Palo Alto Networks 차세대 방화벽 개요

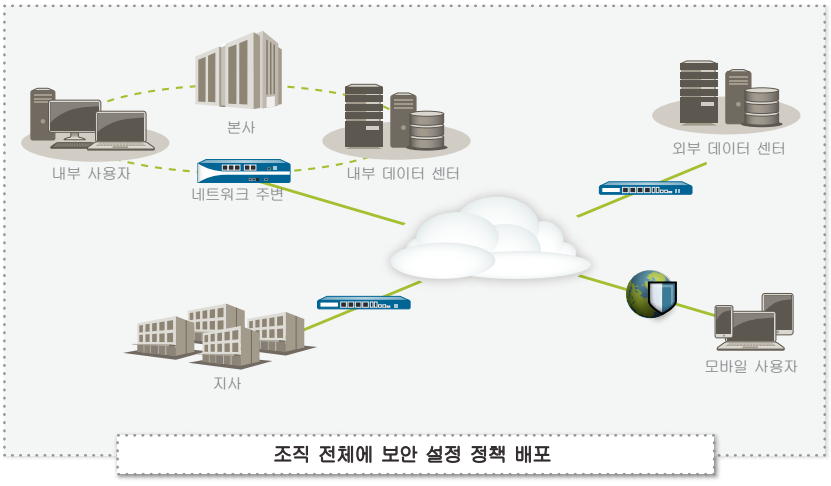
애플리케이션, 위협의 형태, 사용자 행동양식 및 네트워크 인프라가 근본적으로 변하면서 기존의 포트 기반 방화벽이 제공하던 보안 기능은 꾸준히 약화되어 왔습니다. 사용자들은 업무를 하기 위해 다양한 디바이스들을 사용하여 많은 애플리케이션에 액세스 하고 있습니다. 따라서 기업 또한 데이터 센터 확장, 가상화, 이동성 및 클라우드 기반 이니셔티브 등, 급변하는 환경에 따라 애플리케이션 액세스를 허용하면서 네트워크를 보호하는 방법을 재고해야 합니다.

전통적인 대응 방식은 계속 진화하는 개별 기술(Point Technologies)을 방화벽에 애드온하여 모든 애플리케이션 트래픽을 차단하는 것인데, 이는 기업의 비즈니스를 저해할 수 있습니다. 그렇다고 모든 애플리케이션을 허용하는 것 역시 비즈니스 및 보안 위험 때문에 용납되지 않습니다. 기업이 직면한 과제는 기존의 포트 기반 방화벽은 추가적인 애플리케이션 차단을 통해서도 두 접근 방식의 대안을 제시하지 못한다는 것입니다. 모두 허용과 모두 차단 사이에서 균형을 이루기 위해서는 애플리케이션 ID, 애플리케이션을 사용 중인 사람, 콘텐츠 형식 등, 비즈니스 관련 요소를 방화벽 보안 정책의 주요 기준으로 사용하여 애플리케이션 보안을 강화해야 합니다.

주요 보안 설정 요구 사항:

