솔루션 개요

단일 플랫폼 관리로 SD-WAN 운영 간소화

종합 요약

원격 사무실이나 지사 배포의 경우 SD-WAN(Software-defined wide-area networking)이 기존 WAN을 대체하는 경우가 급속히 늘어나고 있습니다. SD-WAN이 새로운 디지털 혁신을 지원하는 성능적 이점을 제공하지만, 대다수의 SD-WAN 솔루션에는 통합된 네트워킹 및 보안 기능이 결여되어 있습니다. 이 때문에 대다수의 네트워크 운영자는 자사 SD-WAN 배포를 관리하고 보호하기 위해 여러 가지 도구와 솔루션을 복잡하게 조합하고 추가해야 했습니다. 하지만 이제는 비용과 위험을 낮추는 동시에 효율성을 개선하기 위하여 보다 단순한 접근법이 필요합니다. FortiGate Secure SD-WAN은 차세대 방화벽(NGFW)을 관리 및 분석용 통합형 솔루션과 결합하여 SD-WAN 운영을 중앙집중화하고 간소화함으로써 이러한 각각의 요구사항에 부합합니다.

포티넷은 패브릭 관리 센터로 SD-WAN 운영 간소화

- 간편한 배포
- 중앙집중형 관리
- 보고 및 분석
- 규정 준수 보고
- 통합 및 자동화

성장 중인 기업을 보안을 유지하면서 혁신까지 지원

분산된 엔터프라이즈는 생산성을 높이고 소통을 개선하며 빠른 비즈니스 성장을 도모하기 위해 SaaS(Software-as-a-Service) 애플리케이션이나 음성이나 영상과 같은 실시간 애플리케이션 등 다양한 디지털 혁신을 도입하고 있습니다. 그러나 대다수의 지사와 원격 사무실에 마련된 기존의 WAN 아키텍처는 대개 이러한 신기술에 따른 트래픽 수요를 지원하기에는 역부족입니다. 이 때문에 좀 더 수용하기 쉬운 직접 인터넷 연결을 활용하는 SD-WAN 아키텍처를 도입하는 사례가 늘어났습니다. SD-WAN의 시장 규모는 2019년부터 2025년까지 58%의 CAGR로 성장할 것으로 전망됩니다.[1]

가트너에 따르면 "응답자의 72%는 WAN과 관련하여 가장 절실한 우려 사항은 보안이라고 밝혔다"고 합니다.[3]

Gartner

SD-WAN은 네트워킹 대역폭을 개선하지만, 동시에 기업이 위험에 노출될 가능성을 높입니다. 가트너 설문조사 분석에 따르면 "고객은 더 나은 WAN 성능과 가시성을 위해 계속해서 애쓰고 있지만, 자사 WAN과 관련한 여러 가지 난제 중 최우선과제는 단연 보안이라고 답했다"라고 합니다.[2]

대다수의 기업에서는 SD-WAN 보안에 대한 요구사항 때문에 네트워크 엔지니어링 및 운영 부서 책임자가 각각의 기능, 위협 노출 또는 규정 준수 요구사항을 해결하기 위해 다양한 도구와 포인트 제품을 들여오게 되었습니다. 그러나 이 방식을 채택하면서 인프라가 복잡해졌고, 관리 편의성에 부담이 가중되는 동시에 네트워크 에지에서는 새로운 방어 간극이 생겼습니다.

포티넷은 SD-WAN 배포를 간소화하고 보안을 유지합니다

보안 중심 SD-WAN 솔루션에 요구되는 네트워킹과 보안 도구를 통합하여 지사 인프라의 복잡성 문제를 없앨 수 있습니다. 이렇게 하면 기업의 공격 면을 줄이면서 디지털 혁신 이니셔티브를 지원할 수 있으며, 네트워킹 팀을 위한 운영도 간소화합니다.

Fortinet Secure SD-WAN은 패브릭 관리 센터에 통합된 일부분으로서 FortiManager의 일부로 제공되는 SD-WAN 오케스트레이터와 함께 단일 플랫폼 콘솔을 활용하여 FortiAnalyzer의 강화된 분석과 개선된 보고 기능을 제공합니다. 이를 통해 고객은 중앙집중화된 배포를 대폭 간소화하고 자동화를 지원하여 시간을 절약하며, 비즈니스 중심적 정책을 제안할 수 있습니다.

