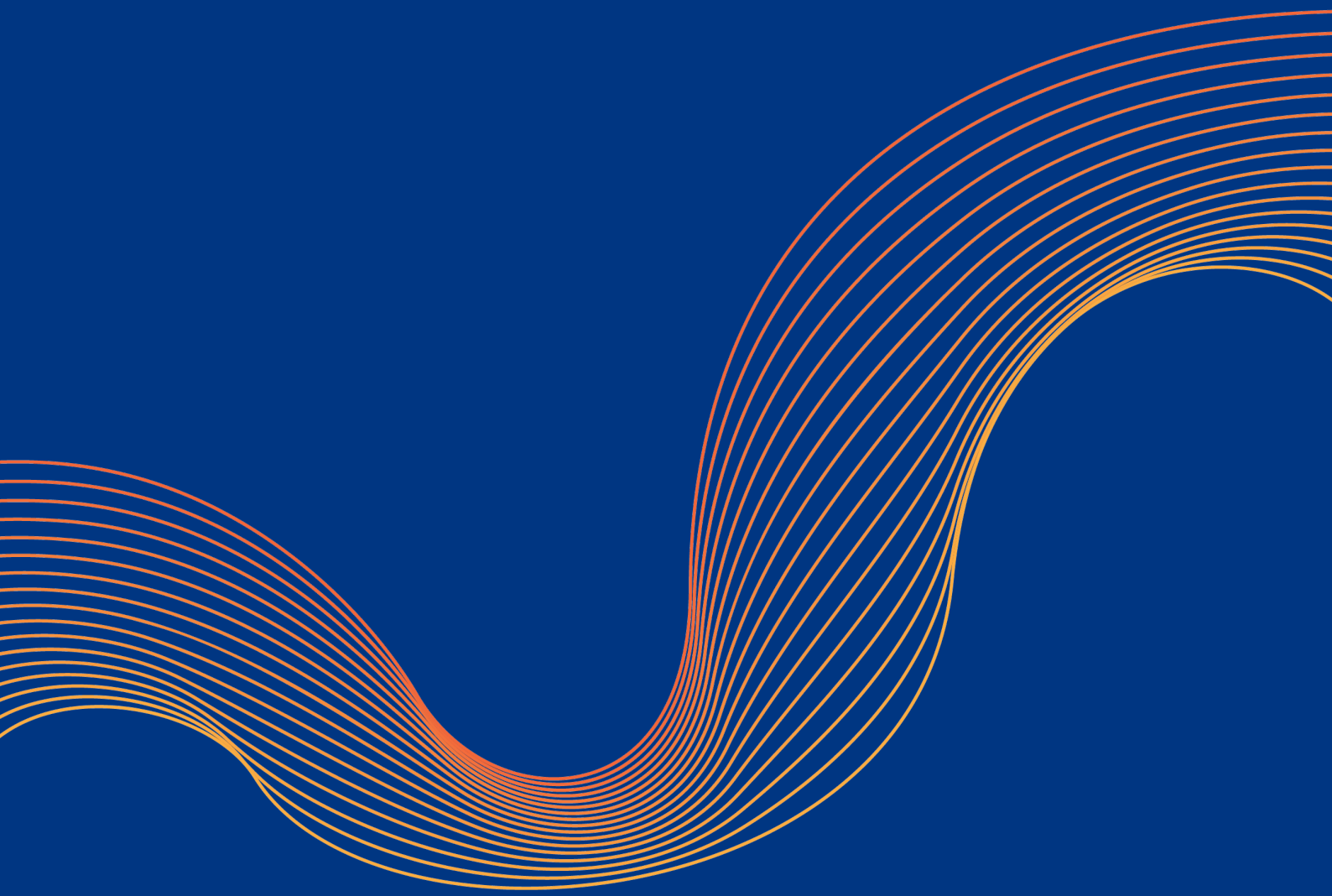
백서

CLOUDFLARE

ZTNA가 VPN을 대체할 수 있을까요? 3가지 원격 액세스 접근 방식을 비교합니다



+82 70 4515 6893 | enterprise@cloudflare.com | www.cloudflare.com

색인

소개

안전하고 원활한 원격 액세스는 비즈니스 조력자로서, 원격 사용자의 생산성을 높이고 IT 팀이 민첩성과 복원력으로 사용자-응용 프로그램 연결을 온보딩하고 유지하는 데 소요되는 시간을 줄입니다. 하지만 원격 액세스는 많은 조직에서 여전히 어려운 과제로 남아 있습니다.

