White Paper

Five Steps For Securing The Data Center: Why Traditional Security May Not Work

주요 내용

데이터 센터 관리자는 새로운 데이터 센터 환경에서 지원되는 기능과 성능에 영향을 미치지 않으면서 데이터 센터를 보호해야 한다는 중대한 과제에 직면했습니다. 많은 관리자들이 인터넷 취약점을 위해 설계된 솔루션을 사용하여 데이터 센터를 보호하려고 하지만 이러한 솔루션으로는 역부족입니다. 데이터 센터에는 프로비저닝, 성능, 가상화, 애플리케이션, 트래픽 등과 관련한 고유한 요구 사항이 있으며, 인터넷 보안 디바이스는 이러한 요구 사항을 충족하도록 설계되지 않았습니다.

데이터 센터를 보호하려면 다음을 실현할 수 있는 솔루션이 필요합니다.

- 맞춤형 데이터 센터 애플리케이션에 가시성과 제어 능력 제공
- 디바이스와 데이터 센터 간의 애플리케이션 트랜잭션과 비대칭 트래픽 흐름 처리
- 가상화, SDN(software-defined networking), NFV(network functions virtualization), Cisco ACI(Application-Centric Infrastructures) 등 데이터 센터의 발전에 발맞춤
- 공격 전(Before), 공격 중(During), 공격 후(After) 등 공격 전범위에 걸쳐 보호
- 전체 네트워크에 통합된 보안 구축
- 프라이빗, 퍼블릭, 클라우드 환경을 비롯하여 지리적으로 분산된 DC 간에 트래픽 및 구축 지원

주요 공격 대상: 데이터 센터

오늘날 수많은 사이버 범죄는 개인 고객 데이터, 금융 데이터, 기업 지적 재산과 같이 중요한 데이터가 보관된 데이터 센터를 대상으로 일어납니다.[1] 하지만 데이터 센터를 보호하는 일은 매우 어렵습니다. 비대칭 트래픽, 맞춤형 애플리케이션, 검사를 위해서는 컴퓨팅 레이어에서 벗어나 데이터 센터 경계까지 추적해야 할 만큼 방대한 트래픽, 여러 하이퍼바이저의 가상화, 지리적으로 분산된 데이터 센터 등의 요소는 이러한 목적을 위해 설계되지 않은 보안 솔루션으로 데이터 센터를 보호하는 데 걸림돌이 되고 있습니다. 그 결과 보안에 허점이 생기고, 데이터 센터의 성능에 심각한 영향을 초래하며, 보안 제약을 수용하기 위해 데이터 센터의 기능을 희생해야 합니다. 뿐만 아니라 보안 솔루션의 복잡한 프로비저닝 때문에 데이터 센터에서 필요에 따라 리소스를 동적으로 프로비저닝하지 못하게 됩니다.

한편 데이터 센터는 발전을 거듭하면서 물리적 데이터 센터에서 가상 데이터 센터를 거쳐 SDN, ACI와 같은 차세대 환경으로 마이그레이션되고 있습니다. 클라우드의 활용도가 높아지는 한편 인터넷과 네트워크가 제조 환경, 에너지 그리드, 의료 시설, 운송 등의 분야로 확장되는 IoT(Internet of Things: 사물 인터넷) 환경이 등장하면서 데이터 센터 트래픽은 이미 기하급수적으로 증가하고 있습니다.

[1] Cisco 2014 연례 보안 보고서: http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html?keycode=000350063.

