Probleemoplossing voor ASA-netwerkadresomzetting (NAT)

Inhoud

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen bij de configuratie van Network Address Translation (NAT) op het platform Cisco adaptieve security applicatie (ASA).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

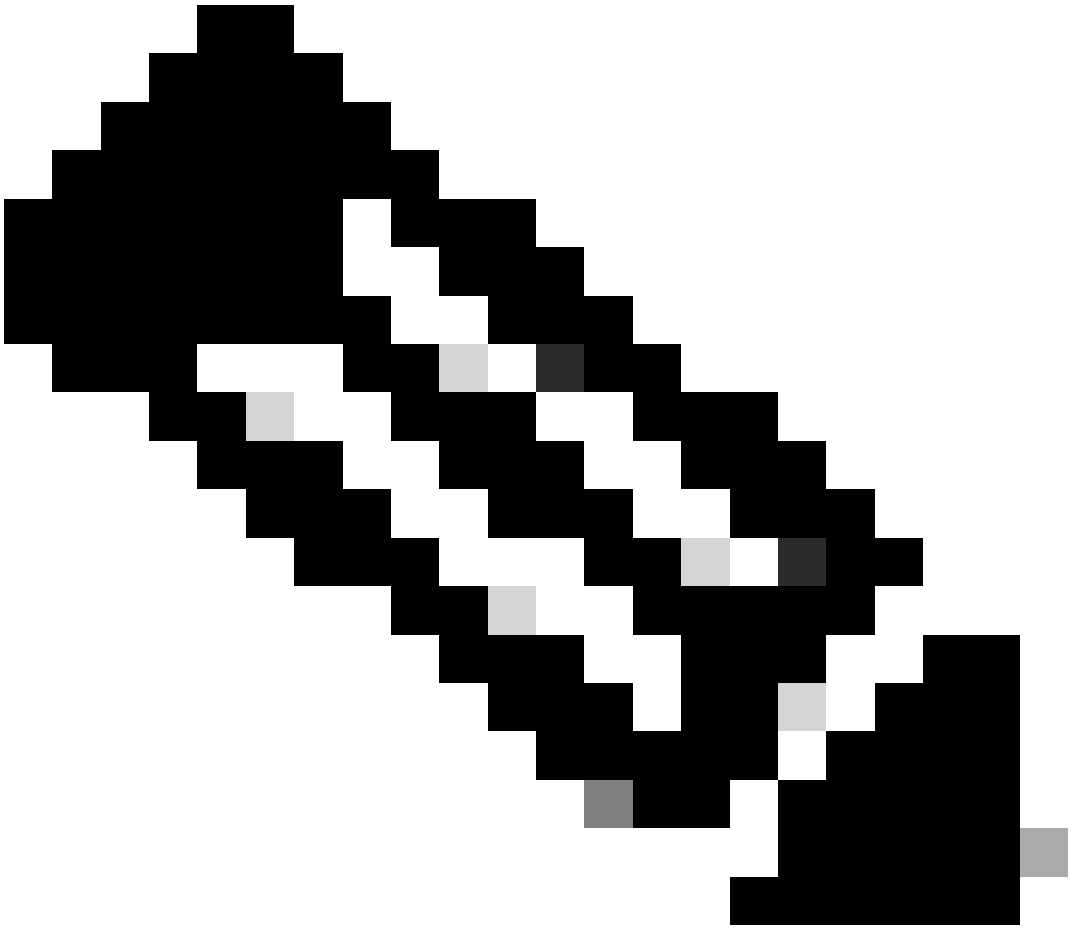
Gebruikte componenten

De informatie in dit document is gebaseerd op ASA versie 8.3 en hoger.

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.

NAT-configuratie voor probleemoplossing op de ASA



> Opmerking: voor een aantal basisvoorbeelden van NAT-configuraties, waaronder een video die een NAT-basisconfiguratie weergeeft, raadpleegt u de sectie Verwante informatie onder in dit document.

Wanneer u NAT-configuraties probleemoplossing biedt, is het belangrijk te begrijpen hoe de NAT-configuratie op de ASA wordt gebruikt om de NAT-beleidstabel te bouwen.

Deze configuratiefouten verklaren de meerderheid van de NAT problemen die door ASA beheerders worden ontmoet:

- De NAT-configuratieregels zijn defect. Bijvoorbeeld, wordt een handNAT regel geplaatst bovenop de NAT lijst, die veroorzaakt dat specifiekere die regels verder beneden de NAT lijst worden geplaatst nooit worden geraakt.

- De netwerkobjecten die in de NAT-configuratie worden gebruikt, zijn te breed, waardoor het verkeer onbedoeld aan deze NAT-regels wordt aangepast en specifiekere NAT-regels mist.

Het hulpprogramma voor pakkettracers kan worden gebruikt om de meeste NAT-gerelateerde problemen op de ASA te diagnosticeren. Zie de volgende sectie voor meer informatie over hoe de NAT configuratie wordt gebruikt om de NAT beleidstabel te bouwen, en hoe u specifieke NAT-problemen kunt oplossen en oplossen.

Bovendien, kan het show nat detailbevel worden gebruikt om te begrijpen welke NAT regels door nieuwe verbindingen worden geraakt.

Hoe de ASA Configuration wordt gebruikt om de NAT Policy Table te bouwen

Alle pakketten die door ASA worden verwerkt worden beoordeeld aan de hand van de NAT-tabel. Deze evaluatie begint bovenaan (Sectie 1) en werkt neer tot een NAT regel wordt aangepast.

In het algemeen, zodra een NAT regel wordt aangepast, dat NAT regel wordt toegepast op de verbinding en geen NAT beleid meer wordt gecontroleerd tegen het pakket maar er zijn sommige voorbehouden die daarna worden verklaard.

