

Inside PAN-OS

World's First ML-Powered NGFW Shifts the Cybersecurity Paradigm

paloalto® NETWORKS



Table of Contents

Reinventing the NGFW 3

Machine Learning Delivers Intelligent Security 4

Top Features in PAN-OS 10.0 5

- IoT Security 6
- Container NGFW 7
- ML-Based Inline Prevention 8
- Simplified Decryption 9
- DNS Security 10
- HA Clustering 11
- More New Features 12

Prior PAN-OS Features 13

Summary 15

Reinventing the Next-Generation Firewall

In June 2020, we introduced our ML-Powered NGFW—the world's first machine learning-powered next-generation firewall. Our mission with this release is to continue to empower you to stay ahead of emerging threats, see and secure your entire enterprise, and support speed and error reduction with automatic policy recommendations. At the heart of this disruptive solution is the new PAN-OS® 10.0.

Why a Paradigm Shift Is Needed

As a security professional, you must continually protect your organization from rapidly morphing attacks that bypass traditional security protections. In addition, the infrastructure and devices you need to protect are quickly expanding, sometimes without notice, and as apps move to the cloud and more users work remotely, your attack surface expands.

The industry's traditional reaction has been to shorten the response time to new attacks—from weeks to days to hours, and in our case, to minutes. However, many of today's most virulent threats—ransomware, for one—inflict considerable damage in just seconds. The need is for a paradigm shift to usher in a new era of proactive and intelligent security utilizing machine learning. PAN-OS 10.0 at the core of our ML-Powered NGFW is continuously learning and proactively improving security across multiple fronts, so you don't just keep up but get ahead.

Recent PAN-OS Releases

PAN-OS 10.0 represents our continued commitment to setting the standards for network security. It enables you to proactively stop threats, secure IoT devices, reduce errors with automatic policy recommendations, and much more. As with all PAN-OS releases, PAN-OS 10.0 incorporates all the features in previous releases. The diagram above shows a sampling of the primary new capabilities in PAN-OS 10.0 as well as the capabilities in previous PAN-OS releases—all of which are inherited by PAN-OS 10.0.



Machine Learning Delivers Intelligent Security

As described earlier, ML is the secret sauce for PAN-OS 10.0. But what does ML really mean for cybersecurity? After all, many vendors have added a few ML functions to their traditional solutions. The difference in our approach is that we infused ML into the core of the NGFW. At Palo Alto Networks, ML is built in, not bolted on. As used in PAN-OS 10.0, ML impacts cybersecurity, to prevent malware and phishing attacks, detect IoT threats, and improve security policies.



PREVENT KNOWN AND UNKNOWN THREATS

In a completely new approach to threat prevention, ML-Powered NGFW with PAN-OS 10.0 uses ML models to identify variants of known attacks as well as many unknown cyberthreats to defend against up to 95% of unknown threats inline on the NGFW. In addition, for threats not blocked by inline ML, this release introduces near-real-time protection with zero-delay signature updates.



DETECT DEVICES AND ANOMALIES

ML-based security service for the NGFW with PAN-OS 10.0 provides complete device visibility, behavioral anomaly detection, and native enforcement to secure IoT devices on your network without the need for additional sensors or infrastructure.



IMPROVE SECURITY POLICIES

PAN-OS 10.0 uses ML modeling to translate telemetry information into recommended security policy changes. This capability is particularly important for IoT security, allowing customers to view and adopt IoT security policy recommendations for safe device behavior. By improving security policies based on telemetry, PAN-OS 10.0 enables you to save time, reduces human error, and boosts security for IoT devices.

Top Features in PAN-OS 10.0

PAN-OS 10.0 includes more than 70 new features—far too many to explain each one in detail here. Some of the most significant enhancements in PAN-OS 10.0 are IoT security, container NGFW, ML-based inline prevention, simplified decryption, DNS security, and HA clustering, each of which is described in the next sections. PAN-OS empowers a consistent, integrated, and best-in class network security available in physical, virtual, containerized, and cloud-delivered form factors—all managed centrally.



IoT Security



ML-Powered NGFW for Kubernetes



ML-Based Inline Prevention



Simplified Decryption



DNS Security



HA Clustering

Top Feature: IoT Security

AT-A-GLANCE

- IoT device visibility
- Anomaly detection
- Risk assessment
- Prevention of all threats
- Policy recommendations
- Native enforcement
- Easy deployment

CHALLENGE

IoT devices account for approximately 30% of all devices in enterprise environments today and pose a rapidly increasing risk. Unmanaged IoT and OT devices are susceptible to a variety of threats, are rarely monitored and have unfettered access to enterprise networks. Traditional security tools cannot provide full visibility of IoT devices and lack controls necessary to stop threats, a prerequisite for effective IoT security.

