ARISTA 솔루션 백서

클라우드 데이터센터의 보안

소프트웨어형 데이터센터 보호를 위한 심층 방어 전략 채택

소개

보안 관련 문제

오늘날에는 첨단 보안 위협이 표적 대상을 더 구체적으로 지정하고 더 은밀하게 작동합니다. 즉, 이제는 DoS(서비스 거부 공격)뿐만이 아니라 데이터센터 내에 상주한 중요 데이터에 대한 공격도 일삼고 있습니다.

침입, DDoS 공격, APT, 감지 불가능한 백도어 침투, 특정 대상에 대한 복잡한 다단계 공격 등은 감지하기가 거의 불가능한 경우가 많습니다.

공격에 대한방어

모든 유형의 기업에서는 공격과 데이터 손실을 방어할 수 있도록 작업 가능한 지능형 기능을 준비하고 일반적인 기준을 마련해야 합니다.

현대의 사이버 방어와 손실 완화 전략에 있어 공격 패턴을 조기에 감지하고 자동화된 방식을 통해 위험에 대응하는 능력은 이제 필수 요소입니다.

솔루션 요소

적극적인 모니터링 정책과 대응 계획을 마련하면 다음과 같은 방식을 사용하여 대상 지정 공격을 가장 효율적으로 방어할 수 있습니다.

- 가상화된 클라우드 네트워크에서 다중 테넌트 액세스 및 테넌트 간 보호
- Arista DANZ를 사용하여 데이터 손실 및 위협 방지 상황을 지속적으로 모니터링
- SDN 트리거와 자동화를 통한 원활한 확장성 및 서비스 통합
- 차세대 방화벽을 사용하여 100Gbps 이상의 클라우드급 성능을 제공하는 DirectFlow 가속

오늘날 대부분의 조직은 데이터센터에 클라우드를 기반으로 한 방식을 도입하고 있습니다. 업무 속도는 높이고 비용은 낮추며 고밀도 가상화의 성능을 강화하기 위해 네트워크 대역폭을 늘리고 고급 분석 기능을 통해 빅데이터가 제공하는 대량의 정보를 보관하는 리소스를 상세하게 가상화하는 등의 방식이 그 예입니다. 그러나 이와 같은 매우 동적인 고성능 컴퓨팅 및 데이터 관리 인프라에서 무중단 업무 방식을 보장하고, 중차대 데이터와 최종 사용자 개인 정보를 보호하고, 안전한 액세스 기능을 제공하는 과정이 매우 복잡하므로 네트워크 및 데이터 보안과 관련한 새로운 방식이 필요하게 되었습니다.

신규 데이터센터 보안 요구 사항

정부, 서비스 제공업체나 기업 조직이나 할 것 없이, 대상이 지정된 사이버 공격에 대응하여 방어 전략 방식을 변경하는 것이 새로운 추세로 떠오르고 있습니다. 오늘날에는 DoS(서비스 거부 공격), 무단 액세스, 맬웨어 삽입, 광범위한 데이터 도용 등이 결합되어 사용자가 알 수 없는 위험한 다단계 공격이 주로 행해지고 있습니다. 발각되지 않고 중요한 데이터 자산에 액세스하거나 해당 자산을 손상시키려는 사이버 범죄자들이 이와 같은 첨단 공격을 감행하는 경우가 종종 있습니다.

2013년에 PwC 지와 CSO 지에서 진행한 사이버 범죄 상태 설문 조사에 따르면, Fortune 500대 기업조차도 사이버 범죄의 피해자가 되고 있는 것으로 나타났습니다.
이 설문은 500명의 미국 기업 임원, 보안 전문가, 그리고 공공/개인 부문의 기타 인원을 대상으로 행해졌습니다. 이러한 조직은 자체 방어를 위한 최적의 최신 도구를 도입하면서 동시에 사이버 범죄를 방지해서 조직에게 오는 경제적 영향이 무엇인지 파악하려고 합니다.

한 가지 도구로는 오늘날 성행하는 수많은 공격 모드와 익스플로잇을 방어하기가 어려운 것이 사실입니다. 그렇다고 광범위한 방어 전략을 펼치면 10Gbps 이상의 액세스 속도에서는 비용적으로 제한되는 부분이 많습니다. 그러나 중요한 데이터 자산을 보호해야 하는 조직은 총체적/비용 효율적으로 확장 가능한 충실도가 높은 지능형 위협 방지 방식을 채택해 위협 범위를 보다 명확하게 파악하는 동시에 적극적인 방어 기능을 이용해야 합니다. 이를 위해 다음과 같은 기능을 이용할 수 있습니다.

- 가상화된 클라우드 내의 경계가 없는 분산형 보호 기능
- 지속적인 엔드 투 엔드 전체 네트워크 및 시스템 모니터링 기능
- 모든 잠재적 위협 활동 감지, 순위 지정, 상관 관계 지정 기능
- 필요 시 컨트롤을 자동으로 활성화하고 보다 세밀한 검사를 수행하는 기능
- 보다 효율적인 배치 및 전반적인 보안 비용 관리 기능

ARISTA

보안 위협에 대응하기 위해 여러 보완 도구를 배치하는 포괄적 방식을 '심층 방어' 전략이라고 합니다. 이러한 전략은 오늘날의 기업 및 서비스 제공업체 데이터센터에 매우 중요합니다. 이 백서에서는 이러한 방식에 대해 간략하게 설명합니다.

