ASA 8.4(4): Configuratie van bepaalde identiteit NAT geweigerd

Inhoud

Inleiding

Adaptieve security applicaties (ASA's) die 8.4(4) of hoger uitvoeren, kunnen bepaalde NAT-configuraties afwijzen en een foutmelding weergeven zoals deze:

```
ERROR: <mapped address range> overlaps with <interface> standby interface
   address
ERROR: NAT Policy is not downloaded
```

Dit probleem kan ook verschijnen wanneer u uw ASA vanaf een vorige release verbetert naar 8.4(4) of hoger. U kunt opmerken dat sommige NAT opdrachten niet langer aanwezig zijn in de in werking stellen-configuratie van de ASA. In deze gevallen kunt u de afdrukken van de consoleborden bekijken om te zien of er berichten in de bovenstaande indeling aanwezig zijn.

Een ander effect dat u kunt opmerken is dat het verkeer voor bepaalde subnetten achter de ASA kan stoppen met het doorgeven door de VPN-tunnel(s) die eindigt op de ASA. In dit document wordt beschreven hoe deze problemen kunnen worden opgelost.

Voordat u begint

Vereisten

Aan deze voorwaarden moet worden voldaan om dit probleem op te lossen:

- ASA versie 8.4(4) of hoger, of bijgewerkt tot versie 8.4(4) of hoger vanaf een voorafgaande release.
- ASA geconfigureerd met een standby IP-adres op ten minste één van zijn interfaces.
- Een NAT is ingesteld met de bovenstaande interface als de in kaart gebrachte interface.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwareversie:

- ASA's met 8.4(4) of meer

Conventies

Raadpleeg voor meer informatie over documentconventies de technische Tips van Cisco.

Probleem

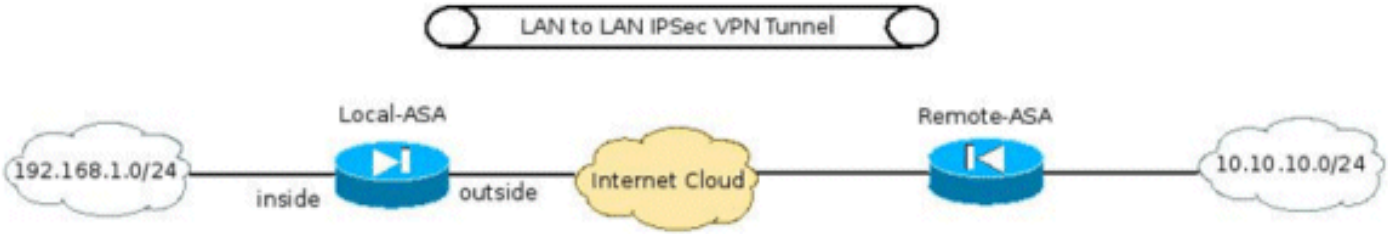
Zoals de foutmelding suggereert, als het in kaart gebrachte adresbereik in een statische NAT-verklaring het "standby" IP-adres bevat dat aan de toegewezen interface is toegewezen, wordt de NAT-opdracht verworpen. Dit gedrag is altijd al bestaand voor Statische poortomleiding, maar het is ook geïntroduceerd voor Statische één-op-één NAT-verklaringen evenals versie 8.4(4) als een oplossing voor Cisco bug ID CSCtw82147 (alleen geregistreerde klanten).

Dit bug is ingediend omdat de ASA gebruikers vóór 8.4(4) toestemming heeft gegeven om het toegewezen adres in een statische NAT-configuratie hetzelfde te zijn als het standby IP-adres dat aan de in kaart gebrachte interface is toegewezen. Kijk bijvoorbeeld naar dit configuratie van een ASA:

```
ciscoasa(config)# show run int e0/0
!
interface Ethernet0/0
 nameif vm
 security-level 0
 ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
ciscoasa(config)# show run nat
!
object network obj-10.76.76.160
 nat (tftp,vm) static 192.168.1.2
```

Ondanks dat de opdracht is geaccepteerd, werkt deze NAT-configuratie nooit volgens plan. Als resultaat hiervan laat de ASA, om te beginnen met 8.4(4), niet toe dat zo'n NAT-regel überhaupt wordt geconfigureerd.

Dit heeft geleid tot een ander onvoorzien probleem. Bedenk bijvoorbeeld het scenario waar de gebruiker een VPN-tunnel beëindigd op de ASA heeft en "binnen"-subnetwerk wil toestaan om met de externe VPN-browser te kunnen praten.



Onder andere opdrachten die vereist zijn voor het configureren van de VPN-tunnel is een van de belangrijkste configuraties om er zeker van te zijn dat het verkeer tussen de VPN-subnetten geen NATed krijgt. Dit wordt geïmplementeerd met 8.3 en hoger door gebruik te maken van een Handleiding/Twice NAT van dit formaat:

```
interface Ethernet0/0
 nameif inside
 security-level 0
 ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
!
object network obj-192.168.1.0
 description Inside subnet
 subnet 192.168.1.0 255.255.255.0
object network obj-10.10.10.0
 description Remote VPN subnet
 subnet 10.10.10.0 255.255.255.0
!
nat (inside,any) source static obj-192.168.1.0 obj-192.168.1.0 destination
   static obj-10.10.10.0 obj-10.10.10.0
!
object network obj-192.168.1.0
 nat (inside,outside) dynamic interface
```

Wanneer deze ASA is bijgewerkt naar 8.4(4) of hoger, zal deze NAT-opdracht niet aanwezig zijn in de actieve-configuratie van de ASA en zal deze fout op de ASA-console worden afgedrukt:

```
ERROR: 192.168.1.0-192.168.1.255 overlaps with inside standby interface
   address
ERROR: NAT Policy is not downloaded
```

Als resultaat hiervan zal het verkeer tussen subnetten 192.168.1.0/24 en 10.10.10.0/24 niet langer door de VPN-tunnel stromen.

Oplossing

Voor deze aandoening zijn twee mogelijke oorzaken:

- Maak de NAT-opdracht zo specifiek mogelijk voordat u deze opwaarteert naar 8.4(4), zodat de toegewezen interface niet "enig" is. Bijvoorbeeld, de bovenstaande NAT opdracht kan in de interface worden veranderd waardoor het afstandsbediening van VPN bereikbaar is (genoemd "buiten" in het bovenstaande scenario):
  ```
  nat (inside,outside) source static obj-192.168.1.0 obj-192.168.1.0 destination
     static obj-10.10.10.0 obj-10.10.10.0
  ```
- Als het bovenstaande werkkader niet mogelijk is, voert u de volgende stappen uit:Wanneer de ASA 8.4(4) of hoger draait, verwijder dan het stand-by IP-adres dat aan de interface is toegewezen.Pas de NAT opdracht toe.Pas het stand-by IP-adres op de interface opnieuw toe.Bijvoorbeeld:
  ```
  ciscoasa(config)# interface Ethernet0/0
  ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
  ciscoasa(config-if)# exit
  ciscoasa(config)# nat (inside,any) 1 source static obj-192.168.1.0
     obj-192.168.1.0 destination static obj-10.10.10.0 obj-10.10.10.0
  ciscoasa(config)# interface Ethernet0/0
  ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
  ```

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems