ASA, настроенный как сервер DHCP, не позволяет хостам получать IP-адрес

Содержание

Введение

Этот документ описывает определенную проблему конфигурации, которая может заставить хосты быть неспособными к aquire IP-адрес от устройства адаптивной защиты Cisco (ASA) с DHCP.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на Версии программного обеспечения 8.2.5 ASA.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Проблема

С ASA, настроенным как Сервер DHCP, хосты неспособны получить IP-адрес.

ASA настроен как сервер DHCP на двух интерфейсах: (внутренний интерфейс) VLAN 6 и VLAN 10 (интерфейс DMZ2). PC на тех VLAN не могут успешно получить IP-адрес из ASA через DHCP.

- DHCP configration корректен.
- Никакие системные журналы не генерируются ASA, которые указывают на причину проблемы.
- Захваты пакета, взятые ASA только, показывают прибытие пакета DHCP DISCOVER. ASA не отвечает назад с пакетом OFFER.

Пакеты отброшены Ускоренным путем безопасности (ASP), и перехват применился к ASP, указывает, что пакеты DHCP DISCOVER отброшены из-за "подведенных проверок безопасности 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
```

Решение

Конфигурация содержит широкую статическую трансляцию сетевых адресов оператор (NAT), который охватывает весь IP - трафик на той подсети. Широковещательные пакеты DHCP DISCOVER (предназначенный к 255.255.255.255) совпадают с этим Выражением NAT, которое вызывает сбой:

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

При удалении неправильно настроенного Выражения NAT оно решает проблему.

Дополнительные сведения

При использовании утилиту packet-tracer на ASA для моделирования пакета DHCP DISCOVER, который вводит интерфейс DMZ2, проблема может быть определена, как вызвано конфигурацией 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
```