Cisco NGIPSv for VMware

제품 개요

업계 최고의 위협 차단. 실시간 상황 인식. 풀스택(full-stack) 가시성. 인텔리전트 보안 자동화. 이 모든 요소를 갖춘 Cisco® NGIPSv for VMware는 Cisco FirePOWER™ NGIPS(next-generation IPS) 솔루션의 가상화 버전으로 신뢰할 수 있는 보안을 실현합니다. 이 효과적인 침입 방지 시스템은 안정적인 성능과 낮은 TCO(total cost of ownership)를 제공하며, 서브스크립션 라이센스 옵션으로 위협 차단 기능을 확장하면, AMP(Advanced Malware Protection), AVC(application visibility and control), URL 필터링 기능까지 제공합니다. Cisco FirePOWER 어플라이언스는 세계적인 정보 보안 리서치 및 자문 회사인 NSS Labs가 실시한 연구에서 측정한 위협 탐지 실효성, 검사 처리량, 그리고 그 가치를 인정받아 업계의 벤치마크로 자리매김하였습니다.

가상화 솔루션의 이점

서버 가상화는 비즈니스 측면에서 중요한 이점을 제공합니다. 비용을 줄이고 신속한 구축을 가능하게 하며 시스템 가용성을 높일 수 있습니다. 그러나 가상화 구현에는 잠재적 보안 위험이 수반됩니다.

- 토폴로지 또는 컨피그레이션의 변경이 감지되지 않아 "사각지대"가 형성됩니다.
- 네트워킹이나 보안과 같이 다른 그룹에서 별도로 관리하던 기능이 통합되어 잘못된 컨피그레이션이 발생할 수 있습니다.
- 적절한 조치나 관리 없이 순식간에 VM(Virtual Machines)이 확산되는데, 이를 VM 스프롤(VM sprawl)이라고 합니다.

Cisco NGIPSv for VMware는 가상 환경 내에서 Cisco의 최고 NGIPS 솔루션을 구축할 수 있도록 함으로써 가상화로 인한 위험을 해결합니다. 이 가상화 NGIPS는 가상 시스템 간의 트래픽을 검사할 수 있으며, 물리적 자산과 가상 자산의 보호를 강화함으로써 리소스가 제한적인 원격 사이트에서의 NGIPS 솔루션 구축 및 관리를 수월하게 합니다.

가상화로 인해 저하된 가시성 보강

가상 네트워크는 동적 특성 때문에 가상 네트워크 토폴로지뿐 아니라 개별 가상 호스트의 컨피그레이션도 정기적으로 변경됩니다. 안타깝게도 대부분의 시스템 관리 솔루션은 이러한 변화를 인식하지 못합니다. 의도적이었든 실수였든 변경이 잘못되면 부지불식간에 주요 처리 환경이 보안 위험에 노출될 수 있습니다.

예를 들어 동일한 물리적 호스트에 서로 다른 두 개의 가상 네트워크가 구축됩니다. 하나는 프로덕션 환경이고 다른 하나는 개발 환경으로서 프로덕션 환경을 위한 소스 코드가 들어 있습니다. 잘못된 컨피그레이션이나 뜻하지 않은 정책 위반으로 이 두 가상 네트워크가 연결되면 막대한 보안 위험으로 이어지나, 외부에서는 이를 인식할 수 없습니다.

Cisco NGIPSv for VMware는 이러한 변화를 알려주므로 잘못된 컨피그레이션과 정책 위반이 실제로 문제를 일으키기 전에 바로잡을 수 있습니다. 또한 가상 네트워크와 개별 VM 간의 악성 트래픽이 있는 경우, 이를 식별하고 방해함으로써 위협을 차단합니다. Cisco NGIPSv for VMware는 가상 세계에 대한 가시성을 제공하므로, 처리 환경에서 결정적인 이 영역을 더욱 효과적으로 제어하고 보호할 수 있습니다.

더욱 편리하고 광범위해진 보호 환경 구축

물리적 어플라이언스에서 사용하는 전용 하드웨어는 데이터 센터와 같은 고성능 구축에 특히 유용하지만, 추가 비용이 발생하며 일부 활용 사례에는 적합하지 않을 수 있습니다. 물리적 어플라이언스는 최종 위치까지 배송되어야 합니다. 전 세계적으로 일부 지역은 까다로운 통관 요건 때문에 하드웨어 배송 시 막대한 비용 또는 시간이 소요될 수 있습니다. 랙 공간과 전원을 할당해야 합니다. 뿐만 아니라 일부 환경에서는 필수 인증 또는 열악한 운영 환경 때문에 매우 까다로운 하드웨어 요구 사항을 따라야 합니다.

가상 어플라이언스는 소프트웨어 기반이므로 Cisco NGIPSv for VMware는 물리적 어플라이언스 구축이 불가능한 NGIPS 활용 사례에 이용할 수도 있고, 운영 비용도 절감됩니다. 다음과 같은 장점이 있습니다.