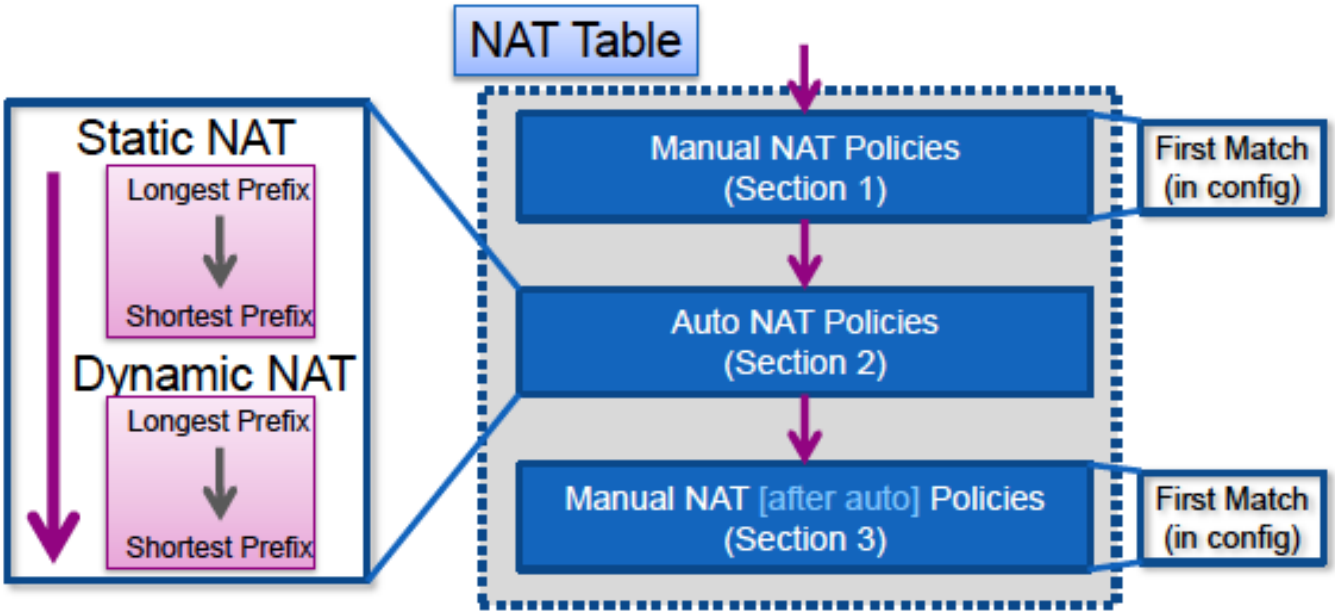
De NAT-beleidstabel

Het NAT-beleid op de ASA is gebaseerd op de NAT-configuratie.

De drie secties van de ASA NAT-tabel zijn:

Afdeling 1	Handmatig NAT-beleid Deze worden verwerkt in de volgorde waarin ze in de configuratie verschijnen.
Afdeling 2	Auto NAT-beleid Deze worden verwerkt op basis van het NAT-type (statisch of dynamisch) en de prefixlengte (subnetmasker) in het object.
Afdeling 3	Na-auto handmatig NAT-beleid Deze worden verwerkt in de volgorde waarin ze in de configuratie verschijnen.

Dit diagram toont de verschillende NAT-secties en hoe deze zijn geordend:



NAT-regelovereenkomst

Afdeling 1

- Een stroom wordt eerst beoordeeld tegen sectie 1 van de NAT-tabel die begint met de eerste regel.
  - Als de bron en bestemming IP van het pakket overeenkomen met de parameters van de handmatige NAT-regel wordt de vertaling toegepast en stopt het proces en worden geen verdere NAT-regels in een sectie geëvalueerd.
  - Als er geen NAT-regel is, wordt de stroom beoordeeld aan de hand van deel 2 van de NAT-tabel.

Afdeling 2

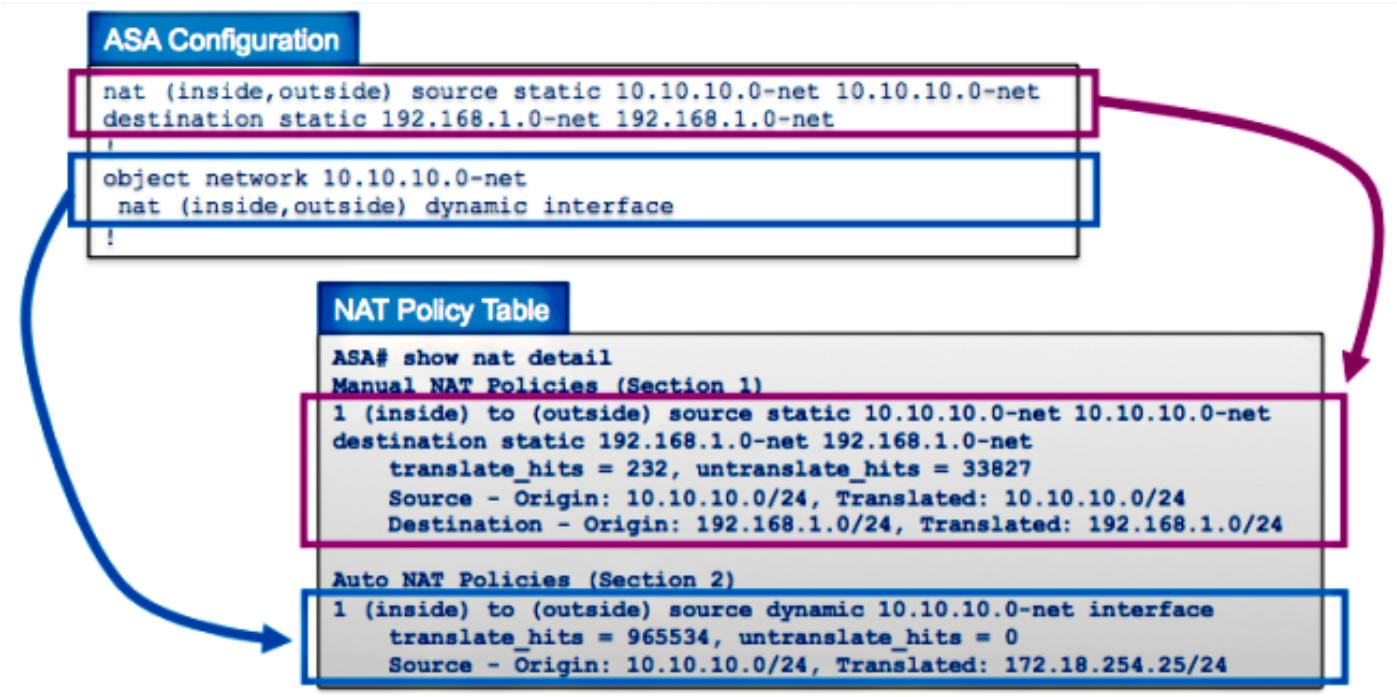
- Een stroom wordt beoordeeld aan de hand van sectie 2 NAT-regels in de eerder gespecificeerde volgorde, eerst de statische NAT-regels en vervolgens de dynamische NAT-regels.
  - Als een vertaalregel of de bron of de bestemming IP van de stroom aanpast, kan de vertaling worden toegepast en de rest van de regels kan blijven worden geëvalueerd om te zien of zij andere IP in de stroom aanpassen. Bijvoorbeeld, kon één auto-NAT regel de bron IP vertalen en een andere auto-NAT regel kon de bestemming vertalen.
  - Als de stroom een auto-NAT regel aanpast, wanneer het eind van sectie 2 wordt bereikt de NAT lookup einden, en de regels in sectie 3 worden niet geëvalueerd.
  - Als er geen NAT-regel uit sectie 2 wordt gekoppeld aan de stroom, gaat de raadpleging verder naar sectie 3

