paloalto NETWORKS

STRATA™
BY PALO ALTO NETWORKS

How Palo Alto Networks Next-Generation Firewalls Secure Your Business

Replace disconnected tools with tightly integrated innovations, automate to focus on what matters, and enforce consistent protection everywhere

The rapid evolution of IT has changed the face of the network perimeter. Data is everywhere, with users accessing it from every location and from all kinds of devices. At the same time, IT teams are adopting cloud, analytics, and automation to accelerate the delivery of new applications and drive business growth. These fundamental shifts have created a threat landscape that exposes weaknesses in legacy security technologies, such as port-based network security, or disparate tools and technologies that are not natively integrated. These tools weren't designed for automation and require analysts to manually stitch together insights from many disconnected sources before acting.

We need a different approach: one that starts with Palo Alto Networks Next-Generation Firewall platform. Our Next-Generation Firewalls offer a prevention-focused architecture that is easy to deploy and operate, using automation to reduce manual effort so your security teams can replace disconnected tools with tightly integrated innovations, automate to focus on what matters, and enforce consistent protection everywhere.

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

Our Next-Generation Firewalls let organizations:

- Securely enable users, content, and applications, including software-as-a-service (SaaS) applications, by classifying all traffic irrespective of port.
- Reduce risk of an attack using a positive enforcement model—allowing all desired applications and blocking everything else.
- Apply security policies to block known vulnerability exploits, viruses, ransomware, spyware, botnets, and other unknown malware, such as advanced persistent threats (APTs).
- Protect data centers, including virtualized data centers, by segmenting data and applications as well as enforcing Zero Trust principles.
- Apply consistent security across your on-premises and cloud environments as well as branch locations.
- Embrace secure mobile computing by extending protections to users and devices, no matter where they are located.
- Get centralized visibility and streamline network security, making vast amounts of data actionable so you can prevent successful cyberattacks.

The following are the key capabilities of our Next-Generation Firewalls that safely enable your business.

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 eliminates the notion of trust. In a Zero Trust world, there are no trusted devices, systems, or people. You identify the data, assets, applications, and services most critical to the business, determine who or what should have access based on their specific job functions, and enforce a least-privileged access model through network segmentation, granular Layer 7 security policy, user access control, and threat prevention.

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.

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. According to Forrester Research, at least 80% of data breaches today involve compromised privileged credentials.[1] Attackers use stolen credentials to gain access to organi-

1. "The Forrester Wave™: Privileged Identity Management, Q4 2018," Forrester, November 14, 2018, https://www.forrester.com/report/The+Forrester+Wave+Privileged+Identity+Management+Q4+2018/-/E-RES141474.

zations' 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 updated every five minutes, 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 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.

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 more than 80% of their time on encrypted websites and applications.[2] Unfortunately, attackers exploit encryption to hide threats from security devices.

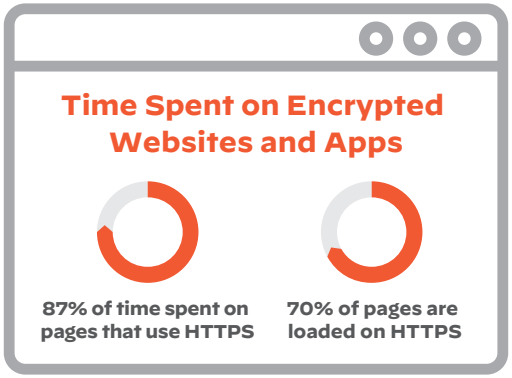

Figure 2: Growing prevalence of web encryption

Our Next-Generation Firewalls use policy-based decryption to allow security professionals to decrypt malicious traffic for the purpose of preventing threats, 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.

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.

Detect and Prevent Advanced Threats

Today, most modern malware, including ransomware variants, makes use of advanced techniques to transport attacks or exploits through network security devices and tools. Our Next-Generation Firewalls identify evasive techniques and automatically counteract them with advanced threat prevention technologies enabled through a single, unified engine:

- Threat Prevention service works with the Next-Generation Firewall to provide intrusion prevention system (IPS) capabilities that block vulnerability exploits, buffer overflows, and port scans; protect against attackers' evasion and obfuscation methods; and provide network anti-malware and command-and-control (C2) protections.

