Cisco Secure Firewall

목차

네트워크와 보안 통합

세계 최고 수준의 보안 제어 기능

일관적인 정책과 가시성

전체 네트워크를 활용하여 보안 아키텍처 확장

비즈니스 크리티컬 애플리케이션이 클라우드와 온프레미스 기반으로 조합되어 있으며 어디에서나 사용자가 리소스에 안전하게 액세스해야 하는 상황에서, 기존의 방화벽 접근 방식으로는 보안을 지키기 어렵습니다. 당사의 단일 네트워크 경계는 여러 마이크로 경계로 진화해 왔습니다. 진화하는 하이브리드 업무 환경 속에서, 애플리케이션은 많은 조직의 새로운 경계입니다. 기존의 방화벽 구축은 물리적, 가상, 클라우드 네이티브 어플라이언스의 혼합으로 진화했습니다. 그 결과, 조직은 최신 애플리케이션 환경을 위한 지원을 운영하는 데 어려움을 겪고 있습니다. 그 어려움이란 조직을 위험에 노출하는 취약성을 개방하지 않고 일관적인 가시성, 정책 시행, 일관된 위협 가시성을 유지하는 방법에 관한 것입니다.

시스코에서는 네트워크 보안 비전인 NetWORK를 구축하고 있으며 이를 통해 현대의 유동적인 애플리케이션과 다양해지는 네트워크에서 정책과 시행의 조화를 이루기 위한 더욱 민첩하고 자동화된 통합 접근 방식이 가능해집니다. Secure Firewall은 코어 네트워킹 기능과 네트워크 보안의 가장 면밀한 통합을 제공하여 가장 안전한 아키텍처를 제공합니다. 그 결과 중소기업에서 대기업 데이터 센터와 통신 사업자에 이르기까지 모든 곳에서 애플리케이션과 사용자를 보호하는 완전한 보안 포트폴리오를 만들 수 있습니다.

장점

- 유동적인 애플리케이션 환경에서의 통합 제어를 위한 통합된 실시간 워크로드와 네트워크 보안
- 네트워크 보안에 대한 플랫폼 접근 방식, 더 빠른 탐지를 위한 주요 소스의 인텔리전스 활용 및 공유, 대응, 문제 해결을 통해 조직, 사용자, 중요 애플리케이션을 보호하는 강력한 위협 방지 기능으로 언제 어디서나 모든 디바이스에서 고도로 안전한 엔터프라이즈 액세스를 사용해 원격 근무자 보호
- Cisco XDR 자격은 Cisco Secure 포트폴리오 전반의 위협 상관관계를 활성화하고 인시던트 대응을 가속화하는 보안에 대한 긴밀한 통합 접근 방식을 위해 모든 Cisco® Secure Firewall에 포함되어 있습니다.

시스코를 선택해야 하는 이유

Cisco Secure Firewall 포트폴리오는 복잡하게 진화하는 위협에 맞서 더 강력한 네트워크 보호를 제공합니다. 시스코와 함께하면, 통합적이고 민첩한 보안의 기반을 다지고 현재의 위협에 효율적으로 대응하며 미래에 대비할 수 있습니다.

데이터 센터, 브랜치 오피스, 클라우드 환경 및 그 사이 어느 곳에서나 시스코의 역량을 활용하여 기존 네트워크 인프라를 방화벽 솔루션의 확장으로 전환할 수 있으며, 필요한 곳 어디서나 세계 최고의 보안 제어를 이용할 수 있습니다.

지금 Secure Firewall 어플라이언스에 투자하면 암호화된 트래픽을 검사할 때 성능 저하 없이 가장 정교한 위협에 대한 강력한 보호를 확보할 수 있습니다. 여기에 다른 시스코와 타사 솔루션을 통합하여 광범위하고 심층적인 보안 제품 포트폴리오를 완성하면 모든 제품이 함께 연동되면서 단절되어 있던 이벤트 간의 상관관계를 찾아내고, 노이즈를 제거하며, 위협을 더 빨리 차단해 줍니다.

우수한 가시성과 제어

위협은 점점 더 정교해지고 있으며 네트워크도 점점 더 복잡해지고 있습니다. 최신 상태를 유지하면서 지속적으로 진화하는 위협을 성공적으로 막는 것만을 전담으로 하는 리소스를 보유한 조직은 많지 않습니다.

위협과 네트워크의 복잡성이 증가함에 따라 데이터, 애플리케이션 및 네트워크를 보호할 적절한 도구를 보유하는 것은 필수입니다. Cisco Secure Firewall은 위협보다 앞서 움직이는 데 필요한 역량과 유연성을 갖추고 있습니다. 규모에 맞게 암호화된 트래픽을 검사하는 목적 기반 하드웨어인 *암호화 가속기*를 통해 이전 세대의 어플라이언스에 비해 크게 향상된 성능을 제공합니다. 또한, 멀티스레드 Snort 3 검사 엔진의 사람이 읽을 수 있는 규칙이 보안을 간소화하는 데 도움이 됩니다. 이와 함께 다양한 네트워크와 워크로드에서 오늘날의 첨단 애플리케이션을 일관된 방식으로 보호해 주는 Cisco Secure Workload 통합을 통해 애플리케이션을 유동적으로 모니터링하고 제어합니다.

귀사에 적합한 방화벽을 찾아보세요.

간소화되고 일관된 정책 관리

Secure Firewall 포트폴리오의 유연한 미래 보장형 관리 기능으로 더 강력한 보안 태세를 갖출 수 있습니다. 시스코는 비즈니스 요구 사항에 맞도록 맞춤화된 다음과 같은 다양한 관리 옵션을 제공합니다.