최신 소프트웨어 정의 데이터센터와 보안 요구 사항

오늘날에는 운영 방식이 매우 복잡해지면서 IT와 보안 운영 측면에서 핵심 요구 사항을 미처 처리하지 못하게 만드는 여러 가지 환경적 요인이 발생하고 있습니다. 실제로 네트워크 운영 팀과 보안 운영 팀 간의 요구 사항이 상충하면서 보안 및 데이터 보호와 관련해 프로필 중요도가 높은 큰 결함이 발생하는 경우도 있습니다. 이러한 상황에서는 현재 데이터센터 IT 운영 팀과 보안 운영 팀이 협력하여 다음과 같은 목표를 달성해야 합니다.

- 제한적인 리소스로 서비스를 제공하고 지속적인 사용 가능성 보장
- 중요한 데이터 자산과 고객의 개인 정보 보호
- 자산이나 서비스 손실이 발생하기 전에 즉시 대처하여 공격 완화
- 1/10Gbps에서 40/100Gbps로 마이그레이션할 때 보안 투자에 대한 ROI(투자 수익률) 극대화

오늘날의 데이터센터 환경에서는 '경계 보호'라는 개념이 사실상 유명무실해졌습니다. 현재 데이터센터에서는 동서 트래픽(East-West Traffic) 패턴이 주로 사용되며, 분산형 어플리케이션 계층마다 상호 작용 모델이 각기 다르므로 리소스를 격리하고 보호하기가 어렵습니다. 이제는 데이터센터를 보호하기 위해 보안 경계에 보호 기능을 삽입하는 것만으로는 충분하지 않습니다. 도구 삽입, 위협 감지, 적극적 완화를 통합하는 방식이 필수입니다.

또한 오늘날의 데이터센터에서는 완전한 어플리케이션을 제공하기 위해 컴퓨터 간 통신 기능을 제공하는 계층형 서비스를 사용하므로 문제를 감지하고 완화하는 과정이 더욱 복잡해졌습니다. 이러한 어플리케이션 아키텍처를 사용하는 경우 최종 사용자용으로 확장 가능한 어플리케이션 서비스를 구축하는 데 대량의 동서 트래픽(East-West Traffic)에 더욱 의존하게 될 수 있습니다. 뿐만 아니라 네트워크 기반 API를 통해 각 계층을 해당 계층의 클라이언트와 통합하는 경우 보호해야 하는 위협 전파 영역이 새롭게 등장할 수도 있습니다. 이러한 상황에서 데이터센터 작업 영역을 보호하고 관리하기 위해 계층 간에 어플리케이션을 중심으로 파악하고 모든 동서 트래픽(East-West Traffic) 및 VM 간의 트래픽을 파악하는 문제 역시 갈수록 중요해지고 있습니다.

보안 기능을 삽입할 위치
대상이 지정된 첨단 방식 위협으로부터 오늘날의 데이터센터를 보호하려면 개선된 파악 기능이 필요하며 보안 도구를 네트워크 자체와 효율적으로 통합해야 합니다.