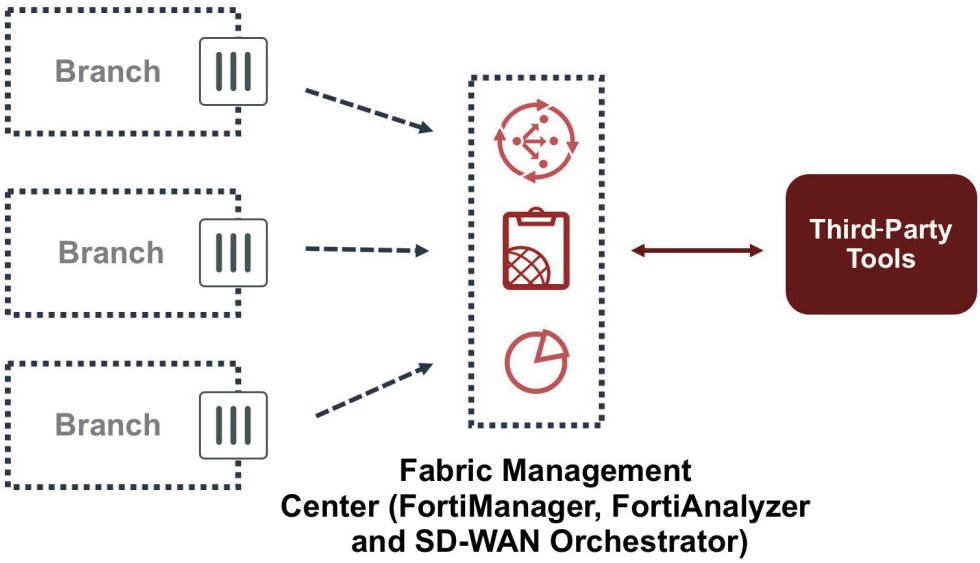


그림 1: 패브릭 관리 센터를 포함한 SD-WAN 사용 사례

간편한 배포

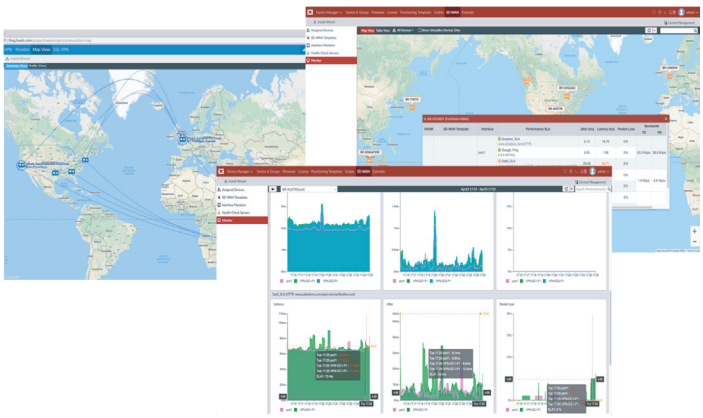
Secure SD-WAN을 구현하는 기업에서는 패브릭 관리 센터를 활용하여 배포 속도를 더 빠르게 하면 며칠씩 걸리던 시간을 분 단위로 절감할 수 있습니다. 패브릭 관리 센터의 간편한 배포 기능을 이용하면 지사에서 FortiGate 디바이스를 플러그인한 다음 광대역 연결을 통해 본사에 있는 FortiManager에서 자동으로 구성될 수 있습니다. 이렇게 하면 설치로 인한 불필요한 시간과 비용이 소모되지 않도록 방지할 수 있습니다. 포티넷 방식을 통하면 기존 SD-WAN 구성을 새로운 지사와 원격 사이트에서의 대규모 배포를 가속할 템플릿으로 사용할 수도 있습니다.

