配置为DHCP服务器的ASA不允许主机获取IP地址

目录

简介

本文档介绍可能导致主机无法从带DHCP的思科自适应安全设备(ASA)获取IP地址的特定配置问题。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于ASA软件版本8.2.5。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

问题

将ASA配置为DHCP服务器后，主机无法获取IP地址。

ASA在两个接口上配置为DHCP服务器：VLAN 6（内部接口）和VLAN 10（DMZ2接口）。这些VLAN中的PC无法通过DHCP从ASA成功获取IP地址。

- DHCP配置正确。
- ASA不生成指示问题原因的系统日志。

- 在ASA上捕获的数据包仅显示DHCP DISCOVER数据包到达。ASA不回复OFFER数据包。

数据包被加速安全路径(ASP)丢弃，应用到ASP的捕获表明DHCP DISCOVER数据包由于“慢路径安全检查失败：”而被丢弃：

```
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
```

解决方案

该配置包含包含该子网上所有IP流量的广泛静态网络地址转换(NAT)语句。广播DHCP DISCOVER数据包（发往255.255.255.255）与此NAT语句匹配，导致故障：

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

如果删除配置错误的NAT语句，它将解决问题。

其他信息

如果在ASA上使用packet-tracer实用程序模拟进入DMZ2接口的DHCP DISCOVER数据包，则问题可以确定为由NAT配置引起的：

```
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
```