Afdeling 3

- De procedure in punt 3 is in wezen dezelfde als in punt 1. Als de bron en bestemming IP van het pakket overeenkomen met de parameters van de handmatige NAT-regel wordt de vertaling toegepast en stopt het proces en worden geen verdere NAT-regels in een sectie

geëvalueerd.

Dit voorbeeld laat zien hoe de ASA NAT-configuratie met twee regels (één handmatige NAT-verklaring en één Auto NAT-configuratie) in de NAT-tabel worden weergegeven:



Hoe NAT-problemen op te lossen

Gebruik het hulpprogramma Packet Tracer

Om problemen met NAT configuraties problemen op te lossen, gebruikt u het hulpprogramma voor pakkettracer om te verifiëren dat een pakket het NAT-beleid raakt. Met Packet tracer kunt u een voorbeeldpakket opgeven dat in de ASA wordt ingevoerd, en de ASA geeft aan welke configuratie van toepassing is op het pakket en of deze al dan niet is toegestaan.

In het volgende voorbeeld wordt een voorbeeld van een TCP-pakket gegeven dat de binnenkant van de interface ingaat en bestemd is voor een host op het internet. Het pakkettracerhulpprogramma toont dat het pakket voldoet aan een dynamische NAT-regel en wordt vertaald naar het externe IP-adres van 172.16.123.4:

<#root>

ASA#

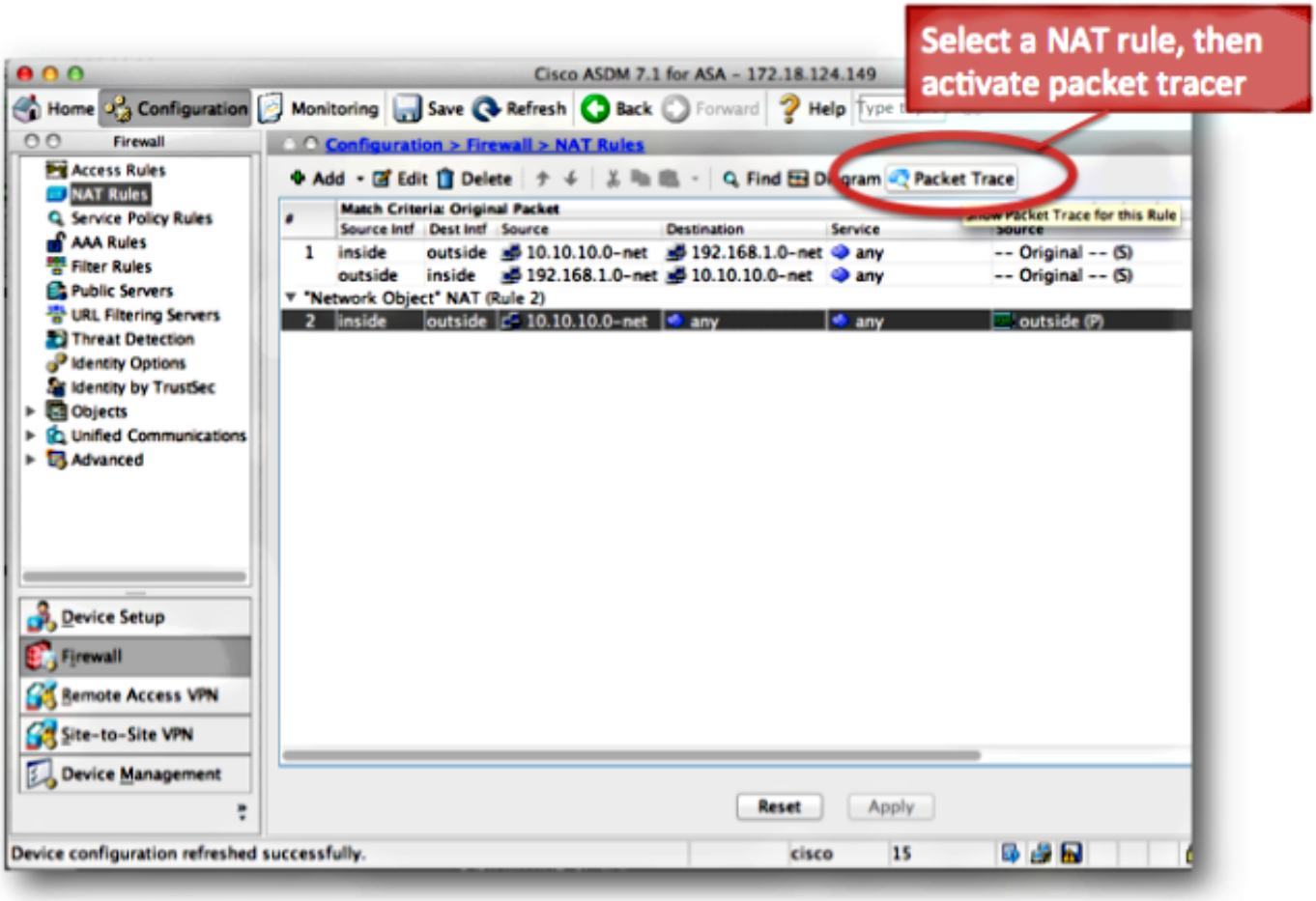
packet-tracer input inside tcp 10.10.10.123 12345 192.168.200.123 80