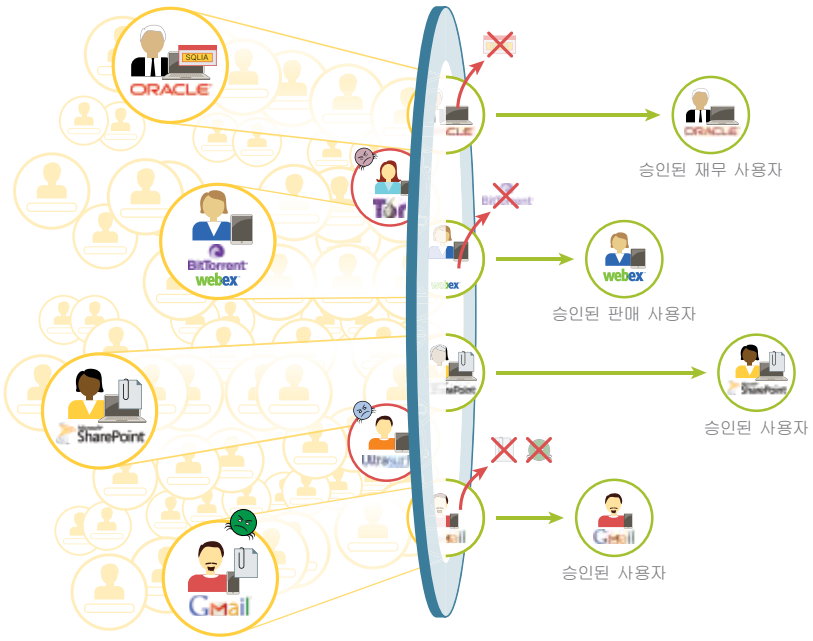
- **포트가 아니라 애플리케이션 자체를 식별해야 합니다.** 트래픽이 방화벽에 도달하자마자 프로토콜, 암호화 또는 우회기술에 관계없이 애플리케이션 **ID**를 식별하여 트래픽을 분류합니다. 그런 다음 해당 **ID**를 기반으로 모든 보안 정책을 설정합니다.
- **위치나 장치에 상관없이 애플리케이션 사용을 IP 주소가 아닌 사용자 ID와 연결해야 합니다.** 엔터프라이즈 디렉터리나 다른 유저 데이터베이스의 사용자 및 그룹 정보를 이용하여 어떤 위치나 장소에서든 모든 사용자에 대해 일관된 보안 정책을 배포합니다.
- **알려진 위협과 알려지지 않은 위협 모두로부터 보호해야 합니다.** 트래픽을 분석하는 동시에 알려진 취약성 공격, 맬웨어, 스파이웨어, 악성 **URL**을 방지하고, 특정 목적을 가졌거나 알려지지 않은 맬웨어에 대한 보호를 자동으로 제공합니다.
- **정책 관리가 간편해야 합니다.** 사용하기 쉬운 그래픽 도구, 통합 정책 편집기, 템플릿 및 장치 그룹을 통해 애플리케이션에 보안을 적용하고 관리 부담을 줄입니다.

애플리케이션 보안 설정 정책은 설치된 위치에 상관없이 보안 수준을 높이는데 도움이 됩니다. 관문단에서는 불필요한 여러 애플리케이션들을 차단하여 위협이 들어올 수 있는 경로를 최소화 한 다음, 허용된 애플리케이션에 대해 위협(알려진 또는 알려지지 않은)을 검사합니다. 데이터센터(전통적인 데이터센터 또는 가상화된 데이터센터)에서는, 애플리케이션 정책을 사용하여 허용된 사용자들에게만 데이터센터 애플리케이션을 사용하도록 하여 위협으로부터 데이터를 보호하고, 이를 통해 가상 인프라스트럭쳐에서 발생할 수 있는 보안 위험에 대응할 수 있게 합니다. 지사 및 원격 사용자는 본사에서 배포되는 동일한 보안 정책에 의해 보호될 수 있으므로 정책 일관성이 보장됩니다.



paloalto NETWORKS
the network security company™

애플리케이션, 사용자, 콘텐츠를 모두 제어할 수 있습니다.



애플리케이션 보안 구현으로 비즈니스 가속화

Palo Alto Networks 차세대 방화벽을 통해 애플리케이션에 보안을 구현하면 기업 네트워크를 통과하는 애플리케이션 수의 급증과 관련된 비즈니스 및 보안 위험을 해결할 수 있습니다. 즉, 로컬, 모바일, 원격 사용자 또는 사용자 그룹에 대해 애플리케이션에 보안을 구현하고 알려진 위협과 알려지지 않은 위협으로부터 트래픽을 보호함으로써 비즈니스 성장을 도모하는 동시에 보안 환경도 개선할 수 있습니다.