아주 옛날에 VPN은 짧은 기간 동안 소수의 원격 사용자를 회사 네트워크에 연결하는 간단한 방법을 제공했습니다. 그러나 인력이 더욱 분산되고 조직에서 원격 사용자를 더 오랜 기간 안전하게 연결해야 했으므로 성능이 부진하고 보안 위험이 증가하며, 확장 가능성까지 우려되면서 이 접근 방식의 결함이 분명히 드러났습니다.

원격 액세스 요구 사항이 증가함에 따라 조직은 점점 더 기존의 VPN 구현에서 더욱 안전하고 성능이 뛰어난 원격 액세스 솔루션으로 전환하고 있습니다. Zero Trust Network Access, 즉 ZTNA는 특정 응용 프로그램, 사설 IP, 호스트 이름 주위에 보안 경계를 만듭니다. 이렇게 하여 기본값을 허용하는 VPN 연결을 기본값을 허용하지 않는 정책으로 대체하며, 이러한 정책은 ID와 컨텍스트에 기반해 액세스를 부여합니다.

2020년 전체 원격 액세스 사용량의 약 5%가 ZTNA에서 주로 사용되었습니다. 기존 VPN 액세스에 한계가 있고 더욱 정확한 액세스 및 세션 제어를 제공해야 하므로 이 숫자는 2024년까지 40%로 증가할 것으로 예상됩니다.[1]

ZTNA는 기업에 VPN에 비해 분명한 이점과 확장된 기능 몇 가지를 제공하지만, 많은 조직에서는 ZTNA가 VPN 인프라를 완전히 대체하지 못한다는 것을 발견했습니다. 하지만 ZTNA가 더욱 강력해지고 VPN이 더욱 문제가 되면서, 이는 빠르게 변화하고 있습니다. 이 백서에서는 VPN과 ZTNA 원격 액세스 솔루션을 대조하여 그 이점과 한계를 밝히고 마이그레이션 프로젝트를 위한 가장 중요한 고려 사항을 조명합니다. 이 백서에서는 Cloudflare가 ZTNA를 제공하는 방법을 설명하고 레거시 VPN 인프라를 원격 사용자를 위한 더욱 빠르고 안전한 Zero Trust 연결로 전환하기 위한 일련의 조치 단계를 권장합니다.

[1] Riley, Steve, MacDonald, Neil, and Orans, Lawrence. "Market Guide for Zero Trust Network Access." Gartner Research, https://www.gartner.com/en/documents/3986053/market-guide-for-zero-trust-network-access. 2021년 6월 21일 액세스함. 자세한 내용은 표 1 참조.

접근 방식 #1: 레거시 VPN

수십 년 동안 VPN을 통해 조직은 어느 정도의 프라이버시 및 보안으로 원격 사용자를 기업 네트워크에 연결할 수 있었습니다. 공격자가 데이터를 스누핑하거나 훔칠 수 있는 공용 인터넷을 통해 중요한 정보에 액세스하는 대신 VPN을 사용하면 사용자가 암호화된 연결로 내부 리소스에 안전하게 액세스할 수 있습니다.

VPN을 구현하는 가장 일반적인 두 가지 모드는 클라이언트 기반 VPN과 클라이언트리스 SSL-VPN입니다. 각각에는 다음과 같은 고유한 이점과 과제가 있습니다.

클라이언트 기반 VPN은 암호화된 터널을 통해 원격 사용자를 사설 네트워크에 연결합니다. 이 연결은 소프트웨어 응용 프로그램 또는 클라이언트를 통해 설정되며, 사용자는 해당 네트워크 내에서 모든 리소스에 지속해서 액세스하기 위해 사용자 이름과 비밀번호로 한 번 인증해야 합니다.

이점: 일단 연결되면 자유로운 수평 이동을 통해 사용자가 응용 프로그램에 액세스하고 내부 호스트에 연결함으로써 여러 리소스에 빠르게 액세스할 수 있습니다.

과제:

