Palo Alto Networks ML-Powered Next-Generation Firewall Feature Overview

The face of the enterprise is changing. Attacks are constantly and automatically morphing. New devices are proliferating rapidly and without notice. Your business needs are driving rapid changes. Typical security products force you to react to these changes manually, straining your resources and leaving your organization exposed.

The world needs a new type of firewall—one with machine learning and analytics at its core, capable of identifying new threats, devices, and more without relying on fingerprinting or signatures. It must continuously update the machine learning models by analyzing data using unlimited cloud computing. It must also continuously collect telemetry and recommend policy and configuration changes to reduce risk and reduce chances of error.

Confidently lead digital transformation with the world's first ML-Powered Next-Generation Firewall, proactively securing your organization. Embrace machine learning to deliver the industry's only inline malware and phishing prevention to stop unknown threats as they reach your network. Automatically reprogram your network with zero-delay signature updates for all other threats. Provide accurate signatureless identification of all unmanaged internet of things (IoT) devices. Use telemetry to optimize security policy and eliminate breaches due to misconfiguration. Adopt a consistent, integrated, and best-in-class network security platform available in physical, virtual, containerized, and cloud-delivered form factors—all managed centrally.

The Foundation of a Network Security Strategy

Our Next-Generation Firewalls inspect all traffic, including all applications, threats, and content, and tie that traffic to the user, regardless of location or device type. The user, application, and content—the elements that run your business—become integral components of your enterprise security policy. As a result, you can align security with your business policies as well as write rules that are easy to understand and maintain.

Figure 1: Core elements of network security

Identify Users and Protect User Identity

User-ID technology enables our Next-Generation Firewalls to identify users in all locations, no matter their device type or operating system. Visibility into application activity—based on users and groups instead of IP addresses—safely enables applications by aligning usage with business requirements. You can define application access policies based on users or groups of users. For example, you can allow only IT administrators to use tools such as Secure Shell, Telnet, and File Transfer Protocol. Policy follows users no matter where they go—headquarters, branch office, or home—and across any devices they may use. Plus, you can use custom or predefined reporting options to generate informative reports on user activities.

Palo Alto Networks introduced Cloud Identity Engine to help aggregate and centralize user information by enabling redistribution of user information (User-ID, IP-Tag, User-Tag, quarantine list, and IP-port user mappings) across all locations. Cloud Identity Engine allows consistent authentication and authorization of users regardless of location and where user identity stores live and effortlessly enables access based on user identity to quickly move towards a Zero Trust security posture—all using a point-and-click configuration automatically synchronizing identity across identity providers. Identity and authentication providers that are supported include all SCIM-compliant providers (e.g., Azure AD, Okta, Ping, Google Identity Cloud), Microsoft AD, and LDAP.

However, the issue of user identity goes beyond user-based policy and reporting. Protecting user identity is equally important. Phishing and the use of stolen credentials were the top two threat action types.[1] In fact, 90% of security incidents in 2021 involved phishing.[2] Attackers use stolen credentials to gain access to organizations' networks, where they find valuable applications and data they can steal. To prevent credential-based attacks, our Next-Generation Firewalls:

- **Stop unknown and highly evasive phishing attacks** via Advanced URL Filtering, using detections powered by inline deep learning for real-time analysis and prevention of both known and unknown web-based threats, stopping 40% more threats than traditional filtering databases.
- **Stop users from submitting corporate credentials to unknown sites**, protecting them from targeted attacks that use new, unknown phishing sites to go undetected.
- **Automate responses that adapt and follow user behavior** via Dynamic User Groups (DUGs). Whether a user's credentials are compromised, or you need to provide temporary access to users, DUGs enable you to leverage user behavior data from Cortex XDR, user and entity behavior analytics (UEBA), and security information and event management (SIEM) systems to automatically enforce security policies in real time.
- **Allow you to enforce multifactor authentication (MFA)** for any application you deem sensitive, including legacy applications that do not lend themselves easily to MFA. This protects you if an adversary already possesses stolen credentials. You can use this capability with the identity vendor of your choice.

Safely Enable Applications

Users are accessing diverse application types, including SaaS. Some of these apps are sanctioned by your organization; some are tolerated, though not mandatory to carry out your business, and the rest must not be allowed since they increase risk. App-ID technology on our Next-Generation Firewalls accurately identifies applications in all traffic passing through the network, including applications disguised as authorized traffic, using dynamic ports, or trying to hide under the veil of encryption. App-ID allows you to understand and control applications and their functions, such as video streaming versus chat, upload versus download, screen-sharing versus remote device control, and so on.

