Cloud NGFW: Best-in-Class Security, Unparalleled Simplicity on AWS

Keep your cybersecurity one step ahead with an ML-powered NGFW managed by Palo Alto Networks and delivered as a cloud-native service on AWS

paloalto NETWORKS | aws

Table of contents

Rising cloud adoption gives way to modern cybersecurity

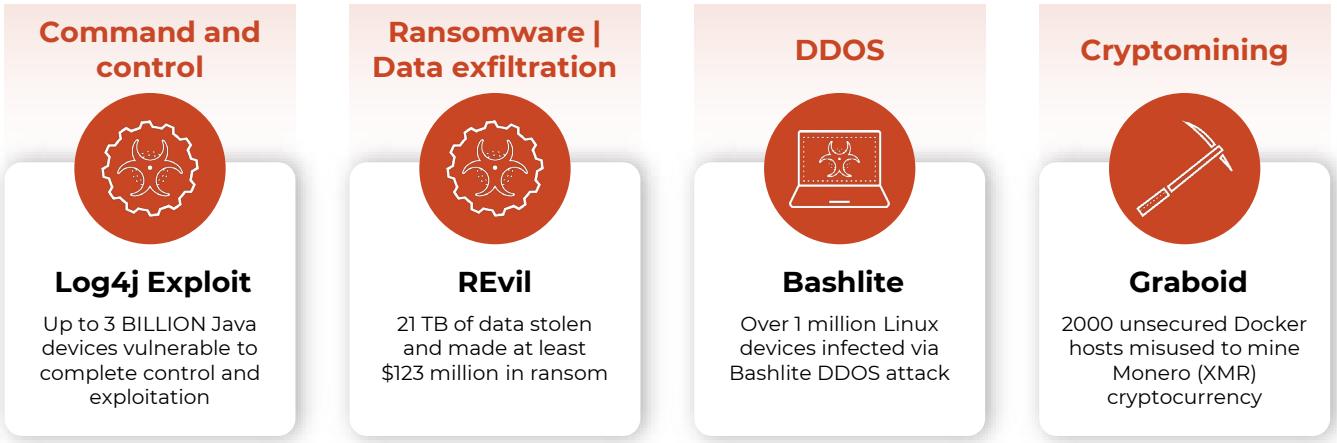
Public cloud adoption has soared in recent years. And throughout the pandemic, organizations expanded their cloud footprint even more. Today, 69% of companies host more than half their workloads in the cloud—a 123% increase from 2020.

But with great cloud power, comes great security responsibility. Public clouds like Amazon Web Services (AWS) enable organizations to gain agility, cut costs, and reduce infrastructure management. Security is accomplished through the Shared Responsibility Model, where AWS protects the cloud infrastructure and customers secure their data. By working with a security partner like Palo Alto Networks, organizations can stay focused on running their business and gain advanced protection. The Shared Responsibility Model is crucial for organizations to stay one step ahead of cybercriminals and be ready for what comes next.

The good news is effective security is here. Next-generation firewalls (NGFWs) are the cornerstone of modern network security, protecting against threats seeking to infiltrate inbound, outbound, and east-west traffic, spanning physical, virtualized, and containerized environments.

Security teams need network protection and cloud simplicity

However, deploying in the cloud is not without risk as the threat landscape also continues to grow exponentially. This includes the recent emergence of the infamous Log4j vulnerability along with ransomware, distributed denial of service (DDOS) attacks and cryptojacking worms.