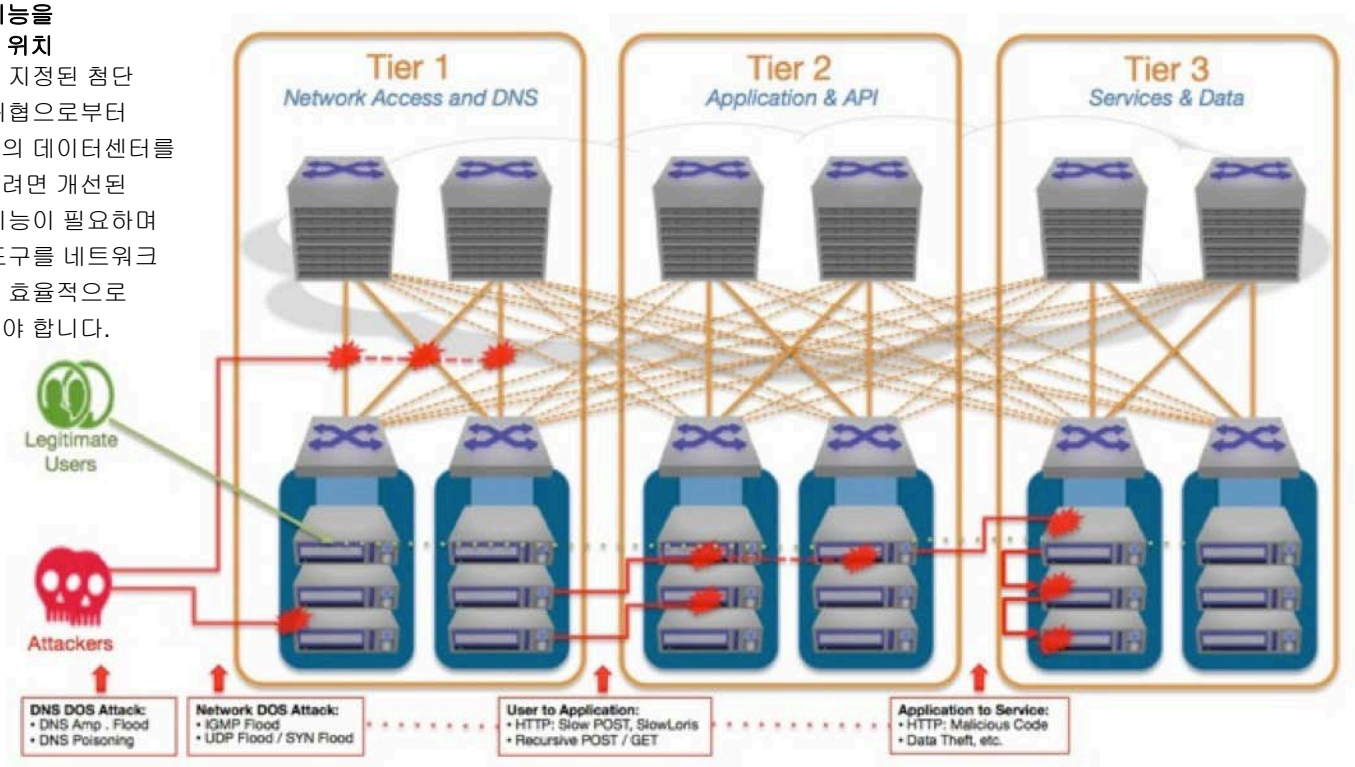

그림 1: 동서 트래픽(East-West Traffic) 패턴으로 인해 새로운 보안 문제가 발생한 클라우드 데이터센터

또한, 소프트웨어형 데이터센터와 관련한 보안 결정을 까다롭게 만드는 주요 요인은 동서 트래픽(East-West Traffic) 파악 시 컴퓨팅, 스토리지, 네트워크 가상화가 주는 영향입니다. VM 간의 트래픽이 증가함에 따라 같은 데이터센터 내의 개별 테넌트를 서로 격리하고 보호해야 하는 중요성도 높아지고 있습니다. 데이터센터 아키텍처와 보안 도구 배치에 주는 영향은 굉장히 클 수 있습니다.

보안 기능 도입 시작

IT 조직은 포괄적인 파악 기능, 적극적인 경로 완화, IT 운영을 위한 고급 지능형 도구의 유동적 배치를 통해 광범위하게 가상화된 클라우드급 데이터센터에서도 새롭게 대두되는 위협 환경에 대처해 효율적으로 방어할 수 있습니다. IT 운영팀과 보안 운영 팀은 Arista의 소프트웨어 중심 클라우드 네트워킹을 기반으로 하는 유동적인 데이터센터 아키텍처를 사용함으로써 네트워크 및 어플리케이션을 파악하기 위한 대역 내/외 요구 사항을 모두 충족하는 소프트웨어 중심 파악 및 제어 기능을 활용할 수 있습니다. 그리고 다음과 같은 작업을 수행하는 데 필요한 자동화, 서비스, 포괄적인 파악 기능을 제공할 수 있습니다.

- 중차대한 리소스 손상 시 트래픽을 작업 가능하게 재분산하도록 허용
- 프로그래밍 방식으로 공격에 대응하고 공격을 기록할 수 있는 중차대한 역할 제공
- 모든 트래픽을 프로필이 지정된 공격 패턴에 따라 검사한 다음 분석을 위해 도구로 리디렉션
- 외부의 받는 사람에게 전송(유출)되는 정보 추적
- 부하 분산 및 HA를 유지하면서 위험한 트래픽에 대해 차세대 방화벽 보안을 인라인으로 유지

포괄적 파악

심층 방어 위협 방지 전략을 도입하려면 먼저 내부에서 위험을 명확하게 평가해야 하며, 공격이 진행 중임을 나타낼 수 있는 외부 작업과 트래픽 패턴을 파악해야 합니다. 위협 벡터를 효율적으로 감지하고 이해하려면 먼저 모든 네트워크 트래픽을 효율적으로 모니터링 및 프로파일링하는 방식을 구축하여 '정상' 기준이 무엇인지부터 이해해야 합니다.

네트워크 액세스 속도가 10Gbps를 초과하면 저속에서 데이터센터의 트래픽을 모니터링하도록 설계된 대부분의 도구에서 확장 문제가 발생합니다. APM(어플리케이션 성능 관리), NPM(네트워크 성능 관리), 보안 도구의 벤더는 보다 빠르고 규모가 큰 플랫폼을 제공함으로써 점점 더 빨라지는 네트워크 캡처와 분석에 대한 수요를 해결해 왔습니다. 하지만 포괄적 모니터링을 수행하는 데에는 여전히 매우 많은 비용이 소요되는 것으로 보입니다.

Arista는 수상 경력에 빛나는 Arista EOS® 소프트웨어를 통해 구동되는 고밀도 non-blocking 10/40/100GbE 네트워크를 제공하는 새로운 모니터링 집적 방식을 제공합니다. 이 방식으로 클라우드급 모니터링 기능을 구축하는 데 드는 비용을 크게 줄일 수 있습니다. Arista DANZ(데이터 분석기) 솔루션은 유동성과 정밀도가 매우 우수한 확장 가능 엔드 투 엔드 네트워크 및 어플리케이션 모니터링 기능을 제공합니다. 그와 동시에 10/40/100Gbps를 지원하도록 확장하면서 기존의 제3자 모니터링 도구를 캡처된 데이터와 비용 효율적으로 직접 통합하는 기능도 제공합니다.

