
Obtaining Best-in-Class Network Security with Cloud Ease of Use

A look at Cloud NGFW for AWS

Industry Context

Cloud is set to become the dominant computing model, and organizations need to find ways to quickly and cost-effectively secure their deployments in these environments. According to Gartner, cloud will be the centerpiece of new digital experiences with 95% of new workloads being deployed in the public cloud.¹ What's more, Palo Alto Networks in its State of Cloud Native Security 2022, found that today, 69% of companies host more than half their workloads in the cloud—a 123% increase from 2020.²

As these workloads shift to the public cloud, they become more interconnected than ever before. A majority of organizations (55%) report a weak security posture and believe they need to improve their underlying activities—such as gaining multi cloud visibility, applying more consistent governance across accounts, or streamlining incident response and investigation—to achieve a stronger posture.⁴ And to compound the issue, 80% of organizations that primarily use open source security tools have weak or very weak security posture.⁵

Accelerated Cloud Adoption Continues...

By 2025, **95%** of new digital workloads will be deployed on cloud-native platforms, up from 30% in 2021

By 2026, public cloud spending will > **45%** of all enterprise IT, up from < 17% in 2021

Source: Gartner Press Release November 2021 and August 2021

...But Risks Abound

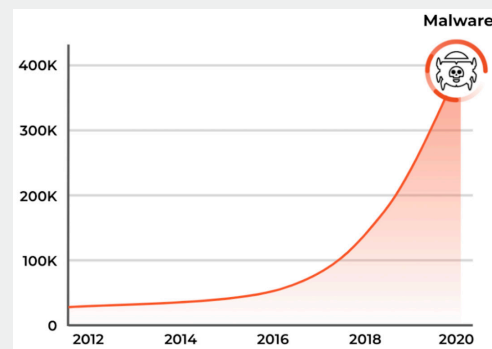


Figure 1: According to Gartner, cloud will be the centerpiece of new digital experiences with 95% of new workloads being deployed in the public cloud.³

¹ Source: Gartner Press Release Nov 2021 and August 2021.

² Source: Palo Alto Networks State of Cloud Native Security 2022.

³ Gartner, op cit.

⁴ Source: Palo Alto Networks State of Cloud Native Security 2022.

⁵ Ibid.

Understanding Network-Based Threats

It is crucial to understand that the network is the common denominator for successful attacks in the cloud. This includes the recent emergence of the infamous Log4j vulnerability and ransomware such as those the REvil hacking group has launched. Other threats, such as Bashlite distributed denial of service (DDOS) attacks and the Graboid cryptojacking worm, which uses Docker hosts to spread and squat on legitimate resources for cryptomining or command-and-control (C2) attacks.

For the vast number of organizations using Amazon Web Services (AWS®)—a leading public cloud platform for hosting applications—understanding who is responsible for securing applications and workloads is the first order of business. AWS takes its responsibility for providing a reliable infrastructure for its customers' business-critical applications very seriously. And by extension, AWS expects its customers to understand they are responsible for protecting their own apps—including their network connectivity—from constantly evolving threats and potential data loss.

Until now, organizations have used third-party firewalls or the built-in, native AWS Network Firewall. Security best practices dictate that your public cloud security posture should mimic your data center security approach: understand your threat exposure through application visibility; use policies to reduce the attack surface area; and then prevent threats and data exfiltration within the allowed traffic.

In cloud environments, that means protecting:

- Internet outbound traffic—workloads that require outbound network access to external developer resources or the internet.
- Internet inbound traffic—internet-facing apps, which may have unpatched vulnerabilities, along with regulated apps that require IPS capabilities.
- VPC-to-VPC (or east-west) traffic—cloud workloads across and within VPCs require advanced segmentation and controls between network segments.

Ultimately, AWS customers need a simple way to apply best-in-class network security to protect their growing public cloud workloads. Their AWS environments require Layer 7 visibility and security to stop modern cyberattacks while minimizing operational overhead for network security and DevOps teams.

