백서

Beyond SD-WAN:

제로 트러스트 보안과 기업 WAN으로서의 인터넷

SD-WAN, 보안 접속, 위협 방어가 하나인 이유

Akamai

기업 광역 네트워크의 미래

광역 네트워크(WAN)는 컴퓨터 간 통신의 초창기인 1960년대부터 존재해 왔습니다. WAN은 기술이 발전하고 트래픽 수요가 증가하면서 지속적으로 발전되고 개선되었습니다. 오늘날의 기업에 있어 WAN은 다양한 위치에 통합 네트워크를 제공하는 인프라입니다.

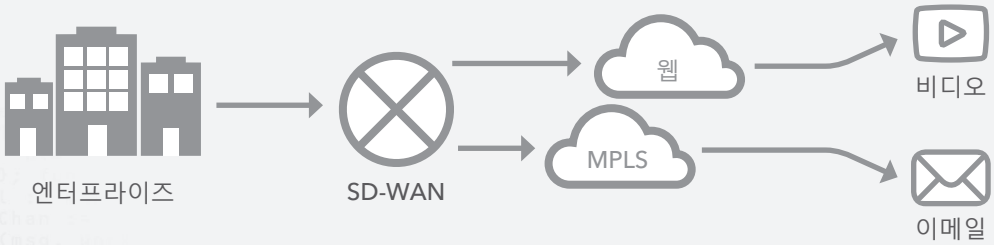
하지만 이 중요한 기술적 토대에는 제약이 존재합니다. WAN은 종종 대역폭이 부족해 특정 애플리케이션의 성능에 문제를 일으키고, 안정성에 변동이 발생하며, 비즈니스에 보안 리스크를 발생시킬 수 있습니다. 또한, WAN은 주로 전용 회선에 구축되거나 인프라에 공용 인터넷과 더불어 회선 교환이나 비동기 전송 모드(ATM), 멀티프로토콜 라벨 스위칭(MPLS)과 같은 패킷 교환 방식을 사용하는 서비스 사업자의 전용 서비스로 제공됩니다. 후자가 비용이 덜 드는 옵션이기는 하지만 여전히 매우 고가이고 확장성 측면에서도 적합하지 않습니다.

혁신 중인 기업 네트워크

기업들은 이러한 성능, 보안, 비용 문제에 대응하기 위해 소프트웨어 정의 WAN(SD-WAN)을 도입해 비용을 줄이고 민첩성을 개선하고 있습니다.

데이터센터에서 처음 사용된 네트워크 기능 가상화(NFV)와 소프트웨어 정의 네트워크(SDN)의 혁신 과정에서 등장한 이 기술은 조직을 연결하는 네트워크를 위해 IT 부서에서 발빠르게 도입했습니다.

SD-WAN은 간단히 말해 데이터와 광역 네트워크의 제어 영역을 분리합니다. 혼합 WAN 데이터 연결인 MPLS, ATM, 인터넷의 성능을 모니터링하고 현재 링크 성능, 연결 비용, 애플리케이션이나 서비스의 필요성에 기반하여 각 트래픽 유형에 가장 적절한 연결을 선택합니다



SD-WAN의 작동 방식

SD-WAN은 지연 시간 발생이 큰 문제가 되지 않으며 비트당 비용이 가장 저렴하기 때문에 이메일을 MPLS로 라우팅할 수 있습니다. 반대로, SD-WAN은 화상 회의 트래픽을 최적의 성능과 최소한의 지연 시간을 보장하기 위해 비트당 비용이 더 높은 인터넷으로 라우팅할 수도 있습니다.

인터넷이 새로운 기업 WAN이 될 수 있을까요?

SD-WAN은 퍼블릭 인터넷을 포함한 여러 전송 서비스를 사용한다면 확실히 유연하고 효과적이며 경제적일 수 있습니다. 하지만 해당 전송 옵션에 대한 성능 보장이나 SLA가 없기 때문에 성능이 중요하지 않은 애플리케이션에는 인터넷만 사용합니다.

기존의 SD-WAN 구축과 공존하는 방식으로 기업 WAN 트래픽을 보다 효율적이고 경제적이며 안전하게 제공하도록 인터넷 사용을 늘리려면 인터넷의 근본적인 한계를 없애는 접근 방식을 채택해야 합니다. 한 가지 방법은 비즈니스 애플리케이션을 안전하고 빠르며 안정적으로 전송하면서 애플리케이션을 퍼블릭 인터넷에 노출시키지 않는 엣지 플랫폼을 사용하는 것입니다. 이를 통해 인터넷으로 더 많은 트래픽을 전환하면서 비용을 절감하고 현재 SD-WAN에 대한 투자를 극대화할 수 있습니다.

최신 기업 네트워크의 추세로 미루어 보면 기업 트래픽의 상당 부분을 인터넷으로 라우팅하는 것은 합리적인 방법입니다. 다양한 모바일 사용자 및 디바이스와 함께 클라우드 워크로드의 증가는 이미 이러한 워크플로우가 인터넷에 크게 의존하고 있다는 의미입니다. 그리고 이 추세는 계속 확산될 것입니다.