- 기존 하드웨어에 구축하고 즉시 트래픽 모니터링 시작
- IT 보안 리소스가 없는 위치 모니터링
- 물리적 어플라이언스 구축이 사실상 불가능한 네트워크 영역 모니터링
  (예: 소매점, 원격 사무실)
- 보안 분석가가 동일한 Cisco FireSIGHT™ Management Center에서 물리적 및 가상 NGIPS 어플라이언스를 모두 관리할 수 있어 책임의 분리 가능

PCI(Payment Card Industry) 규정준수를 가상 환경으로 확대

PCI 보안 표준 위원회의 가상화 SIG(Special Interest Group)에서 발행한 정보 부록인 "Securing Virtual Payment Systems"에는 가상 환경에서 PCI 규정을 준수하고 유지하는 방법에 대한 명확한 지침이 소개되어 있습니다. 이 새로운 지침은 폭넓은 내용을 담고 있으며, 가상 CDE(cardholder data environment)에 대해 구체적인 보안 관련 권고 사항을 제시합니다. 여기에는 다음 내용이 포함됩니다.

- 이제 네트워크 보안은 가상 환경에 적합하게 적용되어야 합니다.
- CDE의 주요 포인트를 모니터링할 때에는 반드시 IDS(Intrusion Detection System) 또는 IPS를 사용해야 합니다(PCI 요건 11.4).
- IDS 및 IPS 툴은 가상 네트워크와 VM 간의 트래픽을 모니터링할 수 있어야 합니다.

Cisco NGIPSv for VMware는 카드 소지자 데이터 또는 PII(Personally Identifiable Information)가 있는 주요 가상 네트워크를 모니터링하고 VM 간의 트래픽을 검사합니다. 물리적 버전과 동일한 NGIPS 컨트롤 및 보호 기능을 제공합니다. Cisco NGIPSv는 최대 8개의 vCPU를 사용하여 검사하고 VMware ESXi 5.x 플랫폼을 지원합니다.

PCI 요건 6.3.2에 따르면 개발, 테스트, 프로덕션 환경은 각각 분리되어야 합니다. Cisco NGIPSv for VMware는 이러한 네트워크 간에 트래픽이 발생하면 알려주기 때문에 이 요건을 준수할 수 있습니다.

Cisco NGIPSv for VMware의 활용 가능 분야

- PCI 핵심 서버, 소규모 지점/지사, 원격 사이트(예: 소매점)
- IT 보안 조직이 분산된 기업
- 하드웨어 제약이 있는 환경(예: 자동차, 군용 선박, 실외 구축)
- 하드웨어 인증 요건이 많은 조직
- 공간 제약이 있는 환경(데이터 센터의 랙 공간 부족)
- 확장된 실시간 네트워크, 사용자, VM 검색
- 연구소 또는 교육장 네트워크
- 관리 보안 서비스 제공업체 또는 클라우드 컴퓨팅 환경

시스템 요구 사항

표 1에서 Cisco NGIPSv for VMware의 최소 요구 사항을 확인할 수 있습니다.

표 1. 시스템 요구 사항

하이퍼바이저	VMware ESX 5.0, 5.1
CPU	vCPU 4개
메모리	4GB
디스크 공간	40GB
네트워크 인터페이스	vNIC 2개 이상, 10개 이하

품질 보증 정보

품질 보증 정보는 Cisco.com의 Product Warranties(제품 보증) 페이지를 참조하십시오.

주문 정보

고객이 제품을 설치하고 사용하기 위해 주문해야 하는 모든 구성 요소나 부품에 대해 이해할 수 있도록 도와주십시오. 부품 번호는 표 2를 참조하십시오. 여기서는 고객의 편의를 위해 Cisco Ordering Tool로 직접 연결되는 링크와 부품 번호 목록도 제공합니다.

주문하려면 How to Buy(구매 방법)를 참조하십시오. 소프트웨어는 여기에서 다운로드할 수 있습니다.

표 2. 주문 정보

제품 이름	부품 번호
Cisco FirePOWER Virtual Appliance and Support Bundle	FP-VMW-IPS-BUN
Cisco FirePOWER Virtual IPS & Apps 1YR Service Subs	FP-VMW-TA-1Y
Cisco FirePOWER Virtual IPS and Apps 3YR Service Subs	FP-VMW-TA-3Y
Cisco FirePOWER Virtual IPS, Apps and URL 1YR Service Subs	FP-VMW-TAC-1Y
Cisco FirePOWER Virtual IPS, Apps and URL 3YR Service Subs	FP-VMW-TAC-3Y
Cisco FirePOWER Virtual IPS, Apps and AMP 1YR Service Subs	FP-VMW-TAM-1Y
Cisco FirePOWER Virtual IPS, Apps and AMP 3YR Service Subs	FP-VMW-TAM-3Y
Cisco FirePOWER Virtual IPS, Apps, AMP and URL 1YR Svc Subs	FP-VMW-TAMC-1Y
Cisco FirePOWER Virtual IPS, Apps, AMP and URL 3YR Svc Subs	FP-VMW-TAMC-3Y
Cisco AMP for FirePOWER Virtual Appl. 1YR Svc Subscription	FP-VMW-AMP-1Y
Cisco AMP for FirePOWER Virtual Appl. 3YR Svc Subscription	FP-VMW-AMP-3Y
Cisco FirePOWER Virtual Appl. URL Filtering 1Y Service Subs	FP-VMW-URL-1Y
Cisco FirePOWER Virtual Appl. URL Filtering 3Y Service Subs	FP-VMW-URL-3Y

자세한 정보

Cisco NGIPSv for VMware에 대한 자세한 내용은 http://www.cisco.com/c/en/us/products/security/index.html을 참조하거나 현지 어카운트 담당자에게 문의하십시오.

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.

Printed in USA C78-733165-00 11/14