클라우드 사용 편의성을 갖춘 동급 최고의 네트워크 보안 확보

AWS용 클라우드 NGFW 한눈에 보기

업계 동향

클라우드가 컴퓨팅 모델의 대세로 자리 잡을 전망이며, 기업에서는 이런 환경에서 자사 구축에 신속하고 비용 효율적인 방식으로 보안을 확보할 방법을 찾아야 합니다. Gartner에 따르면, 클라우드는 새로운 디지털 경험의 중심이 될 전망입니다. 새로운 워크로드 중 전체의 95%는 퍼블릭 클라우드에 구축되고 있습니다.[1] 또한 Palo Alto Networks에서 발표한 2022년 클라우드 네이티브 보안 현황에 따르면, 현재 전체 기업의 69%가 자사 워크로드의 반 이상을 클라우드에서 호스팅한다고 밝혔습니다. 이는 2020년 대비 123% 증가한 수치입니다.[2]

이처럼 워크로드가 퍼블릭 클라우드로 이동하면서, 워크로드끼리 상호 연결성도 전례 없이 심화되고 있습니다. 대부분 기업(55%)에서 자사의 보안 태세가 약하다고 보고해 왔으며, 기본적인 업무 활동을 보강할 필요가 있다고 생각합니다. 예를 들어 멀티 클라우드 가시성을 확보하거나, 여러 계정에 보다 일관성 있는 거버넌스를 적용하거나, 인시던트 대응과 조사를 간소화하여 보안 태세를 강화해야 한다는 것입니다.[4] 게다가, 주로 오픈 소스 보안 도구를 이용하는 기업의 80%는 보안 태세가 약하거나 매우 약한 것으로 드러나 문제가 한층 더 복잡한 양상을 띱니다.[5]

클라우드 도입 속도가 계속 빨라짐에 따라...

2025년에는 신규 디지털 워크로드의 **95%**가 클라우드 네이티브 플랫폼에 구축될 것으로 전망(2021년 30%에서 급증)1

2026년에는 퍼블릭 클라우드에 지출하는 비용이 엔터프라이즈 IT 비용 전체의 **45%**를 넘을 것으로 보이며, 이는 2021년 17% 미만에서 크게 증가한 수치임

출처: Gartner 보도 자료, 2021년 11월 및 2021년 8월

...리스크도 늘어나고 있음

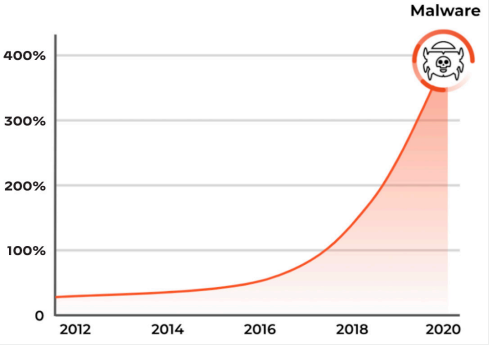

그림 1: Gartner에 따르면 클라우드는 새로운 디지털 환경의 중심이 될 것이며, 새로운 워크로드 중 95%는 퍼블릭 클라우드에 구축될 것으로 예측했습니다.[3]

[1] 출처: Gartner 보도 자료, 2021년 11월 및 2021년 8월.
[2] 출처: Palo Alto Networks 클라우드 네이티브 보안 현황 보고서 2022.
[3] Gartner, 앞서 언급한 자료
[4] 출처: Palo Alto Networks 클라우드 네이티브 보안 현황 보고서 2022.
[5] 출처 동일.

네트워크 기반 위협에 대한 이해

클라우드를 노리고 공격에 성공한 사례의 공통분모는 네트워크라는 점을 알아두어야 합니다. 여기에는 최근 출현한 악명 높은 Log4j 취약점과 REvil 해킹 그룹의 랜섬웨어 등이 포함됩니다. 다른 위협, 예를 들어 Bashlite의 DDoS(Distributed Denial of Service) 공격이나 Graboid의 크립토재킹 웜과 같은 경우 Docker 호스트를 사용해 크립토마이닝이나 C2(command-and-control) 공격에 사용할 리소스를 확산하고 스쿼팅(불법 점유)합니다.

애플리케이션 호스팅에 이용되는 대표적인 퍼블릭 클라우드 플랫폼인 Amazon Web Services(AWS®)를 이용하는 수많은 기업에서는 애플리케이션과 워크로드를 보호할 책임자가 누구인지 파악하는 것이 무엇보다 중요합니다. AWS에서는 고객의 중요 업무용 애플리케이션에 안정적인 인프라를 제공해야 한다는 자사 책임을 매우 진지하게 받아들입니다. 그 연장선상에서 AWS는 고객에게도 자사 앱을 보호할 책임이 있다는 사실을 이해하기 바랍니다. 고객에게는 끊임없이 진화하는 위협과 잠재적인 데이터 손실 위험으로부터 네트워크 연결과 자사 앱을 안전하게 지켜야 할 책임이 있습니다.

