차세대 방화벽 개요

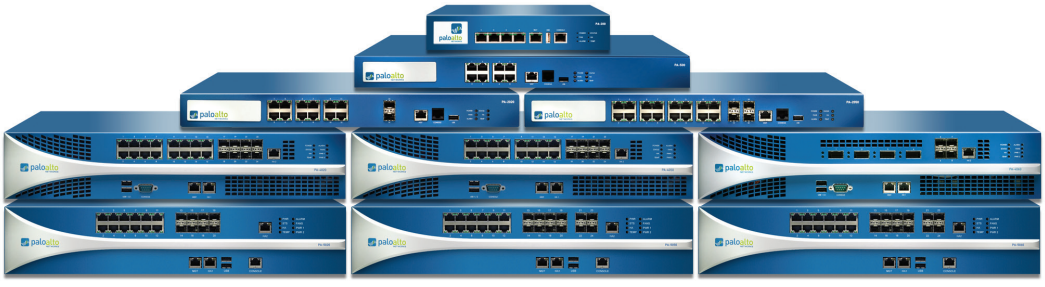
최근 들어 애플리케이션의 작동 및 사용 패턴이 변화하면서 기존의 방화벽이 제공하던 보안 기능은 서서히 취약점이 드러나고 있습니다. 사용자들은 대개 원하는 곳에서 원하는 애플리케이션에 액세스하여 일을 하곤 합니다. 이러한 애플리케이션은 대부분 비 표준 포트를 사용하거나, 포트 호핑을 이용하거나, 암호화를 통해 사용자 액세스를 간소화/합리화하고 방화벽을 우회합니다. 사이버 범죄자들은 이렇게 규제를 벗어난 애플리케이션 이용 방식을 최대한 활용하여 고도로 정교하게 목표가 설정된 첨단 맬웨어 종류를 확산시킵니다. 그 결과 포트와 프로토콜에 의존하는 기존 방화벽으로는 네트워크에 침입하는 애플리케이션들을 통한 위협을 더 이상 파악하고 통제할 수 없게 되었습니다.

그 동안 애플리케이션 사용에 대한 통제권을 강화하고 모든 사용자의 디지털 자산을 보호하고자 하는 노력들은 독립 구성형 또는 각종 보안 솔루션을 통합한 IPS, AV, Proxy, UTM등의 방화벽 보완 제품들로 인해 로컬 및 원격 보안 정책이 중복되는 결과가 빚어졌습니다. 이러한 접근 방식은 부정확하고 불완전한 트래픽 분류, 번거로운 관리 작업, Latency 증가 및 긴 복수의 검사 프로세스로 인해 일관성 없는 정책을 낳게 되며 가시성과 통제권 문제 또한 해결하지 못합니다. 이러한 문제점들을 해결하기 위해서는 차세대 방화벽만이 할 수 있는 완전히 새롭고 혁신적인 접근 방식으로 애플리케이션 보안을 확보해야 합니다.

차세대 방화벽의 핵심 요구 사항:

- 포트가 아니라 애플리케이션 자체를 식별해야 합니다. 프로토콜, 암호화, 회피 기법과 관계없이 애플리케이션을 식별하고 그 정보를 모든 보안 정책의 대상으로 삼아야 합니다.
- IP 주소가 아니라 사용자를 식별해야 합니다. 사용자의 위치를 불문하고 기업 디렉터리의 사용자 및 사용자 그룹 정보를 사용하여 가시성, 정책 생성, 보고 및 포렌식 조사를 실시합니다.
- 위협을 실시간으로 차단해야 합니다. 위험한 애플리케이션, 취약성, 맬웨어, 고 위험 URL, 각종 악성 파일과 위험 콘텐츠등의 위협에 대해 수명 주기가 끝날 때까지 공격으로부터 보호해야 합니다.
- 정책 관리가 간편해야 합니다. 사용하기 쉬운 UI 도구와 통합 정책 편집기로 애플리케이션을 안전하게 사용할 수 있도록 해야 합니다.
- 논리적 경계를 설정할 수 있어야 합니다. 물리적인 경계에서 논리적인 경계까지 일정한 보안 수단을 적용하여 출장 중이거나 재택 근무하는 원격사용자들을 포함한 모든 사용자들을 안전하게 보호해야 합니다.
- 멀티 기가비트급 처리 능력을 갖춰야 합니다. 전용 하드웨어와 소프트웨어를 결합하여 지연률이 적고 멀티 기가비트급 성능을 발휘하면서 모든 서비스를 사용할 수 있도록 해야 합니다.

