FIREWALL OVERVIEW

Palo Alto Networks Next-Generation Firewall

Fundamental shifts in application usage, user behavior, and complex, convoluted network infrastructure create a threat landscape that exposes weaknesses in traditional port-based network security. Your users want access to an increasing number of applications, operating across a wide range of device types, often with little regard for the business or security risks. Meanwhile, data center expansion, network segmentation, virtualization, and mobility initiatives are forcing you to rethink how to enable access to applications and data, while protecting your network from a new, more sophisticated class of advanced threats that evade traditional security mechanisms.

Historically, you were left with two basic choices – either block everything in the interest of network security, or enable everything in the interest of your business. These choices left little room for compromise. The Palo Alto Networks® Next-Generation Security Platform provides you with a way to safely enable the applications your users need by allowing access while preventing cybersecurity threats.

Our Next-Generation Firewall is the core of the Next-Generation Security Platform, designed from the ground up to address the most sophisticated threats. The Next-Generation Firewall inspects all traffic - inclusive of applications, threats and content – and ties it to the user, regardless of location or device type. The application, content and user – the elements that run your business – become integral components of your enterprise security policy. The result is the ability to align security with your key business initiatives. With our Next-Generation Security Platform, you reduce response times to incidents, discover unknown threats, and streamline security network deployment.

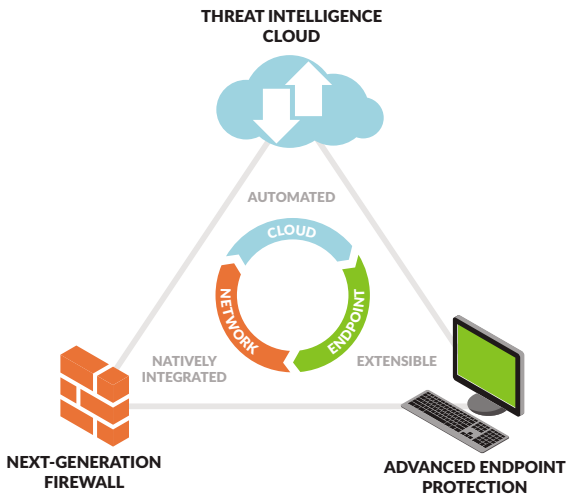

Figure 1: Palo Alto Networks Next-Generation Security Platform

- Safely enable applications, users, and content by classifying all traffic, determining the business use case, and assigning policies to allow and protect access to relevant applications, including software-as-a-service (SaaS) applications.
- Prevent threats by eliminating unwanted applications to reduce your threat footprint and apply targeted security polices to block known vulnerability exploits, viruses, spyware, botnets and unknown malware (APTs).
- Protect your data centers through the validation of applications, isolation of data, control over rogue applications and high-speed threat prevention.
- Secure public and private cloud computing environments with increased visibility and control; deploy, enforce and maintain security policies at the same pace as your virtual machines.
- Embrace safe mobile computing by extending the Next-Generation Security Platform to users and devices no matter where they are located.

- Streamline device, network and policy management with intuitive management features to match your organizational structure.

The Next-Generation Security Platform helps your organization address a spectrum of security requirements based upon a common principle. By using a balanced combination of network security with global threat intelligence and endpoint protection, your organization can support business initiatives while improving your overall security posture, and reducing security-incident response time.

Using Security to Empower Your Business

Our Next-Generation Security Platform allows you to empower your business with policies that revolve around applications, users and content. It uses a positive control model, a design unique to our platform that permits you to enable specific applications or functions and block all else (implicitly or explicitly). The Next-Generation Firewall performs a full stack, single pass inspection of all traffic across all ports, thus providing complete context of the application, associated content, and user identity as the basis for your security policy decisions.