지금까지는 기업에서 주로 타사 방화벽이나 기본 내장된 네이티브 AWS 네트워크 방화벽을 이용해 왔습니다. 보안 모범 사례에 따르면 퍼블릭 클라우드 보안 태세는 데이터센터 보안 접근 방식과 비슷해야 합니다. 즉, 애플리케이션 가시성을 통해 위협에 대한 노출 현황을 파악하고, 정책을 사용해 공격 표면 면적을 줄여야 하며, 허용된 트래픽 내에서 위협과 데이터 유출을 방지해야 합니다.

클라우드 환경에서의 보호 대상은 다음과 같습니다.

- 인터넷 아웃바운드 트래픽 – 외부 개발자 리소스나 인터넷에 대한 아웃바운드 네트워크 액세스가 필요한 워크로드
- 인터넷 인바운드 트래픽 – 패치되지 않은 취약점을 포함할 수 있는 인터넷에 공개된 앱, 그리고 IPS 기능이 필요한 규제 대상 앱
- VPC 간(또는 이스트-웨스트) 트래픽 – VPC를 오가거나 VPC 내부의 클라우드 워크로드에는 네트워크 세그먼트 간 고급 세그먼테이션과 제어가 필요함

궁극적으로, AWS 고객에게는 점점 늘어나는 퍼블릭 클라우드 워크로드를 보호할 동급 최고 수준의 네트워크 보안을 간단하게 적용할 방법이 필요합니다. AWS 환경에서는 레이어 7 가시성과 보안을 갖춰 최신 사이버 공격을 차단하는 동시에 네트워크 보안과 DevOps 팀의 운영 간접비를 최소화해야 합니다.

이런 팀에서는 어느 솔루션을 구현하든 다음과 같은 기능을 갖춘 것이 이상적입니다.

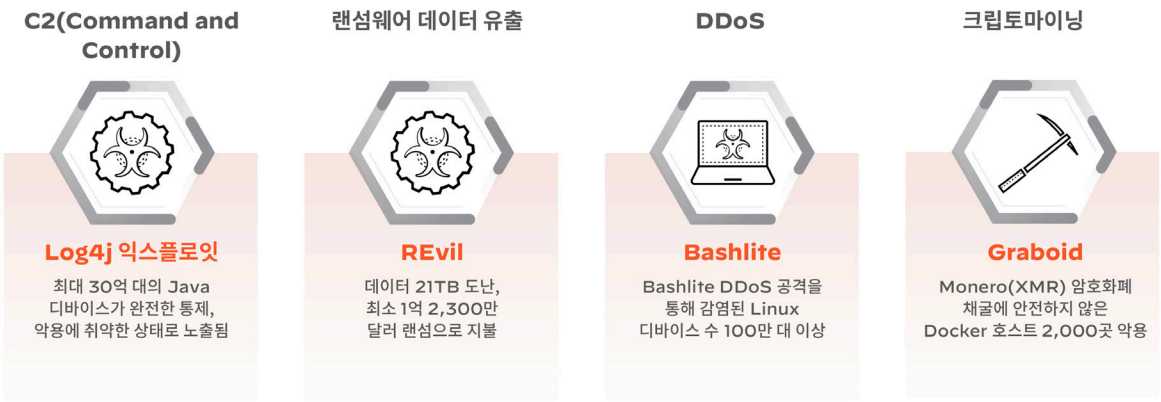

그림 2: 네트워크 기반 위협은 비즈니스 중단과 평판 훼손을 초래하며, 클라우드 공격 성공 사례의 공통분모는 바로 네트워크입니다.

- **네트워크 기반 위협 차단:** 위협의 형태는 끊임없이 변화하고 있습니다. 고객은 기본적인 레이어 4 보안과 IPS 시그니처 수준을 넘어 보안 기능을 강화하고자 합니다. 네트워크 보안팀에서는 새로운 위협을 차단하고 침해 리스크를 줄이기 위해 동급 최고의 보안을 확보해야 합니다.
- **모든 VPC 간 트래픽 보호:** VPC 내 클라우드 워크로드를 고급 세그먼테이션과 Threat Prevention 기능으로 안전하게 지킵니다.
- **현재 보안팀과 DevOps 팀의 업무 방식과 순조롭게 통합:** 기업에서 워크로드 보안 확보에 운영 오버헤드가 발생할지 걱정하는 것은 당연한 일입니다. 수많은 기업에서는 클라우드 서비스를 이용하는 것과 같은 방식으로 네트워크 보안을 이용하고자 합니다. 즉, 구축이 쉽고 유지관리할 필요가 없어야 합니다.

