Cloud NGFW for AWS

Organizations need a simple way to apply best-in-class network security to protect their growing public cloud workloads. This requires Layer 7 visibility and security to stop modern cyberattacks—while not creating operational burdens for network security and DevOps teams.

Highlights

Cloud NGFW for AWS combines best-in-class network security with cloud ease of use and delivers ML-powered NGFW capabilities as a cloud-native service on AWS. Managed by Palo Alto Networks, it extends cutting-edge security capabilities to AWS clouds to help stop even the most sophisticated threats.

- **Secure AWS VPCs**
  Offers best-in-class network security with patented App-ID, industry-leading Threat Prevention, and ML-powered Advanced URL Filtering.
- **Eliminate operational overhead**
  Delivers NGFW security as a cloud service with single-click deployments, built-in scale and resiliency, and zero maintenance.
- **Extend your AWS experience**
  Consumable in AWS Marketplace; natively integrates NGFW capabilities into AWS Firewall Manager, Amazon CloudWatch, Amazon Kinesis Data Firehose, and other AWS services.

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

- **Prevent network-based threats:** Threats are constantly morphing. Port-based security and IPS signatures are not sufficient to secure AWS workloads. Network security teams and their organizations need best-in-class security to stop new threats and reduce the risk of breaches.
- **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 the same way as they consume cloud services, which are easy to deploy and require no maintenance.

Cloud NGFW delivers these capabilities with inline deep learning to help stop zero-day attacks in real time and blocks threats aimed at workloads hosted in Amazon virtual private clouds (VPCs). Now, network security teams can easily procure and deploy best-in-class protection purpose-built for AWS—and secure their apps as they connect to legitimate web-based services.

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

Once deployed, Cloud NGFW inspects all traffic entering and leaving VPCs to secure applications and workloads with advanced security policies.

Real-time, Zero-Day Prevention for Amazon VPCs

Cloud NGFW takes cloud network security to a new level by providing advanced security services, which help secure applications from constantly morphing network-based threats. Cloud NGFW has been designed to automatically stop malware, command-and-control (C2) attacks, and vulnerability exploits, all while controlling traffic within and across VPCs. This allows organizations to easily stop zero-day web attacks in outbound, inbound, and VPC-to-VPC traffic.

Internet Outbound Traffic

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 1).

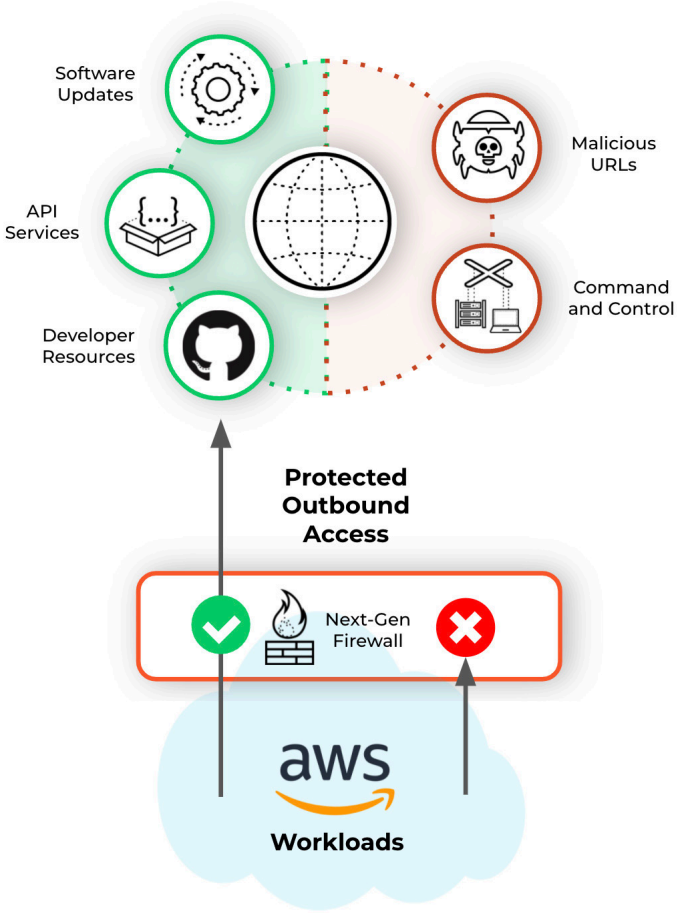

Figure 1: Cloud NGFW protects outbound access in AWS deployments.

