CLOUDFLARE

백서

네트워크 최신화를 위한 전략 개발

목차

3 **레거시 네트워킹: 디지털 최신화의 걸림돌**

4 **여정에 대한 이해**

5 **네 가지 핵심 네트워크 트래픽 경로**

6 **Cloudflare의 클라우드 연결성**

7 **네트워크 최신화 주요 사용 사례**

7 브랜치 연결

8 공개 인프라 보호

9 기업 네트워크 간소화

9 DMZ에서 마이그레이션

10 VPN을 ZTNA로 대체

10 LAN에 대한 과도한 신뢰 타파

10 M&A를 위한 연결 가속화

11 클라우드 연결 및 보호

12 **다음 단계**

레거시 네트워킹: 디지털 최신화의 걸림돌

비즈니스 상황이 급변하는 세계에서 민첩성은 살아남는 데 필수적인 요소입니다. 하지만 민첩성은 단순히 리더십과 의사결정의 문제가 아닙니다. 민첩성은 변화할 수 있는 조직의 능력에 달려 있기도 합니다. 시스템은 고장 없이 유연하게 적응할 수 있는 방식으로 구축되어야 합니다. 비즈니스는 새로운 수익 모델을 받아들이고, 새로운 애플리케이션을 지원하며, 전 세계를 연결할 수 있는 방식으로 재편성될 수 있어야 합니다.

조직에서 경쟁우위를 확보하기 위해 변화하는 과정에서 디지털 최신화를 통해 기대할 수 있는 주요 성과 중 하나가 민첩성입니다. 커뮤니케이션을 전달하고 협업을 지원하는 데 핵심적인 역할을 하는 기존 엔터프라이즈 네트워크의 상태를 고려하면 특히 그렇습니다. 엔터프라이즈 네트워크는 아직도 완고변화를 하게 거부하는데, 타당한 이유가 있습니다. 엔터프라이즈 네트워크는 시스템에 대한 충격을 견딜 수 있게 설계되었으며, 변화하려면 엄청난 비용과 수고가 듭니다.

클라우드가 데이터 센터에 미치는 영향과 같이, 점차적으로 나타나는 변화는 종종 예측할 수 있습니다. 네트워킹의 경우 외생적인 시장 원리가 하룻밤 사이에도 급박한 변화를 이끌어내고 있습니다. 예를 들어, 여러 기업은 원격 근무를 위한 인력을 신속하게 늘리고, 직원 생산성을 유지하며, 텅빈 사무실의 유휴 네트워킹으로 소모되는 예산까지 감안하여 비용을 관리하기가 얼마나 어려운지 팬데믹을 통해 뼈저리게 배워야 했습니다.

이 난관을 겪으면서 상황에 적응하여 오히려 더욱 번성하는 기업도 있다는 것 역시 여실히 드러났습니다. 올바른 비즈니스 의사결정을 내리는 경영진의 능력만이 다가 아니라 발빠르게 변화하고 결정을 과감하게 실행하는 비즈니스 역량 역시 중요했습니다. CIO의 입장에서는 변화에 대처할 전략을 개발하고, 미래의 니즈를 지원할 방안을 마련하며, IT 팀이 변화를 주저하기보다 촉진하도록 만들어야 합니다.

온프레미스 네트워킹에 대규모로 투자한 상황에서는 간단히 최신화를 결정할 수 없을 것입니다. 네트워크 최신화의 이점을 최대한 실현하려면 어떤 성과가 있을 것인지를 검토하여 무엇이 변해야 하는지를 정의해야 합니다.

여정에 대한 이해

몇 년에 걸쳐 이루어지는 네트워크 설계의 모범 사례를 생각하면 이렇게 복잡한 것도 당연한 일입니다. 조직에서는 네트워크를 구축한 이후 수십 년간 새로운 기술이 나올 때마다 여기에 더하고 더하면서 네트워크를 보강해 왔습니다. 네트워크 설계 세대마다, 새로운 혁신이 등장할 때마다 네트워크는 점점 더 복잡해졌습니다. 단순하게 만들어 볼 기회조차 없었으며, 새로운 기술이 추가되면서 속도, 탄력성, 보안이 더 복잡해지는 경우도 많았습니다.