SOLUTION

Our IoT Security service combines ML with our patented App-ID technology to provide the most accurate and deepest level of visibility into your IoT and OT devices, also creating an effective baseline of their normal behavior. The solution empowers security teams to proactively prevent threats, monitor device risk, detect anomalies, and recommend—then automatically apply—policies for enforcement. Deploying our IoT Security service is easy and does not require investment of any single purpose sensors or infrastructure. Simply enable the service on your Palo Alto Networks ML-Powered Next-Generation Firewall to extend leading-edge protections and get additional context of your previously unmanaged IoT and OT assets. With the ML-powered IoT Security, you can now trust every device in your network.

Trust Every Device on Your Network



Learn more.

Top Feature: ML-Powered NGFW for Kubernetes

AT-A-GLANCE

- Native Kubernetes deployment
- Consistent enterprise-wide network security
- Streamlined security for DevOps
- Unified security management

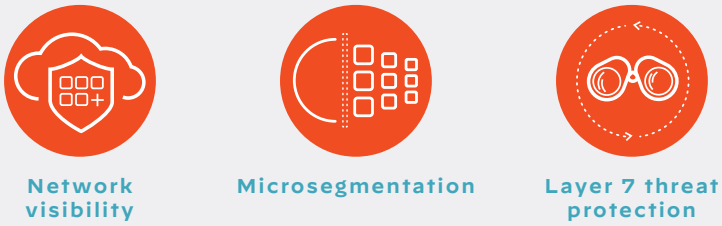
CHALLENGE

In just a few years, containers and Kubernetes have become the predominant methodology for developing and releasing software applications in cloud environments. However, traditional NGFWs lack visibility and control for Kubernetes environments and cannot take advantage of the rich capabilities of these sophisticated tools.

SOLUTION

With PAN-OS 10.0, we released the industry's first ML-Powered NGFW for container security designed specifically for Kubernetes. CN-Series integrates security capabilities directly into the container environment, overcoming the limitations of traditional firewalls. You can now enforce the same level of network security in your cloud native environments as the rest of your environment. To ensure DevOps speed and agility, CN-Series NGFWs make use of native Kubernetes orchestration to integrate firewall deployment directly into the CI/CD development process for frictionless deployments. CN-Series NGFWs are managed with Palo Alto Networks Panorama, which provides security analysts with a single console from which to manage all network security components, a significant time-saver.

Layered Network Protection for Container Environments



Learn more.

Top Feature: ML-Based Inline Prevention

AT-A-GLANCE

- Inline prevention for new attacks
- ML-driven security analytics
- Behavior-based detection
- Powered by intelligence from WildFire, URL Filtering

CHALLENGE

Millions of new cyberthreats emerge every year as organizations constantly race to prevent them. Leveraging cloud-scale resources, automation, and other techniques, today's adversaries enjoy some inherent advantages: the ability to spread their attacks more quickly than ever, and the ability to deploy polymorphic malware and malicious content that evades detection by constantly changing its identifiable features.

SOLUTION

With inline ML powered by intelligence from our WildFire and URL Filtering services, the time from visibility to prevention for unknown network traffic becomes effectively zero. You can now stop new threats instantly, preventing initial infection and potential spread. WildFire and URL Filtering provide protection against weaponized files, credential phishing, malicious scripts, and fileless attacks without affecting the digital workflow. Leveraging existing investments in Palo Alto Networks NGFWs, PAN-OS 10.0 helps you future-proof your defenses to evolve with the latest attacks.



Learn more.

