ASA Configured as a DHCP Server Does Not Allow Hosts to Acquire an IP Address

Contents

Introduction

This document describes a specific configuration problem that can cause hosts to be unable to aquire an IP address from the Cisco Adaptive Security Appliance (ASA) with DHCP.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on ASA Software Version 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.

Problem

With the ASA configured as a DHCP Server, hosts are unable to acquire an IP address.

The ASA is configured as a DHCP server on two interfaces: VLAN 6 (inside interface) and VLAN 10 (DMZ2 interface). PCs on those VLANs cannot successfully obtain an IP address from the ASA

via DHCP.

- The DHCP configration is correct.
- No syslogs are generated by the ASA that indicate the cause of the problem.
- Packet captures taken on the ASA only show the arrival of the DHCP DISCOVER packet. The ASA does not reply back with an OFFER packet.

The packets are dropped by the Accelerated Security Path (ASP), and a capture applied to the ASP indicates the DHCP DISCOVER packets are dropped due to "Slowpath security checks failed:"

```
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
```

Solution

The configuration contains a broad static Network Address Translation (NAT) statement that encompasses all IP traffic on that subnet. The broadcast DHCP DISCOVER packets (destined to 255.255.255.255) match this NAT statement which causes the failure:

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

If you remove the incorrectly configured NAT statement, it resolves the problem.

Additional Information

If you use the packet-tracer utility on the ASA to simulate the DHCP DISCOVER packet that enters the DMZ2 interface, the problem can be identified as caused by the NAT configuration:

```
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