클라우드 지원 네트워킹 및 보안 서비스가 있는 지금은 엔터프라이즈 네트워크 설계의 차세대 변화를 이끌 선두에 서있습니다. 네트워크를 확장하는 것처럼 클라우드 지원 서비스를 활용하는 조직은 새로운 사용 사례를 해결하고, 커버리지를 확장하고 데이터 센터 너머에서까지 애플리케이션을 보호할 수 있습니다. 다른 장비를 추가하기 위해 연결을 중단하지 않은 채로 클라우드 공급자의 PoP에 기존 네트워크를 연결하여 서비스를 제공하기 때문에, 네트워크를 크게 단순화할 수 있습니다. 온프레미스 네트워크와 클라우드 서비스 간 네트워킹은 그대로 유지되면서 클라우드 서비스에 포함된 서비스가 추가되어 사용됩니다.

문제는 모든 클라우드 지원 네트워킹 및 보안 플랫폼이 동일하게 설계되지는 않았으며, 서로 어떻게 다른지 늘 간단하게 확인할 수도 없다는 것입니다. 최신화 여정을 통해 누릴 수 있는 혜택이 제한되어 있는 경우도 많습니다. 그 차이를 이해하려면 네트워크 최신화의 목표를 구체화하여 기존에 복잡함을 초래했던 원인을 다른 원인으로 대체하기만 하는 경우가 없도록 해야 합니다.

네 가지 핵심 네트워크 트래픽 경로

네트워크 최신화 프로젝트의 범위를 정할 때에는 네트워크에 방대한 수의 접점이 있으며, 일부 접점은 같은 인프라에서 만나고(예: 트래픽이 코어 네트워크를 통해 인바운드, 아웃바운드, 이스트 웨스트로 이동), 일부는 네트워크 외부에서 운영(퍼블릭 클라우드 네트워킹 등) 된다는 점을 고려하세요.

인바운드 트래픽: 네트워크의 일부분이 인터넷에 노출되어 있다는 점을 고려할 때, 비즈니스를 무력화하거나 악용하려는 시도로부터 기업을 보호하기 위한 인바운드 방어 기능을 유지하면서도 정상 사용자의 트래픽은 통과할 수 있도록 허용해야 합니다. 기존의 경계 방어 솔루션은 공격에 제압될 수 있고, 분산 서비스 거부에 대처할 수 있는 성능을 필요로 합니다.

아웃바운드 트래픽: 인터넷 및 클라우드 기반 애플리케이션에 연결하려면 위협 보호 기능, 데이터 유출 방지 기능 등 안전한 비즈니스 사용을 위한 가드레일을 마련할 정책이 있어야 합니다. 사용자의 위치가 다양하다는 점을 고려해 조직에서는 방화벽(사용자가 네트워크상에 있을 때), DNS 확인자, 클라우드 기반 프록시(예:SWG 및 CASB, 사용자가 원격 상태일 때) 등 온프레미스 장비를 비롯한 아웃바운드 보호 기술을 혼합하여 마련했습니다.

WAN 네트워킹: WAN과 더불어 WAN이 커버하는 캠퍼스 및 브랜치 등의 경계는 클라우드 우선 이니셔티브와 IoT 지원 기기를 뒷받침할 수 있도록 새로 설계되고 있습니다. 그런데 전통 네트워크 토폴로지가 직접 인터넷 연결 아키텍처를 위한 데이터 센터로의 백홀을 어렵게 만들고 있습니다. 이 분야에서 네트워킹이 빠르게 발전하면서 역으로 보안 솔루션을 추가하기란 더 복잡해졌습니다. 많은 경우, 내부 트래픽 경로는 여전히 에지 배포 보안 장비에 의존하고 있고, 그래서 조직이 변화하는 데 방해가 되고 있습니다.

퍼블릭 클라우드 네트워킹: 조직이 클라우드 여러 곳에 애플리케이션을 만들면서 포인트별로 네트워킹 및 보안 구성을 구축하고 유지하기가 점점 어려워지고 있습니다. 네트워킹을 설정하고 관리하는 데에는 시간, 특히 프로젝트 개발에 써야 할 시간과 리소스가 많이 듭니다.

