ISE에서 리디렉션할 때 Catalyst 9000 Series 엔드포인트가 DHCP 주소를 수신하지 못하는 문제 해결

목차

문제

Cisco Catalyst 9000 Series 스위치에서 Cisco ISE(Identity Services Engine)의 리디렉션을 사용하여 인증을 활성화하면 유선 엔드포인트가 DHCP(Dynamic Host Configuration Protocol)를 통해 IP 주소를 간헐적으로 얻을 수 없습니다. Catalyst 9000 Series 스위치가 아닌 경우 동일한 구성을 사용해도 문제가 발생하지 않습니다.

환경

- 제품군: Catalyst 9000 Series
- DHCP 획득 오류가 발생한 Windows 컴퓨터
- Catalyst 9000 Series 스위치의 리디렉션 ACL(Access Control List)은 DHCP 트래픽을 명시적으로 거부하지 않습니다

해결

1. DHCP 트래픽을 명시적으로 처리하기 위해 리디렉션 ACL에 다음 deny 문을 추가합니다.

```
deny udp any eq bootps any
```

사용자 데이터그램 프로토콜 any any eq bootpc 거부

```
deny udp any eq bootpc any
```

2. ACL을 수정한 후 이전에 실패한 디바이스를 다시 인증하여 DHCP를 통해 IP 주소를 성공적으로 검색할 수 있는지 확인합니다.

원인

Catalyst 9000 Series 스위치는 인증이 활성화된 경우 이전 스위치 모델과 다르게 패킷을 처리합니다. Catalyst 9000 Series 스위치의 패킷 처리 순서는 다음과 같습니다.

1. ACE(액세스 제어 항목 허용) 규칙과 일치하는 패킷이 AAA 서버로의 리디렉션을 위해 CPU로 전송됩니다.

2. 거부 ACE 규칙과 일치하는 패킷은 스위치를 통해 전달됩니다.

3. 허용 또는 거부 ACE 규칙과 일치하지 않는 패킷은 다음 DACL(Downloadable Access Control List)에서 처리하며, DACL이 없는 경우 패킷이 암시적 거부 ACL에 도달하여 삭제됩니다.

이 처리 방법은 기본적으로 DHCP 트래픽을 허용하는 기본 ACL을 사용하며 리디렉션 ACL에 앞서 처리되는 이전 스위치 모델과 다릅니다. Catalyst 9000 Series 모델은 이러한 기본 ACL을 사용하지 않고 세션에서 사용되는 리디렉션 ACL 및 DACL에 전적으로 의존합니다. 이전 Catalyst 스위치의 닫힌 모드 세션에 대한 기본 ACL은 다음과 같습니다.

```
3750#sh ip access-lists Auth-Default-ACL

확장 IP 액세스 목록 Auth-Default-ACL

    10 permit udp any range bootps 65347 any range bootpc 65348(22개 일치)

    20 permit udp any range bootps 65347(12개 일치)

    30 ip any any any
```

관련 콘텐츠

- 802.1X 인증을 위한 기본 ACL
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.