

ASA FAQ: Waarom beantwoordt de ASA op ARP verzoeken om andere IP adressen in Subnet?

Inhoud

[Inleiding](#)

[Waarom beantwoordt de ASA op ARP verzoeken om andere IP adressen in Subnet?](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft waarom de Cisco adaptieve security applicatie (ASA) zou kunnen reageren op verzoeken om adresresolutie Protocol (ARP) van andere IP-adressen op het netwerk. ASA reageert op ARP-verzoeken om IP-adressen anders dan de ASA's interface.

Waarom beantwoordt de ASA op ARP verzoeken om andere IP adressen in Subnet?

De NAT-configuratie (Network Address Translation) op de ASA kan er voor zorgen dat de ASA reageert op ARP-verzoeken om IP-adressen anders dan het ASA-interface-IP-adres.

Probleemscenario:

Denk aan een Ethernet-segment dat apparaten in het 10.0.1.x/24-netwerk heeft aangesloten. De interne interface van ASA wordt gericht op 10.0.1.1. Wanneer een ARP verzoek om 10.0.1.47 van 10.0.1.48 wordt geïnitieerd, antwoordt de ASA met een ARP antwoord dat zijn eigen interface hardware adres bevat. Verder onderzoek onthult dat de ASA op verzoeken om meerdere IP adressen in het net antwoordt.

In dit specifieke geval veroorzaakt de NAT-configuratie op de ASA het gedrag.

Als u het sleutelwoord **no-proxy-arp** toevoegt aan specifieke NAT opdrachten, zal de ASA niet reageren op ARP verzoeken om het globale IP-subsysteem dat in die NAT-verklaringen is geïdentificeerd.

In dit voorbeeld, veroorzaken deze NAT opdrachten de ASA om op om het even welk ARP verzoek in de subnetten 10.0.1.x/24 en 10.0.2.x/24 op het binnen interfacenetwerk te reageren. Deze opdrachten werden waarschijnlijk toegevoegd aan de ASA-configuratie ter ondersteuning van een overlappend NAT-scenario:

```
nat (inside,inside) source static obj-10.0.1.0 obj-10.0.1.0
destination static obj-10.0.2.0 obj-10.0.2.0
nat (inside,inside) source static obj-10.0.2.0 obj-10.0.2.0
destination static obj-10.0.1.0 obj-10.0.1.0
```

Met het **geen-volmacht-arp** sleutelwoord dat aan deze NAT configuratielijnen wordt toegevoegd, reageert de ASA niet langer op ARP verzoeken om die subnetten.

```
nat (inside,inside) source static obj-10.0.1.0 obj-10.0.1.0
destination static obj-10.0.2.0 obj-10.0.2.0 no-proxy-arp
nat (inside,inside) source static obj-10.0.2.0 obj-10.0.2.0
destination static obj-10.0.1.0 obj-10.0.1.0 no-proxy-arp
```

Gerelateerde informatie

- [Cisco ASA Series Firewall CLI Configuration Guide, 9.1 - Netwerkadresomzetting configureren](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)