Haarspeld configureren met Firepower Management Center

Inhoud

Inleiding

In dit document worden de stappen beschreven die nodig zijn om Hairpin succesvol te configureren op een Firepower Threat Defense (FTD) met Firepower Management Center (FMC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower Management Center (FMC)
- Firetower Threat Defense (FTD)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Firepower Management Center Virtual 7.2.4.
- Firepower Threat Defense Virtual 7.2.4.

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

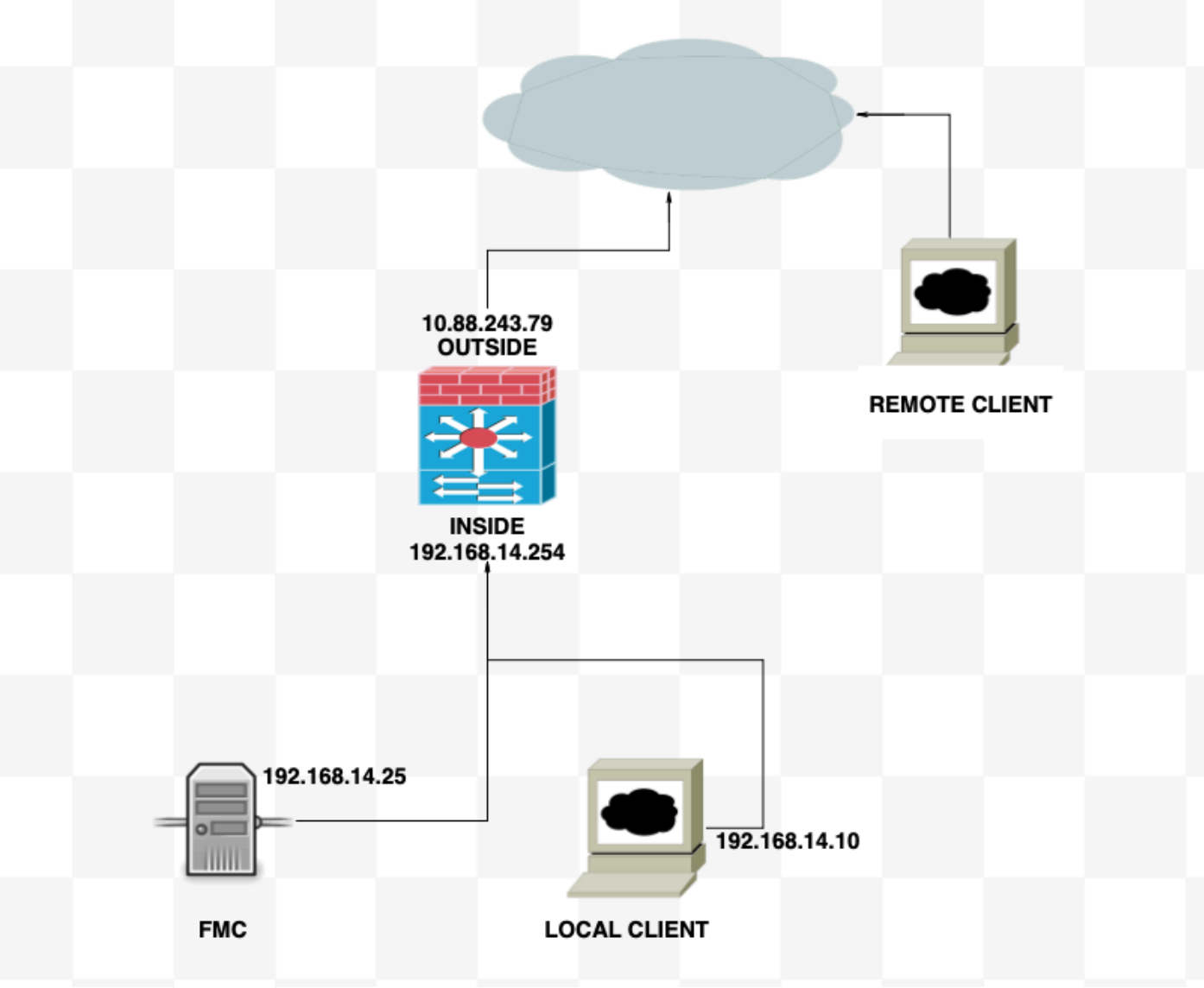
Configureren

De term hairpin wordt gebruikt omdat het verkeer van de client naar de router (of firewall die NAT implementeert) gaat en vervolgens als een hairpin wordt teruggestuurd naar het interne netwerk na vertaling om toegang te krijgen tot het privé-IP-adres van de server.

Deze functie is handig voor netwerkservices zoals webhosting binnen een lokaal netwerk, waarbij de gebruikers op het lokale netwerk toegang moeten krijgen tot de interne server met behulp van hetzelfde URL- of IP-adres dat externe gebruikers zouden gebruiken. Het zorgt voor uniforme toegang tot bronnen, ongeacht of het verzoek afkomstig is van binnen of buiten het lokale netwerk.

