HOW PALO ALTO NETWORKS NEXT-GENERATION FIREWALLS SECURE YOUR BUSINESS

Adopt innovations easily, prevent successful cyberattacks and focus on what matters

The rapid evolution of IT has changed the face of the network perimeter. Data is everywhere, and users are accessing it from everywhere, from all kinds of devices. At the same time, IT teams are adopting cloud, analytics and automation to accelerate delivery of new applications and drive business growth. These fundamental shifts are creating 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 security 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 as the cornerstone of an integrated platform. Our NGFW offers a prevention-focused architecture that is easy to deploy and operate, uses automation to reduce manual effort so your security teams can focus on what matters, and helps you easily adopt new innovations.

The Foundation of the Security Operating Platform

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.

As part of our Security Operating Platform, our NGFWs provide organizations with the ability to:

- Securely enable applications, including software-as-a-service applications, users and content, by classifying all traffic, irrespective of port.
- Reduce risk of an attack using a positive enforcement model – in other words, by 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.

Figure 1: Core elements of network security

- Protect data centers, including virtualized data centers, by segmenting data and applications as well as enforcing the Zero Trust principle.
- Apply consistent security across your on-premises and cloud environments.
- Embrace secure mobile computing by extending the Security Operating Platform 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 NGFW 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. Traditional security models are designed to protect the perimeter while 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 data-centric cybersecurity best practice that removes the assumption of trust and provides a reliable baseline for security. In a Zero Trust world, there are no trusted devices, systems or people. You identify the assets and data that require protection; determine who or what requires access to specific data through a need-to-know, least-privileged access model; define security rules that reflect your business policy; and inspect and log all traffic.

Our NGFWs help with all these steps, 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 to access your critical assets, whether those adversaries are outside or inside your organization.

Identify Users, Protect User Identity

User-ID™ technology enables our NGFWs 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 also define application access policies based on users or groups of users. For example, you can allow only the 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. The 2017 Data Breach Investigations Report by Verizon® found that 81 percent of hacking-related breaches took advantage of weak and/or stolen credentials.[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 NGFW:

- Blocks access to known phishing sites via URL Filtering with PAN-DB, using the latest global threat intelligence updated every five minutes, to protect users from attempts to steal their credentials.
- Stops users from submitting corporate credentials to unknown sites, protecting them from targeted attacks that use new, unknown phishing sites to go undetected.

- Allows you to enforce multi-factor authentication, or 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, as you need to enforce additional authentication mechanisms to control access to critical systems. You can use this capability with the identity vendor of your choice, including Ping Identity®, Okta®, RSA® and Duo Security, so your users' MFA experience stays the same no matter which applications they access.

Safely Enable Applications

Users are accessing diverse types of apps, including software-as-a-service, or SaaS, apps. 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 NGFWs accurately identifies applications in all traffic passing through the network, including applications disguised as authorized traffic as well as those 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® Office 365®, while blocking access to unsanctioned accounts, including personal/consumer accounts.

Secure Encrypted Traffic Without Compromising Privacy

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

Our NGFWs use policy-based decryption to allow security professionals to decrypt malicious traffic for the purpose of preventing threats, while also preserving user privacy and maintaining 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.

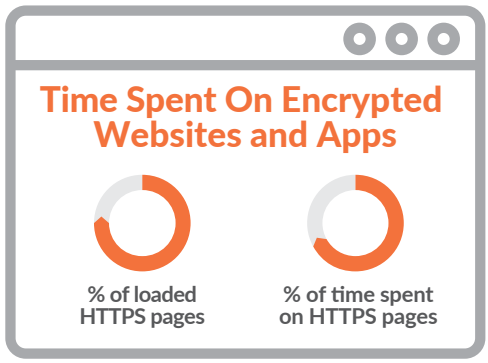

Figure 2: Growing prevalence of web encryption

Support for hardware security modules allows you to manage digital keys securely. Perfect Forward Secrecy ensures the compromise of one encrypted session does not compromise 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. Palo Alto Networks NGFWs identify evasive techniques and automatically counteract them through multiple means:

- Content-ID™ technology delivers an innovative approach based on the complete analysis of all allowed traffic, using multiple advanced threat prevention technologies in a single, unified engine.
- Palo Alto Networks Threat Prevention service works with the NGFW to provide intrusion prevention system capabilities that block vulnerability exploits, buffer overflows and port scans, as well as protect against attackers' evasion and obfuscation methods, while also providing network anti-malware and command-and-control protections.
- Our URL Filtering service blocks access to known malware and phishing download 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.

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. By working with other components of the Security Operating Platform, the NGFW offers further context and more holistic protection. 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 Magnifier™ behavioral analytics detects insider threats and coordinates that information with WildFire.

Moreover, WildFire supports the NGFW in the assessment of traffic by analyzing unknown threats and enforcing high-fidelity automated protections across network, mobile and cloud in as few as five minutes.