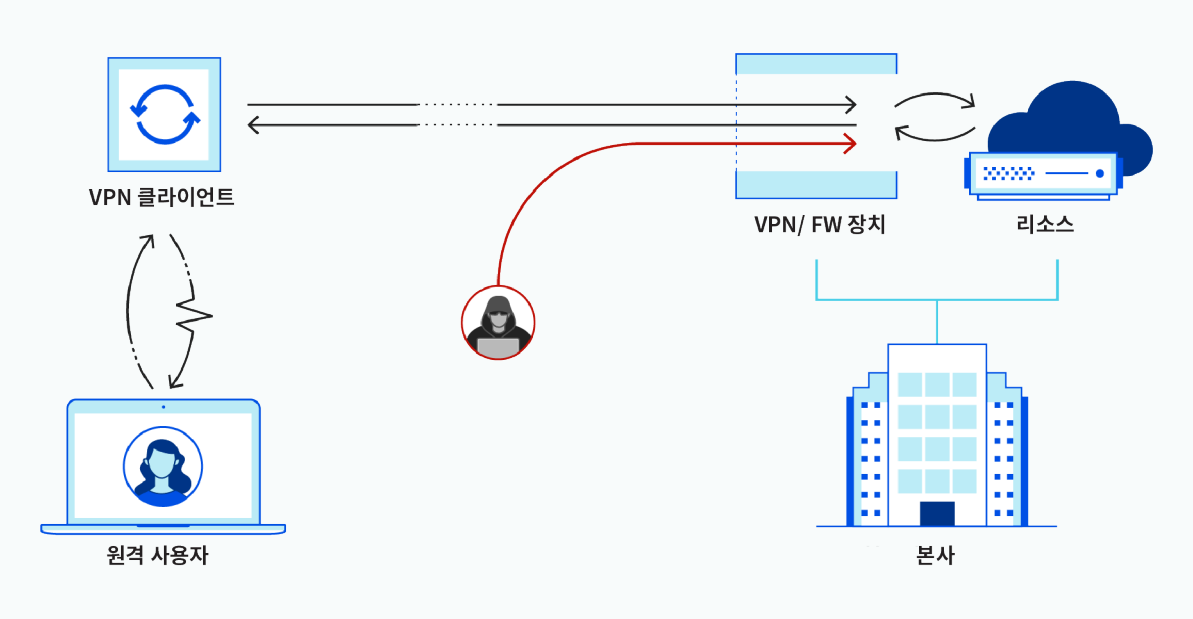
- **로밍하려는 사용자 및 모바일 장치용으로 설계되지 않았습니다.** 사용자가 로밍하면서 무선 네트워크가 위치마다 변경되므로 노트북과 모바일 장치가 모두 원활하게 다시 연결됩니다. 하지만 VPN 클라이언트가 이러한 재연결을 유동적으로 처리하는 데 능숙하지 않아 사용자가 VPN 클라이언트를 다시 시작하고 다시 인증하도록 반복해서 강제해야 하므로 생산성이 떨어지며 IT 티켓을 생성하게 됩니다.
- **가시성이 부족합니다.** VPN 인프라는 이 방법으로 데이터 센터 내부 방화벽 뒤에서 VPN 클라이언트의 암호화된 터널을 종료합니다. 이러한 연결은 로그되지만 사용자가 액세스한 응용 프로그램이나 응용 프로그램 내에서 취한 조치를 나타내는 응용 프로그램별 중앙 집중식 로그는 없습니다.

클라이언트리스 SSL-VPN 포털을 사용하면 소수의 원격 사용자가 사설 네트워크 내의 몇몇 브라우저 기반 응용 프로그램에 연결할 수 있습니다. 이 연결은 VPN 서비스를 실행하는 네트워크 장비에 내장된 웹 서버를 사용하여 이루어질 수 있습니다.

이점: 장치에서 클라이언트를 사용하는 대신 모든 웹 브라우저는 포털의 SSL 인증서를 사용하여 암호화된 HTTPS 연결을 설정하여 관리되지 않는 장치의 계약자를 지원할 수 있습니다.

과제:

- **보안이 우려됩니다.** 데이터 센터 내의 대부분의 VPN 설정은 사용자에게 전체 액세스 권한을 부여하며, 이는 계약자와 같이 직원이 아닌 사람이 중요한 리소스 및 응용 프로그램에 제한 없이 액세스하는 것을 원하지 않는 조직의 경우에는 문제가 됩니다.
- **많은 동시 사용자를 지원하도록 구축되지 않았습니다.** 최신 클라우드 서비스와 달리, 포털의 웹 서버는 더 많은 수요를 충족하기 위해 탄력적으로 확장될 수 없습니다. 대신 포털을 확장하려면 더 많은 네트워크 장비를 설치하고 부하를 분산해야 하며, 이는 장비의 나머지 기능이 충분히 활용되지 않을 수 있으므로 종종 비용이 많이 들고 복잡하며 비효율적입니다.
- **클라이언트리스 SSL-VPN 포털의 경우 방화벽 포트와 웹 서버가 공격에 노출됩니다.** 포털을 호스팅하는 웹 서버가 내부 응용 프로그램에 도달하려면, 관리자가 인바운드 방화벽 포트를 개방하여 이를 외부 공격에 노출시켜야 합니다. 개방된 포트와 웹 서버 자체는 DDoS 및 웹 응용 프로그램 공격으로부터 보호되어야 하며, 이 연결 방법을 보호하기 위해 더 복잡한 구성과 더 많은 비용이 필요합니다.



