

ASA ingesteld als een DHCP-server staat Hosts niet toe om een IP-adres te verkrijgen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Probleem](#)

[Oplossing](#)

[Aanvullende informatie](#)

Inleiding

Dit document beschrijft een specifiek configuratieprobleem dat hosts geen IP-adres kan verkrijgen van de Cisco adaptieve security applicatie (ASA) met DHCP.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op ASA-softwareversie 8.2.5.

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 de potentiële impact van elke opdracht begrijpen.

Probleem

Als ASA als een DHCP-server is ingesteld, kunnen hosts geen IP-adres verkrijgen.

ASA wordt ingesteld als een DHCP-server op twee interfaces: VLAN 6 (binneninterface) en VLAN

10 (DMZ2 interface). PCs op die VLAN's kunnen met succes een IP-adres van de ASA via DHCP niet verkrijgen.

- De configuratie van DHCP is correct.
- Er worden geen syslogs gegenereerd door de ASA die de oorzaak van het probleem aangeven.
- Packet Captures die op de ASA worden genomen tonen alleen de aankomst van het DHCP-DECOVER-pakket. De ASA antwoordt niet met een OFFER-pakket.

De pakketten worden gedropt door het Accelerated Security Path (ASP) en een opname die op de ASP is toegepast, geeft aan dat de DHCP-DECOVER-pakketten zijn gevallen vanwege "Langzame beveiligingscontroles zijn mislukt."

```
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
```

Oplossing

De configuratie bevat een brede statische verklaring van het Adres Vertaling van het Netwerk (NAT) die al IP verkeer op dat net omvat. De pakketten DHCP-DISCOVER van de uitzending (bestemd voor 255.255.255.255) komen deze NAT verklaring overeen die de mislukking veroorzaakt:

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

Als u de niet juist ingestelde NAT-verklaring verwijdert, lost dit het probleem op.

Aanvullende informatie

Als u het Packet-tracer hulpprogramma in de ASA gebruikt om het DHCP-DECOVER-pakket te simuleren dat de DMZ2-interface ingaat, kan het probleem worden geïdentificeerd als veroorzaakt door de NAT-configuratie:

```
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