비즈니스 백서

aruba
a Hewlett Packard Enterprise company

디지털 엔터프라이즈를 강화하는 업계 최고 수준의 SD-WAN 및 SASE와 제로 트러스트

목차

실무 요약

엔터프라이즈는 효율성 향상, 고객 만족도 증가, 새로운 시장 기회 추진, 수익성 증대, 경쟁력 유지 등을 위해 디지털 트랜스포메이션을 계속 도입하고 있습니다. 클라우드로 엔터프라이즈 애플리케이션을 이동하는 것이 모든 성공적인 디지털 트랜스포메이션 과제의 핵심 요소입니다. 왜 그럴까요? 현재 기존의 엔터프라이즈 데이터 센터보다 클라우드에서 실행하는 애플리케이션이 더 많고 애플리케이션의 대다수는 SaaS(서비스형 소프트웨어)로 사용됩니다. 클라우드 우선 세계에서 엔터프라이즈는 언제 어디서나, 사용하는 장치와 상관없이 바로 안전하게 애플리케이션을 이용할 수 있도록 보장해야 하며 한편으로는 네트워크에서 직원과 고객 모두에게 최상의 경험을 일관되게 제공하도록 보장하길 원합니다. 마지막으로 엔터프라이즈의 모바일 및 IoT 디바이스가 급증하면서 공격 표면도 대폭 증가하여 엔터프라이즈가 데이터 손상 및 네트워크 중단 시간으로 이어질 수 있는 보안 침해에 노출되고 있습니다.

오늘날 기업 네트워크는 클라우드 우선 세계에 맞춰 설계되지 않았으며 디지털 트랜스포메이션의 사이버 보안 문제를 해결하기에 부족합니다. 엔터프라이즈는 클라우드의 애플리케이션뿐 아니라 WAN(Wide Area Network)에서 애플리케이션에 연결하는 사용자도 보호해야 합니다. 동시에 IoT 디바이스의 확산으로 증가하는 사이버 보안 위협에 조직이 노출되는 공격 표면도 많이 증가했습니다.

따라서 전략적 필수 요소는 클라우드 제공 보안 서비스와 원활하게 통합되어 업계 최고 수준의 SASE(보안 액세스 서비스 엣지) 아키텍처를 형성하며 지능, 보안, 자동화가 강화된 SD-WAN(소프트웨어 정의 WAN)을 도입하는 것입니다. 사용자 및 IoT 디바이스만 비즈니스 역할에 따라 네트워크의 목적지에 도달할 수 있도록 세분화를 적용하려면 SASE를 ID 기반의 제로 트러스트 보안으로 강화해야 합니다.

WAN 및 보안 전환 여정에서 엔터프라이즈는 WAN 고도화 또는 보안 고도화로 시작할 수 있지만 클라우드 투자의 진정한 가치를 실현하려면 두 가지 측면을 모두 다루어야 합니다.

오늘날 기업 네트워크는 클라우드 우선 세계에 맞춰 설계되지 않았으며 디지털 트랜스포메이션의 사이버 보안 문제를 해결하기에 부족합니다. 엔터프라이즈는 클라우드의 애플리케이션뿐 아니라 이 애플리케이션에 연결하는 사용자도 보호해야 합니다. 동시에 IoT 디바이스의 확산으로 증가하는 사이버 보안 위협에 조직이 노출되는 공격 표면도 많이 증가했습니다.

또한 유연성과 자유로운 선택을 지원하는 기술 솔루션 파트너를 선택하여 공급업체 고정을 방지하는 것도 중요합니다. 네트워크 및 보안 아키텍처를 전환한 엔터프라이즈는 새로운 혁신을 신속하게 도입하여 생산성 향상, 수익 증대와 동시에 비용을 억제할 수 있습니다.

애플리케이션을 클라우드에서 제공하는 것처럼 보안도 클라우드에서 제공해야 함

기존에는 지점의 모든 애플리케이션 트래픽이 프라이빗 MPLS 서비스에서 보안 검사 및 검증을 위해 기업의 데이터 센터로 백홀되었습니다(그림 1 참조). 이 아키텍처는 애플리케이션이 기업의 데이터 센터에서만 호스팅되는 경우에 적합했습니다. 하지만 애플리케이션과 서비스가 클라우드로 마이그레이션하면서 기존의 네트워크 아키텍처가 부족해지는 주요 이유는 인터넷으로 향한 트래픽이 목적지에 도달하기 전에 데이터 센터와 기업의 방화벽을 거쳐 애플리케이션 성능이 저하되고 일관성 없는 사용자 체감 만족도를 제공하기 때문입니다.

또한 기업 네트워크 밖에서 근무하고 바로 클라우드 애플리케이션으로 연결하는 직원 수가 증가함에 따라 기존의 경계 기반 보안으로는 부족하게 되었습니다. 클라우드와 SaaS로 사용자가 애플리케이션에 연결하고 상호 작용하는 방식이 완전히 바뀌었습니다. 엔터프라이즈는 WAN 및 보안 아키텍처를 전환하여 이용하는 장치나 위치와 상관없이 멀티 클라우드 환경에서 직접적으로 안전하게 애플리케이션 및 서비스를 이용할 수 있습니다.