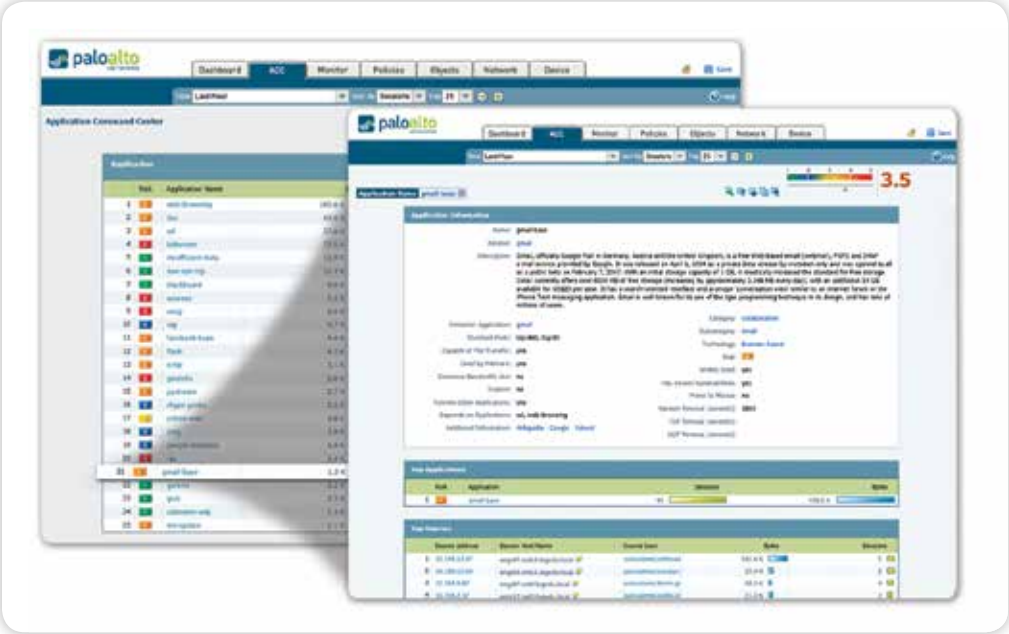
- **항상 모든 포트에서 모든 애플리케이션을 정확히 분류하는 것은 모든 방화벽의 핵심이며, 보안 정책의 기반이 됩니다.** 그러나 오늘날의 애플리케이션은 포트 호핑(hopping), SSL 및 SSH 사용, 80번 포트 잠입, 비 표준 포트 사용 등의 방식으로 포트 기반의 기존 방화벽을 간단히 우회할 수 있습니다. App-ID는 방화벽에서 트래픽을 확인하자마자 트래픽 스트림에 복수의 분류 메커니즘을 적용하여 기존 방화벽의 문제였던 트래픽 분류 가시성의 한계를 해결함으로써 포트, 암호화(SSL 또는 SSH) 또는 우회 기법과 상관없이 네트워크를 통과 중인 애플리케이션을 정확히 식별합니다. 포트 및 프로토콜뿐만 아니라 네트워크를 통과 중인 애플리케이션을 정확히 파악하는 것은 모든 보안 정책을 결정하는 바탕이 됩니다. 식별되지 않은 애플리케이션은 대개 트래픽에서 아주 적은 비중을 차지하지만 잠재적 위험성이 크기 때문에 체계적인 관리를 위해 자동으로 분류됩니다. 이러한 관리에는 정책 제어 및 점검, 위협 포렌식, 사용자 정의 App-ID 생성, Palo Alto Networks App-ID 개발을 위한 패킷 캡처가 포함될 수 있습니다.

- **IP 주소외에 사용자와 디바이스도 정책과 연동.** 디바이스나 위치에 상관없이 애플리케이션 및 사용자 **ID**를 기반으로 보안 정책을 수립하고 관리하면 포트 및 **IP** 주소에만 의존하는 것보다 더욱 효율적으로 네트워크를 보호할 수 있습니다. 광범위한 엔터프라이즈 사용자 데이터베이스와 연동함으로써 애플리케이션에 액세스하는 **Microsoft Windows, Mac OS X, Linux, Android** 또는 **iOS** 사용자에 대한 식별을 제공합니다. 출장 중이거나 원격으로 업무를 보는 사용자도 로컬이나 회사 네트워크에서 사용 중인 동일한 정책으로 일관되게 보호됩니다. 사용자의 애플리케이션 활동에 대한 파악과 제어가 동시에 이루어지면 사용자의 액세스 위치나 방법에 상관없이 **Oracle, BitTorrent, Gmail** 또는 네트워크를 통과하는 다른 애플리케이션도 안전하게 사용할 수 있습니다.

