Next-Generation Firewall Overview

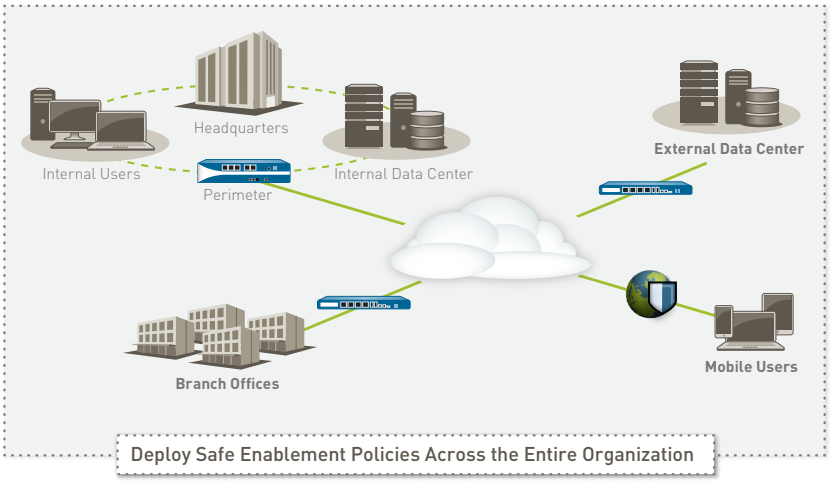
Fundamental shifts in the application and threat landscape, user behavior, and network infrastructure have steadily eroded the security that traditional port-based firewalls once provided. Your users are accessing all types of applications using a range of device types, often times to get their job done. Meanwhile, datacenter expansion, virtualization, mobility, and cloud-based initiatives are forcing you to re-think how to enable application access yet protect your network.

Traditional responses include an attempt to lock down all application traffic through an ever-growing list of point technologies in addition to the firewall, which may hinder your business; or allowing all applications, which is equally unacceptable due to increased business and security risks. The challenge that you face is that your traditional port-based firewall, even with bolt-on application blocking, does not provide an alternative to either approach. In order to strike a balance between allowing everything and denying everything, you need to safely enable applications by using business-relevant elements such as the application identity, who is using the application, and the type of content as key firewall security policy criteria.

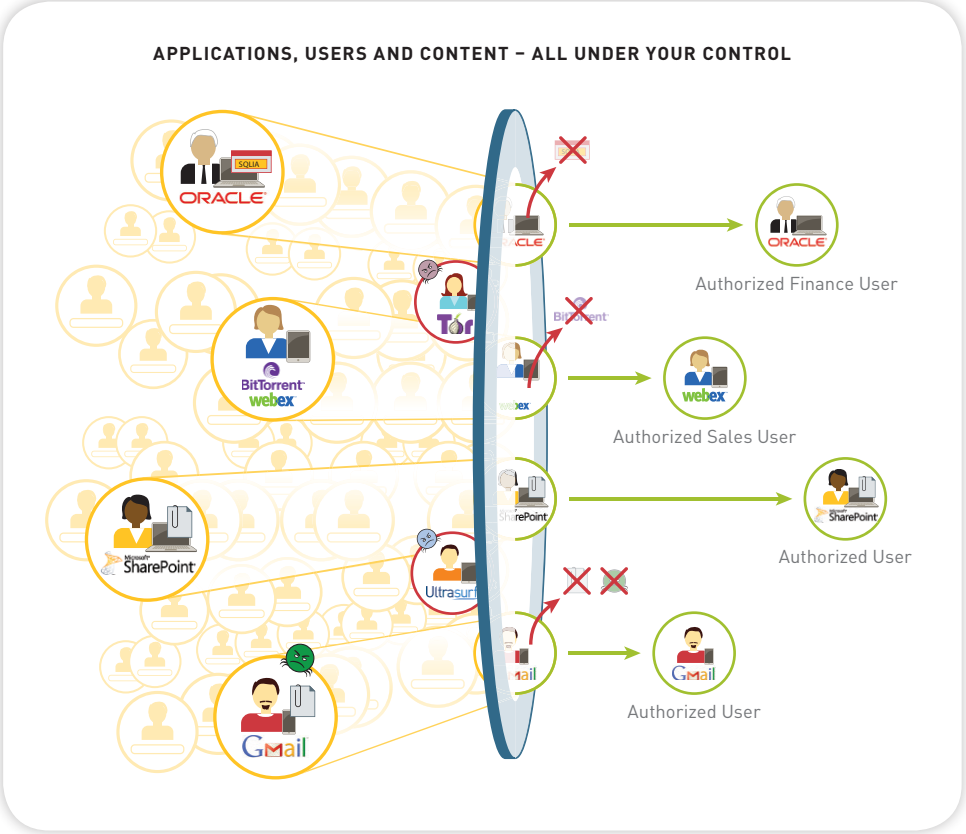
Key safe enablement requirements:

- **Identify applications, not ports.** Classify traffic, as soon as it hits the firewall, to determine the application identity, irrespective of protocol, encryption, or evasive tactic. Then use that identity as the basis for all security policies.
- **Tie application usage to user identity, not IP address, regardless of location or device.** Employ user and group information from enterprise directories and other user stores to deploy consistent enablement policies for all your users, regardless of location or device.
- **Protest against all threats—both known and unknown.** Prevent known vulnerability exploits, malware, spyware, malicious URLs while analyzing traffic for, and automatically delivering protection against highly targeted and previously unknown malware.
- **Simplify policy management.** Safely enable applications and reduce administrative efforts with easy-to-use graphical tools, a unified policy editor, templates, and device groups.

Safe application enablement policies can help you improve your security posture, regardless of the deployment location. At the perimeter, you can reduce your threat footprint by blocking a wide range of unwanted applications and then inspecting the allowed applications for threats—both known and unknown. In the datacenter – traditional or virtualized, application enablement translates to ensuring only datacenter applications are in use by authorized users, protecting the content from threats and addressing security challenges introduced by the dynamic nature of the virtual infrastructure. Your enterprise branch offices and remote users can be protected by the same set of enablement policies deployed at the headquarters location, thereby ensuring policy consistency.



paloalto NETWORKS
the network security company™



Enabling Applications to Empower the Business

Safe application enablement with Palo Alto Networks™ next-generation firewalls helps you address your business and security risks associated with the rapidly growing number of applications traversing your network. By enabling applications for users or groups of users, both local, mobile, and remote, and protecting the traffic against known and unknown threats, you can improve your security posture while growing your business.

