솔루션 브리프

포티넷 LAN EDGE솔루션 유무선 네트워크 보안의 단순화

종합 요약

LAN 엣지(Local-Area Network Edge)는 보안이 가장 까다로운 분야 중 하나입니다. 수많은 사용자와 기기가 연결하며 많은 양의 데이터를 보호해야 합니다. 게다가 IoT(Internet-of-Things) 구축이 증가함에 따라 기본적으로 보호되지 않는 기기가 네트워크에 액세스하는 경우가 늘어나고 있으므로 공격자의 구미를 당기는 기회가 만들어집니다.

미국 설문조사 응답자 중 92%는 지난 12개월 동안 공격의 양이 증가했다고 말했습니다.[1]

LAN 엣지 보안은 모든 네트워크의 성공에 매우 중요합니다. 복잡성을 줄이는 동시에 안전한 네트워크 액세스를 효과적으로 제공하려면 다음과 같은 솔루션이 필요합니다.

- 관리 시간 최소화
- 증가하는 사용량과 다양한 토폴로지를 처리하기 쉬운 확장성
- 보안 기능 극대화

포티넷 보안 패브릭의 일부인 포티넷 LAN 엣지 솔루션은 내장된 보안, 종합적인 네트워크 가시성, 통합 탐지, 자동화된 위협 대응을 제공합니다.

최고 수준의 보안과 간소화된 관리

포티넷 보안 중심 네트워크는 FortiGate 차세대 방화벽(NGFW)을 중심으로 하는 포티넷 LAN 엣지 솔루션이 무선 액세스 포인트(AP) 및 유선 스위치와 직접 통합될 수 있도록 합니다. 이러한 보안 및 네트워크 액세스의 통합은 업계 판도를 바꾸는 이점을 다수 제공합니다. LAN 엣지 솔루션은 공통 보안 운영 체제인 FortiOS와 단일 소스의 위협 인텔리전스인 FortiGuard를 통해 여러 보안 및 네트워킹 공급업체를 함께 이용할 때 발생하는 복잡성과 보안상의 단점을 모두 제거합니다. 전체 에코시스템을 정책 및 로깅 관점에서 다루면 지능적 위협의 리스크를 줄일 수 있습니다. 또한 보안 서비스를 기업의 보안 태세에 따라 세부적으로 조정할 수 있습니다.

네트워크 및 보안 기능의 통합은 FortiLink를 통해 이루어지며, 이더넷 및 무선의 내부 망분리를 위한 우수한 솔루션을 제공합니다. 사용자 및 기기는 역할 및 기기 유형에 따라 세분화될 수 있습니다. FortiLink는 대부분의 FortiGate 모델에 포함되어 있으며, 라이선스가 필요 없고, 무료입니다. 통합을 위해 추가적인 소프트웨어 및 관리 콘솔이 필요하기 때문에 복잡성과 비용이 증가하고 종종 반복적인 요금도 발생하는 대부분의 네트워크 액세스 공급업체와 다릅니다.

또한 포티넷은 사용자 및 네트워크 활동을 지속적으로 모니터링하고 내부 및 규정 준수 요건을 충족하기 위한 보고서를 생성할 수 있는 관리 및 분석 도구 제품군을 제공합니다. 인증 솔루션은 단일 로그인, 소셜 로그인 및 종속 포털 인증 옵션을 지원합니다. 분석은 네트워크 위협, 비효율성 및 대역폭 사용을 해석하고 시각화하기 위한 네트워크 보안 로깅, 분석, 보고 기능을 제공합니다. 중앙 집중식 정책 관리, 분석 및 보고는 관리 비용과 구축 시간을 줄일 뿐만 아니라 구성을 단순화합니다.

모든 위치에 맞는 유연성과 확장성

FortiGate NGFW는 다양한 구성과 여러 가지 폼 팩터로 사용 가능하므로 네트워크 내의 모든 사이트에 적합한 수준의 보호 및 성능을 제공합니다. FortiGate 엔터프라이즈 방화벽은 원격 위치, 사무실 엣지 및 데이터 센터에 적합합니다. 하드웨어 어플라이언스나 가상 머신으로 또는 클라우드 안에 구축될 수 있습니다. 클라우드 또는 데이터 센터에 구축된 FortiGate는 홈 오피스에서 원격 근무자를 보호할 수 있습니다.