이렇게 하려면 네트워크 보안 효율성에 클라우드 네이티브의 사용 편의성을 겸비하여 네트워크 보안팀과 DevOps 조직이 모두 유익하게 이용할 수 있어야 합니다(그림 3 참조).

그림 3: 최신 엔터프라이즈에는 동급 최고 보안과 클라우드 네이티브 사용 편의성이 모두 필요합니다.

클라우드 NGFW 개요

효율성과 사용 편의성을 겸비한 솔루션을 소개해드립니다. 클라우드 NGFW는 동급 최고의 네트워크 보안을 클라우드 사용 편의성과 함께 보장합니다. 클라우드 NGFW는 Palo Alto Networks의 완전 관리형 클라우드 네이티브 서비스 형태로, AWS 마켓플레이스에서 조달하는 방식을 통해 최첨단 Threat Prevention 기능을 AWS 클라우드에도 확대 적용합니다.

클라우드 NGFW는 이러한 기능을 딥 러닝, 인라인 러닝으로 제공하여 실시간으로 제로데이 공격을 막고, 기업에서 워크로드를 보관해둔 AWS Virtual Private Cloud(VPC)를 노리는 위협을 차단합니다. 이제 네트워크 보안팀은 구축 전체에 걸쳐 동급 최고의 보호 기능을 손쉽게 도입하고 구축할 수 있으며, 적법한 웹 기반 서비스에 연결하여 앱을 보호할 수 있습니다.

이 클라우드 기반 서비스는 AWS 방화벽 관리자와 통합되는 첫 NGFW이므로, 고객에게 자동 크기 조정과 고가용성은 물론 유지관리가 필요 없다는 장점까지 제공합니다. AWS 마켓플레이스에서 클라우드 NGFW를 구매하여 네이티브 AWS 서비스에 신속하게 설정하고 통합할 수 있으므로 클릭 몇 번만으로, 몇 분 만에 네트워크 보안을 확보할 수 있습니다.

AWS에서 클라우드 네트워크 보안 간소화

간편한 구축

클라우드 NGFW는 네트워크 보안팀에서 단 몇 분 만에 네트워크 보안을 온전하게 실현하도록 도와줍니다. 담당 팀은 AWS 마켓플레이스를 통해 클라우드 NGFW를 간편하게 구매하여 클릭 몇 번만으로 설정을 마치고 S3, CloudWatch와 Kinesis 등 네이티브 AWS 서비스와 통합할 수 있습니다. 롤스택과 자동 보안 프로필을 설정하는 데 몇 분밖에 걸리지 않습니다(그림 4 참조).

AWS 방화벽 관리자 통합

클라우드 NGFW는 클라우드 네이티브 서비스이므로 AWS 방화벽 관리자와 원활하게 통합됩니다. 따라서 여러 AWS 계정과 VPC 전체에서 일관되게 방화벽 정책을 관리할 수 있습니다. 그뿐만이 아니라, 클라우드 NGFW는 API, CloudFormation 및 Terraform 템플릿을 지원하여 보안을 완전히 자동화하므로 전체 워크플로 자동화를 지원합니다(그림 5).

간편한 구축: 클릭 몇 번만으로, 몇 분 만에 네트워크 보안을 확보합니다.

인프라 관리 불필요: 자동으로 확장성과 회복력을 보장합니다.

폭넓고 심층적인 보안 보장: Palo Alto Networks의 동급 최고 보안 기능을 제공합니다. 업계에서 규모가 가장 큰 보안 플랫폼을 통해 매일 15조 건의 트랜잭션을 분석하고 2,240억 건의 위협을 차단하며 430만 건의 고유한 보안 업데이트를 제공합니다.

네이티브 AWS 환경: 방화벽 관리자, IAM, S3, Cloud Watch, Kinesis 등.

그림 5: 클라우드 NGFW는 실제 보안 난제에 쉽고 빠르게 대처합니다.