각 트래픽 경로마다 조직이 네트워크에 구축하는 기술이나 클라우드에서 사용하는 기술이 다양합니다. 최신화 프로젝트에서 여러 방향으로 트래픽 경로를 다루어야 한다는 점을 감안할 때, 변화로 얻을 수 있는 이점을 제한하는 아키텍처 관련 실수와 더불어 해결되지 않은 사용 사례를 해결하기 위해 이질적인 여러 기술을 필요로 하는 아키텍처 관련 실수를 피하려면 모든 방향을 다루는 네트워크 최신화 여정을 계획해야 합니다.

인바운드 트래픽
인터넷 트래픽으로부터 네트워크와 앱을 보호합니다.

퍼블릭 클라우드 네트워킹
퍼블릭 클라우드와 하이브리드 클라우드에서 앱을 연결하고, 보호하며, 구축하기 위한 네트워킹을 제공합니다.

아웃바운드 트래픽
위협으로부터 사용자와 사무실을 보호하고 사용 정책을 시행합니다. 애플리케이션의 데이터를 제어합니다.

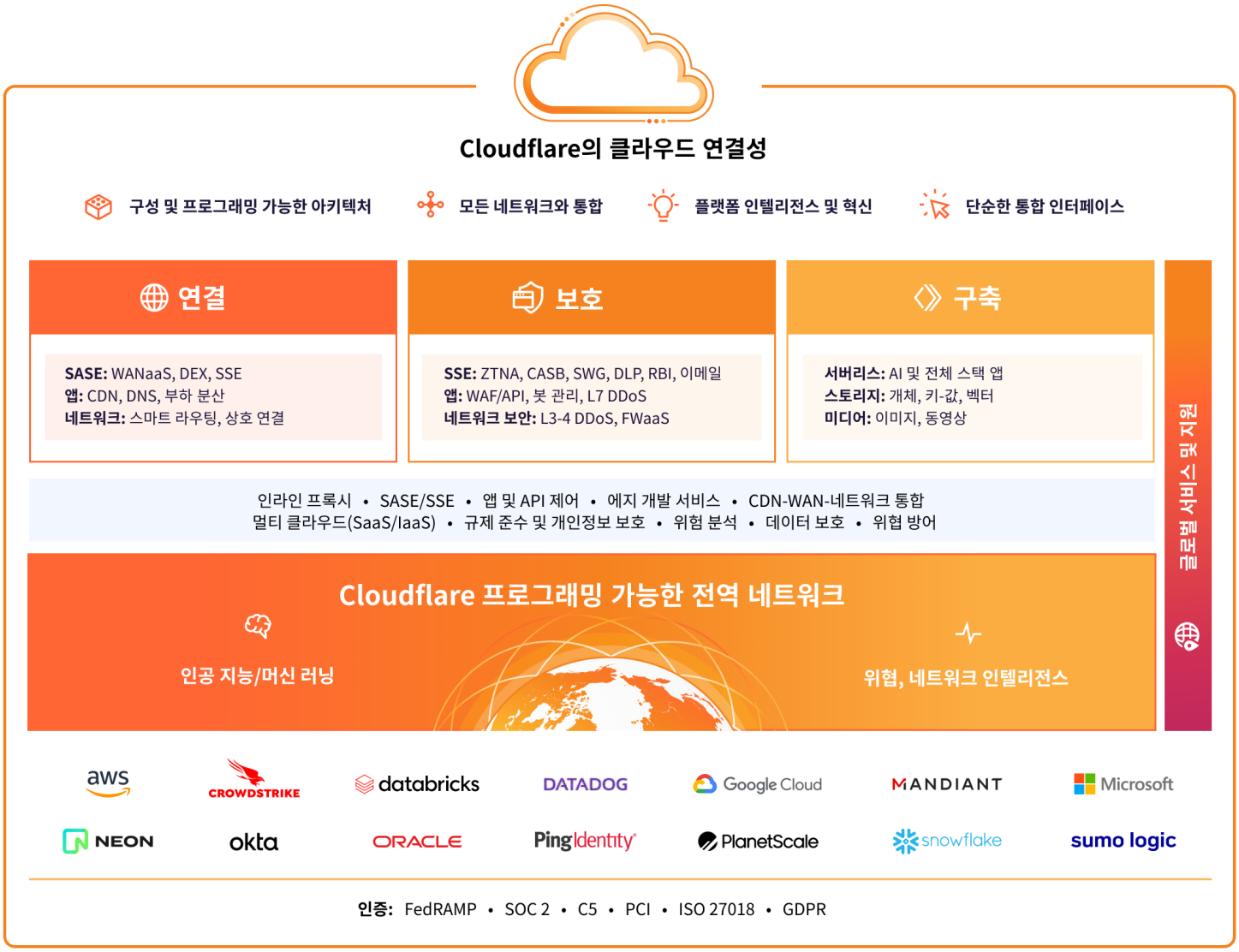
WAN 네트워킹
사무실, 사용자, 장치, 데이터 센터, 인프라를 연결하고 보호합니다.