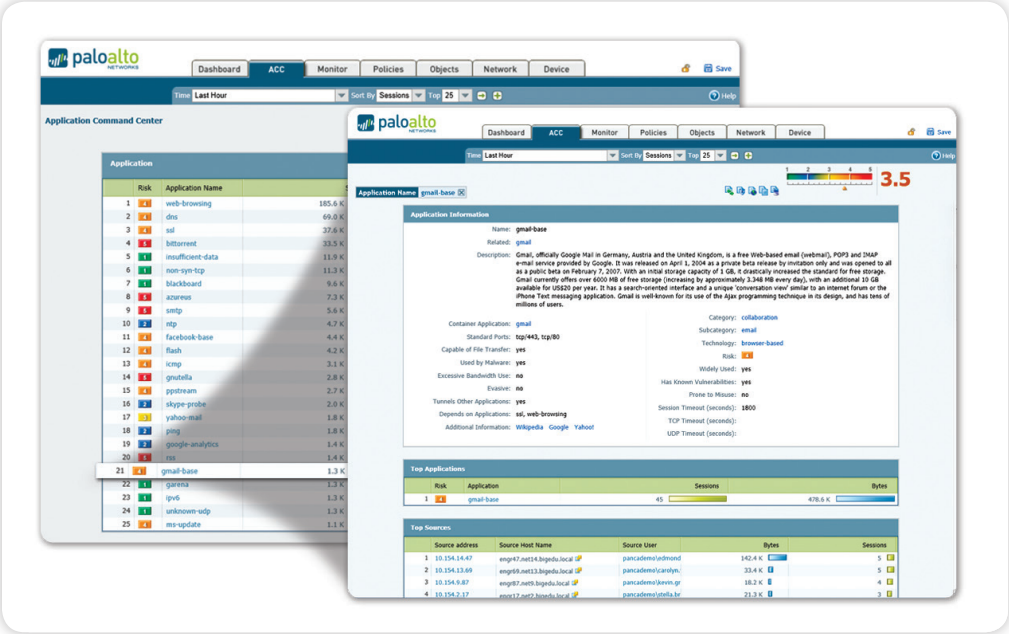
- **Classifying all applications, across all ports, all the time.** Accurate traffic classification is the heart of any firewall, with the result becoming the basis of the security policy. Today, applications can easily bypass a port-based firewall; hopping ports, using SSL and SSH, sneaking across port 80, or using non-standard ports. App-ID™ addresses the traffic classification visibility limitations that plague traditional firewalls by applying multiple classification mechanisms to the traffic stream, as soon as the firewall sees it, to determine the exact identity of application traversing your network, regardless of port, encryption (SSL or SSH) or evasive technique employed. The knowledge of exactly which applications are traversing your network, not just the port and protocol, becomes the basis for all your security policy decisions. Unidentified applications, typically a small percentage of traffic, yet high in potential risk, are automatically categorized for systematic management—which can include policy control and inspection, threat forensics, creation of a custom App-ID, or a packet capture for Palo Alto Networks App-ID development.

- **Integrating users and devices, not just IP addresses into policies**. Creating and managing security policies based on the application and the identity of the user, regardless of device or location, is a more effective means of protecting your network than relying solely on port and IP address. Integration with a wide range of enterprise user repositories provides the identity of the Microsoft Windows, Mac OS X, Linux, Android, or iOS user accessing the application. Users who are traveling or working remotely are seamlessly protected with the same, consistent policies that are in use on the local, or corporate network. The combined visibility and control over a user's application activity means you can safely enable the use of Oracle, BitTorrent, or Gmail, or any other application traversing your network, no matter where or how the user is accessing it.

- **Protect against all threats, both known and unknown.** To protect today's modern network, you must address a blend of known exploits, malware and spyware as well as completely unknown and targeted threats. This process begins by reducing the network attack surface by allowing specific applications and denying all others, either implicitly through a deny-all-else strategy or through explicit policies. Coordinated threat prevention can then be applied to all allowed traffic, blocking known malware sites, vulnerability exploits, viruses, spyware and malicious DNS queries in a single pass. Custom or otherwise unknown malware is actively analyzed and identified by executing the unknown files and directly observing more than 100 malicious behaviors 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. All threat prevention analysis uses full application and protocol context, ensuring that threats are always caught even if they attempt to hide from security in tunnels, compressed content or on non-standard ports.

Deployment and Management Flexibility

Safe application enablement functionality is available in either a purpose-built hardware platform or in a virtualized form factor. When you deploy multiple Palo Alto Networks firewalls, in either hardware or virtual form factors, you can use Panorama, an optional centralized management offering to gain visibility into traffic patterns, deploy policies, generate reports and deliver content updates from a central location.



Application Visibility: 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.

Safe Application Enablement: A Comprehensive Approach

Safe application requires a comprehensive approach to securing your network and growing your business that begins with in-depth knowledge of the applications on your network; who the user is, regardless of their platform or location; what content, if any, the application is carrying. With more complete knowledge of network activity, you can create more meaningful security policies that are based on elements of application, user and content that are relevant to your business. The user location, their platform and where the policy is deployed—perimeter, traditional or virtualized datacenter, branch office or remote user—make little or no difference to how the policy is created. You can now safely enable any application, any user, and any content.