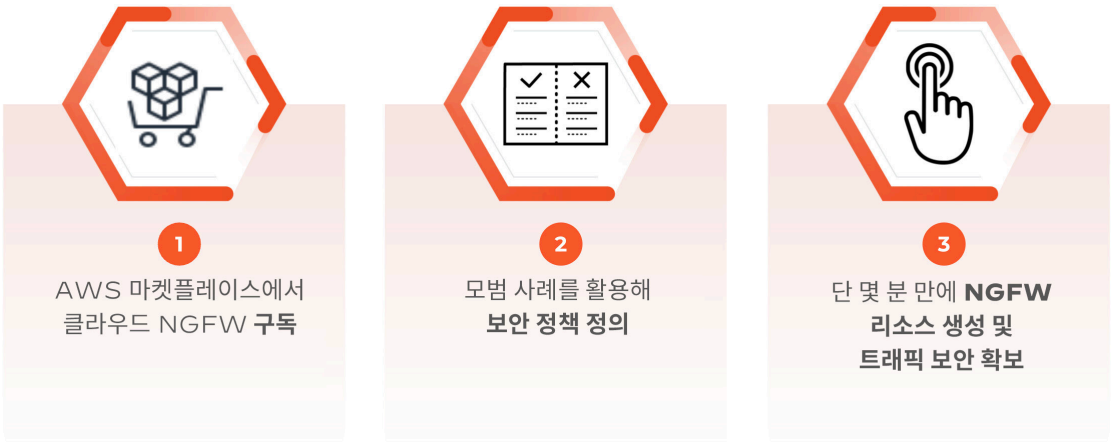

그림 4: 몇 가지 간단한 단계를 거치면 클라우드 NGFW를 구매, 구축 및 관리할 수 있습니다.

인프라 관리 불필요

유지관리 작업을 완전히 해소하여 클라우드 앱에 일관성 있는 동급 최고의 네트워크 보안을 확보하세요. 자동 클라우드 NGFW는 네트워크 트래픽에 맞춰 동적으로 크기가 조정됩니다. 클라우드 NGFW는 완전 관리형 클라우드 서비스이므로 기업에서 인프라를 구축, 업데이트 또는 관리할 걱정을 할 필요가 없습니다. 이 서비스는 AWS Gateway Load Balancer를 활용하여 고가용성, 확장성을 보장하므로 예측하기 어려운 처리량 요구 사항에도 잘 부응합니다.

클라우드 NGFW는 고가용성, 로드 밸런싱과 크기 조정을 기본 내장한 클라우드 네이티브 서비스입니다.

네이티브 AWS 환경

클라우드 NGFW는 네트워크 보안팀이 이미 AWS에서 네트워크 보안을 관리하는 방식과 딱 들어맞습니다. 클라우드 NGFW는 AWS 방화벽 관리자와 함께 사용할 수 있으므로 여러 개의 AWS 계정과 VPC를 통틀어 NGFW 보안 정책을 중앙에서 관리할 수 있습니다.

클라우드 NGFW는 기본적으로 Amazon CloudWatch, S3와 Kinesis 등 AWS 서비스의 로깅과 모니터링을 제공합니다. 따라서 담당 팀은 귀사에서 직접 선택한 네이티브 AWS 로깅 서비스에서 NGFW 활동을 모니터링하여 모든 앱에 동급 최고의 일관된 네트워크 보안을 보장할 수 있습니다(그림 6 참조).

그림 6: 클라우드 NGFW는 보안팀이 AWS를 다루는 기존 업무 처리 방식에 맞춰 고안되었습니다.

동급 최고의 네트워크 보안으로 클라우드 보안 확보

AWS VPC에 실시간 제로데이 차단

클라우드 NGFW는 고급 보안 서비스를 제공하여 클라우드 네트워크 보안을 새로운 차원으로 끌어올립니다. 이 덕분에 끊임없이 모양을 바꾸는 네트워크 기반 위협을 차단하는 데 유리합니다. 클라우드 NGFW는 멀웨어, C2 공격과 취약점 익스플로잇을 자동으로 차단하면서 VPC 및 구축의 내부와 서로 간을 오가는 트래픽을 제어하도록 고안되었습니다. 이러한 보안 태세를 갖추면 기업에서 자사 AWS 구축을 노리는 제로데이 웹 기반 공격을 쉽게 막을 수 있습니다(그림 7 참조).

