Die als DHCP-Server konfigurierte ASA lässt Hosts keine IP-Adresse zu.

Inhalt

Einführung

Dieses Dokument beschreibt ein spezifisches Konfigurationsproblem, das dazu führen kann, dass Hosts keine IP-Adresse von der Cisco Adaptive Security Appliance (ASA) mit DHCP beziehen können.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der ASA Software Version 8.2.5.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Problem

Wenn die ASA als DHCP-Server konfiguriert ist, können Hosts keine IP-Adresse abrufen.

Die ASA wird als DHCP-Server auf zwei Schnittstellen konfiguriert: VLAN 6 (interne Schnittstelle) und VLAN 10 (DMZ2-Schnittstelle). PCs in diesen VLANs können über DHCP keine IP-Adresse von der ASA erhalten.

- Die DHCP-Konfiguration ist korrekt.
- Die ASA generiert keine Syslogs, die auf die Ursache des Problems hinweisen.
- Paketerfassungen auf der ASA zeigen nur die Ankunft des DHCP-DISCOVER-Pakets an. Die ASA antwortet nicht mit einem OFFER-Paket.

Die Pakete werden vom Accelerated Security Path (ASP) verworfen, und eine auf den ASP angewendete Erfassung weist darauf hin, dass die DHCP DISCOVER-Pakete aufgrund von "Slowpath Security Checks failed:" verworfen wurden.

```
ASA# capture asp type asp-drop all
ASA# show capture asp

3 packets captured
1: 14:57:05.627241 802.1Q VLAN#10 P0 0.0.0.0.68 > 255.255.255.255.67:
udp 300 Drop-reason: (sp-security-failed) Slowpath security checks failed
2: 14:57:08.627286 802.1Q VLAN#10 P0 0.0.0.0.68 > 255.255.255.255.67:
udp 300 Drop-reason: (sp-security-failed) Slowpath security checks failed
3: 14:57:16.626966 802.1Q VLAN#10 P0 0.0.0.0.68 > 255.255.255.255.67:
udp 300 Drop-reason: (sp-security-failed) Slowpath security checks failed
```

Lösung

Die Konfiguration enthält eine allgemeine statische Network Address Translation (NAT)-Anweisung, die den gesamten IP-Datenverkehr in diesem Subnetz umfasst. Die Broadcast DHCP DISCOVER-Pakete (bestimmt für 255.255.255.255) stimmen mit dieser NAT-Anweisung überein, die den Fehler verursacht:

```
static (DMZ1,DMZ2) 0.0.0.0 0.0.0.0 netmask 0.0.0.0
```

Wenn Sie die falsch konfigurierte NAT-Anweisung entfernen, wird das Problem behoben.

Zusätzliche Informationen

Wenn Sie das Paket-Tracer-Dienstprogramm auf der ASA verwenden, um das DHCP-DISCOVER-Paket zu simulieren, das in die DMZ2-Schnittstelle eingeht, kann das Problem als durch die NAT-Konfiguration verursacht identifiziert werden:

```
tutera-firewall#packet-tracer input DMZ2 udp 0.0.0.0 68 255.255.255.255 67 detail
.....
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Configuration:
static (DMZ1,DMZ2) 0.0.0.0 0.0.0.0 netmask 0.0.0.0
match ip DMZ1 any DMZ2 any
static translation to 0.0.0.0
translate_hits = 0, untranslate_hits = 641
```

Additional Information:
NAT divert to egress interface DMZ1
Untranslate 0.0.0.0/0 to 0.0.0.0/0 using netmask 0.0.0.0
Result:
input-interface: DMZ2
input-status: up
input-line-status: up
output-interface: DMZ1
output-status: up
output-line-status: up
Action: drop
Drop-reason: (sp-security-failed) Slowpath security checks failed