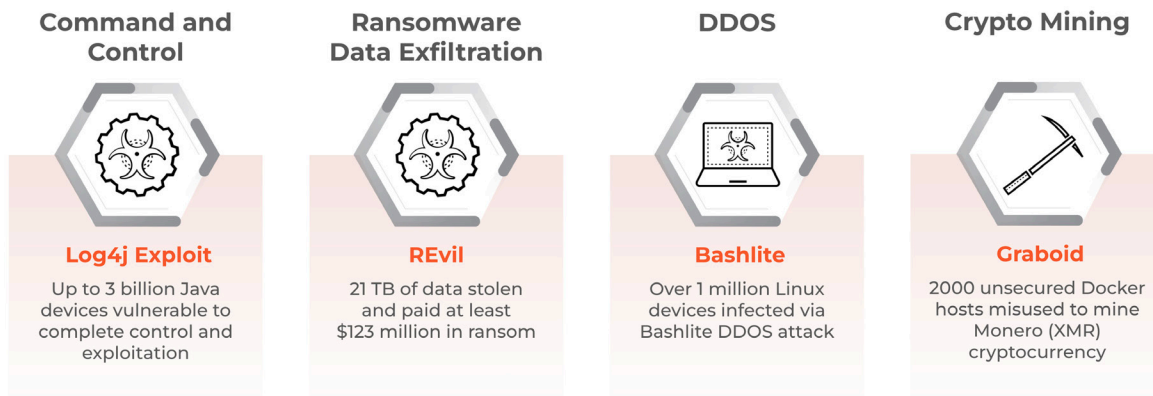


Figure 2: Network-based threats cause business disruption and loss of reputation—and the network is the common denominator for successful attacks in the cloud.

For these teams, any solution implemented should ideally be able to:

- **Prevent network-based threats:** Threats are constantly morphing. Customers want to increase their security capabilities above and beyond basic Layer 4 security and IPS signatures. Network security teams need best-in-class security to stop new threats and reduce risk of breaches.
- **Secure all VPC-to-VPC traffic**—Safeguard cloud workloads in your VPCs with advanced segmentation and threat prevention capabilities.

- **Integrate with the way security and DevOps teams currently work:** Organizations are understandably wary about incurring operational overhead to secure workloads. Many organizations want to consume network security in the same way as they consume cloud services, which are easy to deploy and require no maintenance.
- **Easily extend best-in-class security from on-prem to AWS**—Network security encompasses on-premises environments as well as public cloud environments. Organizations need to be able to centrally manage security, regardless of where they run their applications.

This calls for full network security efficacy coupled with cloud native ease of use for the benefit of network security teams and DevOps organizations alike (see figure 3).

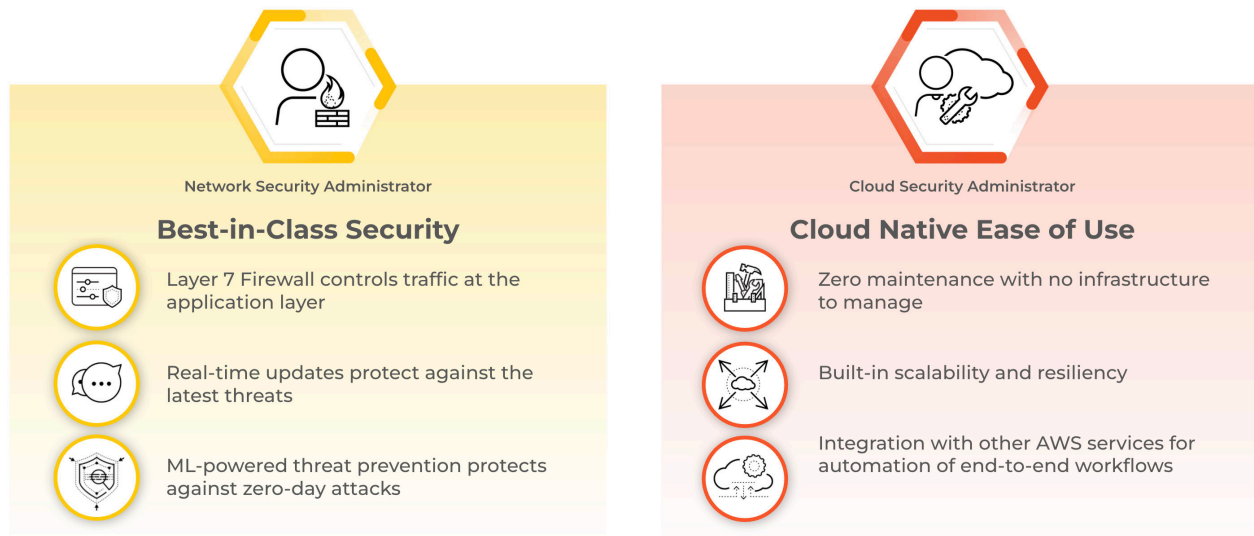


Figure 3: Modern enterprises need both best-in-class security and cloud native ease of use.