Cloudflare의 클라우드 연결성

네트워크 최신화를 위해 Cloudflare 클라우드 연결성을 고려해 보세요. Cloudflare 클라우드 연결성은 사용자와 더불어 클라우드 지원 비즈니스 인프라 및 애플리케이션 전체에 네트워킹 및 보안 서비스를 제공할 수 있도록 구성 및 프로그래밍 가능한 아키텍처를 사용하는 원칙에 따라 구축되었습니다. 그 결과로 클라우드 연결성은 최신화 여정에서 현재와 미래의 요구 사항을 모두 충족합니다.

Cloudflare를 이용하면 장비를 추가하지 않고 서비스만 활성화하여 기능을 추가하고 새로운 사용 사례를 지원할 수 있습니다. Cloudflare Anycast 데이터 센터 연결은 동일하게 유지되며, 트래픽을 처리하기 위해 통합 관리 인터페이스에서 서비스를 구성하고 배포하면 됩니다. 현재 요구 사항을 충족할 수 있으며, 미래 사용 사례와 네트워크 최신화 여정 전체를 지원하기 위해 플랫폼을 도입할 수 있습니다.

전역 인프라를 구축하는 대신 Cloudflare 인프라를 사용해 보세요. 조직에서 Cloudflare 전역 네트워크를 통한 초고속 전송의 이점을 누릴 수 있습니다. 거의 모든 서비스 공급자 및 클라우드 공급자와 직접 연결되는 Cloudflare 네트워크는 전 세계 인터넷 연결 인구의 95%에 약 50밀리초 이내에 도달합니다.



네트워크 최신화 주요 사용 사례

먼저 조직에 비즈니스 관련된 영향을 미치며 이점이 유의미한 사용 사례들로 시작하세요. 사용 사례에 특정한 순서가 정해져 있지는 않습니다. 비즈니스마다 우선 순위가 다르기 때문입니다. 중요한 것은 단기적인 니즈를 충족하는 동시에, 어떤 경로를 따르든 네트워크 최신화 여정을 지원할 수 있는 아키텍처를 구축하는 것입니다.

	최신화 프로젝트
브랜치 연결 비용 절감, 사용자 경험 개선	• MPLS에서 클라우드 연결성으로 전환 • SD-WAN에서 클라우드 연결성으로 전환
공개 인프라 보호 FW, DMZ 투자 수명 주기 연장	• 네트워크 방화벽 부하 감소 • DMZ 보안을 클라우드 연결성으로 전환
기업 네트워크 간소화 Zero Trust 구현으로 보안 강화 및 자본비용 절감	• DMZ 축소 / 제거 • VPN을 ZTNA로 대체 • LAN에 대한 과도한 신뢰 타파 • M&A를 위한 연결 가속화
클라우드 연결 및 보호 앱에 최선의 클라우드 사용	• 앱 개발 및 보호 • 개발자 서비스를 활용해 핵심 기능 중앙 관리

브랜치 연결

WAN 네트워킹의 주요 요소는 사용자와 장치를 애플리케이션에 연결하는 기능을 의존하는 지사나 매장 등의 소규모 위치를 이어 주는 것입니다. 전통적인 허브 및 스포크 아키텍처는 값비싼 MPLS 회로를 이용하여 데이터 센터에 위치를 연결했지만, 클라우드 애플리케이션을 지원원할 필요성이 커지면서 광대역을 통한 직접 인터넷 연결 아키텍처를 사용하는 조직이 늘어나고 있습니다.