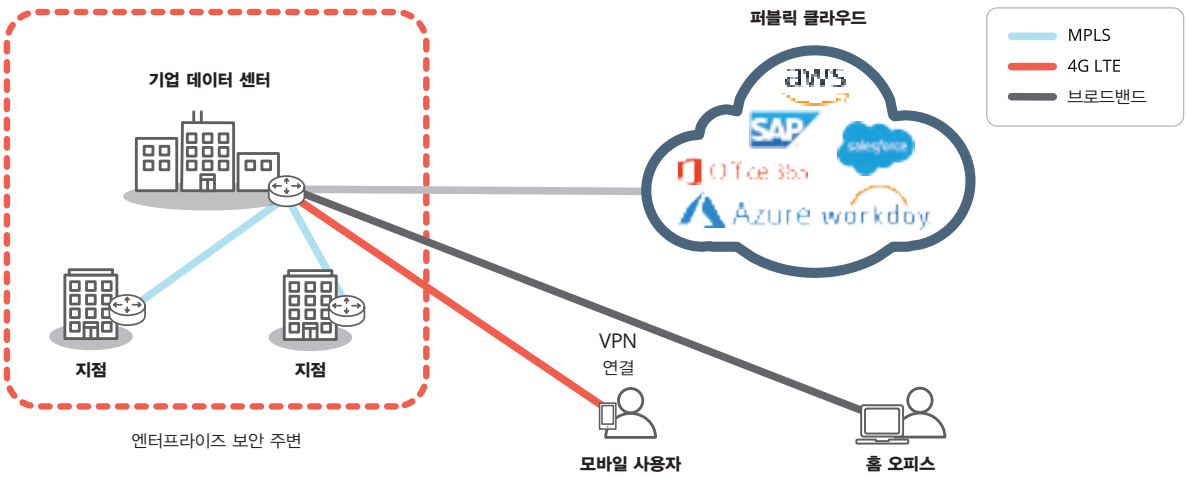

그림 1: 기존의 엔터프라이즈 WAN 및 경계 기반 보안 방식은 클라우드용으로 설계되지 않았습니다. 지점의 모든 애플리케이션 트래픽을 데이터 센터로 백홀하면 성능이 저하되고 제공하는 사용자 체감 만족도의 일관성이 떨어집니다.

2019년 Gartner는 SD-WAN과 SWG(보안 웹 게이트웨이), FWaaS(서비스형 방화벽), CASB(클라우드 액세스 보안 브로커), ZTNA(제로 트러스트 네트워크 액세스) 등과 같은 클라우드 제공 SSE(보안 서비스 엣지) 기능을 결합하는 프레임워크를 위한 SASE(보안 액세스 서비스 엣지)라는 용어를 만들었습니다. 이러한 기능들은 이전에는 각각 고유한 전용 기능이었지만 지금은 통합된 방식으로 클라우드에서 제공할 수 있게 되었습니다(그림 2 참조).

초기에 SSE 솔루션을 도입한 경우 일부는 지점 사무실에서 바로 적응형 인터넷 브레이크아웃을 적용할 수 없어 SD-WAN을 구현하는 데 실패했습니다. 따라서 트래픽을 지점 사무실에서 클라우드로 바로 전달하지 못했습니다. SD-WAN 구성요소가 없는 경우 클라우드를 향한 트래픽은 여전히 데이터 센터로 백홀되어 애플리케이션 성능에 부정적인 영향을 줍니다.

Security Service Edge 솔루션과 SD-WAN을 적용하면 온프레미스의 다중 방화벽 관리에 따르는 비용과 복잡성이 제거되지만, 들어오는 위협을 차단하기 위해서는 지점 사무실에서 여전히 방화벽 기능이 필요합니다. 그림 3에서와 같이 고급 SD-WAN 솔루션을 사용하는 엔터프라이즈는 브로드밴드 인터넷 연결을 사용하여 적응형 인터넷 브레이크아웃을 통해 클라우드에 직접 연결할 수 있습니다. 화이트리스트로 설정된 애플리케이션을 인식하는 인텔리전스로 지점 사무실에서 가장 가까운 PoP(Points of Presence)로의 로컬 브레이크아웃이 가능하여 대기 시간이 없으며 Microsoft Office 365, 8x8, RingCentral 등과 같이 신뢰하는 SaaS 및 클라우드 애플리케이션에 최상의 경험을 제공할 수 있습니다. 애플리케이션 인식을 통해 인터넷을 향한 다른 트래픽을 SaaS 공급자에 전달하기 전에 고급 검사를 위해 클라우드 제공 보안 공급자에 먼저 전달할 수 있습니다. 고급 SD-WAN 기능이 최신 클라우드 제공 보안 서비스와 통합되어 사용자, 장치, 애플리케이션, IoT의 일관된 정책 적용 및 접근제어를 보장합니다. 따라서 엔터프라이즈는 컴플라이언스 적용, 중단 시간 방지, 보안 침해와 관련된 데이터 손상 위험 완화와 같은 효과를 얻을 수 있습니다.