- Classify all traffic, across all ports, all the time. Today, applications and their associated content can easily bypass a port-based firewall using a variety of techniques. Our Next-Generation Security Platform natively applies multiple classification mechanisms to the traffic stream to identify applications, threats and malware. All traffic is classified, regardless of port, encryption (SSL or SSH), or evasive techniques employed. Unidentified applications – typically a small percentage of traffic, yet high in potential risk – are automatically categorized for systematic management.
- Reduce the threat footprint; prevent cyberattacks. Once traffic is fully classified, you can reduce the network threat footprint by allowing specific applications and denying all others. Coordinated cyberattack prevention can then be applied to block known malware sites and prevent vulnerability exploits, viruses, spyware and malicious DNS queries. Any custom or unknown malware is analyzed and identified by executing the files and directly observing their malicious behavior in a virtualized sandbox environment. When new malware is discovered, a signature for the infecting file and related malware traffic is automatically generated and delivered to you.
- Map application traffic and associated threats to users and devices. To improve your security posture and reduce incident response times, it's critical to map application usage to user and device type – and be able to apply that context to your security policies. Integration with a wide range of enterprise user repositories provides

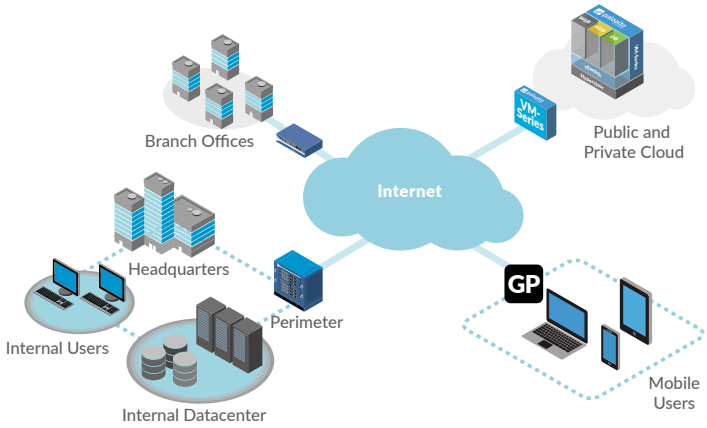

Figure 1: Deploy safe enablement policies accross the entire organization

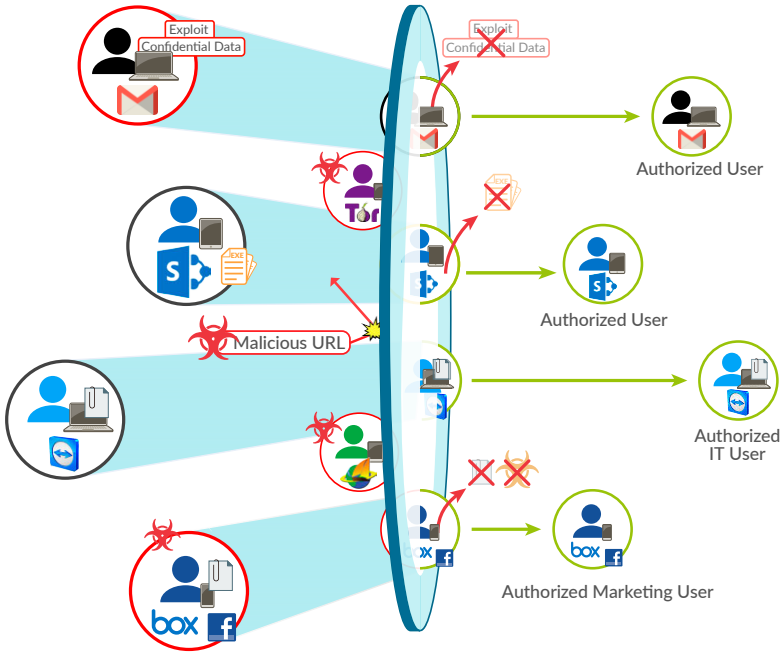

Figure 2: Applications, content, users and devices – all under your control

Figure 3: View application activity in a clear, easy-to-read format. Add and remove filters to learn more about the application, its functions and who is using them

the identity of the Microsoft® Windows®, Mac® OS X®, Linux®, Android®, or iOS user and device accessing the application. The combined visibility and control over both users and devices means you can safely enable the use of any application traversing your network, no matter where the user is or the type of device being used.

Establishing the context of the specific applications in use, the content or threat they may carry, and the associated user or device helps you streamline policy management, improve your security posture, and accelerate incident investigation.