In dit voorbeeld moet een FMC toegankelijk zijn via het IP van de externe interface van de FTD

Diagram

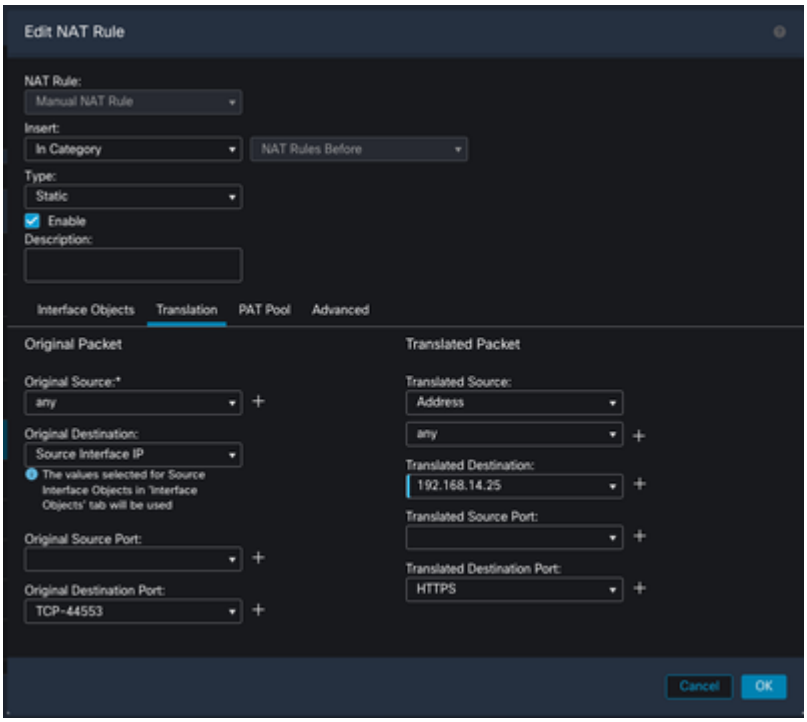


Stap 1. Buiten-Binnen-NAT configureren

Als eerste stap moet een statische NAT worden geconfigureerd; in dit voorbeeld worden de bestemmings-IP en bestemmingspoort vertaald met behulp van het IP van de externe interface en is de poortbestemming 44553.

Navigeer vanuit de FMC naar Apparaat > NAT om het bestaande beleid te maken of te bewerken en klik vervolgens op het vak Regel toevoegen.

- NAT-regel: handmatige NAT-regel
- Oorspronkelijke bron: Any
- Oorspronkelijke bestemming: Source Interface IP
- Oorspronkelijke bestemmingshaven: 44553
- Vertaalde bestemming: 192.168.14.25
- Vertaalde bestemmingshaven: 443



Configureer het beleid. Navigeer naar Beleid > Toegangsbeheer om het bestaande beleid te maken of te bewerken en klik vervolgens op het vak Regel toevoegen.

Bronzone: Buiten

Bestemmingszone: binnen

Bronnetwerk: willekeurig

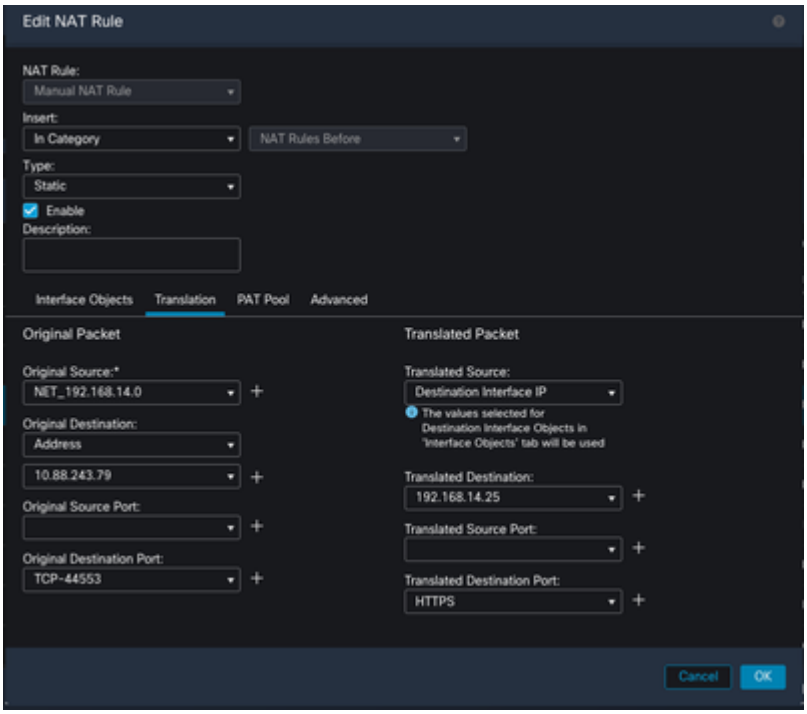
Netwerk van bestemming: 10.88.243.79

Stap 2. Inside-Inside NAT (haarspeld) configureren

Als tweede stap moet een statische NAT worden geconfigureerd van Inside naar Inside; in dit voorbeeld worden de IP-bestemmingspoort en de bestemmingspoort vertaald met behulp van een object met het IP van de externe interface en de bestemmingspoort is 44553.

