CISCO
SECURE

백서
Cisco Public

방화벽의 미래

지금 당장 더 강력한 보안 태세를 실현하는 동시에 미래의 비즈니스 및 보안 요구에 부응할 수 있는 디딤돌 마련

cisco The bridge to possible

목차

요약

이 백서는 네트워크 보안의 진화를 소개하고 미래의 조직 환경을 보호하려면 어떤 조치가 필요한지 알아보기 위해 제작되었습니다.

네트워크에 이기종 장비가 계속 늘어남에 따라 정책을 일관되게 관리 및 시행하고 통합된 가시성을 유지하기가 점점 더 어려워지고 있습니다. 이렇게 상호 연결된 네트워크는 복잡하기 때문에 종종 구성 오류나 실수가 발생하고, 따라서 끊임없이 발전하는 정교한 위협에 취약해집니다.

네트워크에 대한 통제력을 되찾고 일관성을 실현하려면 어떻게 해야 할까요? 무엇보다 방화벽을 중심으로 하는 통합된 보안 방식에서 출발해야 합니다.

방화벽은 여전히 조직 네트워크 보안 전략의 핵심이지만, 네트워크가 진화한 만큼 방화벽도 그에 따라 발전해야 합니다. 과거의 방화벽은 단일 어플라이언스였으며, 네트워크의 수신/발신 '경계부'에서 정책에 따라 네트워크 트래픽을 허용하거나 거부하는 제어 지점의 역할을 했습니다. 그러나 오늘날과 같은 디지털 시대에 성공을 거두려면 방화벽은 단일 장치라는 고정관념에서 벗어나 생각의 폭을 넓혀 '연속 방화벽 구축'이라는 개념을 받아들여야 합니다. 연속 방화벽 구축이란 이기종 네트워크 전체의 논리적 제어 지점에 걸쳐 정책에 따라 전략적으로 조율되는 고급 보안 보호를 위한 방법입니다.

연속 방화벽 구축은 변화하는 비즈니스 및 네트워킹 요구 사항에 맞춰 보안을 더 균형있게 조율하기 위한 핵심 단계가 될 것입니다. 시스코는 기업이 혁신할 수 있도록 방화벽을 토대로 한 통합형 보안 플랫폼 구축에 심혈을 기울여 왔습니다.

> "방화벽은 여전히 조직 네트워크 보안 전략의 핵심이지만, 네트워크가 진화한 만큼 방화벽도 그에 따라 발전해야 합니다."

디지털 혁신을 진행 중인 조직은 연속 방화벽 구축을 통해 지금 당장 더욱 강력한 보안 태세를 실현하는 동시에, 미래의 비즈니스 및 보안 요구 사항을 충족하기 위한 가교를 마련할 수 있습니다.

섹션 1: 방화벽의 역사

네트워크 보안의 진화

전통적으로 방화벽은 네트워크 엣지에서 문지기 역할을 맡아 왔습니다. 방화벽은 모든 것을 포괄하는 제어 지점으로서 네트워크의 경계를 통과하는 네트워크 트래픽을 검사하는 역할을 했습니다. 네트워크의 인그레스/이그레스 지점에 배치된 방화벽에서 통신을 검증했습니다. 본질적으로 내부 네트워크 트래픽은 신뢰할 수 있고 외부 트래픽은 신뢰할 수 없는 것으로 간주되었습니다. 방화벽이라는 단일 제어 지점에서 규칙 집합과 정책을 생성하고 시행하여 원하는 트래픽은 네트워크 안팎으로 이동할 수 있도록 보장하고 원치 않는 트래픽은 차단했습니다.

네트워크 경계가 성을 둘러싼 해자라고 가정하면, 방화벽은 모든 트래픽을 요새 안으로 들여보내거나 밖으로 내보내는 도개교의 역할을 했습니다.