Cloud NGFW for AWS Overview

Efficacy paired with ease of use is now here. Cloud NGFW for AWS combines best-in-class network security with cloud ease of use. Delivered as a fully managed cloud native service by Palo Alto Networks and procured in AWS Marketplace, Cloud NGFW for AWS extends cutting-edge threat prevention capabilities to AWS clouds.

Cloud NGFW for AWS delivers these capabilities with deep, inline learning to help stop zero-day web attacks in real time, and block threats aimed at AWS Virtual Private Clouds (VPCs) where organizations place their workloads. Now, network security teams can easily obtain and deploy best-in-class protection across all of their deployments and secure their apps as they connect to legitimate web-based services.

As the first NGFW to integrate with AWS Firewall Manager, the cloud-delivered service lets AWS customers take advantage of automatic scaling and high availability with no maintenance requirements. Cloud NGFW for AWS can be procured in AWS Marketplace, then quickly set up and integrated with native AWS services, enabling network security in minutes with just a few clicks.

Simplify Cloud Network Security in AWS

Easy to Deploy

Cloud NGFW for AWS helps network security teams realize full network security in minutes. They can simply procure Cloud NGFW Marketplace, set it up with a few clicks, and integrate with native AWS services such as S3, CloudWatch, and Kinesis. Setting up rulestacks and automated security profiles only takes a few minutes (see figure 4).



Figure 4: Cloud NGFW for AWS just takes a few simple steps to procure, deploy, and manage.

Centralized NGFW Management From On-prem to AWS

Integration with Palo Alto Networks Panorama™ network security management streamlines network security administration. With Panorama, organizations can centrally manage all of their next-generation firewalls, across all environments. This provides unified visibility into network traffic, threat activity, and blocked activity. It also means organizations can apply consistent policies and employ the same best-in-class security capabilities for all applications, whether they are running on premises or in the cloud.

AWS Firewall Manager Integration

As a cloud-native service, Cloud NGFW for AWS seamlessly integrates with AWS Firewall Manager. This integration enables consistent firewall policy management across multiple AWS accounts and VPCs. What's more, Cloud NGFW for AWS fully automates security, with support for APIs, CloudFormation, and Terraform templates, which enables automation of end-to-end workflows (see figure 5).



Easy to deploy: Network security in minutes with just a few clicks.



No infrastructure to manage: Automatically delivers scalability and resilience.



Security breadth and depth: Best-in-class security capabilities from Palo Alto Networks. Every day, the industry's largest security platform analyzes 15 trillion transactions, blocks 224 billion threats, and provides 4.3 million unique security updates.



Native AWS experience: Firewall Manager, IAM, S3, Cloud Watch, Kinesis, and more.

Figure 5: Cloud NGFW for AWS meets real security challenges quickly and easily.

No Infrastructure to Manage

Make the most of zero maintenance for consistent, best-in-class network security for cloud apps. Automated Cloud NGFW for AWS dynamically scales with network traffic. Because the product is a fully managed cloud service, organizations don't need to worry about deploying, updating, or managing any infrastructure. The service leverages the power of AWS Gateway Load Balancer, providing high availability and scalability to meet unpredictable throughput needs.

Cloud NGFW is a cloud-native service with built-in high availability, load balancing, and scaling.

Native AWS Experience

Cloud NGFW for AWS dovetails with the way network security teams already manage network security on AWS. It works with AWS Firewall Manager, allowing central management of NGFW security policies across multiple AWS accounts and VPCs.

Cloud NGFW for AWS natively provides logging and monitoring with AWS services such as Amazon CloudWatch, S3, and Kinesis. Your team can monitor NGFW activity from native AWS logging services of your choice and deliver consistent, best-in-class network security for all your apps (see figure 6).