NSS Labs 테스트 결과 FortiGate Secure SD-WAN은 간편한 배포 기능으로 지사 한곳을 네트워크에 연결하는 데 6분이 채 걸리지 않는 것으로 나타났습니다.[4]

분산형 기업을 위한 중앙 집중식 관리

기업 전체에 걸친 분산형 네트워크 전체를 중앙 집중식 관리로 네트워크 운영자 입장에서 사이버 위험 노출과 네트워크 중단을 불러올 수 있는 오류가 발생할 기회를 크게 줄일 수 있습니다.

Secure SD-WAN의 오케스트레이터는 패브릭 관리 센터의 일부분입니다. 이를 통해 고객은 중앙집중화된 배포를 대폭 간소화하고 자동화를 지원하는 동시에 시간을 절약하며, 비즈니스 중심적 정책을 제안할 수 있습니다. 포티넷 관리 도구는 경쟁사 솔루션과 비교해 최대 FortiGate 디바이스 100,000대까지 훨씬 규모가 큰 배포도 지원할 수 있습니다. SD-WAN과 NGFW 템플릿, 엔터프라이즈급 구성 관리 및 역할 기반 액세스 제어 등을 통해 네트워크 엔지니어링 및 운영자는 담당자의 실수를 간편하게 수습할 수 있습니다.



SD-WAN 보고 및 분석

WAN 링크 가용성, 성능 SLA와 런타임의 애플리케이션 트래픽, 그리고 이전 통계 등의 분석 기능이 강화되어 인프라팀에서 문제를 해결하고 네트워크 문제를 신속하게 해결할 수 있습니다. 패브릭 관리 센터는 애플리케이션 가시성과 네트워크 성능에 대한 지능형 텔레메트리를 제공하여 더욱 빠른 해결을 달성하고 IT 지원 티켓 수를 줄여줍니다. 온디맨드 SD-WAN 보고서가 위협 환경과 신뢰 수준, 그리고 자산 접근에 대한 더 자세한 인사이트 정보를 제공하며 이러한 정보는 규정 준수를 위해 필수적으로 입수해야 합니다.

이러한 기능 중에는 SD-WAN 대역폭 모니터링 보고서와 데이터세트, 데이터세트와 차트, 보고서를 통한 SLA(Service-Level Agreement) 로깅 및 이력 모니터링, 그리고 사용자 지정 가능한

SLA 경고와 애플리케이션 사용량 보고서 및 대시보드 등이 있습니다. 또한 SD-WAN 이벤트에 적합한 적응형 대응 처리기는 물론 애플리케이션과 인터페이스의 SLA를 중심으로 한 이벤트 로깅과 아카이빙 기능까지 제공합니다.

규정 준수 보고

고객에게는 감사업체에 규정 준수를 입증하기 위한, 사용자 지정에 관한 보고서와 도구가 필요합니다. 다만 규정 준수 관리란 네트워킹팀에는 예전부터 비용도 많이 들고 노동집약적인 프로세스였습니다. 정규직 인력을 여럿 동원하고 몇 달에 걸쳐 여러 포인트 보안 제품으로부터 데이터를 집계해 정규화해야 했기 때문입니다.

포티넷은 보안 인프라를 간소화하고 수많은 수동 프로세스의 필요성을 배제하여 규정 준수 보고 프로세스의 속도를 빠르게 해줍니다. 패브릭 관리 센터에는 사용자가 지정 가능한 규제 템플릿과 형식이 미리 지정된 보고서가 포함되어 있어 PCI DSS(Payment Card Industry Data Security Standard, 결제카드 산업정보보안표준), SAR(Security Activity Report), CIS(Center for Internet Security) 및 NIST(National Institute of Standards and Technology, 미국 국립표준기술원)와 같은 표준에 맞출 수 있습니다. 또한 패브릭 관리 센터는 감사 로깅 기능과 역할 기반 액세스 제어(RBAC)도 제공하여 직원들이 각자 맡은 직무를 다하기 위해 필요한 정보에만 액세스할 수 있도록 보장합니다.