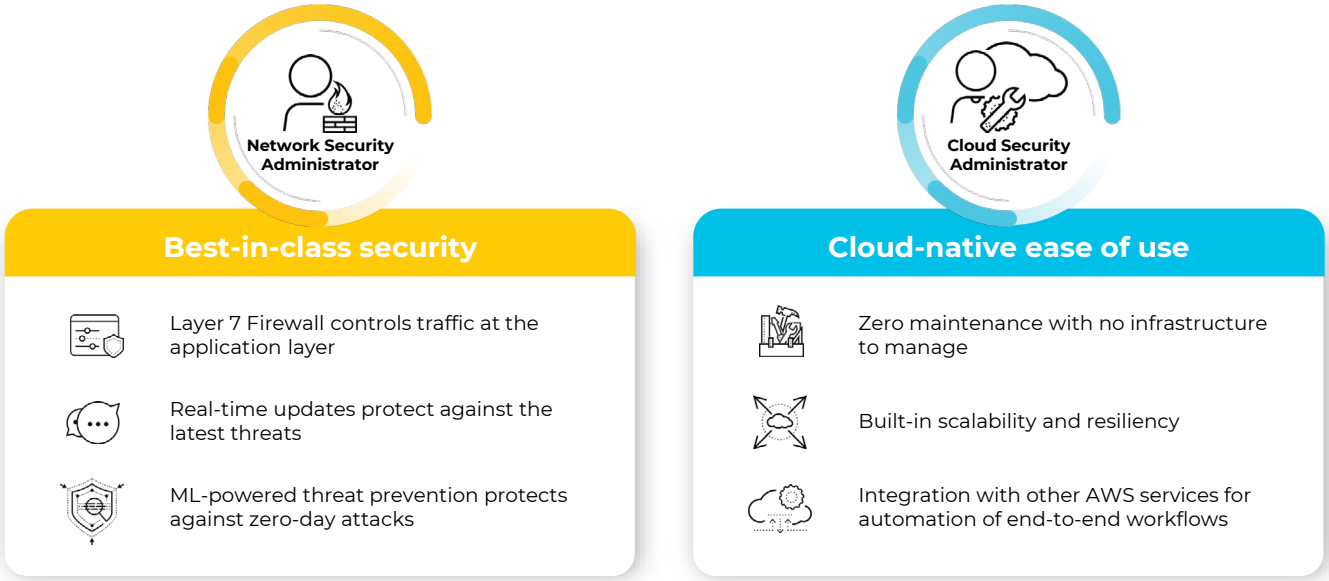


These network-based threats can cause business disruption and loss of reputation. Ultimately, AWS customers need a simple way to apply best-in-class network security to protect their growing public cloud workloads. Their environments require Layer 7 visibility and security to stop modern cyberattacks, while minimizing operational overhead for network security and DevOps teams. Today's security teams want to know: How can they have the best of both worlds—NGFW protection and the ease of use of the cloud?

Introducing Cloud NGFW from Palo Alto Networks

Cloud NGFW is the first NGFW integrated with AWS Firewall Manager. Managed by Palo Alto Networks, Cloud NGFW delivers industry-leading protections with unparalleled simplicity designed to help stop even the most sophisticated threats in real time. It works like any other native AWS service, but is totally unique in letting AWS customers easily secure their workloads with the best-in-class protections that Palo Alto Networks is known for.

Experience the best of both worlds with natively integrated network security delivered as a service on AWS.



Modern enterprises need *both* best-in-class security + cloud-native ease of use

Protect your AWS experience with cloud-native network security

With Cloud NGFW, you'll get ML-powered network protection for your Amazon Virtual Private Clouds (VPCs). Protections like Palo Alto Networks App-ID, Threat Prevention, and Advanced URL Filtering are designed to stop known and zero-day threats.

App-ID: Reduce the risk of attacks by controlling traffic based on Palo Alto Networks' patented Layer 7 traffic classification technology. App-ID identifies applications traversing your network by applying multiple classifications to your network traffic stream. It determines what an application is, regardless of port, protocol, encryption (SSH or SSL) or any other evasive tactic. Once the application has been identified, App-ID uses a policy check to decide whether to block, scan, inspect, or shape it.

Threat prevention: Automatically stop known malware, vulnerability exploits, and command and control infrastructure (C2) hacking with industry-leading threat prevention. Daily threat intelligence is automatically curated, delivered to the Cloud NGFW, and implemented to stop all threats. Powerful intrusion prevention system (IPS) capabilities, including single pass architecture and policy management provide full threat detection and prevention without sacrificing performance.

Advanced URL Filtering: Stop unknown web-based attacks in real time to prevent patient zero. Advanced URL Filtering analyzes web traffic, categorizes URLs, and blocks malicious threats in seconds. Multi-category and custom category support enable additional layers of protection, such as targeted SSL decryption and advanced logging. Alongside its own analysis, Advanced URL Filtering uses shared threat information from WildFire® malware prevention service and other sources to automatically update protections against malicious sites.

