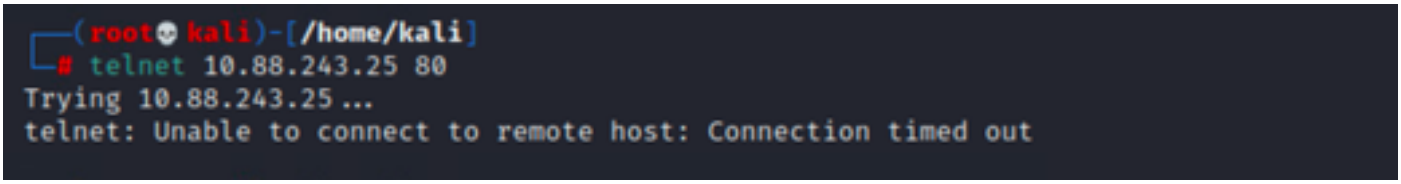
<#root>

```
ciscoasa
(config-service-object)# nat (Inside,Inside) source dynamic Local_Client interface destination static P_
```

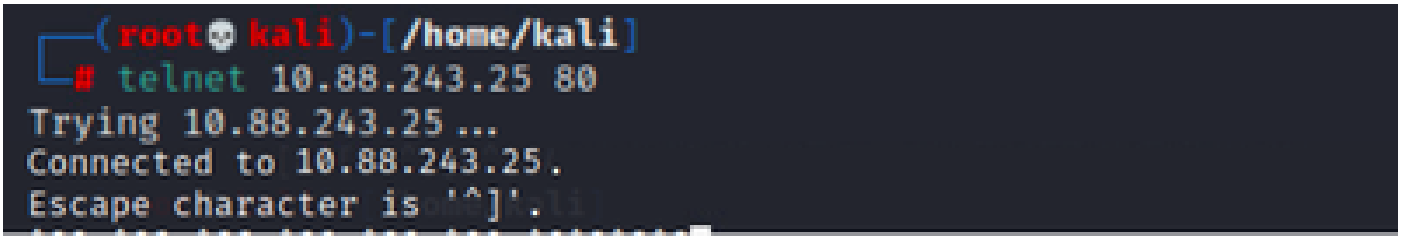
Vérifier

À partir du client local, exécutez une commande telnet destination IP avec le port de destination de :

Si le message « telnet cannot connect to remote host : Connection timed out » s'affiche, un problème est survenu à un moment donné au cours de la configuration.



Mais si elle dit "Connected", ça marche !



Dépannage

Si vous rencontrez des problèmes avec la traduction d'adresses de réseau (NAT), utilisez ce guide étape par étape pour dépanner et résoudre les problèmes courants.

Étape 1 : vérification de la configuration des règles NAT

- Vérifier les règles NAT : vérifiez que toutes les règles NAT sont correctement configurées. Vérifiez que les adresses IP source et de destination, ainsi que les ports, sont corrects.
- Interface Assignment : vérifiez que les interfaces source et de destination sont correctement attribuées dans la règle NAT. Un mappage incorrect peut empêcher la traduction ou le routage du trafic.
- NAT Rule Priority : vérifiez que la priorité de la règle NAT est supérieure à celle de toute autre règle pouvant correspondre au même trafic. Les règles sont traitées dans un ordre séquentiel, de sorte qu'une règle placée plus haut est prioritaire.

Étape 2 : Vérification des règles de contrôle d'accès (ACL)

- Vérifier les listes de contrôle d'accès : vérifiez les listes de contrôle d'accès pour vous assurer qu'elles sont appropriées pour autoriser le trafic NAT. Les listes de contrôle d’accès doivent être configurées pour reconnaître les adresses IP traduites.
- Rules Order : vérifiez que la liste de contrôle d'accès est dans le bon ordre. Comme les règles NAT, les listes de contrôle d’accès sont traitées de haut en bas et la première règle qui correspond au trafic est celle qui est appliquée.
- Traffic Permissions : vérifiez qu'il existe une liste de contrôle d'accès appropriée pour autoriser le trafic du réseau interne vers la destination traduite. Si une règle est manquante ou mal configurée, le trafic souhaité peut être bloqué.

Étape 3 : Diagnostics supplémentaires

- Utiliser les outils de diagnostic : utilisez les outils de diagnostic disponibles pour surveiller et déboguer le trafic transitant par le périphérique. Cela inclut l'affichage des journaux en temps réel et des événements de connexion.
- Connexions de redémarrage : dans certains cas, les connexions existantes ne reconnaissent pas les modifications apportées aux règles NAT ou aux listes de contrôle d'accès tant qu'elles n'ont pas été redémarrées. Supprimez les connexions existantes pour forcer l'application de nouvelles règles.

<#root>

```
ciscoasa(config)#
```

```
 clear xlate
```

- Verify Translation : utilisez des commandes telles que `show xlate` et `show nat` sur la ligne

de commande si vous travaillez avec des périphériques ASA pour vérifier que les traductions NAT sont effectuées comme prévu.

<#root>

ciscoasa(config)#

show xlate

<#root>

ciscoasa(config)#

show nat

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.