Internet Inbound Traffic

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 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 2).

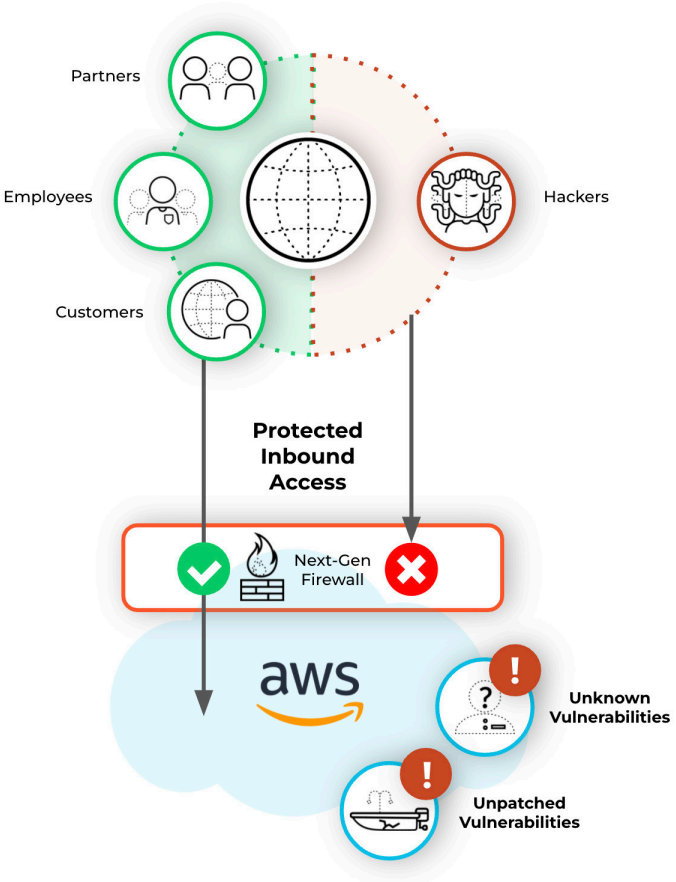

Figure 2: Cloud NGFW secures inbound access in AWS deployments.

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 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 3).

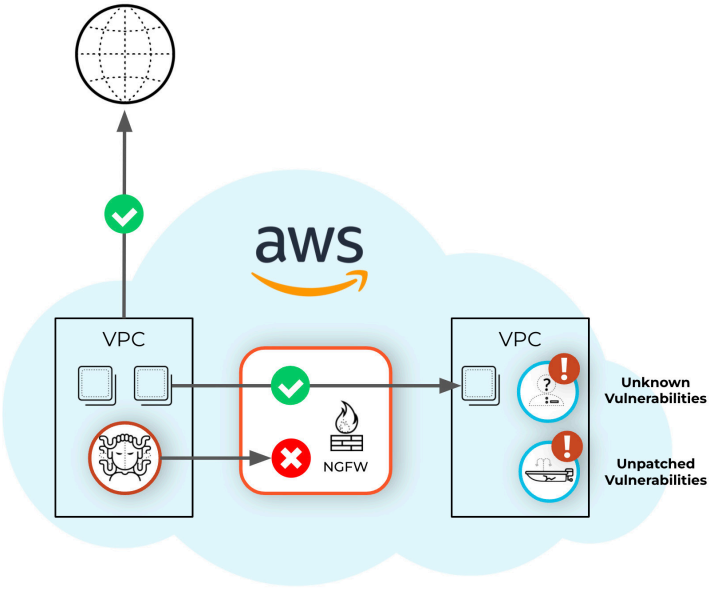

Figure 3: Cloud NGFW protects VPC-to-VPC traffic.

To secure traffic, Cloud NGFW provides Palo Alto Networks protections such as:

App-ID

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. Cloud NGFW identifies applications and application functions 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.