Simplify management and easily scale on AWS

Cloud NGFW integrates security into the way you work with AWS. It cuts down complexity that allows your team to easily safeguard data, applications, and workloads with cloud agility.

Simplified management and automation capabilities: Use AWS Firewall Manager for larger deployments and gain consistent firewall policy management across multiple AWS accounts and Amazon VPCs. Cloud NGFW natively integrates with AWS Firewall Manager so you can simplify your cloud network security. Easily secure your automated workflows and take advantage of load balancing and auto-loading capabilities from AWS to scale.

What's more, Cloud NGFW meets unpredictable throughput needs by leveraging the power of AWS Gateway Load Balancer (GWLB), which provides on-demand high availability and elastic scaling.

Zero maintenance: Eliminate infrastructure management with a resilient cloud service that scales dynamically with your network traffic. Cloud NGFW removes the heavy lifting of designing and supporting firewall architecture with high availability and eliminates manual deployment and configuration. Ensure network security performance and resiliency with a firewall specifically designed for AWS.

Contextual visibility: Gain comprehensive visibility into applications, content, and traffic, regardless of ports, protocol, and evasion tactics.

Eliminate operational headaches with cloud-native design

With infrastructure as code (IaC) and the ability to embed into your continuous integration and continuous delivery (CI/CD) pipelines, Cloud NGFW makes life easier for cloud security practitioners.

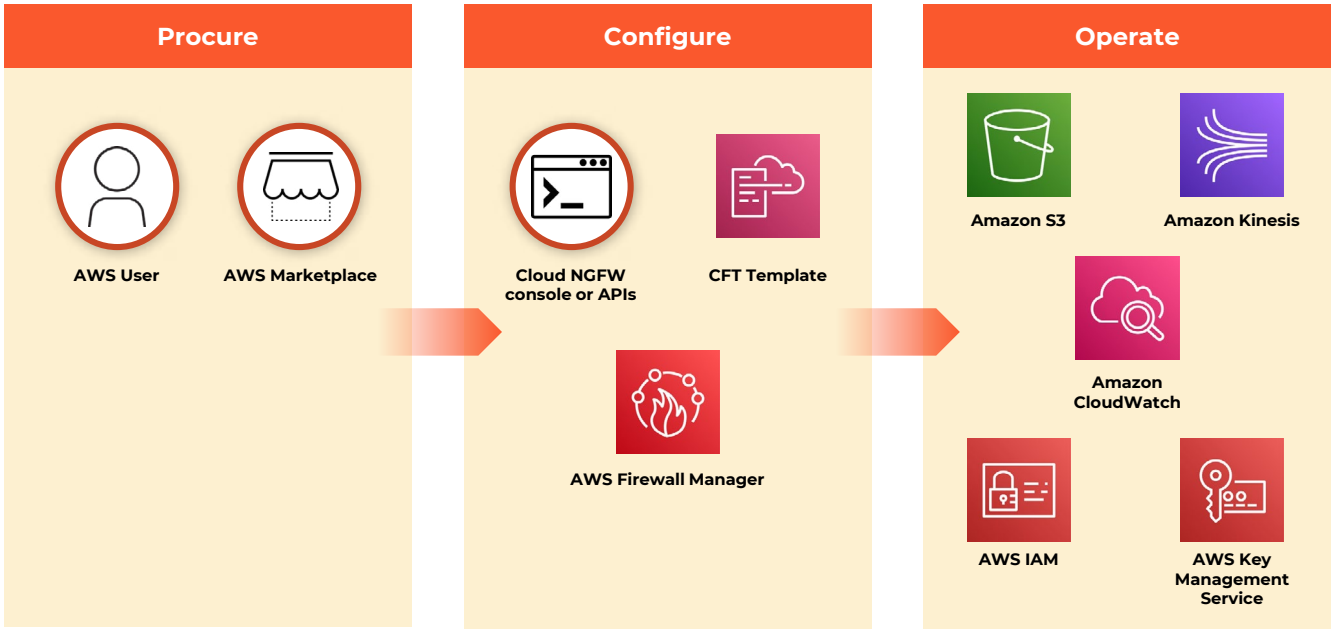
IaC for automating security best practices: Equip DevSecOps teams with IaC tools they're familiar with so they can provision next-generation firewall security quickly and easily.