여기서 한 단계 더 나아가 안전하고 확장 가능하며 효율적인 기업 WAN을 인터넷에 구현할 수 있다면 어떨까요?

본 백서에서는 네트워크를 SD-WAN과 제로 트러스트 보안으로 혁신하는 과정, SD-WAN을 넘어서는 혁신을 위해 조직을 포지셔닝하는 방법, 완전한 인터넷 기반의 기업 네트워크를 도입하는 방법을 살펴봅니다.

엣지 플랫폼은 안전하고 빠르며 안정적인 비즈니스 애플리케이션을 인터넷을 통해 전송하면서 퍼블릭 인터넷에 애플리케이션을 노출시키지 않습니다.

> 2023년 말까지 WAN 엣지 인프라 갱신 이니셔티브의 90% 이상이 기존 라우터(현재 최대 40% 이하) 대신 vCPE(Virtualized Customer Premises Equipment) 플랫폼이나 소프트웨어 정의 WAN(SD-WAN) 소프트웨어/애플리케이션을 기반으로 할 것으로 보입니다."
>
> - Gartner, Magic Quadrant for WAN Edge Infrastructure, 2018년 10월

SD-WAN의 가치

SD-WAN은 주로 링크 밸런싱, 자동 디바이스 설정, 써드파티 보안 서비스 추가 기능을 제공합니다. 이러한 기능은 사용자 경험 개선, 링크 비용과 운영 비용의 감소 등 상당한 효과를 제공할 수 있습니다. 활용도가 뛰어나며 성능도 입증되었습니다.

여러 벤더사에서 SD-WAN 기능을 제공하고 있지만, 다음과 같이 크게 3가지 카테고리로 일반화할 수 있습니다.

1. 탄력적인 링크 제어
2. 관리 역량
3. 서비스 삽입

탄력적인 링크 제어

첫 번째 기능인 탄력적인 링크 제어는 SD-WAN의 주요 기능입니다. 클라우드가 많은 조직에서 주요 목표가 되어감에 따라, 전용 네트워크에서 실질적인 중앙 집중식 컨트롤 포인트로 기능하는 데이터센터로 트래픽을 백홀하는 것은 실용적이지 않습니다. SD-WAN은 동적 라우팅 선택을 비롯한 지능적인 트래픽 제어로 이 문제를 해결합니다. 또한, 데이터센터를 통하지 않고 트래픽을 클라우드로 전송하는 로컬 또는 지사 인터넷 브레이크아웃(다이렉트 인터넷 접속(DIA)이라고도 불림)을 설정합니다. 음성 및 비디오를 포함한 레거시 애플리케이션은 MPLS 링크로 지정되며 클라우드 애플리케이션과 인터넷 트래픽은 인터넷으로 바로 전송됩니다.