VPN은 원격 사용자에게 기본적인 수준의 프라이버시를 제공하지만, 보안 또는 확장 가능성을 염두에 두고 설계되지 않았습니다. 전통적으로 조직에서는 VPN을 사용하여 짧은 기간 동안 소수의 원격 사용자를 기업 네트워크에 연결했습니다. 하지만 원격 근무가 보편화되자 다음과 같은 VPN 문제가 증가하기 시작합니다.

- **사용자는 느린 성능을 경험합니다.** VPN 인프라에 직원이 생성한 트래픽 처리량 및 동시 연결을 처리할 수 있는 용량이 없는 경우, 사용자는 인터넷 연결 속도 저하를 경험합니다. 게다가 VPN이 액세스하려는 사용자와 응용 프로그램 서버 모두에서 멀리 떨어져 있을 때 이동 시간으로 인해 대기 시간이 발생합니다.
- **기업 네트워크는 공격에 취약합니다.** VPN은 일반적으로 성과 해자 모델을 사용하며, 이 모델에서는 사용자가 네트워크에 연결되면 모든 기업 리소스에 대한 무제한 액세스 권한이 부여됩니다. 중요한 인프라 및 데이터에 대한 액세스를 제한하는 기본 제공 방법이 없는 상황에서 조직은 차세대 방화벽 및 네트워크 액세스 제어와 같이 비용이 많이 들고 복잡한 보안 서비스를 구성해야 하거나 악의적인 수평 이동에 취약한 상태로 머물러 더 큰 데이터 유출을 초래할 수 있습니다.

호스트형 VPN 서비스의 과제

일부 공급자는 VPN 서비스를 실행하는 네트워크 장비를 하나 이상의 데이터 센터에서 가상 머신으로 실행하는 공용 클라우드로 전환했습니다. VPN은 추가 보안 서비스 또는 데이지 체인 방식을 통해 번들로 제공되거나 제공되지 않을 수 있습니다.

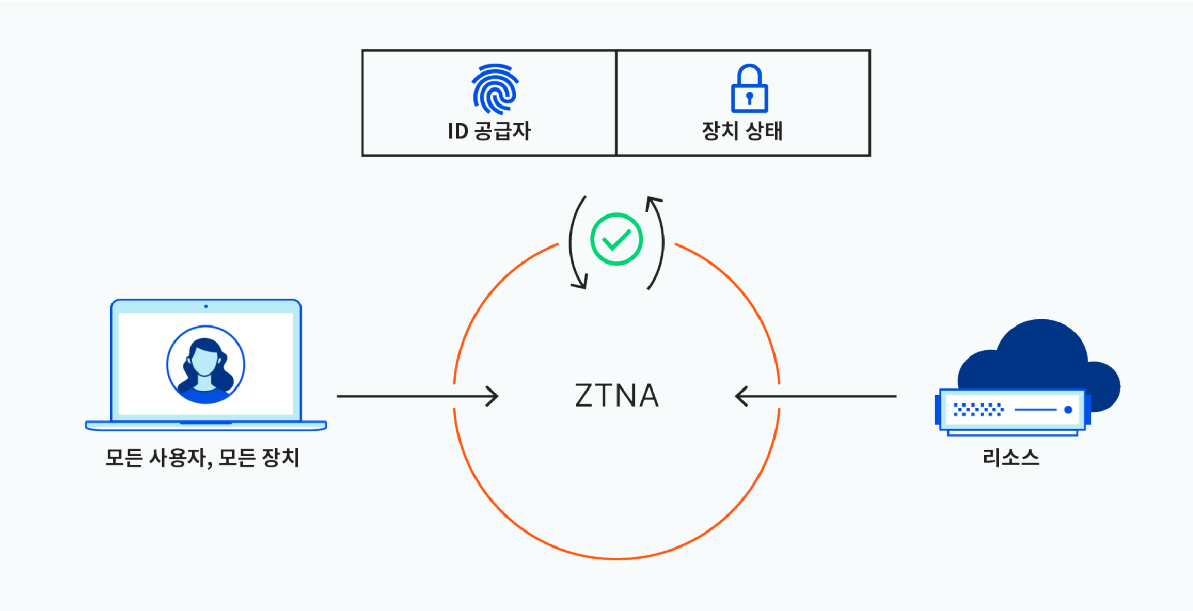
VPN을 클라우드에 배치하면 하드웨어 VPN 장비 고유의 확장 가능성 문제 중 일부를 해결하는 것으로 보일 수 있습니다. 하지만 그렇게 하면 몇 가지 중요한 보안 및 확장 가능성 문제도 발생합니다.