동급 최고의 NGFW 기능은 업계의 인정은 물론, 엄청난 양의 위협을 관리한 경험에서 비롯된 결과입니다. Gartner는 Palo Alto Networks의 NGFW를 가장 최고의 실행력, 가장 미래지향적인 비전을 갖춘 솔루션으로 지목했으며, 10회 연속 네트워크 방화벽 부문의 리더(Leader)로 선정했습니다.[6]

또한 Palo Alto Networks는 세계 각지에 NGFW와 엔드포인트 보호를 구축한 85,000여 고객을 보유하고 있습니다. Palo Alto Networks의 ML 기반 위협 분석 엔진은 일일 15조 건이 넘는 트랜잭션을 분석하며, Palo Alto Networks Unit 42 리서치 팀 소속의 위협 리서치 연구진 200여 명이 해당 분석을 보강합니다. 위협 연구진은 새롭게 발견된 위협에 좀 더 심층적인 분석을 제공하며, 전체적인 위협 현황에 대한 전문가의 견해도 제시합니다. 그 결과 430만 건의 고유한 보안 업데이트를 출시했으며, 매일 2,240건의 위협을 차단하여 바로 귀사와 같은 고객을 끊임없이 진화하는 최신 위협으로부터 안전하게 보호하고 있습니다.

포트가 아니라 애플리케이션을 기준으로 트래픽 분류

클라우드 NGFW는 레이어 7 전체 검사, 정밀한 제어는 물론 서비스 형태로 제공되는 특허받은 트래픽 분류 기술인 App-ID를 사용해 애플리케이션 레벨에서 Threat Prevention을 제공합니다. App-ID는 포트, 프로토콜, 회피 기법이나 암호화(TLS/SSL)와 관계없이 Amazon VPC를 통과하는 애플리케이션을 식별하여 트래픽을 분류합니다.

포트 및 프로토콜 기반 보안과는 달리, App-ID를 사용하면 세분화된 제어가 가능합니다. 예를 들어 모든 웹 트래픽을 허용하는 것이 아니라, GitHub 업로드를 허용하는 동시에 파일 다운로드를 차단할 수 있습니다. 클라우드 NGFW는 안전하게 애플리케이션을 지원하고 Amazon VPC 보안을 확보하는 데 필요한 지식과 유연성을 제공합니다.

App-ID 서비스는 특허받은 레이어 7 트래픽 분류 기술을 사용해 네트워크상에 존재하는 애플리케이션을 확인하고, 그러한 앱의 작동 원리를 파악하며, 동작 특징을 관찰해 상대적인 리스크를 파악할 수 있도록 합니다. 애플리케이션과 애플리케이션 기능을 애플리케이션 시그니처, 복호화, 프로토콜 디코딩과 추론 등의 여러 가지 기법을 통해 식별합니다. 이러한 기능을 통해 포트 호핑(port hopping)이나 암호화를 이용해 적법한 트래픽으로 가장하고 탐지를 피하려는 앱을 포함하여 네트워크를 통과하는 애플리케이션의 정체를 정확하게 파악할 수 있습니다.

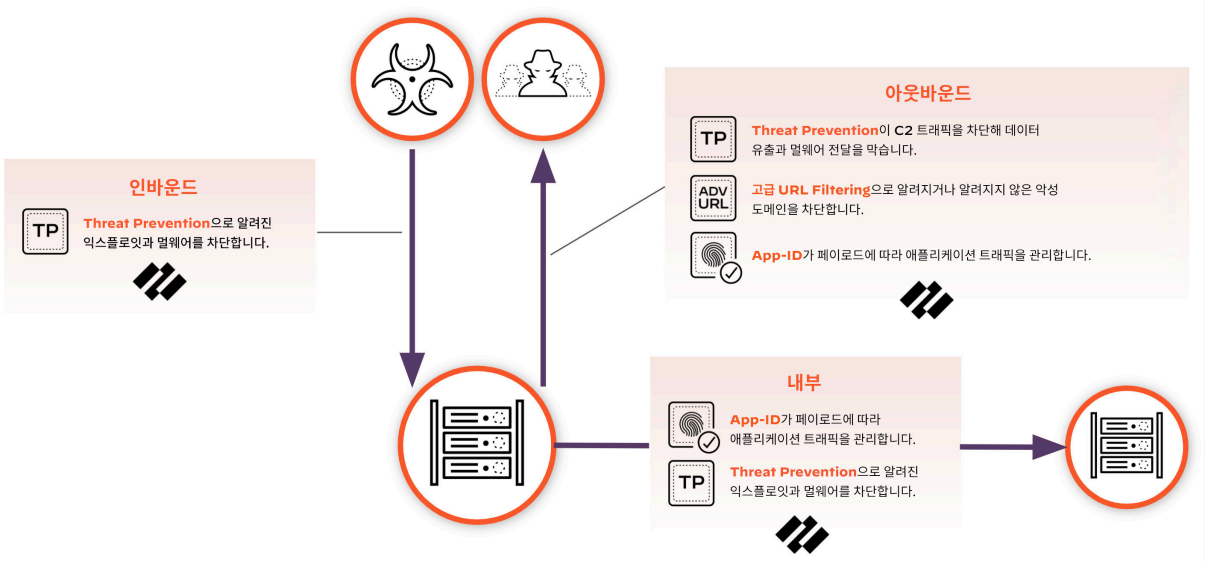

그림 7: 클라우드 NGFW는 제로데이 위협을 막도록 고안된 솔루션입니다.