전통적인 네트워크 보안

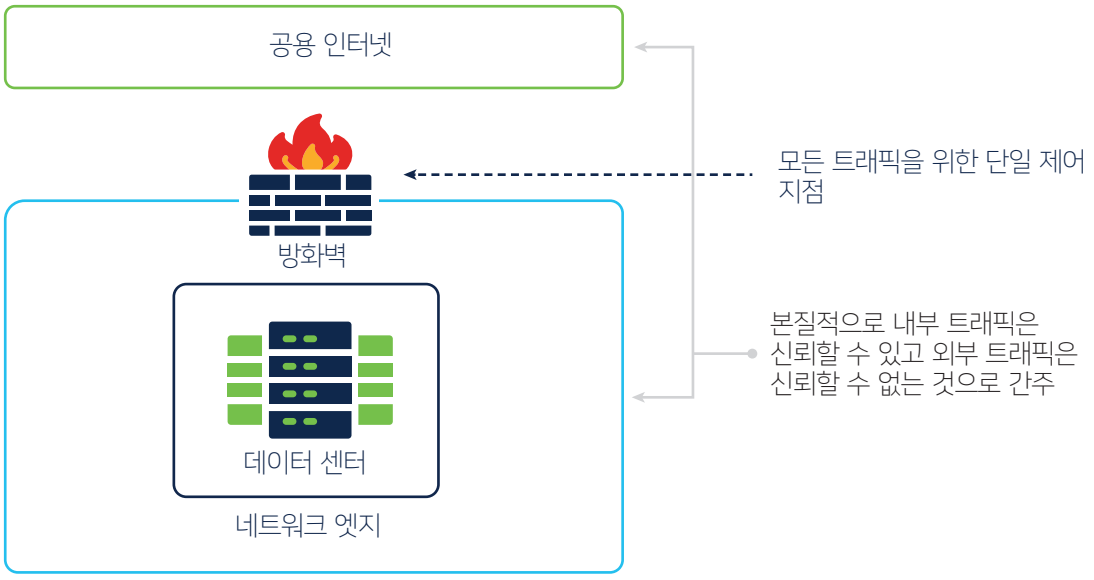


그림 1. 전통적인 네트워크 방화벽 접근 방식

클라우드와 앱의 등장

단일 제어 지점에서 보안을 시행하는 이러한 방식에 문제가 생기기 시작한 것은 얼마 전부터입니다. 먼저 원격 액세스와 엔터프라이즈 이동성이라는 개념이 등장했습니다. 하지만 진정한 혁신은 클라우드 컴퓨팅과 함께 시작되었습니다. 기업이 클라우드로 전환하자 디바이스와 사용자들도 제어형 내부 네트워크를 벗어나 대거 마이그레이션하기 시작했는데, 이로 인해 단일 제어 지점 모델의 효과가 사라졌습니다. 이내 경계는 여러 곳으로 늘어났고, 이러한 모든 경계를 보호해야 했습니다. 네트워크 주변에 해자 하나를 파는 방법은 더 이상 통하지 않았습니다.

오늘날에는 브랜치 오피스와 원격 직원, 클라우드 서비스의 사용 증가로 인해 더 많은 데이터가 전통적인 보안 제어 지점을 완전히 우회하여 기존의 "경계"를 벗어나고 있습니다. 그뿐 아니라 많은 기업이 BYOD(Bring Your Own Device) 모델을 채택함에 따라 직원들은 개인 컴퓨터 또는 모바일 디바이스를 통해 민감한 비즈니스 애플리케이션에 액세스할 수 있게 되었습니다. 실제로 직원 중 67% 이상이 직장에서 개인 디바이스를 사용하고 있으며 이러한 추세는 앞으로도 계속 증가할 전망입니다. 공공 장소에서 제공되는 Wi-Fi 네트워크를 통해 모바일 디바이스와 노트북 컴퓨터를 연결하는 경우도 흔히 볼 수 있으며, 심지어 이런 방법이 일상적인 비즈니스 운영에서 매우 중요한 역할을 합니다.

게다가 중요한 애플리케이션과 데이터 중 대부분이 클라우드 기반으로 작동하는 요즘과 같은 상황에서는 압도적 다수의 사업장과 사용자가 인터넷에 직접 연결해야 합니다. 다양한 클라우드 서비스, 운영 체제, 하드웨어 어플라이언스, 데이터베이스 등에 기업의 워크로드가 지속적으로 쌓여 갑니다. 애플리케이션과 데이터는 점점 더 탈중앙화되고, 이에 따라 네트워크는 더욱 다변화되는 추세입니다.

새로운 현실

천편일률적인 과거의 접근 방식은 오늘날의 환경에는 통하지 않는다는 사실이 입증되었습니다.

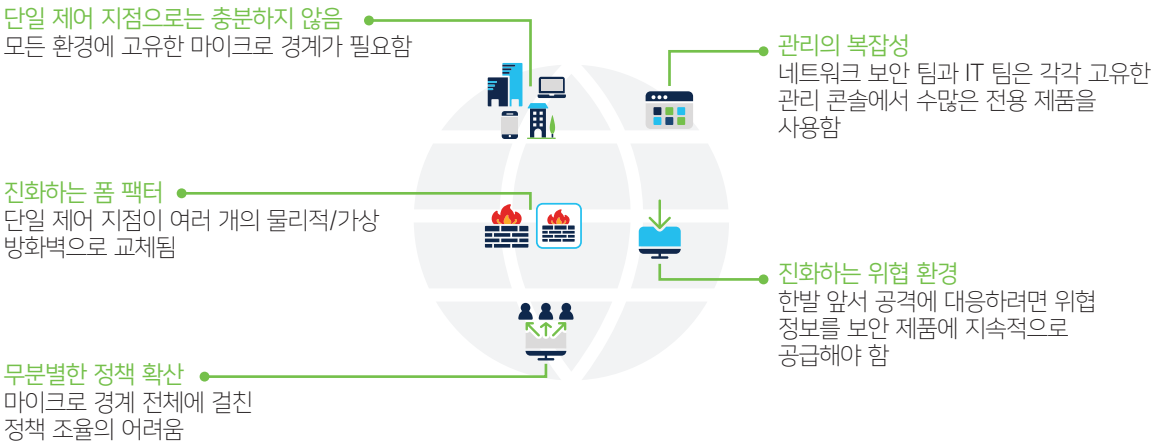
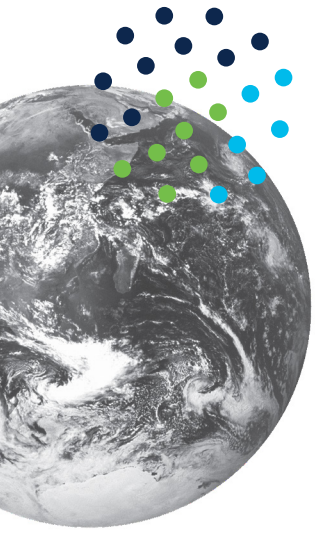


그림 2. 네트워크의 복잡성과 진화하는 위협으로 인해 고전하는 전통적인 방화벽 모델

더욱 복잡해진 새로운 현실

이러한 혁신 기술은 더 촘촘하게 상호 연결되고 생산성 높은 업무 환경을 만들어 주었지만, 그와 동시에 우리의 업무 수행 방식도 완전히 바꾸어 놓았습니다. 온프레미스에서 애플리케이션을 제어하고 사용자를 인증하던 시절은 끝났습니다. 이제 서비스와 애플리케이션을 전사적으로 제공하는 동적 멀티클라우드 에코시스템의 시대입니다. 여기에 더해 비즈니스에 꼭 필요한 서드파티 관계까지 관리해야 합니다. 광범위한 확장과 아웃소싱은 규모의 경제와 효율성을 제공하지만, 여기에는 기회 비용이 따릅니다. 이러한 네트워크 아키텍처의 진화로 인해 공격 표면이 크게 증가했으며 비즈니스 네트워크, 데이터, 사용자를 보호하기가 훨씬 더 복잡해졌습니다.

