완벽한 보안 서비스: 상황 인식 기반 차세대 방화벽

Cisco 백서

요약 정보

- 2012년에 인터넷에 연결된 장치는 90억 대였으며 2020년에는 500억 대로 증가할 것으로 예상됩니다.
- 글로벌 데이터 센터 트래픽은 향후 5년간 4배 증가할 것으로 예상되며, 그 중 클라우드 데이터가 가장 빠르게 증가할 것으로 예상됩니다.
- SaaS 및 B2B 애플리케이션은 포르노보다 15배, 불법 소프트웨어보다 8배 더 많이 악성 콘텐츠 전송에 이용될 것입니다. (출처: Cisco 2013 연례 보안 보고서)

IT 혁신이 세계 곳곳에서 변화를 일으키고 있습니다. 2013년 Cisco VNI(Visual Networking Index) 조사에 따르면 2013년 말까지 모바일 연결 장치 수가 전 세계의 인구 수를 초과할 것으로 나타났습니다. 10억 명의 사람들이 Facebook과 Twitter를 사용하고 있으며, 새로운 태블릿, 스마트폰 및 기타 모바일 장치가 빠른 속도로 출시되면서 머스트 해브(must-have) 장치, 애플리케이션 및 서비스를 끝없이 제공하며 소비자를 유혹하고 있습니다.

모빌리티로 인해 비즈니스와 개인 사이의 벽이 허물어지면서 기업의 생산성이 급증하고 일과 생활 사이에서 균형을 찾는 사람들이 늘어났습니다. BYOD(bring-your-own-device) 현상은 업무, 가족 및 여가에 항상 연결되어 있기 위한 방식입니다. 새로운 상황에 적응하지 않고 직원들이 원하는 방식으로 언제 어디서나 일할 수 있도록 허용하지 않는 기업은 고급 인력을 잃을 위험이 있으며 새로운 세대의 인재를 확보하지 못 할지도 모릅니다.

클라우드는 규모와 상관없이 모든 기업의 필수적인 IT 전략이 되었으며 퍼블릭 클라우드 서비스도 매년 두 자릿수의 성장을 하고 있습니다. Gartner는 2013년 퍼블릭 클라우드 시장이 1,310억 달러 규모에 달할 것으로 예측하며 IaaS(infrastructure-as-a-service) 시장이 SaaS(software-as-a-service) 시장보다 빠르게 성장할 것으로 내다보았습니다.[1]

편리한 클라우드 서비스를 이용하는 사람들이 급증하면서 콘텐츠 및 애플리케이션 모델도 변화하고 있습니다. 엔터테인먼트나 협업을 위한 비디오에 대한 수요도 끝이 없어 보입니다. 비디오로 인해 2014년까지 모든 IP 트래픽이 4배로 증가하고, 2016년까지 세계 모바일 트래픽의 70퍼센트를 비디오가 차지할 것으로 예상됩니다.[2]

[1] "Forecast Overview: Public Cloud Services, Worldwide, 2011-2016, 4Q12 Update," Gartner. 2013년 2월 8일. ID G00247462
[2] Cisco Visual Networking Index: 글로벌 모바일 데이터 트래픽 예측 업데이트, 2012년 ~ 2017년. 2013년 2월 6일.

완벽한 보안 서비스: 상황 인식 기반 차세대 방화벽

"향후 10년간 나타날 역동적인 비즈니스와 IT 인프라를 안전하게 지원할 수 있는 유일한 방법은 상황 인식 기반 보안뿐입니다. 정보 보안의 미래는 상황 인식 기반 보안입니다."

Gartner 부사장 및 선임 연구원
Neil MacDonald

새로운 보안 시대

IT의 소비화로 인해 문화의 구조적 변화가 일어나면서 조직이 면밀히 구축해 놓은 기존 보안 계획을 재정비해야 합니다. 합법적, 전문적 사이트를 포함한 백만 개 이상의 웹 사이트가 악성코드에 감염되고 있습니다.[3] 실제로 직원들은 대체적으로 위험하다고 알려진 사이트보다 신뢰하는 사이트의 광고에서 악성코드에 감염될 확률이 더 높습니다.