- **알려진 위협과 알려지지 않은 위협 모두로부터 보호합니다.** 오늘날의 첨단 네트워크를 보호하려면 알려진 공격, 맬웨어 및 스파이웨어뿐 아니라 완전히 알려지지 않은 위협과 특정 목적을 가진 위협을 차단해야 합니다. 이 프로세스는 특정 애플리케이션을 제외한 다른 모든 애플리케이션을 차단하는 정책을 통해 안전한 애플리케이션만 하용하고 나머지는 차단함으로써 네트워크 공격 가능성이 있는 영역을 줄이는 것으로 시작합니다. 이렇게 조직적으로 구성된 위협 방지는 허용되는 모든 트래픽에 적용되고, 알려진 맬웨어 사이트, 취약성 공격, 바이러스, 스파이웨어 및 단일 경로를 통한 악의적인 **DNS** 쿼리를 차단할 수 있습니다. 알려지지 않은 맬웨어는 가상화 샌드박스 환경으로 보낸 후, 파일을 실행해서 **100** 여가지 이상의 악의적인 행위를 직접 관찰한 후 능동적으로 분석하고 식별합니다. 새로운 맬웨어가 발견되면 감염 파일 및 관련 맬웨어 트래픽에 대한 시그니처가 자동으로 생성되어 관리자에게 전달됩니다. 모든 위협 방지 분석은 전체 애플리케이션 및 프로토콜 컨텍스트를 사용하므로 터널, 압축 콘텐츠, 비표준 포트 등으로 보안에 노출되지 않도록 시도하는 위협도 모두 포착됩니다.

개발 및 관리 유연성

애플리케이션 보안 구현 기능은 목적 기반 플랫폼이나 가상화 폼 팩터에서 사용할 수 있습니다. 여러 대의 Palo Alto Networks 방화벽을 설치해야 하는 경우에는 중앙 관리 서버인 Panorama를 사용하여 중앙에서 트래픽 분석, 정책 배포, 보고서 생성, 컨텐츠 업데이트 등을 할 수 있습니다.



애플리케이션 가시성: 애플리케이션 활동을 명확하고 쉽게 읽을 수 있는 형식으로 보여 줍니다. 애플리케이션, 애플리케이션의 기능 및 사용 중인 사람에 대해 자세히 알아보려면 필터를 추가하거나 제거합니다.

애플리케이션 보안 구현: 포괄적 접근

애플리케이션 보안 구현을 위해서는 플랫폼이나 위치에 상관없이 사용자가 누구인지, 애플리케이션이 전달하는 콘텐츠가 무엇인지 등, 네트워크의 애플리케이션을 완전히 이해하는 것으로 시작하여 네트워크를 보호하고 비즈니스를 성장시키기 위한 포괄적 접근이 필요합니다. 네트워크 활동을 보다 완벽하게 파악하면 비즈니스와 관련된 사용자와 콘텐츠, 애플리케이션 요소를 기반으로 훨씬 의미 있는 보안 정책을 수립할 수 있습니다. 사용자 위치, 사용자의 플랫폼 및 정책이 배포되는 위치(네트워크 주변, 기존 또는 가상화 데이터 센터, 지사 또는 원격 사용자)는 정책이 만들어지는 방식과 거의 차이가 없습니다. 이제 어떤 애플리케이션, 사용자, 콘텐츠에도 보안을 구현할 수 있습니다.

완전한 이해는 보다 완벽한 보안 정책과 직결

보안 모범 사례를 분석해 보면 네트워크 상황을 잘 이해하는 것이 더욱 견고한 보안 정책을 구현하는 데 도움이 된다는 사실이 잘 드러납니다. 예를 들어, 포트 기반의 광범위한 트래픽 집합과 대조적으로, 네트워크를 통과 중인 애플리케이션을 정확하게 알고 있으면 관리자는 원치 않는 애플리케이션은 차단하고 비즈니스에 필요한 애플리케이션은 허용할 수 있습니다. IP 주소뿐만 아니라 사용자가 누군지 파악할 경우 보다 구체적인 정책 할당이 가능하도록 다른 정책 기준을 추가할 수도 있습니다. Palo Alto Networks 차세대 방화벽은 네트워크 환경을 그래픽으로 알기 쉽게 나타내는 강력한 도구로, 관리자가 애플리케이션 활동과 보안에 미칠 수 있는 잠재적인 영향에 대해 더욱 완벽하게 이해하고 현명한 정책 결정을 내릴 수 있도록 지원합니다. 사용하기 쉬운 웹 기반 인터페이스에서 애플리케이션이 끊임없이 분류되며 애플리케이션 상태가 변하면 그래픽 요약이 동적으로 업데이트됩니다.