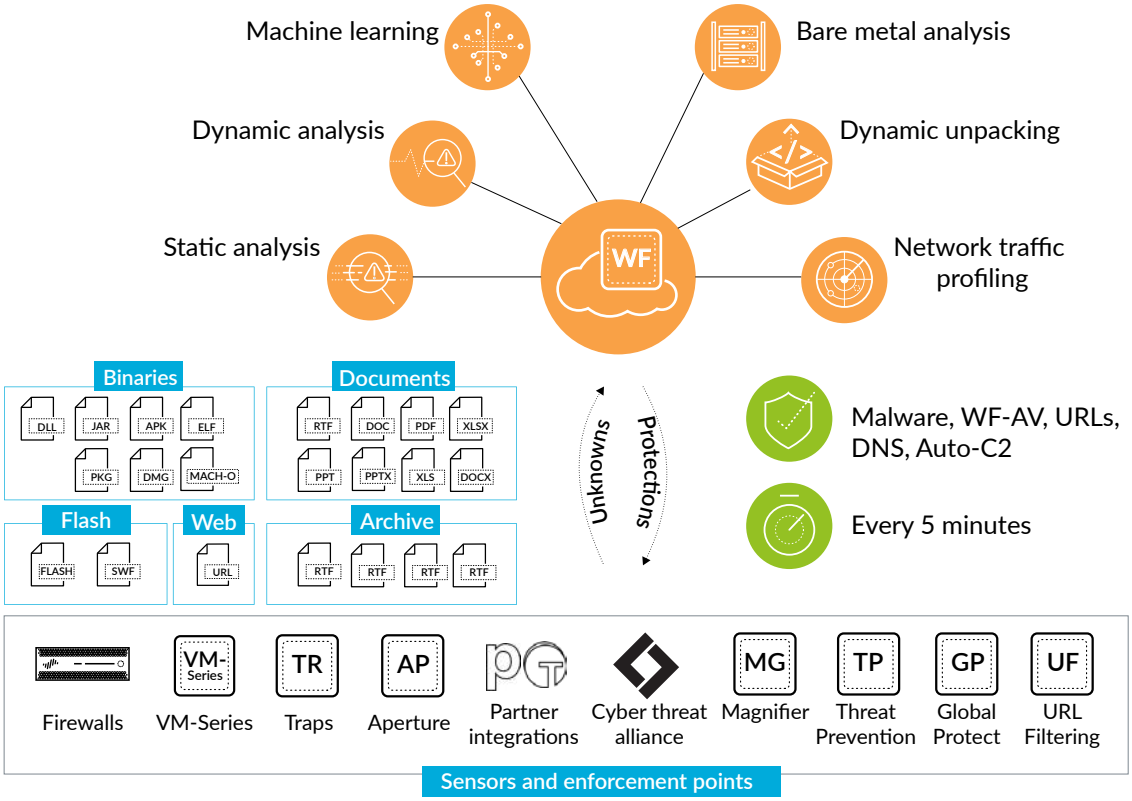

Figure 3: Detect and prevent new threats with WildFire

Single-Pass Architecture

Protection against the evolving threat landscape often requires new security functions to be introduced. Palo Alto Networks NGFWs are built on a single-pass architecture, enabling new functions added to an NGFW 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 a legacy architecture that still works on IP addresses, ports and protocols. Our NGFW performs 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. Its architecture allows us to add innovative, new capabilities easily, as we've already done with WildFire and, more recently, Magnifier.

If a customer's NGFW 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 returned to the customer in Singapore as well as all other WildFire customers worldwide.

Flexible Deployment

Our NGFWs can be deployed in multiple form factors:

- Hardware: A blend of power, intelligence, simplicity and versatility protects enterprise and service provider deployments at headquarters, data centers and branches.
- VM-Series: Our virtualized next-generation firewall protects your private and public cloud deployments by segmenting applications and preventing threats.
- GlobalProtect cloud service: Our next-generation firewall delivers operationally efficient security globally from the cloud through GlobalProtect™ network security for endpoints.

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. The Security Operating Platform helps by making it easy to manage security as well as visualize and interact with the data. Individual firewalls can be managed 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, combined with pre- and post-rules, allows you to balance central supervision with the need for local policy editing and device configuration flexibility. The Application Command Center 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 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 Security Operating Platform provides:

- **Logging:** Palo Alto Networks goes beyond traditional processing and listing events. You can view logs in ways that make sense, including graphs, maps, trend charts and more, to interpret network data. The automated correlation engine eliminates manual correlation tasks and surfaces threats that would otherwise go unnoticed because of the noise. You can also forward logs using any filtering criteria to create workflows that can automate actions within our Security Operating Platform or third-party systems. You have the flexibility to aggregate logs on-premises or in the cloud-based Logging Service.
- **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.

Why Palo Alto Networks NGFW?

Our NGFWs enable your users to access data and applications based on business requirements, protect you from credential-based attacks, and prevent known and previously unknown threats, including in encrypted traffic. 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 NGFWs are managed consistently with Panorama.

As part of the Security Operating Platform, Palo Alto Networks next-generation firewalls help organizations rapidly adopt natively integrated security innovations, such as WildFire and Magnifier, while sharing data and intelligence across endpoints and cloud.

Figure 4: Palo Alto Networks Security Operating Platform

More than 54,000 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 Enterprise Network Firewalls seven times in a row and 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 NGFWs? Visit our network security overview page.
- ✓ Ready to test-drive our NGFWs? Take an Ultimate Test Drive.
- ✓ Looking to build a prevention-oriented architecture into your business? Take your Prevention Posture Assessment.
- ✓ Ready to take full advantage of the features and tools you need to protect your business? Sign up for a Best Practice Assessment.

1. Verizon Communications. "2017 Data Breach Investigations Report," July 26, 2017. https://www.knowbe4.com/hubfs/rp_DBIR_2017_Report_execsummary_en_xg.pdf
2. Google, Inc. "Google Transparency Report: HTTPS encryption on the web," Accessed September 6, 2018. https://transparencyreport.google.com/https/overview?hl=en