SD-WAN은 네트워크 연결을 더 안정적으로 만들기 위한 것이지만 보안 기능을 추가하는 측면에서는 불완전합니다. 대부분의 SD-WAN 아키텍처는 무거운 에지 장비와 로컬 방화벽에 의존하여 SD-WAN 패브릭에 보안 정책을 시행하고 있으며, 아웃바운드 트래픽에는 SSE/SASE 솔루션만 사용할 뿐입니다.

레거시 서비스를 강화하려고 하든, 아예 대체하려고 하든, 브랜치 연결과 마이그레이션 여정을 전적으로 뒷받침하는 Cloudflare의 클라우드 연결성을 사용해보세요. Cloudflare는 "에지는 가볍게 / 클라우드는 무겁게" 주의에 기반한 아키텍처를 통해 네트워킹 및 보안 서비스를 제공합니다. Cloudflare Magic WAN을 통해 지사, 리테일 매장, 공장 등 모든 네트워크 위치에 사이트 간 연결을 구축해보세요. Magic WAN은 기업 전체 네트워킹에 비용 복잡성과 운영 복잡성을 줄이면서도 안전한 고성능 연결과 라우팅을 제공합니다. 보안 측면을 고려하더라도, Cloudflare Magic Firewall은 Magic WAN과 원활하게 함께 배포되기 때문에 트래픽이 Cloudflare 네트워크에서 노스/사우스로 이동하든, 이스트/웨스트로 이동하든 네트워크 제어 정책을 원활하게 시행할 수 있습니다.

공개 인프라 보호

엔터프라이즈 네트워크 및 DMZ에는 자체 주소가 있고 인터넷에 노출되기 때문에 피해를 입히려는 공격자를 막을 수단이 필요합니다. 이상적으로는 기존의 네트워크 방화벽으로도 원치 않는 모든 트래픽을 가려내 차단할 수 있어야겠지만 어떤 방화벽이든 용량에 한계가 있습니다(가용 대역폭, 사용률/컴퓨팅, 세션 수 등). 결국 공격자의 성공 여부는 규모의 문제입니다. 다시 말해, 공격자가 여러 네트워크 프로토콜 계층에 회사의 운영 능력을 압도할 만큼 충분한 노이즈를 만들 수 있는지 여부에 달려 있는 것입니다.

단지 트래픽 용량만이 문제가 아닙니다. 인바운드 트래픽을 받을 때는 인증되지 않은 트래픽/사전 인증 트래픽에 대한 공격면이 생깁니다. 애플리케이션 및 운영 체제의 결함은 시스템 계정도 없는 공격자조차 악용할 수 있습니다. 다른 데이터 침해를 통해 알려진 사용자 이름/암호를 사용해 접속하는 자격 증명 스터핑 역시 엄청난 위험을 초래할 수 있습니다. 조직에서 DMZ 내 애플리케이션에 Zero Trust 정책을 적용한다면 인터넷 노출을 줄일 수 있고, 가능하다면 아예 없앨 수도 있습니다.

조직에서는 심층 방어 원칙을 적용하여 공개 인프라에서 유입되는 악의적인 트래픽 업스트림을 흡수해 버림으로써 네트워크 보호를 강화할 수 있습니다. Cloudflare Anycast 네트워크를 통해 배포되며 Magic Firewall을 기본 제공하는 Cloudflare Magic Transit은 조직에서 현관처럼 기능하면서 불필요한 악성 트래픽을 걸러내고 깨끗한 인바운드 트래픽만 전달합니다.

장비에서 네트워크 방화벽으로 DDoS를 완화하더라도, 연결을 차단할 수 있으려면 먼저 연결을 처리해야 합니다. Cloudflare 네트워크는 고객의 접두사를 브로드캐스팅하는 방식으로 경계 방화벽으로 향했을 트래픽을 유도합니다. Anycast의 힘으로 Cloudflare는 모든 데이터 센터에 고루 부하를 분산함으로써 DDoS 공격을 효과적으로 흡수해 냅니다. 봇넷들은 가장 가까운 Anycast PoP를 찾아 Magic Transit 및 Magic Firewall 정책에 따라 트래픽을 처리합니다.