- 새롭거나 낯선 애플리케이션이 있으면 클릭 한 번으로 애플리케이션의 설명, 동작의 특징 및 현재 사용하는 사람 등, 세부 정보를 볼 수 있습니다.
- URL 범주, 위협 요소, 데이터 패턴을 그래픽으로 자세히 보여 주므로 네트워크 상황을 완벽하고 철저하게 파악할 수 있습니다.
- 알려지지 않은 애플리케이션은 대개 트래픽에서 아주 적은 비중을 차지하지만 잠재적 위험성이 크기 때문에 내부 애플리케이션인지, 아직 식별되지 않은 상용 애플리케이션인지 또는 위협인지 확인하는 분석을 위해 분류해 놓습니다.
- 많은 사용자는 업무를 수행하기 위해 자신이 원하는 애플리케이션에 액세스합니다. 따라서 애플리케이션, 사용자, 관련 콘텐츠와 비즈니스의 관련성이 날이 갈수록 커지고 있습니다. 관리자는 네트워크 환경을 잘 이해함으로써 해당 정보를 애플리케이션 보안 구현 정책에 반영하여 위험을 줄일 수 있습니다.

애플리케이션 보안 구현 및 위험 감소

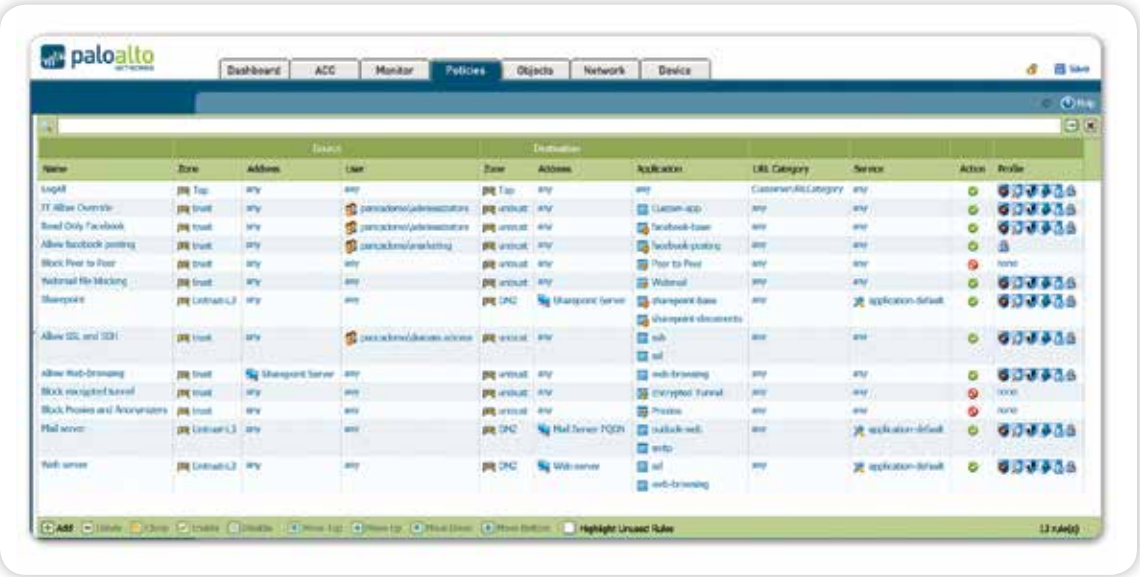
애플리케이션 보안 구현에서는 모든 애플리케이션을 거부할 경우의 비즈니스 제약과 모든 애플리케이션을 허용할 경우의 높은 위험 간에 균형을 유지하는 수단으로써 애플리케이션/애플리케이션 기능, 사용자 및 그룹, 콘텐츠를 포함하는 정책 결정 기준을 사용합니다.

지사, 모바일 및 원격 사용자를 비롯한 네트워크 경계에서의 보안 정책은 모든 트래픽을 식별하고 사용자 ID를 기반으로 트래픽을 선택적으로 허용한 다음 위협에 대해 트래픽을 감시하는 데 초점을 둡니다. 정책에는 다음과 같은 예가 포함됩니다.