매초마다 4개의 새로운 악성코드가 만들어지는 이 시대에 정보 보안은 속도 경쟁입니다. 기존 보안 방식과 고정된 정책을 따르기 위해 노력한다면 IT 리소스는 계속 축나게 될 것입니다. 하지만 전담 관리자들은 끊임 없이 노력합니다. 일반적인 방화벽에는 모든 직원에 대해 5개가 넘는 규칙이 있으며 이러한 규칙은 매일 변경됩니다. 보안 관리자는 누가 어떤 애플리케이션에 액세스할 수 있는가를 항상 주시하고 결정해야 하며, 이것은 규정이 복잡한 환경에서 절대 위험성이 작은 것이 아닙니다.

이것은 만만치 않은 도전입니다. IT는 회사의 지적 재산권에서부터 택시에 두고 내린 스마트폰까지 모든 것을 보호해야 할 책임을 집니다. 모빌리티와 BYOD의 증가에도 불구하고 이용 목적 제한 방침(Acceptable Use Policies)을 시행해야 합니다. 이용 목적 제한 방침의 실행은 직원이 어디에 있건 상관이 없으며 직원의 스마트폰, 랩톱 또는 태블릿이 개인 장치이거나 회사에서 발급한 장치이거나도 상관이 없습니다. 또한 애플리케이션을 비즈니스용으로 사용하거나 개인 용도로 사용하는 것도 상관이 없습니다.

보안 리소스는 뜻밖에 얻게 되는 것이 아니며 IT는 지속적으로 악성코드 시그니처를 수정하고 블랙리스트를 업데이트하면서 계속해서 소중한 리소스를 낭비하면 안 됩니다. 다른 공급업체의 방화벽을 추가하는 것도 해답이 될 수 없습니다. 이렇게 하면 복잡성과 구성 오류 위험만 커질 뿐입니다. Gartner에 따르면 "단일 공급업체보다 여러 공급업체의 방화벽을 구성 및 관리할 때의 위험이 더 크다"고 합니다.[4]

IT는 업무 패턴의 변화를 비롯해 장치 및 애플리케이션의 사용의 변화에 맞추어 보안 및 보호를 적용하는 데 더 효율적인 수단이 필요합니다. 이러한 과제를 충족하기 위해서는 사용자의 ID, 사용하는 애플리케이션, 애플리케이션을 사용하는 상황을 고려하는 보안이 요구됩니다.

[3] 2012년 3월 기준 1,159,000개의 사이트가 감염됨. www.stopbadware.com
[4] "One Brand of Firewall Is a Best Practice for Most Enterprises," Greg Young, Gartner Research, 2012년 11월. ID G00217262

완벽한 보안 서비스: 상황 인식 기반 차세대 방화벽

Gartner는 2015년까지 90%의 엔터프라이즈 보안 솔루션이 상황 인식 기능을 제공할 것으로 예측합니다.[5]

차세대 방화벽 - 상황 인식 기반 보안

Cisco ASA 5500-X Series Next-Generation Firewalls는 표적성 공격과 웹기반 악성코드의 위협에 대해 가장 포괄적인 보호를 제공하며 끊임없이 진화하는 위협에 대응할 수 있습니다. Cisco의 차세대 방화벽에는 세계에서 가장 폭넓게 설치되어 보안성과 안정성이 검증된 방화벽(ASA 5500 Series), 동급 최고의 Cisco AnyConnect® VPN 및 네트워크 침입 방지(IPS)의 강점을 갖추고 있으며 Cisco SIO(Security Intelligence Operations)와 연계된 새로운 애플리케이션 제어 및 웹 보안 기능이 추가로 구축됩니다.

이렇게 넓고 깊은 정책 시행을 통해 ASA 5500-X Series는 네트워크 전반의 완벽한 보안을 제공합니다. 조직은 일반적으로 비즈니스 및 개인 용도로 사용하는 협업 애플리케이션 및 Web 2.0을 상황 인식 기반 정책을 바탕으로 모니터링 및 제어할 수 있습니다. 조직은 물리적 및 가상 도메인 전반에 완벽한 보호와 간소화된 관리를 보장하는 보안 정책이 적용된다는 것을 확신할 수 있습니다.

ASA 5500-X Series는 사용자 ID, 장치 유형, 장치 위치, 애플리케이션 유형, 웹 평판 및 위협 정보 등의 상황을 정책에 활용합니다. 관리자는 어떤 사용자와 장치가 네트워크에 액세스하고 있는지를 완전히 파악하고 있기 때문에 장치별 또는 사용자별로 정책을 구현하는 것이 아니라 장치와 사용자 모두를 고려하여 정책을 적용할 수 있습니다. 네트워크 성능에는 영향을 미치지 않고 정책이 네트워크 전반의 상황 안에서 지속적으로 시행됩니다.