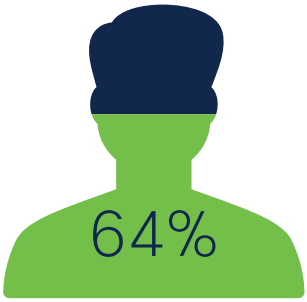
전용 제품으로 반격하기



일반적으로 조직은 새로운 문제가 발생할 때마다 특정 목적으로 구축된 "최상의" 보안 솔루션을 추가하여 그 문제를 해결하고자 했습니다. 이러한 접근 방식 때문에 수많은 디바이스가 무분별하게 "확산"되었고, 평균적인 기업에서는 최대 75개의 보안 툴을 사용하는 것으로 나타났습니다[1]. 서로 다른 벤더의 여러 가지 보안 제품을 사용하면 네트워크 보안 측면에서 심각한 관리 문제를 야기할 수 있습니다. 대부분의 경우, 보안 디바이스와 기능이 늘어날수록 공격 위험은 증가하기 마련입니다. 조사에 따르면 IT 및 정보 보안 전문가의 94%는 네트워크 복잡성 심화로 인한 취약점 증가를 우려하고 있으며, 88%는 네트워크 보안 정책을 애자일 방식으로 바꾸고 싶어합니다[2].

2019년 1월부터 7월 사이에 공개된 데이터 보안 침해 사건은 3,800건에 달하는데, 이는 2018년 상반기에 비해 54%나 급증한 결과입니다[3]. 이러한 급격한 증가세는 공격자가 점점 더 정교한 방법으로 네트워크에 침투하고 있다는 증거입니다. 보안 침해 사건의 성공률이 증가한다는 것은 전통적인 네트워크 보안 방식으로는 더 이상 현대의 위협을 차단하지 못한다는 뜻이기도 합니다.

1 "Defense in depth: Stop spending, start consolidating(심층 보안: 지출 중지, 통합 시작)", CSO, 2016년 3월 4일.
2 "Navigating Network Security Complexity(복잡한 네트워크 보안의 방향 제시)", ESG Research Insights Report, 2019년 6월.
3 "Navigating Network Security Complexity(복잡한 네트워크 보안의 방향 제시)", ESG Research Insights Report, 2019년 6월.



사람의 실수가 설정 오류의 주된 원인

위협, 잡음, 그리고 위험의 증가

공격자는 이메일, BYOD 정책에 따라 검증되지 않은 엔드포인트, 웹 포털, 사물 인터넷(IoT) 디바이스 같은 새로운 벡터를 공격하기 때문에 조직은 여러 가지 새로운 보호 방식을 시도해야 합니다.

위에서 언급했듯이, 전용 제품을 추가하는 방식으로는 조직 전반의 보안 태세를 개선할 수 없습니다. 오히려 그 반대입니다. 이런 방식은 보안 팀이 관리해야 할 "잡음"을 늘리는 결과만 낳습니다. 보안 팀은 알려지거나 알려지지 않은 취약점을 악용하는 새로운 공격과 악성코드를 찾기 위해 경계 태세를 늦추지 않지만, 이처럼 복잡성이 가중되면 보안 정책을 만들고, 관리하고, 시행하는 일이 더욱 까다로워집니다.

이에 대응하기 위해 네트워크 보안 팀은 여러 가지 클라우드 리소스를 개별적으로 구성해야 하는 업무까지 떠안게 되는데, 여기에서 보안 설정 오류가 발생하고 보안 침해로 이어질 가능성이 더 높아집니다. 보안 제어를 아예 구현하지 않는 것도 문제지만, 잘못 구현된 보안 제어는 모든 사고의 가장 큰 주범이 될 가능성이 있습니다. 64%의 조직에서 사람의 실수가 설정 오류의 주된 원인이라고 답변했습니다[4]. 이러한 실수가 컴플라이언스 위반이나 가동 중단으로 이어지든 공격자에게 문을 열어주는 계기가 되든 간에 이것은 조직이 감당할 수 없는 위험입니다.

방화벽에 대해 다시 생각할 때

네트워크 보안은 벅찬 일이 되었습니다. 오늘날의 네트워크 담당자는 방대하게 뒤섞인 전용 제품 솔루션, 클라우드 리소스, 어플라이언스를 관리할 엄두를 내지 못하는 실정입니다. 이제는 다른 접근 방식이 필요합니다.

방화벽을 통합된 애자일 네트워크 보안 플랫폼을 위한 토대로 삼아 현재는 물론 미래의 비즈니스까지 보호해야 합니다.

섹션 2: 방화벽에서 연속 방화벽 구축까지

연속 방화벽 구축 개념을 도입해야 하는 이유

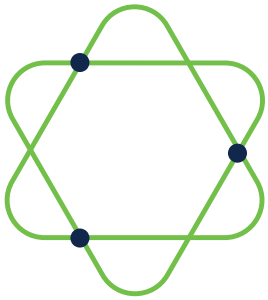
네트워크는 새로운 업무 방식을 수용하는 쪽으로 진화하고 있으며, 네트워크 보안도 그에 따라 발전해야 합니다. IT 에셋이 분산된 현재와 같은 환경에서도, 방화벽은 여전히 강력한 보안 태세의 구심점으로 남아 있습니다.

