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

Contenido

Introducción

Este documento describe un problema de configuración específico que puede hacer que los hosts no puedan adquirir una dirección IP del Cisco Adaptive Security Appliance (ASA) con DHCP.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Problema

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

El ASA se configura como servidor DHCP en dos interfaces: VLAN 6 (interfaz interna) y VLAN 10 (interfaz DMZ2). Los PC en esas VLAN no pueden obtener con éxito una dirección IP del ASA a

través de DHCP.

- La configuración de DHCP es correcta.
- El ASA no genera registros del sistema que indiquen la causa del problema.
- Las capturas de paquetes tomadas en el ASA sólo muestran la llegada del paquete DHCP DISCOVER. El ASA no responde con un paquete OFFER.

La ruta de seguridad acelerada (ASP) descarta los paquetes, y una captura aplicada al ASP indica que los paquetes DHCP DISCOVER se descartan debido a que "fallaron las comprobaciones de seguridad de la ruta lenta":

```
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 instrucción de traducción de direcciones de red (NAT) estática que abarca todo el tráfico IP de esa subred. Los paquetes DHCP DISCOVER de difusión (destinados a 255.255.255.255) coinciden con esta sentencia NAT que causa la falla:

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

Si elimina la sentencia NAT configurada incorrectamente, resuelve el problema.

Additional Information

Si utiliza la utilidad packet-tracer en el ASA para simular el paquete DHCP DISCOVER que ingresa a la interfaz DMZ2, el problema puede ser identificado como causado por la configuración 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
```