Palo Alto Networks의 차세대 방화벽은 App-ID™, User-ID, Content-ID라는 세 가지 독특한 식별 기술을 사용하여 애플리케이션과 사용자 및 콘텐츠에 대해 최고의 가시성과 통제력을 발휘합니다. Palo Alto Networks의 모든 방화벽에 포함되어 있는 이 식별 기술로 인해 기업에서는 애플리케이션 사용의 안전과 보안을 확보하는 동시에 통합 구성으로 TCO를 상당히 절감할 수 있게 됩니다.



paloalto NETWORKS
the network security company™

App-ID: 모든 포트, 모든 애플리케이션을 항상 분류

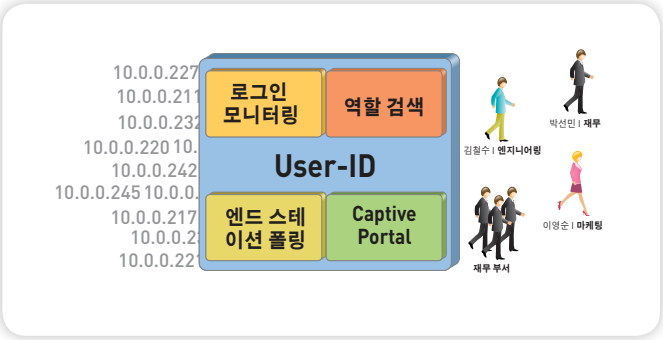
정확한 트래픽 분류는 모든 방화벽의 핵심이며 따라서 보안 정책의 기반이 됩니다. 기존의 방화벽은 포트와 프로토콜로 트래픽을 분류했는데 당시에는 이것이 네트워크 보안 메커니즘으로 충분했습니다. 그러나 오늘날의 애플리케이션은 포트 홉(hopping), SSL 및 SSH 사용, 80번 포트 잠입, 비 표준 포트 사용 등의 방식으로 포트 기반의 기존 방화벽을 간단히 우회할 수 있습니다. App-ID는 방화벽에서 트래픽을 확인하자마자 트래픽 스트림에 복수의 분류 메커니즘을 적용하여 기존 방화벽의 문제였던 트래픽 분류 가시성의 한계를 해결함으로써 네트워크를 통과 중인 애플리케이션을 정확히 식별합니다.

포트 기반으로 트래픽을 분류한 이후에 IPS 시그니처에만 의존하는 애드온(add-on) 솔루션과 달리 모든 App-ID는 최대 4개의 서로 다른 트래픽 분류 메커니즘을 자동으로 사용하여 애플리케이션을 식별합니다. App-ID는 애플리케이션의 상태를 지속적으로 모니터링하면서 트래픽을 다시 분류하고 사용 중인 각종 기능을 확인합니다. 보안 정책은 차단, 허용, 보안 유지(검사 실시, 포함된 위협 요소 차단, 인증되지 않은 파일 전송 및 데이터 패턴 검사, QoS를 사용하여 대처) 등 애플리케이션의 처리 방식을 결정합니다.