하지만 광범위한 네트워크 인프라, 커넥티드 디바이스, 운영 체제를 고급 위협으로부터 보호해야 한다는 방화벽 요구 사항이 대폭 증가했습니다. 결과적으로 "전통적인" 방화벽 디바이스는 물리적 및 가상 어플라이언스를 혼합하여 보강한 상태입니다. 그 중 일부는 네트워크에 임베디드되어 있고 다른 일부는 서비스로 제공되거나, 호스트 기반이거나, 퍼블릭 클라우드 환경 내에 포함되어 있습니다. 또 어떤 경우는 대용량 트래픽 요구 사항으로 확장되는 클러스터링 어플라이언스, 개인 디바이스에서 실행되는 소프트웨어, SD-WAN 라우터, 보안 인터넷 게이트웨이 같은 새로운 폼 팩터 형태를 취하기도 합니다. 일관된 위협 가시성과 강력한 보안 태세를 유지하려면 위치에 상관없이 이러한 모든 상이한 방화벽 디바이스 전체에 걸쳐 위협 정보를 공유하는 것이 매우 중요합니다.

현재의 네트워크를 완전히 혁신하고 보안을 강화하려면 전통적인 "경계" 개념에서 벗어나 보호해야 할 정보 또는 애플리케이션에 더 가까운 곳에 전략적 시행 지점을 마련하고, 이를 전체 네트워크 패브릭에 적용해야 합니다. 구체적으로 말하자면 물리적 제어 지점과 논리적 제어 지점 양쪽에 마이크로 경계를 만들어야 합니다.

방화벽을 독립된 물리적 네트워크 디바이스라고 생각하기보다는, 연속 *방화벽* 구축으로 얻을 수 있는 기능에 주력해야 합니다.

4 "Cloud Security Breaches and Human Errors", Fugue, 2019년 2월 7일.



연속 방화벽 구축이란?

오해하지 마세요. 현재 방화벽은 그 어느 때보다 중요한 디바이스입니다. 실제로 오늘날의 네트워크를 보호하려면 **모든 곳에 더 많은** 방화벽이 필요합니다. 차이점이라면 연속 방화벽 구축에서는 **어떻게** 모든 지점에 정책 기반 제어를 구축할 수 있는지 그 방법에 초점을 맞춘다는 것입니다.

연속 방화벽 구축 개념을 선택하면 민첩하고 통합된 접근 방식에 따라 나날이 더 복잡해지는 이기종 네트워크 전체에 대해 정책을 중앙화하고, 고급 보안 기능을 도입하고, 일관되게 시행할 수 있습니다. 이를 통해 포괄적인 보호, 가시성, 정책 조율, 그리고 강력한 사용자 및 디바이스 인증을 확보할 수 있을 것입니다. 또한 연속 방화벽을 구축하면 모든 제어 지점에서 위협 정보를 공유하여 단일화된 위협 가시성과 제어를 확립하는 데도 유리합니다. 이 경우 위협을 탐지하고, 조사하고, 해결하는 데 필요한 시간과 노력이 대폭 줄어들 것입니다.

이렇게 해서 연속 방화벽 구축은 오늘날의 복잡한 네트워크를 보호하기 위한 핵심 전략으로 부상했습니다. 그리고 연속 방화벽은 비즈니스와 위협 환경이 지속적으로 진화하는 미래로 우리를 데려다 줄 가교 역할을 하게 될 것입니다.

연속 방화벽의 형태

클라우드, 온프레미스 또는 원격 위치의 에셋과 데이터를 보호하려면 연속 방화벽 구축을 통해 지능형 위협을 차단하고, 정책을 시행하고, 위협 정보를 공유해야 합니다. 문제는 서로 다른 디바이스를 구축하고 활용하는 상이한 환경 전반에 걸쳐 일관성을 제공하는 것입니다.

보안 침해 사건은 인터넷에 액세스하는 모든 디바이스에서 발생할 수 있습니다. 기업 본사, 데이터 센터, 원격 사이트, 퍼블릭 클라우드 또는 직원이 원격 근무를 하는 위치 등 장소를 가리지 않습니다. 따라서 강력한 보안 제어 지점을 더욱 논리적인 위치에 통합하여 노출을 줄이고 위험을 완화하는 것이 무엇보다 중요합니다. 소유형 환경(물리적 또는 가상 어플라이언스, 라우터 같은 네트워크 디바이스)과 비소유형 환경(SECaaS[Security as a Service]), 네이티브 제어, 워크로드에 대해 필요에 따라 보안 제어를 적용해야 합니다.

연속 방화벽 구축이란?

오늘날의 이기종 네트워크 전체가 연속 방화벽의 시행 지점이 됩니다.

연속 방화벽 구축이란 일관된 정책과 위협 가시성을 토대로 일관된 위협 차단 기능을 제공하여 모든 곳에서 더 빠르고 더 정확하게 공격을 예방, 탐지, 차단할 수 있도록 지원한다는 뜻입니다.

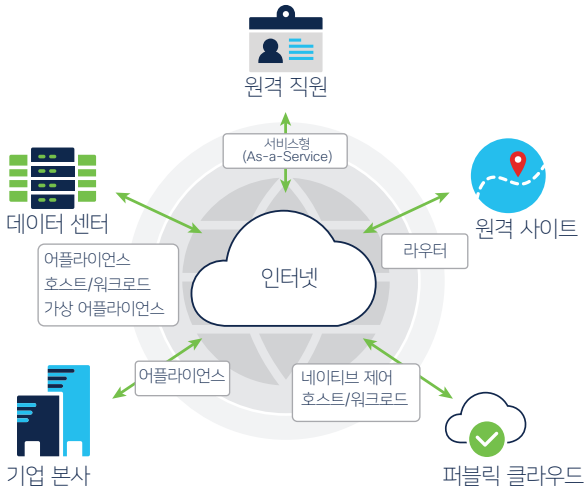


그림 3. 현대식 네트워크의 보안 문제를 해결하기 위해 구축하는 연속 방화벽의 핵심 구성 요소

보안 제어 확장

전통적인 방화벽 개념에 따르면 모든 내부 트래픽과 인증된 사용자는 본질적으로 신뢰할 수 있으므로(외부 트래픽은 제외) 네트워크 경계에서 전체 조직을 보호하기 위한 조치를 취했습니다. 이러한 네트워크 경계는 전체 조직을 보호하기 위한 논리적 보안 제어 지점이 되었고 본사, 데이터 센터 또는 원격 작업에서 발생하는 모든 네트워크 트래픽은 이 단일 제어 지점을 통해 한곳으로 모였습니다.