Complete Knowledge Means Tighter Security Policies

Security best practices dictate that more complete knowledge of what's on your network is beneficial to implementing tighter security policies. For example, knowing exactly which applications are traversing your network, as opposed to the broader set of traffic that is port-based, enables your administrators to specifically allow the applications that enable your business while blocking, unwanted applications. The knowledge of who the user is, not just their IP address, adds another policy criteria that allows you to be more specific in your policy assignment.

- Using a powerful set of graphical visualization tools, your administrators can gain a more complete picture of the application activity, the potential security impact, and make a more informed policy decision. Applications are continuously classified and as their state changes, the graphical summaries are dynamically updated, displaying the information in an easy-to-use, web-based interface.
- New or unfamiliar applications can be quickly investigated with a single click that displays a description of the application, its behavioral characteristics, and who is using it.
- Additional visibility into URL categories, threats, and data patterns provides a complete and well-rounded picture of network activity.
- Unknown applications, typically a small percentage on every network, yet high in potential risk, are categorized for analysis to determine if they are internal applications, as yet unidentified commercial applications, or threats.

Enabling Applications and Reducing Risk

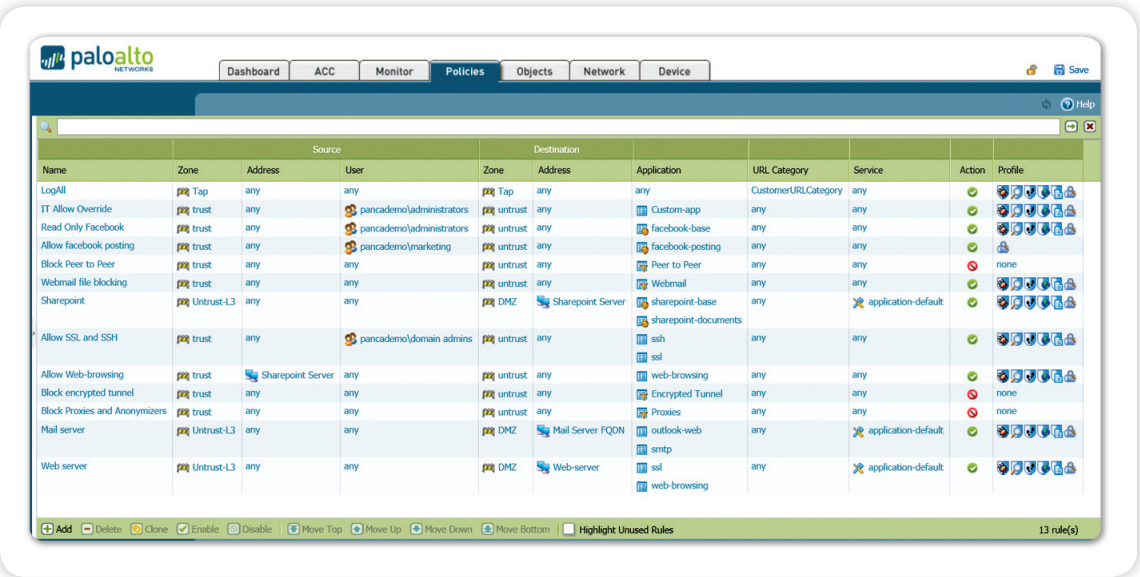
Safe application enablement uses policy decision criteria that includes application/application function, users and groups, and content as a means of striking a balance between business limiting denying of all applications and the high risk alternative of allowing all applications.