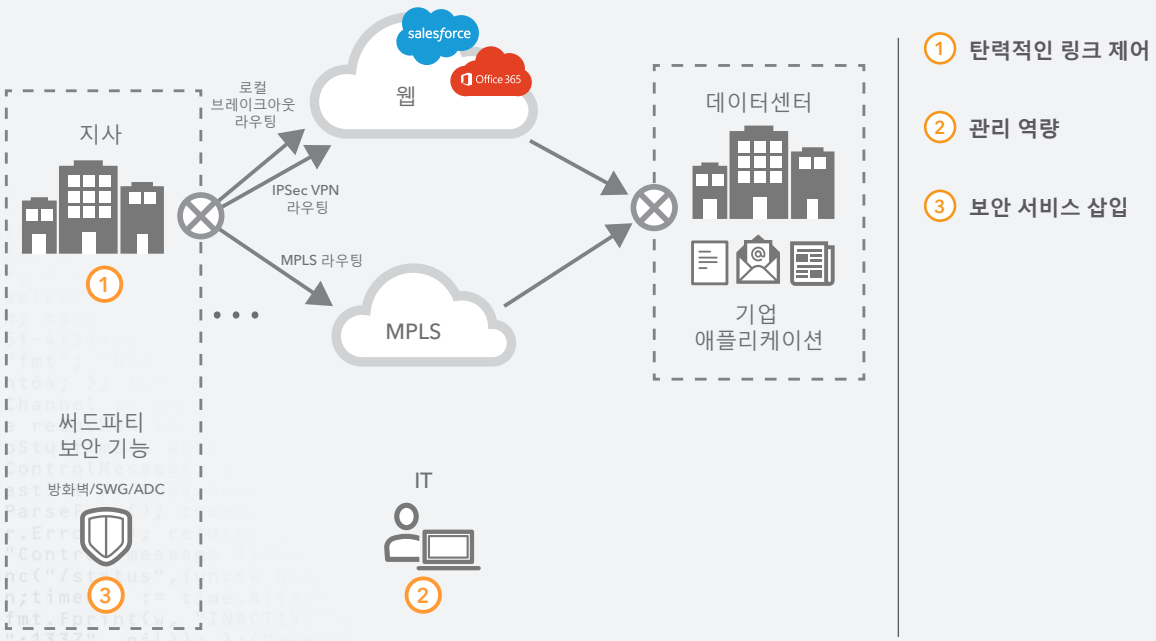
관리 역량

SD-WAN 벤더사에서는 관리 역량을 제공하여 네트워크 디바이스의 운영과 관리를 간소화합니다. 기업 WAN은 1990년대부터 멀티레이어 스위치 및 라우터와 같은 네트워크 디바이스로 구성되었습니다. 이 디바이스는 대체로 어플라이언스 기반으로 관리되었습니다. 다시 말해서, 관리자는 전체 조직의 수백 또는 수천 대에 달하는 디바이스를 개별적으로 설정 및 유지하고, 각 디바이스의 소프트웨어 스택을 모니터링해야 합니다. 디바이스가 동적으로 라우팅 정보를 교환하거나 라우팅 프로토콜을 사용하여 고가용성을 구현하더라도 막대한 노력이 필요합니다. SD-WAN을 사용하면 중앙화된 단일 콘솔에서 모든 디바이스를 관리할 수 있습니다.

서비스 삽입

서비스 삽입에 전문성을 갖고 있는 SD-WAN 제공업체도 있습니다. WAN의 최소 요구사항은 IP 연결, 다시 말해 조직 전체의 레이어 3 네트워크 연결입니다. 네트워크가 발전함에 따라 보안 기능도 발전했는데, 몇가지 예로는 방화벽, 침입 방지 시스템(IPS), 애플리케이션 전송 컨트롤러 등이 있습니다. 과거에는 네트워크에 이러한 기능을 추가하려면 해당 서비스를 제공하는 디바이스가 일반적으로 동적 라우팅 프로토콜(최단 경로 우선 프로토콜[OSPF], 경계 게이트웨이 프로토콜[BGP])과 통신할 수 없었기 때문에 복잡한 라우팅 설계가 필요했으며, 이로 인해 고정 라우팅과 재배포의 복잡한 조합을 야기하게 됩니다. SD-WAN은 보통 써드파티가 제공하는 이러한 기술을 통합 포털을 통해 손쉽게 설정하고 간편하게 관리하도록 지원합니다.

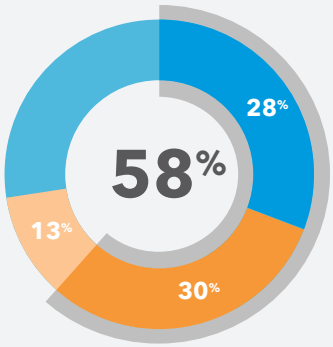
SD-WAN의 비즈니스 가치



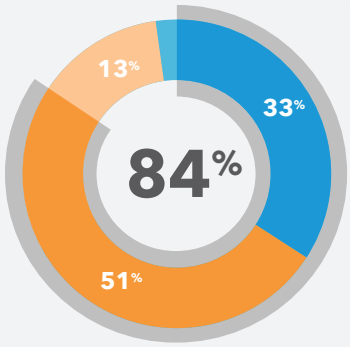
새로운 모델: 제로 트러스트 보안

새로운 아키텍처에는 새로운 보안이 필요합니다. 트랜잭션이 클라우드와 인터넷으로 옮겨감에 따라, 네트워크가 고도로 분산되고 추가적인 공격면이 발생하게 됩니다. 애플리케이션, 사용자, 데이터, 디바이스가 기존의 통제 영역을 벗어나고 있으며 그에 따라 한때 신뢰했던 기업의 경계를 와해시키고 있습니다. 기업의 경계에 의존하는 보안 모델의 구축과 적용은 이제 불가능합니다. 최신 방어 전략은 오늘날의 분산된 워크로드와 인력 문제를 해결해야 합니다.

얼마나 동의하십니까?



"네트워크 경계는 오늘날의 분산된 클라우드 네트워크와 모바일/원격 사용자의 기술 생태계를 방어할 수 없습니다."



"디지털 혁신의 필요성이 기존의 보안 전략 (경계 기반)을 수정합니다."

Forrester Research, Build Your Zero Trust Security Strategy With Microsegmentation, 2018년 9월

제로 트러스트 보안 모델은 내부라는 것은 없다고 가정하고 모든 사용자와 디바이스를 신뢰하지 않습니다. 모든 접속 요청에 대해 권한과 인증을 확인합니다. 애플리케이션과 데이터는 확인된 이후에만 제한된 범위 내에서 임시적으로 제공됩니다. 이 보안 프레임워크는 모든 애플리케이션이 인터넷에 연결되어 있고 네트워크 전체가 위협적이며 감염된 것으로 간주합니다. 또한, 가시성을 중시하여 전체 로깅 및 행동 분석을 필수적으로 수행합니다.

제로 트러스트 보안의 핵심 원리는 다음과 같습니다.

- 위치, 호스팅 모델 등과 관계없이 모든 리소스에 안전한 접속 보장
- 애플리케이션 접속 적용 시 '최소 권한' 및 '기본 거부' 전략을 채택
- 기업이 제어하거나 제어하지 않는 애플리케이션 모두를 검사하고 트래픽을 로깅하여 악성 활동 식별

제로 트러스트 보안의 구현을 지원하는 두 가지 주요 구성 요소는 다음과 같습니다.