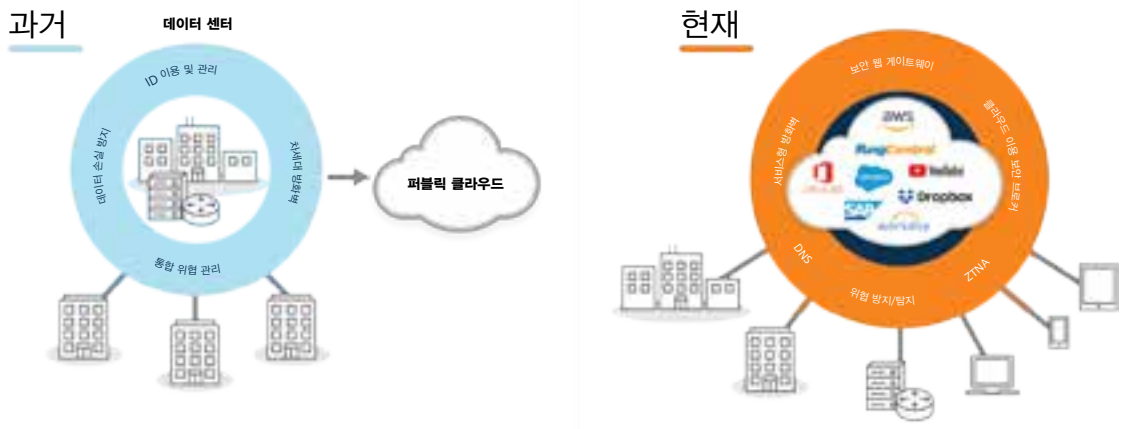

그림 2: 과거엔 애플리케이션을 단독으로 호스팅하는 엔터프라이즈 데이터 센터의 보안이 중요했습니다. 지금은 애플리케이션이 클라우드로 이동하고 클라우드에서 제공되어 엔터프라이즈 경계 기반 보안의 효과가 점점 떨어지고 있습니다. 이제 다르게 생각하고 보안을 클라우드로 이동해야 합니다.

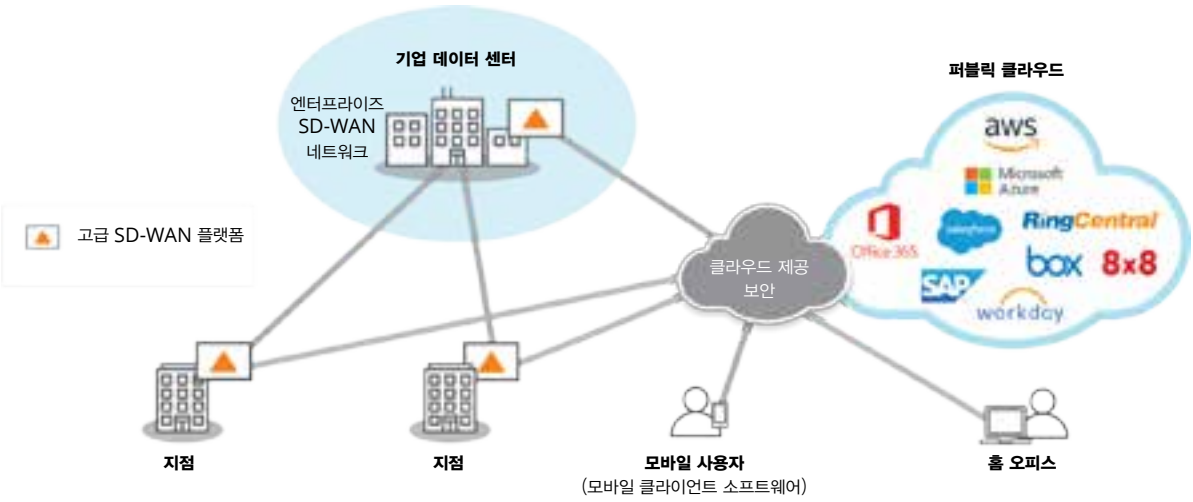

그림 3: 고급 SD-WAN이 엔터프라이즈에 클라우드로 진입하는 안전한 길을 제공합니다. 지점 사무실에서는 브로드밴드 연결과 적응형 인터넷 브레이크아웃을 사용하여 사용자를 클라우드 애플리케이션으로 바로 연결하고 애플리케이션 성능과 사용자 체감 만족도를 최적화할 수 있습니다. 고급 SD-WAN과 클라우드 제공 보안을 결합하면 사용자, 장치, 애플리케이션의 끊임없는 보안을 보장하는 SASE(보안 액세스 서비스 엣지)가 생성됩니다.