At the perimeter, including branch offices, mobile, and remote users, enablement policies are focused on identifying all the traffic, then selectively allowing the traffic based on user identity; then scanning the traffic for threats. Policy examples may include:

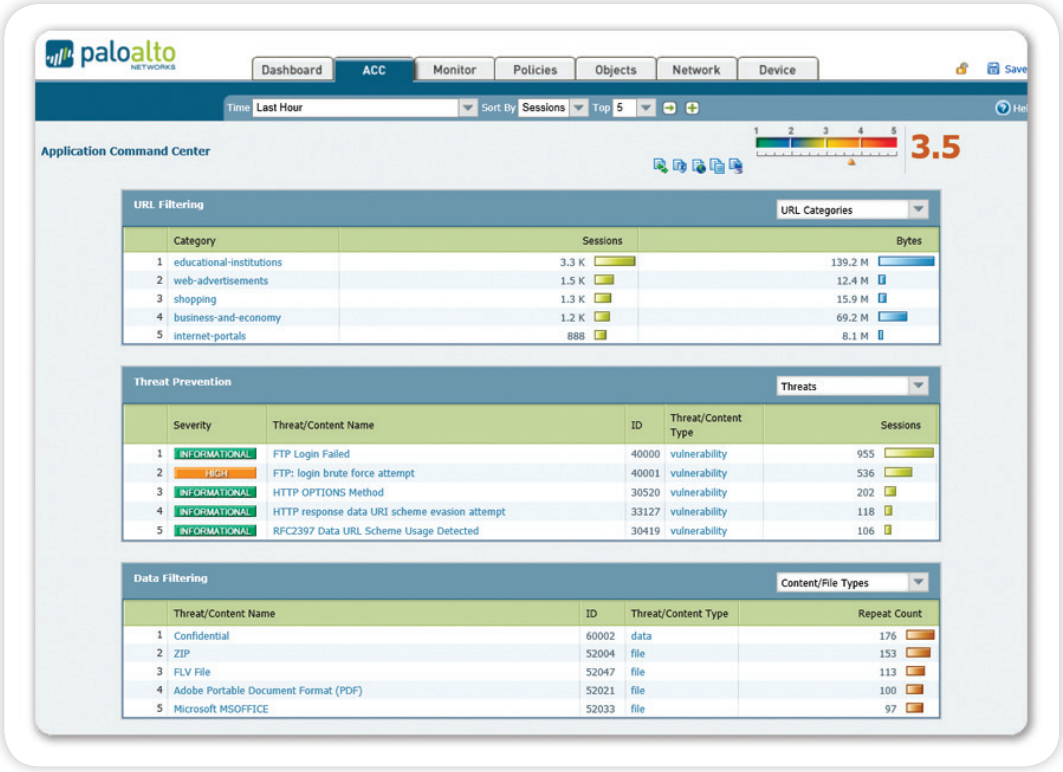
- Limit the use of webmail and instant messaging usage to a select few variants; decrypt those that use SSL, inspect the traffic for exploits and upload unknown files to WildFire™ for analysis and signature development.
- Allow streaming media applications and websites but apply QoS and malware prevention to limit the impact on VoIP applications and protect your network.
- Control Facebook by allowing all your users to "browse", blocking all Facebook games and social plugins; and allowing Facebook posting only for marketing. Scan all Facebook traffic for malware and exploits
- Control web-surfing by allowing and scanning traffic to business related web sites while blocking access to obvious non-work related web sites; "coach" access to questionable sites through customized block pages.
- Enforce consistant security by transparently deploying the same policies to all users, local, mobile, or remote, with GlobalProtect™.
- Use an implicit deny-all-else strategy or explicitly block unwanted applications such as P2P and circumventors or traffic from specific countries to reduce the application traffic that introduces business and security risk.

In the datacenter—traditional, virtualized or a combination thereof—enablement examples are focused on confirming applications, looking for rogue applications, and protecting the data.

- Isolate the Oracle-based credit card number repository in its own security zone; control access to finance groups, forcing the traffic across its standard ports, and inspecting the traffic for application vulnerabilities.
- Enable only the IT group to access the datacenter using a fixed set of remote management applications (e.g., SSH, RDP, Telnet) across their standard ports.
- Allow Microsoft SharePoint Administration to be used by only your administration team, and allow access to Microsoft SharePoint Documents for all other users.