- 보안 애플리케이션 접속을 위한 ID 인지 프록시
- 사용자 보호를 위한 보안 인터넷 게이트웨이

보안 애플리케이션 접속을 위한 ID 인지 프록시

사용자, 데이터, 애플리케이션이 클라우드에 있고 SD-WAN이 활성화한 DIA가 연결을 제공한다면, 보안과 DMZ 스택도 클라우드로 이동시킬 수 있지 않을까요? 제로 트러스트를 활용하면 기업이 제어하는 애플리케이션에 안전하게 접속하고 기업이 제어하지 않는 애플리케이션에 사용자가 접속할 때 발생하는 리스크를 경감할 수 있습니다.

현재 단순한 VPN 설정을 통해 기업 애플리케이션에 대한 접속을 제공한다면, 로그인한 사용자에게 전체 네트워크에 대한 IP 수준의 접속을 허용했을 가능성이 높습니다. 이는 매우 위험하며 제로 트러스트 보안의 원리에도 어긋납니다. 콜 센터 직원에게 소스 코드 리포지토리의 사용 권한이 필요할까요? 기업 요금 청구 시스템을 사용하는 계약직 직원이 신용카드 처리 터미널의 접속 권한을 보유해야 할 이유가 있을까요? 업무에 필요한 애플리케이션에 대해서만 접속 권한을 부여해야 합니다. 기존의 VPN은 이런 세분화된 접속을 허용하지 않는 대신 허브 앤 스포크(hub-and-spoke) 네트워크 모델의 지속적인 의존성을 필요로 합니다.

ID 인지 프록시(IAP) 아키텍처는 클라우드 기반 프록시를 통해 애플리케이션 접속을 제공합니다. ID와 권한 확인은 엣지에서 진행되며, 소프트웨어 정의 경계(SDP)를 통한 접속과 비슷하게 '필요한 때에 필요한 것만' 제공하는 최소 권한 원칙을 기반으로 하지만 대신 애플리케이션 레이어(레이어 7)에서 표준 HTTPS 프로토콜을 사용합니다.