2. "Google Transparency Report: HTTPS encryption on the web," Google, accessed November 12, 2019, https://transparencyreport.google.com/https/overview?hl=en.

- URL Filtering service blocks access to known malware and phishing sites in addition to reducing the risks associated with unauthorized file and data transfers.
- WildFire® malware prevention service uses multiple methods of analysis to detect unknown threats, including static analysis with machine learning, dynamic analysis, and bare metal analysis. Its cloud-based architecture supports threat detection and prevention at mass scale across your network, endpoints, and clouds to stop known and unknown threats.
- DNS Security service applies predictive analytics and machine learning to disrupt attacks that use DNS for C2 or data theft. Tight integration with our Next-Generation Firewalls gives you automated protection and eliminates the need for independent tools.

Shared Threat Intelligence

Organizations rely on multiple sources of threat intelligence to ensure the widest visibility into unknown threats, but they struggle to aggregate, correlate, validate, and share that information to enforce protections across their network. WildFire detects unknown threats with data from a global community and automatically blocks them; AutoFocus™ contextual threat intelligence service provides context, aggregation, and attribution information so security teams can respond more quickly; and Cortex XDR uncovers insider threats and coordinates that information with WildFire.

Moreover, WildFire supports our Next-Generation Firewalls with traffic assessment by analyzing unknown threats and enforcing high-fidelity automated protections across network, mobile, and cloud environments in as few as five minutes.

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.