물론 이 모델은 오늘날과 같이 복잡한 환경에서는 효과가 없습니다. 오늘날 조직의 IT 인프라는 광범위한 폼 팩터 및 제공 모델(물리적/가상 어플라이언스, 네트워크 임베디드 라우터 또는 스위치, 서비스형 제공, 호스트 기반, 퍼블릭 클라우드에 포함 등)로 구성되어 있기 때문입니다.

연속 방화벽 구축 방식에서는 일관된 보안 제어를 구축하여 완전한 가시성, 통합된 정책, 포괄적인 위협 가시성을 제공할 수 있습니다. 갈수록 이기종 디바이스가 늘어나는 네트워크 환경에서 이러한 보안 제어를 토대로 더욱 강력한 사용자 및 디바이스 인증을 구현할 수 있습니다. 사용자, 위치, 디바이스 등에 대한 상황 정보를 수집, 공유, 대응하여 정해진 보안 요구 사항을 충족하는 디바이스만 액세스를 허용합니다. 모든 마이크로 경계에서 일관된 보안 제어를 사용하면 보안 팀은 업무 자동화(예: 컴플라이언스 위반 사용자 및 디바이스 자동 격리, 모든 보안 제어 전체에서 의심스러운 도메인 차단, 효과적인 마이크로 세그멘테이션 지원)를 시작할 수 있습니다. 연속 방화벽을 구축하면 완전한 가시성을 바탕으로 모든 보안 알림과 보안 침해 지표를 총체적으로 파악할 수 있으며, 공유된 위협 정보에 따라 연결된 모든 디바이스에서 최신 위협 탐지가 가능합니다.

클라우드 기반 관리

그리고 이는 단순한 전용 제품이 아닙니다. 네트워크 경계 및 클라우드 리소스의 폭증으로 인해 보안 침해에 노출될 가능성도 높아졌습니다. 복잡한 클라우드 환경에서 비즈니스의 가장 중요한 에셋을 안전하게 보호하는 동시에 다양한 보안 제품을 관리하는 것은 결코 간단한 일이 아닙니다. 보안 팀에 필요한 것은 설정 오류를 줄일 수 있는 즉각적인 가시성과 간소한 관리 방식입니다.

클라우드 기반의 중앙 집중적 관리가 가능한 연속 방화벽을 구축하면 보안 태세가 더욱 강화됩니다. 따라서 보안 팀은 복잡하지 않게 정책을 조정하고 조직 전체에 적용할 수 있습니다. 템플릿은 정책을 한번 작성한 후 네트워크 전체의 수많은 보안 제어 전 범위에 걸쳐 이러한 정책 시행을 확장하므로, 정책 설계 및 일관성을 향상할 수 있습니다. 표준 정책 템플릿을 사용하여 새로운 디바이스를 신속하게 구축하면 설정 오류를 줄이는 데 도움이 됩니다. 조직이 성장하여 새로운 솔루션을 구축할 때도 최신 정책이 자동으로 적용됩니다. 확장 가능한 정책 관리 시스템이 여러 가지 보안 기능을 단일 액세스 정책으로 통합하고, 보안 디바이스 전반에 걸쳐 정책을 최적화하여 불일치 항목을 식별한 후 이를 신속하게 수정합니다.

그뿐만 아니라, 중앙화된 클라우드 기반 관리 솔루션은 팀의 역량을 한 차원 더 높여 줍니다. 모든 디바이스의 위험을 신속하게 파악하여 보다 일관되고 철저한 보안을 실현할 수 있습니다. 단일 관리 콘솔에서 모든 디바이스의 개체를 비교하면서 취약점을 찾아내고 현재의 보안 태세를 최적화할 수 있습니다. 담당자는 정책 관리를 간소화하고, 효율성을 향상하고, 더욱 일관된 보안을 실현하는 동시에 복잡성을 줄일 수 있습니다.

위협 정보를 활용한 방어

네트워크 경계가 확장되고 인터넷에 직접 연결하는 디바이스 수가 늘어나면서 공격 표면도 넓어지고 있습니다. 악성코드, 암호화폐, 피싱, 봇넷을 이용한 사이버 보안 위협이 증가하고 있으며, 사이버 범죄자는 머신러닝 및 AI로 방향을 틀어 기존의 소프트웨어 취약점을 악용하고 악의적인 공격에 박차를 가하고 있습니다. 모든 소프트웨어 벤더의 취약점 패치를 완전히 테스트하고 선별할 수 있을 만큼 리소스가 충분한 조직은 거의 없습니다. 대부분의 조직은 새롭게 진화하는 위협의 맹렬한 공격을 막아내는 데 어려움을 겪고 있습니다.

바로 이 부분에서 연속 방화벽의 또 한 가지 장점이 진가를 발휘합니다. 최첨단 기술에 기반한 최신 위협 연구를 통한 업계 최고의 위협 정보를 활용하고, 보호 업데이트를 적용하면 끊임없이 지속되는 위협을 완화하는 데 도움이 됩니다. 위협 연구원은 보안 침해 지표를 신속하게 식별하고 위협을 빠르게 확인한 후 이를 공유합니다. 목표는 규모의 경제를 이용하여 위협이 더 커지기 전에 조직을 보호하는 것입니다. 상호 연결된 네트워크, 엔드포인트, 워크로드, 클라우드 환경 전체에서 위협 정보를 공유하면 보안 팀이 연관성 없어 보이는 이벤트의 상관관계를 분석하고, 잡음을 제거하고, 위협을 더 빨리 차단하는 데 도움이 됩니다.