IAP의 두 가지 작동 방법

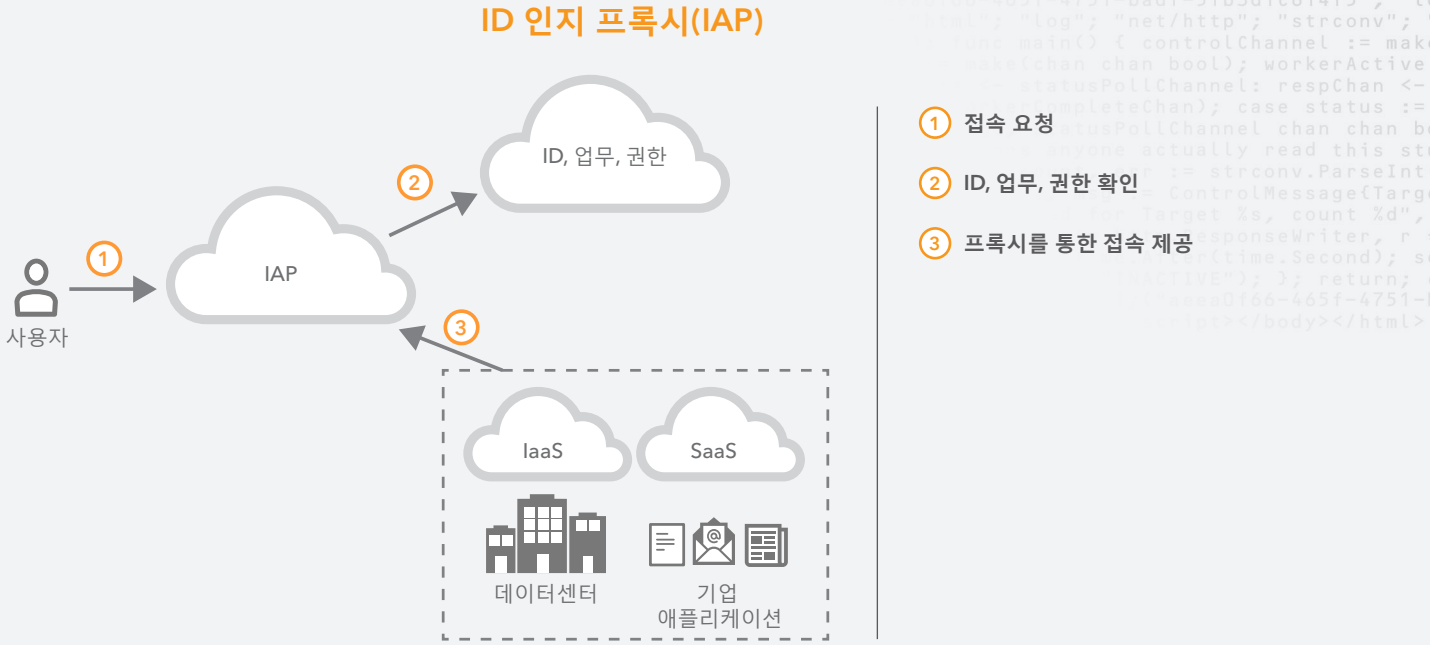
CDN을 국가 간 트랜잭션에 통합하여 애플리케이션 응답 속도 향상

또는

웹 애플리케이션 방화벽(WAF)을 사용하여 기업 웹 서버를 SQL 인젝션이나 크로스 사이트 스크립팅과 같은 일반적인 취약점으로부터 보호

IAP의 주요 구성 요소는 사용자와 디바이스의 신뢰 여부(인증)와 무엇에 대해 접속이 허용되었는지(권한) 확인하는 ID 소스입니다. 이 ID 소스는 기업 디렉터리를 기반으로 하거나 클라우드 기반의 ID 제공업체를 기반으로 합니다. 사용자의 ID가 확인되기 전에 디바이스의 상태를 확인하여 접속을 시도하는 디바이스가 인증서를 보유하고, 최신 OS를 실행하고, 비밀번호로 보호되며, 적절한 엔드포인트 탐지·응답 솔루션이 설치되고 작동하는지와 같은 보안 조건을 충족하는지 확인할 수 있습니다.

다른 접속 기술과 비교했을 때 IAP는 매우 중요한 장점을 하나 갖고 있습니다. 사용자를 확인할 뿐 아니라 사용자의 트래픽을 검사하며 개별 애플리케이션 요청을 종료하고, 조사하고, 권한을 부여할 수 있습니다. 트랜잭션이 프록시에서 종료되면 사용자 경험 개선과 애플리케이션 보안을 위해 추가 서비스를 통합할 수 있습니다.



IAP는 방화벽 룰이 아닌 애플리케이션 수준에서 접속이 관리되기 때문에 설정된 정책이 포트 및 IP 뿐만 아니라 사용자와 애플리케이션의 의도를 반영할 수 있습니다. 또한, SDP처럼 클라우드 내부 또는 방화벽 뒤에 애플리케이션과 기타 자산을 숨길 수 있으며, 웹 애플리케이션에 대해 클라이언트리스 방식을 사용합니다.

클라우드 도입이 증가하면서 기업용 애플리케이션을 마이그레이션하는 과제에 많은 관심이 집중되고 있습니다. 많은 조직이 클라우드 네이티브 및 기존 애플리케이션 모두에 클라우드를 활용하고자 노력하고 있습니다. IAP는 네이티브 SaaS 애플리케이션의 사용자 인증에도 사용되지만, 근본적으로 데이터센터의 'SaaS화된' 레거시 애플리케이션에도 사용될 수 있습니다 게다가 프록시는 전면적인 교체에 의존하지 않고 클라우드 마이그레이션과 애플리케이션 현대화를 가능하게 합니다. 그 결과 기업은 기존의 경계 기반의 제어와 기존 VPN 관련 기술적 부채를 줄이며 제로 트러스트 구현을 향한 체계적인 단계별 접근방식을 시작할 수 있습니다.

사용자 보호를 위한 보안 인터넷 게이트웨이

제로 트러스트 보안 모델로 전환하는 데 있어서 한 가지 중요한 측면은 기업이 제어하지 않는 애플리케이션에 접속할 때 사용자의 보안을 유지할 수 있다는 점입니다. 많은 사이버 위협이 인터넷의 모든 부분에 숨어 있습니다. 사용자가 기업 네트워크와 매니지드 디바이스를 사용하던 과거에는 멀웨어, 랜섬웨어, 피싱의 방어가 엔드포인트 안티바이러스를 롤아웃하고, 데이터센터에 어플라이언스 스택을 설치하며, 검사 및 제어를 위해 트래픽을 백홀하는 등 단순했습니다.

여러 지역에 사용자가 있는 경우 인터넷을 기업 네트워크로 활용하고 클라우드 기반 SIG를 안전한 온램프로 이용하여 사용자의 위치와 관계없이 선제적으로 사용자를 보호합니다.

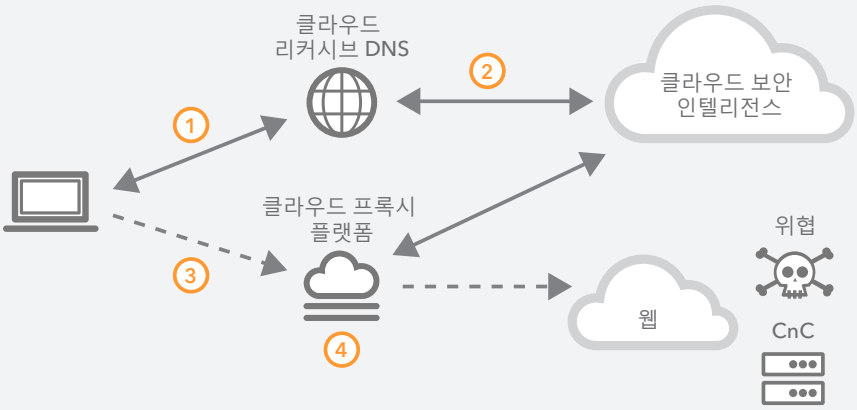
하지만 이제 사용자는 경계를 벗어났고, 디바이스는 관리되지 않으며, 인터넷이 기업의 네트워크가 되었습니다. DIA 연결은 중앙 제어 및 검사 보안 솔루션을 무용지물로 만듭니다. 한 가지 대안은 각 인터넷 브레이크아웃의 보안 어플라이언스 스택을 교체하는 것입니다. 하지만 대부분의 기업에게 있어 이는 논리적으로나 재정적으로 불가능한 일입니다. 그리고 더욱 중요한 문제는 이러한 접근 방식에 내제된 복잡성으로 인해 제로 트러스트 모범 사례에 반하는 보안 결함이 발생할 수 있다는 점입니다.

