

ESN 협상으로 인한 Versa Networks Router와의 보안 액세스 IPsec 터널 연결 문제

목차

문제

Versa-Network Router를 에지 디바이스로 사용하여 지사에 Cisco Secure Access를 구축하는 동안 두 IPsec 터널이 모두 작동하는 경우에도 연결 문제가 발생했습니다. T

구체적인 증상은 다음과 같습니다.

- 지사에서 Cisco Secure Access로의 연결 없음
- 고정 경로를 통한 인터넷 액세스가 작동하지 않음
- 단방향 암호화 트래픽 관찰(보안 액세스로의 아웃바운드 전용)
- 전송 중인 아웃바운드 패킷은 표시하지만 수신된 인바운드 패킷은 표시하지 않는 라우터 통계
- SD-WAN 라우터와 Secure Access 간에 양방향으로 작동하는 데드 피어 감지
- 아웃바운드 트래픽에 대한 SPI(Security Parameter Index) 값이 올바르게 일치합니다.
- 터널 플래핑(재설정)으로 인해 연결 문제가 해결되지 않았습니다.
- 패킷 캡처 및 스크린샷은 인바운드 트래픽의 부족을 확인했습니다
- 터널 암호를 CBC에서 GCM으로 변경해도 문제가 해결되지 않았습니다

조사 결과 Cisco 측에서 체크섬 오류로 인해 트래픽이 해독되지 못했으며, 이는 ESN(Extended Sequence Number) 기능을 협상하는 Versa 라우터로 추적되었습니다.

환경

- Cisco Secure Access 구축

- Versa-Networks Router as edge device
- IP-Identity 터널 컨피그레이션
- CBC 및 GCM 암호화 시도를 모두 사용하는 IPsec 터널 컨피그레이션

해결

해결 방법에는 Cisco Secure Access 헤드엔드에서 암호 해독 실패를 일으키는 체크섬 오류를 방지하기 위해 Versa 라우터에서 ESN(Extended Sequence Number) 협상을 비활성화하는 것이 포함되었습니다.

해결 단계

1단계: 근본 원인 파악

조사 결과 Versa 라우터가 ESN(Extended Sequence Number)을 협상하고 있는 것으로 확인되었으며, 이로 인해 Cisco Secure Access 헤드엔드는 체크섬 오류를 수신하고 ESN에서 생성한 패킷의 해독에 실패했습니다.

2단계: Versa 라우터에서 ESN 비활성화

Versa 라우터 컨피그레이션에서 ESN 확인 및 협상을 비활성화하려면 Versa Networks 지원 또는 라우터 관리자에게 문의하십시오. 이렇게 하면 ESN이 잘못 협상된 알려진 Versa 버그가 해결됩니다.

3단계: 연결 확인

ESN 협상을 비활성화한 후 양방향 트래픽 흐름이 설정되었고 브랜치에서 보안 액세스 및 인터넷으로의 전체 연결이 복원되었는지 확인합니다.

4단계: 트래픽 흐름 모니터링

라우터의 인바운드 및 아웃바운드 패킷 통계가 양방향으로 적절한 트래픽 흐름을 표시하는지 확인하여 단방향 트래픽 문제를 성공적으로 해결했는지 확인합니다.

원인

근본 원인은 알려진 Versa Networks 버그로 식별되었습니다(Versa 지원 버그 ID: 122437 - ESN은 VOS에 의해 협상되어서는 안 됩니다.) IPsec 터널 설정 중에 Versa 라우터가 ESN(Extended Sequence Number) 기능을 잘못 협상합니다. 이 ESN 협상으로 인해 Cisco Secure Access 헤드엔드가 체크섬 오류가 있는 패킷을 수신함으로써, 적절한 암호 해독을 방해하고 단방향 트래픽 흐름을 초래합니다. Versa 라우터가 아웃바운드 패킷을 성공적으로 전송했지만 ESN 관련 암호 해독 실패로 인해 반환 트래픽을 제대로 처리할 수 없습니다.

관련 콘텐츠

- [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.