Top Feature: Simplified Decryption

AT-A-GLANCE

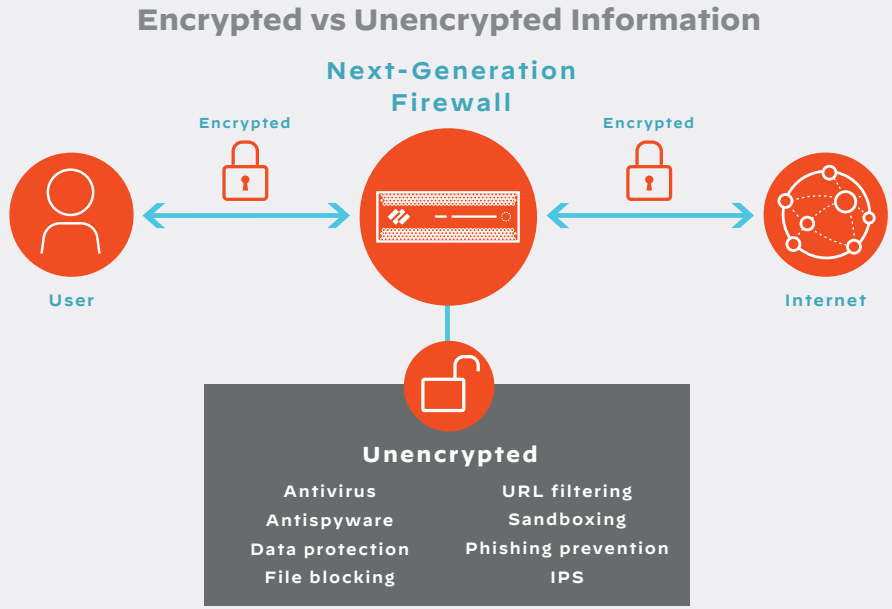
- Full visibility into encrypted traffic
- Works with URL filtering
- Support for TLS 1.3
- 2X performance boost

CHALLENGE

Encryption via SSL and TLS protocols is a useful tool for keeping information more secure. Unfortunately, cyberattackers also use encryption to bypass traditional perimeter security and steal valuable personal identifiable information (PII) and launch devastating ransomware attacks.

SOLUTION

NGFWs running PAN-OS 10 provide full visibility into the details of all encrypted connections to make it even easier to deploy and maintain decryption. Tools such as URL filtering allow security teams to prioritize what to decrypt and quickly implement decryption policies and gain threat prevention capabilities on encrypted traffic. PAN-OS 10.0 also supports the TLS 1.3 protocol, future proofing your investments in network security.



Learn more.



Top Feature: DNS Security

AT-A-GLANCE

- Simplified security through automation
- Prediction and blocking of new malicious domains
- Intelligence to act on threats over DNS

CHALLENGE

DNS attacks are on the rise and can take on many different forms. A DNS attack can render the DNS service unavailable, causing internet connectivity loss and disrupting your business.

SOLUTION

Our DNS Security service applies predictive analytics, machine learning, and automation to block attacks that use DNS. Tight integration with the ML-Powered NGFW gives you automated protection, prevents attackers from bypassing security measures, and eliminates the need for independent tools or changes to DNS routing. Comprehensive analytics allow deep insights into threats and empower you with the context to optimize your security posture.

Learn more.



Top Feature: HA Clustering

AT-A-GLANCE

- Failover support for always-on data centers
- Cost management with incremental addition of firewalls to existing HA pair
- Simplified scaling of HW firewalls and VM firewalls in private cloud environments

CHALLENGE

As businesses scale, they require a simple and cost-effective way to scale security against sophisticated attacks, regardless of where their applications reside.

SOLUTION

Our HA Clustering service enables you to gain consistent, industry-leading security that seamlessly scales with your application requirements. Unlike other competitive products, PAN-OS 10.0 allows you to simply add new appliances to scale performance and capacity. Now you can confidently spread and secure your traffic load across multiple data centers and firewalls to ensure flexibility, always-on availability, and exceptional user experience.

Learn more.

More New Features

Real-Time Signature Streaming

For unknown threats that cannot be prevented inline, WildFire® delivers protections in real time after cloud analysis, offering zero-delay signature updates for rapid threat prevention.

Fastest Next-Generation Firewall

The new Data Processing Card enables your process-intensive operations such as decryption to run with even better speed, making the PA-7000 Series the fastest NGFW available.

Automated Device Quarantine for Stronger Security

GlobalProtect Device Quarantine reliably and automatically identifies compromised devices and restricts their network access to prevent other users and devices getting infected.

SNORT Support

PAN-OS 10.0 offers rapid protection for newly discovered vulnerabilities with UI and API support for SNORT and Suricata signatures.

Device-ID

Complementing PAN-OS 9.x features App-ID™ and User-ID™, PAN-OS 10.0 introduces Device-ID™, which allows you to target ML-enabled policy recommendations to devices.

Flexible Monitoring for SaaS Applications

Ability to monitor and measure the end-to-end application health between your branches and SaaS application servers to provide better user experience.

For a complete list of all PAN-OS 10.0 features, see the PAN-OS New Features Guide.



Prior PAN-OS Features

Like its predecessors, PAN-OS 10.0 builds on capabilities contained in previous releases. This section describes the most important incremental features of PAN-OS 9.1 and 9.0. All of the features described in this section are available in PAN-OS 10.0.