최고의 전 세계적 위협 정보

전 세계의 최신 위협 정보를 바탕으로 상황 인식 기반의 차세대 통합 보안을 구현합니다. 쉬지 않고 운영되는 Cisco SIO는 클라우드에서 위협 정보를 방화벽 및 다른 보안 인프라에 실시간으로 알리므로 가장 최신 위협 정보뿐만 아니라 도메인, IP, URL 및 발신자의 평판을 기준으로 결정을 내릴 수 있습니다. 클라우드 기반 정보와 상황 인식 기반 방화벽의 결합으로 최고의 장점을 제공합니다. Cisco는 여러분의 조직이 위협에 노출되기 수 개월 전부터 조직을 보호해줍니다.

예를 들어, 2012년 9월, 보안 연구원들이 IE(Internet Explorer) 버전 6,7 또는 9를 실행하는 취약한 머신에 대해 공격자가 모든 관리자 권한을 갖게 되는 IE의 제로 데이 취약성을 경고하자 보안 제공업체들은 잠재적인 공격으로부터 보호할 수 있는 기존 시그니처를 개발하고 발표하는데 급급했습니다. 그러나, 그로부터 2주 정도가 지나 Cisco SIO는 공격용 악성코드를 호스팅하는 악성 사이트를 자동으로 차단하였습니다. 뿐만 아니라, Cisco는 결과적으로 악성코드를 전파하는데 사용된 도메인의 액세스를 발빠르게 차단하고 같은 공격자가 등록한 40개 이상의 유휴 도메인을 찾아냈습니다. Cisco는 클라우드 기반 정보 및 평판 분석을 통해 소스에서 공격을 저지하고 경쟁사의 솔루션이 어떤 조치를 취하기 몇 주 전에 공격자를 무력화했습니다.

[5] "The Future of Information Security Is Context Aware and Adaptive," Gartner, 2010년 5월 14일. ID G00200385

완벽한 보안 서비스: 상황 인식 기반 차세대 방화벽

Cisco Security Intelligence Operation 하이라이트

- 하루 100TB의 보안 정보
- 1,000개 이상의 애플리케이션 및 150,000개 이상의 마이크로 애플리케이션
- 160만 개의 구축된 보안 장치
- 하루 130억 개의 웹 요청
- 전 세계 엔터프라이즈 이메일 트래픽의 35%
- 하루 930억 개의 이메일 메시지
- 5,500개 이상의 IPS 서명
- 3 ~ 5분 간격으로 업데이트

어디에서나 위협 중단

Cisco Next-Generation Firewalls에서 제공하는 포괄적 위협 보호를 통해 장소와 상관없이 어디에서나 위협을 중단할 수 있습니다. ASA 5500-X Series는 악성코드, 표적 공격, 봇네트(botnet) 및 웹 기반 위협에 대해 동급 최고의 보호 기능을 제공합니다. 내장된 평판 기반 보호 기능으로 공격용 악성코드가 게시되기 훨씬 전에 조직을 보호하고 위협을 가하기 훨씬 전에 차단할 수 있습니다.

웹 기반 악성코드부터 보호를 통해 백만 개가 넘는 감염된 웹 사이트에서 전혀 의심하지 않는 피해자에게 악성코드가 전파되지 않도록 보장합니다. 클라우드에서 모든 웹 트래픽에 대해 최적의 효율성과 구축 간소성을 검사합니다.

ASA 5500-X Series는 또한 세계에서 유일한 평판 기반 침입 방지 시스템을 통합하여 공격자들이 방화벽과 중요 시스템에 침입하지 못하도록 보장합니다. 전 세계에서 거의 2백만 개 이상의 Cisco 보안 장치와 1억 5천만 대의 엔드포인트 장치가 전송하는 원격 정보 제공 기능을 사용하여 Cisco SIO는 데이터를 분석하고 상관관계를 파악하여 웹 사이트의 평판을 평가하고 제로 데이 위협에 대해 실시간에 가까운(near-real-time) 보호를 구현합니다. Cisco SIO는 이 정보를 업데이트하고 전 세계의 Cisco 보안 장치에 하루 24시간, 주 7일 연중 무휴로 3 ~ 5분 간격으로 적용합니다.