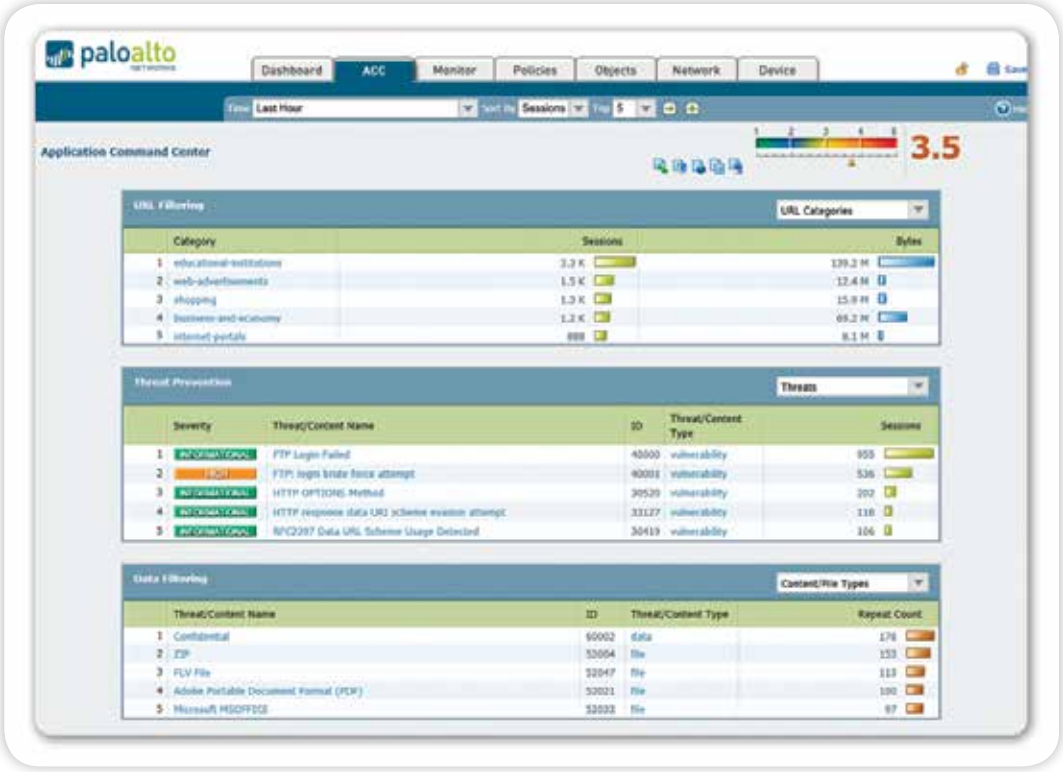
- 몇 가지 선택적인 경우에 있어 웹 메일 및 메신저 사용을 제한합니다. SSL을 사용하는 웹 메일 및 메신저의 암호를 해독하고, 공격에 대비하여 트래픽을 검사하고, 분석 및 시그니처 개발을 위해 알 수 없는 파일을 WildFire에 업로드합니다.
- 스트리밍 미디어 애플리케이션과 웹 사이트를 허용하되, QoS 및 맬웨어 방지를 적용하여 VoIP 애플리케이션에 미치는 영향을 제한하고 네트워크를 보호합니다.
- 모든 사용자에게 "인터넷검색"을 허용하고 Facebook 게임과 소셜 플러그인을 차단하는 방식으로 Facebook을 제어합니다. 또한 마케팅용으로만 Facebook 게시물을 허용하고, 맬웨어 및 공격에 대비하여 모든 Facebook 트래픽을 감시합니다.
- 비즈니스 관련 웹 사이트에 대한 트래픽을 허용하고 감시하여 웹 서핑을 제어하는 한편, 업무와 무관한 것이 확실한 웹 사이트 액세스를 차단하고 다른 사이트에 대한 액세스를 맞춤 차단 페이지를 통해 공지하는 웹 허용 정책을 배포합니다.
- GlobalProtect를 통해 모든 사용자, 로컬, 모바일 또는 원격에 동일한 정책을 투명하게 배포하여 일관성 있는 보안을 구현합니다.
- 특정 애플리케이션을 제외한 다른 모든 애플리케이션은 거부하는 암시적 정책을 사용하거나, P2P 같은 원치 않는 애플리케이션 및 프록시 서버, 특정 국가로부터의 트래픽을 명시적으로 차단하여 비즈니스와 보안에 위험을 초래하는 애플리케이션 트래픽을 줄입니다.

데이터 센터 환경에서는 애플리케이션 확인, 악성 애플리케이션 감지 및 데이터 보호에 초점을 둡니다.

- Oracle 기반 신용 카드 번호 리포지토리를 자체 보안 영역에 격리합니다. 즉, 재무 부서에 대한 액세스를 제어하고, 표준 포트를 통해 트래픽이 전송되도록 하며, 애플리케이션 취약성에 대해 트래픽을 검사합니다.
- IT 부서에서만 정해진 원격 관리 애플리케이션(예: SSH, RDP, Telnet) 그룹을 사용하여 표준 포트를 통해 데이터 센터에 액세스할 수 있도록 합니다.
- Microsoft SharePoint Administration을 관리 부서에서만 사용할 수 있도록 하고, Microsoft SharePoint Documents는 다른 모든 사용자가 액세스할 수 있도록 합니다.