Unified Policy Editor: A familiar look and feel enables the rapid creation and deployment of policies that control applications, users and content.



Content and Threat Visibility: View URL, threat and file/data transfer activity in a clear, easy-to-read format. Add and remove filters to learn more about individual elements.

Protecting Enabled Applications

Safe application enablement means allowing access to certain applications, then applying specific policies to block known exploits, malware and spyware – known or unknown; controlling file or data transfer, and web surfing activity. Common threat evasion tactics such as port-hopping and tunneling are addressed by executing threat prevention policies using the application and protocol context generated by the decoders in App-ID. In contrast, UTM solutions take a silo-based approach to threat prevention, with each function, firewall, IPS, AV, URL filtering, all scanning traffic without sharing any context, making them more susceptible to evasive behavior.

- **Block Known Threats: IPS and Network Antivirus/Anti-spyware.** A uniform signature format and a stream-based scanning engine enables you to protect your network from a broad range of threats. 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, as well as any malware-generated command-and-control traffic, PDF viruses, and malware hidden within compressed files or web traffic (compressed HTTP/HTTPS). Policy-based SSL decryption across any application on any port protects you against malware moving across SSL encrypted applications.

- **Block Unknown, Targeted Malware: Wildfire.** Unknown or targeted malware is identified and analyzed by WildFire, which directly executes and observes unknown files in a cloud-based, virtualized sandbox environment. WildFire monitors for more than 100 malicious behaviors and the result is delivered immediately to the administrator in the form of an alert. An optional WildFire subscription offers enhanced protection, logging, and reporting. As a subscriber, you are protected within an hour when a new piece of malware is found anywhere in the world, effectively stopping the spread of new malware before it impacts you. As a subscriber, you also gain access to integrated WildFire logging and reporting and an API for submitting samples to the WildFire cloud for analysis.

- **Identify Bot-Infected Hosts.** App-ID classifies all applications, across all ports, including any unknown traffic, which can often expose anomalies or threats in your network. The behavioral botnet report correlates unknown traffic, suspicious DNS and URL queries and a variety of unusual network behaviors to reveal devices that are likely infected with malware. The results are displayed in the form of a list of potentially infected hosts that can be investigated as possible members of a botnet.
- **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 and safeguarding the enterprise from a full spectrum of legal, regulatory, and productivity risks. In addition, the URL categories can be leveraged into the policies to provide further granularity of control for SSL decryption, QoS, or other rule bases.

Ongoing Management and Analysis

Security best practices dictate that your administrators strike a balance between proactively managing the firewall, whether it is a single device or many hundreds, and being reactive, investigating, analyzing, and reporting on security incidents.

- **Management:** Each Palo Alto Networks platform can be managed individually via a command line interface (CLI) or full-featured browser-based interface. For large-scale deployments, Panorama can be licensed and deployed as a centralized management solution that enables you to balance global, centralized control with the need for local policy flexibility using features such as templates and shared policy. Additional support for standards-based tools such as SNMP, and REST-based APIs allow you to integrate with third-party management tools. Whether using the device's web interface or Panorama's, 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. Role-based administration is supported across all management mediums, allowing you to assign features and functions to specific individuals.
- **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. Log filter results can be exported to a CSV file or sent to a syslog server for offline archival or additional analysis.

Purpose-Built Hardware or Virtualized Platforms

Palo Alto Networks offers a full line of purpose-built hardware platforms that range from the PA-200, designed for enterprise remote offices to the PA-5060, which is designed for high-speed datacenters. The platform architecture is based on a single pass software engine and uses function specific processing for networking, security, threat prevention and management to deliver you predictable performance. The same firewall functionality that is delivered in the hardware platforms is also available in the VM-Series virtual firewall, allowing you to secure your virtualized and cloud-based computing environments using the same policies applied to your perimeter or remote office firewalls.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com