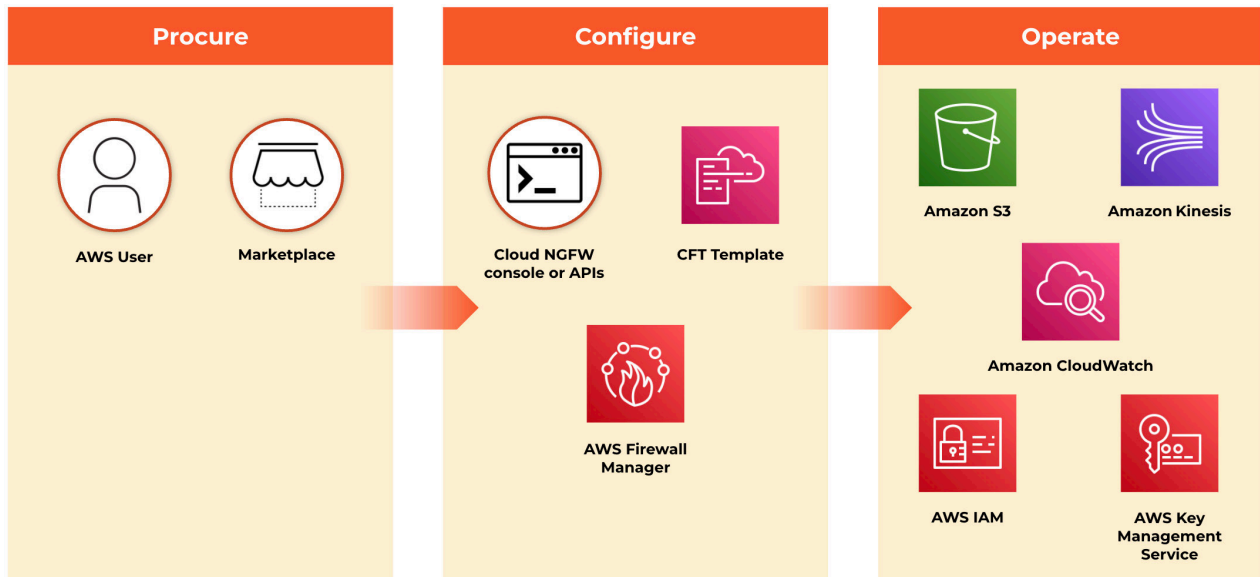


Figure 6: Cloud NGFW has been designed to work with the way security teams work with AWS.

Secure Your Cloud With Best-in-class Network Security

Real-time, Zero-Day Prevention for AWS VPCs

Cloud NGFW for AWS takes cloud network security to a new level by providing advanced security services, which help prevent constantly morphing network-based threats. Cloud NGFW for AWS has been designed to automatically stop malware, command-and-control (C2) attacks, and vulnerability exploits while controlling traffic within and across VPCs and deployments. This security posture helps organizations stop zero-day web attacks in their AWS deployments easily (see figure 7).

Best-in-class NGFW capabilities stem from industry recognition and the sheer volume of threats managed. Gartner lists our NGFWs as highest in execution and furthest in vision—and a Leader in Network Firewalls for the 10th time in a row.⁶

What’s more, Palo Alto Networks has over 85,000 customers who have deployed the company’s NGFWs and end-point protections across the world. Its ML-powered threat analysis engine analyzes over 15 trillion transactions per day—and this analysis is further augmented by the over 200 threat researchers from the Palo Alto Networks Unit 42 research team. These threat researchers provide further in-depth analysis of newly discovered threats, as well as an expert understanding of the overall threat landscape. The result is 4.3 million unique security updates released and 224 billion threats blocked every day to protect customers like you from the ever-evolving latest threats.

Classify Traffic Based on Applications, Not Ports

Cloud NGFW for AWS delivers full Layer 7 inspection, precise control, and threat prevention at the application level with **App-ID**, a patented traffic classification technology delivered as a service. App-ID classifies traffic by identifying the applications traversing your Amazon VPCs irrespective of port, protocol, evasive techniques, or encryption (TLS/SSL).

Unlike port-based and protocol-based security, App-ID allows granular control. For example, instead of allowing all web traffic, you can allow GitHub uploads but block file downloads. Cloud NGFW for AWS provides you with the knowledge and flexibility you need to safely enable applications and secure your Amazon VPCs.

Based on patented Layer 7 traffic classification technology, the App-ID service allows you to see the applications on your network, learn how they work, observe their behavioral characteristics, and understand their relative risk. Applications and application functions are identified via multiple techniques, including application signatures, decryption, protocol decoding, and heuristics. These capabilities determine the exact identity of applications traversing your network, including those attempting to evade detection by masquerading as legitimate traffic by hopping ports or using encryption.