User-ID: 사용자 및 그룹별로 애플리케이션 허용

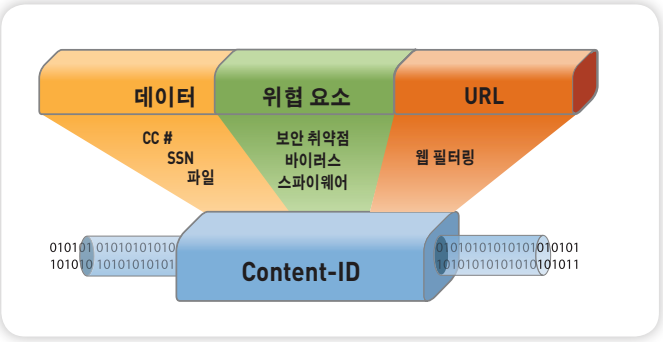
예전에는 IP 주소를 기반으로 보안 정책을 적용했지만 사용자와 컴퓨팅 방식이 점점 더 역동적으로 변화함에 따라 IP 주소만으로는 사용자의 활동을 효과적으로 모니터링하고 통제할 수 없게 되었습니다. User-ID를 사용하면 Microsoft Windows, Apple Mac OS X, Apple iOS, Linux 사용자에 대해 사용자별 또는 그룹별 애플리케이션 허용 정책을 적용할 수 있습니다.

기업 디렉터리(Microsoft Active Directory, eDirectory, Open LDAP) 및 터미널 서비스 제품(Citrix 및 Microsoft Terminal Services)에서 사용자 정보를 수집하는 한편 Microsoft Exchange, Captive Portal, XML API와 통합함으로써 도메인 외부에 상주하는 Apple Mac OS X, Apple iOS 및 UNIX 사용자들에게도 정책을 확대 적용할 수 있게 됩니다.



Content-ID: 허용된 트래픽 보호

오늘날의 애플리케이션 중에는 상당한 장점을 갖추고 있으면서 최신 맬웨어 및 위협 요소의 전달 수단으로 악용되는 것들이 많습니다. 관리자는 Content-ID와 App-ID를 함께 사용하는 병렬 처리를 통해 네트워크를 보호할 수 있습니다. 즉, App-ID로 원치 않는 애플리케이션을 식별하고 차단한 다음 포트와 프로토콜, 회피 방식을 불문하고 보안 취약점, 최신 맬웨어, 바이러스, 봇넷, 각종 맬웨어 등이 네트워크 전체로 확산되지 않도록 차단함으로써 허용되는 애플리케이션만 안전하게 사용하도록 할 수 있습니다. 여기에 웹 서핑 및 데이터 필터링 기능을 제어하는 종합 URL 데이터베이스로 Content-ID의 제어 요소를 완벽하게 보완합니다.



보안 강화된 상태로 애플리케이션 허용

기업에서는 App-ID, User-ID, Content-ID를 완벽하게 통합함으로써 기본적인 허용/거부 수준을 넘어 애플리케이션 기능 수준까지 적용되는 일관성 있는 애플리케이션 허용 정책을 수립할 수 있습니다. GlobalProtect™를 사용하면 기업 본사의 사용자를 보호하는 모든 정책을 어떤 위치의 사용자에게든 확대 적용할 수 있으며, 이로써 네트워크 외부 사용자에 대한 논리적 경계가 설정되는 효과를 얻을 수 있습니다.

보안 허용 정책은 먼저 App-ID가 애플리케이션을 식별하는 것으로 시작됩니다. 그런 다음 User-ID를 사용하여 이 정보를 해당 사용자와 매핑하는 한편 트래픽 콘텐츠에 위협 요소나 파일, 데이터 패턴, 웹 활동 등이 있는지를 Content-ID로 검사합니다. 이 결과는 ACC(Application Command Center)에 표시되며 관리자는 이를 통해 거의 실시간으로 네트워크 상황을 파악할 수 있습니다. 그런 다음 ACC에서 확인한 애플리케이션, 사용자, 콘텐츠등 관련 정보를 사용하여 정책 편집기에서 적당한 보안 정책, 즉 원치 않는 애플리케이션을 차단하는 동시에 나머지 애플리케이션은 안전하게 사용할 수 있도록 하는 보안 정책을 만듭니다. 마지막으로 애플리케이션, 사용자 및 콘텐츠 정보를 사용하여 자세한 분석과 보고 또는 포렌식 등을 다시 한 번 수행할 수 있습니다.