...(output omitted)...

Phase: 2
Type: NAT
Subtype:

```
Result: ALLOW
Config:

object network 10.10.10.0-net
 nat (inside,outside) dynamic interface


Additional Information:
Dynamic translate 10.10.10.123/12345 to 172.16.123.4/12345

...(output omitted)...

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up

Action: allow



ASA#
```

Kies de NAT-regel en klik op Packet Trace om de pakkettracer te activeren vanuit Cisco Adaptive Security Device Manager (ASDM). Dit gebruikt de IP-adressen die in de NAT-regel zijn gespecificeerd als de ingangen voor het pakkettracergereedschap:

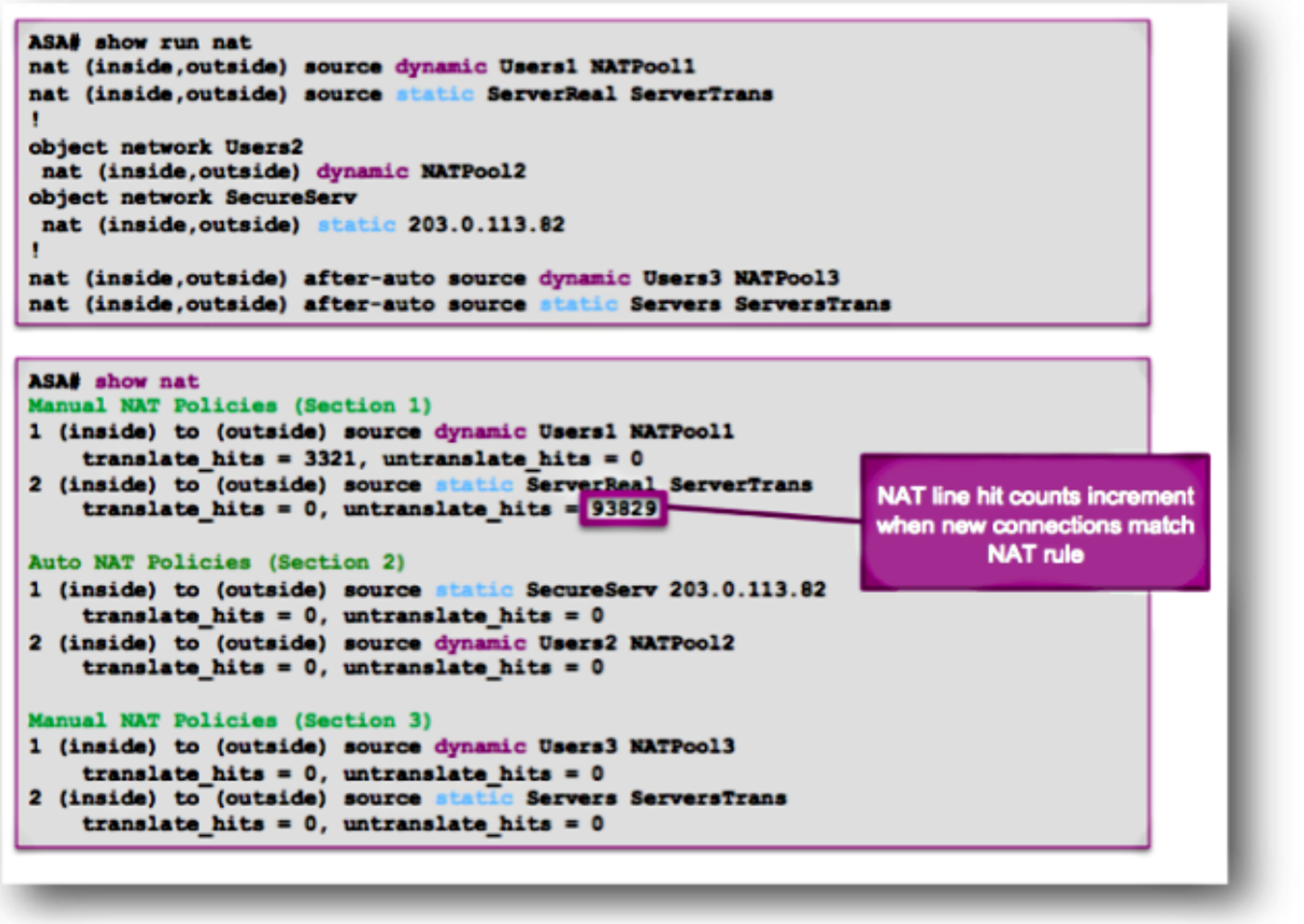


Bekijk de output van de Show Nat Command

De output van de show nationaal detailbevel kan worden gebruikt om de NAT beleidslijst te bekijken. Met name de tellers translate_hits en untranslate_hits kunnen gebruikt worden om te bepalen welke NAT-waarden gebruikt worden op de ASA.

