Cloud NGFW for AWS

Organizations need a straightforward solution to implement cutting-edge network security for their expanding public cloud workloads. This includes robust Layer 7 visibility to analyze application behavior and advanced security to mitigate modern cyberattacks, all while minimizing operational complexity for network security, cloud security, and DevOps teams.

Key Benefits of Cloud NGFW for AWS

Cloud NGFW for AWS combines industry-leading network security with the simplicity and scalability of a fully cloud-native service on AWS. Built by Palo Alto Networks, this AI-powered solution defends against sophisticated cyberthreats, while delivering unparalleled reliability and flexibility. With Cloud NGFW for AWS, organizations can:

- **Extend best-in-class security from on-premises to AWS:** Seamlessly integrate with Panorama® and Palo Alto Networks Strata® Cloud Manager to unify policy management and gain centralized visibility across all environments.
- **Secure AWS VPCs:** Protect workloads with patented App-ID™ for precise application identification, Palo Alto Networks Advanced Threat Prevention for real-time security, and ML-powered Advanced URL Filtering to block unknown threats instantly.
- **Streamline operations with zero maintenance:** Experience the benefits of a fully managed NGFW service that includes automated scaling, resilience, and simplified deployment—eliminating the need for manual updates or infrastructure management.
- **Enhance the AWS experience:** Access Cloud NGFW for AWS through AWS Marketplace, which now offers deep integration with AWS Firewall Manager, Amazon CloudWatch, and Kinesis Data Firehose. Additionally, AWS PrivateLink integration ensures secure connectivity to NGFW instances without traversing the public internet. New flexible credit management ensures dynamic resource allocation and efficient scaling across regions.

Why Cloud NGFW for AWS

As cloud adoption accelerates, organizations face increasing challenges in securing workloads at scale. Traditional security solutions often lack the agility, visibility, and advanced protections needed for dynamic AWS environments. Built for cloud-native workflows, Cloud NGFW for AWS directly addresses these challenges by offering:

- **Proactive threat prevention:** Stop evolving threats in real time with AI-powered protections from zero-day exploits, malware, and command-and-control (C2) attacks. Replace port-based security and outdated intrusion prevention system (IPS) signatures with advanced detection and prevention capabilities.
- **Comprehensive cloud security:** Provide full visibility into cloud traffic with Layer 7 classification, ensuring granular application, user, and workload awareness. Protect all traffic types, including outbound, inbound, and virtual private cloud (VPC)-to-VPC, with advanced segmentation and dynamic policies.
- **Seamless AWS integration:** Ensure operational consistency and simplicity for network security, cloud security, and DevOps teams, with effortless integration into existing AWS services like AWS Firewall Manager, Amazon CloudWatch, and AWS PrivateLink.
- **Zero maintenance, full scalability:** Eliminate operational overhead with a fully managed service that offers automated scaling, high availability, and centralized management so that security teams can focus on strategic priorities rather than routine maintenance.
- **Flexible credit management:** Adapt quickly to changing needs with a dynamic credit allocation system that ensures cost efficiency and scalability across regions.

Cloud NGFW for AWS empowers network security, cloud security, and DevOps teams to secure their environments without complexity, delivering best-in-class security purpose-built for AWS workloads. By integrating cutting-edge technologies like App-ID, Advanced Threat Prevention, and AI-driven insights, organizations can protect their cloud applications with confidence.

Real-Time, Zero-Day Protection for Amazon VPCs

Cloud NGFW for AWS redefines cloud network security by using advanced, AI-powered services to protect applications from rapidly evolving cloud-based and network-based threats. It automatically detects and blocks malware, C2 traffic, and vulnerability exploits while managing traffic within and across VPCs. Organizations can confidently stop zero-day attacks across outbound, inbound, and VPC-to-VPC traffic.

Internet Outbound Traffic

Cloud workloads often require access to external resources or the internet:

- **Challenges:** Outbound traffic exposes workloads to data exfiltration, malicious websites, phishing attempts, and non-web-based attacks such as file transfers or encrypted traffic.
- **Solution:** Cloud NGFW for AWS combines ML-powered Advanced URL Filtering with inline Threat Prevention to provide robust protection. Real-time filtering blocks malicious web content and phishing domains, while Threat Prevention secures workloads against encrypted attacks, ransomware, and other sophisticated risks. Enhanced outbound traffic controls now allow for dynamic profiling and improved compliance with organizational security policies.