통합 정책 편집기: 사용자에게 익숙한 UI를 제공하므로 애플리케이션, 사용자 및 콘텐츠를 제어하는 정책을 신속하게 수립하고 배포할 수 있습니다.



콘텐츠 및 위협 가시성 : URL, 위협 및 파일/데이터 전송 활동을 명확하고 쉽게 읽을 수 있는 형식으로 보여 줍니다. 개별 요소에 대해 자세히 알아보려면 필터를 추가하거나 제거합니다.

허용된 애플리케이션 보안

애플리케이션 보안 구현은 특정 애플리케이션에 대한 액세스를 허용하고, 알려진 공격, 알려졌거나 알려지지 않은 맬웨어 및 스파이웨어를 차단하는 정책을 적용함으로써 파일이나 데이터 전송, 웹 서핑 활동을 제어하는 것입니다. 포트 호핑(hopping), 터널링과 같은 일반적인 우회 공격 방법은 App-ID에서 디코더로 생성된 애플리케이션 및 프로토콜 컨텍스트를 사용하여 위협 방지 정책을 실행하면 해결됩니다. 그러나 UTM 솔루션은 위협 방지에 대해 기능, 방화벽, IPS, AV, URL 필터링을 각각 사용하는 분산형 접근 방식을 취하기 때문에 컨텍스트를 공유하지 않고 트래픽을 감시함으로써 우회 공격에 취약한 단점이 있습니다.

- **알려진 위협 차단: IPS 및 네트워크 바이러스 백신/안티 스파이웨어.** 동일한 시그니처 형식과 스트림 기반 감시 엔진을 통해 광범위한 위협에서 네트워크를 보호합니다. IPS (Intrusion Prevention System) 기능으로 네트워크 및 애플리케이션 차원의 취약성 공격, 버퍼 오버플로, DoS 공격 및 포트 검사를 차단합니다. 또한 바이러스 백신/안티 바이러스 보호 기능으로 맬웨어에서 생성된 명령 및 제어 트래픽, PDF 바이러스, 압축 파일 또는 웹 트래픽(압축 HTTP/HTTPS)에 숨겨진 맬웨어를 비롯하여 수백만 바이러스 변종을 차단합니다. 아울러, 모든 포트에서 모든 애플리케이션에 대해 정책을 기반으로 SSL 암호를 해독하므로 SSL 암호화 애플리케이션을 통해 이동하는 맬웨어로부터 네트워크를 보호합니다.

- **알려지지 않았거나 특정 목적을 가진 맬웨어 차단: Wildfire™.** WildFire는 클라우드 기반의 가상화 샌드박스 환경에서 알 수 없는 파일을 직접 실행하고 관찰하여 알려지지 않았거나 특정 목적을 가진 맬웨어를 분석합니다. WildFire는 100가지 이상의 악의적인 동작을 모니터링하고 그 결과를 즉시 관리자에게 경고 형태로 전송합니다. 옵션으로 제공되는 WildFire에 가입하면 한층 강화된 보호, 로그 기록 및 보고 기능을 사용할 수 있습니다. 세계 어디에서든 새로운 맬웨어가 발견되면 가입자에게 피해를 입히기 전에 효과적으로 맬웨어의 확산을 막고, 한 시간 내로 가입자를 보호합니다. 또한 가입자는 통합 WildFire 로그 기록 및 보고 기능과 API에 액세스하고, 분석을 위해 WildFire 클라우드에 샘플을 제출할 수 있습니다.