Als u ziet dat uw nieuwe NAT-regel geen translate_hits of untranslate_hits heeft, betekent dit dat het verkeer niet bij de ASA aankomt, of dat een andere regel met een hogere prioriteit in de NAT-tabel overeenkomt met het verkeer.

Hier is de NAT-configuratie en de NAT-beleidstabel vanuit een andere ASA-configuratie:



In het vorige voorbeeld zijn er zes NAT-regels geconfigureerd op deze ASA. De show nat output toont hoe deze regels worden gebruikt om de NAT beleidstabel te bouwen, evenals het aantal translate_hits en untranslate_hits voor elke regel.

Deze hit tellers worden slechts één keer per verbinding verhoogd. Nadat de verbinding via de ASA is opgebouwd, verhogen latere pakketten die overeenkomen met de huidige verbinding de NAT-lijnen niet (net als de manier waarop toegangslijsten indrukken op de ASA werken).

Translate_hits: Het aantal nieuwe verbindingen die overeenkomen met de NAT-regel in de voorwaartse richting.

"Voorwaartse richting" betekent dat de verbinding door de ASA werd gebouwd in de richting van de interfaces die in de NAT-regel zijn gespecificeerd.

Als een NAT-regel aangeeft dat de interne server vertaald is naar de buiteninterface, is de volgorde van de interfaces in de NAT-regel "nat (binnen, buiten)..."; als die server een nieuwe verbinding met een host aan de buitenkant start, wordt de teller translate_hit verhoogd.

Untranslate_hits: Het aantal nieuwe verbindingen die overeenkomen met de NAT-regel in de omgekeerde richting.

Als een NAT-regel aangeeft dat de interne server is vertaald naar de buiteninterface, is de volgorde van de interfaces in de NAT-regel "nat (binnenkant, buitenkant)..."; als een client buiten

de ASA een nieuwe verbinding met de server binnenin initieert, wordt de teller untranslate_hit verhoogd.

Opnieuw, als u ziet dat uw nieuwe NAT regel geen translate_hits of untranslate_hits heeft, betekent dat dat of het verkeer niet bij ASA aankomt, of misschien een andere regel die een hogere prioriteit in de NAT tabel heeft het verkeer aanpast.

NAT-methode voor probleemoplossing

Gebruik pakkettracer om te bevestigen dat een voorbeeldpakket voldoet aan de juiste NAT-configuratieregel op de ASA. Gebruik de opdracht show nat detail om te begrijpen welke NAT-beleidsregels zijn getroffen. Als een verbinding een andere NAT-configuratie aanpast dan verwacht, kunt u met deze vragen problemen oplossen:

- Is er een andere NAT-regel die voorrang krijgt op de NAT-regel die u hebt bedoeld om het verkeer te laten toeslaan?
- Is er een andere NAT-regel met objectdefinities die te breed zijn (het subnetmasker is te kort, zoals 255.0.0.0) waardoor dit verkeer overeenkomt met de verkeerde regel?
- Is het handmatige NAT-beleid buiten bedrijf, waardoor het pakket aan de verkeerde regel voldoet?
- Is uw NAT-regel niet correct geconfigureerd, waardoor de regel niet overeenkomt met uw verkeer?

Zie de volgende sectie voor steekproefproblemen en oplossingen.

Gemeenschappelijke problemen met NAT-configuraties

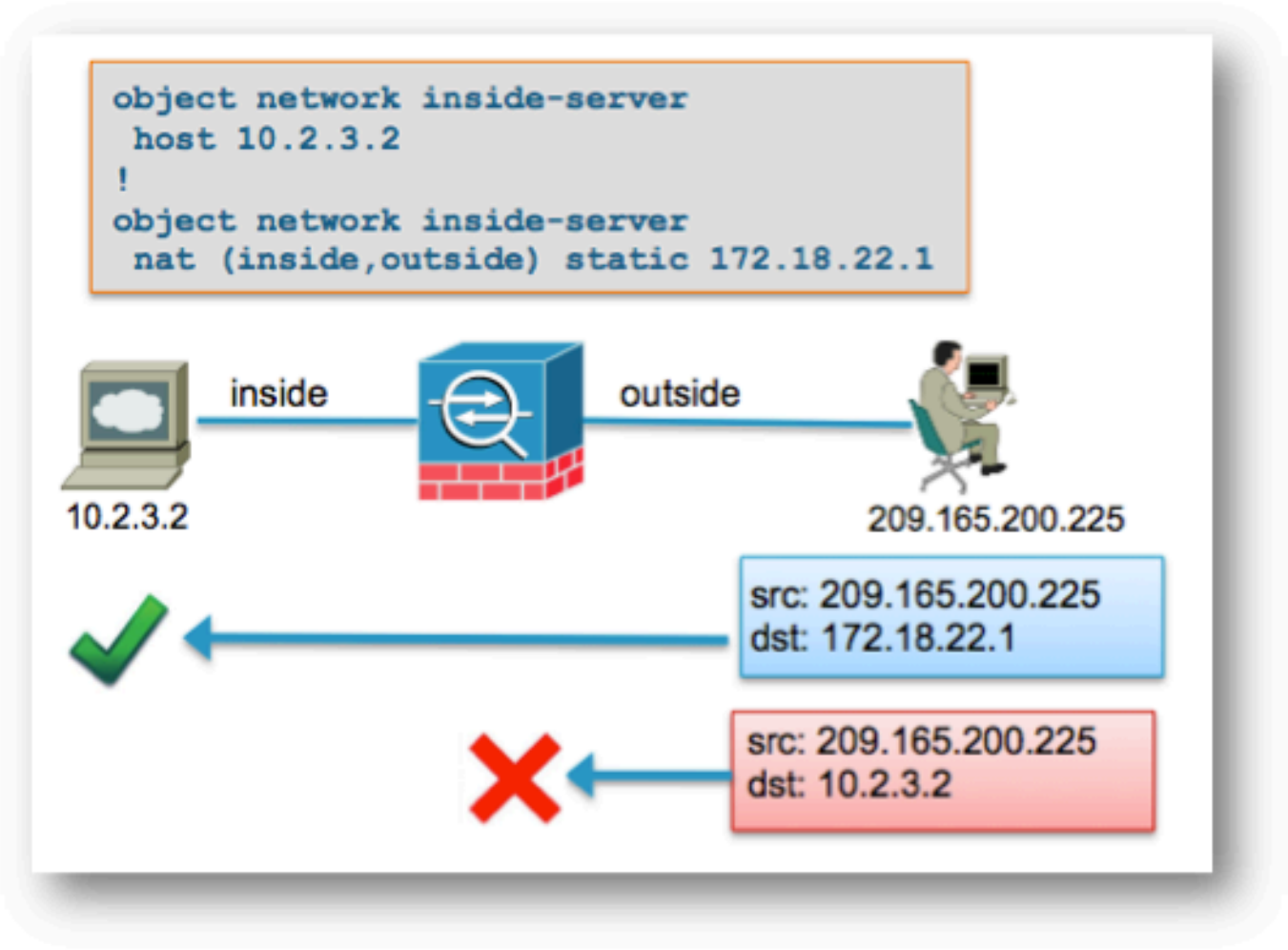
Hier zijn enkele veel voorkomende problemen die optreden wanneer u NAT op de ASA configureert.

