Trey Research Corporation

VPN(가상 사설망): Fabrikam, Inc. 기술 개요

2023년 12월 15일

VPN(가상 사설망)은 널리 사용되는 네트워크 보안 솔루션으로서, 네트워크 트래픽 암호화에 도움이 될 수 있습니다. 보안 채널로 작동하는 VPN은 인터넷 트래픽을 암호화하므로 제3자가 인터넷의 활동을 추적하고 데이터를 도용하기가 어려워집니다[1].

VPN 구현 시의 장점:

- 인터넷 트래픽을 암호화하는 VPN에서는 개인 정보 보호 및 보안 레이어가 적용됩니다. 따라서 제3자가 인터넷의 활동을 추적하고 데이터를 도용하기가 어려워집니다.
- VPN을 구현하면 공항, 도서관 등의 공용 Wi-Fi 사용 시 해킹을 방지하는 데 도움이 될 수 있습니다. VPN이 보안 터널로 작동하여 인터넷 트래픽을 암호화하기 때문입니다.
- VPN 구현 시에는 사용자가 방문한 사이트를 인터넷 서비스 공급자가 확인할 수 없습니다. 컴퓨터에서 전송 및 수신되는 모든 트래픽이 VPN 서버나 VPN에서 유료로 사용하는 서버를 통과하기 때문입니다[1].
- VPN 구현 시에는 콘텐츠에 적용되는 지리적 제한을 우회할 수 있습니다[2]. VPN은 IP 주소를 마스킹하고 인터넷 연결을 암호화하기 때문입니다. VPN 서버에 연결하면

인터넷 트래픽이 VPN 서버를 통해 라우팅되므로 새 IP 주소가 할당됩니다. 즉, 다른 위치에서 인터넷에 액세스하는 것으로 표시되므로 콘텐츠에 적용되는 지리적 제한을 우회할 수 있습니다.

VPN 구현 시의 단점:

- ISP 연결 사용 시에 비해 연결 속도가 느려질 수 있습니다. VPN이 인터넷 트래픽에 암호화 및 라우팅을 위한 추가 레이어를 적용하기 때문입니다[2].
- 엄격한 규제가 적용되는 일부 국가에서는 VPN 사용이 금지됩니다. VPN 사용이 금지되거나 엄격한 규제가 적용되는 국가도 있습니다[2].
- 무료 VPN 사용 시 광고 표시, 맬웨어 감염, 데이터 유출 등이 발생할 위험성이 있습니다. 무료 VPN에서는 타사 광고주에 사용자 데이터를 판매하거나 웹 페이지에 광고를 삽입할 수도 있습니다[2].

구체적인 설치 방법:

- VPN은 VPN 클라이언트를 실행하는 시스템과 VPN 서버 간에 암호화된 터널을 설정합니다. 그러면 VPN 서버가 터널을 통해 엔터프라이즈 네트워크의 다른 위치로 트래픽을 프록시합니다[4]. 구체적인 단계는 다음과 같습니다.

    1. 사용자 디바이스에 설치된 VPN 클라이언트가 디바이스와 VPN 서버 간에 전송되는 모든 트래픽을 암호화합니다.
    2. VPN 서버가 트래픽 암호를 해독한 후 적절한 대상으로 트래픽을 전달합니다.
    3. 대상 서버가 VPN 서버로 트래픽을 다시 전송하는 방식으로 요청에 응답합니다.
    4. VPN 서버가 트래픽을 암호화한 후 VPN 클라이언트로 다시 전송합니다.

5. VPN 클라이언트가 트래픽 암호를 해독한 후 사용자 디바이스로 전송합니다[1].

- VPN 서버를 설치 및 구성하려면 다음 단계를 수행합니다.
    1. 컴퓨터에서 VPN 프로필을 만듭니다.
    2. 시작을 클릭한 후 설정을 클릭하여 설정 메뉴를 엽니다.
    3. 설정 메뉴에서 네트워크 및 인터넷과 VPN을 차례로 클릭합니다.
    4. VPN 연결 추가를 선택합니다.
    5. VPN 연결 추가 창에서 몇 가지 작업을 수행합니다.
    6. 변경한 내용을 저장합니다[5].

발생 가능한 위험 및 완화 방법:

- 공격자들은 오래 전부터 원격 작업을 위협 벡터로 활용해 왔습니다. 공격자들이 원격 작업 환경 공격을 선호하는 이유에는 여러 가지가 있습니다. 우선, 홈 네트워크 환경은 전문적으로 관리되지 않습니다. 무엇보다도 홈 네트워크의 많은 시스템에는 정기적으로 패치가 설치되지 않으며 시스템에서 취약성을 완화한 시점도 오래 전인 경우가 많습니다. 엔터프라이즈 네트워크에서 특정 시스템 악용에 성공한 공격자가 공격을 계속 진행하려면 감지와 수정 조치를 피해야 합니다. 그러므로 대개 위협 감지가 설정되어 있지 않으며 PC 실행 속도가 느려 운영 체제를 다시 설치하거나 사용을 중지하는 등의 상황이 발생해야 수정 작업이 수행되는 홈 네트워크를 공격 대상으로 선호하는 경우가 많습니다. 원격 작업 환경을 보호하려면 홈 네트워크에도 제로 트러스트 원칙을 적용해야 합니다. 네트워크뿐 아니라 기업이 통제할 수 없는 모든 요소를 공격자로 간주해야 합니다[4].

- 최신 소프트웨어 패치를 설치하고 보안을 구성하여 VPN, 네트워크 인프라 디바이스 및 원격으로 작업 환경에 액세스하는 데 사용되는 디바이스를 업데이트해야 합니다[6].

구현 모범 사례:

회사 네트워크에서 VPN을 구현하는 모범 사례는 다음과 같습니다.

- IKE/IPSec(Internet Key Exchange/인터넷 프로토콜 보안) 등의 허용되는 표준을 사용하는 표준 기반 VPN을 선택합니다. 이러한 VPN은 대개 사용자 지정 코드를 사용하여 TLS를 통해 트래픽을 전송하는 SSL/TLS(Secure Sockets Layer/전송 계층 보안) VPN에 비해 위험성은 낮고 보안 수준은 높습니다[12].
- 강력한 암호화를 적용하는 VPN을 사용합니다. VPN이 FIP에서 검증된 강력한 암호화 알고리즘, 인증 알고리즘 및 프로토콜을 사용하는지 확인합니다. 모든 VPN이 MFA(다단계 인증)를 사용하도록 구성하고, 가능한 경우 암호 기반 인증 방식을 스마트 카드에 저장된 디지털 인증서를 사용하는 클라이언트 인증으로 교체합니다.[12].
- 소프트웨어 취약성을 관리합니다. 사이버 범죄자들은 VPN의 취약성을 악용하는 공격 벡터를 흔히 사용합니다. 취약성 패치 실적이 우수한 VPN 공급업체를 선택하고, SBOM(Software Bill Of Materials)을 요청하여 제3자 코드가 최신 상태이며 안전한지를 확인합니다. 또한 침입 가능성 감지를 위해 실행되는 코드의 유효성 검사를 수행할 수 있는 제품을 모색합니다. VPN 배포 후에는 소프트웨어 업데이트를 정기적으로 확인하여 즉시 적용합니다[12].
- 사용량 급증 상황에 대비합니다. IT 보안 담당자는 대규모 사용에 대비해 VPN 제한을 테스트해야 합니다[2].
- 무료 VPN 사용을 지양합니다. 무료 VPN 사용 시 광고 표시, 맬웨어 감염, 데이터 유출 등이 발생할 위험성이 있습니다[3].