Complete Context Means Tighter Security Policies

Security best practices dictate that the decisions you make regarding policies, your ability to report on network activity, and your forensics capacity depend on context. The context of the application in use, the website visited, the associated payload, and the user are all valuable data points in your effort to protect your network. When you know exactly which applications are traversing your Internet gateway, operating within your data center or cloud environment, or being used by remote users, you can apply specific policies to those applications, complete with coordinated threat protection. The knowledge of who the user is, not just their IP address, adds another contextual element that empowers you to be more granular in your policy assignment.

A rich set of highly interactive visualization and log filtering tools provides you with the context of the application activity, the associated content or threat, who the user is, and on what type of device. Each of these data points by itself paints a partial picture of your network, yet when taken in complete context provides a full view of the potential security risk, allowing you to make more-informed policy decisions. All traffic is continuously classified. As the state changes, the changes are logged for analysis, and the graphical summaries are dynamically updated, displaying the information in an easy-to-use, web-based interface.

- At the Internet gateway, you can investigate new or unfamiliar applications to quickly see a description of the application, its behavioral characteristics, and who is using it. Additional visibility into URL categories, threats, and data patterns provides a more well-rounded picture of network traffic traversing the gateway.
- All files analyzed for unknown malware by WildFire™ are logged on-box with full access to details, including the application used, the user, the file type, target OS and malicious behaviors observed.
- Within the data center, verify all applications under use, and ensure that they are only being used by authorized users. Added visibility into data center activity can confirm that there are no misconfigured applications or rogue uses of SSH or RDP.
- Threat analysis, forensics and hunting workflows are accelerated with the AutoFocus™ threat intelligence service, providing unique contextual threat data directly in PAN-OS® from the device.
- In public and private cloud environments, enforce policy and protect applications with the Next-Generation Security Platform while keeping pace with the creation and movement of your virtual servers.
- Across all deployment scenarios, unknown applications – typically a small percentage on every network – can be categorized for analysis and systematic management.

In many cases, you may not be fully aware of which applications are in use, how heavily they are used, or by whom. Complete visibility into the business-relevant aspects of your network traffic – the application, the content and the user – is the first step toward more-informed policy control.

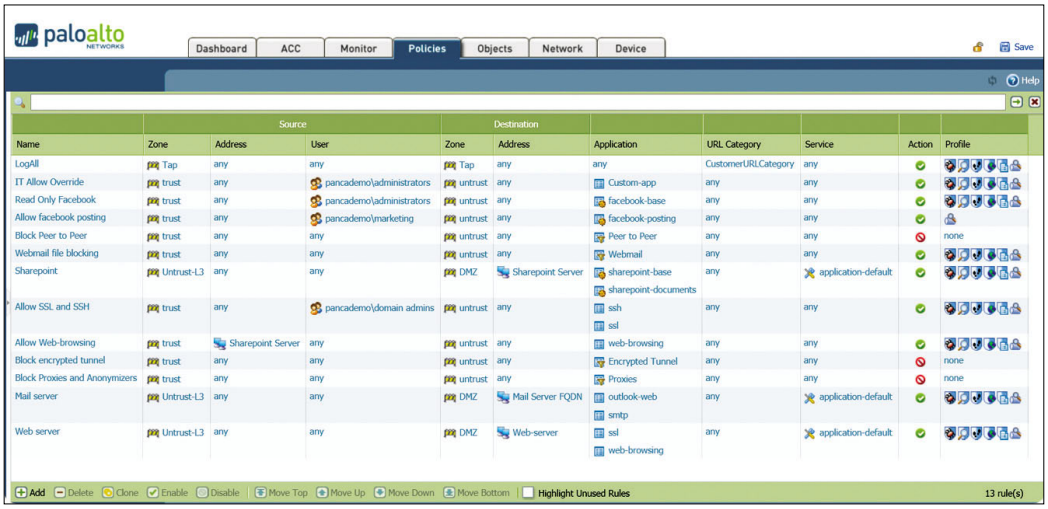

Figure 4: Unified policy editor enables the rapid creation and deployment of policies that control applications, users and content

Reducing Risk by Enabling Applications

Traditionally, the process of reducing risk meant that you had to limit access to network services and possibly hinder your business. Today, risk reduction means safely enabling applications using a business-centric approach that helps you strike a balance between the traditional deny-everything approach and the allow-all approach.