예를 들어 VPN과 방화벽 및 추가 보안 기능을 결합한 완전한 NGFW(차세대 방화벽)를 호스팅하는 조직을 고려해 보십시오. NGFW는 번들 서비스로 제공되므로 주문형 특정 기능을 독립적으로 확장하는 것은 불가능합니다. 하나의 기능을 확장하려면 전체 서비스를 확장해야 하며, 이렇게 하려면 각 VM에서 수행되는 소량의 컴퓨팅 부하를 분산하기 위해 더 많은 VM을 스핀업해야 합니다. 이는 비현실적이고 다루기 힘든 솔루션일 뿐만 아니라 조직의 원격 액세스 요구 사항이 계속 확장됨에 따라 큰 비용이 발생할 수 있습니다.

접근 방식 #2: ZERO TRUST NETWORK ACCESS

Zero Trust 보안은 VPN에 내재된 많은 문제를 우회합니다. 이는 기본적으로 네트워크 내부 또는 외부의 사용자나 장치는 신뢰할 수 없다는 원칙을 기반으로 합니다. 데이터 유출, 내부 공격 및 기타 위협의 위험과 영향을 줄이기 위해, Zero Trust 접근 방식은…

- 모든 로그인 및 요청을 인증하고 기록하며,
- 모든 사용자 및 장치에 대한 엄격한 확인을 요구하고,
- ID 및 컨텍스트를 기반으로 각 사용자와 장치가 액세스할 수 있는 정보를 제한하며,
- 전체적인 암호화를 추가하여 네트워크 내에서 응용 프로그램과 데이터를 격리합니다.



VPN과 마찬가지로 ZTNA를 구성할 수 있는 방법에는 여러 가지가 있습니다.

1. **클라이언트리스(또는 서비스 시작) ZTNA**는 클라이언트 대신 기존 브라우저를 사용하여 안전한 연결을 생성하고 사용자 장치를 인증합니다. 전통적으로 클라이언트리스 ZTNA는 HTTP/HTTPS 프로토콜을 사용하는 응용 프로그램으로 제한되지만, 호환성은 빠르게 진화하고 있습니다.[2]
   - **이점:** 클라이언트리스 ZTNA는 역방향 프록시 연결을 사용하여 응용 프로그램에 대한 직접 액세스를 방지하고, 사용자가 볼 권한이 없을 수 있는 응용 프로그램 및 데이터에 액세스하는 것을 차단하고 관리 시 관리자에게 더 큰 제어 및 유연성을 허용합니다.
2. **클라이언트 기반 (또는 엔드포인트 시작) ZTNA**는 제어 에이전트와 승인된 응용 프로그램 간에 암호화된 연결을 설정하기 전에 사용자 장치에 소프트웨어를 설치합니다.
   - **이점:** 클라이언트 기반 ZTNA를 통해 관리자는 장치 상태, 위치, 응용 프로그램에 액세스하는 사용자의 위험 상황에 대한 더 많은 통찰력을 얻을 수 있으므로 더욱 세분화된 정책을 수립하고 시행할 수 있습니다. 그리고 이 방법은 HTTP/HTTPS에 국한되지 않으므로 SSH, RDP, VNC, SMB, 기타 TCP 연결에 의존하는 응용 프로그램 등 더 넓은 범위의 비 HTTP 응용 프로그램에 액세스하는 데 사용할 수 있습니다.

[2] 2021년 6월 현재 Cloudflare의 ZTNA 솔루션은 SSH 및 VNC 응용 프로그램에 대한 클라이언트리스 액세스를 지원하며 향후 RDP를 위한 지원이 계획되어 있습니다.

ZTNA 구현의 과제

ZTNA는 기존 VPN에 비해 분명한 이점을 제공하지만, 원격 사용자를 위한 네트워크 액세스 보호 측면에서는 결점 없는 접근 방식은 아닙니다. 기업은 Zero Trust 채택의 장단점을 저울질하면서 다음과 같은 문제 중 하나 이상에 직면할 수 있습니다.

솔루션이 진정한 클라우드 네이티브가 아닙니다.

공급자가 클라우드 기반 ZTNA를 제공하지 않는 경우(즉, 고객이 자체 데이터 센터에 소프트웨어를 배포해야 함을 의미) 사용자는 즉각적인 확장 가능성 및 무제한 처리량과 같은 주요 이점을 놓치게 됩니다.

공급자가 클라이언트 기반 및 클라이언트리스 ZTNA 옵션을 제공하지 않을 수 있습니다.

이러한 옵션이 없으면 원격 데스크톱, SSH 응용 프로그램, 파일 공유 등의 비 HTTP 응용 프로그램에 사용자를 연결해야 하는 조직의 가치가 제한됩니다.