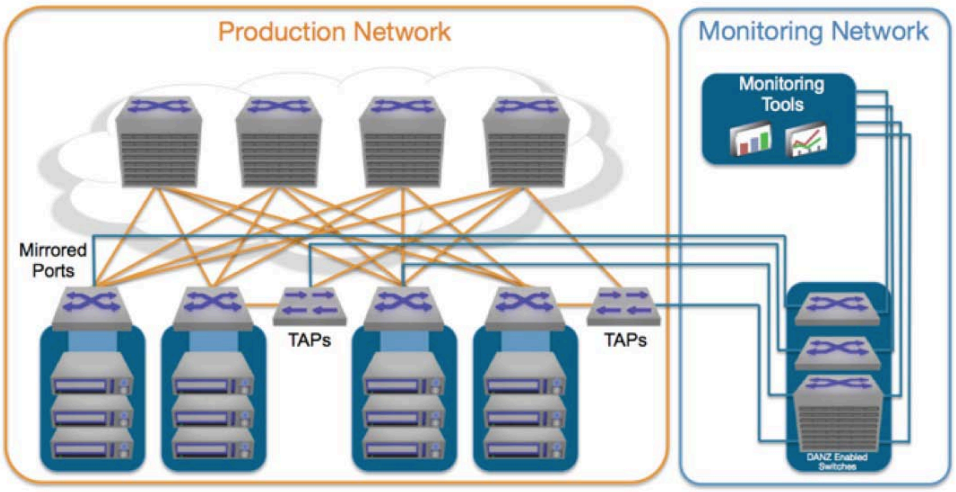

그림 2:DANZ – 실시간 분석을 위해 모든 트래픽에 액세스

보안, 성능, 문제 해결 정보를 모니터링하기 위한 가장 유용하고 자세한 정보 출처는 원시 패킷 데이터이지만, 유용하게 활용할 수 있는 다른 정보 출처도 있습니다. 여기에는 sFlow의 대략적인 흐름 분석 데이터, Splunk에서 제공하는 컴퓨터 로그 및 네트워크 이벤트 메커니즘의 내부 네트워크 운영 데이터, 그리고 Arista 스위치의 LANZ 큐 분석과 같은 기능이 제공하는 정밀 데이터가 포함됩니다.

Arista DANZ 기능 세트는 Arista의 데이터센터급 스위치를 통해 기존과는 전혀 다른 새로운 기능을 제공합니다.

- 고급 트래픽 관리 기능을 사용한 고밀도 non-blocking 와이어 스피드 패킷 캡처를 통해 모든 네트워크 트래픽을 손실 없이 모니터링할 수 있습니다.
- Arista EOS의 프로그래밍 기능을 통해 제공되는 SDN(소프트웨어형 네트워크)이 지원됩니다. 이를 통해 원하는 분석 도구로 향하도록 특정 네트워크 흐름을 직접 조종할 수 있습니다.
- 플로우별 대칭 부하 분산 기능을 통해 세션별 인식을 그대로 유지하면서 테라비트 속도를 지원하도록 인라인 보안 및 모니터링 도구를 확장할 수 있습니다.
- LANZ(레이턴시 분석기) 기능을 통해 툴 포트에서 마이크로버스트 및 혼잡 상황을 감지할 수 있습니다. 따라서 네트워크 운영자가 부하가 많을 때에도 네트워크를 계속 파악할 수 있도록 적절한 작업을 수행하고 100% 충실도로 보안 감독 기능을 보장할 수 있습니다.
- 새롭게 등장한 네트워크 가상화 모델(예: vMotion, VXLAN, NVGRE)을 지원함으로써 매우 동적으로 가상화된 공개/비공개 클라우드의 모든 작업 부하를 지속적으로 파악할 수 있습니다.

네트워크 인프라에 직접 사용할 수 있는 API를 통해 트리거 및 자동화된 작업이 지원됩니다. 로그 모니터링과 패킷 캡처를 통해 직원들이 이메일로 팀 멤버에게 알림을 보내고 의심스러운 트래픽과 이벤트 로그를 SIEM과 트래픽 기록 도구로 자동 리디렉션함으로써 빠르게 대응할 수 있습니다. 그러면 대응자가 공격자의 신원과 현재 진행 중인 공격 시나리오의 세부 사항을 즉시 파악할 수 있습니다.

DANZ를 통해 보안 모니터링 과정에 적극적인 완화 기능 추가

일반적으로 패킷 캡처의 원시 패킷 데이터를 사용하는 도구와 DANZ 등의 모니터링 아키텍처는 성능 분석 정보 제공, 문제 파악과 해결, 복잡한 계층 간 어플리케이션의 변칙 감지 등의 작업을 중점적으로 수행합니다. 그러나 이러한 도구의 지능형 기능을 사용하여 공격을 적극적으로 완화하는 새로운 방식에서는 이제 SDN(소프트웨어형 네트워킹) API를 통한 네트워크 프로그래밍 기능을 활용하여 적극적인 완화 기능을 신속하게 제공합니다.