Cisco에서는 2017년이면 데이터 센터 트래픽의 76%가 데이터 센터 내에서 발생하며 대부분이 가상 환경의 스토리지, 프로덕션, 개발 데이터에서 생성될 것으로 예측하고 있습니다.[2] Gartner에서는 2015년 말에는 초당 데이터 센터 연결 수가 3,000% 증가할 것으로 예측하고 있습니다.[3]

오늘날 데이터 센터에서는 이미 수많은 애플리케이션, 서비스, 솔루션을 기업에 제공하고 있습니다. 많은 조직에서 지리적으로 분산된 데이터 센터에 구축된 서비스를 이용하여 지속적으로 증가하는 클라우드 컴퓨팅 및 트래픽 요구 사항을 지원하고 있습니다. 이러한 조직에서는 빅 데이터 분석 및 비즈니스 연속성 관리와 같은 전략적 이니셔티브도 지원해야 하는 만큼, 기업의 중추에 있어서 데이터 센터가 차지하는 역할이 더욱 중요합니다. 하지만 이와 동시에 데이터 센터는 악성 공격자의 주요 목표가 되었으며, 공격자는 탐지를 피해 데이터 센터 리소스에 액세스하기 위해 더욱 정교한 위협을 만들어 내고 있습니다. 즉, 보안 팀에서 데이터 센터를 모니터링하고 보호하기가 더욱 까다로워지고 있습니다.

데이터 센터 관리자와 관리 팀이 안고 있는 또 다른 문제는 차세대 방화벽 같은 보안 솔루션을 구축하고 트래픽을 검사하는 데 있어 프로비저닝과 성능 제한이 크게 영향을 미친다는 것입니다. 보안이 데이터 센터의 성능에 영향을 주어서는 안 됩니다. 오늘날의 데이터 센터에서는 보안 프로비저닝에 걸리는 시간이 며칠이나 몇 주가 아니라 몇 시간 또는 몇 분 이내여야 합니다. 또한 방대한 트래픽을 처리할 수 있도록 성능을 동적으로 확장해야 합니다.

데이터 센터 보안을 위한 5단계

포괄적인 데이터 센터 보안을 위해서는 5가지 핵심 영역에서 적용 가능한 심층 방어 전략을 수립해야 합니다. 보안 솔루션은 다음과 같은 요구 사항을 충족해야 합니다.

1. **맞춤형 데이터 센터 애플리케이션에 가시성과 제어 능력을 제공해야 합니다.** 데이터 센터 관리자는 기존의 웹 기반 애플리케이션(예: Facebook, Twitter)과 기존의 인터넷 보안 디바이스에서 검사하는 관련 마이크로애플리케이션 뿐만 아니라 맞춤형 데이터 센터 애플리케이션에 대한 가시성과 제어력을 확보해야 합니다. 대부분의 차세대 방화벽은 인터넷 엣지를 통해 이동하는 트래픽 유형을 검사하도록 설계되었으므로 맞춤형 데이터 센터 애플리케이션을 보호하지 못합니다.
2. **디바이스와 데이터 센터 간의 애플리케이션 트랜잭션과 비대칭 트래픽 흐름을 관리해야 합니다.** 엣지만 보호해서는 안 되며, 데이터 센터 패브릭에 보안이 통합되어야 합니다. 구축된 솔루션으로는 north-south(인바운드-아웃바운드) 트래픽과 east-west(애플리케이션 간) 트래픽 흐름을 모두 검사할 수 없습니다. 오늘날의 데이터 센터 트래픽에서는 애플리케이션 간 트래픽이 많은 비중을 차지합니다. 검사를 위해 애플리케이션 트래픽을 데이터 센터 경계에서 차세대 방화벽으로 전송한 다음 다시 컴퓨터 레이어로 라우팅(헤어핀)해야 할 경우, 솔루션이 오늘날 데이터 센터에 필요한 동적 트래픽 흐름을 방해하는 요소가 됩니다.

   대부분의 차세대 방화벽은 비대칭 트래픽을 보호하지 못합니다. 데이터 센터에 일반적인 비대칭 라우팅의 경우, 패킷이 소스로 복귀할 때는 다른 경로로 이동합니다. 이는 많은 차세대 방화벽이 하나의 예측 가능한 경로로 이동하는 트래픽을 추적, 검사, 관리하도록 설계되었기 때문에 문제가 됩니다.