Probleem: verkeer mislukt vanwege NAT-fout (RPF) bij omgekeerd pad: asymmetrische NAT-regels afgestemd op voorwaartse en omgekeerde stromen

De NAT RPF-controle zorgt ervoor dat een verbinding die door de ASA in de voorwaartse richting wordt vertaald, zoals TCP synchroniseren (SYN), wordt vertaald door dezelfde NAT-regel in de omgekeerde richting, zoals TCP SYN/acknowledged (ACK).

Meestal wordt dit probleem veroorzaakt door inkomende verbindingen die bestemd zijn voor het lokale (niet-vertaalde) adres in een NAT-verklaring. Op basisniveau controleert de NAT RPF dat de omgekeerde verbinding van de server naar de client overeenkomt met dezelfde NAT-regel; als dat niet het geval is, mislukt de NAT RPF-controle.

Voorbeeld: 209.165.200.225



Wanneer de externe host op 192.168.200.225 een pakket rechtstreeks naar het lokale (niet-vertaalde) IP-adres van 10.2.3.2 verstuurt, laat de ASA het pakket vallen en registreert deze syslog:

```
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows;
Connection for icmp src outside:192.168.200.225 dst inside:10.2.3.2 (type 8, code 0)
denied due to NAT reverse path failure
```

Oplossing:

Zorg er eerst voor dat de host gegevens naar het juiste wereldwijde NAT-adres stuurt. Als de host pakketten verstuurt die bestemd zijn voor het juiste adres, controleer dan de NAT-regels die door de verbinding worden geraakt.

Controleer dat de NAT-regels correct zijn gedefinieerd en dat de objecten waarnaar in de NAT-regels wordt verwezen, juist zijn. Controleer ook of de volgorde van de NAT-regels juist is.

Gebruik het pakkettracerhulpprogramma om de details van het geweigerde pakket te specificeren. De pakkettracer moet het gedropte pakket tonen vanwege de fout bij de RPF-controle.

Daarna, bekijk de output van pakkettracer om te zien welke NAT regels in de NAT fase en de fase NAT-RPF worden geraakt.

Als een pakket een NAT-regel aanpast in de NAT RPF-controlefase, die aangeeft dat de omgekeerde stroom een NAT-vertaling zou raken, maar niet overeenkomt met een regel in de NAT-fase, die aangeeft dat de voorwaartse stroom GEEN NAT-regel raakt, wordt het pakket gedropt.

Deze output komt overeen met het scenario dat in het vorige diagram wordt getoond, waar de buitenhost onjuist verkeer naar het lokale IP-adres van de server verzendt en niet naar het globale (vertaalde) IP-adres:

```
<#root>

ASA#

packet-tracer input outside tcp 192.168.200.225 1234 10.2.3.2 80



    .....

Phase: 8
Type: NAT
Subtype: rpf-check
Result:

DROP


Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
...
ASA(config)#
```

Wanneer het pakket is bestemd voor het juiste toegewezen IP-adres van 172.18.22.1, komt het pakket overeen met de juiste NAT-regel in de UN-NAT-fase in de voorwaartse richting en dezelfde regel in de NAT RPF-controlefase:

```
<#root>

ASA(config)#

packet-tracer input outside tcp 192.168.200.225 1234 172.18.22.1 80


...
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network inside-server
```

```
 nat (inside,outside) static 172.18.22.1
Additional Information:
NAT divert to egress interface inside
Untranslate 172.18.22.1/80 to 10.2.3.2/80
...
Phase: 8
Type: NAT
Subtype: rpf-check
Result:
```