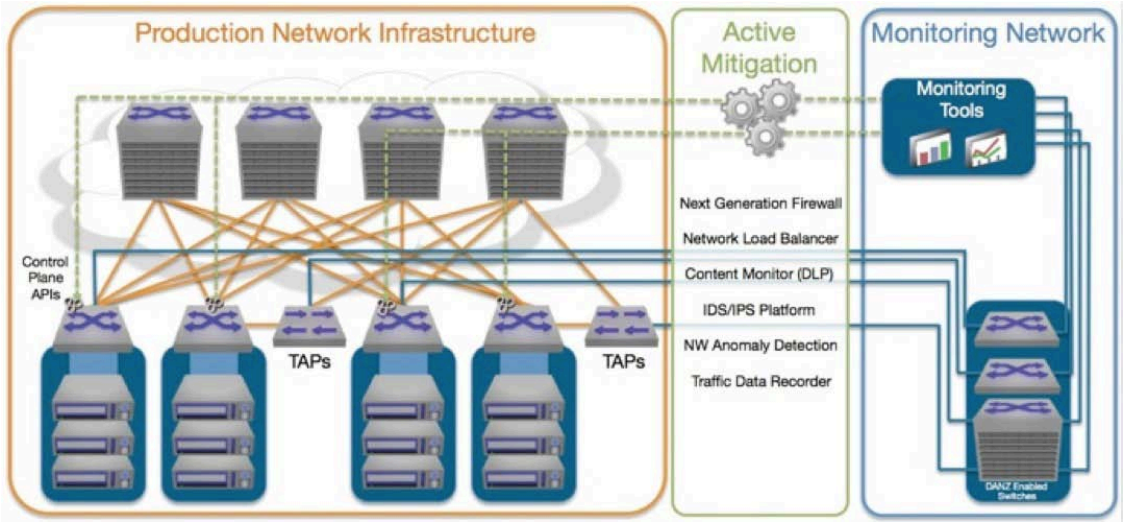

그림 3:DANZ – 고급 보안 도구를 통한 적극적인 완화

DANZ 등의 최신 네트워크 모니터링 아키텍처는 고급 네트워크 하드웨어 기능을 사용하여 각 도구에 대해 네트워크에서 대상이 지정된 특정 데이터 액세스 권한을 제공하며, 효율성을 최대화하기 위해 트래픽이 도구에 도착하기 전에 트래픽 조건을 지정합니다. 인라인 보안 장치로 인해 레이턴시가 증가하고 전반적인 네트워크 성능의 효율성이 저하될 수 있는 인라인 완화 솔루션을 사용하는 경우 대역 외 모니터링을 수행하여 단점을 보완할 수 있습니다.

심층 방어를 위해 적절한 보안 도구 선택

현실적으로 하나의 보안 도구나 벤더가 정보 보안과 관련된 모든 문제를 처리할 수는 없으며, 그렇게 주장해서도 안 됩니다. 대부분의 벤더가 널리 사용되는 보안 기술의 비효율성과 관련하여 주장하는 내용은 타당합니다. 서명 기반 또는 통계 기반 위협 감지 방식의 다양한 단점을 그 예로 들 수 있습니다. 실제 솔루션에는 정상 상태의 기준을 정하기에 적절한 정보, 제품 및/또는 서비스가 효율적으로 조합되어 있어야 하며, 갈수록 정교해지는 공격 방식에 대응할 수 있는 완화 솔루션이 포함되어 있어야 합니다. 현재는 갈수록 심각해지는 가로채기 공격에 팀이 효율적으로 대응하는 데 필요한 다양한 기술이 제공되고 있습니다.

표 1: 보안 기술 - 체감된 장단점

보안 기술	장점	단점
네트워크 트래픽 모니터(스니퍼, IDS, IPS, 패킷 레코더, 데이터 분석)	적절한 분석을 통해 정상 및 비정상 네트워크 트래픽 둘 모두에 대한 정보를 제공할 수 있습니다. 트래픽 레코더는 포렌식스 도구로도 매우 유용하게 활용될 수 있습니다.	보안 데이터 스트림(IPSEC, HTTPS, 암호화된 터널)을 모니터링할 수 없으며, SIEM 데이터를 함께 사용하지 않으면 보안 위험을 명확히 확인할 수 없습니다.
활성 네트워크 스캐너(리소스 및 노출된 PII(개인 식별 정보)를 파악하기 위한 어플리케이션 탐사, 포트 탐사)	지속적인 탐사 및 모니터링을 통해 상황을 인식할 수 있으며 자산이 네트워크 내부에 배치된 기록 내역을 확인할 수 있습니다.	동적인 고성능 세그먼테이션 클라우드에 배치하려면 비용이 많이 들 수 있습니다. 대용량 데이터를 저장하고 보호하는 속도가 느리며, 복잡한 분석으로 인해 정보를 제때 확인하기 어려울 수 있습니다.
인라인 방화벽 및 게이트웨이(스테이트풀 필터링, 이메일 모니터링, 컨텐츠 검사, 바이러스 백신 등)	외부 출처의 알 수 없는 제로 데이 익스플로잇을 캡처하고 차단하는 유일한 옵션입니다. 호스트에 의해 네트워크로 유입되는 취약성 또는 테넌트 간 취약성의 캡처 효율성은 더 떨어집니다.	클라우드의 가상화된 게이트웨이 및 방화벽은 맬웨어를 효율적으로 감지하거나 차단하지 못하며 제로 데이 익스플로잇은 서명 기반의 게이트웨이를 우회할 수 있습니다.

SIEM(보안 정보 및 이벤트 분석)	다양한 도구, 플랫폼 등을 통해 매크로(로그) 데이터에 대한 통합 및 분석 기능을 제공하며, 심층 방어 전략을 관리하기가 가장 쉽습니다.	단독으로는 작동할 수 없으며 실제 위협 상황과 이벤트를 감지하려면 여러 가지 도구를 같이 배치해야 합니다. 다른 도구를 보완하는 기술로 간주할 수 있습니다.

적절한 보안 정책을 가장 효율적으로 적용하려면 새롭게 등장하는 공격 도구와 동급 최고의 방어 도구 사이에서 끊임없이 대처해 나아가야 하며, 개별 분야에서 가장 뛰어난 기능을 제공하는 것으로 입증된 보완 장치와 기술을 전문 지식과 함께 활용해야 합니다. 조직은 네트워크 및 어플리케이션 작동 기준을 확립할 다양한 도구를 사용하여 실제 위협이 진행 중임을 나타낼 수 있는 위험 및 중요 영역을 파악할 수 있습니다.

또한 정상 트래픽 패턴을 파악하고 나면 과학적인 방식을 통해 공격과 공격 전에 나타날 수 있는 탐사 과정을 실시간으로 검색할 수 있습니다. 그러면 확인되지 않았거나 예상치 못한 공격자의 공격을 방어할 수 있는 자동화된 정책과 트리거를 준비하도록 작업 가능한 정보를 사용할 수 있습니다. 다양한 모니터링 기능을 기반으로 지능형 IT 운영 기능을 보다 광범위하게 사용하는 경우 획일적인 모니터링 아키텍처에 비해 제로 데이 공격, APT 등 새롭게 등장하는 위협을 더 잘 파악하는 것으로 나타났습니다.

