L'appliance ASA configurata come server DHCP non consente agli host di acquisire un indirizzo IP

Sommario

Introduzione

In questo documento viene descritto uno specifico problema di configurazione che può impedire agli host di acquisire un indirizzo IP da Cisco Adaptive Security Appliance (ASA) con DHCP.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è il software ASA versione 8.2.5.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

Se l'appliance ASA è configurata come server DHCP, gli host non sono in grado di acquisire un

indirizzo IP.

L'ASA è configurata come server DHCP su due interfacce: VLAN 6 (interfaccia interna) e VLAN 10 (interfaccia DMZ2). I PC su tali VLAN non possono ottenere correttamente un indirizzo IP dall'appliance ASA tramite DHCP.

- La configurazione DHCP è corretta.
- L'ASA non genera syslog che indicano la causa del problema.
- Le acquisizioni dei pacchetti sull'appliance ASA mostrano solo l'arrivo del pacchetto DHCP DISCOVER. L'ASA non risponde con un pacchetto offer.

I pacchetti vengono scartati dall'ASP (Accelerated Security Path) e un'acquisizione applicata all'ASP indica che i pacchetti DISCOVER di DHCP vengono scartati a causa di "Controlli di sicurezza Slowpath non riusciti:"

```
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
```

Soluzione

La configurazione contiene un'istruzione NAT (Network Address Translation) statica di grandi dimensioni che include tutto il traffico IP su tale subnet. I pacchetti broadcast DHCP DISCOVER (destinati a 255.255.255.255) corrispondono all'istruzione NAT che causa il problema:

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

Se si rimuove l'istruzione NAT configurata in modo errato, il problema viene risolto.

Ulteriori informazioni

Se si usa l'utility packet-tracer sull'appliance ASA per simulare il pacchetto DHCP DISCOVER che entra nell'interfaccia DMZ2, il problema può essere identificato come causato dalla configurazione NAT:

```
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
```