DIA 트래픽의 보안을 위한 보다 간편하고 빠르며 경제적인 방법은 클라우드 기반의 보안 인터넷 게이트웨이(SIG)를 사용하는 것입니다. 인터넷에 대한 안전한 온램프인 SIG는 위험한 트래픽을 프록시로 전송하고 이를 제어 및 검사하여 위치와 관계없이 사용자를 최신 위협으로부터 선제적으로 보호합니다. 모든 DNS 요청을 검사하고, 악성 도메인에 대한 요청을 차단하고, 안전한 도메인으로의 요청을 정상적으로 허용하며, 위험한 도메인으로의 요청을 클라우드 프록시로 포워딩하고 추가 검사를 진행합니다.

이 최종 단계에서 프록시가 HTTPS 요청을 수신하면 요청받은 URL을 클라우드 기반의 지능형 기술 자료와 비교하여 악성 URL을 차단합니다. 프록시는 위험한 것으로 분류된 기타 모든 URL에 멀티 멀웨어 분석 엔진을 통해 인라인 페이로드 분석용 웹 콘텐츠를 전송합니다. 이 엔진은 시그니처, 시그니처리스, 머신 러닝과 같은 광범위한 탐지 기술을 사용하여 알려진 위협과 이전에 알려지지 않았던 제로데이 위협을 식별하고 차단합니다. 광범위한 탐지 수단을 보유하여 콘텐츠 유형에 따라 가장 적합한 엔진에 페이로드를 전달하여 최적의 탐지율과 낮은 오탐율을 제공합니다.

이 접근 방식은 보안 웹 게이트웨이(SWG)와 같은 레거시 보안 어플라이언스에서 사용하는 접근 방법과는 상당히 다릅니다. 구체적으로 SWG는 프록시를 사용하여 모든 정상 및 악성 인터넷 트래픽을 검사하는데, 이는 특히 복잡한 웹페이지와 대용량의 HTTPS 콘텐츠에 악영향을 끼칩니다. 이 접근 방식은 성능을 저하하고 지연 시간이 발생하며 모든 트래픽을 프록시로 전송했을 때 발생할 수 있는 웹사이트 및 애플리케이션 문제를 증가시킵니다. SWG에서는 종종 더 많은 보안 사고와 오탐을 유발하여 헬프 데스크 요청이 급증하고 IT 리소스의 투입을 야기합니다.

보안 인터넷 게이트웨이 아키텍처



1. **DNS 룩업**
2. **정상, 악성, 의심스러운 도메인으로 분류**
3. **의심스러운 도메인은 클라우드 프록시로 리디렉션**
4. **URL 위협 인텔리전스 및 페이로드 분석**

스마트한 선별적 프록시를 통해 DNS를 온램프 및 1차 보안 방어선으로 이용할 수 있습니다. 안전한 트래픽은 인터넷으로 바로 전송하고 악성 트래픽은 차단하며 위험한 트래픽은 프록시를 통과하게 함으로써 다음과 같은 혜택을 얻을 수 있습니다.

- 보안 간소화
- 지연 시간 감소 및 성능 향상
- 손상된 웹 페이지와 애플리케이션 감소

보다 적은 리스크로 네트워크 혁신: 제로 트러스트를 SD-WAN 환경에 구현

인터넷 기반 아키텍처로 마이그레이션하는 여러 기업에서는 링크 제어와 MPLS 운영에 따른 재정적 부담을 줄일 수 있는 SD-WAN을 주요 지원 수단으로 고려하고 있습니다. 광대역 인터넷 또는 무선 네트워크를 사용하여 MPLS 연결을 확장하거나 보완하여 하이브리드 WAN을 생성합니다. 하지만 이미 DIA를 사용하는 경우 같은 접근 방식의 보안 모델을 사용하는 것이 좋습니다.

기업은 SD-WAN을 채택하면서 보안을 경계 기반 프레임워크에서 엣지의 제로 트러스트 기반 프레임워크로 발전시켜야 합니다. 그렇다면 현재 어떤 상황에 처해 있으며 다음 단계는 무엇일까요?

SD-WAN이 있는 네트워크는 기업의 접근방식과 장기 전략에 따라 일반적으로 다음의 3가지 상황 중 하나에 속합니다.

