Configuration de Hairpin avec Firepower Management Center

Table des matières

Introduction

Ce document décrit les étapes nécessaires pour configurer correctement Hairpin sur un pare-feu Firepower Threat Defense (FTD) avec Firepower Management Center (FMC).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Firepower Management Center (FMC)
- Protection contre les menaces Firepówer (FTD)

Composants utilisés

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

- Firepower Management Center Virtual 7.2.4.
- Défense contre les menaces Firepower Virtual 7.2.4.

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.

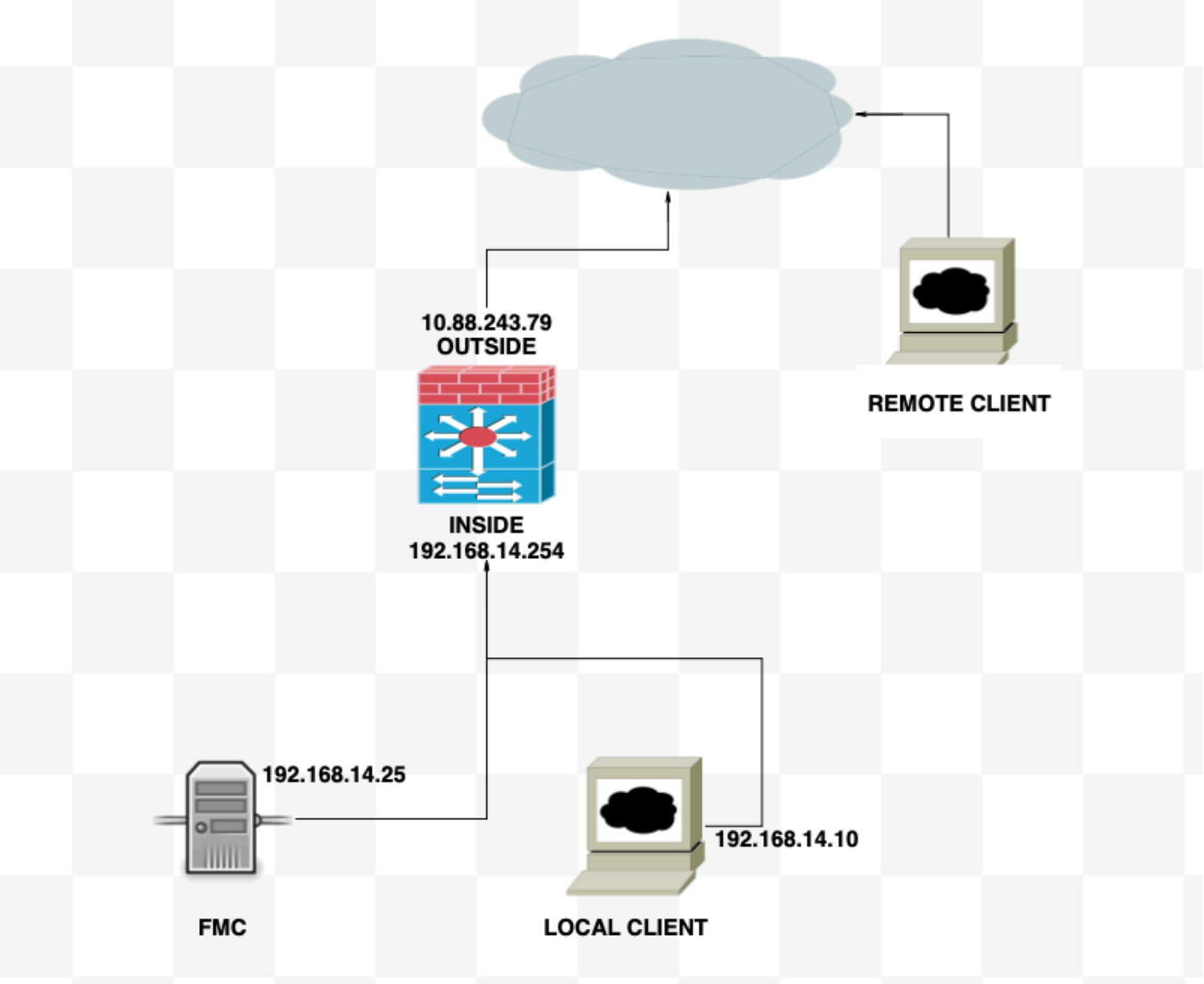
Configurer

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

Cette fonction est utile pour les services réseau tels que l'hébergement Web au sein d'un réseau local, où les utilisateurs sur le réseau local doivent accéder au serveur interne en utilisant la même URL ou adresse IP que les utilisateurs externes. Elle garantit un accès uniforme aux ressources, que la requête provienne de l'intérieur ou de l'extérieur du réseau local.

