STRATA™
BY PALO ALTO NETWORKS

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 compute. It must 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.

However, the issue of user identity goes beyond user-based policy and reporting. Protecting user identity is equally important. Phishing and use of stolen credentials were the top two threat action types across the 1,774 breaches investigated for Verizon's 2019 Data Breach Investigations Report.[1] 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:

- **Block access to known phishing sites** via URL Filtering, using the latest global threat intelligence that stops the vast majority of unknown file- and web-based threats instantly, and the rest in seconds, to protect users from attempts to steal their credentials.
- **Stop users from submitting corporate credentials to unknown sites**, protecting them from targeted attacks that use new, unknown phishing sites to go undetected.
- **Allow you to enforce multi-factor 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, including Ping Identity, Okta, RSA, and Duo Security.
- **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.

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 allow access to sanctioned enterprise accounts on SaaS applications, such as Microsoft 365™, while blocking access to unsanctioned accounts, including personal/consumer accounts.

1. "2019 Data Breach Investigations Report," Verizon, May 2019, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.

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.[2] 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 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.

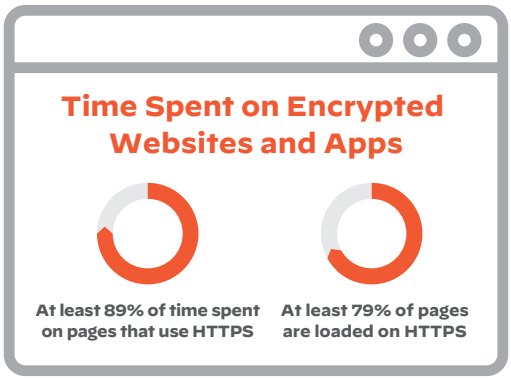

Figure 2: Growing prevalence of web encryption

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.

Threat Prevention

Threat Prevention goes beyond typical intrusion prevention system (IPS) technology to inspect all traffic for threats—regardless of port, protocol, or encryption—and automatically block known vulnerabilities, malware, exploits, spyware, and command and control (C2). Customers can 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.

URL Filtering

URL Filtering protects organizations against web-based threats such as phishing, malware, and command-and-control. Inline machine learning identifies and prevents new and unknown malicious websites instantly, before they can be accessed by users. Web security rules are an extension of your Next-Generation Firewall policy, reducing complexity by giving you a single policy set to manage.

WildFire

WildFire® malware prevention service leverages cloud-based malware detection and multiple analysis techniques to identify and protect against unknown file-based threats while resisting attacker evasion techniques. With its unique real-time signature streaming capability, WildFire ensures your organization is protected against previously unknown threats within seconds after they are first discovered. In an industry first, WildFire deploys inline machine learning modules on your Next-Generation Firewalls to identify as well as prevent new and unknown file-based threats, protecting users before a threat can even enter your network.

DNS Security

DNS Security applies predictive analytics, machine learning, and automation to block attacks that use DNS. Tight

2. "Google Transparency Report: HTTPS encryption on the web," Google, accessed May 2020, https://transparencyreport.google.com/https/overview?hl=en.

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.

IoT Security

IoT Security is the industry's first complete IoT security solution, delivering a machine learning based approach to discover all unmanaged devices, detect behavioral anomalies, recommend policy based on risk, and automate enforcement without the need for additional sensors or infrastructure. 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.

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. 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.