마찬가지로, Cisco IPS는 장치 인식, 소스의 네트워크 평판, 대상 값, 사용자 ID를 사용하는 유일한 상황 인식 기반 IPS이므로 관리자는 더 적극적인 정책을 시행할 수 있어 네트워크 리소스에 더 심각하거나 즉각적인 위험을 일으킬 수 있는 위협에 더 적극적으로 대응할 수 있습니다.

ASA 5500-X Series는 봇네트(botnet) 감시 기능도 제공합니다. 따라서 감염된 USB 같이 조직의 장치가 감염될 경우 빠르게 식별하고 격리하여 더 큰 피해가 발생하지 않도록 합니다.

비즈니스 요건이 변화하더라도 차세대 방화벽에 대한 투자를 보호할 수 있습니다. Cisco ASA 5500-X Series Next-Generation Firewalls는 업계에서 가장 폭넓게 설치된 보안성과 안정성이 검증된 방화벽과 포괄적 차세대 네트워크 보안 서비스를 결합하므로, 조직에서 현재 필요한 보호 기능부터 사용하기 시작하여 필요에 따라 추가 보안 서비스 레이어를 더할 수 있습니다. 단, 위협 정의, 애플리케이션 제어, 위협 관리, 포괄적 보안을 추가하더라도 성능에 미치는 영향은 없습니다.

세밀한 애플리케이션 가시성 및 제어

비즈니스와 개인 애플리케이션 사이의 선이 모호해지면서 IT는 더 이상 Facebook, Twitter, LinkedIn을 일괄적으로 "나쁜" 것으로 규정하고 사용을 차단할 수 없습니다. 소셜 미디어 애플리케이션의 사용이 비즈니스에 꼭 필요하게 되면, IT는 유연하게 애플리케이션과 해당 구성 요소에 대한 단계적인 제어를 할 수 있어야 합니다.

Cisco AVC(Application Visibility and Control) 소프트웨어 모듈은 모바일, 협업, Web 2.0 애플리케이션뿐만 아니라 Facebook 게임과 같은 마이크로 애플리케이션에도 가장 높은 수준의 가시성과 제어 기능을 제공합니다. AVC는 1,000개 이상의 애플리케이션과 15만 개 이상의 마이크로 애플리케이션을 식별하므로 관리자가 전체 애플리케이션 범주를 손쉽게 허용 또는 거부할 수 있고 마이크로 애플리케이션에 대한 액세스를 선택적으로 허용할 수 있습니다.

AVC는 또한 애플리케이션 행동을 식별하고 애플리케이션 안에서 사용자가 취하는 개별적인 행위를 식별할 수 있습니다. 예를 들어, 직원이 Facebook을 보는 것은 허용하되 게시를 금지할 수 있습니다. 또는 3G 셀룰러 네트워크에 연결된 직원이 음악이나 영화를 스트리밍하거나 구매하는 것을 금지할 수 있습니다. AVC는 또한 다른 TCP 포트 사이를 이동하는 Skype, BitTorrent와 같은 애플리케이션의 보안을 보장하여 애플리케이션의 프록시로서 포트 번호를 사용하는 관행이 필요 없어집니다. 그러므로 관리자가 소셜 미디어, 스트리밍 미디어 및 기타 애플리케이션에 새로운 차원의 제어 기능을 갖출 수 있습니다.

평판 기반 웹 보안

Cisco WSE(Web Security Essentials)는 AntiVirus 엔진이 웹에서 기인하는 위협을 탐지하기 몇 개월 전부터 평판 기반 보안을 제공합니다. WSE는 Cisco SIO의 글로벌 위협 상관관계를 사용하여 URL, 도메인, IP 주소에 대해 평판 보안을 제공합니다. 그러므로 긴급 시그니처 업데이트 또는 시스템 패치 없이도 감염된 사이트를 제로데이 공격으로부터 보호합니다. Cisco SIO에서 제공하는 웹 평판 정보를 사용하여 호스트 사이트의 평판을 기반으로 하는 세밀한 정책은 물론 가장 효과적이고 시기적절한 보안을 적용할 수 있습니다.

Cisco WSE는 또한 강력한 콘텐츠 기반 URL 필터링을 통해 사용자, 그룹, 장치 및 역할별로 차별화된 액세스 정책을 제공합니다. 65개의 URL 범주와 포괄적 URL 데이터베이스를 통해 200개 이상의 국가의 60개 이상 언어로 된 사이트를 지원합니다.

