

ASA Häufig gestellte Fragen: Warum antwortet die ASA auf ARP-Anfragen für andere IP-Adressen im Subnetz?

Inhalt

[Einführung](#)

[Warum antwortet die ASA auf ARP-Anfragen für andere IP-Adressen im Subnetz?](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird erläutert, warum die Cisco Adaptive Security Appliance (ASA) möglicherweise auf die ARP-Anfragen (Address Resolution Protocol) für andere IP-Adressen im Netzwerk reagiert. Die ASA reagiert auf ARP-Anfragen für andere IP-Adressen als die ASA-Schnittstelle.

Warum antwortet die ASA auf ARP-Anfragen für andere IP-Adressen im Subnetz?

Die Network Address Translation (NAT)-Konfiguration auf der ASA kann dazu führen, dass die ASA auf ARP-Anfragen für andere IP-Adressen als die IP-Adresse der ASA-Schnittstelle reagiert.

Beispielproblemszenario:

Nehmen wir ein Ethernet-Segment, in dem Geräte im 10.0.1.x/24-Netzwerk verbunden sind. Die interne ASA-Schnittstelle wird unter 10.0.1.1 adressiert. Wenn eine ARP-Anfrage für 10.0.1.47 vom 10.0.1.48 an initiiert wird, antwortet die ASA mit einer ARP-Antwort, die ihre eigene Schnittstellen-Hardwareadresse enthält. Weitere Untersuchungen zeigen, dass die ASA Anfragen nach mehreren IP-Adressen im Subnetz beantwortet.

In diesem speziellen Fall verursacht die NAT-Konfiguration auf der ASA das Verhalten.

Wenn Sie das Schlüsselwort **no-proxy-arp** bestimmten NAT-Befehlen hinzufügen, reagiert die ASA nicht auf ARP-Anforderungen für das globale IP-Subnetz, das in diesen NAT-Anweisungen identifiziert wurde.

In diesem Beispiel veranlasst diese NAT-Befehle die ASA, auf alle ARP-Anfragen in den Subnetzen 10.0.1.x/24 und 10.0.2.x/24 im internen Schnittstellennetzwerk zu reagieren. Diese Befehle wurden wahrscheinlich der ASA-Konfiguration hinzugefügt, um ein sich überschneidendes NAT-Szenario zu unterstützen:

```
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
```

Wenn das Schlüsselwort **no-proxy-arp** zu diesen NAT-Konfigurationslinien hinzugefügt wird, reagiert die ASA nicht mehr auf ARP-Anforderungen für diese Subnetze.

```
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
```

Zugehörige Informationen

- [CLI-Konfigurationsleitfaden für die Firewall der Cisco ASA-Serie, 9.1 - Konfigurieren der Network Address Translation](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)