- **봇 감염 호스트 식별.** App-ID는 네트워크를 위협에 노출시킬 수 있는 알 수 없는 트래픽을 포함하여 모든 애플리케이션을 모든 포트에서 분류합니다. 행위 기반 봇넷 보고서는 알 수 없는 트래픽, 의심스러운 DNS 및 URL 쿼리, 특이한 네트워크 동작 간의 상관 관계를 분석하여 맬웨어에 의해 감염되기 쉬운 장치를 가려냅니다. 결과는 감염 가능성이 있는 호스트 목록으로 표시되며, 이러한 호스트를 대상으로 봇넷 조사를 실시할 수 있습니다.
- **인증되지 않은 파일 및 데이터 전송 제한.** 관리자는 데이터 필터링 기능을 사용하여 인증되지 않은 파일 및 데이터 전송에 수반되는 위험을 줄이는 정책을 구현할 수 있습니다. 파일 확장명만이 아니라 파일의 내용을 검사하여 전송 동작의 허용 여부를 결정함으로써 파일 전송을 제어할 수 있고, 일반적으로 드라이브 바이(drive-by) 다운로드에서 발견되는 실행 파일을 차단하여 미확인 맬웨어가 네트워크에 확산되지 않도록 막을 수 있습니다. 데이터 필터링 기능을 사용하면 기밀 데이터 패턴(신용 카드 또는 사회보장 번호, 사용자 정의 패턴 등)의 흐름을 감지하고 제어할 수 있습니다.
- **웹 서핑 제어.** 관리자는 사용자 정의가 가능한 완전 통합형 URL 필터링 엔진을 사용하여 세부적인 웹 브라우징 정책을 적용함으로써 애플리케이션 가시성 및 제어 정책을 보완하고 법적 위험, 규제 위험, 생산성 위험으로부터 회사를 완벽하게 보호할 수 있습니다. 또한 URL 범주를 정책에 활용하여 SSL 암호화, QoS 또는 다른 규칙 기반에 대해 보다 세분화된 제어가 가능합니다.

지속적 관리 및 분석

보안 모범 사례를 살펴보면 관리자는 장치의 수와 상관없이 사전 대응적인 방화벽 관리와 보안 사고 발생 시 사후 대응, 분석 및 보고 간에 조화롭게 균형을 유지합니다.

- **관리:** 각 Palo Alto Networks 플랫폼은 CLI(명령줄 인터페이스) 또는 완벽한 기능을 갖춘 브라우저 기반 인터페이스를 통해 개별적으로 관리할 수 있습니다. 대규모 구성인 경우 Panorama 중앙관리 솔루션을 사용하여 중앙관리를 할 수 있으며, 템플릿, 공유 정책 등의 기능을 사용하여 로컬 정책과 글로벌 제어를 적절히 병행할 수 있습니다. 또한 SNMP 같은 표준 기반 도구 및 REST 기반 API가 추가로 지원되므로 타사 관리 도구와 연동할 수 있습니다. 방화벽 장비와 Panorama의 유저 인터페이스가 동일하므로 인터페이스를 전환할 때 시행 착오를 겪지 않아도 됩니다. 관리자는 제공된 인터페이스를 사용하여 동기화 문제에 대한 걱정 없이 언제든지 변경할 수 있습니다. 모든 관리 방식에 대해 역할 기반 관리가 지원되며, 특정 개인별로 특정 권한을 할당할 수 있습니다.
- **보고서:** 기본 제공되는 보고서를 그대로 사용하거나, 필요에 따라 사용자 정의하거나, 하나로 묶을 수 있습니다. 모든 보고서는 CSV 또는 PDF 형식으로 내보낼 수 있으며 예약 실행 및 이메일 전송이 가능합니다.
- **로그 기록:** 실시간 로그 필터링으로 네트워크의 모든 세션에 대해 간편하고도 신속하게 포렌식 검사를 할 수 있습니다. 로그 필터 결과는 CSV 파일로 내보내거나, 오프라인 보관 또는 추가 분석을 위해 syslog 서버로 보낼 수 있습니다.

목적 기반 하드웨어 또는 가상화 플랫폼

Palo Alto Networks에서는 엔터프라이즈 원격 지사용으로 설계된 PA-200에서부터 고속 데이터 센터용으로 설계된 PA-5060에 이르는 다양한 목적 기반 하드웨어 플랫폼 제품군을 제공합니다. 플랫폼 아키텍처는 싱글 패스(Single-Pass) 소프트웨어 엔진을 기반으로 하며 네트워킹, 보안, 위협 방지 및 관리에 대해 기능별 처리를 사용하여 예측 가능한 성능을 제공합니다. VM 시리즈 가상 방화벽에서도 하드웨어 플랫폼과 동일한 방화벽 기능을 사용할 수 있으므로, 네트워크 주변 또는 원격 지사 방화벽에 적용된 것과 동일한 정책을 사용하여 가상화 환경과 클라우드 기반 컴퓨팅 환경을 안전하게 보호할 수 있습니다.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Accueil : +1.408.573.4000
Ventes : +1.866.320.4788
Assistance : +1.866.898.9087

www.paloaltonetworks.com

PAN_DS_FFOV_112712