El ASA configurado como servidor DHCP no permite que los host adquieran una dirección IP

Contenido

Introducción

Este documento describe un problema de configuración específico que pueda hacer a los host no poder adquirir una dirección IP del dispositivo de seguridad adaptante de Cisco (ASA) con el DHCP.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en la versión de software 8.2.5 ASA.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Problema

Con el ASA configurado como servidor DHCP, los host no pueden adquirir una dirección IP.

El ASA se configura como servidor DHCP en dos interfaces: VLA N 6 (interfaz interior) y VLAN10 (interfaz DMZ2). Los PC en esos VLA N no pueden obtener con éxito una dirección IP del ASA vía el DHCP.

- La configuración DHCP está correcta.
- No se genera ningunos Syslog por el ASA que indican la causa del problema.
- Las capturas de paquetes tomadas en el ASA muestran solamente la llegada del paquete DHCP DISCOVER (Detección). El ASA no contesta detrás con un paquete de la OFERTA.

Los paquetes son caídos por la trayectoria acelerada de la Seguridad (ASP), y una captura aplicada al ASP indica que los paquetes DHCP DISCOVER (Detección) son caídos debido a las “revisiones de seguridad de Slowpath falladas: ”

```
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
```

Solución

La configuración contiene una declaración amplia de la traducción de dirección de red estática (NAT) que abarque todo el tráfico IP en esa subred. Los paquetes DHCP DISCOVER (Detección) del broadcast (destinados a 255.255.255.255) hacen juego esta sentencia NAT que cause el error:

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

Si usted quita la sentencia NAT incorrectamente configurada, resuelve el problema.

Información adicional

Si usted utiliza la utilidad del paquete-trazalíneas en el ASA para simular el paquete DHCP DISCOVER (Detección) que ingresa la interfaz DMZ2, el problema se puede identificar según lo causado por la configuración del 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
```