자유로운 선택이 가능한 업계 최고 수준의 SASE

네트워크 보안 제공 방식의 끊임없는 발전과 복잡한 네트워킹 솔루션 구축의 복잡성으로 인해 경험과 주력 제품이 검증된 벤더가 제공하는 업계 최고 수준의 보안 및 네트워크 솔루션을 평가해야 합니다. 두 영역에서 모두 업계 최고 수준의 SASE 역량을 지원하는 단일 벤더를 찾는 것은 어려운 일이지만 엔터프라이즈는 두 가지 중 하나의 기본적인 역량을 타협해서는 안 됩니다.

끊임없이 발전하는 위협 환경으로 보안이 최우선 과제 중 하나인 상황에서 엔터프라이즈는 단일 벤더 솔루션에 고정되지 않고 새로운 보안 솔루션을 빠르고 경제적으로 도입할 수 있어야 합니다. 독립적인 네트워크 솔루션을 보유한 엔터프라이즈는 계속 변하는 비즈니스 및 보안 요건에 적합하게 조정되는 클라우드 보안 솔루션을 안심하고 선택 및 구축할 수 있습니다.

고급 SD-WAN 솔루션이 여러 SSE 벤더와 긴밀하게 통합되어 자동화된 오케스트레이션을 사용하여 SD-WAN과 클라우드 제공 보안을 통합하는 업계 최고 수준의 벤더 솔루션을 자유롭게 선택할 수 있습니다. 업계 최고 수준의 SASE를 통해 엔터프라이즈는 비즈니스 민첩성을 높이고 복잡성은 줄이면서 사이버 공격의 영향을 차단하는 일관된 보안 아키텍처를 구축할 수 있습니다. 따라서 클라우드 애플리케이션 및 서비스에 대한 기존 투자뿐 아니라 지속적인 투자를 통해 승수 효과를 얻게 됩니다.

제로 트러스트 방식으로 엔터프라이즈 IOT 보안

엔터프라이즈에서 IoT 디바이스의 확산으로 제조 라인부터 에너지 절감을 위한 HVAC 및 조명 자동화에 이르기까지 비즈니스 과정을 모니터링, 보고, 경고, 자동화, 최적화하는 새로운 방식이 등장했습니다. IoT가 자동화를 통해 비즈니스의 효율성을 높여주지만 새로운 차원의 복잡성이 추가되어 공격 표면도 증가하게 됩니다. IT 팀이 증가하는 모바일 장치의 보안 문제를 해결하는 방식은 제로 트러스트 모델에 기반한 ZTNA(제로 트러스트 네트워크 액세스) 솔루션을 구축하는 것입니다. ZTNA 솔루션은 노트북, 태블릿 또는 휴대폰과 같은 사용자 장치에 엔드포인트 에이전트를 설치함으로써 작동합니다.

소프트웨어 에이전트는 장치의 트래픽이 SaaS 애플리케이션 또는 IaaS 공급자로 향하기 전에 클라우드 제공 보안 서비스로 연결되도록 보장합니다. 하지만 태블릿이나 스마트폰과 달리 ZTNA 소프트웨어 에이전트를 IoT 디바이스에 설치할 수 없습니다. IoT 디바이스가 에이전트-리스이며 타사 소프트웨어 에이전트 설치를 지원하지 않기 때문입니다. 따라서 엔터프라이즈는 네트워크를 침해하고 일상적인 비즈니스 운영을 중단할 수 있는 취약성으로부터 기업의 네트워크를 보호하기 위한 다른 IoT 디바이스용 보안 솔루션이 필요합니다.

제로 트러스트 아키텍처를 지원하는 고급 SD-WAN이 네트워크를 동적으로 세분화하고, 최소 권한의 이용 원칙을 적용하여 엔터프라이즈가 IoT 디바이스를 배포할 때 침해와 관련된 위험을 줄일 수 있습니다. 이렇게 하면 사용자와 장치가 ID, 이용 권한, 보안 상태에 기반한 역할에 따른 대상과만 커뮤니케이션하도록 보장합니다. 엔터프라이즈 LAN-WAN-LAN 및 LAN-WAN-데이터 센터/클라우드를 아우르는 엔드 투 엔드 세분화를 오케스트레이션하면 일관성 있는 자동화된 보안 정책 적용 및 가시성 향상이 지원됩니다. 엔드 투 엔드 세분화를 통해 엔터프라이즈는 IoT 디바이스 트래픽을 위한 분리된 세그먼트를 생성할 수 있습니다. 독립적인 보안 정책을 각 세그먼트에 대해 정의하여 장치 트래픽에 적용할 보안 정책을 규정할 수 있습니다. 한 세그먼트의 트래픽이 다른 세그먼트의 트래픽과 분리되기 때문에 무단 이용을 방지할 수 있습니다. 위협이 발생하더라도 그 영향은 해당 세그먼트로 제한됩니다.

