Hairpin op ASA instellen

Inhoud

Inleiding

Dit document beschrijft de stappen die nodig zijn om Hairpin op een Cisco adaptieve security applicatie (ASA) met succes te configureren

Voorwaarden

Vereisten

Cisco raadt u aan deze onderwerpen te kennen:

- NAT-configuratie op ASA
- ACL-configuratie op ASA

Gebruikte componenten

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

- Software voor Cisco adaptieve security applicatie, versie 9.18(4)22

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

Hairpin Network Address Translation (NAT), ook bekend als NAT-loopback of NAT-reflectie, is een techniek die wordt gebruikt bij netwerkrouting waarbij een apparaat op een privaat netwerk via een openbaar IP-adres toegang heeft tot een ander apparaat op hetzelfde privaat netwerk.

Dit wordt gebruikt wanneer een server achter een router wordt ontvangen, en u wilt apparaten op hetzelfde lokale netwerk als de server toelaten om toegang tot het te krijgen met behulp van het openbare IP-adres (het adres dat door de Internet Service Provider aan de router is toegewezen) net zoals een extern apparaat zou doen.

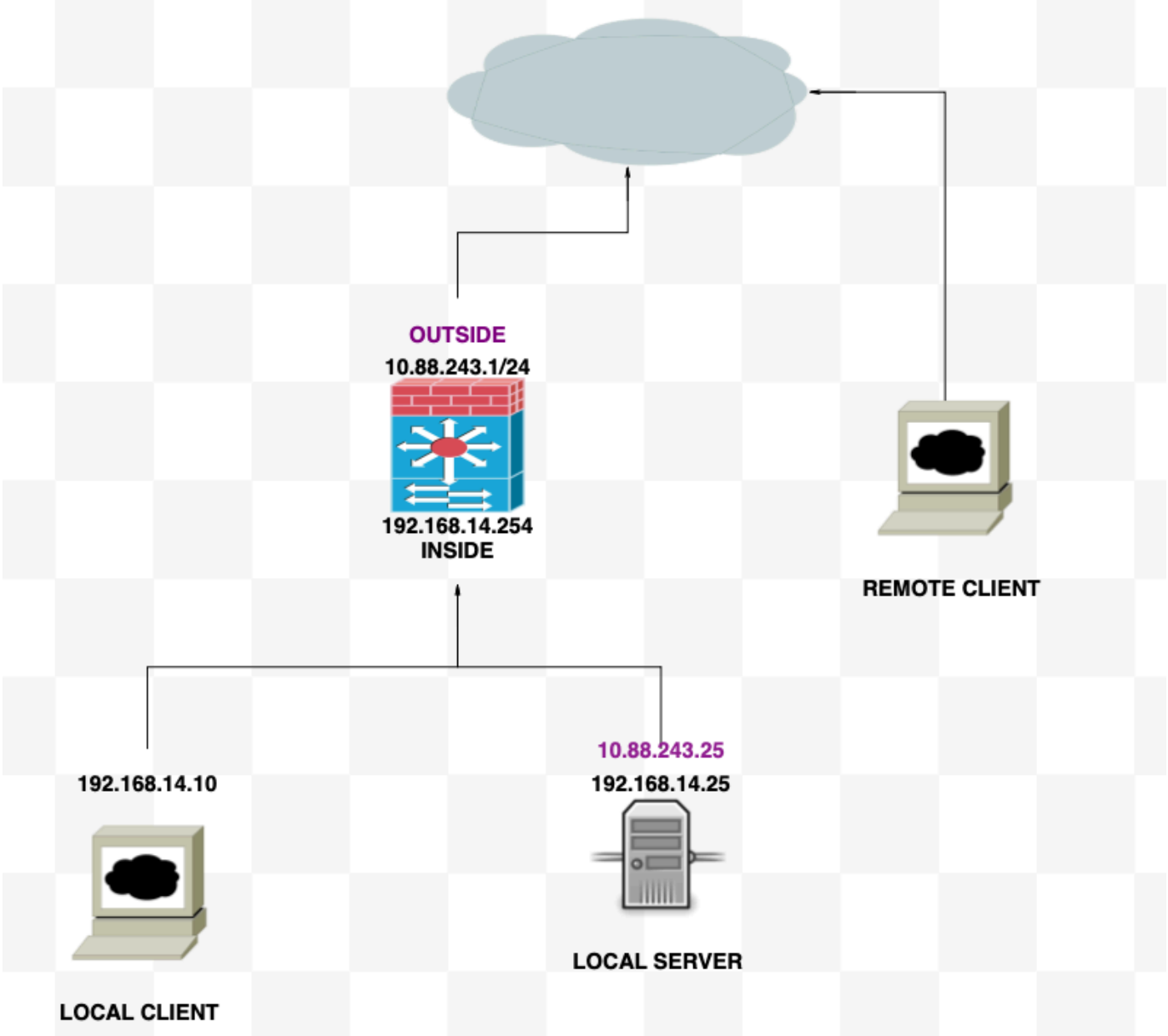
De term "hairpin" wordt gebruikt omdat het verkeer van de client naar de router (of firewall die NAT implementeert) gaat en vervolgens als een hairpin naar het interne netwerk wordt "teruggedraaid" na een vertaling om toegang te krijgen tot het privé IP-adres van de server.

U hebt bijvoorbeeld een webserver op uw lokale netwerk met een privé IP-adres. U wilt toegang krijgen tot deze server met behulp van zijn openbare IP-adres of een domeinnaam die zich ontleent aan het openbare IP-adres, zelfs wanneer u zich op hetzelfde lokale netwerk bevindt.