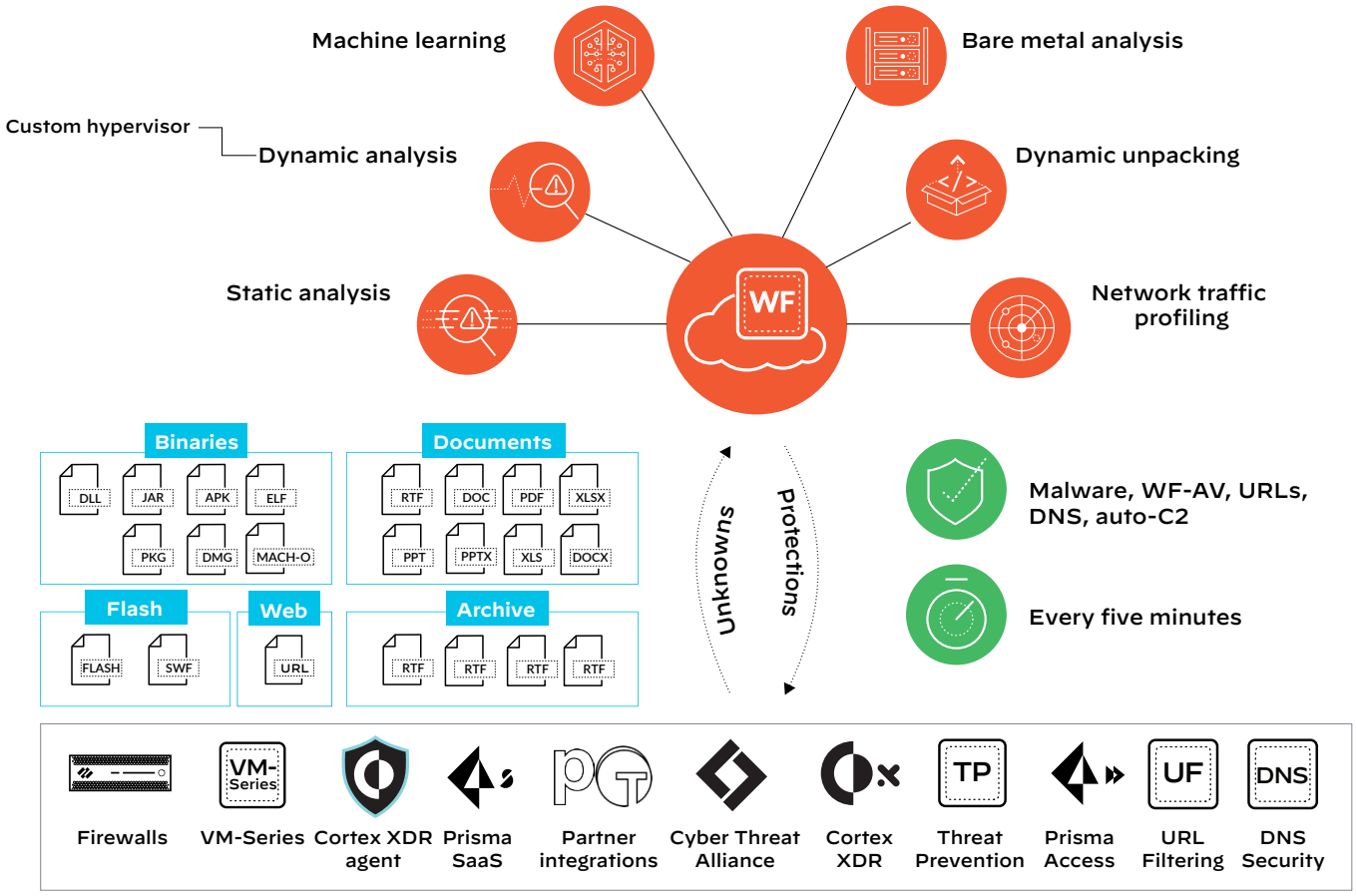

Figure 3: Shared threat intelligence across the ecosystem

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, enabling newly added functions to natively integrate with other functions. This integrated approach offers added security and ease of use 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 Cortex XDR.

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 private and public cloud deployments by segmenting applications and preventing threats.
- Prisma™ Access: Our Next-Generation Firewalls deliver operationally efficient security globally from the cloud through a secure access service edge (SASE) solution.

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. For 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 either interface is identical. 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.

Panorama's role-based access control (RBAC), 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 the standards-based tools, such as Simple Network Management Protocol (SNMP) and REST-based APIs, allow for easy integration with third-party management tools.

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 of your physical and virtual firewalls, cloud, and endpoint data. It is secure, resilient, and scalable, allowing you to stitch together data from across the network, endpoint, and cloud 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 more enterprises embrace digital transformation and move applications to the cloud, IT teams are challenged to connect corporate and remote users to critical business resources quickly, reliably, and securely.

Although software-defined wide area network (SD-WAN) technology promises to increase bandwidth and improve the user experience, organizations must be careful not to compromise security, performance, or simplicity. Palo Alto Networks Next-Generation Firewalls enable IT teams to easily adopt end-to-end SD-WAN architecture with natively integrated, world-class security and connectivity. Using Prisma Access as your SD-WAN hub, you can minimize latency and ensure reliability to optimize the performance of your entire network while delivering an exceptional user experience at your branches.

Palo Alto Networks supports multiple SD-WAN deployment options, including mesh, hub-and-spoke, and cloud-based deployments. You can consume Prisma Access SD-WAN hub as a service or simply enable the SD-WAN subscription on your Next-Generation Firewalls. Our Next-Generation Firewalls can operate as SD-WAN edge devices in the branch and as SD-WAN hubs in central locations, reducing the number of appliances you need. Our physical appliances and Prisma Access also integrate with SD-WAN offerings from vendors such as VeloCloud, CloudGenix, Nuage Networks, Aruba Networks, Viptela, Citrix, Silver Peak Systems, Aryaka Networks, Riverbed Technology, Talari Networks, and Ecessa.

Whatever your deployment model, our tight integration will allow you to manage security and SD-WAN on a single, intuitive interface.

Why Palo Alto Networks Next-Generation Firewalls?

Our Next-Generation Firewalls protect you from credential-based attacks; prevent known and previously unknown threats, including in encrypted traffic; and enable your users to access data and applications based on business requirements. Automation saves you time with security rules that mirror business policy, are easy to maintain, adapt to your dynamic environment, and trigger automated policy-based actions. Available in physical, virtualized, or cloud-delivered form factors, our Next-Generation Firewalls can be managed consistently with Panorama.

Palo Alto Networks Next-Generation Firewalls help organizations rapidly adopt natively integrated security innovations, such as WildFire and Cortex XDR, while sharing data and intelligence across endpoints and cloud.

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.

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-041320