   데이터 센터용 보안 솔루션은 가상 디바이스를 포함한 디바이스 또는 데이터 센터 간의 애플리케이션 트랜잭션도 처리할 수 있어야 합니다. 가상 디바이스도 물리적 디바이스 못지않게 취약한 만큼, 데이터 센터 보안으로 지속적 워크로드 생성, 해체, 마이그레이션을 비롯한 가상 환경 고유의 당면 과제를 해결할 수 있어야 합니다.

[2] Cisco Global Cloud Index: Forecast and Methodology, 2012-2017: http://www.cisco.com/2012–2017/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html.
[3] Security Week: http://www.securityweek.com/data-centered-focusing-security-combat-rise-data-center-attacks

3. **데이터 센터의 발전에 발맞출 수 있어야 합니다.** 데이터 센터 환경이 물리적 환경에서 가상 환경을 거쳐 차세대 SDN, ACI, NFV 모델로 마이그레이션됨에 따라 보안 솔루션을 동적으로 확장할 수 있어야 하며 발전하는 하이브리드 데이터 센터 환경 전체에서 원활하게 작동하는 보호 기능을 지속적으로 제공해야 합니다. 이처럼 새로운 데이터 센터 모델에서는 가상 디바이스와 물리적 디바이스가 빠르게 프로비저닝되므로 보안 규칙이 제대로 제어되지 않은 상태로 급격히 확장될 수 있습니다. 이미 많은 IT 팀에서 ACL(Access Control List) 관리에 어려움을 겪고 있습니다.

   새 디바이스가 프로비저닝될 때 규칙이 자동으로 적용되어야 보안 문제 없이 구축 기간을 며칠에서 몇 분으로 단축할 수 있습니다. 마찬가지로 하이퍼바이저(가상화 머신 모니터)가 여러 개인 하이브리드 데이터 센터 전체에 단일 보안 솔루션을 구축할 수 있다면 IT 팀에서 보안 관리 오버헤드에 대한 부담 없이 데이터 센터 기능에 집중할 수 있습니다.

4. **공격 전(Before), 공격 중(During), 공격 후(After) 등 공격 전범위에서 데이터 센터를 보호해야 합니다.** 기존의 보안 접근법은 데이터 센터 환경에 대한 위협 인식과 가시성이 제한적이며 주로 경계에서의 차단에 집중합니다. 공격 전범위에서 대처하기 위해서는 네트워크, 엔드포인트, 모바일 디바이스 및 가상 환경 등 위협이 발생할 수 있는 모든 위치에서 동작하는 솔루션을 이용하여 폭넓은 공격 벡터 전반을 모니터링해야 합니다. 오늘날 데이터 센터와 그 고유의 트래픽을 보호하기 위해서는 공격 전, 중, 후에 대한 보안을 포함하여 위협 중심의 전반적인 접근법으로 데이터 센터를 보호해야 합니다.

   전통적인 차세대 방화벽에는 방어 기능을 통과하도록 설계된 스텔스 공격을 식별 및 완화하는 솔루션이 거의 없으며 공격 중지 후 교정 및 분석을 제공하지 못합니다. 또한 데이터 센터에서 생성되는 비대칭 트래픽을 추적하고 보호할 수 없습니다. 이들 방화벽은 거의 방어에만 사용되는 툴이지만 취약한 서버, 고유 애플리케이션, 중요 데이터를 목표로 하는 알려지지 않은 새로운 위협은 방어할 수 없습니다.

5. **전체 네트워크를 보호해야 합니다.** 데이터 센터 보안 솔루션은 중요 데이터 센터 리소스에 직접 연결해야 하는 원격 사용자의 요구 사항을 수용해야 합니다. 따라서 해당 솔루션은 원격 사용자와 데이터 센터 리소스 간에 투명성을 제공해야 하며 브랜치 사무실, 데이터 센터, 클라우드까지 확장되는 복잡한 네트워크 환경의 일부여야 합니다. 보안 솔루션은 데이터 센터 아키텍처의 일부여야 하며, 이와 동시에 전체 데이터 경로에서 보호를 제공하면서 데이터 센터를 표적으로 하는 공격과 인터넷 기반 위협을 모두 파악할 수 있는 더욱 광범위한 솔루션의 일부여야 합니다.