- Use application groups and SSL decryption to limit webmail and instant messaging to a few specific application variants; inspect them for all threats and upload unknown suspect files (EXE, DLL, ZIP files, PDF documents, office documents, Java®, and Android® APK) to WildFire for analysis and signature development.
- Control web-surfing for all users by allowing and scanning traffic to business-related websites and blocking access to obvious non-work related websites; "coach" access to questionable sites through customized block pages.
- Explicitly block all peer-to-peer file transfer applications for all users using dynamic application filters.
- Understand SaaS application usage in your organization, establish granular access and usage controls for each application, and prevent the delivery of malware through these applications.
- Embrace mobile devices by extending your Internet gateway policies and threat prevention capabilities to remote users with GlobalProtect™ mobile security service.

In the data center, use context to confirm that your data center applications are running on their standard ports, find rogue applications, validate users, isolate data, and protect business-critical data from threats. Examples may include:

- Using security zones, isolate the credit card number repository based on Oracle® forcing the Oracle traffic across its standard ports while inspecting the traffic for inbound threats and limiting access only to the finance group.
- Create a remote management application group (e.g., SSH, RDP, Telnet) for only the IT department to use within the data center.
- In your virtual data center, use dynamic objects to help automate security policy creation as SharePoint® virtual machines are established, taken down, or travel across your virtual environment.

Protecting Enabled Applications and Content

When you apply threat prevention and content scanning policies, the context of the application and the user become integral components of your security policy. Full context within your threat prevention policies neutralizes evasion tactics such as port-hopping and tunneling. Reduce the threat target surface area by enabling a select set of applications, and then apply threat prevention and content scanning policies to that traffic.

Threat protection and content scanning elements available within your policies include:

- **Prevent known threats using IPS and network antivirus/anti-spyware.** Protection from a range of known threats is accomplished with single pass inspection using a uniform signature format and a stream-based scanning engine. Intrusion prevention system (IPS) features block network and application layer vulnerability exploits, buffer overflows, DoS attacks and port scans. Antivirus/anti-spyware protection blocks millions of malware variants, including those hidden within compressed files or web traffic (compressed HTTP/HTTPS), as well as known PDF viruses. For traffic encrypted with SSL, you can selectively apply policy-based decryption and then inspect the traffic for threats, regardless of port.
- **Block unknown or targeted malware with WildFire.** Unknown or targeted malware (e.g., advanced persistent threats) hidden within files can be identified and analyzed by WildFire across multiple operating systems and application versions which directly observes and executes unknown files in a virtualized sandbox environment in the cloud or on the WF-500 appliance. WildFire monitors more than 420 malicious behaviors and, if malware is found, a signature is automatically developed and delivered to you in as little as 5 minutes. All major file types are supported by WildFire including: PE files; Microsoft Office .doc, .xls, and .ppt; Portable Document Format (PDF); Java Applet