Threat Prevention

The Palo Alto Networks Threat Prevention service protects your network 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.

Advanced URL Filtering

This critical service built into Cloud NGFW stops unknown web-based attacks in real-time to prevent patient zero with the industry's only ML-powered Advanced URL Filtering. Advanced URL Filtering combines the renowned Palo Alto Networks malicious URL database with the industry's first real-time web protection engine so organizations can automatically and instantly detect and prevent new malicious and targeted web-based threats.

Easy AWS Workflow Integration

AWS Firewall Manager Integration

As a cloud-native service, Cloud NGFW has been designed to seamlessly integrate with AWS Firewall Manager. AWS Firewall Manager is a security management service that allows you to centrally configure and manage firewall policies across all of the accounts and applications in your AWS Organization. As you create new applications and AWS accounts, Firewall Manager makes it easy to bring them into compliance by enforcing a common set of security rules. Now you have a single service to build firewall rules, create security policies, and enforce them in a consistent, hierarchical manner across your entire infrastructure, from a central administrator account.

This integration enables simple and consistent firewall policy management across multiple AWS accounts and VPCs. What's more, Cloud NGFW fully automates security, with full support for API, CloudFormation, and Terraform templates, which enables automation of end-to-end workflows.

Simple Procurement and Setup

Realize next-generation network security in minutes. Simply procure Cloud NGFW via AWS Marketplace, set it up with a few clicks, and integrate with native AWS services, including logs being sent natively to Amazon Simple Storage Service (S3), CloudWatch, and Kinesis Firehose. Setting up rulestacks and automated security profiles has been also designed to take only a few minutes.

No Infrastructure to Manage

Make the most of zero maintenance for consistent, best-in-class network security for all your cloud applications. Because Cloud NGFW is a 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 elasticity on demand to meet unpredictable throughput needs. Access as much or as little capacity as you need—and scale up and down as required.

How to Buy and Regional Availability

Procurement

Cloud NGFW is available as a pay-as-you-go service in AWS Marketplace. You pay an hourly rate for each availability zone, your NGFW is deployed in. You also pay for the amount of traffic, billed by the gigabyte, processed by the NGFW.

Regional Availability

Cloud NGFW will be available in US West (N. California) Region and US East (N. Virginia) Region in April. Rapid expansion to both Europe and APAC is planned. To procure, please visit AWS Marketplace.

Support

Palo Alto Networks Cloud NGFW support services make it simple and easy to set up and onboard. Comprehensive digital services, technical support, and education services underscore our commitment to the ongoing success of your Palo Alto Networks deployment.

Two Cloud NGFW Customer Support Services options help provide the maximum uptime and streamline resolving issues:

- **Standard**
  Cloud NGFW Standard Support provides self-service, digital support capabilities to assist you. Access to all the product documentation and knowledge base articles aids in answering questions. LIVEcommunity moderated by Palo Alto Networks experts provide our online community with collective expertise from thousands of users.
- **Premium**
  Premium Support proactive monitoring gives you the extra assurance that your service is always up and running. Customers can access assistance through LIVEcommunity and our Customer Support Portal. Callback phone support from technical experts 24/7 assists with any questions or issues you encounter. The Premium Support software subscription can be added on through the Cloud NGFW management console.

Get more from your Cloud NGFW implementation through our Cloud NGFW Customer Support Services, including:

- In-product "Get Help" lets you quickly find answers within the product.
- Deep knowledge of the AWS platform quickens our support engineers' ability to provide fast solutions.
- Operational metrics, proactive monitoring, and notifications enable management and operating capabilities.
- Digital learning provides anytime online access to Cloud NGFW courses, which help build your product and technology knowledge, skills, and confidence.
- Micro-credentialing validates and demonstrates your product and technology knowledge and expertise gained from completing the required courses.

Using a budget-friendly, pay-as-you-go (PAYG) subscription model, Cloud NGFW support services are designed to deliver smooth, secure, and scalable cloud-based network firewall cybersecurity.

Visit the Customer Support Portal to learn more.

paloalto NETWORKS

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

© 2022 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-datasheet-042022