1. 중앙 집중식 브레이크아웃이 존재하는 기존의 전용 WAN(예: SD-WAN을 고려 중이지만 아직 구현하지 않음)
2. 기존의 전용 WAN을 기존 사이트에 구현하고 SD-WAN을 새로운 지사에 구현한 하이브리드 모델
3. 주로 SD-WAN을 사용

제로 트러스트 보안 접근 방식은 위의 모든 시나리오에 잘 맞습니다. 하지만 기업에서 이미 SD-WAN을 고려하고 있거나 구현 중인 경우, 인터넷을 실행 가능한 비즈니스 네트워크 도구로 이미 사용하고 있을 수도 있기 때문에 제로 트러스트 보안 전략을 기업 네트워크 환경에 사용할 준비가 되어 있을 것입니다.

현 상태의 아키텍처를 고찰하여 제로 트러스트를 구현하고 향후 원하는 목표를 향해 나아갈 때 어떤 영향을 주는지 알아보겠습니다.

중앙 집중식 브레이크아웃이 있는 기존 전용 WAN

인터넷 기반 네트워크 아키텍처가 제공하는 비용, 민첩성, 유연성이 SD-WAN 마이그레이션의 동기라면 SD-WAN을 넘어가고 바로 제로 트러스트 프레임워크로 진행하는 것이 좋습니다. IAP는 제로 트러스트 기반 애플리케이션 접속을 위치에 관계없이 활성화하고 SIG는 사용자에게 안전한 인터넷 접속을 제공합니다. 기업은 각 인터넷 브레이크아웃에 보안 스택을 구축할 필요가 없습니다.

한 가지 중요한 점은 비즈니스에서 VoIP 및 인터넷 클라우드 서비스 제공업체를 통한 화상 회의와 같은 실시간 서비스를 이미 지원하는 경우, 인터넷 기반 네트워크와 접속 아키텍처를 완벽하게 구현할 수 있는 이상적인 상황이라는 것입니다. 만약 이 서비스를 여전히 온프레미스로 제공하는 경우, 일부 '전용' 네트워크가 전용(예: MPLS 기반) 또는 SD-WAN 기반 위치에 남아있을 수 있습니다.

기존 WAN과 SD-WAN의 하이브리드

이 시나리오에서는 기업이 이미 보다 효율적인 인터넷 기반 아키텍처로의 첫 단계를 이미 진행했습니다.

이 환경에서는 사용자 트래픽이 처리되는 방법을 이해하는 것이 중요합니다.

- 사용자가 원격 사무실에서 다이렉트 인터넷 접속이 가능하거나 핵심 사이트로 돌아가는 네트워킹에만 사용되는 인터넷 링크가 있습니까?
- 주요 사용자 애플리케이션은 온프레미스, 데이터센터, 클라우드 중 어디에 호스팅되어 있습니까?
- 클라우드를 사용하는 경우, 사용자는 이 애플리케이션에 어떻게 연결됩니까? 지사의 DIA를 이용하거나 직접 연결 링크로 백홀합니까?
- SaaS 애플리케이션의 사용 범위는 얼마나 됩니까?
- 지사 수준의 DIA에서 각 위치의 보안 스택은 얼마나 포괄적입니까?

답은 사용자 트래픽의 처리 방법에 따라 달라지며, 그에 따라 네트워크 마이그레이션도 복잡해집니다. 하지만 변하지 않는 두 가지가 있습니다. 인터넷 사용의 증가와 경계 기반 보안에서 제로 트러스트 모델로의 전환에 대한 필요성입니다.

예를 들어 원격 사무실에서 일부 DIA 연결이 존재하는 상황을 살펴보겠습니다. SIG는 중앙 집중식 보안 스택에 추가적인 보안 기능을 제공할 수 있으며, 일부 스택을 제거하여 복잡성과 비용을 낮출 수도 있습니다.

사용자가 클라우드 기반 애플리케이션에 접속하는 경우 IAP 기반 접근 방식은 조직의 보안 체계를 강화하고 사용자 경험을 개선할 수 있습니다. 또한 CDN으로 인터넷을 통한 애플리케이션 직접 접속을 활성화하여 애플리케이션 성능도 개선합니다.

원격 사무실을 위한 DIA를 활성화하고 제로 트러스트 보안 원칙을 도입하여 기존 WAN 환경에서 SD-WAN 환경으로 전환할 수 있습니다.

소프트웨어 정의(SD-WAN) 네트워크 기술을 언제 사용하실 계획입니까?

Forrester Research, Digital Transformation Drives Distributed Store Networks to the Breaking Point, 2018년 4월

