VPN 3000 Concentrator에서 IPSec을 위한 NAT 투명 모드 구성

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[표기 규칙](#)
[보안 페이로드 캡슐화](#)
[NAT 투명 모드는 어떻게 작동합니까?](#)
[NAT 투명 모드 구성](#)
[NAT 투명성을 사용하기 위한 Cisco VPN 클라이언트 컨피그레이션](#)
[관련 정보](#)

소개

NAT(Network Address Translation)는 주소 공간이 부족한 IPV4(Internet Protocol Version 4)의 문제를 해결하기 위해 개발되었습니다. 오늘날 가정용 사용자와 소규모 사무실 네트워크는 등록된 주소를 구매하는 대신 NAT를 사용합니다. 기업은 내부 리소스를 보호하기 위해 NAT만 구현하거나 방화벽과 함께 구축합니다.

가장 일반적으로 구현되는 다대일 NAT 솔루션인 다대일(Many-to-one)는 여러 개인 주소를 하나의 라우팅 가능(공용) 주소에 매핑합니다. 이를 PAT(Port Address Translation)라고도 합니다. 연결은 포트 레벨에서 구현됩니다. PAT 솔루션은 포트를 사용하지 않는 IPSec 트래픽에 문제를 만듭니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco VPN 3000 Concentrator
- Cisco VPN 3000 클라이언트 릴리스 2.1.3 이상
- NAT-T용 Cisco VPN 3000 Client and Concentrator Release 3.6.1 이상

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.

표기 규칙

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

보안 페이로드 캡슐화

Protocol 50(ESP(Encapsulating Security Payload))은 IPSec의 암호화/캡슐화된 패킷을 처리합니다. 대부분의 PAT 디바이스는 TCP(Transmission Control Protocol), UDP(User Datagram Protocol) 및 ICMP(Internet Control Message Protocol)에서만 작동하도록 프로그래밍되었으므로 ESP에서 작동하지 않습니다. 또한 PAT 디바이스는 여러 SPI(Security Parameter Indexes)를 매핑할 수 없습니다. VPN 3000 클라이언트의 NAT 투명 모드는 UDP 내에서 ESP를 캡슐화하여 협상된 포트로 전송하여 이 문제를 해결합니다. VPN 3000 Concentrator에서 활성화할 특성의 이름은 NAT를 통한 IPSec입니다.

IETF 표준인 새로운 프로토콜 NAT-T(이 문서를 작성하는 현재 DRAFT 단계에 있음)도 UDP에서 IPSec 패킷을 캡슐화하지만 포트 4500에서 작동합니다. 해당 포트는 구성할 수 없습니다.

NAT 투명 모드는 어떻게 작동합니까?

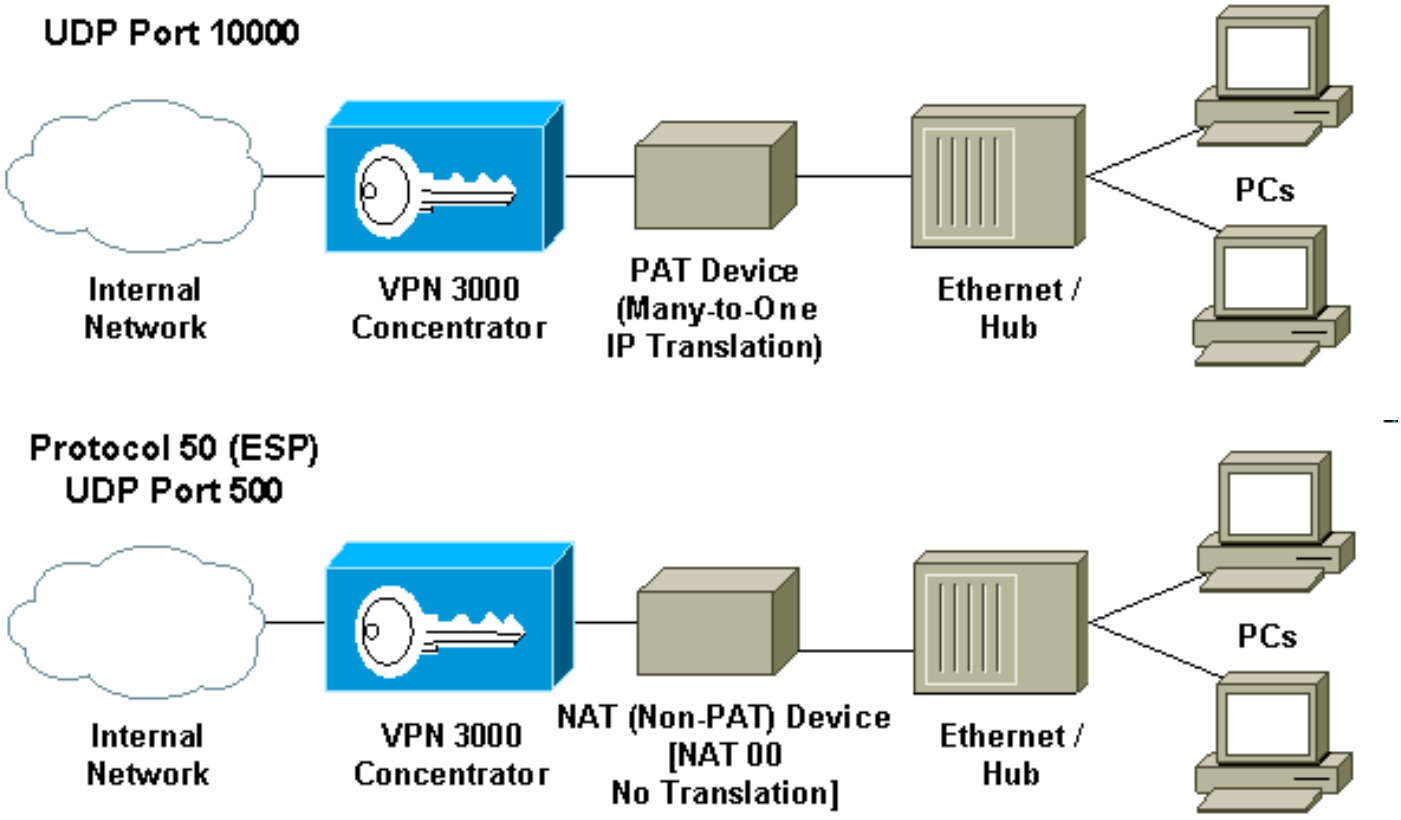
VPN Concentrator에서 IPSec 투명 모드를 활성화하면 보이지 않는 필터 규칙이 생성되어 공용 필터에 적용됩니다. 그런 다음 VPN 클라이언트가 연결되면 구성된 포트 번호가 VPN 클라이언트에 투명하게 전달됩니다. 인바운드 측에서 해당 포트의 UDP 인바운드 트래픽이 처리를 위해 IPSec에 직접 전달됩니다. 트래픽은 해독되고 역캡슐화된 다음 정상적으로 라우팅됩니다. 아웃바운드 측면에서 IPSec은 UDP 헤더를 암호화, 캡슐화 및 적용합니다(구성된 경우). 런타임 필터 규칙은 다음 세 가지 조건에 따라 비활성화되고 해당 필터에서 삭제됩니다. 그룹에 대해 IPSec over UDP를 비활성화하거나, 그룹이 삭제되거나, 해당 포트의 마지막 활성 IPSec over UDP SA가 삭제될 때. NAT 디바이스가 비활성화로 인해 포트 매핑을 닫지 않도록 keepalive가 전송됩니다.