Declarative policies as part of CI/CD: Provision Cloud NGFW capabilities by creating declarative policies with Terraform and CloudFormation templates. Integrating policy creation into your CI/CD pipeline brings consistency to your workflows and makes it easier to add or remove policy tags.

Automation capabilities: Whether you're using Cloud NGFW or AWS Firewall Manager to manage your Cloud NGFW deployments, take advantage of automation capabilities to streamline workflows, eliminate repetitive tasks, and free up time. Cloud NGFW supports AWS CloudFormation templates, Terraform Provider, and APIs. AWS Firewall Manager supports the same automation capabilities, plus command line interface and software development kits.

Single-click setup: Get up and running fast—in about five minutes. Procure Cloud NGFW via AWS Marketplace and set up with a single click.

Native logging: Easily integrate with native AWS services including Amazon Simple Storage Service (Amazon S3), Amazon CloudWatch, and Amazon Kinesis to meet compliance requirements for centralized logging.



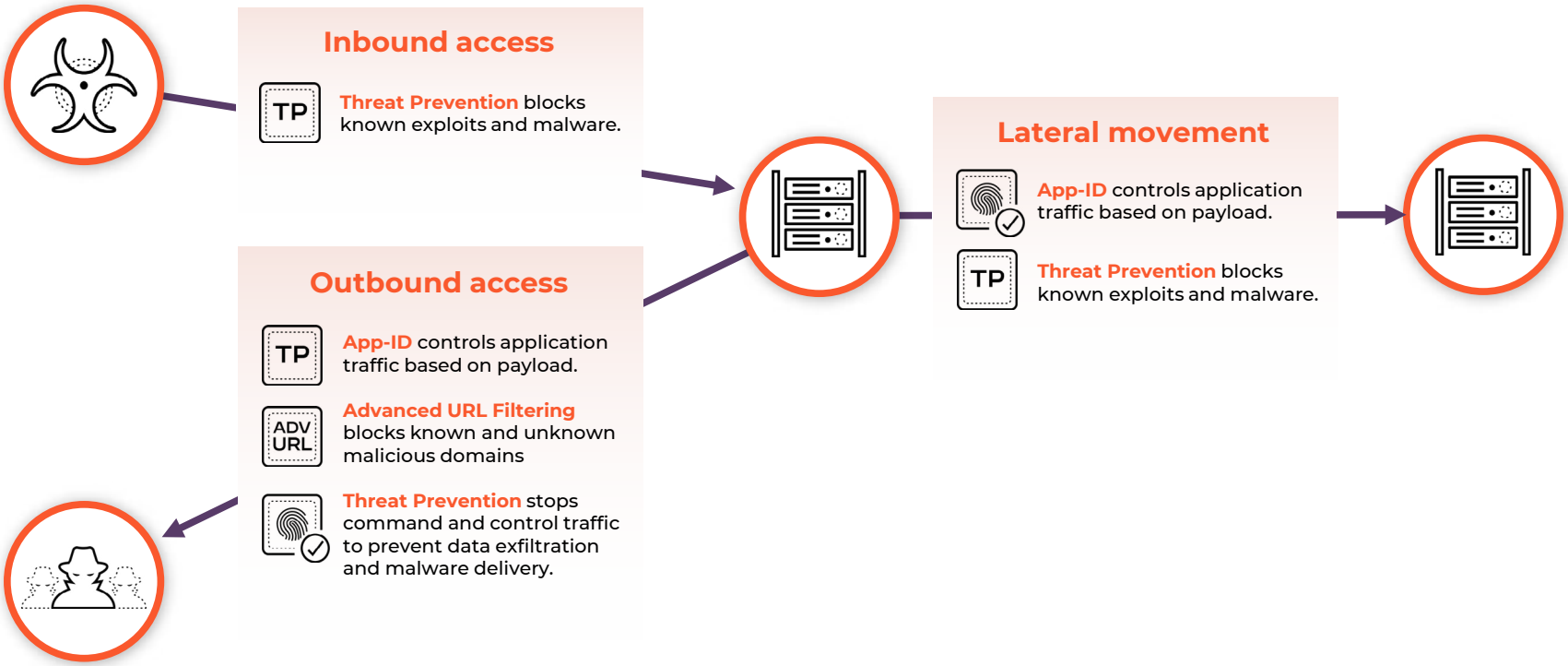
Cloud NGFW integrates with the way you work with AWS

Deploy next-generation protection quickly and easily

Palo Alto Networks and AWS have made it easy for you to deploy Cloud NGFW so you can get ML-powered network security up and running fast.