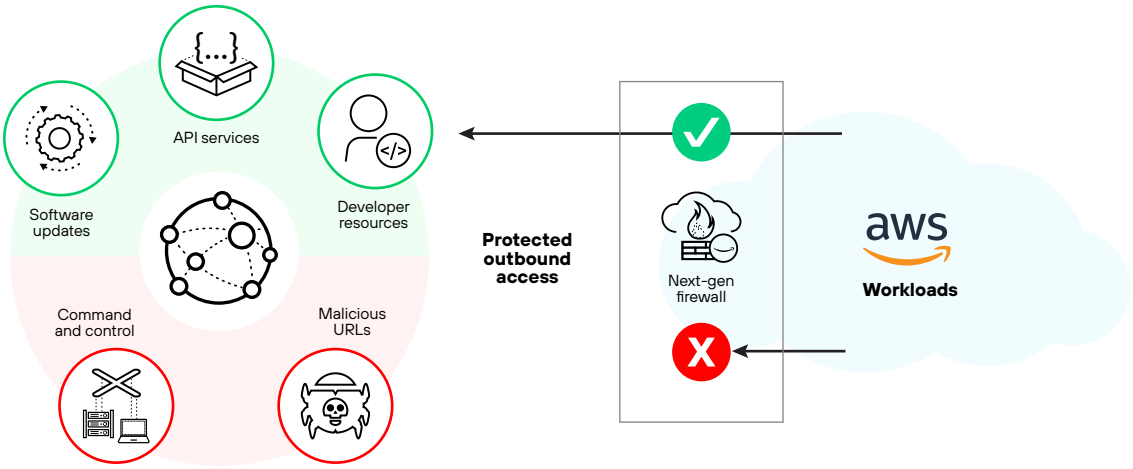

Figure 1. Cloud NGFW for AWS protects outbound access in AWS deployments

Internet Inbound Traffic

Applications exposed to the internet face constant threats, especially from unpatched vulnerabilities and sophisticated attack vectors that target application-layer weaknesses:

- **Challenges:** Adversaries exploit vulnerabilities in web-facing apps using techniques like remote code execution, SQL injection, or bypassing traditional web application firewalls (WAFs). Additionally, non-web-based services like SSH or RDP face significant risk.
- **Solution:** Cloud NGFW for AWS integrates patented App-ID and Threat Prevention technologies to block both web- and non-web-based attacks with granular, application-layer controls. By automating defenses against inbound attacks, it reduces risks while meeting compliance standards for regulated traffic.

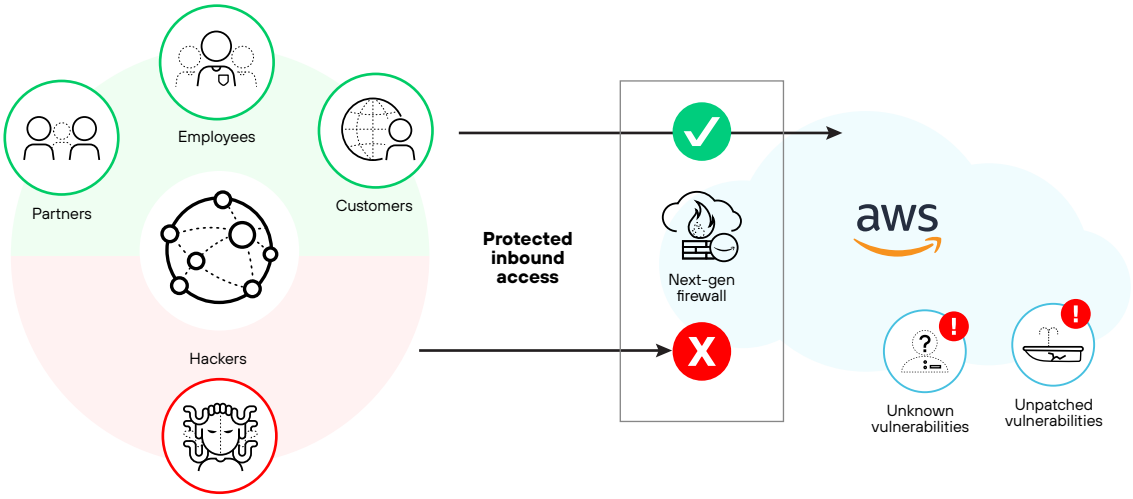

Figure 2. Cloud NGFW for AWS secures inbound access in AWS deployments

VPC-to-VPC or Between VPC Subnets

Intracloud traffic between VPCs or subnets presents a significant attack surface, especially if malware propagates laterally in a breach scenario:

- **Challenges:** Without proper segmentation, malicious actors can move laterally across workloads, exploiting trust relationships between applications.
- **Solution:** To prevent lateral movement and achieve Zero Trust, Cloud NGFW for AWS applies advanced segmentation, Threat Prevention, and App-ID controls between VPC subnets. This prevents unauthorized communication, protects sensitive workloads, and supports compliance goals, ensuring a hardened AWS security posture.

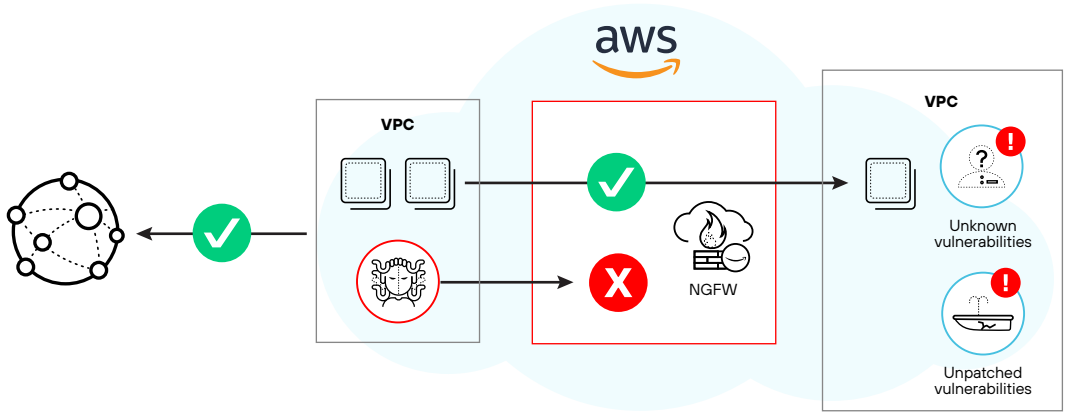

Figure 3. Cloud NGFW for AWS protects VPC-to-VPC traffic

Advanced Threat Prevention Powered by Precision AI

Cloud NGFW for AWS delivers Advanced Threat Prevention with the power of Precision AI®, setting a new standard in defending against modern cyberthreats. This innovative approach enables dynamic, real-time protection that's tailored to an organization's workloads, ensuring security teams stay ahead of evolving attack vectors:

- **Proactive Threat Prevention:** Detects and stops sophisticated threats with proactive threat identification powered by Precision AI. Cloud NGFW takes on zero-day exploits, ransomware, and malware in real time. Its AI engine analyzes vast amounts of network traffic data to identify malicious activity instantly, minimizing false positives and maximizing accuracy.

- **Inline zero-day prevention:** Stops unknown threats before they can impact workloads by leveraging machine learning-based detection. Unlike legacy intrusion prevention systems, this solution continuously adapts to emerging threats with behavioral analytics and real-time updates, ensuring robust defense.
- **AI-driven App-ID:** Provides granular visibility and control with AI-powered Layer 7 traffic classification, allowing security teams to precisely identify applications, users, and workloads. This capability reduces the attack surface and enables enforcement of highly targeted security policies. By intelligently classifying traffic, App-ID enhances real-time threat prevention and strengthens the security posture across AWS workloads.
- **Advanced URL Filtering:** Protects against web-based threats with AI-powered URL filtering that blocks malicious and unknown URLs in real time. By using deep learning models, Cloud NGFW proactively mitigates phishing attacks, ransomware delivery, and other web-based risks.
- **Behavioral threat analytics:** Identifies abnormal traffic patterns and behaviors to enhance an organization's security posture, providing early detection of threats such as lateral movement or C2 communication. Precision AI continuously analyzes network activity to detect anomalies in real time, enabling proactive threat response and reducing security risks.
- **Seamless integration with threat intelligence:** Continuously incorporates insights from the industry's largest threat intelligence database, ensuring real-time updates and preemptive defense against the latest attack techniques. Cloud NGFW leverages global threat intelligence to proactively detect and mitigate emerging threats, reducing risk and enhancing security posture.