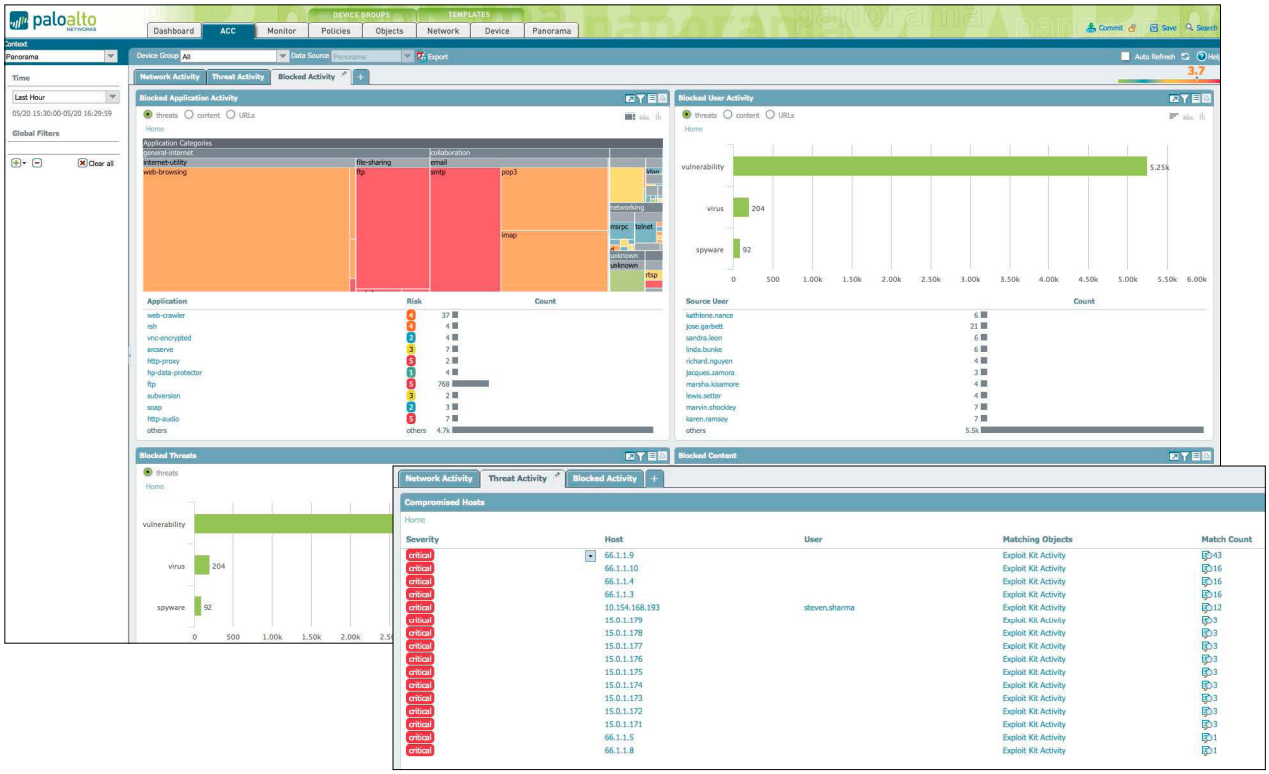

Figure 5: Content and threat visibility – view URL, threat and file/data transfer activity as well as compromised hosts in a clear, easy-to-read format that is highly customizable. Add and remove filters to learn more about individual elements

(jar and class); and Android Application Package (APK). In addition, WildFire analyzes links in email to stop spear phishing attacks.

- **Identify bot-infected hosts and disrupt network activity from malware.** Complete, contextual classification of all applications, across all ports, including any unknown traffic, can often expose anomalies or threats in your network. Use command and control App-ID™, behavioral botnet report, DNS sinkholing, and passive DNS to quickly correlate unknown traffic, suspicious DNS, and URL queries with infected hosts. Apply global intelligence to intercept and sinkhole DNS queries for malicious domains.
- **Limit unauthorized file and data transfers.** Data filtering features enable your administrators to implement policies that will reduce the risks associated with unauthorized file and data transfers. File transfers can be controlled by looking inside the file (as opposed to looking only at the file extension) to determine if the transfer action should be allowed or not. Executable files, typically found in drive-by downloads, can be blocked, thereby protecting your network from unseen malware propagation. Data filtering features can detect and control the flow of confidential data patterns (credit card or Social Security numbers, as well as custom patterns).
- **Control web surfing.** A fully integrated, customizable URL filtering engine allows your administrators to apply granular web-browsing policies, complementing application visibility and control policies that safeguard the enterprise from a full spectrum of legal regulatory, and productivity risks.
- **Device-based policy for application access.** Using GlobalProtect, an organization can set specific policies to control which devices can access particular applications and network resources. For example, ensure that laptops are compliant with the corporate image before allowing access to the data center. Check if the mobile device is up to date, corporate-owned, and fully patched before accessing sensitive data.
- **Automatically confirm compromised hosts.** An automated correlation engine looks for predefined indicators of compromise network-wide, correlates matches, and automatically highlights compromised hosts, reducing the need for manual data mining.