구성이 복잡하고 시간이 많이 소요될 수 있습니다.

(Terraform과 같은 도구를 통해) 정책 조정 및 자동화를 지원하지 않는 공급자는 ID 공급자에게서 이미 발생하는 구성 외에 관리자에게 더 많은 수동 작업을 도입할 수 있습니다.

원격 액세스에 대한 CLOUDFLARE의 접근 방식

원격 액세스 확보 및 확장은 원활한 프로세스여야 하며, 투박한 보안 솔루션을 계층화하거나 성능 상충 관계를 생성하거나 불필요한 비용을 발생시키지 않아야 합니다. Cloudflare는 다음과 같은 이점을 통해 팀에서 모든 원격 액세스 사용 사례를 처리할 수 있도록 지원합니다.

- **사용자 및 관리자를 위한 쉽고 위험 없는 온보딩.** Cloudflare는 기존 ID 제공자 및 엔드포인트 보호 플랫폼과 쉽게 통합하여 기업 응용 프로그램 및 리소스에 대한 액세스를 제한하는 Zero Trust 정책을 시행합니다.
- **클라이언트 기반 및 클라이언트리스 ZTNA 배포를 위한 유연성.** Cloudflare는 웹, SSH, VNC (및 곧 RDP) 응용 프로그램에 대한 연결을 위한 클라이언트리스 지원과 비 HTTP 응용 프로그램 및 내부 IP에 대한 비공개 라우팅을 위한 클라이언트 기반 지원을 제공합니다.