Dans cet exemple, un FMC doit être accessible via l'adresse IP de l'interface externe du FTD

Diagramme

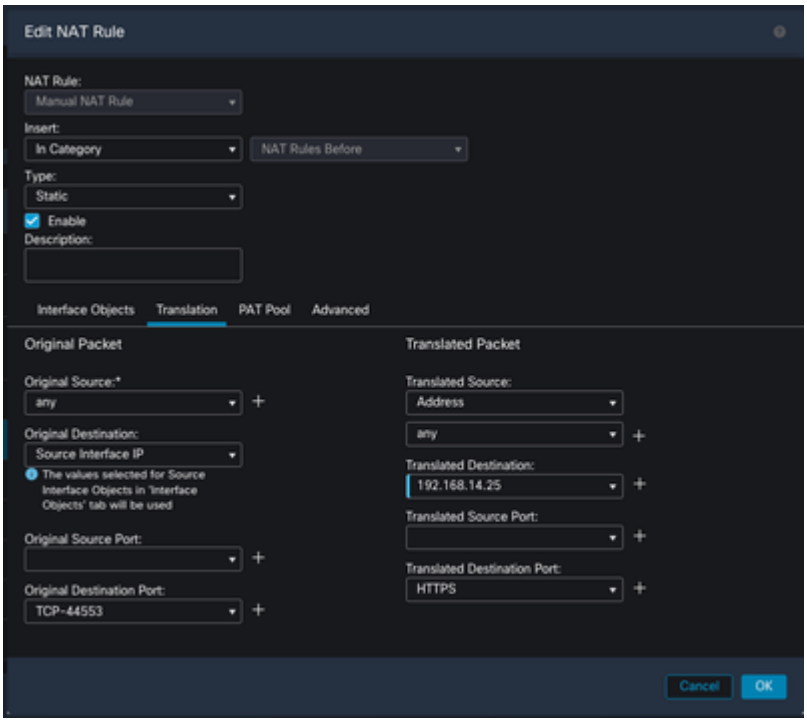


Étape 1 : configuration de la fonction Nat externe-interne

Comme première étape, une NAT statique doit être configurée ; Dans cet exemple, l'adresse IP de destination et le port de destination sont traduits à l'aide de l'adresse IP de l'interface externe et la destination du port est 44553.

Dans le FMC, accédez à Device > NAT pour créer ou modifier la stratégie existante, puis cliquez sur la zone Add Rule.

- Règle NAT : Règle Nat Manuelle
- Source originale : tous les modèles
- Destination initiale : IP d'interface source
- Port de destination initial : 44553
- Destination traduite : 192.168.14.25
- Port de destination traduit : 443



Configurez la stratégie. Accédez à Policies > Access Control pour créer ou modifier la stratégie existante, puis cliquez sur la zone Add Rule.