1. Find Cloud NGFW in AWS Marketplace where you can subscribe in just a few clicks. From there you can onboard your AWS accounts and determine payment options like pay-as-you-go usage.
2. Start creating Cloud NGFW resources that don't require manual, operational tasks like architecting for high availability and configuring for scale.
3. Easily define security policies through AWS Firewall Manager or the Cloud NGFW console, which connects via an API. This is when you can set security policies for App-ID, Threat Prevention, and Advanced URL Filtering so Cloud NGFW can automatically take action to keep your AWS environments safe.
4. Route Cloud NGFW to GWLB as your endpoint to secure traffic and inspect for egress, ingress, Amazon VPC to Amazon VPC, and inter-subnet within an Amazon VPC. This provides a highly available cluster that dynamically scales with traffic and enables seamless software upgrades. GWLB provides easy, transparent insertion into existing AWS environments.

See Cloud NGFW in action



Cloud NGFW secures inbound/outbound access and prevents lateral movement

Cloud NGFW in action

Outbound: Cloud workloads with outbound access inherit the risk of malicious behavior from the web and exfiltration. In addition, regulated apps that comply with Payment Card Industry (PCI) or HIPAA standards require IPS capabilities for outbound traffic.

Cloud NGFW stops emerging web-based attacks, reducing complexity for your security team and overall risk for your business. Threat prevention capabilities allow you to address IPS requirements for compliance.

Inbound: Internet-facing apps and regulated apps require protection from malicious behavior.

Cloud NGFW reduces risk and manual tasks through automatic threat prevention. You can also easily address IPS requirements for compliance with regulation such as PCI and HIPAA.

Amazon VPC to Amazon VPC: To achieve zero trust, stop lateral movement, and address compliance requirements, cloud workloads need advanced segmentation and threat prevention.

Cloud NGFW delivers threat prevention and App-ID between network segments to prevent lateral-movement attacks and satisfy compliance requirements. It also eliminates the complexity of inserting legacy IPS appliances.

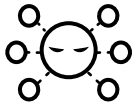
Amazon VPC to on premises: Traffic between VPCs and on-premises environments require advanced segmentation and threat prevention to achieve zero trust, stop lateral movement, and address compliance requirements.

Cloud NGFW provides threat prevention and App-ID between network segments to prevent lateral-movement attacks and satisfy compliance requirements. It also eliminates the complexity of inserting legacy IPS appliances.

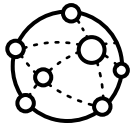
Rely on a global cybersecurity leader

Cloud NGFW is backed by the industry's largest network security platform, and a leading cybersecurity company. Palo Alto Networks stays ahead of malicious actors, protecting you from what might come next.

4.3M
Unique security updates per day



224B
Threats blocked per day



15M
Transactions secured per day

95%
of Fortune 100 companies rely on Palo Alto Networks

#1
in enterprise security

10 TIMES
a leader in Gartner® Magic Quadrant™ for Network Firewalls

Palo Alto Networks provides continuous visibility, compliance enforcement, reporting, and threat protection for all your AWS resources. From Amazon Elastic Cloud Compute (Amazon EC2) to Amazon Elastic Container Service (Amazon ECS), to AWS Lambda, and everything in between, Palo Alto Networks keeps you protected with native AWS services. Together, AWS and Palo Alto Networks provide the broadest set of integrated security capabilities, whether your organization is just beginning its cloud journey or you're already running your business in the cloud.

Take the next step

Get started with Cloud NGFW by subscribing through the AWS Marketplace where you can get started today securing your applications and workloads with best-in-class security and cloud-native ease of use.

Get started in AWS Marketplace>>

cloud-ngfw-ebook-033022