SaaS application characteristics allow you to understand application usage. For example, you can identify which SaaS applications accessed from your organization lack the required certifications or have a history of data breaches. You can also allow access to sanctioned enterprise accounts on SaaS applications, such as Microsoft 365, while blocking access to unsanctioned accounts, including personal/consumer accounts.

With Policy Optimizer, you can strengthen security by closing dangerous policy gaps left by legacy firewall policies. Policy Optimizer helps your security team easily replace legacy rules with intuitive, application-based policies. Because App-ID-based rules are easy to create, understand, and modify as business needs evolve, they minimize configuration errors that leave you vulnerable to data breaches. These policies strengthen security and take significantly less time to manage.

Secure Encrypted Traffic Without Compromising Privacy

Users spend almost all of their time on encrypted websites and applications.[3] Unfortunately, attackers use encryption to hide threats from security devices.

Our Next-Generation Firewalls use policy-based decryption to allow security professionals to decrypt malicious traffic, including traffic using TLS 1.3 and/or HTTPS/2, yet preserve user privacy and predictable performance. Flexible controls allow you to leave traffic encrypted if it is sensitive—for instance if it is associated with shopping, military, healthcare, or government websites. You can prevent users from accessing websites that use self-signed, untrusted, or expired certificates. You can also block access if a website is using unsafe TLS versions or weak cipher suites. To preserve user privacy, you can define decryption exclusions by policy and additionally allow users to opt out of

1. *2019 Data Breach Investigations Report*, Verizon, May 2019.
2. Ibid.
3. "HTTP encryption on the web," Google Transparency Report, accessed May 2020.

decryption for specific transactions that may contain personal data. The rest of your traffic can be decrypted and secured. If you're unsure where to start, you can use our Next-Generation Firewalls to gain full visibility into the details of all encrypted connections.

Support for hardware security modules allows you to manage digital keys securely. Perfect Forward Secrecy ensures the compromise of one encrypted session does not lead to the compromise of multiple encrypted sessions.

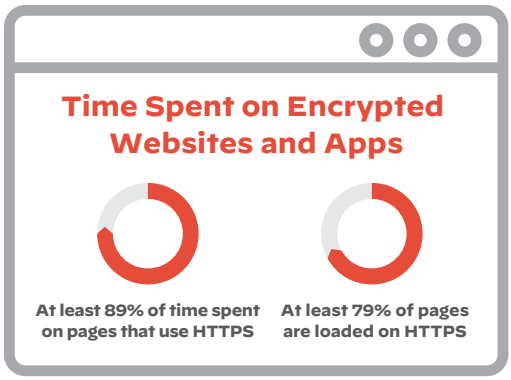

Figure 2: Growing prevalence of web encryption

Detect and Prevent Advanced Threats

Cyberattacks have increased in volume and sophistication, now using advanced techniques to transport attacks or exploits through network security devices and tools. This challenges organizations to protect their networks without increasing their security teams' workloads or hindering business productivity. Seamlessly integrated with the industry-leading Next-Generation Firewall platform, our cloud-delivered security subscriptions coordinate intelligence and provide protections across all attack vectors, eliminating the coverage gaps that disparate network security tools create. Take advantage of market-leading capabilities with the consistent experience of a platform, and secure your organization against even the most advanced and evasive threats.

Advanced Threat Prevention

Advanced Threat Prevention is the industry's first IPS to stop zero-day attacks inline in real time. In addition to best-in-class prevention of known threats, it reliably stops never-before-seen exploit attempts and command and control with the industry's only inline deep learning engines that provide 60% more prevention of zero-day injection attacks and 48% more highly evasive command and control than traditional IPS solutions. Customers can also import, sanitize, manage, and completely automate workflows to rapidly apply IPS signatures in popular formats such as Snort and Suricata, further adding to our leading threat coverage.