VPN Concentrator에서 IPSec over NAT-T가 활성화된 경우 VPN Concentrator/VPN Client는 UDP 캡슐화의 NAT-T 모드를 사용합니다. NAT-T는 IKE 협상 중에 VPN 클라이언트와 VPN Concentrator 간의 NAT 디바이스를 자동으로 탐지하여 작동합니다. NAT-T를 위한 VPN Concentrator/VPN 클라이언트 간에 UDP 포트 4500이 차단되지 않도록 해야 합니다. 또한 해당 포트를 이미 사용 중인 이전 IPSec/UDP 컨피그레이션을 사용하는 경우 다른 UDP 포트를 사용하도록 이전 IPSec/UDP 컨피그레이션을 재구성해야 합니다. NAT-T는 IETF 초안이므로 다른 벤더가 이 표준을 구현하는 경우 멀티벤더 디바이스를 사용할 때 도움이 됩니다.

NAT-T는 IPSec over UDP/TCP와 달리 VPN 클라이언트 연결 및 LAN-to-LAN 연결과 함께 작동합니다. 또한 Cisco IOS® 라우터와 PIX 방화벽 디바이스는 NAT-T를 지원합니다.

NAT-T가 작동하도록 IPSec over UDP를 활성화할 필요가 없습니다.

NAT 투명 모드 구성



VPN Concentrator에서 NAT 투명 모드를 구성하려면 다음 절차를 사용합니다.

참고: IPSec over UDP는 그룹 단위로 구성되고 IPSec over TCP/NAT-T는 전역으로 구성됩니다.

1. UDP를 통한 IPSec 구성:VPN Concentrator에서 Configuration(구성) **> User Management(사용자 관리) > Groups(그룹)를** 선택합니다.그룹을 추가하려면 **추가**를 선택합니다. 기존 그룹을 수정하려면 그룹을 선택하고 수정을 **클릭합니다**.IPSec 탭을 클릭하고 NAT를 **통해 IPSec**을 확인하고 NAT **UDP Port를 통해 IPSec을 구성합니다**. NAT를 통한 IPSec의 기본 포트는 10000(소스 및 대상)이지만 이 설정은 변경될 수 있습니다.
2. IPSec over NAT-T 및/또는 IPSec over TCP를 구성합니다.VPN Concentrator에서 **Configuration > System > Tunneling Protocols > IPSec** > NAT **Transparency를** 선택합니다 .IPSec over **NAT-T 및/또는 TCP** 확인란을 선택합니다.

모든 것이 활성화된 경우 다음 우선 순위를 사용합니다.

1. TCP를 통한 IPSec
2. IPSec over NAT-T.
3. UDP를 통한 IPSec

NAT 투명성을 사용하기 위한 Cisco VPN 클라이언트 컨피그레이션

IPSec over UDP 또는 NAT-T를 사용하려면 Cisco VPN Client 3.6 이상에서 IPSec over UDP를 활성화해야 합니다. UDP 포트는 UDP를 통한 IPSec의 경우 VPN Concentrator에 의해 할당되고 NAT-T의 경우 UDP 포트 4500으로 고정됩니다.

TCP를 통해 IPSec을 사용하려면 VPN 클라이언트에서 IPSec을 활성화하고 수동으로 사용해야 하는 포트를 구성해야 합니다.

관련 정보

- Cisco VPN 3000 Series Concentrator 지원 페이지
- Cisco VPN 3000 Series 클라이언트 지원 페이지
- IPSec 지원 페이지
- Technical Support - Cisco Systems