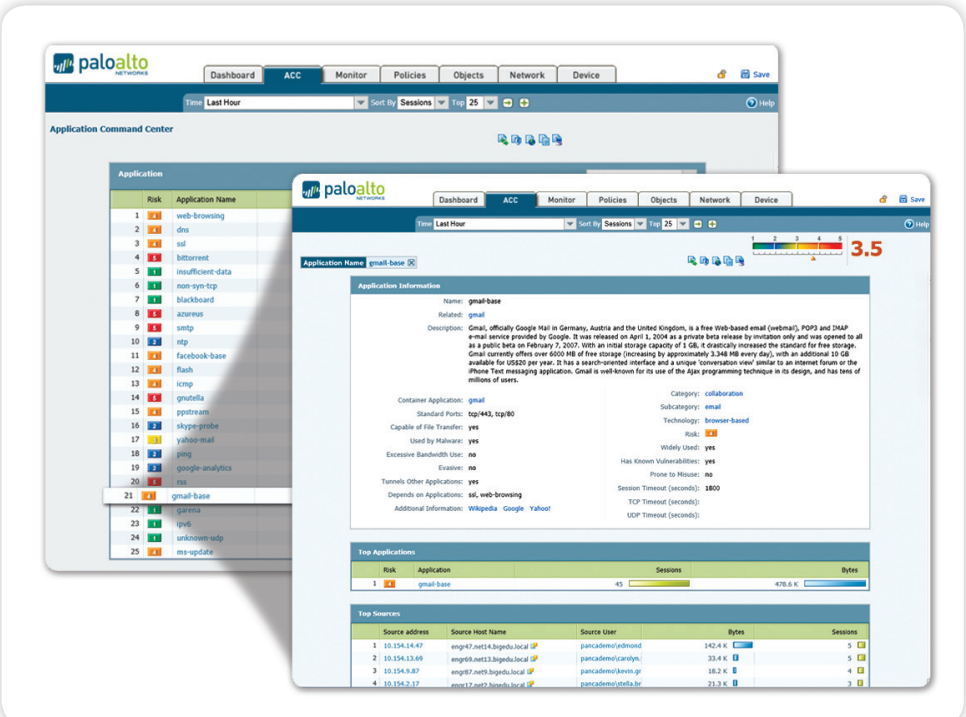
ACC(Application Command Center): 아는 것이 힘이다

ACC(Application Command Center)는 로그 데이터들을 그래픽으로 요약하여 네트워크를 통과 중인 애플리케이션은 무엇이고 누가 그것을 사용하며 보안에 어떤 영향을 미칠 수 있는지를 보여 줍니다. ACC는 App-ID의 지속적인 트래픽 분류에 따라 동적으로 업데이트되며, 포트나 동작을 바꾸는 애플리케이션이 있을 경우 App-ID가 해당 트래픽을 계속 추적하면서 ACC에 결과를 표시해 줍니다. 새로운 애플리케이션이나 미확인 애플리케이션이 ACC에 나타날 경우 클릭 한 번만 하면 애플리케이션에 대한 설명과 주요 기능, 작동 특성, 사용자 등이 표시되므로 신속하게 조사할 수 있습니다. 또한 URL 범주, 위협 요소, 데이터 등을 보다 자세히 확인함으로써 네트워크 상황을 완벽하고 철저하게 파악할 수 있습니다. 관리자는 ACC에서 네트워크를 통과 중인 트래픽을 신속하게 파악한 다음 그 정보를 바탕으로 보다 섬세한 보안 정책을 만들 수 있습니다.