사무실 보호

IT 팀이 오늘날의 사무실 환경에서 동적이고 복잡한 다계층 LAN을 구축, 관리, 보호하는 데 어려움을 겪는 경우가 흔합니다. 종종 여러 공급업체의 제품이 설치되기 때문에 이러한 문제는 크기와 구성 모두에 기인합니다. 공통 프레임워크가 없으면 네트워크가 통합 솔루션보다는 "볼트온" 방식으로 결합된 개별 보안 솔루션으로 구성됨으로써 구축 및 관리 문제를 모두 야기하는 경우가 많습니다.

보안 중심 네트워크를 통해 포티넷 LAN 솔루션은 FortiGate 내에 LAN 관리 및 보안 기능을 중앙 집중화함으로써 사무실의 LAN 복잡성을 줄입니다. FortiLink를 활용하는 FortiGate는 보안 및 네트워크 액세스 계층의 중앙 집중식 컨트롤러로, 액세스 계층을 자동화된 포티넷 보안 패브릭에 연결하고 보안 중심 네트워크를 지원합니다. 액세스 계층 관리를 FortiGate에 통합한 FortiLink는 네트워크 및 보안 기능 모두를 단일 대시보드에서 관리할 수 있도록 합니다.

유무선 구성 및 관리를 FortiGate와 통합하면 지원하고 관리해야 할 운영 체제가 하나뿐이며 네트워크 액세스 기능과 보안 기능을 위한 구성도 하나뿐입니다. 따라서 이동, 추가, 변경, 문제 해결, 정책 변경 및 일상적인 작업이 단순해집니다. 오류 가능성이 줄어들고 네트워크 및 보안 기능의 알림과 상태를 간단하게 관리할 수 있습니다.

지사 보호

디지털 혁신으로 인해 최신 기술과 혁신을 활용하는 새로운 아키텍처와 비즈니스 요건이 등장하면서 지사 네트워크도 발전해 왔습니다. IT 기업은 멀티 클라우드 아키텍처를 지원하고, SaaS (Software-as-a-Service) 애플리케이션에 신속하게 액세스하고, BYOD(Bring-Your-Own-Device) 및 IoT 기기를 안전하게 네트워크에 연결해야 합니다. 이러한 혁신에 네트워크를 맞추다 보면 보안이 필요한 새로운 네트워크 엣지가 생깁니다.

분산된 기업들은 지사 운영을 재검토하면서 LAN 및 광역 네트워크(WAN) 플랫폼의 통합이 개선될 것을 기대합니다. LAN-엣지 장비를 기반으로 하는 포티넷 SD-Branch 솔루션은 SD-WAN의 기능을 엔터프라이즈 브랜치 네트워크로 확장합니다. 포티넷 시큐어 SD-WAN 기술이 네트워크 액세스와 통합되어 업계에서 가장 안전하고 관리하기 쉬운 원격 브랜치를 제공합니다. IoT 장치의 폭증을 해결하기 위해 포티넷 시큐어 SD-Branch는 추가적인 온보드 NAC(Network Access Control) 기능과 함께 FortiGate를 네트워크 센서로 활용하여 관리자가 IoT 기기를 검색하고 보호할 수 있도록 합니다.

SD-Branch는 공통 관리 플랫폼과 통합 보안이 포함된 FortiLink를 통해 작동하므로 방화벽 인터페이스와 동일한 수준으로 유선 이더넷 스위치 및 무선 WLAN 인터페이스를 제어할 수 있습니다. FortiLink 스위치 및 무선 통합에는 라이선스가 필요하지 않습니다. 모든 FortiGate에서 실행되는 FortiOS에 포함되어 있습니다.

FortiGate 내의 유무선 네트워킹 융합은 NGFW 보안, 스위치, 익스텐더 및 AP를 하나의 상호운용 가능한 솔루션에 결합함으로써 보안 SD-WAN 솔루션의 기능을 브랜치 액세스 계층으로 확장합니다.

