DHCP 서버로 구성된 ASA는 호스트가 IP 주소를 취득하는 것을 허용하지 않습니다.

목차

소개

이 문서에서는 호스트가 DHCP를 사용하는 Cisco ASA(Adaptive Security Appliance)에서 IP 주소를 수신하지 못하게 할 수 있는 특정 컨피그레이션 문제에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 ASA 소프트웨어 버전 8.2.5을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제

ASA가 DHCP 서버로 구성된 경우 호스트가 IP 주소를 획득할 수 없습니다.

ASA는 두 인터페이스에서 DHCP 서버로 구성됩니다.VLAN 6(내부 인터페이스) 및 VLAN 10(DMZ2 인터페이스).이러한 VLAN의 PC는 DHCP를 통해 ASA에서 IP 주소를 성공적으로 가져올 수 없습니

다.

- DHCP 구성이 올바릅니다.
- ASA에서 문제의 원인을 나타내는 syslog가 생성되지 않습니다.
- ASA에서 가져온 패킷 캡처는 DHCP DISCOVER 패킷의 도착만 표시합니다.ASA는 OFFER 패킷으로 회신하지 않습니다.

패킷은 ASP(Accelerated Security Path)에 의해 삭제되고 ASP에 적용된 캡처는 "Slowpath security checks failed:"(느린 경로 보안 검사 실패:)" 때문에 DHCP DISCOVER 패킷이 삭제되었음을 나타냅니다.

```
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
```

솔루션

컨피그레이션에는 해당 서브넷의 모든 IP 트래픽을 포함하는 광범위한 고정 NAT(Network Address Translation) 문이 포함되어 있습니다.브로드캐스트 DHCP DISCOVER 패킷(255.255.255.255으로 지정됨)은 이 NAT 문과 일치하며, 이로 인해 오류가 발생합니다.

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

잘못 구성된 NAT 문을 제거하면 문제가 해결됩니다.

추가 정보

ASA에서 packet-tracer 유틸리티를 사용하여 DMZ2 인터페이스에 들어가는 DHCP DISCOVER 패킷을 시뮬레이션하는 경우 NAT 컨피그레이션으로 인해 문제가 식별될 수 있습니다.

```
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
```