Cisco Secure Access Fragmented ICMP 패킷 처리

목차

문제

MTU보다 큰 ICMP 에코 요청은 DF(Don't Fragment) 비트가 비활성화된 상태로 전송될 때 회신을 수신하지 않습니다. 이 동작은 두 가지 특정 시나리오에서 발생합니다.

- DF 비트가 지워진 상태에서 VPN 인터페이스 MTU 크기를 초과하는 ICMP 패킷을 전송할 때 VPN 인터페이스를 통해 RAVPN 엔드포인트에서
- DF 비트가 지워진 상태에서 IPsec 터널 인터페이스 MTU 크기를 초과하는 ICMP 패킷을 전송할 때 사이트 라우터와 CSA(Cisco Secure Access) 사이의 IPsec 터널을 통해 온-프레미스 엔드포인트에서

두 경우 모두 ICMP 응답이 수신되지 않으므로 CSA에서 DF 비트가 비활성화된 프래그먼트된 패킷을 삭제하는지 여부에 대한 질문이 발생합니다.

환경

- CSA(Cisco Secure Access)
- RAVPN(원격 액세스 VPN) 엔드포인트
- 사이트 라우터와 CSA 간의 IPsec 터널
- 인터페이스 MTU 크기를 초과하는 ICMP 트래픽
- DF 비트가 지워진 프래그먼트된 패킷 시나리오

해결

Cisco Secure Access는 언더레이 및 오버레이 시나리오에서 프래그먼트된 패킷을 삭제합니다. 이 동작은 Cisco Secure Access Help 설명서에 설명되어 있으며, 여기에는 명시적으로 다음과 같은 내

용이 포함되어 있습니다. "언더레이 또는 오버레이의 조각화된 패킷은 삭제됩니다."

예상 동작

Cisco Secure Access는 프래그먼트된 패킷이 언더레이 또는 오버레이 네트워크에서 발생하는지 여부에 관계없이 삭제하도록 설계되었습니다. 이는 다음 경우에 적용됩니다.

- DF 비트가 지워진 VPN 인터페이스 MTU를 초과하는 RAVPN 엔드포인트에서 전송된 ICMP 패킷
- DF 비트가 지워진 터널 인터페이스 MTU를 초과하는 IPsec 터널을 통해 온프레미스 엔드포인트에서 전송되는 ICMP 패킷

이 동작은 Cisco Secure Access 인프라 내의 단편화된 패킷을 포함하는 모든 시나리오에서 일관됩니다.

이에 대한 기능 요청 CSE-I-5739가 생성되었습니다.

원인

Cisco Secure Access는 보안 및 성능 설계 결정으로 단편화된 패킷을 삭제하도록 설계되었습니다. 이 동작은 언더레이 및 오버레이 네트워크 시나리오에서 패킷 리어셈블과 관련된 잠재적인 보안 취약성 및 처리 오버헤드를 방지하기 위해 구현됩니다.

관련 콘텐츠

- Cisco Secure Access 도움말 설명서 - 단편화된 패킷 처리
- 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.