By delivering Advanced Threat Prevention powered by Precision AI, Cloud NGFW for AWS empowers organizations to protect their workloads with unprecedented accuracy, speed, and effectiveness. This level of precision ensures threats are mitigated before they disrupt business operations, enabling teams to focus on growth while maintaining robust security.

Rapid AWS Workflow Integration

Cloud NGFW for AWS integrates seamlessly with existing AWS workflows, enabling centralized management, consistent policy enforcement, and operational simplicity for network security, cloud security, and DevOps teams.

AWS Firewall Manager Integration

As one of the first next-generation firewalls to integrate with AWS Firewall Manager, Cloud NGFW simplifies security policy enforcement across AWS organizations:

- **Ensures consistent compliance** with centralized policy management. Configures and applies firewall rules across multiple accounts and resources within the AWS environment.
- **Reduces administrative overhead** with automatic policy enforcement. AWS Firewall Manager automatically applies security rules to new AWS accounts, workloads, or applications, eliminating configuration drift.
- **Streamlines multiaccount protection** and simplifies security across AWS accounts by enforcing uniform policies, providing centralized control and holistic visibility into resource activities.

Centralized NGFW Management with Panorama and Strata Cloud Manager

Cloud NGFW for AWS integrates seamlessly with Panorama and Strata Cloud Manager, enabling security teams to unify management across hybrid, multicloud, and on-premises environments:

- Improves the security posture by monitoring and managing traffic, threats, and policies from a single interface.
- Extends existing workflows seamlessly by enabling Panorama users to integrate Cloud NGFW for AWS without additional training or configuration.
- Maintains consistency across environments by enforcing uniform security policies across on-premises, cloud, and hybrid deployments.

AWS Service Integrations

Cloud NGFW for AWS works natively with key AWS services to streamline operations and enhance efficiency through seamless integrations, including:

- **AWS PrivateLink:** Ensures data privacy and eliminates unnecessary risk. Securely connects to Cloud NGFW instances without exposing traffic to the public internet.
- **Amazon CloudWatch and Kinesis Data Firehose:** Proactively detects and responds to threats. Uses real-time monitoring and logging integrations to enhance threat detection and incident response.
- **AWS Gateway Load Balancer (GWLB):** Achieves high availability and elastic scaling. Seamlessly distributes traffic to meet fluctuating throughput demands without manual intervention.

Zero Infrastructure Overhead

Cloud NGFW for AWS doesn't have any internal infrastructure to manage so organizations can focus on securing their applications without the operational burden of maintaining hardware or software:

- **Fully managed service:** Palo Alto Networks handles all aspects of the firewall's infrastructure, from deployment to scaling, updates, and maintenance. This frees network security, cloud security, and DevOps teams to focus on strategic initiatives instead of routine management.
- **Elastic scaling for unpredictable workloads:** Cloud NGFW automatically scales up or down to meet workload demands, ensuring high performance and cost-efficiency during peak traffic or low-utilization periods.
- **High availability:** Built on the AWS resilient architecture, the service uses AWS Gateway Load Balancer (GWLB) to ensure failover, redundancy, and continuous availability, maintaining a 99.99% uptime SLA.[1]
- **Seamless performance optimization:** Cloud NGFW automatically adapts to network changes without manual intervention, ensuring consistent security and operational efficiency across all AWS regions.

Flexible Procurement Options

Cloud NGFW for AWS offers multiple procurement models to meet diverse organizational needs, ensuring seamless deployment and cost-effective scalability:

- **Free Trial:** Get started with a free trial of Cloud NGFW for AWS, allowing organizations to explore security capabilities before committing to a paid subscription.

1. "Support Policies and SLAs," Palo Alto Networks, April 2022.

