

作为DHCP服务器配置的ASA不允许主机获取IP地址

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[问题](#)

[解决方案](#)

[其他信息](#)

简介

本文描述能造成主机无法获取从思科可适应安全工具的特定配置问题(ASA)的一个IP地址有DHCP的。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据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

使用作为DHCP服务器配置的ASA，主机无法获取IP地址。

ASA配置作为在两个接口的一个DHCP服务器：VLAN 6 (内部接口)和VLAN10 (DMZ2接口)。在那些VLAN的PCs不能从ASA顺利地获取IP地址通过DHCP。

- DHCP配置正确。
- 指示问题的原因的Syslog没有由ASA生成。
- 在ASA采取的数据包捕获只显示DHCP DISCOVER数据包的到达。ASA不应答有提供数据包的上一步。

数据包由加速的安全路径(ASP)丢弃，并且捕获应用对ASP指示DHCP DISCOVER数据包是丢弃由于“失败的Slowpath安全性检查：”

```
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

配置包含包含在该子网的所有IP数据流的一个清楚的静态网络地址转换(NAT)语句。广播DHCP DISCOVER数据包(被注定对255.255.255.255)匹配导致失败的此NAT语句：

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

如果删除不正确地配置的NAT语句，解决问题。

其他信息

如果使用在ASA的数据包追踪器工具模拟进入DMZ2接口的DHCP DISCOVER数据包，问题可以识别如造成的是由NAT配置：

```
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
```