[6] 2021 Gartner® 네트워크 방화벽 부문 Magic Quadrant™ .

Threat Prevention으로 일반적인 IPS 기술의 한계 넘기

클라우드 NGFW에는 Threat Prevention 서비스가 포함되어 있습니다. 이 서비스는 모든 트래픽(포트, 프로토콜이나 암호화 불문)에 위협이 있는지 검사하여 알려진 취약점, 멀웨어, 익스플로잇, 스파이웨어와 C2 등을 자동으로 차단합니다. 클라우드 NGFW는 시그니처를 자동으로 계속 업데이트하므로 AWS 앱과 데이터를 최신 위협으로부터 안전하게 지켜줍니다.

이처럼 지속적인 업데이트는 여러 겹의 예방 기능을 제공하여 공격의 각 단계에 대응하여 VPC를 보호합니다. Threat Prevention에는 기본적인 IPS(Intrusion Prevention Service) 기능 외에도 고유한 위협 탐지 및 차단 기능이 있어 몇몇 사전정의된 포트를 기준으로 시그니처를 호출하기만 하는 데 그치지 않고 모든 포트를 보호합니다.

고급 URL Filtering을 사용해 실시간으로 웹 기반 위협 차단

클라우드 NGFW는 고급 URL Filtering을 통해 동급 최고의 웹 보호를 제공합니다. 이 중요한 보호 메커니즘은 알려지지 않은 웹 기반 공격을 실시간으로 차단하고, 업계에서 유일한 ML 기반 URL Filtering으로 최초 감염을 방지합니다. 고급 URL Filtering은 Palo Alto Networks의 악성 URL 데이터베이스와 업계 최초의 실시간 웹 보호 엔진을 결합하여 기업에서 악성 위협, 표적화된 웹 기반 위협을 자동으로 탐지하여 차단할 수 있도록 합니다.

사용 사례

클라우드 NGFW를 구축하면 모든 VPC 트래픽을 검사하여 애플리케이션과 워크로드 보안을 확보하며, 그와 동시에 고급 보안 정책을 제공하여 클라우드 구축을 보호합니다(그림 8 참조).

아웃바운드 액세스 방지: 신종 웹 기반 위협과 유출에 맞서 방어합니다.

인바운드 액세스 방지: 인터넷에 공개된 앱과 규제 대상 앱을 웹 및 웹 이외의 위협으로부터 보호합니다.

VPC 간 액세스 보호: 고급 세그먼테이션과 Threat Prevention을 활용해 제로 트러스트를 달성하고 내부망 이동을 차단하며 규정 준수 문제를 해결하세요.

그림 8: 클라우드 NGFW는 AWS 구축 전체에서 트래픽 흐름을 보호하도록 고안되었습니다.

인터넷 아웃바운드

외부 개발자 소스나 인터넷에 액세스하기 위해 아웃바운드 네트워크 액세스가 필요한 클라우드 워크로드의 경우, 최신 웹 기반 공격과 데이터 유출 리스크에 노출되게 됩니다. 규정 준수 요구 사항이 적용되는 규제 대상 앱도 마찬가지입니다. 이런 앱에도 아웃바운드 인터넷 트래픽에 IPS 기능이 필요하기 때문입니다. 고급 URL Filtering은 알려지거나 알려지지 않은 웹 기반 위협을 실시간으로 자동 차단하도록 고안되었으며, 인라인 Threat Prevention이 규정 준수를 위해 IPS 요구 사항에 부합하고 웹 기반 이외의 공격에 맞서 더욱 강력한 방어 기능을 제공합니다(그림 9 참조).