연속 방화벽을 구축하지 않을 경우 발생하는 위험

네트워킹이 발전함에 따라 조직은 비즈니스 요구 사항 및 운영을 지원하기 위해 다양한 전용 제품을 채택하고 구축해 왔습니다. 문제는 새로운 공격 벡터가 확인될 때마다 똑같은 조치를 취했다는 것입니다. 즉, 이들은 XYZ 위협을 차단하기 위해 제품을 계속 추가했습니다. 여러 경계 전체에서 연결된 모든 디바이스를 보호하려 하는 전통적인 방화벽에 의존하는 조직의 경우, 가장 중요한 데이터와 에셋이 보안 침해에 노출될 위험이 있습니다. 2019 Cybersecurity Almanac에 따르면 사이버 범죄로 인한 전 세계의 피해 금액은 2021년까지 연간 6조 달러에 이를 것으로 예상됩니다[5].

이러한 위협은 포괄적 네트워크 보안 및 엔드포인트 가시성이 부족한 기업의 네트워크에 빠르게 잠입한 후 비즈니스 운영을 위태롭게 할 수 있습니다.

하지만 조직의 모든 사이트에 있는 네트워크, 클라우드 환경, 디바이스, 데이터를 보호하는 것은 보안 팀에 막대한 부담을 안겨 줍니다.

연속 방화벽 구축은 미래에 대비한 네트워크 보안의 핵심인 방화벽에서 시작해서 방화벽으로 끝납니다.

시스코는 이러한 비전을 실현하기 위해 각고의 노력을 기울여 왔습니다. 시스코는 전 세계 모든 규모의 기업 및 엔터프라이즈와 협업을 진행하고 있습니다. 그리고 이러한 모든 기업에는 더욱 민첩하고 더욱 통합된 네트워크 보안이 필요하며, 네트워크 자체에 이러한 기능이 통합되어 있어야 합니다. 그렇기 때문에 시스코는 역대 최고로 안전한 아키텍처이자 방화벽이 포함된 강력하고 포괄적인 플랫폼을 기본 토대로 제공하고자 합니다.

이러한 개념을 통해 지금껏 접해본 적 없는 수준의 보호 기능을 제공하는 것이 시스코 보안 전략의 핵심입니다. 시스코 보안 포트폴리오 및 시스코의 방화벽 제품군은 필요한 모든 곳에서 세계적인 수준의 보안 제어, 일관된 정책 및 가시성, 보안 운영을 향상하는 혁신으로 진화하는 위협에 맞서 늘 한발 앞설 수 있도록 뒷받침합니다.

위협 환경이 그 어느 때보다 동적으로 변화한 이 시대에, 시스코는 네트워킹 리더십과 최첨단 기술을 함께 제공하여 현재는 물론 미래에도 가장 강력한 보안 태세를 유지할 수 있도록 합니다.

5 "2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics (2019 사이버보안 연감: 100가지 사실, 수치, 통계)", Cybercrime Magazine, 2019년 2월 6일.

전통적인 방화벽은 시야가 한정적이었습니다. IT 팀이 위협을 조기에 더 빨리 탐지하고 차단하려면 위협 정보 공유를 통해 전체 네트워크를 폭넓게 조망할 수 있어야 합니다. 통합된 관리와 포괄적인 보안 기능(예: 침입 차단, URL 필터링, 자동화 및 머신러닝을 활용한 고효율 고급 악성코드 차단)을 기반으로 종합적인 보안 태세를 보장하여 연속 방화벽을 한층 더 강화할 수 있습니다.

연속 방화벽 구축 전략을 마련하지 않을 경우, 네트워크 복잡성이 설정 오류로 이어져 보안 침해의 위험을 높일 수 있습니다. Gartner 보고서에 따르면 "2022년까지 클라우드 보안 오류의 약 95%는 고객의 실수로 인해 발생할 것으로 예상"된다고 합니다.[6] 여러 제어 지점에서 보안 정책을 조율하는 연속 방화벽 구축 전략을 채택하면 조직의 전반적인 보안 태세가 향상됩니다.

섹션 3: 연속 방화벽 구축 전략을 수립하는 4단계 과정

1단계: 현대적인 차세대 방화벽을 활용하여 성공적인 연속 방화벽 구축 전략의 토대를 마련합니다. 귀사에 꼭 맞는 Cisco Secure Firewall을 선택하세요. 일관된 보안 정책, 가시성, 향상된 위협 대응으로 통합형 보안 솔루션을 구축할 수 있습니다.

2단계: 원하는 Cisco Secure Firewall을 선택했으면, 그 다음 단계는 관리 솔루션을 표준화하는 것입니다. 귀사에 알맞은 솔루션을 결정할 때 고려해야 할 요인은 다음과 같습니다.

- 기본 관리 위치(온프레미스 또는 클라우드) 및 보안 관리를 담당할 그룹(보안 운영 또는 네트워크 운영)을 결정합니다.
- 관리 솔루션을 IT 팀의 현재와 미래 목표에 맞춰 조율하는 것이 가장 중요합니다. 워크로드를 클라우드로 전환하거나, 벤더 포털을 시작하거나, 디지털 혁신 프로젝트 또는 SaaS 애플리케이션을 처리하기 위해 클라우드 기반의 관리를 채택할 수 있습니다. 모놀리식(Monolithic, 일체형) 레거시 애플리케이션에 의존하는 조직이라면 온프레미스 애플리케이션이 적합할 수 있습니다. 일반적으로 레거시 애플리케이션을 클라우드에서 올바르게 실행하려면 약간의 리팩토링이 필요하며, 이러한 애플리케이션으로 즉시 업그레이드할 계획이 없다면 온프레미스 관리 시스템이 대개 가장 알맞습니다.
- 네트워크 운영 팀이 조직 전체의 정책을 조율하고, 복잡성을 줄이고, 중앙 대시보드에서 모든 보안 제어 지점을 관리하는 데 도움이 되는 클라우드 기반 관리 솔루션입니다. 이러한 솔루션은 한 지점에서 정책을 오케스트레이션하고 일관되게 관리하는 작업을 간소화하여 최신 위협을 차단합니다. 중앙화된 클라우드 기반 애플리케이션을 활용하여 보안 관리를 간소화하고, 템플릿으로 새 디바이스 구축 속도를 단축하고, 환경 전체에서 시간 경과에 따른 변경 사항을 추적할 수 있습니다.