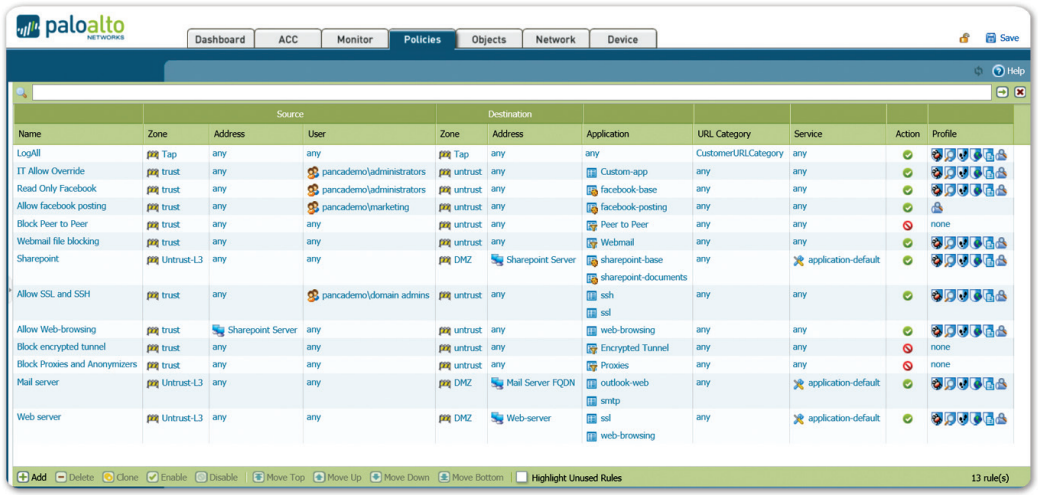
정책 편집기: 습득한 정보로 안전한 보안 허용 정책 만들기

관리자는 네트워크를 통과 중인 애플리케이션이 무엇이고 누가 그것을 사용하며 잠재적인 보안 위험은 무엇인지 등에 대한 정보를 이용하여 애플리케이션/애플리케이션 기능/포트 기반의 허용 정책을 체계적이고 통제된 방식으로 신속하게 설정할 수 있습니다. 정책에 대한 반응은 개방(허용), 절제(특정 애플리케이션이나 기능을 허용한 다음 이를 검사, QoS 제어, 스케줄링), 폐쇄(거부)까지 다양합니다. 다음과 같은 예를 들 수 있습니다.

- Oracle 데이터베이스에 대한 액세스를 재무 부서로 제한하고 트래픽에 표준 포트만 사용하도록 하며 트래픽의 애플리케이션 취약성을 검사하여 데이터베이스를 보호합니다.
- 정해진 원격 관리 애플리케이션(예: SSH, RDP, Telnet) 그룹을 IT 부서에서만 표준 포트를 통해 사용하도록 허용합니다.
- 특정 웹메일 및 인스턴트 메시징의 사용을 허용하고 검사하지만 각각의 파일 전송 기능은 차단하는 정책을 정의하여 시행합니다.
- Microsoft SharePoint Administration을 관리 팀에서만 사용할 수 있도록 허용하고, Microsoft SharePoint Documents는 다른 모든 사용자가 액세스할 수 있도록 합니다.
- 업무 관련 웹 사이트에 대한 트래픽을 허용하고 감시하는 한편, 업무와 무관한 것이 확실한 웹 사이트 액세스를 차단하고 다른 사이트에 대한 액세스를 맞춤 차단 페이지를 통해 공지하는 웹 허용 정책을 배포합니다.



애플리케이션 가시성
사용중인 애플리케이션들을 쉽고 간결한 형식으로 볼 수 있습니다. 애플리케이션과 애플리케이션의 기능 및 사용자에 대한 추가 정보를 보기 위해 필터를 추가하고 제거할 수 있습니다.



통합 정책 편집기
편리한 인터페이스를 통해 애플리케이션, 사용자 및 콘텐츠 제어 정책을 신속하게 작성하고 배포할 수 있습니다.