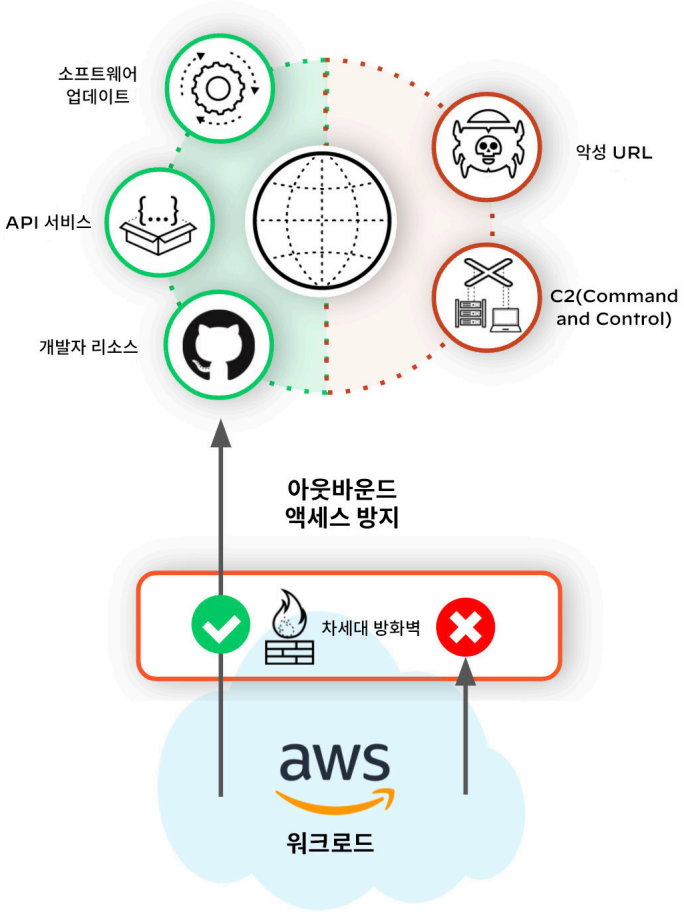

그림 9: 클라우드 NGFW는 AWS 구축 내 아웃바운드 액세스를 보호합니다.

인터넷 인바운드

인터넷에 공개된 앱은 패치되지 않은 취약점을 노출하여 공격자에게는 손쉬운 표적입니다. 그리고 규제 대상 앱의 경우 인터넷에서 유입되는 트래픽에 IPS 기능이 필요합니다. 대부분의 기업은 VPC 경계에 WAF(Web Application Firewall)를 삽입하지만, 이 방화벽은 웹 이외의 트래픽(예: SSH 또는 RDP 등)에 맞서 네트워크를 보호하지는 않습니다.

하지만 클라우드 NGFW는 App-ID와 Threat Prevention을 제공하여 세분화된 애플리케이션 제어를 지원하며, 인터넷에서 유입되는 웹 기반, 웹 이외 기반의 위협에 대응한 자동 보호 기능도 제공합니다. 이와 같은 제어 기능이 있으면 기업에서 규정 준수에 필요한 IPS 요구 사항에 부합하는 데도 도움이 됩니다(그림 10 참조).

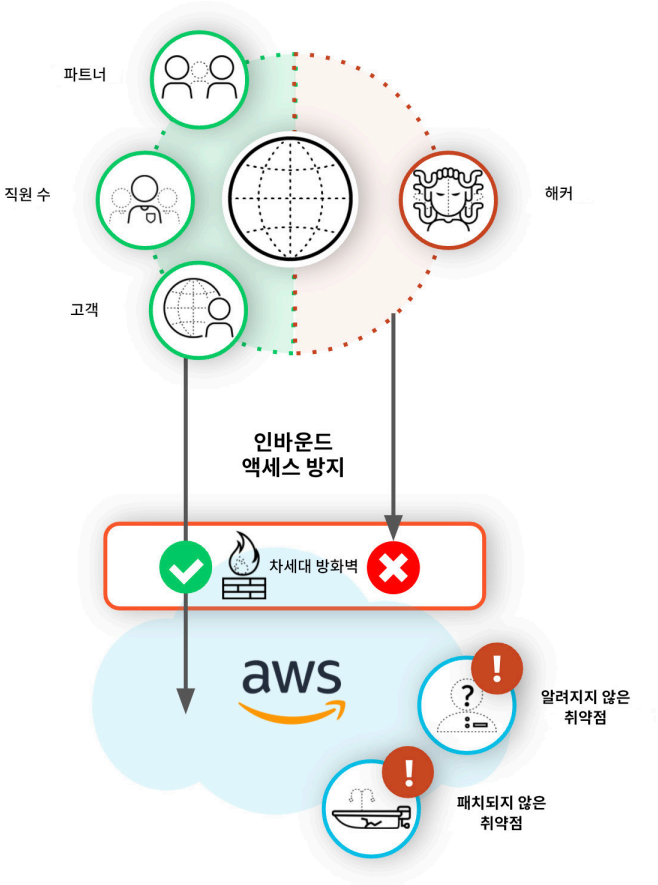

그림 10: 클라우드 NGFW는 AWS 구축 내 인바운드 액세스를 보호합니다.