- **Cisco Secure Firewall Device Manager:** 로컬로 단일 방화벽을 관리합니다. Firewall Threat Defense에 대한 내장형 관리 솔루션입니다.
- **Cisco Secure Firewall Management Center:** 대규모 방화벽 구축을 관리합니다. 온프레미스, 프라이빗 클라우드, 퍼블릭 클라우드, SaaS(Software as a service)와 같은 모든 폼 팩터에서 사용할 수 있습니다.
- **Cisco Defense Orchestrator:** Cisco Secure Firewall, Meraki MX, Cisco IOS® 디바이스와 같은 여러 시스코 제품의 보안 정책과 디바이스 관리를 간소화하는 클라우드 기반 관리자입니다.

시스코는 또한 확장 가능한 로그 관리를 위해 Cisco Security Analytics and Logging을 제공합니다. 이는 위협 탐지를 강화하고 더 오랜 보존과 동작 분석 기능을 통해 조직의 컴플라이언스 요건을 충족합니다.

고객 사례

Cisco Secure Firewall의 고급 기능

고급 기능	세부 사항
Cisco Secure Workload 통합	• 오늘날의 애플리케이션은 광범위한 네트워크 및 워크로드에 알맞게 분산되어 동적으로 작동합니다. 이러한 첨단 애플리케이션에 대한 포괄적인 가시성과 정책 이행을 보장하는 Cisco Secure Workload(Tetration) 통합을 활용하면 확장 가능한 보안을 일관성 있게 구축할 수 있습니다.
Cisco Secure Firewall Cloud Native	• Kubernetes를 통해 구축되었으며 AWS에서 최초로 사용 가능한 Secure Firewall Native Cloud는 고도로 탄력적인 클라우드 네이티브 인프라 구축을 위한 개발자 친화적인 애플리케이션 액세스 솔루션입니다.
동적 정책 지원	• 유동적 속성은 고정 IP 주소를 사용할 수 없는 상황을 위해 VMware, AWS, Azure 태그를 지원합니다. • 시스코는 보안 그룹 태그(SGT), Cisco Identity Services Engine(ISE) 속성 지원을 통해 태그 기반 정책의 선구자 역할을 해왔습니다.
Snort 3 침입 방지 시스템	• 업계를 선도하는 오픈 소스 Snort 3을 사용한 위협 보호의 다음 단계가 탐지를 개선하고, 사용자 지정을 간소화하고, 성능을 강화하는 데 도움이 됩니다.
암호화된 가시성 엔진	• Cisco Secure Firewall의 고유한 암호화된 가시성 엔진 기능은 머신러닝과 인공 지능을 사용해 암호 해독 없이도 암호화된 트래픽의 섀도우 IT와 악의적인 애플리케이션을 식별합니다.
TLS(전송 계층 보안) 서버 ID 및 검색	• 암호화된 TLS 1.3 트래픽에서 레이어 7 정책을 유지할 수 있습니다. 모든 트래픽 플로우를 하나하나 암호 해독하고 검사하는 것이 현실적으로 불가능한 암호화된 환경의 가시성과 제어를 유지합니다. 경쟁사의 방화벽이 암호화된 TLS 1.3 트래픽으로 레이어 7 정책을 무력화합니다.
Cisco Secure Firewall Management Center	• 방화벽, 애플리케이션 제어, 침입 방지, URL 필터링, 악성코드 방어 정책에 대한 통합형 관리 기능을 제공합니다. • Cisco Secure Workload(구 Tetration)와 통합하면 네트워크와 워크로드 전반에서 유동적인 애플리케이션을 위한 일관적인 가시성 확보와 정책 시행이 가능합니다.
Cisco Defense Orchestrator	• Cisco Secure Firewall 전반의 정책을 일관적이고 쉽게 관리하도록 지원하는 클라우드 기반 방화벽 관리입니다.
Cisco Security Analytics and Logging	• 실시간 위협 탐지와 더 빠른 대응 시간을 위한 동작 분석을 통해 고도로 확장 가능한 온프레미스 및 클라우드 기반 방화벽 로그 관리입니다. 또한 보안 태세를 개선하여 향후 공격 시도를 더 잘 방어하기 위해 지속적으로 분석합니다. • 모든 Cisco Secure Firewall에서 로그 어그리게이션을 통해 컴플라이언스 요구 사항을 충족합니다. • 직관적인 단일 뷰에서의 방화벽 로그 데이터 수집과 확장된 기록 및 분석을 위해 방화벽 관리자와 긴밀히 통합합니다.
Cisco XDR	• Cisco XDR 플랫폼을 활용하여 위협 탐지와 문제 해결 속도를 높이세요. 모든 Cisco Secure Firewall에는 Cisco XDR을 위한 자격이 포함되어 있습니다. Firewall Management Center의 내장된 리본을 통해 SecOps가 Cisco XDR 개방형 플랫폼으로 즉시 전환하여 인시던트 대응을 더 빠르게 할 수 있습니다.
Cisco Talos® 위협 정보	• Cisco Talos Intelligence Group은 세계 최대 규모의 위협 정보 기업 중 하나입니다. 시스코 고객, 제품, 서비스를 위해 정확하고 신속하며 실행 가능한 위협 정보를 제공합니다. Talos는 Snort.org, ClamAV, SpamCop의 공식 규칙 집합을 유지 관리합니다.

다음 단계

Cisco Secure Firewall에 대한 자세한 내용은 cisco.com/go/firewall을 참조하세요.

구입 옵션을 확인하고 시스코 영업 담당자와 상담하려면 cisco.com/c/en/us/buy를 방문하세요.

미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

미국에서 인쇄 C45-736624-06 05/23