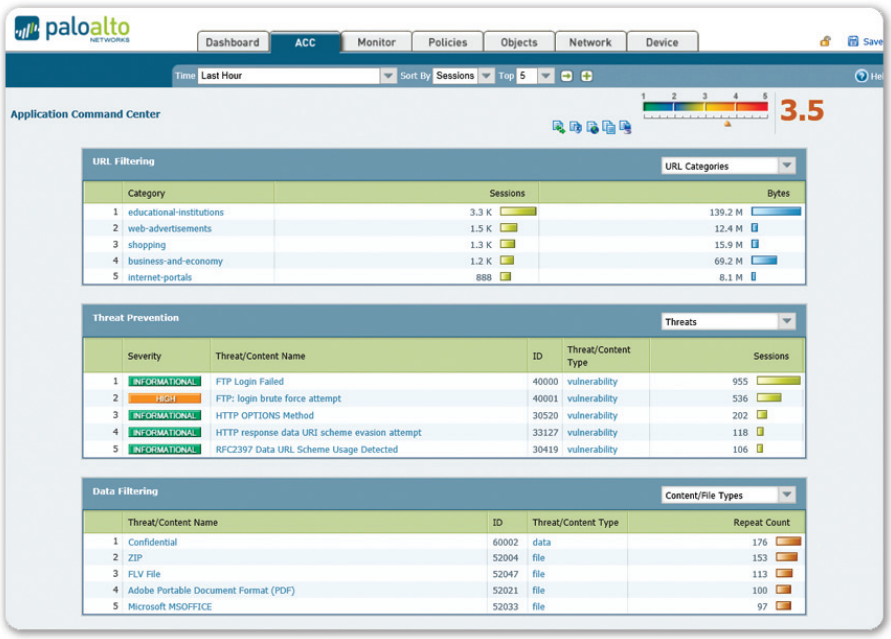
- 대역폭을 많이 사용하는 미디어 애플리케이션과웹 사이트를 모두 허용하되 그것이 VoIP 애플리케이션에 미치는 영향은 제한하는 QoS 정책을 구현합니다.
- 소셜 네트워크 및 웹메일 사이트에 대한 SSL 트래픽을 해독하고 맬웨어나 취약성 공격이 있는지 검사합니다.
- 제로데이 공격을 통한 드라이브 바이(drive-by) 다운로드를 하지 않겠다는 사용자의 동의가 있은 후에만 미분류 웹 사이트의 실행 파일 다운로드를 허용합니다.
- 특정 국가로부터의 모든 트래픽을 거부하거나 P2P 파일 공유, 우회 프로그램, 외부 프록시 등 원치 않는 애플리케이션을 차단합니다.

기업에서는 이렇게 사용자 및 그룹을 기반으로 완벽히 통합된 애플리케이션 제어 기능과 허용 트래픽에 대해 광범위하게 위협 요소를 검사하는 기능을 통해 매일 발생할 수 있는 직원 증가, 이동, 변동뿐 아니라 설정하는 정책의 수를 상당히 줄일 수 있습니다.

정책 편집기: 보안 상태로 애플리케이션 허용

애플리케이션을 보안 유지 상태로 허용한다는 것은 애플리케이션에 대한 액세스를 허용한 다음 특정한 위협 차단 정책 및 파일/데이터/URL 필터링 정책을 적용한다는 의미입니다. Content-ID에 포함된 요소 각각을 애플리케이션별로 구성할 수 있습니다.

- **IPS(Intrusion Prevention System):** 취약점 방어는 다양한 IPS(침입 방지 시스템) 기능을 통합하여 네트워크 및 애플리케이션 차원의 보안 취약점, 버퍼 오버플로우, DoS 공격, 포트 검사 등을 막아 줍니다.
- **네트워크 바이러스:** 스트림 기반의 바이러스 백신 방어는 압축 파일이나 웹 트래픽(압축 HTTP/HTTPS)에 숨겨져 있는 맬웨어와 PDF 바이러스를 포함하여 수백만 가지 변종 맬웨어를 차단합니다. 정책 기반의 SSL 해독(decryption)은 SSL 암호화 애플리케이션을 통해 이동하는 맬웨어를 차단합니다.
- **URL 필터링:** 관리자는 사용자 정의 가능한 완전 통합형 URL 필터링 데이터베이스를 사용하여 세부적인 웹 브라우징 정책을 적용할 수 있으며, 이로써 애플리케이션 가시성 및 제어 정책을 보완하고 법적 위험, 규제 위험, 생산성 위험으로부터 회사를 완벽하게 보호할 수 있습니다.
- **파일 및 데이터 필터링:** 관리자는 데이터 필터링 기능으로 파일 및 데이터 전송에 수반되는 위험을 경감하는 정책을 구현할 수 있습니다. 파일 확장자만이 아니라 파일의 내용을 검사하여 허용 여부를 결정함으로써 파일 전송과 다운로드를 제어할 수 있습니다. 일반적으로 드라이브 바이(drive-by) 다운로드에서 발견되는 실행 파일을 차단함으로써 미확인 맬웨어가 네트워크에 확산되지 않도록 막을 수 있습니다. 끝으로 데이터 필터링 기능을 사용하여 기밀 데이터 패턴(신용카드 번호 및 주민등록번호 등)을 감지하고 제어할 수 있습니다.



