O ASA configurado como um servidor DHCP não permite que os hosts adquiram um endereço IP

Contents

Introduction

Este documento descreve um problema de configuração específico que pode fazer com que os hosts não consigam obter um endereço IP do Cisco Adaptive Security Appliance (ASA) com DHCP.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no software ASA versão 8.2.5.

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

Com o ASA configurado como um servidor DHCP, os hosts não conseguem adquirir um endereço

IP.

O ASA é configurado como um servidor DHCP em duas interfaces: VLAN 6 (interface interna) e VLAN 10 (interface DMZ2). Os PCs nessas VLANs não podem obter com êxito um endereço IP do ASA via DHCP.

- A configuração do DHCP está correta.
- Nenhum syslog é gerado pelo ASA que indica a causa do problema.
- As capturas de pacotes realizadas no ASA mostram apenas a chegada do pacote DHCP DISCOVER. O ASA não responde com um pacote OFFER.

Os pacotes são descartados pelo caminho de segurança acelerada (ASP), e uma captura aplicada ao ASP indica que os pacotes DHCP DISCOVER são descartados devido a "falha nas verificações de segurança do Slowpath:"

```
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
```

Solução

A configuração contém uma instrução de Conversão de Endereço de Rede (NAT - Network Address Translation) estática ampla que abrange todo o tráfego IP nessa sub-rede. Os pacotes DHCP DISCOVER de broadcast (destinados a 255.255.255.255) correspondem a esta instrução NAT que causa a falha:

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

Se você remover a instrução NAT configurada incorretamente, o problema será resolvido.

Additional Information

Se você usar o utilitário packet-tracer no ASA para simular o pacote DHCP DISCOVER que entra na interface DMZ2, o problema pode ser identificado como causado pela configuração do 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
```