Advanced URL Filtering

Advanced URL Filtering is the industry's only web security engine to stop known and unknown web-based threats, such as phishing, malware, and ransomware, all in real time. With the power of inline deep learning, Advanced URL Filtering can perform real-time analysis of your web traffic, allowing you to prevent unknown and highly evasive threats instantly as well as prevent patient zero. With this latest technology, Advanced URL Filtering can prevent 40% more web-based threats than any other vendor. Web security rules are an extension of your Next-Generation Firewall policy, reducing complexity by giving you a single policy set to manage.

Advanced WildFire

Advanced WildFire is the largest cloud-based malware analysis and prevention engine that uses machine learning and crowdsourced intelligence to protect organizations from highly evasive threats. Utilizing over 25 patented detection engines and inline machine learning modules on the NGFW to identify and prevent 99% of known and unknown file-based threats, Advanced WildFire can protect users before a threat even enters your network.

DNS Security

DNS Security applies predictive analytics, machine learning, and automation to block the latest and most sophisticated attacks that use DNS. Tight integration with the Next-Generation Firewall gives you automated protections, 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 security personnel with the context to optimize their security posture. DNS Security offers industry-first detections, giving your 40% more threat coverage against DNS-layer attacks.

IoT Security

IoT Security is the industry's most comprehensive Zero Trust security for IoT devices, delivering ML-powered visibility, prevention, and enforcement in a single platform. This unique combination of IoT visibility and the Next-Generation Firewall enables context-aware network segmentation to reduce risk exposure and applies our leading security subscriptions to keep IoT and IT devices secure from all threats.

In order to meet the specific needs of different industry verticals, we have designed two separate IoT security products:

- **Medical IoT Security** makes it push-button easy for you to see, secure, govern, and report on your specialized medical devices like infusion pumps, MRI machines, and patient monitors, and helps you achieve HIPAA compliance.
- **Enterprise IoT Security** makes it push-button easy to see, secure, govern, and report on all of your IoT devices, like printers, security cameras, and HVAC systems, and meet FedRAMP and NIST guidelines.

Next-Generation CASB

As SaaS apps rapidly proliferate and collaboration apps emerge in highly distributed workforces, traditional CASB solutions fail to adequately secure them. Legacy approaches limit visibility and scale and offer poor data protection while being costly.

Our Next-Gen CASB solution has the capacity to keep any and all of your SaaS apps secure across your entire enterprise in real time. With comprehensive data protection that's leading the industry, you can contain rapid implementation of SaaS products with confidence while securely enabling your hybrid workforce.

Shared Threat Intelligence

Organizations rely on threat intelligence from multiple sources to provide the widest visibility into unknown threats. Unfortunately, ingesting such high volumes of data leaves businesses struggling to aggregate, correlate, validate, and glean insights to share information and enforce protections across their networks.

Advanced WildFire quickly detects unknown threats, maintains shared intelligence from a global community, and automatically delivers protections to enforcement points in seconds, alleviating the manual tasks of reversing malware, sifting through large pools of data, and importing intelligence. Advanced WildFire users receive integrated logs, malware analysis reports, and visibility into malicious events through their existing applications, including PAN-OS, Panorama network security management, AIOps, Cortex XSOAR, and Cortex XDR. This enables security teams to rapidly review reports, correlate observed network events, locate potential threats, investigate, and respond.

If a customer's Next-Generation Firewall or endpoint in Singapore encounters a suspicious file, that file is sent to Advanced WildFire for analysis. The results of the analysis, including verdicts and protections, are then automatically sent to the customer in Singapore as well as all other Advanced WildFire customers worldwide.