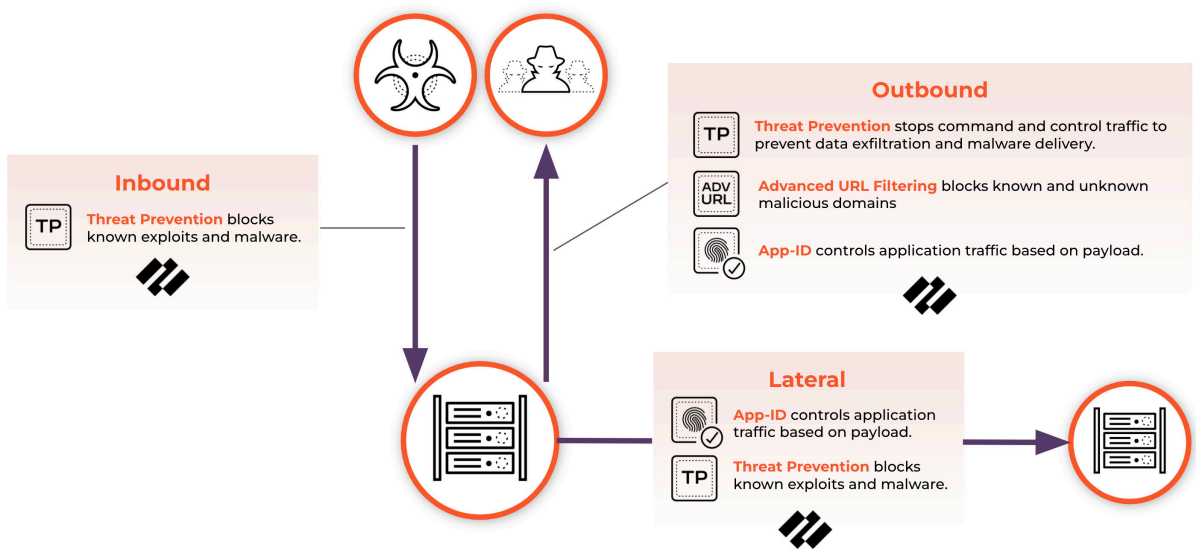


Figure 7: Cloud NGFW for AWS is built to stop zero-day threats.

⁶ 2021 Gartner® Magic Quadrant™ for Network Firewalls.

Go Beyond Typical IPS Technologies With Threat Prevention

Cloud NGFW for AWS comes with the **Threat Prevention** service, which inspects all traffic for threats—regardless of port, protocol, or encryption—and automatically blocks known vulnerabilities, malware, exploits, spyware, and command and control (C2). Cloud NGFW for AWS continuously updates signatures, automatically, ensuring your apps and data on AWS are safe from the latest threats.

These continuous updates protect your VPCs by providing multiple layers of prevention to confront each phase of an attack. In addition to essential intrusion prevention service (IPS) capabilities, Threat Prevention possesses the unique ability to detect and block threats on any and all ports rather than simply invoking signatures based on a limited set of predefined ports.

Prevent Web-based Threats in Real-Time Using Advanced URL Filtering

Cloud NGFW for AWS delivers best-in-class web protection with **Advanced URL Filtering**. This critical protection mechanism stops unknown web-based attacks in real time to prevent patient zero with the industry's only ML-powered URL filtering. Advanced URL Filtering combines the Palo Alto Networks malicious URL database with the industry's first real-time web protection engine so organizations can automatically detect and prevent malicious and targeted web-based threats.

Use Cases

Once deployed, Cloud NGFW for AWS inspects all VPC traffic to secure applications and workloads while providing advanced security policies to protect cloud deployments (see figure 8).




- 
Protect outbound access: Defend against emerging web-based threats and exfiltration.
- 
Protect inbound access: Protect internet-facing and regulated apps from web and non-web threats.
- 
Protect VPC to VPC access: Get advanced segmentation and threat prevention, achieve zero trust, stop lateral movement, address compliance.

Figure 8: Cloud NGFW for AWS has been designed to protect traffic flows throughout AWS deployments.