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

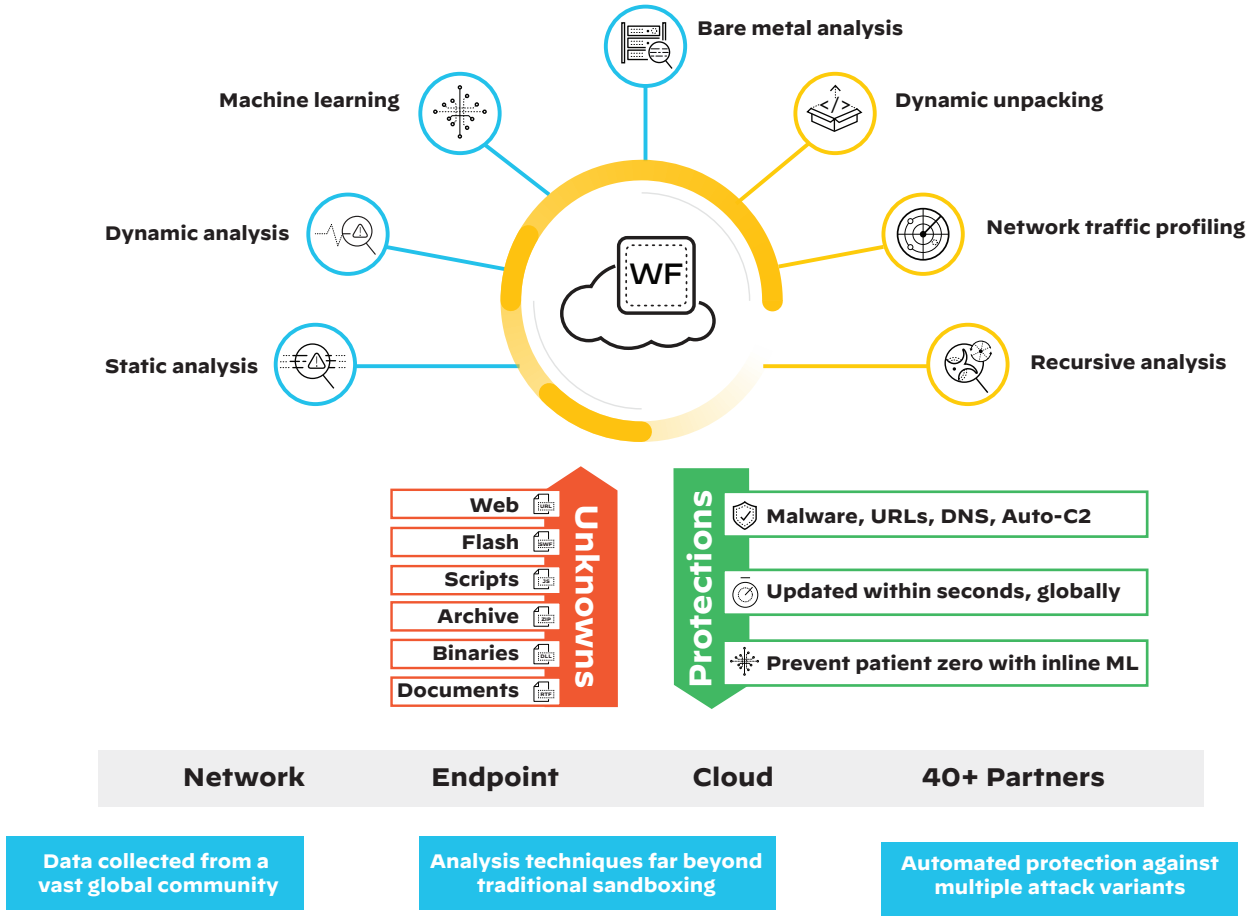

Figure 3: Shared threat intelligence across the ecosystem

WildFire users receive integrated logs, malware analysis reports, and visibility into malicious events through their existing applications, including PAN-OS®, Panorama™ network security management, AutoFocus™ contextual threat intelligence service, Cortex XDR, and Cortex™ XSOAR. This enables security teams to rapidly review reports, correlate observed network events, locate potential threats, investigate, and respond.

In combination with WildFire, organizations can use AutoFocus to home in on the most targeted threats with high relevance and context. AutoFocus enables threat researchers to analyze large amounts of intelligence gathered by WildFire as well as correlate sample data and indicators of compromise (IOCs) with additional human intelligence from our Unit 42 threat research team in the form of tags. Together, WildFire and AutoFocus provide a complete picture of unknown threats targeting your organization and industry, allowing you to track adversary movement, determine attacker intent, and quickly take action.

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 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 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.
- **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 teams are stretched to the limit trying to manage today's complex security deployments. Our Next-Generation Firewalls help by making it easy to manage security as well as visualize and interact with the data. Your administrators can manage individual firewalls through a full-featured, browser-based interface. Whether managing two firewalls or large-scale deployments, you can use Panorama to obtain centralized visibility, edit security policies, and automate actions for all your firewalls in any form factor. The look and feel of Panorama is identical to that of an individual firewall's browser-based interface, making it easy to transition from managing one firewall to managing thousands.

Role-based access control (RBAC) in Panorama, combined with pre- and post-rules, allows you to balance centralized supervision with the need for local policy editing and device configuration flexibility. The Application Command Center (ACC) and log management capabilities create a single pane of glass for actionable visibility across multiple devices, no matter where the devices are deployed. Additional support for standards-based tools, such as Simple Network Management Protocol (SNMP) and REST-based APIs, allows for easy integration with management tools you already use.

When required, the Panorama Interconnect plugin can link multiple Panorama nodes to centralize configuration management and scale your unified view to tens of thousands of firewalls.

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 the 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 as well as 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 as well as 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 by 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 stay ahead of new emerging threats, see and secure your entire enterprise, including IoT, and support speed and error reduction with automatic policy recommendations.

More than 70,000 customers in more than 150 countries have adopted our prevention-focused architecture. 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.
- √ Looking to build a prevention-oriented architecture into your business? Take a Prevention Posture Assessment.
- √ 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

how-palo-alto-networks-next-generation-firewalls-secure-your-business-wp-061120