VPC 간 또는 VPC 서브넷 간

클라우드 침해가 발생하면 단 몇 분 만에 멀웨어가 수천 개의 워크로드에 확산될 수 있습니다. 클라우드 워크로드에는 고급 세그먼테이션과 Threat Prevention을 적용해야 제로 트러스트를 달성하고 내부망 이동을 막으며 규정 준수 요구 사항에 부합할 수 있습니다.

클라우드 NGFW는 네트워크 세그먼트 간에 Threat Prevention과 App-ID 제어를 적용하여 내부망 이동 공격을 막고 제로 트러스트 목표를 달성하도록 도우며 규정 준수 요구 사항에 부합하도록 지원할 수 있습니다(그림 11 참조).

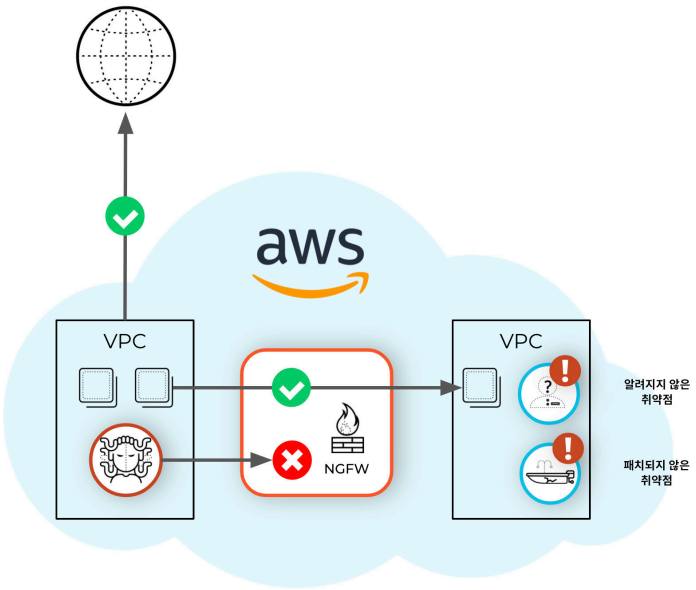

그림 11: 클라우드 NGFW는 VPC 간 트래픽을 보호합니다.

중요한 이유

클라우드 NGFW는 기업이 다음의 네 가지 핵심 부문에서 가장 중요한 목표를 달성할 수 있도록 지원합니다.

동급 최고의 보안 제공

Palo Alto Networks는 10년 연속 Gartner Magic Quadrant® 네트워크 방화벽 부문에서 리더(Leader)로 선정되었습니다. 당사 방화벽과 고급 보안 서비스는 전 세계 85,000여 고객 기업을 보호하고 있습니다.

클라우드 네트워크 보안 운영, 구축, 관리 간소화

클라우드 NGFW 인프라는 Palo Alto Networks에서 관리합니다. 클릭 한 번만으로 클라우드 NGFW를 구축하고, 트래픽 수요에 맞춰 크기가 조정되므로 고객이 자체적으로 NGFW 인프라를 구축하고 유지관리에 대해 걱정하지 않아도 됩니다.

제로 트러스트를 클라우드로 확장

클라우드 NGFW는 제로 트러스트와 일맥상통하므로, 안전한 애플리케이션 액세스를 지원하고 모든 트래픽을 검사하며 최소 권한 액세스 제어를 적용하고 지능형 위협을 탐지 및 차단합니다. 따라서 공격자가 Amazon VPC의 어디에 위치하든 관계없이 중요 자산에 액세스할 경로를 대폭 줄일 수 있습니다.

규정 준수 요구 사항 부합

클라우드 NGFW는 PCI DSS(Payment Card Industry Data Security Standard), 1996년 HIPAA(Health Insurance Portability and Accountability Act), SWIFT CSCF(Customer Security Controls Framework) 등과 같은 규제 기관의 규정 준수 표준에 따라 필요한 Threat Prevention 기능과 세그먼테이션을 제공합니다. 단순하고 종합적인 보고 기능을 통해 감사를 간소화하는 데 필요한 정보를 제공하고 규제 관련 실책을 방지해줍니다.

가용성 및 구매 방법

클라우드 NGFW는 오는 4월부터 미국 서부(캘리포니아 북부) 리전과 미국 동부(버지니아 북부)에서 제공할 예정이며, 유럽과 APAC 지역으로 빠르게 확장할 계획입니다. 구매를 원하시는 경우 AWS 마켓플레이스를 방문하시기 바랍니다.

paloalto NETWORKS

서울시 강남구 테헤란로 518, 10층
(위워크 삼성역 2호점, 섬유센터빌딩)

영업 문의

Tel: 82-2-568-4353 /
Mail: Sales-KR@paloaltonetworks.com

www.paloaltonetworks.co.kr

cloud-ngfw-solution-brief-033022