Internet Outbound

Cloud workloads that require outbound network access to external developer resources or the internet face the risk of emerging web-based attacks and data exfiltration. The same goes for apps regulated by compliance, which require IPS capabilities for outbound internet traffic. Advanced URL Filtering is designed to automatically block known and unknown web-based threats in real time and inline Threat Prevention addresses IPS requirements for compliance and provides stronger defenses against non-web-based attacks (see figure 9).

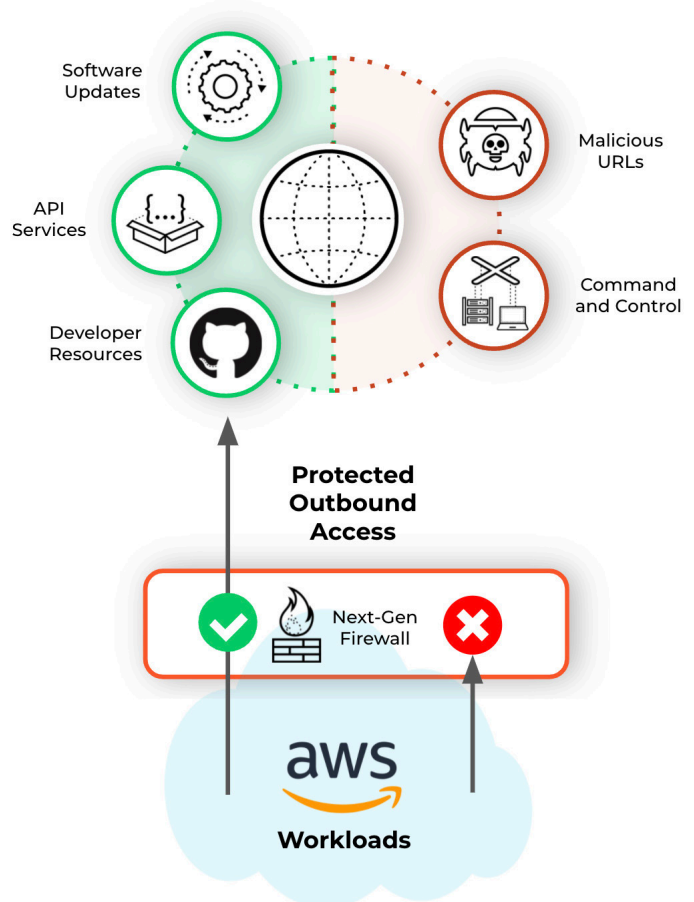


Figure 9: Cloud NGFW for AWS protects outbound access in AWS deployments.

Internet Inbound

Internet-facing apps exposing unpatched vulnerabilities are low-hanging fruit for adversaries and regulated apps require IPS capabilities for traffic from the internet. While most organizations insert Web Application Firewalls (WAF) at the perimeter of their VPCs, it doesn't protect against non-web traffic (e.g., SSH or RDP).

Instead, Cloud NGFW for AWS delivers App-ID and Threat Prevention, which enables fine-grained application controls and automatic protection against web and non-web threats coming from the internet. These controls also help organizations address IPS requirements for compliance (see figure 10).