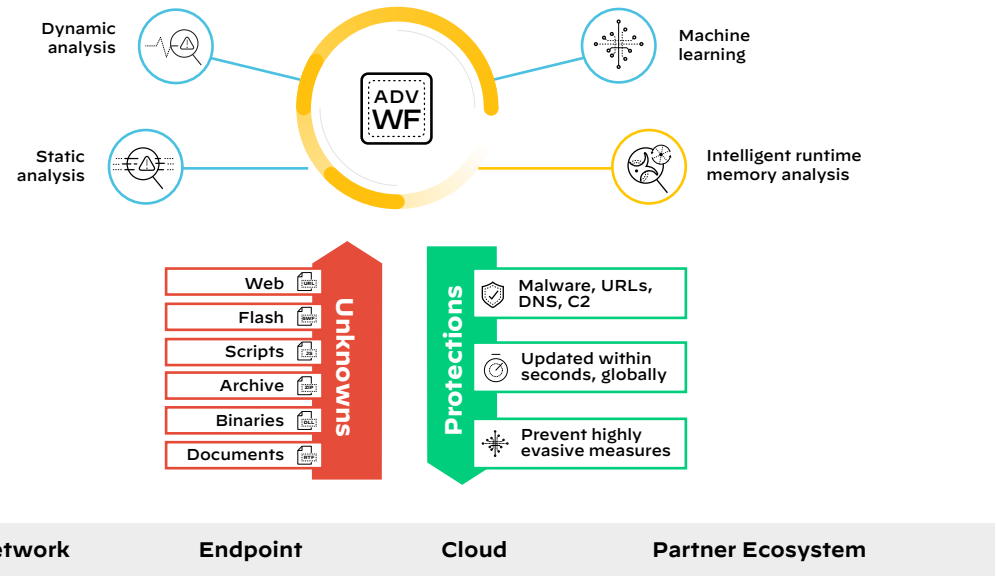

Figure 3: Shared threat intelligence across the ecosystem

Zero Trust

Conventional security models operate on the outdated assumption that everything inside an organization's network can be trusted. These models are designed to protect the perimeter. Meanwhile, threats that get inside the network go unnoticed and are left free to compromise sensitive, valuable business data. In the digital world, trust is nothing but a vulnerability. Zero Trust is a cybersecurity strategy that prevents data breaches. In Zero Trust, each step a user makes through the infrastructure must be validated and authenticated across all locations. Our Next-Generation Firewalls directly align with Zero Trust, including enabling secure access for all users irrespective of location, inspecting all traffic, enforcing policies for least-privileged access control, and detecting and preventing advanced threats. This significantly reduces the pathways for adversaries, whether they are inside or outside your organization, to access your critical assets.

Single-Pass Architecture

Protection against the evolving threat landscape often requires new security functions to be introduced. Palo Alto Networks Next-Generation Firewalls are built on a single-pass architecture, which offers predictable performance and native integration—features that cannot be attained by layering new capabilities on legacy architecture that still works on IP addresses, ports, and protocols. Our Next-Generation Firewalls perform a full-stack, single-pass inspection of all traffic across all ports, providing complete context around the application, associated content, and user identity to form the basis of your security policy decisions. This architecture allows us to add innovative, new capabilities easily—as we've already done with Advanced WildFire and, more recently, IoT Security.

Flexible Deployment

Our Next-Generation Firewalls can be deployed in multiple form factors:

- **PA-Series**: A blend of power, intelligence, simplicity, and versatility protects enterprise and service provider deployments at headquarters, data centers, and branches.
- **VM-Series**: Our Virtual Next-Generation Firewalls protect your hybrid cloud and branch deployments by segmenting applications and preventing threats.
- **CN-Series**: Our containerized firewall is the best-in-class next-generation firewall purpose-built to secure your Kubernetes environment from network-based attacks.
- **Cloud NGFW**: With Cloud NGFW for Amazon Web Services (AWS), customers gain both best-in-class security and an easy, managed cloud-native experience delivered by Palo Alto Networks on the AWS platform.
- **Prisma Access**: Our secure access service edge (SASE) offering delivers operationally efficient security globally from the cloud.

You can choose one of these or a combination to match your requirements by location, and manage all deployments centrally through Panorama network security management.

Network Security Management

IT and network security teams are stretched thin with having to manage increasingly complex security tools and management consoles. Their security tools are accompanied by complex and outdated security policies spread across multiple rule bases, causing a lack of visibility and control over their security posture. They want to **simplify** network security management and **reduce administrative overhead** by automating day-to-day tasks. Organizations also want to integrate firewall management with other third-party tools for operational efficiency. Whether managing two firewalls or large-scale deployments, you can use Panorama to save time and reduce complexity by managing network security with a single pane of glass for all your Palo Alto Networks firewalls, irrespective of their form factor, location, or scale. Gain visibility into your network security deployment and increase efficiency through automation.

1. **Centrally manage** device lifecycle and network security configuration for all firewall form factors in one unified UI.

2. **Streamline** configuration sharing with templates and device groups. Scale log collection as logging needs increase.
3. **Obtain** deep visibility and monitor network traffic and security threats with Application Command Center (ACC), reporting, and detailed log views.
4. **Use** built-in automation and customize security workflows using APIs to integrate with third-party systems and operational tools.
5. **Benefit from** the latest security innovations with a straightforward, single reboot upgrade process that fits into a typical maintenance window. This simplifies the upgrade for HA pairs.