이러한 통합을 통해 보안, 네트워크 액세스 및 SD-WAN의 브랜치 관리를 간소화함으로써 인프라 복잡성을 줄일 수 있습니다. 제한된 인력에 부담을 줄 수 있는 여러 공급업체, 인터페이스 및 운영 체제를 없애는 동시에 서로 다른 솔루션 사이에 발생하는 틈새를 메웁니다. SD-Branch는 단일 대시보드 인터페이스를 통해 민첩성을 높임으로써 브랜치를 더 정확하게 파악하고 제어할 수 있게 해줍니다. 또한 TCO(Total cost of Ownership) 개선을 위해 간편한 배포를 지원합니다.

원격 근무자 원격 사무소 보안

원격 근무가 새로운 것은 아니지만, 일반적으로 원격 근무를 최소화하는 것에서 최대화하는 것으로 세계적인 흐름이 바뀌었습니다. 수많은 설문조사에 따르면 기업들은 2020년 팬데믹이 종식된 후에도 이전보다 더 많은 원격 근무자를 고용할 예정인 것으로 나타났습니다. 이는 원격 근무 보안에 대한 투자가 현재와 미래의 핵심이라는 것을 의미합니다.

포티넷은 원격 인력을 안전하게 지원하기 위한 완벽한 솔루션을 제공합니다. 포티넷 원격 AP 솔루션 세트는 강력합니다. 기업 네트워크에서 FortiGate에 의해 관리되는 FortiAP 하드웨어를 기반으로 합니다. 포티넷 보안 패브릭을 원격 근무자의 집으로 확장하면 원격 근무자를 최신 사이버 위협으로부터 보호함으로써 네트워크 보안을 보장할 수 있습니다. FortiGate NGFW는 로컬 및 원격 AP를 모두 관리할 수 있습니다. SSID(Service Set IDentifier) 트래픽은 방화벽 포트와 동일한 수준의 검사 및 보안을 받으며 기업의 전체 보안 프로파일의 통합 요소가 됩니다. 포티넷 보안 패브릭은 FortiAP 무선 액세스 포인트는 물론 해당 AP에 있는 모든 전환 포트를 통해 원격 근무자의 홈 오피스까지 확장됩니다.

FortiDeploy 옵션(FortiCloud 제품군의 일부)을 사용하면 원격 AP를 간단하게 설치할 수 있습니다. FortiAP는 IP 주소를 얻고 인터넷에 연결되면 FortiDeploy 시스템에 체크인하여 어떤 FortiGate를 연결하여 관리해야 하는지를 파악합니다. IT 부서가 FortiDeploy 인터페이스 내에서 해야 할 일은 각 FortiAP의 무선 관리에 사용될 FortiGate의 IP 주소를 설정하는 것뿐입니다. 사용자는 이 정보를 알고 있거나 수동 구성 단계를 수행할 필요가 없습니다. FortiGate는 발견된 FortiAP에 자동으로 맞추고 구성을 푸시하도록 구성될 수 있습니다. FortiAP가 연결되면 AP에 올바른 기업 이미지를 설치하며, AP가 기업 SSID를 만들기 시작합니다.

요약

포티넷 보안 중심 네트워크 덕분에 기업은 전반적으로 동일한 수준의 서비스와 보호를 유지하면서 대규모 에코시스템의 일부분으로 LAN 엣지를 포괄적으로 보호할 수 있습니다. 구축 스타일을 유연하게 선택할 수 있는 이 솔루션을 회사의 보안 태세에 맞게 조정함으로써 보안과 개방성 간의 균형을 유지할 수 있습니다.

포티넷 LAN 엣지 솔루션은 단일 대시보드에서 보고 제어할 수 있는 포티넷 보안 패브릭에 통합되어 있습니다. 포티넷 보안 패브릭의 모든 요소는 다른 부분과 통신하여 워크플로 및 위협 인텔리전스 공유를 자동화합니다. 따라서 과중한 업무에 시달리는 보안 팀이 수동 프로세스에 소비하는 시간을 최소화하는 동시에 빠르게 위협, 침입 및 침해에 대응할 수 있습니다.

[1] "VMware Releases Cybersecurity Threat Survey Report Detailing Increased Attack Volume and Breach Levels in the United States," VMware, 2020년 7월 14일.

www.fortinet.com/kr

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

766366-0-0-EN