ALLOW

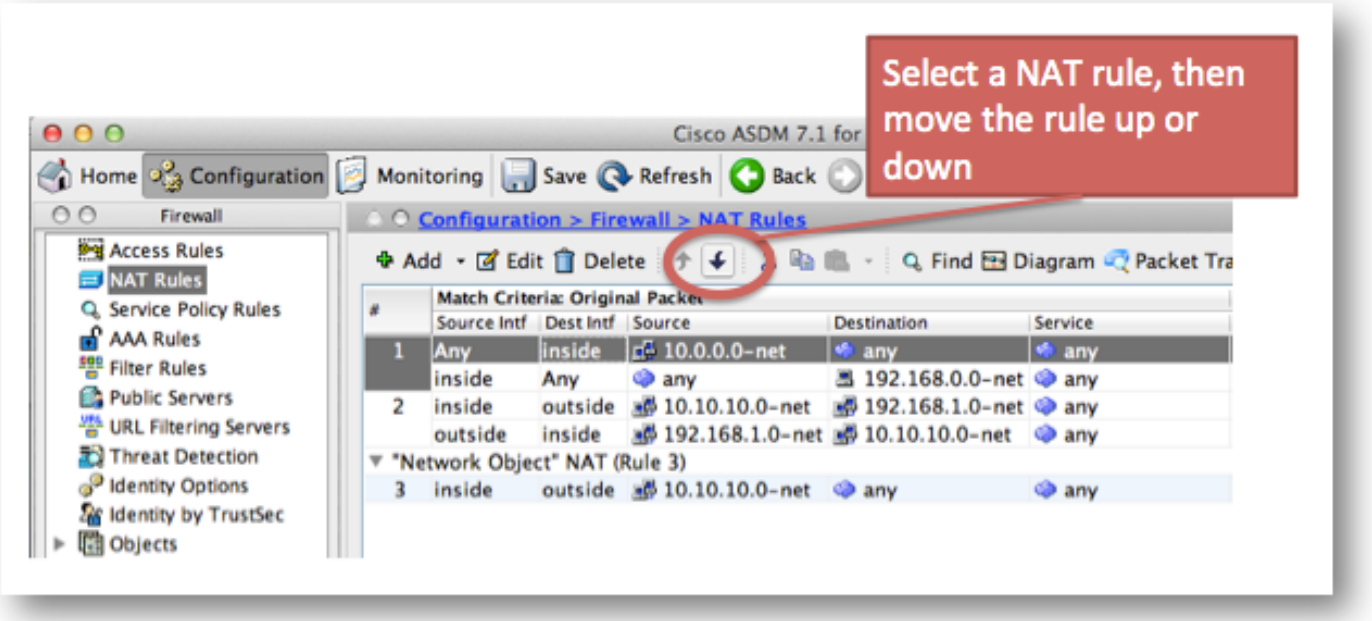
```
Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
...

ASA(config)#
```

Probleem: Handmatige NAT-regels zijn buiten bedrijf, waardoor onjuiste pakketovereenkomsten worden veroorzaakt

De handmatige NAT-regels worden verwerkt op basis van hun verschijning in de configuratie. Als een zeer brede NAT regel eerst in de configuratie wordt vermeld, kan het een andere, specifiekere regel verder beneden in de NAT lijst met voeten treden. Gebruik pakkettracer om te verifiëren welke NAT-regel uw verkeer raakt; het kan nodig zijn om de handmatige NAT-vermeldingen in een andere volgorde te rangschikken.

Oplossing:

Herstelt NAT-regels met ASDM.



Oplossing:

NAT-regels kunnen opnieuw worden geordend met de CLI als u de regel verwijdert en opnieuw invoert bij een specifiek regelnummer. Als u een nieuwe regel op een specifieke regel wilt invoegen, voert u het regelnummer in nadat de interfaces zijn gespecificeerd.

Voorbeeld:

```
<#root>

ASA(config)#

nat (inside,outside) 1 source static 10.10.10.0-net
10.10.10.0-net destination static 192.168.1.0-net 192.168.1.0-net
```

Probleem

Een NAT-regel is te breed en komt onbedoeld met wat verkeer overeen. Soms worden NAT-regels gemaakt die gebruik maken van objecten die te breed zijn. Als deze regels dichtbij de bovenkant van de NAT-tabel worden geplaatst (bij de bovenkant van sectie 1, bijvoorbeeld), kunnen ze meer verkeer aan dan bedoeld en zorgen dat NAT-regels verderop in de tabel nooit worden geraakt.

Oplossing

Gebruik pakkettracer om te bepalen of uw verkeer een regel aanpast met objectdefinities die te breed zijn. Als dit het geval is, moet u de omvang van die objecten beperken, of de regels verder naar beneden in de NAT-tabel verplaatsen, of naar de sectie na de auto (Sectie 3) van de NAT-tabel.

Probleem

Een NAT-regel leidt verkeer naar een onjuiste interface af. NAT-regels kunnen voorrang krijgen op de routeringstabel wanneer zij bepalen welke interface een pakket aan de ASA koppelt. Als een inkomend pakket een vertaald IP adres in een NAT verklaring aanpast, wordt de NAT regel gebruikt om de uitgangsinterface te bepalen.

De NAT divert check (dat is wat de routeringstabel kan overschrijven) controleert om te zien of er een NAT-regel is die doeladresomzetting specificeert voor een inkomend pakket dat op een interface aankomt.