3단계: 통합하여 보안 태세를 강화합니다. 연속 방화벽 구축 전략은 모든 마이크로 경계 전체를 포괄하고, 연결된 모든 디바이스와 보안 솔루션에 보호 및 제어 기능을 제공해야 합니다. 이기종 네트워크 전체의 클라우드 앱, 서비스, 회사 이메일, 모든 연결된 엔드포인트에서 보안을 통합하면 점점 더 확장되는 위협 환경으로부터 비즈니스를 안전하게 보호할 수 있습니다.

이 단계에서 보안 팀은 더 많은 위협을 차단하고, 지능형 위협에 더 빨리 대응하고, 네트워크 전체의 클라우드 앱과 엔드포인트에 대해 자동화를 수행합니다.

6 "Is the Cloud Secure?(클라우드는 과연 안전한가?)" Gartner, 2018년 3월 27일.

4단계: 마지막으로, 연속 방화벽 구축 전략에 지속적인 지능형 위협 분석을 통합하여 비즈니스 에셋을 보호하고 새로운 위협을 선제적으로 차단합니다. 가장 쉬운 한 가지 방법은 방화벽을 통해 네트워크에 최신 위협 정보를 자동으로 제공하는 솔루션을 선택하는 것입니다. 보안 팀은 최신 정보와 완전한 가시성을 활용하여 최신 취약점을 파악할 수 있습니다. 그리고 위협이 내부로 침입할 경우 위협이 발생한 지점과 발생 경위를 파악할 수 있습니다. 구축 당시 기본으로 내장된 차세대 IPS 기능이 위험 점수 평가 및 영향 플래그를 자동화하여 우선순위를 알려 주므로 가장 중요한 에셋과 정보를 식별하고 우선순위를 정할 수 있습니다. 보안 팀은 즉시 시정 조치를 취하고 위협을 해결할 수 있습니다. "잡음"에 파묻히는 대신 가장 중요한 에셋에 계속 집중할 수 있으므로 SOC 운영의 보안이 더욱 강화됩니다.

적절한 기반 방화벽을 선택하는 단계부터 시작

오늘날 보안 팀에게 필요한 사항:

복잡한 네트워크를 보호하고 위협을 조기에 탐지한 후 더 빨리 조치를 취할 수 있도록 업계 최고의 위협 정보를 제공하는 **향상된 보안**

네트워크 전반에 걸쳐 **보안 정책을 효율적으로 설정, 확장, 조율**할 수 있는 방법

통합된 관리 및 자동화로 보안 운영을 가속화하고 경험을 향상하기 위한 **가시성 및 낮은 복잡성**

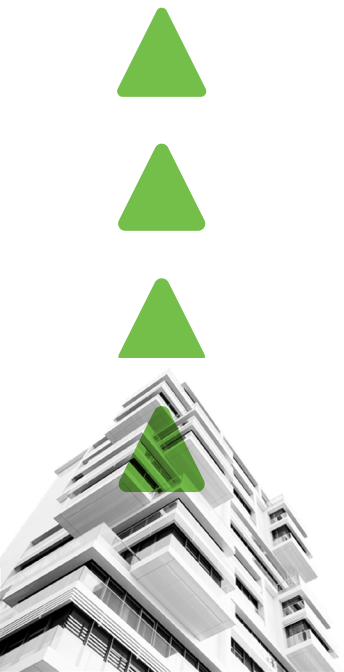
서로 연동되면서 기존의 투자 가치를 극대화하는 네트워킹 및 보안 심층적인 통합을 바탕으로 모든 곳에서 모든 것을 보호하는 포괄적인 보안 솔루션이 이상적입니다.

Cisco Secure Firewall을 사용한 연속 방화벽 구축 전략의 이점

전체 네트워크를 보안 아키텍처의 확장으로 전환: 공통된 정책, 침입 방지 기능 및 기타 핵심 기능을 Cisco Secure Firewall와 공유하면 스위치 및 라우터에서 보안을 시행하고 네트워크 인프라를 포괄적인 보안 포트폴리오로 연계할 수 있습니다. 아키텍처 전체에서 위협 정보를 공유하면 연관성 없어 보이는 이벤트의 상관관계를 분석하고, 잡음을 제거하고, 위협을 더 빨리 차단할 수 있습니다.

세계적인 수준의 보안 제어: Cisco Secure Firewall은 오늘날 갈수록 더 정교해지는 공격에 맞서 복잡한 네트워크를 보호할 수 있는 뛰어난 위협 차단 효과를 제공합니다. 조직은 업계 최고의 고급 위협 정보를 통해 새로운 악성코드 도메인 및 악성 URL, 알 수 없는/발견되지 않은 취약점을 찾아내 위협을 조기에 탐지하고 더 빨리 조치를 취할 수 있습니다. 구축 당시 기본으로 내장된 차세대 IPS는 자동화된 위험 점수 평가 및 영향 플래그로 포괄적인 가시성을 제공하여 보안 팀이 우선순위를 파악한 후 잡음을 최소화할 수 있도록 합니다. 회귀적 보안을 통해 최초 탐지 후 지속적으로 알림을 제공하고 위협을 분석하므로 처음에는 탐지되지 못했던 정교한 악성코드를 더욱 잘 식별할 수 있게 됩니다.