기업 네트워크 간소화

단순화하면 최신화 관련 이점이 많습니다. IT 팀에서는 설계상 고장날 수 있는 구성 요소 수가 적을수록 더 안정적으로 네트워크를 유지할 수 있고, 액세스 권한에 Zero Trust '모두 거부' 접근법을 취함으로써 보안을 강화할 수 있습니다.

네트워크 단순화를 위한 고려 사항:

DMZ에서 마이그레이션

네트워크 DMZ는 특히 제로 데이(zero-day) 익스플로잇에 민감하기 때문에 운영 측면에서 골칫거리입니다. 공격자가 DMZ 내 서버와 통신하는 데 내부 네트워크 액세스가 필요하지 않으므로, 조직에서 익스플로잇과 남용을 방지하려면 촉각을 곤두세워야 합니다.

그런데, 과거에 중요한 역할을 맡았던 DMZ가 오늘날에도 필요할까요? 네트워크 구성 요소로서 DMZ의 중요성은 옅어지고 있습니다. 애플리케이션을 구축하여 호스팅할 수 있는 다른 방법이 있기 때문입니다.

- 공개 앱의 경우, 워크로드를 퍼블릭 클라우드로 이전할 때 경제적이고 기술적인 이점이 있습니다.
- SaaS 방식에서는 대부분의 공개 애플리케이션 및 비공개 애플리케이션을 고객 관리 인프라에서 실행할 필요가 전혀 없습니다.

이와 같이 보안 및 네트워크 설계 관점에서 매우 실용적이기 때문에 DMZ의 필요성을 줄이거나 아예 없애는 방법을 고민할 수 있게 됩니다. 운영 측면에서도 매우 합리적이지만 방화벽, WAF, 그리고 이를 지원할 부하 분산 장치 같은 네트워크 인프라가 사라지니 아키텍처 역시 크게 단순화할 수 있습니다.

직원, 파트너, 계약업체로 액세스를 확대하기 위해 DMZ에 마련된 비공개 앱은 어떨까요? 비공개 네트워크에 비공개 앱을 격리하여 직원 및 파트너의 액세스를 확대할 때에는 Zero Trust 네트워크 액세스(ZTNA)를 사용하면 훨씬 안전합니다.

ZTNA를 사용하면 애플리케이션에 인바운드 네트워크 트래픽이 없어지기 때문에 공격면을 효과적으로 줄일 수 있습니다. ZTNA는 Cloudflare의 클라우드 연결성을 통해 컨텍스트에 맞으며 브로커가 적용된 액세스를 리소스에 사용합니다. 네트워크 방화벽의 포트를 열 필요도 없고, 어떤 리소스에 누가 접근했는지 보안 팀에서 완벽하게 파악할 수 있다는 장점도 있습니다.

VPN을 ZTNA로 대체

VPN을 이용해 애플리케이션에 액세스하는 경우가 줄어들고 있습니다. 사용자가 인터넷과 클라우드에 액세스할 때마다 아주 긴 터널을 지나야 한다면 네트워크 설계 관점에서 매우 실용성이 떨어집니다. 사용자(그리고 잠재적으로 손상된 엔드포인트)가 VPN을 통해 네트워크에 접속하는 방식은 보안상으로도 위험이 큽니다.

애플리케이션 액세스만이 VPN의 유일한 기능인 것도 아닙니다. 조직에서 엔드포인트 관리, 서버 개시 커뮤니케이션 등 엔드포인트와 네트워크를 더 폭넓게 연결해야 하는 경우를 생각해 보세요. 전통적으로 이러한 사용 사례에서는 양방향 모두 VPN의 네트워크 연결 기능을 활용하고 있으며, VPN이 시장에서 초기 ZTNA 제품을 압도했습니다. 마땅한 대안이 없었기 때문에 조직은 ZTNA와 VPN을 함께 운영했습니다.

네트워크 인프라를 최신화하려는 조직은 Cloudflare의 ZTNA와 기능을 통합하면 됩니다. 조직에서 Cloudflare를 이용하면 전형적인 ZTNA 사용 사례와 서버 개시 트래픽, 양방향 트래픽까지 모두 지원할 수 있기 때문입니다. 조직에서는 이러한 기능을 통해 VPN에서 벗어나 애플리케이션 액세스 요구량을 줄이고, 나아가 보안을 강화하면서도 단순성의 이점을 누릴 수 있습니다.