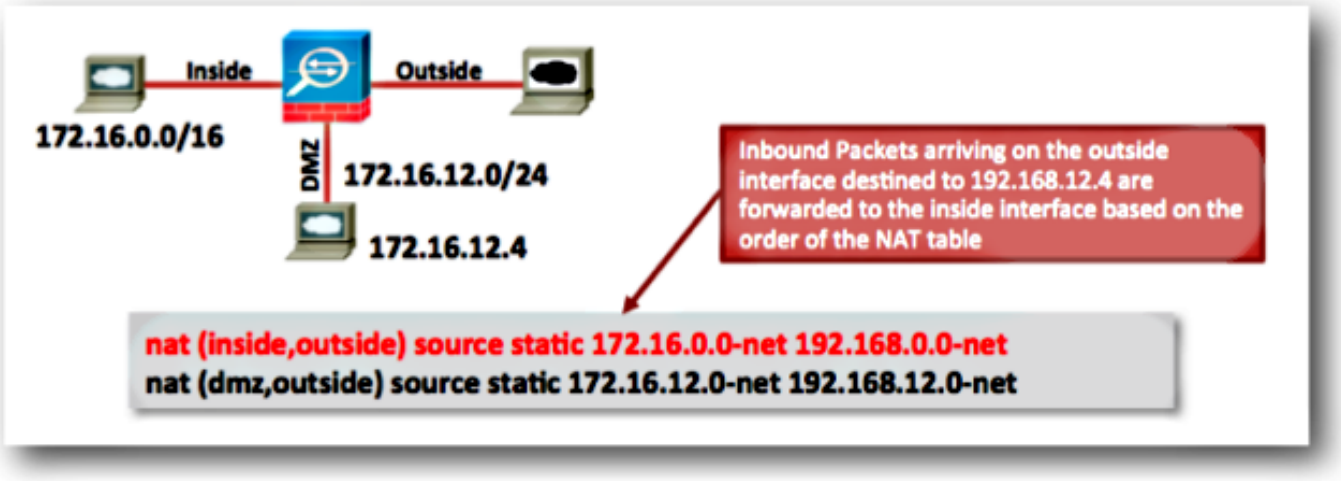
Als er geen regel is die expliciet specificeert hoe dat IP-adres van de pakketbestemming moet worden vertaald, wordt de globale routeringstabel geraadpleegd om de uitgangsinterface te bepalen.

Als er een regel is die expliciet specificeert hoe u het IP-adres van de pakketbestemming vertaalt, dan haalt de NAT-regel het pakket naar de andere interface in de vertaling en wordt de globale

routeringstabel effectief omzeild.

Dit probleem wordt het meest gezien voor inkomend verkeer, dat op de buiteninterface aankomt, en is gewoonlijk toe te schrijven aan out-of-order NAT-regels die verkeer naar onbedoelde interfaces afleiden.

Voorbeeld:



Oplossingen:

Dit probleem kan worden opgelost met een van de volgende maatregelen:

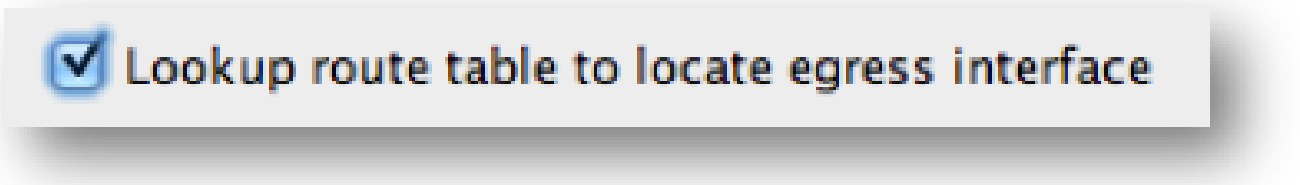
- Geef de NAT-tabel een nieuwe volgorde, zodat eerst de specifiekere vermelding wordt vermeld.
- Gebruik niet-overlappende wereldwijde IP-adresbereiken voor de NAT-verklaringen.

Merk op dat als de NAT-regel een identiteitsregel is (wat betekent dat de IP-adressen niet door de regel worden gewijzigd), het trefwoord route-lookup kan worden gebruikt (dit trefwoord is niet van toepassing op het vorige voorbeeld omdat de NAT-regel geen identiteitsregel is).

Het route-lookup sleutelwoord veroorzaakt ASA om een extra controle uit te voeren wanneer het een NAT regel aanpast. Het controleert dat de routeringstabel van ASA het pakket door:sturen aan de zelfde uitgangsinterface waaraan deze NAT configuratie het pakket afleidt.

Als de Routing Table Out-interface niet overeenkomt met de NAT-afleidingsinterface, wordt de NAT-regel niet aangepast (de regel wordt overgeslagen) en gaat het pakket door langs de NAT-tabel die moet worden verwerkt door een latere NAT-regel.

De optie voor het opzoeken van routes is alleen beschikbaar als de NAT-regel een identiteits-NAT-regel is, wat betekent dat de IP-adressen door de regel niet worden gewijzigd. De optie route-lookup kan per NAT regel worden ingeschakeld als u route-lookup toevoegt aan het einde van de NAT-lijn, of als u de lijst van de Lookup-route controleert om het vakje van de uitgangsinterface te vinden in de NAT-regelconfiguratie in ASDM:



Probleem: een NAT-regel veroorzaakt dat de ASA Proxy Address Resolution Protocol (ARP) gebruikt voor verkeer op de toegewezen interface

ASA Proxy-ARP's voor het wereldwijde IP-adresbereik in een NAT-verklaring op de wereldwijde interface. Deze Proxy ARP functionaliteit kan worden uitgeschakeld op een per-NAT regelbasis als u het no-proxy-arp sleutelwoord aan de NAT verklaring toevoegt.

Dit probleem wordt ook gezien wanneer globale adressubnette onbedoeld om wordt gemaakt om veel groter te zijn dan het bedoeld was te zijn.

Oplossing

Voeg indien mogelijk het no-proxy-arp-sleutelwoord toe aan de NAT-regel.

Voorbeeld:

<#root>

```
ASA(config)#
object network inside-server

ASA(config-network-object)#
nat (inside,outside) static 172.18.22.1 no-proxy-arp

ASA(config-network-object)#
end

ASA#
  ASA#
 show run nat

object network inside-server
 nat (inside,outside) static 172.18.22.1
no-proxy-arp

ASA#
```

Dit kan ook met ASDM worden bereikt. Controleer binnen de NAT-regel het aanvinkvakje Proxy ARP uitschakelen op uitgang interface.

.

Gerelateerde informatie

- VIDEO: ASA poort doorsturen voor DMZ server toegang (versies 8.3 en 8.4)
- Basis ASA NAT-configuratie: webserver in de DMZ in ASA versie 8.3 en hoger
- Boek 2: Configuratiehandleiding voor Cisco ASA Series firewall-CLI, 9.1
- Cisco Technical Support en downloads

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.