예를 들어보겠습니다. PoS, HVAC 시스템과 같은 에이전트-리스 IoT 디바이스가 설치된 원격 사이트에서(그림 4 참조) 고급 SD-WAN 플랫폼이 장치에서 고유하게 사용하는 애플리케이션을 식별합니다. 시스템 정책이 PoS 트래픽을 가로채서 신용 카드 트랜잭션 처리 애플리케이션이 호스팅된 기업의 데이터 센터로 향하게 합니다. 이 예시에서는 데이터 센터에 배포된 기존 방화벽 보안 서비스가 적용되었습니다. 반면에 HVAC 시스템 정책이 HVAC 트래픽을 세분화하고 클라우드 제공 보안 서비스로 향하게 하여 퍼블릭 클라우드에서 호스팅되는 IoT 제어 센터에 도달하기 전에 보안 검사가 추가됩니다. IoT 트래픽이 비즈니스 정책에 따라 분리되기 때문에 HVAC 세그먼트에 침해가 발생하더라도 PoS 세그먼트의 신용 카드 및 개인 데이터가 손상되거나 위험이 발생하지 않습니다. 세분화는 조직이 비즈니스에서 PCI(또는 다른) 컴플라이언스 필수 요건을 충족하는 데에도 도움이 됩니다. 예시에서와 같이 고급 SD-WAN 플랫폼을 사용한 포괄적인 보안 구축으로 IoT의 이점을 적용하는 동적인 엔터프라이즈의 전환 여정에서 보안이 강화됩니다.

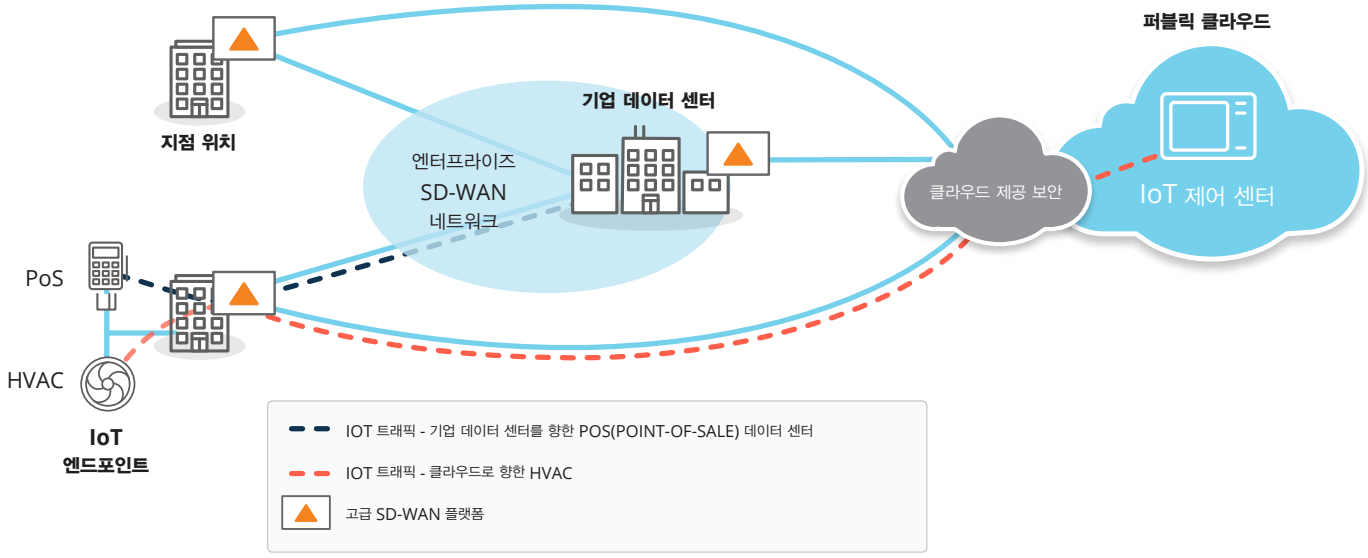

그림 4: IoT 엔드포인트가 급증하고 보안 침해에 대한 새로운 위험 요소가 등장합니다. 고급 SD-WAN 플랫폼을 통해 엔터프라이즈는 제로 트러스트 아키텍처를 구현하고 네트워크를 동적으로 세분화함으로써 IoT 디바이스를 보호할 수 있습니다. 그림에서와 같이 지점의 모든 PoS 트랜잭션 데이터는 엔터프라이즈 데이터 센터를 향하지만, HVAC 트래픽은 클라우드의 IoT 제어 센터로 향합니다.

고급 SD-WAN으로 외부의 위협으로부터 지점 보호

엔터프라이즈의 디지털화로 지난 10년간 사이버 공격 위험이 대폭 증가했습니다. 기존의 라우터 기반 네트워크 환경에서 지점 사무실은 네트워킹 및 보안 장비가 많지만, 이러한 장비는 구성 및 유지관리뿐 아니라 최신 위협 정보에 대응하는 것이 어렵습니다. 원격 사이트도 숙련된 IT 인력이 부족하여 보안 침해 가능성이 있습니다.