AIOps for NGFW

AIOps for NGFW redefines firewall operational experience by empowering security teams to proactively strengthen security posture and resolve firewall disruptions. It provides continuous best practice recommendations powered by machine learning (ML) based on industry standards, security policy context, and advanced telemetry data collected from all Palo Alto Networks firewalls to improve security posture. AIOps can also intelligently predict firewall health, performance, capacity, and other firewall health problems up to seven days in advance and provides actionable insights to resolve the predicted disruptions. AIOps offers a unified view into the activity seen in your organization across applications, threats, networks, users, and security subscriptions like WildFire and DNS Security to help achieve a unified view of your security effectiveness. AIOps for NGFW is a cloud-based service on ML-Powered Next-Generation Firewalls and Panorama that runs on PAN-OS 10.0 and above. Today, it processes over 49 billion metrics across 60,000 firewalls and proactively shares 24,000 misconfigurations and 17,000 firewall health issues for resolution every month.

Reporting and Logging

To identify, investigate, and respond to security incidents, the Next-Generation Firewall platform provides:

- **Cortex Data Lake**: You have the flexibility to aggregate logs, build workflows, and visualize your data either on-premises or in the cloud-based Cortex Data Lake. Cortex Data Lake offers cloud-based, centralized log storage and aggregation for your hardware, software, and cloud-delivered firewalls. It is secure, resilient, and scalable, allowing you to stitch together data from across all parts of your network to increase visibility as well as accelerate incident investigation and response. The automated correlation engine uses machine learning to eliminate manual correlation tasks and surface threats that would otherwise be lost in the noise.
- **Reporting**: You can use our standard reports or create custom versions to render the data to suit your specific requirements. All reports can be exported to CSV or PDF format, as well as executed and emailed on a schedule.
- **Threat hunting**: With collective insight from thousands of global enterprises, service providers, and governments, AutoFocus provides unprecedented visibility into unknown threats. Integration of AutoFocus into PAN-OS speeds up threat analysis and hunting workflows without requiring additional specialized resources.

Natively Integrated SD-WAN

As businesses increasingly move applications to the cloud, they are actively adopting software-defined wide area networks (SD-WAN) to increase bandwidth and improve user experience in branch and retail locations. However, SD-WAN brings many challenges, such as subpar security, poor performance, and complexity. Palo Alto Networks enables you to adopt an end-to-end SD-WAN architecture with natively integrated, world-class security and networking. You can simplify your SD-WAN deployment by leveraging Next-Generation Firewalls as your edge devices in the branch, eliminating the need to add a dedicated SD-WAN appliance. Use Prisma Access as your SD-WAN hub and interconnect to minimize latency and ensure reliable performance on your network. Consuming Prisma Access as a service is the simplest way to enable SD-WAN for your organization. Alternatively, you can follow a do-it-yourself model using Next-Generation Firewalls as hub devices. To use this model, simply enable our SD-WAN subscription on your Next-Generation Firewalls. Palo Alto Networks supports multiple SD-WAN deployment options, including mesh and hub-and-spoke. Whichever you select, our tight integration allows you to manage security and SD-WAN on a single intuitive interface.

Why Palo Alto Networks Next-Generation Firewalls?

Our ML-Powered Next-Generation Firewalls empower you to stop zero-day threats using ML, AI, and inline deep learning. The consolidated platform approach simplifies network security for our customers with the addition of AIOps to help improve security posture and IoT Security to quickly discover and protect devices against known and unknown threats. We've been recognized as a Leader in Gartner's *Magic Quadrant for Network Firewalls* eight times in a row, and our firewalls have received a Recommended rating from NSS Labs—the highest rating NSS Labs offers.

Welcome to the era of intelligent security—protecting your enterprise from the threats of tomorrow.

Here are some helpful resources to get you started:

- ✓ Want to learn more about our Next-Generation Firewalls? Visit our Secure the Network page.
- ✓ Ready to get your hands on our Next-Generation Firewalls? Take an Ultimate Test Drive.
- ✓ Ready to see what's on your network right now? Request a free Security Lifecycle Review to gain unprecedented visibility into the threats and risks present in your environment.

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