패브릭 관리 센터 기능의 확장인 FortiGuard 보안 평가 서비스가 감사 점검을 실행하여 보안 및 네트워킹팀이 자사 보안 패브릭 설정 내에서 중요한 취약점과 약점을 파악하고, 나아가 모범 사례 권장 사항을 구현할 수 있습니다. 서비스의 일부분으로 네트워크 운영자는 자사의 기업 보안 상태 점수를 동종 업계의 유사한 동료 기업과 비교해볼 수도 있습니다.[5]

규정 준수는 보안이 아닙니다. 사이버 복원력이 가장 뛰어난 기업은 규정 준수를 기본적인 기준치로 취급하는 기업입니다.[6]

통합 및 자동화

보안 기능이 제대로 효과를 거두려면 분산된 기업의 모든 부분에 원활하게 통합되어야 합니다. 즉 지사와 원격 사무실도 예외가 아니어야 합니다. 네트워크 엔지니어링 및 운영자는 한 곳에서 전체 공격 면의 완전한 가시성을 확보할 수 있어야 합니다. 그런 다음 자동 대응으로 탐지부터 수정까지 걸리는 시간 범위를 줄이고, 팀원들의 수동 작업 부담을 덜어야 합니다.

패브릭 관리 센터는 보안 워크플로와 위협 인텔리전스 자동화를 가능하게 하는 통합형 보안 아키텍처인 포티넷 보안 패브릭 전체에 걸쳐 정책 기반 자동 대응 조치를 조율하여 위협 수정 시간을 몇 달 단위에서 몇 분 단위로 크게 단축합니다. 한 곳의 지사에서 컨텍스트 인식형 데이터와 함께 탐지된 인시던트 경고를 보내면 네트워크 관리자가 발생 가능한 협조 공격에 대비하여 엔터프라이즈 전체를 보호할 방법을 신속하게 결정할 수 있습니다. 특정 이벤트도 디바이스 구성에 대한 자동 변경을 트리거하여 순식간에 공격 완화를 위해 루프를 닫을 수 있습니다.

FortiAnalyzer와 패브릭 관리 센터는 수많은 필수 SD-WAN 작업도 자동화하여 네트워크 운영자의 인력 배분에 가해지는 부담을 더는 데 도움이 됩니다. 두 제품 모두 보안 정보 및 이벤트 관리(SIEM), IT 서비스 관리(ITSM), DevOps(예: Ansible, Terraform)와 같은 타사 도구와 통합하여 기존 워크플로를 보전하고 다른 보안 및 네트워킹 도구에 투입한 예전의 투자 가치를 보전하는 데 유리합니다.

가치와 간결성, 그리고 보안 보장

패브릭 관리 센터는 다음과 같은 업계 최고의 이점을 비롯한 엔터프라이즈급 보안과 지사 네트워킹 기능을 제공합니다.

TCO감소. 포티넷의 보안 중심 SD-WAN에 대한 통합형 접근 방식을 이용하면 자본 지출(CapEx)로 필요한 네트워킹과 보안 도구 수를 통합하여 총소유비용(TCO)을 개선하면서, 그와 동시에 간소한 관리와 워크플로 자동화를 통해 운영 경비(OpEx)도 절감할 수 있습니다. 공용 광대역으로 이동한다는 것은 고가의 멀티프로토콜 레이블 전환(MPLS) 연결을 더욱 비용 효율적인 옵션으로 대체할 수 있습니다. 이때 FortiGate Secure SD-WAN은 경쟁사와 비교해 10배 나은 업계 최고의 TCO를 보장합니다.[7]

효율성 개선. 이와 동시에, 포티넷은 SD-WAN에 맞는 간소화된 인프라를 도입하여 지사는 물론 분산된 기업 전체를 총망라하여 운영의 복잡성을 줄여줍니다. FortiGate Secure SD-WAN은 간단하고 직관적인 관리 콘솔을 통해 관리할 수 있습니다. FortiGate 디바이스는 FortiManager와 함께 사용하면 진정한 플러그 앤 플레이 형식으로 활용할 수 있습니다. FortiManager로 중앙집중형 정책과 디바이스 정보를 구성할 수 있으며, FortiGate 디바이스는 최신 정책 구성으로 자동 업데이트됩니다.