데이터 센터 보안은 다릅니다. 오늘날 데이터 센터 그리고 새롭게 등장하는 데이터 센터 모델에 진정한 보안을 적용하려면 차세대 방화벽에만 의존해서는 안 됩니다. 데이터 센터와 클라우드에 이르기까지 분산된 네트워크 전체에서 성능 저하 없이 일관되고 지능적인 보호를 제공하는 포괄적인 통합 보안 전략과 아키텍처가 필요합니다.

오늘날 데이터 센터의 보안

Cisco에서는 데이터 센터 엣지뿐만 아니라 발전을 거듭하는 오늘날의 데이터 센터 환경까지 방어할 수 있는 강력한 툴을 제공합니다. 데이터 센터 보안을 위한 혁신적인 Cisco® ASA(Adaptive Security Appliances) 솔루션은 물리적 환경과 가상 환경 모두를 보호하도록 설계되었습니다. 조직에서는 이 솔루션을 사용하여 전통적 데이터 센터를 차세대 데이터 센터로 원활하게 마이그레이션하고 미래에 대비한 구축, 투자 보호, 포괄적 보호를 실현할 수 있습니다. Cisco ASA 플랫폼에 새로 추가된 솔루션은 다음과 같습니다.

- **Cisco ASAv(Adaptive Security Virtual Appliance):** Cisco ASAv는 전체 Cisco ASA 방화벽 기능 세트의 가상화 버전으로, 가상 환경에 필요한 동적 확장성과 간소화된 프로비저닝이 결합되어 있습니다. 또한 다양한 하이퍼바이저에서 실행되도록 설계되었고 VMware vSwitch 기술에서 독립적입니다. 따라서 Cisco 환경, 하이브리드 환경, 타사 환경에서도 사용이 가능한, 데이터 센터에 종속되지 않는 솔루션입니다. Cisco ASAv의 유연한 아키텍처는 전통적인 보안 게이트웨이로 구축할 수 있을 뿐만 아니라 지능형 SDN 및 ACI 환경용 보안 리소스로 구축하여 애플리케이션 서비스 체인에 동적으로 직접 통합할 수도 있습니다.

- **Cisco ASA 5585-X with FirePOWER Services:** Cisco ASA 5585-X Adaptive Security Appliance with FirePOWER Services는 전통적 데이터 센터, SDN 및 ACI 데이터 센터 환경을 완벽하게 지원하는 데이터 센터 보안 어플라이언스로, 맞춤형 데이터 센터 애플리케이션을 탐지 및 검사하는 기능을 비롯한 고급 방화벽 및 차세대 IPS 보안 기능을 갖추고 있으며 향상된 성능 및 프로비저닝 기능이 결합되었습니다. 최대 16개 노드의 고급 클러스터링 기능을 제공하며 여러 데이터 센터에 640Gbps의 데이터 센터급 성능을 제공할 수 있습니다. 클러스터링된 솔루션을 단일 디바이스처럼 관리하므로 관리 오버헤드가 크게 줄어듭니다. 5585-X 역시 ASAv와 마찬가지로 SDN, NFV, ACI와 같은 차세대 데이터 센터 환경과 전통적 환경에서 작동하도록 설계되었으며 하이브리드 환경 전체의 보안성을 유지하는 한편 데이터 센터를 마이그레이션할 때도 원활하게 보호해 줍니다.
- **Cisco FirePOWER Next-generation IPS:** FirePOWER는 시장 최고의 NGIPS로 물리적 또는 가상 솔루션으로 사용 가능하며, 데이터 센터 리소스에 대한 연결을 식별 및 평가하고 의심스러운 네트워크 활동을 모니터링합니다. 파일 활동을 거의 실시간으로 모니터링 및 제어하며 특정 파일(특히 악성코드일 가능성이 있는 알려지지 않은 파일)은 샌드박싱(격리하여 파일 실행 및 동작 분석)을 통해 더 상세히 분석하거나 클라우드에서 조회합니다(대규모 커뮤니티 인텔리전스를 통해 평판 확인). 이러한 접근법을 통해 중요한 데이터 센터 트래픽을 세밀하게 분석하고 대응할 수 있습니다.