업계 최고 수준의 SASE를 활용한 클라우드 운영 보호에 더해 고급 SD-WAN 솔루션으로 지점 사무실을 악의적인 위협으로부터 보호할 수 있습니다. 침입 탐지 및 방지(IDS/IPS), DDoS와 같은 위협 방어 기능이 포함된 차세대 방화벽이 구축되어 지점 사무실을 악의적인 위협으로부터 보호합니다.

일반적으로 서명 기반 IDS 시스템이 네트워크 트래픽을 모니터링하여 특정 공격 서명과 일치하는 패턴을 찾아냅니다. 침입이 탐지되면 센서가 트래픽 끊기, 검사, 허용과 같은 조치를 제공합니다. 침입 방지 시스템은 강력 보안 모드 또는 고성능 모드에서 운영할 수 있습니다. 강력 보안 모드에서는 트래픽이 센서를 통과하여 침입이 발생할 경우 트래픽이 즉시 차단됩니다. 고성능 모드에서는 분석을 위해 트래픽 사본이 전송되어 네트워크 성능에 영향을 주지 않으면서 효율성이 향상됩니다. 탐지 후 침입을 차단합니다. 보안 요건에 따라 조직에서 강력 보안 모드 또는 고성능 모드 중에서 선택할 수 있습니다.

또한 고급 SD-WAN이 프로토콜 공격, ICMP 홍수, SYN 홍수, IP 스푸핑 공격과 같은 DDoS 공격을 동적으로 탐지할 수 있습니다. 네트워크의 이상 현상을 탐지한 후 솔루션이 빠른 에이징, 초과량 끊기, 소스 차단 등과 같은 조치를 사용하여 요청 수를 제한합니다. 또한 DDoS 공격이 발생한 경우 영향을 받지 않은 네트워크 라인으로 트래픽을 라우팅하여 비즈니스 연속성을 보장합니다.

조직은 라우팅, WAN 최적화, 차세대 방화벽 등과 같은 고급 네트워킹 및 보안 기능을 단일 SD-WAN 솔루션에 통합하고 지점의 네트워크 운영을 대폭 간소화할 수 있습니다. 또한 제로 터치 프로비저닝으로 중앙 위치에서 보안 정책을 자동으로 적용하여 네트워크 및 보안 정책 구성을 촉진합니다. 새로운 지점을 빠르고 간편하게 구축하고, 오류를 최소화하면서 보안 정책 변경 사항을 수백 또는 수천 개의 지점에 몇 분 만에 자동으로 배포할 수 있습니다.

WAN 전환이 성공적인 디지털 트랜스포메이션의 핵심

최신 클라우드 제공 보안 아키텍처로 마이그레이션하고 얻는 모든 이점에 더해 오늘날 클라우드 우선 엔터프라이즈에 적합하게 WAN을 전환하고 엄청난 가치를 얻을 수 있습니다. 기존의 라우터 중심 WAN은 클라우드용으로 설계되지 않았습니다. 엔터프라이즈는 WAN 아키텍처를 고도화하고 지점 네트워크의 설계를 최적화하여 클라우드 애플리케이션의 성능과 보안을 개선하는 방법을 재고해야 합니다. 엔터프라이즈에서 사용자에게 최고 수준의 경험을 제공하는 것에 집중하면서 클라우드 및 SaaS의 사용을 늘리고 있습니다.

WAN 전환은 사용자와 클라우드 사이의 더 효율적인 경로와 개선된 경험을 제공합니다. 앞에서 언급한 것과 같이 지점에서 바로 클라우드 호스팅 및 SaaS 애플리케이션에 적응형 인터넷 브레이크아웃을 도입하면 이용 가능한 대역폭을 최적화하고 사용자의 생산성에 부정적인 영향을 주는 대기 시간도 줄일 수 있습니다.

많은 조직에서 네트워크 엣지를 전환하고 SD-WAN을 도입하여 브로드밴드 인터넷 연결을 통해 지점에 연결하고 있습니다. SD-WAN은 중앙에서 정의한 정책을 바탕으로 다중 WAN 링크(MPLS, 브로드밴드 인터넷, LTE 등)에서 애플리케이션 기반의 지능형 경로 선택을 지원합니다. SD-WAN의 이점은 다음과 같습니다.

- 비즈니스 애플리케이션 제공의 경제성 향상
- 애플리케이션 성능, 가용성, 최종 사용자의 경험 개선
- 최신 지점/원격 사이트 또는 위치의 요건 충족
- SaaS와 클라우드 기반 애플리케이션 및 서비스 도입
- 자동화된 서비스 프로비저닝을 통해 지점의 IT 효율성 개선

애플리케이션 SLA의 요구 사항 해결

엔터프라이즈의 생산성과 비즈니스의 민첩성이 대폭 향상됩니다. 엔터프라이즈는 비즈니스 크리티컬 애플리케이션을 안정적으로 지원하는 높은 가용성을 기반으로 구축된 고성능 네트워크가 필요합니다. 보안은 절대 나중에 고려하는 요소가 되어서는 안 됩니다. 마이크로 세분화 기능과 세분화된 정책 시행을 지원하여 엔터프라이즈가 WAN을 보호하고 규제 준수 요건을 준수하고 침해로부터 방어할 수 있습니다.