PAN-OS 9.1

PAN-OS 9.1 introduced new services and features that help organizations extend security into branch offices, apply security dynamically to users, and provide better visibility for mobile users connecting to the network.

Secure SD-WAN

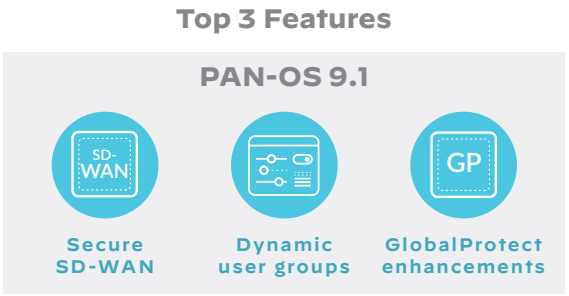
With PAN-OS 9.1, Palo Alto Networks integrated NGFW security and SD-WAN functionality in a single management system. Prisma™ Access, our secure access service edge (SASE), integrates directly with SD-WAN partners to deliver SD-WAN as a cloud service. Prisma Access helps organizations optimize performance and eliminates the need to build out custom SD-WAN hubs and interconnects. Secure SD-WAN comes with zero-touch provisioning (ZTP) to streamline the onboarding process for branch and remote offices.

Dynamic User Groups

The Dynamic User Groups service allows security teams to automatically include users as members without manually creating and committing policy or group changes. Dynamic User Groups maintain user-to-data correlation at the device level even before the firewall scans the traffic. Security teams can configure and manage a single security policy to auto-remediate anomalous behavior and malicious activity while maintaining user visibility.

GlobalProtect Enhancements

PAN-OS 9.1 provided greater visibility, rapid troubleshooting, and enhanced logging enhancements to help security teams monitor and rectify connection failures with existing deployments of GlobalProtect™ network security for endpoints. The logging enhancements are available for any Palo Alto Networks NGFW deployed as a GlobalProtect gateway or portal or in a Prisma Access mobile user deployment.



Prior PAN-OS Features

PAN-OS 9.0

With PAN-OS 9.0 we introduced simplified operations through analytics and automation while giving security teams end-to-end visibility and control across the data center, perimeter, branch, mobile, and cloud networks.

DNS Security

The DNS Security service applies predictive analytics to disrupt attacks that use DNS for command and control or data theft. Tight integration with the next-generation firewall provides automated protections and eliminates the need for stand-alone tools. Threats hidden in DNS traffic are rapidly identified with shared threat intelligence and machine learning. Cloud-based protections are always up to date and scale infinitely, giving organizations a critical new control point to stop DNS-based attacks.

Policy Optimizer

Moving from port-based legacy firewall rules to App-ID™ technology-based ones greatly reduces the opportunity for attack. However, that transformation takes time, effort and resources. The new Policy Optimizer uses simple workflows and intelligence gathered by PAN-OS to move from legacy rules to App-ID-based controls.

New Hardware for the PA-7000 Series

New enhancements make the PA-7000 Series next-generation firewalls blazingly fast. The all-new Network Processing Card (NPC), Switch Management Card (SMC) and Log Forwarding Card (LFC) intelligently distribute processing demands, each with massive amounts of computing power and dedicated memory. The combination of enhanced performance and advanced prevention capabilities makes it possible for the new PA-7000 Series to stop the most sophisticated cyberattacks at the highest throughput levels.



Summary

PAN-OS 10.0 is both evolutionary and revolutionary. Like all PAN-OS releases, PAN-OS 10.0 incorporates and builds on all the capabilities developed over the past, including every feature described in this e-book. With PAN-OS 10.0, firewalls can detect unknown threats instantly and see into encrypted traffic, evolutionary upgrades that add value to existing security infrastructures with little effort.

At the same time, PAN-OS 10.0 embeds machine learning into the NGFW core and incorporates new capabilities for IoT and container security—revolutionary upgrades. By bringing these industry-firsts into a single system, Palo Alto Networks ML-Powered NGFW helps you protect your organization against up to 95% of unknown file and web-based threats instantly; automate policy recommendations to save time and reduce the chance of human error; adapt and provide instantaneous real-time protection; and extend visibility and security to all devices, including unmanaged IoT devices without the need to deploy additional sensors.

Taken together, the set of new features in PAN-OS 10.0 constitute a giant step forward for NGFW technology. Upgrade now to PAN-OS 10.0 to take advantage of all these benefits.

For more information, read the PAN-OS New Features Guide.

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

© 2020 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.
(Title and date)