콘텐츠 및 위협 요소 가시화
URL, 위협 요소 및 파일/데이터 전송 활동을 쉽고 간결한 형식으로 볼 수 있습니다. 필터를 추가 및 제거하여 개별 요소를 보다 자세히 파악합니다.

최신 맬웨어 감지 및 방지

확장 가능한 네트워크형 애플리케이션으로 진화한 맬웨어 덕분에 공격자들은 목표로 삼은 네트워크에 그 어느 때보다 손쉽게 액세스하여 위협할 수 있게 되었습니다. 최신 맬웨어의 힘이 커진 데 따라 기업에서는 위협 시그니처가 아직 정의되지 않았더라도 즉각적으로 위협 요소를 감지할 능력을 반드시 갖춰야만 합니다. Palo Alto Networks의 차세대 방화벽은 실행 파일과 네트워크 트래픽을 모두 사용하는 다면적 접근 방식으로 시그니처가 아직 공개되지 않은 상태에서도 기업 네트워크를 보호해 줍니다.

- **WildFire™:** 클라우드 방식의 WildFire는 안전한 가상 환경에서 실행 파일의 동작을 직접 관찰함으로써 아직 확인되지 않은 악성 실행 파일의 정체를 보여 줍니다. WildFire는 Microsoft Windows 실행 파일 안에 레지스트리 값 또는 운영 체제 파일을 바꾸거나, 보안 메커니즘을 무력화하거나, 실행 프로세스에 코드를 삽입하는 등의 악성 요소가 숨겨져 있는지 검사합니다. 이러한 직접 분석을 통해 보호 메커니즘이 아직 완성되지 않은 상태에서도 빠르고 정확하게 맬웨어를 식별할 수 있습니다. 결과는 관리자가 적절한 조치를 취할 수 있도록 즉각 전달되며, 이어서 자동으로 시그니처가 만들어지고 다음 번 콘텐츠 업데이트를 통해 모든 고객에게 배포됩니다.
- **행위기반 봇넷 탐지:** App-ID는 애플리케이션 수준에서 모든 트래픽을 분류하여 네트워크에 있는 미확인 트래픽의 정체를 밝혀냅니다. 이러한 트래픽은 대개 맬웨어나 기타 위협 요소를 의미합니다. 행위기반 봇넷 보고서는 맬웨어 사이트 반복 방문, 동적 DNS 사용, IRC, 기타 의심스러운 행동 등 봇넷 감염을 암시하는 네트워크 상황을 분석합니다. 결과는 감염 가능성이 있는 호스트 목록으로 표시되며, 이러한 호스트를 대상으로 봇넷 조사를 실시할 수 있습니다.

트래픽 모니터링: 분석, 보고 및 포렌식

최선의 보안은 관리자가 회사 자산을 보호하기 위해 적극적이고 지속적으로 정보를 수집하고 조정하는 한편 보안 사건에 대한 사후 대응, 조사, 분석 및 보고를 균형 있게 수행할 때 이루어집니다. ACC와 정책 편집기를 사용하여 애플리케이션 허용 정책을 사전에 적용하고, 다양한 모니터링 및 보고 도구로 Palo Alto Networks 차세대 방화벽을 통과하는 애플리케이션, 사용자, 콘텐츠 등을 분석 및 보고할 수 있습니다.