- **PAYG Pricing:** Choose a budget-friendly subscription model with pay-as-you-go (PAYG) billing via AWS Marketplace. Organizations are charged hourly per availability zone and based on traffic processed (billed per GB), ensuring cost efficiency and flexibility.
- **Private Offers:** For long-term or large-scale deployments, Palo Alto Networks provides customized Private Offers via AWS Marketplace. These tailored pricing and deployment options help enterprises meet specific security and budgetary requirements.
- **Flexible Credit Management & Consumable Credits:** Leverage credit fungibility to dynamically allocate resources across AWS regions. This flexible model supports cost optimization, scales security consumption based on business needs, and eliminates inefficiencies.
- **Scalable Services:** Support scales with the organization's needs, whether managing a single AWS workload or deploying across multiple regions.

Regional Availability

Cloud NGFW for AWS is accessible in most AWS commercial regions globally, ensuring consistent security regardless of an organization's workload location:

- **Global coverage:** The service is available in a wide range of AWS regions, enabling organizations to protect their applications and data in compliance with local and international regulations.
- **Expanding footprint:** Palo Alto Networks continues to extend availability into new AWS regions to support growing customer needs. For the most up-to-date list of supported regions, refer to the Cloud NGFW Supported Regions & Zones page.

Support and Education

Palo Alto Networks provides robust support and educational resources to ensure Cloud NGFW for AWS customers can maximize the value of their investment. From onboarding to troubleshooting, our services are designed to deliver a smooth, secure, and scalable experience.

Premium Support Services

Ensure seamless deployment and continuous protection with 24/7 expert support and proactive monitoring:

- **LIVEcommunity access:** Tap into a vibrant customer community and knowledge base for quick answers to common questions.
- **Customer Support Portal:** Access technical documentation, troubleshooting guides, and ticketing services for personalized assistance.
- **Proactive monitoring:** Get real-time monitoring of your organization's Cloud NGFW instance to ensure optimal performance and uptime.
- **Callback support:** Receive callback assistance from Palo Alto Networks technical experts anytime, day or night, to address critical issues.

In-Product Help

Simplify troubleshooting and operations with built-in help features:

- **Get help within the product:** Quickly find solutions to common issues directly within the Cloud NGFW interface, reducing downtime and the need for external searches.
- **AWS expertise:** Speak with support engineers who have a deep knowledge of the AWS platform and ensure fast, accurate solutions tailored to cloud-native environments.

Education and Training

Empower teams with the knowledge and skills needed to secure AWS environments effectively:

- **Build expertise with on-demand training:** Access digital learning modules to gain proficiency in using Cloud NGFW for AWS, including configuration, management, and threat analysis.
- **Validate skills with industry-recognized certifications:** Achieve microcredentials that demonstrate expertise in securing AWS environments using Palo Alto Networks technologies.
- **Enhance operational efficiency with proactive insights:** Leverage operational metrics and notifications to monitor firewall performance and security trends, optimizing team workflows.

Start with No Obligation. Take the Next Step.

Experience Cloud NGFW for AWS today with zero commitment and discover how it can enhance your cloud security.

Get started with a free trial and explore how Cloud NGFW simplifies security for your AWS workloads.

About Amazon Web Services

Since 2006, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud. AWS has been continually expanding its services to support virtually any workload, and it now has more than 240 fully featured services for compute, storage, databases, networking, analytics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, media, and application development, deployment, and management from 114 Availability Zones within 36 geographic regions, with announced plans for 12 more Availability Zones and four more AWS Regions in New Zealand, the Kingdom of Saudi Arabia, Taiwan, and the AWS European Sovereign Cloud. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—trust AWS to power their infrastructure, become more agile, and lower costs. To learn more about AWS, visit aws.amazon.com.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, empowers businesses to embrace digital transformation with industry-leading, AI-powered solutions for network and cloud security, and security operations. Powered by Precision AI®, our technologies deliver precise threat detection and swift response, minimize false positives, reduce complexity and improve security outcomes. Our platformization approach integrates today's security solutions into a unified, scalable platform, streamlining management and providing operational efficiencies with comprehensive protection. For more information, visit www.paloaltonetworks.com.

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

strata_ds_cloud-ngfw-for-aws_032425