엔터프라이즈는 새로운 지점을 신속하게 시작하고 정책 및 보안 규칙을 동적으로 조정할 수 있어야 합니다. 정책 컨텍스트를 적용하는 역량은 지점 자동화의 필수 요건입니다. 따라서 고급 SD-WAN 솔루션 개념은 매우 매력적이며, 엔터프라이즈에서 다중 어플라이언스가 전담 보안 기능을 수행할 필요가 없어 지점의 WAN 엣지 아키텍처를 간소화 및 통합하는 데 도움이 됩니다. 고급 SD-WAN 엣지 플랫폼을 통해 엔터프라이즈는 SD-WAN, 라우팅, WAN 최적화, 세분화, 지점 보안을 하나의 중앙 집중식 관리형 플랫폼으로 통합하고 WAN을 전환할 수 있습니다.

중앙 집중식 SD-WAN 오케스트레이션 및 애플리케이션별 접근 방식으로 비즈니스의 우선 순위가 항상 네트워크의 행동 방식에 반영되도록 보장합니다. 또한 네트워크 오케스트레이션과 보안 정책을 통합하여 이용하는 위치나 방법과 상관없이 QoS와 보안이 애플리케이션 또는 애플리케이션 클래스에 일관되게 적용되고 시행되도록 보장합니다. 상향식 기술 제약이 아닌 하향식 비즈니스 정책으로 애플리케이션의 성능과 보안을 결정할 수 있습니다. 고급 SD-WAN이 지속적으로 네트워크 및 애플리케이션 상태를 모니터링하고, 상태의 변화를 탐지하며, 즉시 자동화된 실시간 대응을 트리거하여 부분 정전, 완전 정전, 보안 위협 이벤트의 영향을 제거합니다. 또한 API(애플리케이션 프로그래밍 인터페이스)를 통해 통합하고 클라우드 플랫폼 연결을 자동화하면 IT 운영이 간소화되고, 엔터프라이즈에 클라우드 제공 보안 서비스, IaaS, SaaS 등을 신속하게 이용할 수 있습니다. 오늘날 네트워크는 멀티 클라우드 환경에 필요한 성능, 보안뿐 아니라 최고 수준의 경험을 동적으로 보장하기 위해 엔드 투 엔드 가시성, 프로그래밍, 자동화가 필요합니다. 업계 최고 수준의 SD-WAN 및 클라우드 제공 보안 솔루션이 적용된 지능형 WAN이 디지털 트랜스포메이션 과제를 개선하고, 엔터프라이즈가 생산성과 성장을 제한하지 않으면서 새로운 혁신을 신속하게 도입하고 발전하는 동시에 보안 위험에 대한 노출을 최소화하도록 지원합니다.

결론

최신 클라우드 우선 엔터프라이즈가 계속 데이터 센터에서 클라우드로 애플리케이션을 이동하는 상황에서 클라우드 투자 수익을 극대화하기 위해서는 WAN 및 보안 전환을 도입해야 합니다. SASE(보안 액세스 서비스 엣지)로 업계가 이러한 새로운 방향으로 이동하고 있습니다. 그림 5에서와 같이 엔터프라이즈는 SASE를 설계할 때 중단 없는 경험을 지원하기 위해 WAN뿐만 아니라 보안 전환도 고려해야 합니다.

고급 SD-WAN 플랫폼을 통해 업계 최고 수준의 다양한 클라우드 보안 서비스에 중단 없이 연결하고 동급 최강의 SASE 아키텍처를 제공할 수 있습니다. 결과적으로 하나의 플랫폼에서 업계 최고 수준의 네트워크 및 보안 기술을 제공할 수 있는 단일 SASE 벤더는 없습니다. 위협 환경이 계속 진화함에 따라 엔터프라이즈는 새로운 보안 솔루션을 빠르고 비용 효율적으로 도입할 수 있는 민첩성을 유지하고 자유롭게 선택하여 업계 최고 수준의 SASE를 통합할 수 있는 플랫폼을 평가해야 합니다. 그래야만 독점 단일 벤더 솔루션에 종속되거나 기본 기능에 만족해야 하는 상황을 피할 수 있습니다.