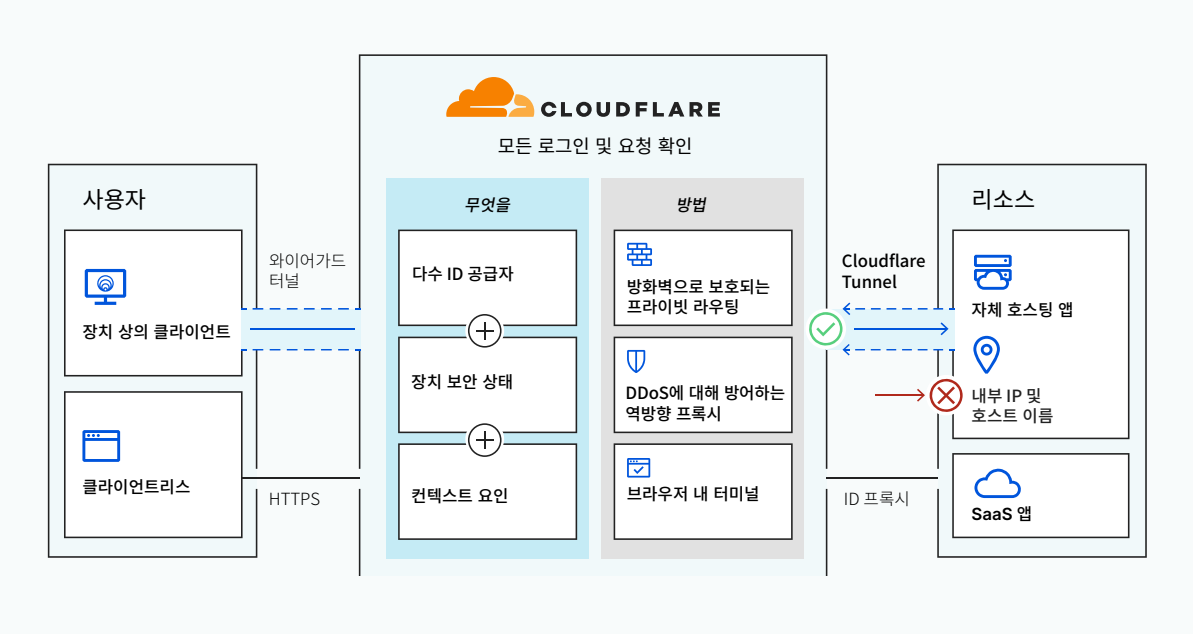


표 1: Cloudflare가 원격 액세스 문제를 해결하는 방법

⚠ 문제	✓ 솔루션	⚙ Cloudflare 구현
확장의 어려움	글로벌 에지 네트워크	확장 가능성 문제는 클라우드 네이티브가 아닌 VPN과 ZTNA 서비스에 문제를 일으켜 원격 사용자가 응용 프로그램과 데이터에 액세스하기 어렵게 됩니다. Cloudflare의 전역 Anycast 네트워크는 사용자 연결을 VPN보다 빠르게 만들 뿐만 아니라 크기와 관계없이 원격 인력이 관리자의 시간 소모적인 추가 구성없이 필요에 따라 기업 리소스에 안전하고 신속하게 연결할 수 있도록 합니다.
모바일 장치와의 호환성 부족	경량 클라이언트	IPSec 및 SSL 프로토콜을 사용하는 VPN 및 ZTNA 솔루션은 모바일 및 로밍 장치에서 종종 성능이 저하되는 경우가 있습니다. Cloudflare WARP 클라이언트는 사용자 공간에서 실행되는 더욱 현대적인 Wireguard 프로토콜을 활용하여 기존 옵션보다 더 빠른 사용자 경험을 통해 광범위한 OS 옵션 세트를 지원합니다. Cloudflare의 WARP 클라이언트는 Windows, MacOS, iOS, Android 및 곧 Linux 장치에서 구성할 수 있습니다.
통합되거나 취약한 DDoS 방어 기능 없음	업계를 선도하는 DDoS 방어 기능 내장	통합 DDoS 방어 기능이 없으면 조직은 종종 구성 문제, 확장 가능성 문제, 보안 과제를 발생시킬 수 있는 추가 보안 서비스를 데이지 체인 방식으로 연결해야 합니다. Cloudflare의 67Tbps가 넘는 네트워크는 모든 ZTNA 모드를 위한 내장형 DDoS 방어 기능을 제공하여 대규모 볼류메트릭 공격으로부터 네트워크를 보호합니다.
프로토콜 제한	비 웹 앱 지원	✓ 모드 호환성: SSH/VNC 응용 프로그램을 위한 클라이언트리스 ZTNA, 다른 모든 비 웹 응용 프로그램을 위한 클라이언트 기반 ZTNA.
통합 네트워크 방화벽 없음	기본 제공 네트워크 방화벽	기업 네트워크가 성장하면 조직이 균형을 맞춰야 하는 보안 하드웨어 스택도 성장하여 비용, 성능, 보안 측면에서 트레이드오프가 발생합니다. Cloudflare를 사용하면 관리자가 에지에서 네트워크 방화벽 정책을 시행할 수 있으므로 네트워크 안팎에서 허용되는 데이터를 세밀하게 제어하고 트래픽이 네트워크를 통과하는 방식에 대한 가시성을 향상할 수 있습니다. ✓ 모드 호환성: 클라이언트 기반 ZTNA
세밀한 제어 부족	내장형 보안 웹 게이트웨이 (SWG)	승인되지 않은 응용 프로그램을 사용하면 조직에 심각한 보안 문제가 발생할 수 있습니다. 엄격한 정책을 마련하지 않으면 사용자가 중요한 데이터 및 기타 기업 리소스에 액세스해서 이를 변경할 수 있습니다. ZTNA와 SWG를 결합한 Cloudflare를 통해 관리자는 응용 프로그램 내에서 사용자 및 장치 액세스 권한을 더욱 세밀하게 제어할 수 있으므로 사용자와 역할 기반 그룹이 필요한 리소스에만 액세스할 수 있습니다. ✓ 모드 호환성: 클라이언트 기반 ZTNA

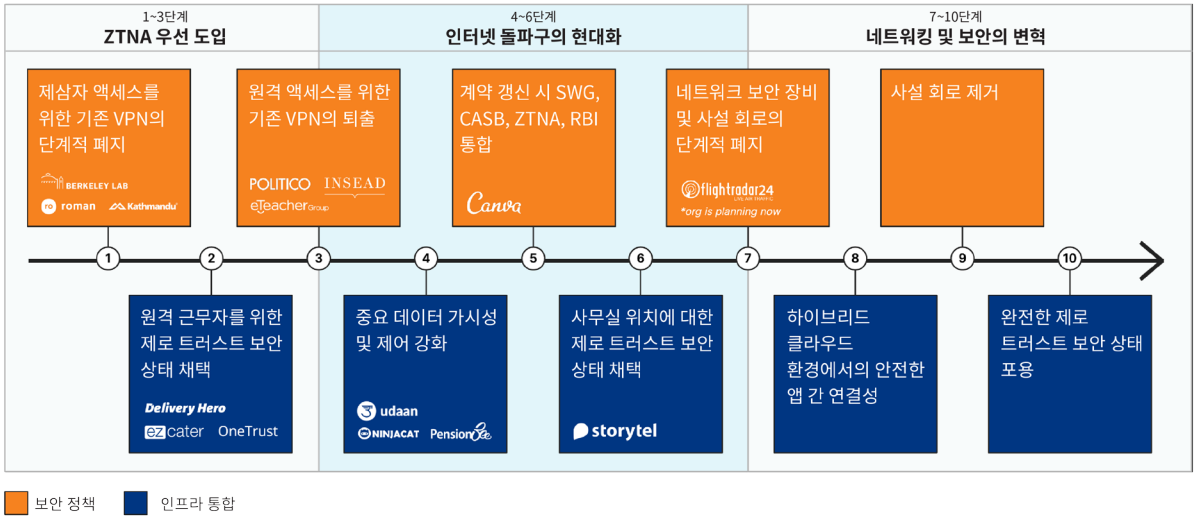
레거시 VPN을 ZERO TRUST NETWORK ACCESS로 교체합니다