단일 플랫폼 관리는 유연성이 뛰어나 확장 가능한 원격 보안 및 모든 지사와 위치를 대상으로 클라우드를 통한 네트워크 제어까지 포함합니다.

위험확산 차단. 포티넷의 추적 및 보고 기능은 기업에서 개인정보 보호법, 보안 표준 및 업계 규정을 준수하도록 보장하는 동시에 보안 침해가 발생하는 경우 벌금이나 법적 비용과 관련한 위험을 경감해줍니다. FortiAnalyzer는 실시간으로 위협 활동을 추적하고 위험 평가를 진행하며 잠재적인 문제를 탐지하여 실제 문제가 발생하는 경우 이를 완화하도록 돕습니다. FortiGate Secure SD-WAN과 긴밀하게 통합하면 방화벽 정책을 모니터링하고 분산된 비즈니스 인프라 전체에 걸쳐 규정 준수 감사를 자동화하는 데 도움이 됩니다.

시스템 복잡성 때문에 평균 데이터 침해 비용(392만 달러)이 인상되었습니다(290,000달러 증가).
위협 인텔리전스 공유(240,000달러 감소)와 보안 분석(200,000달러 감소)은 둘 다 그러한 비용을 절감해줍니다.[8]

포티넷의 보안 중심형 SD-WAN 구현

보안 중심형 SD-WAN의 사용 사례는 많지만, 포티넷 방식은 모든 유형의 SD-WAN 프로젝트에서 가장 효과적인 방식으로 이용할 수 있습니다. SD-WAN 운영을 간소화하는 것은 디지털 혁신 이니셔티브를 지원하면서 SD-WAN을 무사히 구현하고 확장하는 데 필요합니다. 패브릭 관리 센터의 Fortinet Secure SD-WAN으로 동급 최고의 SD-WAN 관리 및 분석 기능을 제공하여 네트워크 운영자는 운영 비용을 절감하고 네트워크 에지의 위험을 줄일 수 있습니다.

[1] "SD-WAN 인프라, 2022년까지 45억 달러 규모를 달성할 것으로 전망(SD-WAN Infrastructure Market Poised to Reach $4.5 Billion in 2022)" IDC, 2019년 7월.

[2] "포티넷, 2020년 가트너 피어 인사이트에서 WAN 이지 인프라 부문 고객의 선택으로 선정(Fortinet Recognized as a 2020 Gartner Peer Insights Customers' Choice for WAN Edge Infrastructure)" Fortinet, 2020년 3월 26일.

[3] "Fortinet Secure SD-WAN: 동급 최고의 NGFW와 SD-WAN을 단일 제품으로(Best-of-Breed NGFW and SD-WAN in a Single Offering)" Gartner, 2018년 11월.

[4] Ahmed Basheer, "SD-WAN 테스트 보고서(Software-Defined Wide Area Network Test Report): Fortinet FortiGate 61E," NSS Labs, 2019년 6월 19일.

[5] "포티넷 보안 평가 서비스로 사전 예방적, 조치 가능한 위험 관리(Proactive, Actionable Risk Management with the Fortinet Security Rating Service)" Fortinet, 2019년 4월 5일.

[6] Frances Dewing, "규정 준수는 보안이 아니기에(Compliance Is Not Security): 고위 경영진이 사이버 보안 기술을 확보해야 하는 이유(Why You Need Cybersecurity Chops In The Boardroom)" Forbes, 2019년 8월 15일.

[7] "포티넷, 2019 가트너 매직 쿼드런트 WAN 에지 인프라의 챌린저 쿼드런트에서 실행 능력 부문 1위 차지(Fortinet Placed Highest in Ability to Execute in the Challengers Quadrant of the 2019 Gartner Magic Quadrant for WAN Edge Infrastructure)" Fortinet, 2019년 12월 4일

[8] "2019년 데이터 침해 비용 보고서(2019 Cost of a Data Breach Report)" Ponemon Institute and IBM, 2019년 7월.

www.fortinet.com/kr

서울특별시 강남구 영동대로 325에스타워 14 /15층 전화: 080-559-8989 Email: **kr-callcenter@fortinet.com**

476710-A-1-EN