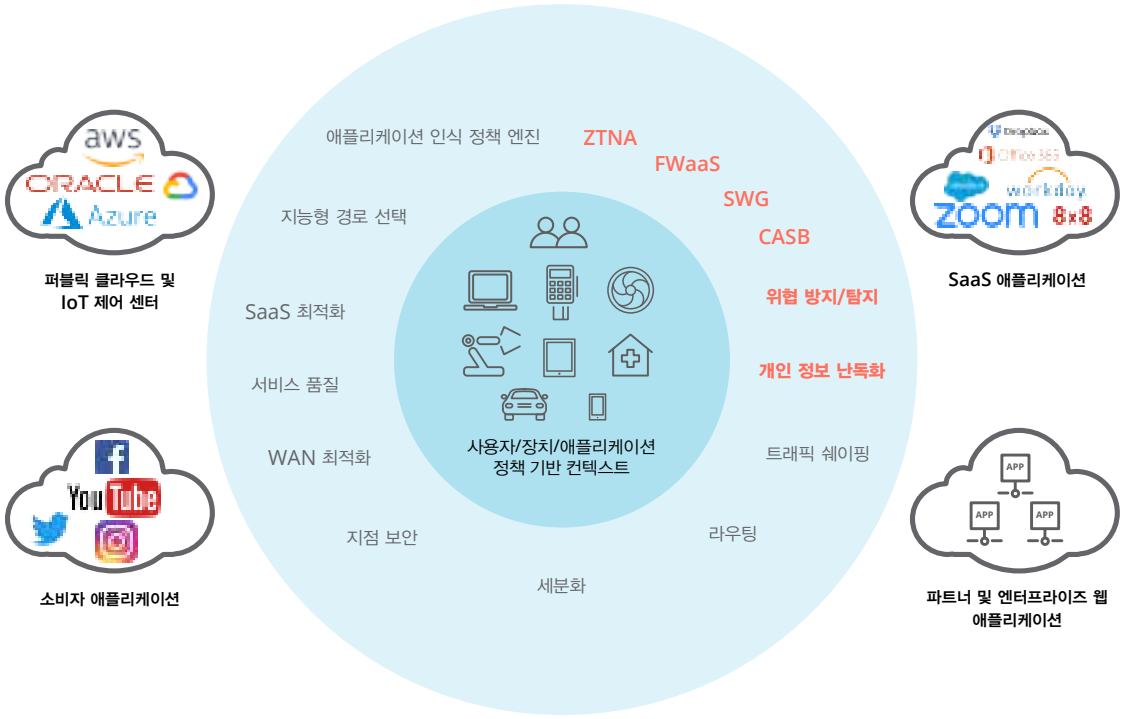

그림 5: 엔터프라이즈의 디지털 트랜스포메이션 과제(예: 클라우드 우선 전략 및 직원의 모빌리티 요구 사항)를 지원하는 데 SASE가 필요합니다. 강력한 SASE 아키텍처에서 사용자, 장치, 애플리케이션에 대한 디지털 엔터프라이즈의 동적인 보안 이용 요구 사항 지원을 위해 포괄적인 WAN 기능이 포괄적인 네트워크 보안 기능과 함께 작동해야 합니다.

또한 IoT 디바이스의 확산으로 사용자와 IoT 디바이스가 비즈니스의 역할에 따라 네트워크 목적지에 도달할 수 있도록 ID 기반의 트래픽을 동적으로 세분화하는 제로 트러스트 보안 프레임워크로 SASE를 보완해야 합니다.

고급 SD-WAN으로 차세대 방화벽에 IDS/IPS 기능을 적용함으로써 지점에서 필요한 기본 보안 기능을 지원하고, 엔터프라이즈 전체에서 원활한 엔드투 엔드 보안 정책을 시행하도록 클라우드 제공 보안을 보완할 수 있습니다. 따라서 엔터프라이즈는 네트워크 인프라를 간소화하고, 타협 없이 원하는 속도로 최신 클라우드 우선 보안 WAN 아키텍처로 전환할 수 있습니다.

마지막으로 지점의 방화벽을 폐기하고 완전히 클라우드 제공 보안 모델로 이동할 준비가 안 된 엔터프라이즈는 지점에서 통합 솔루션으로 실행하는 선도적인 타사 UTM(통합 위협 관리) 소프트웨어 솔루션을 지원하는 제품을 자유롭게 선택할 수 있는 고급 SD-WAN 플랫폼을 찾아야 합니다. 이를 통해 각각의 전용 방화벽으로 발생하는 추가 비용 및 관리 복잡성을 제거하고, 업계 최고 수준의 솔루션을 유연하게 구축하여 클라우드 제공 보안 모델로 원활하게 마이그레이션할 수 있습니다.

엔터프라이즈가 계속 클라우드에 상당한 비용을 투자하는 상황에서 WAN 및 보안 전환의 요건을 고려하면 사용자에게 최고 수준의 경험을 제공하는 동시에 오늘날 사이버 보안 문제를 처리하는 데 도움이 됩니다. 신중하게 타협 없는 WAN 및 보안 전환 여정을 시작하여 결과적으로 디지털 자산을 보호하고 기존 및 진행 중인 클라우드 투자에서 승수 효과를 얻을 수 있습니다.

aruba
a Hewlett Packard Enterprise company

BP_Successful-WAN-and-Security-Transformation_RVK_080422 a00110932kop

문의하기: www.arubanetworks.com/contact