Zone source : Extérieur

Zone de destination : Intérieur

Réseau source : tous les modèles

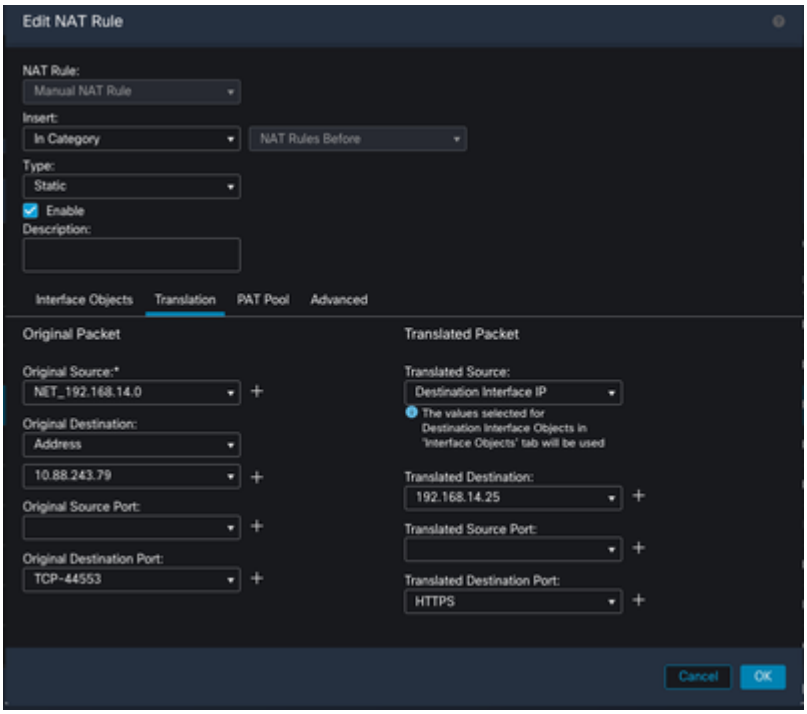
Réseau de destination : 10.88.243.79

Étape 2 : configuration de la fonction Nat interne (épingle à cheveux)

Dans la deuxième étape, une NAT statique doit être configurée de l'intérieur vers l'intérieur ; dans cet exemple, l'adresse IP de destination et le port de destination sont traduits à l'aide d'un objet avec l'adresse IP de l'interface externe et le port de destination est 44553.

Dans le FMC, accédez à Device > NAT pour modifier la stratégie existante, puis cliquez sur la zone Add Rule.

- Règle NAT : Règle Nat Manuelle
- Source originale : 192.168.14.0/24
- Destination initiale : Adresse 10.88.243.79
- Port de destination initial : 44553
- Source traduite : Adresse IP de l'interface de destination
- Destination traduite : 192.168.14.25
- Port de destination traduit : 443



Configurez la stratégie. Accédez à Policies > Access Control pour modifier la stratégie existante, puis cliquez sur la zone Add Rule.

Zone source : tous les modèles

Zone de destination : tous les modèles

Réseau source : 192.168.14.0/24

Réseau de destination : 10.88.243.79

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks
Mandatory - la primera (1-4)					
1	nat-fmc	OUTSIDE	INSIDE	any	Any
2	Hairpin	Any	Any	NET_192.168.14	10.88.243.79

Vérifier

À partir du client local, établissez une connexion Telnet avec l'adresse IP de destination et le port de destination :

Si ce message d'erreur « telnet cannot connect to remote host : Connection timed out", quelque chose s'est mal passé à un moment de la configuration.

```
┌──(root💀 kali)-[/home/kali]
└─# telnet 10.88.243.79 44553
Trying 10.88.243.79 ...
telnet: Unable to connect to remote host: Connection timed out
```

Mais si le message Connected (Connecté) s'affiche, la configuration a réussi.

```
┌──(root💀 kali)-[/home/kali]
└─# telnet 10.88.243.79 44553
Trying 10.88.243.79 ...
Connected to 10.88.243.79.
Escape character is '^]'.
```

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

- Examiner les règles NAT : Assurez-vous que toutes les règles NAT sont correctement configurées dans FMC. Vérifiez que les adresses IP source et de destination, ainsi que les ports, sont corrects.
- Affectation d'interface : 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.

- Priorité de la règle NAT : Vérifiez que la règle NAT est placée en haut de toute autre règle pouvant correspondre au même trafic. Les règles dans FMC sont traitées dans l'ordre séquentiel, de sorte qu'une règle placée plus haut a la priorité.

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

- Vérifier les ACL : 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.
- Ordre des règles : Assurez-vous 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.
- Autorisations de trafic : 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 dans FMC pour surveiller et déboguer le trafic passant par le périphérique. Cela inclut l'affichage des journaux en temps réel et des événements de connexion.
- Redémarrer les connexions : Dans certains cas, les connexions existantes ne peuvent pas reconnaître les modifications apportées aux règles NAT ou aux listes de contrôle d'accès tant qu'elles ne sont pas redémarrées. Supprimez les connexions existantes pour forcer l'application de nouvelles règles.

De LINA :

```
<#root>
firepower#
 clear xlate
```

- Vérifier la traduction : Utilisez des commandes telles que show xlate et show nat sur la ligne de commande si vous travaillez avec des périphériques FTD pour vérifier que les traductions NAT sont effectuées comme prévu.

De LINA :

```
<#root>
firepower#
 show nat
```

<#root>

firepower#

show xlate

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.