완벽한 보안 서비스: 상황 인식 기반 차세대 방화벽

ID 및 장치 액세스 보장

모빌리티와 BYOD가 보편화되면서 IT는 모바일 장치 및 위치를 기반으로 다른 액세스 권한을 손쉽게 적용할 수 있어야 합니다. 예를 들어, 직원이 회사 소유 랩톱 또는 가상 데스크톱을 사용할 때보다 개인 태블릿을 사용할 때 액세스를 제한하고, 개인 랩톱을 사용할 때는 액세스를 더욱 제한해야 할 수 있습니다. 이러한 액세스는 사용자가 본사에 있을 때, 지사에 있을 때 또는 가정에서 Wi-Fi를 사용하거나 거리에서 셀룰러를 사용할 때와 같이 각 상황에 따라 다르게 적용할 수 있습니다.

Cisco ASA 5500-X Series와 Cisco AnyConnect Secure Mobility Client를 함께 사용하면 사용자 ID, 네트워크 위치 및 사용한 특정 장치에 따라 다른 액세스를 유연하게 적용할 수 있습니다. 이렇게 하면 제조 담당 부사장이 새 Android 태블릿으로 로그인하거나 VPN을 통해 원격으로 로그인할 경우 IT는 변화된 상황에 따라 액세스 정책이 적용되도록 보장할 수 있습니다.

Active Directory 에이전트 및 LDAP(Lightweight Directory Access Protocol)를 이용한 수동적 인증 방법 이외에, Kerberos 및 NT LAN Manager를 사용하여 사용자, 그룹 및 역할을 기반으로 차별화된 액세스 제어를 적용하는 능동적 인증을 제공할 수 있습니다.

Cisco ASA 5500-X Series는 Cisco TrustSec®과 통합하여 관리자가 네트워크에서 기존에 사용하던 사용자 ID와 장치를 사용할 수 있습니다. 이 정보를 사용하여 직원, 외주업체 및 방문객의 트래픽을 식별하고 태깅한 다음 액세스를 제어할 수 있습니다. 예를 들어, 방문객 트래픽은 방문객 네트워크로 제한할 수 있으며, Cisco ASA 5500-X Series 방화벽으로 이 방문객이 사용할 수 있는 애플리케이션 또는 웹 사이트를 제한할 수 있습니다. 다른 어떤 차세대 방화벽도 이렇게 다양한 액세스 제어 메커니즘을 제공하지 못 합니다.

완벽한 보안 서비스: 상황 인식 기반 차세대 방화벽

Cisco 백서

강력한 기반 위에 구축

상황 인식 기반 보안은 모빌리티, 클라우드 및 협업의 새로운 세계에서 지능적인 위협으로부터 보호해 줍니다. 다른 "차세대" 공급업체와 달리, 조직은 업계에서 가장 신뢰할 수 있고 가장 폭넓게 설치된 보안성과 안정성이 검증된 방화벽의 보안 기능의 성능 저하 없이 추가 할 수 있는 Cisco ASA Next-Generation Firewall Services의 포괄적 제품을 신뢰할 수 있습니다. 관리자는 네트워크 노하우를 활용하여 효율성을 극대화하는 동시에 유연한 상황 인식 기반 정책을 만들 수 있습니다. Cisco ASA 5500-X Series Next-Generation Firewalls는 소규모 기업부터 글로벌 엔터프라이즈까지 확장을 통해 모든 요건을 충족할 수 있도록 설계되었으며 수천 개의 사이트에서도 정책을 간단히 유지 관리하고 감사할 수 있습니다.

성능 저하 없는 보안

업무가 물리적 장소에 머무르지 않고 활동으로 전환되면서 기업 네트워크에는 전례 없는 변화가 진행되고 있습니다. 언제 어디서나 엔터프라이즈 및 클라우드 기반 리소스에 액세스해야 하는 직원이 늘어남에 따라 IT는 비즈니스 혁신을 가로막지 않고도 조직을 보호할 수 있는 새로운 방법이 필요합니다. Cisco ASA 5500-X Series Next-Generation Firewalls는 대규모 보안 성능을 제공하는 동시에 탁월한 애플리케이션 가시성 및 제어, 웹 보안, 침입 방지, 원격 액세스 및 클라우드 기반 위협 보호를 제공하여 현재와 미래에 유연한 엔터프라이즈급 보안을 구현합니다.

자세히 보기

Cisco ASA 5500-X Series Next-Generation Firewalls

Cisco ASA Next-Generation Firewall Services