Arista SDN을 통해 차세대 보안 기능 확장

SDN의 원칙과 기술을 따르면 대역 외 분석을 통해 네트워크를 전역적으로 파악하면서 도구를 방화벽 등에 인라인으로 삽입해야 하는 요구 사항을 충족할 수 있습니다. Arista EOS 네트워크 운영 체제의 SDN 기능에는 DireectFlow와 OpenFlow API를 사용하는 컨트롤러 독립적 아키텍처, 그리고 OpenStack과 기타 유명 네트워크/컴퓨팅 가상화 플랫폼(예: VMware vSphere/NSX, Microsoft Hyper-V)과의 자동화된 클라우드 통합 등이 포함됩니다.

또한 보안 서비스를 Arista의 VM 인식 아키텍처와 동적으로 바인딩하면 매우 동적으로 가상화된 클라우드 환경에서 보안을 지속적으로 유지할 수 있습니다. 이동 중인 작업 부하를 수용하기 위해 가상화된 네트워크, 가상화된 컴퓨팅 및 스토리지 인프라가 변경될 때마다 네트워크 자동화 스크립트를 통해 관련 정책과 도구 구성을 동적으로 구성할 수 있습니다. 이 모델을 적용하면 모든 동적 클라우드 환경을 영속적으로 파악할 수 있습니다. 따라서 네트워크의 규모에 맞게 지속적인 실시간 모니터링을 통해 적극적인 방어 기능을 제공하면서 Arista VM Tracer를 통한 VM 인식 방식으로 환경을 파악하고 모든 공격 가능 지점에서 트립 와이어를 원하는 대로 확장하여 프로비저닝할 수 있습니다.

Arista DFA(DirectFlow Assist)를 사용하는 동적 심층 방어 예제

DFA(DirectFlow Assist)는 EOS 확장으로, Arista 스위치에서 실행되어 Arista의 DirecFlow API를 통해 흐름 테이블 항목을 동적으로 삽입함으로써 방화벽 등의 연결된 인라인 또는 대역 외 보안 플랫폼을 오프로드하거나 지원합니다. DFA는 방화벽으로의 네트워크 포워딩을 통합 제어하는 기능을 제공함으로써 대역 외 모니터링을 통해 파생된 지능형 기능, DPI(딥 패킷 검사), 기타 분석 기술을 기반으로 네트워크에서 하는 동적 보안 정책을 적용할 수 있도록 합니다.

DFA는 확장성과 성능이 우수하므로 정적 인라인 배치에 비해 보안 플랫폼의 성능을 10~50배까지 높일 수 있으며, 모든 가상화된 환경 또는 클라우드 기반 환경에 적용할 수 있는 확장 모델을 제공합니다. DFA 솔루션의 사용 사례에는 차세대 방화벽, 컨텐츠 검사 플랫폼, IDS/IPS에 대한 DDoS 공격 완화 및 오프로드 등이 있습니다.

- DDoS 공격 완화(연결된 분석 플랫폼에서 감지된 DoS를 기반으로 흐름 내의 패킷을 선택적으로 차단)
- 엘리펀트 플로우 오프로드(백업 등의 신뢰할 수 있는 어플리케이션 트래픽이 방화벽을 우회하도록 흐름 엔트리 삽입)
- 방화벽 확장(방화벽 DPI 검색 및 분류를 기준으로 하는 흐름 단위 우회 및 필터링 기능 제공)
- 공격자 프로파일링 및 을 처벌을 위해 대상 트래픽을 "허니팟"(유인) 플랫폼으로 리디렉션

공격 중에 DFA에서 수행되는 작업

공격이 발생하면 어플리케이션은 SDN 사용 가능 스위치로 구성된 네트워크에 시스템이나 네트워크의 성능에 영향을 주지 않고 하드웨어에서 공격 트래픽 흐름을 삭제하도록 명령할 수 있습니다.

아니면 차세대 방화벽, IDS/IPS 플랫폼 또는 기타 보안 솔루션을 통해 심층 분석하도록 의심스러운 트래픽을 리디렉션할 수도 있습니다. 적극적인 완화를 통해 명령할 수 있는 트래픽 조작에는 다음 사항이 포함됩니다.

- 네트워크의 대상 흐름을 우회 또는 차단
- 나중에 분석하고 공격자를 처벌할 수 있도록 의심스러운 트래픽 캡처 및 기록
- 허니팟이나 트래픽 레코더 등의 대상에게로 명시적 트래픽 리디렉션
- 기타 사용자 정의 작업(예: 경보나 다른 플랫폼을 트리거하여 추가 기능을 수행하도록 명령)

방화벽 웹 콘솔, Arista EOS API를 사용하는 사용자 프로그램 또는 Arista CLI를 사용하면 DFA를 통해 원하는 네트워크 트래픽 흐름을 삽입하는 데 사용할 정책을 구성할 수 있습니다. DDoS 공격 완화 사례의 경우에는 DDoS 보호 정책이 만들어지며 방화벽에서 공격 볼륨 임계값과 부하 프로필을 지정합니다.

엘리펀트 플로우 사례에는 표준 보안 정책을 구성할 수 있습니다. 이러한 정책 내에서 "Log at Session Start(세션 시작 시 기록)"를 선택하고 "Log Forwarding(로그 포워딩)" 기능을 구성하면 DirectFlow Assist 프로세스가 수신 대기 중인 Arista 스위치에서 UDP 포트로 메시지를 보냅니다.