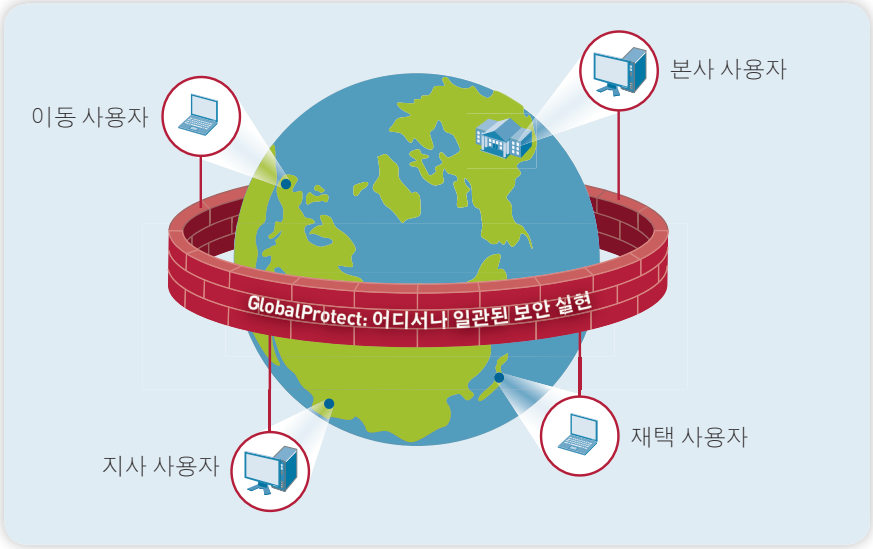
- **App-Scope:** 사용자가 직접 정의 가능한 App-Scope에는 시간에 따른 애플리케이션, 트래픽, 위협 활동 등이 동적으로 표시되어 실시간으로 표시되는 ACC의 애플리케이션 및 콘텐츠 정보를 보완합니다.
- **보고서:** 기본 제공되는 보고서를 그대로 사용하거나, 필요에 따라 사용자 정의하거나, 보고서를 하나로 묶을 수 있습니다. 모든 보고서는 CSV 또는 PDF 형식으로 내보낼 수 있으며 예약 실행 및 이메일 전송이 가능합니다.
- **로그 기록:** 실시간 로그 필터링으로 네트워크의 모든 세션에 대해 간편하고도 신속하게 포렌식 검사를 할 수 있습니다. 로그 필터 결과는 CSV 파일로 내보내거나, 오프라인 보관 또는 추가 분석을 위해 syslog 서버로 보낼 수 있습니다.
- **세션 추적 도구:** 트래픽, 위협 요소, URL, 애플리케이션 등 개별 세션과 관련된 모든 로그의 상관 관계를 중앙에서 파악할 수 있어 포렌식 또는 사고 조사의 속도가 빨라집니다.

Global Protect: 어디서나 일관된 보안 실현

기업의 변화를 요구하는 것은 애플리케이션만이 아닙니다. 점점 더 많은 최종 사용자들이 어떤 장소에서나 자신의 기기로 접속하여 업무를 하는 것이 당연하다고 생각하고 있습니다. 이에 따라 IT 부서에서는 과거 기업의 영역을 한참 벗어나는 이러한 기기 및 위치에까지 보안을 확장하느라 애쓰고 있습니다. Global Protect는 위치와 기기를 불문하고 모든 사용자에게 일관된 보안 정책을 확대 적용함으로써 이러한 난관을 해결합니다.

첫째, GlobalProtect는 Microsoft Windows, Apple Mac OS X, Apple iOS 등 다양한 장치를 지원하는 투명한 VPN을 통해 모든 사용자에게 안전한 연결을 보장합니다. 일단 연결된 후에는 방화벽에서 모든 트래픽을 분류하고, 허용 정책을 적용하며, 트래픽의 위협 요소를 검사하여 네트워크와 사용자를 보호합니다.

또한 GlobalProtect는 최종 사용자의 기기 상태에 따라 별도의 통제 수단을 적용할 수도 있습니다. 예를 들어 바이러스 백신이 구형인 장치나 디스크 암호화가 설정되지 않은 장치를 사용하는 경우, 네트워크의 민감한 영역 또는 특정 애플리케이션에 대한 사용자 액세스를 거부할 수 있습니다. IT 부서에서는 이로써 최종 사용자의 광범위한 장치에 대해 안전한 애플리케이션 사용을 보장하는 한편 혁신적인 보안 방식을 일관성 있게 적용할 수 있습니다.



GlobalProtect
위치와 관계없이 모든 사용자에 대해 일관된 애플리케이션 보안 허용 정책을 적용합니다.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

본사: +1.408.573.4000
영업: +1.866.320.4788
지원: +1.866.898.9087

www.paloaltonetworks.com

PAN_DS_FFOV_090111