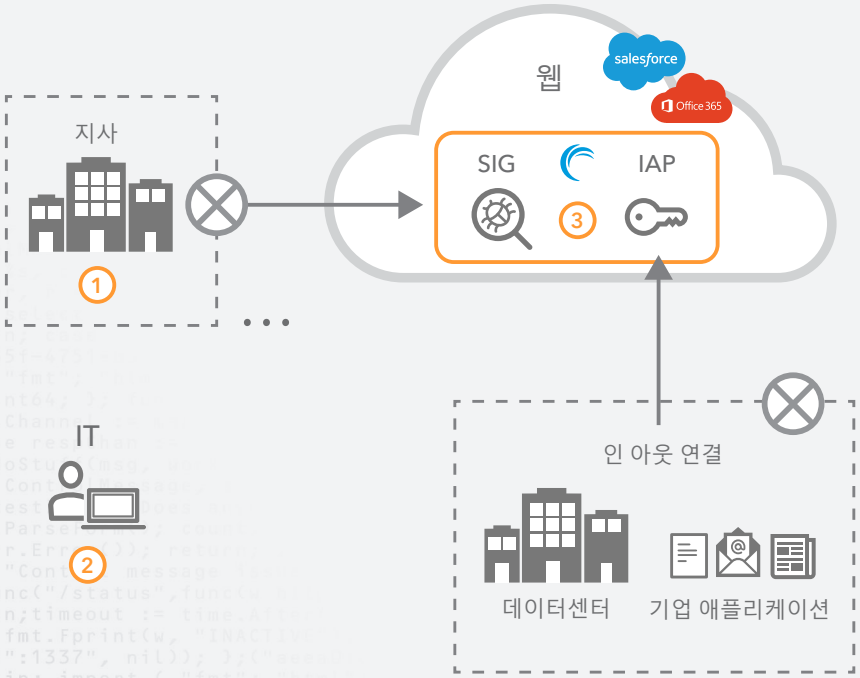
주로 SD-WAN을 사용

이 상태의 기업은 사무실 내 커뮤니케이션용 사이트 사이의 인터넷 링크에 지능형 라우팅을 사용하는 기존 전용 WAN 네트워크에서 DIA의 이점을 완벽히 활용하는 상태로 이동했을 가능성이 높습니다. 이러한 기업은 이미 대부분의 사이트에서 인터넷 연결에 의존하고 있으므로 SD-WAN을 초월하는 네트워크로 발전하는 것은 논리적인 방향입니다.

다음 단계는 애플리케이션을 인터넷으로 이동하고 MPLS 링크에 대한 의존을 줄여 민첩성을 제공하고 비용을 절감하는 것입니다. 기업 애플리케이션은 DIA 환경에서도 IAP를 통해 접속할 수 있습니다. 애플리케이션이 이미 클라우드 환경에 있는 경우, 중앙 위치(예: 직접 연결 유형 토폴로지 사용)에서 브레이크아웃을 하기 전에 트래픽을 데이터센터로 백홀하여 접속하는 것은 도움이 되지 않습니다.

마지막으로, 이 환경은 미래의 완전한 인터넷 기반 연결 및 접속에 적합하며, 온프레미스 또는 클라우드 기반 등 위치에 상관없이 IAP를 통해 모든 기업 애플리케이션에 접속할 수 있습니다. 모든 사용자 트래픽의 보안은 SIG가 보장합니다. 또한, 인터넷 기반 제공업체가 음성이나 비디오와 같은 실시간 커뮤니케이션을 제공하는 경우 결국 SD-WAN과 심지어 기업 WAN까지 완전히 제거할 수도 있습니다. 이는 비용과 복잡성을 줄이고 제로 트러스트 아키텍처 모델로 보안을 향상할 수도 있습니다.

제로 트러스트 보안 모델과 인터넷 기반 아키텍처의 가치



1. **가장 간단한 네트워크 접속**
   - 인터넷 접속만
   - 아웃 인 접속 없음
2. **관리 역량**
   - 단일 관리 지점
   - 디바이스 모니터링
   - 사용자 모니터링
3. **추가 보안 통제**
   - 제로데이 공격 방어
   - 중앙 집중식 AAA(인증, 권한 확인 및 계정)
   - 클라이언트 상태 확인
   - 피싱, 멀웨어, CnC 방어

비즈니스 혁신

오늘날의 비즈니스 현실은 갈수록 리스크와 복잡성이 가득한 환경에 노출되고 있습니다. 전용 WAN의 허브 앤 스포크 트랜잭션으로 관리되는 네트워크 모델은 경계 기반 기업 방어 만큼이나 오래되었기 때문에 네트워크와 보안 아키텍처 모두가 발전해야 합니다. SD-WAN은 현재 기업 네트워크가 트래픽을 효과적으로 처리하고 워크로드를 클라우드로 옮기는 것을 지원하고 있으나, 지속적으로 개선되어야 합니다. 머지 않아 인터넷이 기업 WAN이 될 것입니다.

Akamai는 적절한 제로 트러스트 준수 보안 및 접속 서비스와 SD-WAN의 조합이 인터넷을 회사 네트워크로 전환하기 위한 첫 단계라고 생각합니다. SD-WAN과 Akamai Intelligent Edge Platform을 연결하면 접속 및 보안 정책을 전체적으로 적용할 수 있으며 인터넷을 통해 빠르고 안정적인 최종 사용자 애플리케이션 경험을 보장할 수 있습니다.

Akamai는 기업의 네트워크 및 보안 혁신을 안내하는 최고의 파트너입니다. 고객 담당팀에 문의하여 Akamai의 제로 트러스트 평가에 대해 자세히 알아보십시오. Akamai의 보안 전문가가 실질적인 권장사항을 전달하고 제로 트러스트 혁신의 시작과 진행 방법을 알려드립니다. 또한 제로 트러스트 보안을 간편하게 시작하는 3가지 방법에서 전환에 필요한 리소스를 확인할 수도 있습니다.