LAN에 대한 과도한 신뢰 타파

하이브리드 근무 시, 사무실에서 근무하는 방식과 다른 위치에서 근무하는 방식 간 차이는 점점 사라져 가고 있습니다. 사용자가 커피숍이나 공용 오피스 같은 신뢰할 수 없는 공개 네트워크에서 자주 근무한다면 특히 그렇습니다.

어떤 면에서 개방된 공개 네트워크는 Zero Trust의 전형이라고 할 수 있습니다. 권한이 부여된 액세스를 가진 사람은 아무도 없고, 누구도 무엇도 믿을 수 없습니다. 원칙상 공용 오피스, 홈 오피스, 커피숍에서 일할 수 있다면 엔터프라이즈 네트워크에서도 신뢰 가능성을 없앨 수 있지 않을까요?

신뢰 가능성을 없앤다고 해서 네트워크 설계를 발전시켜야 필요는 없습니다. 오히려 단순해질 수 있습니다. 인증 사용자용으로 따로 상급 액세스를 만들고 리소스 연결을 열기 위한 네트워크 정책을 적용하는 대신, 전체 네트워크를 신뢰할 수 없다고 가정하는 편이 훨씬 안전합니다. 조직에서 SASE를 통한 보안 표현식을 이용한다면 네트워크 자체에 대한 신뢰를 가정할 필요 없이 애플리케이션을 안전하게 보호하는 적절한 보안 기능으로 필요한 애플리케이션에 액세스할 수 있습니다. Zero Trust는 네트워크에 신뢰를 더하는 것이 아닙니다. 과거의 명시적이고 과도한 권한 없이, 더 확실하고 안전한 상태에 도달할 때까지 신뢰를 없애는 것입니다.

M&A 활동을 위한 연결 가속화

조직에서는 다른 방식이었다면 즉시 이용할 수 없을 비즈니스 리소스 및 성능을 이용할 수 있는 권한을 얻으려는 수단으로 M&A를 활용합니다. 이 기회를 제대로 살리려는 조직은 따로 떨어진 부분을 합쳐놓은 회사가 아니라 하나로 뭉친 회사를 만들기 위해 발 빠르게 움직여야 합니다. 하지만 두 조직의 애플리케이션과 근간 네트워크 인프라가 쉽게 통합되는 경우는 극히 드물기 때문에 IT 팀에서 빠르게 움직이기는 어렵습니다.

조직에서 M&A를 위한 연결을 가속화하려면 애플리케이션 액세스가 네트워크 통합과 별도의 작업인 것처럼 접근해야 합니다. 통합 네트워크 아키텍처를 설계하는 데에는 몇 년이 걸릴 수도 있지만 애플리케이션 액세스의 경우 그렇게 먼 마일스톤에 따를 필요가 없습니다.

신뢰할 수 있는 사용자가 신뢰할 수 없는 네트워크에서도 애플리케이션에 액세스해야 하는 1일차의 상황이 사실상 Zero Trust 사용 사례인 이유도 거기에 있습니다. 통합 네트워크 액세스에 의존하지 않고도 M&A 시 연결할 수 있는 수단을 제공하는 Cloudflare One으로 액세스를 확대하세요.