다음은 포괄적 데이터 센터 보안에 도움이 되는 Cisco의 솔루션입니다.

- **Cisco Identity Services Engine and TrustSec:** UCS Director를 통해 데이터 센터 환경에 새 디바이스나 사용자가 추가될 때 IT 팀에서 보안 정책을 동적으로 생성, 공유, 구현할 수 있습니다. 그런 다음 ISE에서 보안 정책과 시행 규칙이 포함된 보안 그룹 태그를 개별 패킷에 직접 첨부합니다. 또한 이러한 보안 태그 지정을 사용하면 VLAN 및 ACL과 관련된 복잡성과 오버헤드 없이 데이터 센터를 사용자 및 디바이스 역할을 기준으로 세분화할 수 있습니다.
- **Cisco OpenAppID technology for Snort:** IT 팀에서 Cisco OpenAppID 기술을 사용하여 애플리케이션 탐지 기능을 생성, 공유, 구현하고 데이터 센터의 맞춤형 애플리케이션을 위한 맞춤형 규칙을 개발할 수 있습니다. 이 제품은 현재 Cisco에 인수된 Sourcefire에서 개발한 IPS(침입 방지 시스템) 및 IDS(침입 탐지 시스템)인 Snort™를 위한 개방형의 애플리케이션 중심 탐지 언어 및 처리 모듈입니다. Cisco OpenAppID는 Snort 프레임워크와 완벽히 통합되므로 관리자가 네트워크에서 사용되는 애플리케이션에 대해 더욱 자세히 살펴볼 수 있습니다.

  Snort 사용자는 Cisco OpenAppID 탐지기를 사용하여 애플리케이션을 탐지 및 식별하고 애플리케이션 사용에 관해 보고할 수 있습니다. Cisco OpenAppID에서는 보안 관련 이벤트를 포함한 애플리케이션 레이어 컨텍스트를 제공하여 분석을 향상시키고 교정 속도를 높입니다. 또한 Snort에서 특정 애플리케이션 탐지 시 이를 차단하거나 경고하여 모든 위협 표면을 관리하여 리스크를 최소화합니다.
- **Cisco FireAMP™ 및 FireSIGHT™ 솔루션:** 공격 전(Before), 공격 중(During), 공격 후(After)를 비롯한 공격 전범위에서 데이터 센터를 보호하기 위한 전체적인 위협 중심 접근을 제공하려면 지능형 악성코드 분석 및 차단이 필요합니다. Sourcefire의 Cisco FireAMP를 사용하면 빅 데이터를 활용하여 지능형 악성코드 공격을 탐지, 파악, 차단할 수 있습니다. 또한 다른 보안 레이어에서 놓친 위협도 차단할 수 있도록 우수한 가시화 및 통제 기능을 제공합니다. 사용자는 Cisco FireAMP 제품과 Cisco ASA를 결합하여 비대칭 데이터 센터 트래픽에 대한 상세한 조사 및 보호를 제공할 수 있습니다.

  마찬가지로 Sourcefire에서 개발한 Cisco FireSIGHT는 변화하는 환경과 새로운 공격에 대응하는 데 필요한 네트워크 가시성, 컨텍스트, 자동화를 제공합니다. 관리자는 Cisco FireSIGHT Management Center를 사용하여 수백 개의 어플라이언스를 중앙에서 관리할 수 있습니다.

추가 정보

Cisco ASAv 방화벽, Cisco ASA 5585-X 어플라이언스, Cisco Secure Data Center 솔루션 및 Sourcefire 보안 솔루션을 비롯한 Cisco 보안 제품에 대한 자세한 정보를 보려면 www.cisco.com/c/en/us/products/security/index.html을 방문해 주십시오.

Snort 및 Cisco OpenAppID에 대한 자세한 정보를 보려면 www.snort.org를 방문해 주십시오.

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 C11-732259-00 07/14