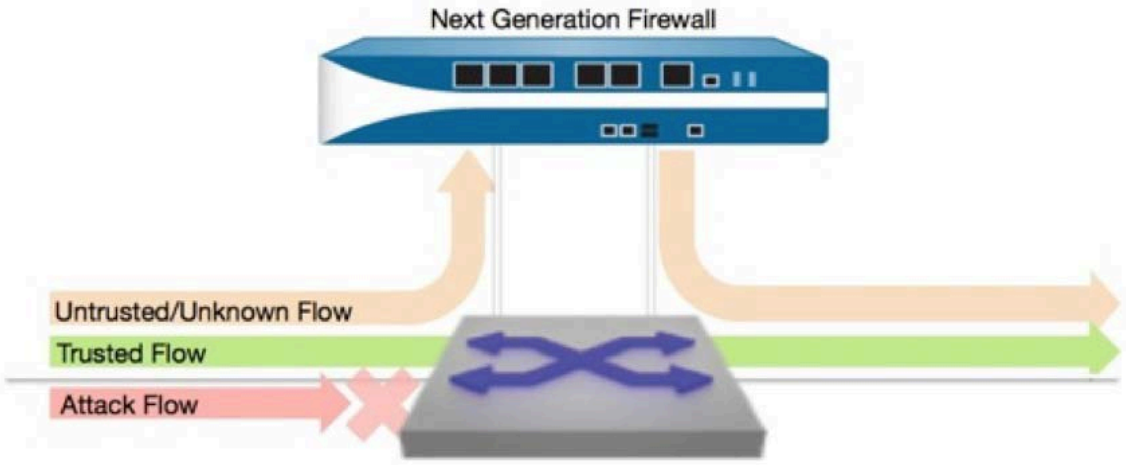

그림 4: DFA를 통해 SDN 방화벽 삽입 기능 사용

DFA는 방화벽에서 흐름 분류 메시지를 받으면 해당 메시지를 확인한 다음 "DFA Flow Specification(DFA 흐름 사양)"을 구문 분석합니다. 흐름 사양에는 고유한 흐름 이름, 일치 기준, 원하는 작업, 우선 순위, 수명이 포함됩니다. 일치 기준에는 흐름의 유형 및 맞춤 구성 파일 설정에 따라 원본/대상 IP 주소, 원본/대상 레이어 4 포트 및 프로토콜(ICMP, TCP, UDP)이 포함될 수 있습니다. 그리고 스위치에서는 방화벽을 우회하거나 추가 분석 정보를 제공하기 위해 특정 스위치 포트로 패킷을 출력하거나, 흐름의 패킷을 삭제하는 작업이 수행됩니다.

우회된 흐름의 경우에는 대칭이 되도록 역방향 반환 트래픽 흐름에 대한 추가 흐름 사양이 자동으로 만들어집니다. 흐름 엔트리는 노화 기능을 사용할 수 있으며, 이 경우 지정된 수명 주기 간격이 지나면 EOS가 흐름 엔트리를 삭제하거나 방화벽이 흐름을 명시적으로 제거할 수 있습니다.

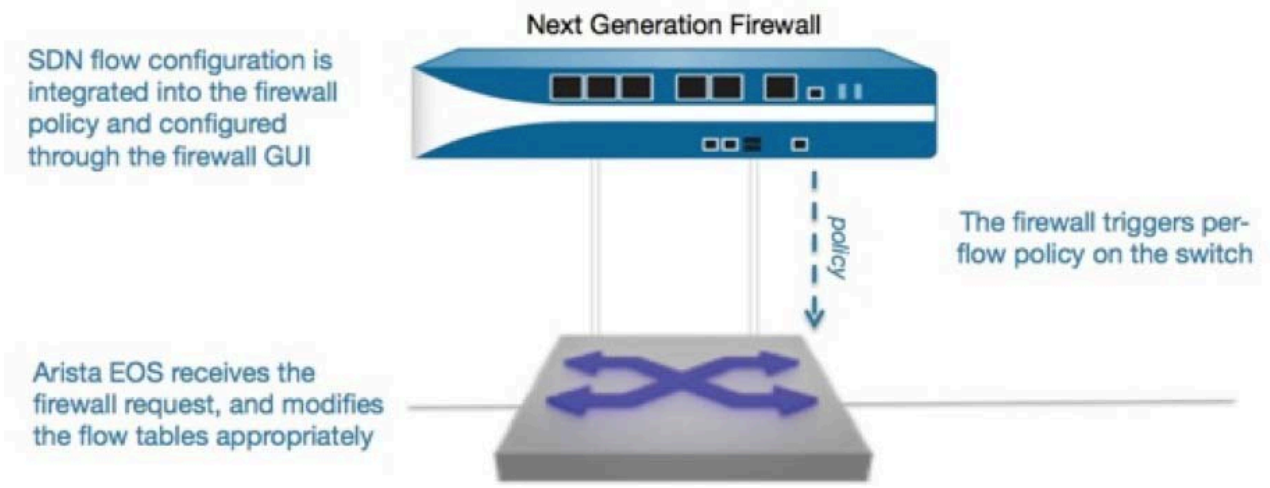

그림 5: 정책 삽입 - 트리거 및 작업

DFA는 흐름 사양에서 EOS DirectFlow API 구성 명령 시퀀스를 생성하여 흐름 테이블 엔트리를 생성합니다. 그런 다음 eAPI를 사용하여 이 구성 명령 시퀀스를 EOS로 보냅니다. DFA는 현재 활성 상태인 흐름을 모니터링하기 위한 여러 명령(예: 흐름 삭제, DirectFlow Assist 프로세스 시작/중지)이 들어 있는 명령줄 셸을 포함합니다.

