ASA를 통해 트래픽이 이동할 때 TCP를 통한 IPsec 실패

목차

소개

IPsec over TCP를 사용하여 VPN 헤드엔드에 연결하는 Cisco VPN Client는 헤드엔드 미세(headend fine)에 연결할 수 있지만, 잠시 후에 연결이 실패합니다.이 문서에서는 문제를 해결하기 위해 UDP 또는 네이티브 ESP IPsec 캡슐화를 통해 IPsec으로 전환하는 방법에 대해 설명합니다.

시작하기 전에

요구 사항

이 특정 문제를 해결하려면 IPsec over TCP를 사용하여 VPN 헤드엔드 디바이스에 연결하도록 Cisco VPN 클라이언트를 구성해야 합니다.대부분의 경우 네트워크 관리자는 TCP 포트 10000을 통한 Cisco VPN 클라이언트 연결을 허용하도록 ASA를 구성합니다.

사용되는 구성 요소

이 문서의 정보는 Cisco VPN Client를 기반으로 합니다.

표기 규칙

문서 표기 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

문제

VPN 클라이언트가 TCP를 통한 IPsec(cTCP)에 대해 구성된 경우 VPN 클라이언트 소프트웨어는 중복 TCP ACK가 VPN 클라이언트에 데이터를 다시 전송하도록 요청하는 경우 응답하지 않습니다.VPN 클라이언트와 ASA 헤드엔드 사이에 패킷 손실이 있는 경우 중복 ACK가 생성될 수 있습니다

.간헐적인 패킷 손실은 인터넷에서 꽤 흔한 현실입니다.그러나 VPN 엔드포인트가 TCP 프로토콜을 사용하지 않으므로(cTCP를 사용 중임을 기억함) 엔드포인트는 계속 전송되며 연결이 계속됩니다.

이 시나리오에서는 TCP 연결을 상태 적으로 추적하는 방화벽과 같은 다른 디바이스가 있는 경우 문제가 발생합니다.cTCP 프로토콜이 TCP 클라이언트를 완전히 구현하지 않고 서버 중복 ACK가 응답을 받지 않기 때문에, 이 네트워크 스트림에 연결된 다른 디바이스가 TCP 트래픽을 삭제할 수 있습니다.패킷이 손실되면 TCP 세그먼트가 누락되어 문제가 트리거됩니다.

이는 버그가 아니라 네트워크에서 패킷 손실 및 cTCP가 실제 TCP가 아니라는 사실의 부작용입니다.cTCP는 TCP 헤더 내에서 IPsec 패킷을 래핑하여 TCP 프로토콜을 에뮬레이션하려고 하지만, 이는 프로토콜의 범위입니다.

이 문제는 일반적으로 네트워크 관리자가 IPS가 포함된 ASA를 구현하거나, 방화벽이 연결의 전체 TCP 프록시 역할을 하게 하는 ASA에서 일종의 애플리케이션 검사를 수행할 때 발생합니다.패킷 손실이 있는 경우 ASA는 cTCP 서버 또는 클라이언트를 대신하여 누락된 데이터에 대해 ACK를 수행하지만 VPN 클라이언트는 응답하지 않습니다.ASA는 기대하는 데이터를 수신하지 않으므로 통신을 계속할 수 없습니다.따라서 연결이 실패합니다.

솔루션

이 문제를 해결하려면 다음 작업 중 하나를 수행합니다.

- IPsec over TCP에서 IPsec over UDP로 또는 ESP 프로토콜을 통한 네이티브 캡슐화로 전환합니다.
- 완전히 구현된 TCP 프로토콜 스택을 사용하는 VPN 종료를 위해 AnyConnect 클라이언트로 전환합니다.
- 이러한 특정 IPsec/TCP 흐름에 tcp-state-bypass를 적용하도록 ASA를 구성합니다.이렇게 하면 기본적으로 tcp-state-bypass 정책과 일치하는 연결에 대한 모든 보안 검사가 비활성화되지만 이 목록의 다른 해결 방법이 구현될 때까지 연결이 작동합니다.자세한 내용은 TCP State Bypass Guidelines and Limits를 참조하십시오.
- 패킷 손실의 소스를 식별하고 IPsec/TCP 패킷이 네트워크에서 삭제되는 것을 방지하기 위해 수정 조치를 취합니다.이 문제는 일반적으로 문제의 트리거가 인터넷에서 일반적으로 패킷 손실이므로 불가능하거나 매우 어렵습니다. 삭제를 방지할 수 없습니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems