FORTINET

백서

손쉬운 유무선 보안 네트워크 구축

주요 과제 및 해결 방안

종합 요약

액세스 계층은 기업 네트워크에서 가장 넓은 공격면을 노출합니다. 유선 이더넷 스위치 및 무선 액세스 포인트를 통해 IoT(Internet-of-Things) 기기는 물론 직원, 계약업체 및 방문고객을 위한 모든 네트워크 연결까지 지원합니다. 매일 네트워크에 연결하는 기기 수가 계속 증가함에 따라 액세스 계층 보안을 보장하는 것이 매우 중요합니다. 또한, COVID-19 팬데믹 동안(그리고 그 이후에도) 원격 작업이 새로운 표준이 됨에 따라 액세스 계층 공격을 막기 위한 적절한 보안이 그 어느 때보다 중요해졌습니다.[1]

사무실 LAN을 업그레이드하면 네트워크의 방치된 부분이 새로 교체될 뿐만 아니라 완벽한 종합적 관리 및 가시성을 구현하기 위한 토대가 마련됩니다.[3]

기존 액세스 아키텍처의 문제점

특히 모든 부문의 기업들이 네트워크 연결에 의존하고 있는 현 상황에서 LAN 엣지는 사이버 범죄자들에게 거대하면서도 매우 취약한 목표물이 될 수 있으며, 실제로 공격 횟수는 증가하고 있습니다. 예를 들어 2020년 1분기에는 네트워크 연결 과부하를 일으키려고 시도하는 분산 서비스 거부(DDoS) 공격이 전 분기(2019년 4분기)보다 542% 증가했습니다.[2]

IT 팀이 액세스 계층을 관리할 때 직면하는 구체적인 과제는 다음과 같습니다.

- 다양한 구성 동기화
- 네트워크에 대한 가시성 확보
- 다양한 액세스 수준 관리
- 높은 TCO(Total Cost of Ownership)

보안 네트워크를 보다 효율적으로 관리하기 위해 기업들은 통합 플랫폼 접근 방식을 모색하고 있습니다. IT 팀이 효율적인 운영 방법을 모색함에 따라 유무선 및 보안 기능을 통합적으로 관리하는 솔루션이 보편화되고 있습니다. 그러나 모든 네트워킹 솔루션이 필요한 단순성, 기능 및 성능을 제공하는 것은 아닙니다.

복잡성으로 인해 LAN(Local-Area Network) 과제 발생

기존 LAN 네트워크는 비즈니스의 성장과 사용자 및 기기의 추가로 인해 물리적으로 확장되면서 복잡해지고 있습니다. 따라서 IT 관리자는 다양한 활동을 추적하는데 더 많은 시간을 할애해야 합니다. 지사 또는 원격 사무소가 배치되고 재택 근무자가 증가함에 따라 LAN 상황은 점점 더 복잡해지고 비용이 증가하고 있습니다.

구성 관리

- 큰 사무실에서 하나의 작은 변경 사항 때문에 네트워크의 주요 부분이 중단될 수 있습니다. 기업은 네트워크의 모든 부분이 동기화되어 작동하도록 추가, 변경 및 업데이트를 추적하고 관리할 수 있어야 합니다.
- 원격 사이트의 네트워크 구축도 잠재적인 구성 문제를 안고 있습니다. 여러 원격 위치 및 상이한 브랜치 토폴로지에 공통 표준을 설치하고 감독하면 IT 리소스가 빠르게 소모될 수 있습니다.

네트워크 가시성

- 사무실 네트워크는 항상 드나드는 직원, 계약업체 및 방문고객들의 기기로 인해 언제나 유동량이 넘칩니다. 일반적인 LAN 엣지 가시성은 기기 연결에 대한 세부 정보를 제공할 수 있지만, 사용자 인증 수준 및 관련 리소스 액세스 제한과 같은 상위 계층 기기 컨텍스트가 누락될 수 있습니다.

- IoT 기기는 가시성 측면에서 특별한 문제를 야기합니다. 이러한 기기가 네트워크에 나타남에 따라 IT 팀은 네트워크의 전체적인 보안을 위험에 빠뜨리지 않고 애플리케이션을 지원해야 한다는 압박을 받고 있습니다. 특정 기기에 대한 정보가 액세스 계층 인터페이스에서 제공되는 것뿐이기 때문에 현장 IT 직원이 없는 곳에서는 그렇게 하기가 더 어려울 수도 있습니다.

LAN은 암호화, 액세스 제어, 세분화된 가시성 등의 주요 기능이 누락되는 등 보안 관점에서는 방치되어 왔습니다. 범죄자들은 이제 LAN이 약점이라는 것을 빠르게 깨닫고 있습니다.[4]

높은 TCO(Total Cost of Ownership)

- 현대의 LAN 네트워크는 IT 팀의 다양한 요구를 해결하는 라이선스 및/또는 구독옵션을 더 추가함으로써 복잡성 문제를 해결하려고 노력했습니다. 이러한 모든 기능을 추가하는 과정에서 전체 솔루션 비용은 네트워킹 장비 비용의 2배 또는 심지어 3배까지 증가합니다.
- 또한 LAN 엣지를 관리하고 보호하기 위해 더 많은 시스템과 오버레이 도구가 온라인으로 전환됨에 따라, 이러한 서로 다르고 분리된 솔루션 인터페이스를 모두 배우고 관리해야 하는 IT 팀의 부담이 가중되고 있습니다.

보안

- LAN 네트워크가 점점 더 복잡해짐에 따라, 다양한 인증된 네트워크 사용자를 위한 모든 네트워크 수신 지점의 보안도 지나치게 복잡해질 수 있습니다. 많은 기업은 한 번에 하나씩 격차를 좁히기 위해 개별 포인트 보안 제품을 추가합니다. 이렇게 복잡하고 세분화된 보안 접근 방식은 전체 기업을 위험에 빠뜨릴 수 있습니다. LAN 보안 솔루션의 잘못된 구성 하나가 방대한 네트워크의 침해 사고로 이어질 수 있습니다.

솔루션을 평가할 때 고려할 사항

유무선 LAN 네트워크를 업데이트할 때, 어떠한 기업에서든 의사 결정 프로세스에 고려해야 할 몇 가지 사항이 있습니다.

√ **토폴로지 구조.** 보안 LAN을 구축하는 방법을 살펴볼 때, 한 가지 중요한 측면은 네트워크가 구축될 곳의 특성입니다. 큰 사무실의 집합입니까? 아니면 여러 작은 브랜치의 집합입니까? 연결이 필요한 원격 근무자가 있습니까? 솔루션은 두 가지 이상의 운영 요구 사항이 혼합된 것일 경우가 많습니다. 토폴로지마다 각각의 문제와 한계가 있으므로 선택된 솔루션은 가치를 더하고 각 시나리오에 적합한 기능을 제공할 수 있도록 확장이 가능해야 합니다.

√ **연결된 기기.** 어떤 유형의 기기들이 네트워크에 연결할 예정입니까? 그리고 어떤 사용자들입니까? 외부 기기를 사용하는 게스트 및 계약업체도 액세스해야 하는 경우 LAN을 안전하게 보호해야 합니다. 우수한 LAN 엣지 솔루션은 IT 직원의 지속적인 개입 없이도 모든 유형의 기기와 사용자가 연결할 때 이를 처리할 수 있어야 합니다. 링크 어그리게이션 기술 덕분에 네트워크 설계자는 최종 장치의 증가하는 대역폭 요구를 비교적 쉽게 충족할 수 있습니다.[5]

√ **낮은 TCO.** 위의 모든 기능을 제공하는 솔루션이 있다 하더라도 라이선싱, 활성화, 개별 기능 서브스크립션에 드는 누적 비용이 더해질 수 있습니다. 네트워크 의사결정자는 기업 전체에서 원하는 기능을 모두 사용하려면 얼마나 많은 시스템과 솔루션을 구입해야 하는지, 얼마나 많은 라이선스가 필요한지 그리고 주요 기능에 반복적인 서브스크립션이 필요한지 여부를 주의 깊게 살펴봐야 합니다.

또한 소유 비용이 자본 투자와 서브스크립션을 초과합니다. 각 솔루션마다 구축 및 유지관리를 위해 요구되는 직원 시간도 크게 다를 수 있습니다. 의사결정자는 관리해야 할 솔루션이 얼마나 복잡한지를 물어볼 준비가 되어 있어야 합니다. 박스에서 꺼내서 곧바로 사용할 수 있습니까? 아니면 제대로 작동하기 위해서는 여러 개의 연동 제품이 필요합니까?

√ **통합 보안.** 많은 LAN 솔루션에는 기본 제공되는 보안이 부족합니다. 따라서 사후에 네트워크를 보호하는 "볼트온" 접근 방식이 필요하며, 이는 비용과 복잡성을 모두 가중시킵니다. 보안 옵션을 사용할 수는 있지만, LAN 엣지와 통합되어 있지 않은 경우도 있습니다. 따라서 구성이 새어 나가고 범죄자들이 침입할 수 있는 "틈"이 네트워크에 생깁니다. 네트워크는 최상의 보호는 물론 LAN 인프라 전체를 관리하는 데 최소한의 영향을 미치도록 보안 컨텍스트 내에서 구축 및 유지, 관리되어야 합니다.

안전한 액세스를 위해서는 원활한 솔루션이 필요

유무선 LAN 네트워크는 모든 기업의 중추 역할을 할 수 있지만, 모든 IT팀에 상당한 금전적 및 시간적 투자를 의미하기도 합니다. 올바른 솔루션을 선택하면 IT 및 보안 팀이 회사 이니셔티브를 완벽하게 지원하고 추진하는 데 도움이 됩니다.

현재 시장에는 많은 네트워크 장비 공급업체들이 있으며, IT팀의 VP는 모든 옵션을 면밀히 검토하여 액세스 계층에서의 구축 유연성과 보안 통합을 통해 지속적인 운영을 보장하는 솔루션을 찾아야 합니다.

[1] "In addition to traditional DDoS attacks, researchers see various abnormal traffic patterns," Help Net Security, 2020년 7월 21일.

[2] 상게서

[3] Andrew Froehlich, "A Network's Weakest Link May be Different Than you Think," Network Computing, 2019년 11월 26일.

[4] 상게서

[5] 상게서

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

762006-0-0-EN