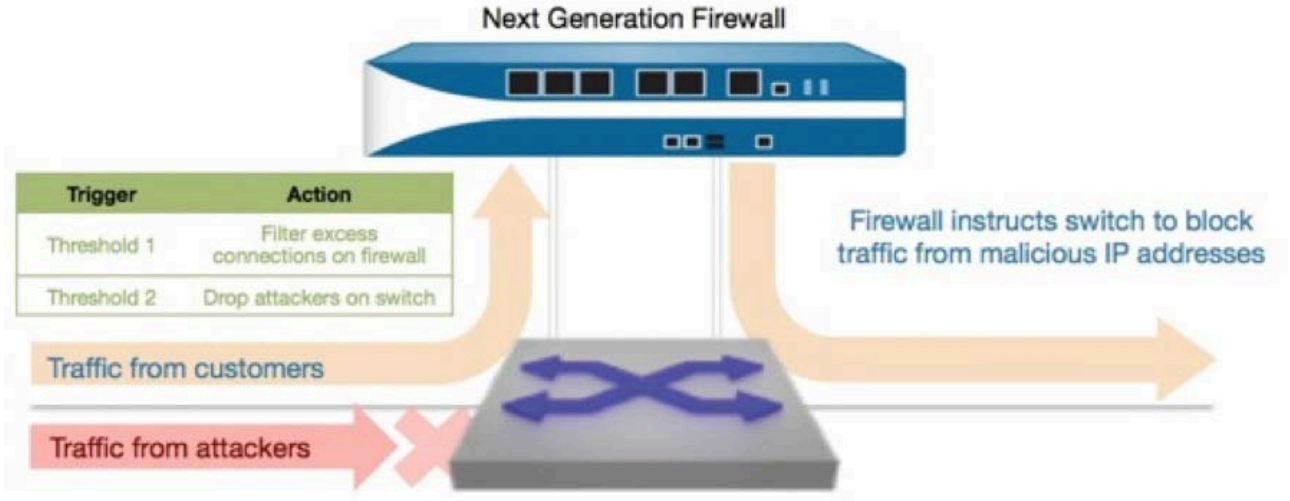

그림 6: 정책 실행 - DoS 완화 예제

Arista SDCN(소프트웨어 중심 클라우드 네트워킹)의 유동적 기능 중 한 가지 예인 DFA는 Arista EOS 운영 체제와 해당 API의 하위 기능을 일부 사용합니다. Arista의 SDCN은 클라우드 컴퓨팅의 필수 원칙인 자동화, 자체 프로비저닝, 성능/비용을 모두 고려한 일정하게 증가하는 확장 기능뿐만 아니라 네트워크 가상화, 맞춤형 프로그램 기능, 간소화된 아키텍처, 뛰어난 효율성을 모두 제공합니다.

결론

SDN 프로그래밍 기능을 제공하는 Arista EOS 소프트웨어 플랫폼의 클라우드 기능, 고급 네트워크 파악 기능을 제공하는 DANZ, 그리고 DFA(DirectFlow Assist)를 통해 기업과 서비스 제공업체 데이터센터 모두에 네트워크 보안을 최대화하는 동급 최고 소프트웨어의 기초를 확립합니다. 즉, 관리와 프로비저닝을 간소화하고, 서비스 제공 속도를 높이고, 비용을 줄이면서, 서비스를 차별화할 기회를 마련하고 네트워크, 보안 및 시스템 관리자에게 네트워크 제어 및 파악 능력을 되돌려주는 새로운 아키텍처를 IT 인프라 내의 가장 중차대한 위치에 구축할 수 있습니다.

Arista의 SDCN을 보안 협력사의 제품과 함께 사용하면 오늘날의 클라우드 데이터센터를 확장하고 효율적인 보안 기능을 통합하는 까다로운 작업을 수행할 수 있는 포괄적인 솔루션이 됩니다. 이러한 솔루션은 즉시 사용 가능하며, 갈수록 증가하는 심층 방어 기능에 대한 요구를 해결합니다.

2013년에 진행된 Ponemon Institute의 연구 결과에 따르면 특정 서버를 대상으로 하는 사이버 공격은 2013년에 발생한 데이터센터 장애 원인 중 18%를 차지한 것으로 나타났습니다. 2010년의 2%에 비해 크게 증가한 수치입니다. 상용으로 제공되는 공격 도구가 발전하고 네트워크 속도가 빨라짐에 따라 대량의 더미 트래픽을 생성하여 인라인 방어 기능을 무력화하기가 보다 쉬워지면서 이러한 공격이 크게 증가했습니다. Ponemon에 따르면 이러한 공격에 대응하기 위해서는 고급 분석 기능과 포렌식스 전문 지식을 사용해야 하는 경우가 종종 있다고 합니다.

산타 클라라 - 본사
5453 Great America Parkway
Santa Clara, CA 95054
전화: 408-547-5500
www.aristanetworks.com

아일랜드 - 국제부 본사
4325 Atlantic Avenue
Westpark Business Campus
Shannon
Co. Clare, Ireland

싱가포르 - APAC 관리 사무소
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

저작권 부분의 내용을 조정해야 하는 경우 법률 자문 부서에 문의하십시오.

저작권 © 2014 Arista Networks, Inc. 모든 권한을 보존합니다. CloudVision 및 EOS 는 Arista Networks, Inc.의 등록 상표이며 Arista Networks 는 Arista Networks, Inc 의 상표입니다. 다른 모든 기업의 이름은 각 권리 보유자의 상표입니다. 본 문서에 포함되어 있는 정보는 통지 없이 변경될 수 있습니다. 특정 기능은 아직까지 제공되지 않을 수 있습니다. Arista Networks, Inc.는 본 문서에 있는 일체의 오류에 대해 책임을 지지 않습니다. 년/월