통합된 정책 및 위협 가시성: 보안 팀은 네트워크 어플라이언스에서 호스트까지, 그리고 클라우드 전체까지 모든 디바이스에 걸쳐 보안 제어를 표준화하고 푸시하여 정책 일관성 및 조율을 실현할 수 있습니다. 시스코의 유연하고 중앙화된 관리를 통해 확장형 제어를 여러 디바이스에 적용하여 일관된 정책을 빠르고 쉽게 유지할 수 있습니다. 애플리케이션 방화벽, NGIPS, AMP 등 긴밀하게 통합된 보안 기능 간에 자동화된 위협 상관관계 분석과 통합 관리를 통해 복잡성을 해소합니다. 확장된 네트워크 전체에서 보안 정책 및 디바이스 관리를 간소화하고, 주요 보안 운영(예: 탐지, 조사, 해결)의 속도를 높입니다.



섹션 4: 미래에 대비한 보안 솔루션

이제 우리의 업무 방식은 달라졌습니다. 비즈니스와 네트워크의 혁신으로 인해 네트워크 보안의 규칙도 달라졌습니다. 이제 우리도 방화벽에 대해 다시 생각하고 연속 방화벽 구축이라는 개념을 받아들여야 합니다.

시스코는 업계 최고의 위협 정보에 기반한 일관된 보안 정책과 가시성을 통해 고객이 필요한 모든 곳에서 세계 정상급 보안 제어를 제공하는 보안 플랫폼을 활용하여 혁신을 주도하고 있습니다. 최신 Cisco Secure Firewall은 긴밀하게 통합된 시스코 제품 포트폴리오의 기본 토대입니다.

시스코의 플래그십 클라우드 관리 솔루션인 **Cisco Defense Orchestrator**로 시스코의 다양한 보안 제품 전체에 대해 정책을 조율할 수 있습니다.

모든 시스코 보안 제품에는 **보안 위협 대응** 기능이 포함되어 있으며, 이는 전체 보안 아키텍처에서 보안 대책을 자동으로 공유 및 구축하여 새로운 사이버 공격에 대응하는 자동화된 위협 대응 솔루션입니다.

보안 엔드포인트는 글로벌 위협 정보, 고급 샌드박싱, 실시간 악성코드 차단 기능을 제공합니다. AMP는 확장된 네트워크 전체에서 파일 활동을 지속적으로 분석하여 지능형 악성코드를 신속하게 탐지하고, 억제하고, 제거합니다.

Talos Threat Intelligence는 기존의 위협 및 진화하는 위협에 대한 정보를 수집하는 위협 연구원, 데이터 과학자, 엔지니어로 구성된 세계적으로 유명한 위협 정보 연구 팀입니다. Talos는 전체 시스코 보안 에코시스템을 지원하고 공격 및 악성코드를 차단하는 보호 기능을 제공합니다. Talos는 최신 글로벌 위협, 방어 및 완화에 대한 실행 가능한 정보, 모든 시스코 고객을 적극적으로 보호하기 위한 집단 대응을 정교한 가시성으로 지원합니다.

SNORT NGIPS(SNORT Next-Generation Intrusion Prevention System)는 트래픽 분석, 패킷 스니핑/로깅, 프로토콜 분석을 수행하는 세계 최고의 오픈 소스 NGIPS입니다. SNORT NGIPS는 Talos 위협 정보를 활용해 진화하는 위협을 차단하는 정책을 공유하여 전체 보안 커뮤니티를 지원합니다.

ISE(Identity Services Engine)를 통해 모든 곳에서 상황 기반의 신뢰할 수 있는 적응형 액세스를 제공합니다. 이러한 액세스는 인텐트 기반 정책 및 컴플라이언스 솔루션을 통해 지능적이고 통합된 보호 기능을 제공합니다.

Secure Access by Duo는 다단계 인증, 엔드포인트 가시성, 원격 액세스 및 SSO(Single Sign-On, 단일 인증)를 통한 적응형 인증 및 정책 시행을 제공하여 애플리케이션에 대한 액세스를 선제적으로 보호합니다.

Secure Network Analytics, Secure Workload, ACI(Application Centric Infrastructure)는 서로 연동되므로 머신러닝, 행동 모델링, 네트워크 인프라 텔레메트리, 세그멘테이션을 사용해 모든 곳에서 사용자 및 애플리케이션 워크로드를 감시하여 새로운 위협보다 한발 앞서 정보를 파악합니다.

시스코 보안 플랫폼 및 Cisco Secure Firewall에 투자하여 미래에 대비한 연속 방화벽 구축 전략을 수립하세요. 현 시점에서 가장 강력한 보안 태세가 보장될 뿐 아니라 미래에도 대비할 수 있습니다.

섹션 5: 오늘부터 시작하는 방화벽의 미래

시스코는 네트워킹 분야의 리더십과 최첨단 보안 기술을 결합하여 가장 안전한 아키텍처를 제공합니다. 기존의 투자를 최적화하여 네트워크 보안을 향상하려는 경우든 아니면 라우터를 방화벽으로 전환하려는 경우든, 시스코는 지속적으로 혁신을 추진해 나갈 것입니다.

Cisco Secure Firewall은 네트워크를 구축한 기업에서 디지털 환경으로 혁신 중인 기업을 위해 설계된 네트워크 보안입니다.

Cisco Secure Firewall에 대해 자세히 알아보고 바로 지금 미래에 대비한 연속 방화벽을 구축하기 시작하세요. 2020년 글로벌 네트워킹 트렌드 보고서(GlobalNetworking Trends Report)에서 미래의 네트워크를 만들어 나가는 최신 동향을 자세히 알아보세요.