Navigeer vanuit de FMC naar Apparaat > NAT om het bestaande beleid te bewerken en klik vervolgens op het vak Regel toevoegen.

- NAT-regel: handmatige NAT-regel
- Oorspronkelijke bron: 192.168.14.0/24
- Oorspronkelijke bestemming: Adres 10.88.243.79
- Oorspronkelijke bestemmingshaven: 44553
- Vertaalde bron: Bestemmingsinterface IP
- Vertaalde bestemming: 192.168.14.25
- Vertaalde bestemmingshaven: 443



Configureer het beleid. Navigeer naar Beleid > Toegangsbeheer om het bestaande beleid te bewerken en klik vervolgens op het vak Regel toevoegen.

Bronzone: Alle

Bestemmingszone: Alle

Bron: Netwerk: 192.168.14.0/24

Netwerk van bestemming: 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

Verifiëren

Vanuit de lokale client voert u een telnet uit met IP-bestemmingspoort en bestemmingspoort:

Als deze foutmelding "telnet kan geen verbinding maken met externe host: time-out verbinding" wordt weergegeven, is er op een gegeven moment tijdens de configuratie iets misgegaan.

```
┌──(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
```

Maar als er staat dat de verbinding tot stand is gebracht, is de configuratie gelukt.

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

Problemen oplossen

Als u problemen ondervindt met Network Address Translation (NAT), gebruikt u deze stapsgewijze handleiding om veelvoorkomende problemen op te lossen en op te lossen.

Stap 1: Configuratiecontrole van NAT-regels

- NAT-regels controleren: zorg ervoor dat alle NAT-regels correct zijn geconfigureerd in FMC. Controleer of de IP-adressen van de bron en de bestemming, evenals de poorten, nauwkeurig zijn.
- Toewijzing van interface: Bevestig dat zowel de bron- als de doelinterfaces correct zijn toegewezen in de NAT-regel. Onjuiste toewijzing kan ertoe leiden dat het verkeer niet correct wordt vertaald of gerouteerd.
- NAT Regel Prioriteit: Controleer of de NAT-regel bovenaan een andere regel staat die

hetzelfde verkeer kan evenaren. Regels in FMC worden in opeenvolgende volgorde verwerkt, dus een regel die hoger is geplaatst, heeft voorrang.

Stap 2: Verificatie van toegangscontroleregels (ACL)

- Controleer ACL's: Controleer de toegangscontrolelijsten om ervoor te zorgen dat ze geschikt zijn voor het toestaan van NAT-verkeer. ACL's moeten worden geconfigureerd om de vertaalde IP-adressen te herkennen.
- Regels: Zorg ervoor dat de toegangscontrolelijst in de juiste volgorde staat. Net als NAT-regels worden ACL's van boven naar beneden verwerkt en de eerste regel die overeenkomt met het verkeer is degene die wordt toegepast.
- Verkeersrechten: Controleer of er een geschikte toegangscontrolelijst bestaat om verkeer van het interne netwerk naar de vertaalde bestemming toe te staan. Als een regel ontbreekt of verkeerd is geconfigureerd, kan het gewenste verkeer worden geblokkeerd.

Stap 3: Aanvullende diagnose

- Diagnostische hulpmiddelen gebruiken: gebruik de diagnostische hulpmiddelen die beschikbaar zijn in FMC om het verkeer dat door het apparaat gaat te bewaken en te debuggen. Dit omvat het bekijken van real-time logs en verbindingsgebeurtenissen.
- Verbindingen opnieuw starten: In sommige gevallen kunnen bestaande verbindingen wijzigingen in NAT-regels of ACL's niet herkennen totdat ze opnieuw zijn opgestart. Overweeg om bestaande verbindingen op te schonen om nieuwe regels af te dwingen.

Van LINA:

<#root>

firepower#

```
 clear xlate
```

- Vertaling verifiëren: Gebruik opdrachten zoals xlate tonen en nat weergeven op de opdrachtregel als u met FTD-apparaten werkt om te controleren of NAT-vertalingen worden uitgevoerd zoals verwacht.

Van LINA:

<#root>

firepower#

```
 show nat
```

<#root>

```
firepower#
 show xlate
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.