클라우드 연결 및 보호

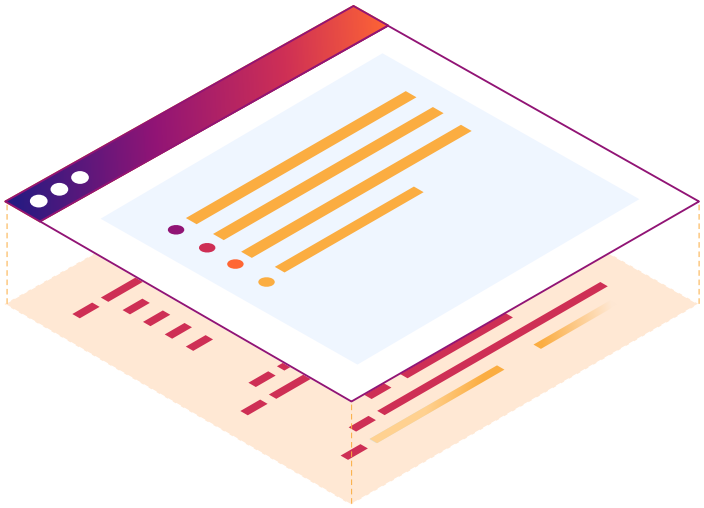
클라우드 개발이 계속 진화하고 있으니, 한 클라우드의 구성 요소를 다른 클라우드에서 용도에 맞게 개조할 수 있다는 장점도 생길 것입니다. 점차로 모든 조직이 결국 멀티 클라우드 조직이 된다면, 모두 퍼블릭 클라우드 네트워킹을 관리하게 될 것입니다. 애플리케이션 개발 시 자연스럽게 고유한 방식이 만들어지는 경향이 있습니다. 조직 내 여러 부서의 DevOps가 가장 익숙한 도구를 이용하려 하기 때문입니다. 그런데, 클라우드 연결성을 관리하기 위한 조직 역량을 키우려면 이렇게 완전히 다른 프레임워크를 기반으로 개발된 도구 세트들을 이용해야 하기 때문에 복잡합니다.

멀티 클라우드가 복잡한 또 다른 이유는 하이브리드 클라우드 때문입니다. 하이브리드 클라우드는 온프레미스 프라이빗 클라우드와 가상 프라이빗 클라우드의 조합입니다. 이 네트워크는 AWS Direct Connect 등의 전용 네트워킹으로 설계되곤 하는데, 이러한 네트워킹은 비용이 많이 들고 하나의 클라우드에 종속될 수도 있습니다. 조직에서 멀티 클라우드 애플리케이션을 개발하더라도 클라우드 각각의 전용 네트워킹 비용을 감안하고 싶지는 않을 수 있습니다.

하나의 애플리케이션에서 다른 애플리케이션으로 네트워킹 및 보안을 직접 구축하는 대신, Cloudflare를 통해 여러 퍼블릭 클라우드 네트워킹 서비스를 오케스트레이션하고 연결하세요. Cloudflare의 클라우드 연결성은 이러한 아키텍처에서 이상적입니다. 클라우드 연결성은 방대한 Cloudflare 네트워크를 통해 클라우드 사이를 이동하는 트래픽에 이상적인 교통 요충지가 될 것입니다. 고객은 이제 퍼블릭 클라우드 네트워킹 관리 기능을 추가하여 Cloudflare를 통해 워크로드 연결 설정을 오케스트레이션할 수도 있습니다.

Cloudflare의 퍼블릭 클라우드 네트워킹은 기본적인 배관 작업의 오케스트레이션 그 이상으로 뻗어갈 수 있습니다. Cloudflare 아키텍처는 멀티 클라우드 애플리케이션 개발 및 통합에 사용할 수 있는 개발자 서비스까지 제공하여 한 발 더 나아갑니다. 개발자 플랫폼은 오픈 소스와 공개 표준에 기반한 기초 기술로 풍부하게 구성된 생태계를 제공합니다. 개발자 플랫폼의 모든 요소를 사용해도 되고, 몇 가지만 선택해 사용해도 됩니다. 특정 클라우드 내 특정 서비스로 제약할 필요도 없습니다.

다음 단계



귀사의 네트워크 최신화 여정에서 다음 단계로 나아가려면 Cloudflare에 연락해 전략 개발에 도움을 받으세요. Cloudflare는 이미 수천 곳의 고객과 긴밀하게 협력하여 고객의 아키텍처를 클라우드 연결성으로 바꾸었습니다.

자세한 내용은 http://www.cloudflare.com/ko-kr/을 참고하세요.

© 2024 Cloudflare Inc. All rights reserved.
Cloudflare 로고는 Cloudflare의 상표입니다. 기타 모든 회사
및 제품 이름은 관련된 각 회사의 상표일 수 있습니다.

007-9814-2030-192 | enterprise@cloudflare.com | cloudflare.com/ko-kr

REV:BDES-5483.2024JAN30