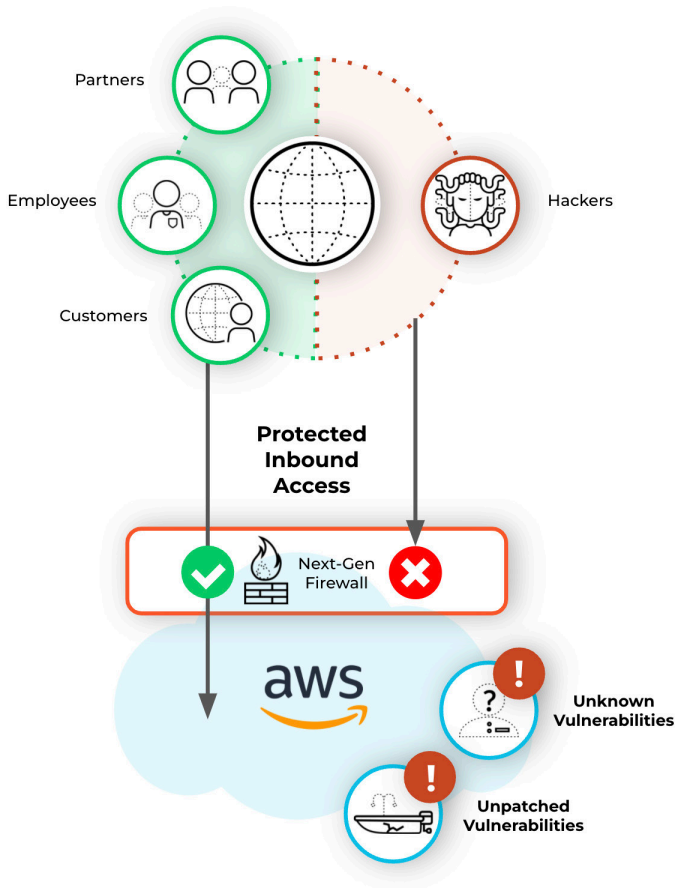


Figure 10: Cloud NGFW for AWS secures inbound access in AWS deployments.

VPC-to-VPC or Between VPC Subnets

In the event of a cloud breach, malware can spread to thousands of workloads in a matter of minutes. Cloud workloads require advanced segmentation and threat prevention to achieve zero trust, stop lateral movement, and address compliance requirements.

Cloud NGFW for AWS can apply Threat Prevention and App-ID controls between network segments in order to prevent lateral movement attacks, help achieve Zero Trust goals, and satisfy compliance requirements (see figure 11).

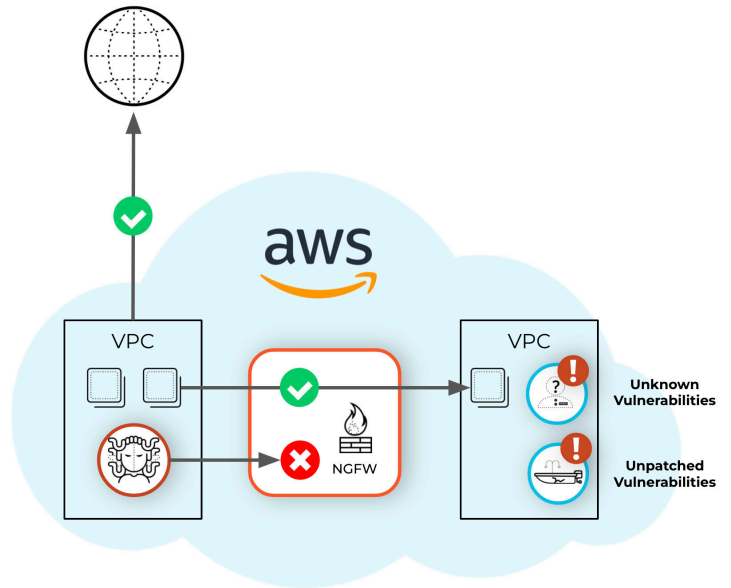


Figure 11: Cloud NGFW for AWS protects VPC-to-VPC traffic.

Why It Matters

Cloud NGFW for AWS helps enterprises achieve their most critical goals across four key areas:

Delivers Best-in-Class Security

Palo Alto Networks has been a Leader in the Gartner Magic Quadrant® for Network Firewalls for ten consecutive years. Our firewalls and advanced security services protect more than 85,000 organizations worldwide.

Simplifies Cloud Network Security Operations, Deployment, Management

Cloud NGFW for AWS infrastructure is managed by Palo Alto Networks. With a single click, Cloud NGFW for AWS is deployed and built to scale based on traffic demands so you don't have to worry about building and maintaining your own NGFW infrastructure.

Extends Zero Trust into the Cloud

Cloud NGFW for AWS directly aligns with Zero Trust, including enabling secure application access, inspecting all traffic, enforcing least-privileged access control, and detecting and preventing advanced threats. This significantly reduces the pathways for adversaries, whether they are inside or outside your Amazon VPCs, to access your critical assets.

Addresses Compliance Requirements

Cloud NGFW for AWS delivers the threat prevention capabilities and segmentation required by regulatory compliance standards, such as The Payment Card Industry Data Security Standard (PCI DSS), The Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the SWIFT Customer Security Controls Framework (CSCF). Simple, comprehensive reporting provides the information necessary to streamline audits and avoid regulatory missteps.

Availability and How to Buy

Cloud NGFW for AWS is available throughout the world. To get started with a free trial, visit [AWS Marketplace](#).



3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2023 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. [cloud-ngfw-solution-brief-072823](#)