Network Security Management

The Next-Generation Security Platform can be managed individually via a command-line interface (CLI) or through a full-featured browser-based interface. For large-scale deployments, you can use Panorama™ to globally deliver visibility, policy editing, reporting, and logging features for all of your hardware and virtual appliance firewalls. Panorama provides you the same level of contextual control over your global deployment as you have over a single appliance.

Role-based administration, combined with pre- and post-rules, allows you to balance centralized control with the need

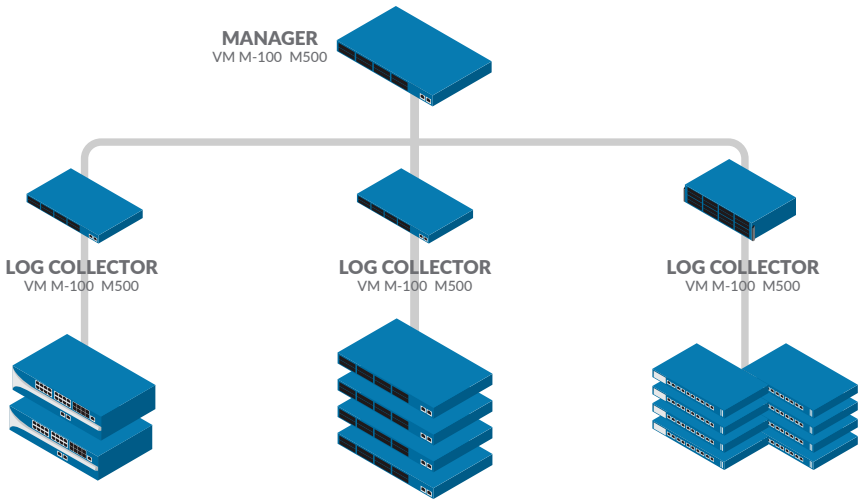

Figure 6: Panorama can be deployed on a dedicated appliance or in a distributed manner to maximize scalability

for local policy editing and device configuration flexibility. Whether using the device's web interface or the Panorama one, the interface look and feel is identical, ensuring that there is no learning curve when moving from one to another. Your administrators can use any of the provided interfaces to make changes at any time without needing to worry about synchronization issues. Additional support for standards-based tools, such as SNMP and REST-based APIs, allows you to integrate with third-party management tools.

Reporting and Logging

Security best practice means striking a balance between ongoing management efforts and being reactive, which may involve investigating and analyzing security incidents or generating day-to-day reports.

- **Reporting:** Predefined reports can be used as-is, customized, or grouped together as one report in order to suit the specific requirements. All reports can be exported to CSV or PDF format and can be executed and emailed on a scheduled basis.
- **Logging:** Real-time log filtering facilitates rapid forensic investigation into every session traversing your network. Complete context of the application, the content – including malware detected by WildFire – and the user can be used as a filter criteria, and the results can be exported to a CSV file or sent to a syslog server for offline archiving or additional analysis. Logs that have been aggregated by Panorama can also be sent to a syslog server for added analysis or archival purposes.
- **Threat hunting:** Threat intelligence from the AutoFocus service is made directly accessible in PAN-OS, speeding threat analysis and hunting workflows, without additional specialized resources. When further analysis is required, users can sweep between AutoFocus and PAN-OS, with pre-populated searches for both systems.

In addition to the reporting and logging capabilities provided by the Palo Alto Networks Next-Generation Security Platform, integration is available with third-party SIEM tools, such as Splunk® for Palo Alto Networks. These tools provide further reporting and data visualization capabilities, and they enable you to correlate security events across multiple systems in your enterprise.

Purpose-Built Hardware or Virtualized Platforms

Our Next-Generation Firewall is available in either a purpose-built hardware platform that scales from an enterprise branch office to a high-speed data center or in a virtualized form factor to support your cloud-based computing initiatives. We support the broadest range of virtual platforms to cover your diverse, virtualized data center and public and private cloud requirements. The VM-Series firewall platform is available for VMware® ESXi™, NSX™, Citrix® SDX™, Microsoft Hyper-V®, Amazon® Web Services (AWS), Microsoft Azure™, and KVM hypervisors. When you deploy our platforms in either hardware or virtual form factors, you can use Panorama for centralized management.

paloalto NETWORKS®

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com