Zonder Hairpin NAT zou uw router dit verzoek niet begrijpen omdat het verwacht dat verzoeken voor het openbare IP-adres van buiten het netwerk komen.

Hairpin NAT lost dit probleem op door de router toe te staan om te erkennen dat, hoewel het verzoek wordt gedaan aan een openbaar IP, het moet worden gerouteerd aan een apparaat op het lokale netwerk.

Netwerkdiagram



Configuraties

Stap 1. De objecten maken

- Intern netwerk:192.168.14.10
- Webserver: 192.168.14.25
- Openbare webserver: 10.88.243.25
- Poort: 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
```

Stap 2. NAT maken

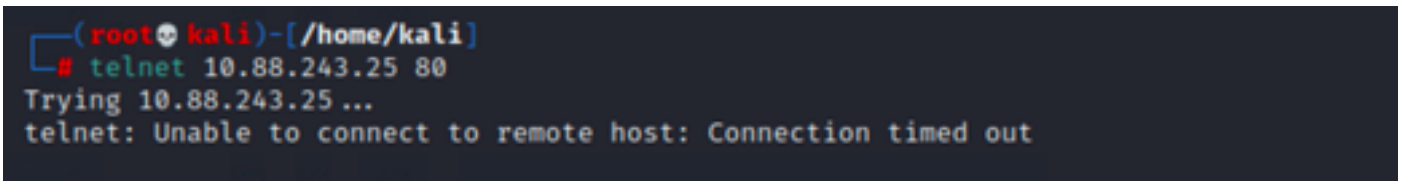
<#root>

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

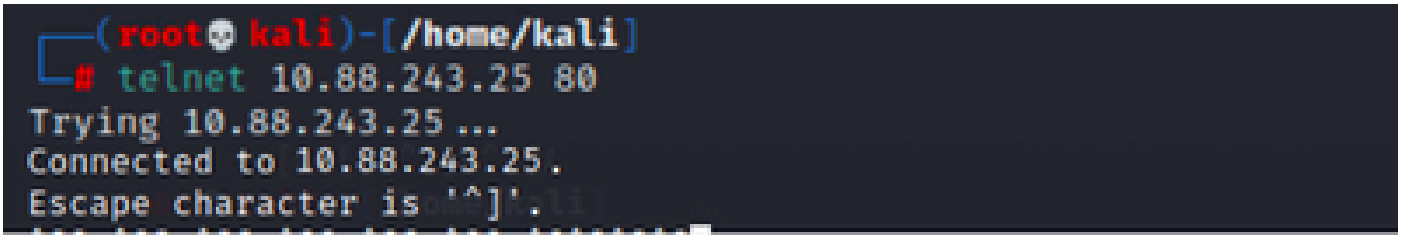
Verifiëren

Voer vanuit de lokale client een Telnet-bestemming IP uit met de bestemmingshaven:

Als dit bericht "Telnet kan geen verbinding maken met externe host: Verbindingstime-out" prompt, ging er op een bepaald moment tijdens de configuratie iets mis.



Maar als er 'Verbonden' op staat, werkt het!



Problemen oplossen

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

Stap 1: Configuratie NAT-regels controleren

- NAT-regels bekijken: zorg ervoor dat alle NAT-regels correct zijn geconfigureerd. Controleer of de IP-adressen van herkomst en bestemming, evenals de poorten, nauwkeurig zijn.
- Interfacetoewijzing: Bevestig dat zowel de bron- als doelinterfaces correct in de NAT-regel worden toegewezen. Onjuiste mapping kan ervoor zorgen dat verkeer niet wordt vertaald of op de juiste manier wordt gerouteerd.
- NAT-regelprioriteit: controleer of de NAT-regel een hogere prioriteit heeft dan alle andere regels die mogelijk overeenkomen met hetzelfde verkeer. Regels worden in een sequentiële volgorde verwerkt, dus een hogere regel heeft voorrang.

Stap 2: Verificatie van toegangscontroleregels (ACL)

- Review ACL's: controleer de toegangscontrolelijsten om te controleren of deze geschikt zijn voor het toestaan van NAT-verkeer. ACL's moeten worden geconfigureerd om de vertaalde IP-adressen te herkennen.
- Regels Volgorde: Zorg ervoor dat de toegangscontrolelijst in de juiste volgorde staat. Als NAT-regels worden ACL's van boven naar onder verwerkt en is de eerste regel die overeenkomt met het verkeer de regel die wordt toegepast.
- Traffic Permissions: Controleer dat er een geschikte toegangscontrolelijst bestaat om verkeer van het interne netwerk naar de vertaalde bestemming toe te staan. Als een regel ontbreekt of niet juist is geconfigureerd, kan het gewenste verkeer worden geblokkeerd.

Stap 3: Aanvullende diagnostiek

- Gebruik diagnostische tools: gebruik de diagnostische tools die beschikbaar zijn om het verkeer te bewaken en te debuggen dat door het apparaat loopt. Dit omvat het bekijken van real-time logboeken en verbindingsgebeurtenissen.
- Aansluitingen opnieuw starten: in sommige gevallen herkennen bestaande verbindingen wijzigingen in NAT-regels of ACL's niet totdat deze opnieuw zijn gestart. Overweeg om bestaande verbindingen te verwijderen om nieuwe regels te dwingen om toe te passen.

<#root>

```
ciscoasa(config)#
```

```
 clear xlate
```

- Verifieer de vertaling: Gebruik opdrachten zoals 'show xlate' en 'toon nat' op de

opdrachtregel als u met ASA-apparaten werkt om te verifiëren dat NAT-vertalingen worden uitgevoerd zoals verwacht.

<#root>

ciscoasa(config)#

show xlate

<#root>

ciscoasa(config)#

show nat

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.