VPN 없는 보안을 향한 길고 고통스러운 전환 과정에서 IT 보안 리더는 Zero Trust의 약속이 공허한 것으로 느낄 수 있습니다. 하지만 프로토콜 지원 또는 기능의 트레이드오프 없이 VPN을 Zero Trust Network Access로 교체하는 것이 가능합니다.

권장하는 마이그레이션 경로는 프로젝트를 추진하는 비즈니스 우선순위에 따라 다릅니다.

- 응용 프로그램에 대한 더 빠른 연결이 우선인 경우 **비 웹 앱을 위한 클라이언트 기반 ZTNA를** 먼저 배포합니다.
- 응용 프로그램 Access 규칙의 보안을 강화하는 것이 더 중요한 경우 **웹 응용 프로그램**으로 시작합니다.

VPN 교체는 전체 네트워크 전환의 첫 단계일 뿐입니다. SASE 모델로의 전환은 압도적일 수 있으므로 고객이 취한 접근 방식을 기반으로 Zero Trust 보안에 대한 공통 경로를 세분화했습니다.



Cloudflare의 Zero Trust 플랫폼이 VPN 의존도를 줄이고 궁극적으로 이를 대체하는 데 도움을 주는 방법을 자세히 알아보세요.

자세한 정보

VPN과 ZTNA 간의 실제 비교와 Cloudflare Access가 응용 프로그램 액세스를 위한 보안을 향상하는 방법을 확인하세요.

데모 보기

부록

인터넷 돌파구의 현대화

ZTNA 구현은 SASE(안전한 액세스 서비스 에지) 모델을 배포하는 중요한 단계입니다. **Cloudflare One**은 포괄적인 NaaS(서비스로서의 네트워크) 솔루션으로, 모든 규모의 팀을 위한 기업 네트워킹을 단순화하고 보호합니다. Cloudflare One을 통해 조직은 다음을 수행할 수 있습니다.

- **Zero Trust Access 수용.** 광범위한 보안 경계를 모든 리소스에 대한 모든 요청의 일대일 검증으로 대체합니다. 어떠한 사용자가 어떠한 위치에 있든 상관없이 기업 응용 프로그램의 모든 연결 지점에 Zero Trust 규칙을 실행합니다.
- **인터넷 트래픽 확보.** 인터넷상의 위협이 빠르게 발전할 때 이를 방어하기 위한 노력은 더욱 선제적으로 이루어져야 합니다. Cloudflare One은 모든 사이트에서 빠르고 완벽한 사용자 경험을 제공하는 Zero Trust 브라우저 격리를 실행함으로써 인터넷상의 위협으로부터 원격 근무 직원을 보호하며, 소중한 데이터가 조직 밖으로 유출되는 것을 방지하는 정책을 합니다.
- **사무실과 데이터 센터를 보호하고 연결합니다.** 기업 네트워킹은 지나치게 복잡해졌으며, 이는 사용자 트래픽이 목적지에 도달하기 위해 일반적으로 여러 홉을 거쳐 이동해야 함을 의미합니다. Cloudflare One을 사용하면 기업이 일관되고 통합된 하나의 클라우드 플랫폼을 통해 사무실과 데이터 센터를 보호할 수 있습니다.

Cloudflare One에 대해 자세히 알아보려면 10분 소개 및 데모를 시청하세요.

네트워크 변혁

곧 Cloudflare의 Zero Trust와 서비스 오퍼링으로서의 WAN이 하나로 통합되어 직원이 어디에서 일하든 일관성 있게 기업 리소스에 액세스할 수 있습니다.

오늘날 VPN 및 WAN 제품을 사용하면 직원이 비공개 기업 네트워크에 있는 리소스에 액세스할 수 있지만, 이들 제품의 경우 연결 및 보안 정책을 다르게 관리해야 합니다.

이제 Cloudflare는 통합 제어판을 제공하며, 다수의 포인트 제품을 동시에 관리할 필요 없이 전체 인력과 작업장에 동일한 Zero Trust 보안 정책을 적용할 수 있는 더 많은 유연성을 제공합니다.

자세한 내용은 https://www.cloudflare.com/cloudflare-one/을 확인하세요.

문서 유형