



## The Palo Alto Networks Difference

Written By: Tom Abner, Sr. Federal Systems Engineer

Palo Alto Networks' next-generation firewalls enable enterprises to see and control applications, users, and content – not just ports, IP addresses, and packets – using three unique identification technologies: App-ID, User-ID, and Content-ID. These identification technologies enable enterprises to create business-relevant security policies – safely enabling organizations to adopt new applications, instead of the traditional “all-or-nothing” approach offered by traditional port-blocking and/or proxy-based firewalls.

The innovative technologies provided by the Palo Alto next-gen firewall also eliminates the need for firewall helpers such as URL filters and web proxies in many cases. Instead of deploying multiple devices to compensate for a lack of evolution in firewall technologies, Palo Alto simply fixed the firewall so that it meets today's networking requirements.

This brief highlights some of the unique capabilities of the Palo Alto devices and attempts to explain how it addresses today's firewalling requirements.

### **Application Identification, Visibility, and Control (App-ID)**

Today many applications are web-based so they run over port 80 or 443. In addition, developers have learned to write applications to use these ports in order to evade traditional firewalls. In both cases, traditional firewalls see all this traffic as HTTP or SSL so they have lost visibility and control over the network. In order to evolve the firewall to enable access control in today's world, Palo Alto Networks developed App-ID, which accurately identifies the applications, irrespective of port, protocol, SSL, or evasive tactic. This allows firewall policy to be based on actual applications rather than destination ports like traditional firewalls. This is a core firewall function rather than an additional engine that is bolted on to the firewall.

It should be noted that App-ID does not require a rewrite of the traffic like a proxy-based firewall. Therefore, it doesn't have the issues associated with being impacted by modifications to the applications that is often the case with proxy-based firewalls. Avoiding the need to proxy also means that the Palo Alto firewall does not suffer from the performance issues commonly known to exist with proxy-based firewalls. An additional contrast with proxy-based firewalls is that there is no need for any configuration on the users' browsers as is required by proxy-based firewalls.

It's important that the term “application” be clarified since it doesn't have an industry standard definition. In the context of Palo Alto Networks firewalls, an Application is a specific program or feature of a program that can be detected, monitored, and/or controlled. For example, Facebook is an application, but Facebook Chat is also an application. Each of them can be

detected, monitored, and controlled independently as a base/core function of a Palo Alto firewall while both would appear as a single HTTP session to traditional firewalls.

iGoogle home pages are another good example of the difference between the PAN App-ID based firewall and traditional port-based firewalls. Depending on what widgets (e.g. Gmail) have been added to a user's home page, the single page may launch multiple "Applications". While a traditional firewall, proxy or web filtering device would see this as a single HTTP session, Palo Alto would see this as multiple applications.

Below are examples of functions that can be achieved with PAN firewalls by utilizing the core App-ID technology:

- Allow WebEx conferencing, but don't allow users to share their desktops
- Allow Facebook, but not Facebook apps (e.g. Mafia Wars), chat, and/or mail
- Allow users to access Twitter, but only to see their company's tweets
- Allow YouTube, but only videos with specific tags (e.g. categories)
- Allow AOL Instant Messenger (or many other IM applications), except for file transfers
- View all application usage including bandwidth, session count, source (username and/or IP), destination (username and/or source), source country, destination country, etc. in a single view within the Application Command Center (ACC)
- Identify and block applications using port 80 or 443 that are used to provide anonymous access to the Internet or to evade traditional firewalls such as Ultrasurf, tor, and cgifproxy
- Apply QOS on a per application basis to ensure performance of mission critical applications during periods of congestion

## **User Identification (User-ID)**

Palo Alto Networks' User-ID technology provides user-level visibility and control, which is lacking in traditional firewalls. By integrating with Active Directory, PAN firewalls allow administrators to configure firewall rules based on user and group membership. In addition, the logs, reports, and ACC include user information. This is accomplished by seamlessly integrating with Active Directory to dynamically map IP address to user and group information.

In Citrix and terminal services environments, User-ID can associate the individual user with their network activity. This addresses the fairly common practice of users connecting to terminal servers using remote desktop, for example, to use them as "jump boxes". This is done to prevent IT from identifying who is actually sourcing the traffic since it all appears to come from the terminal server's IP. With visibility into user activity, enterprises can monitor and control applications and content in these scenarios on a per-user and per-group basis.

Below are examples of functions that can be achieved with PAN firewalls by utilizing User-ID technology:

- Only allow members of the "IT Security" AD group to use SSH to access the internal management network
- Only allow members of the "Corporate Executive" AD group to access Hulu to watch The Office as long as they are on the non-mission critical LAN segment
- Only allow the "linux admins" group to use BitTorrent since that's how they download Linux ISOs
- Identify the top 100 users of peer-to-peer applications (all of them)
- Identify all the users that are sourcing traffic destined to China
- Identify all users that are victims of the Conficker virus
- Identify the applications being used and web sites visited by John Smith when he is logged onto a Windows machine via remote desktop even when many other users are simultaneously logged into the same server thus the traffic is being sourced by a single IP address
- Generate user activity reports that include all application usage, web sites visited, URL categories visited, and specific URLs visited (with time stamps) for a specific person
- Integrate with active directory to map users to IP addresses without any modification to the domain controller(s) or user PCs

## **Content Identification (Content-ID)**

The accurate identification of, and control over applications solves only part of the visibility and control challenge. Inspecting permitted application traffic becomes the next significant challenge and one that is addressed by the threat prevention, URL filtering and data filtering elements within Content-ID.

- Threat prevention: The threat prevention engine provides IPS/IDS, AV, and Anti-Spyware functionality. This can be done at very high performance by using a uniform signature format that enables all three types of inspection in a single pass through the engine.
- URL filtering: A fully integrated, customizable URL filtering database of over 20M URLs across 76 categories is provided on the PAN device. To augment the on-box database, cloud lookups can be enabled on a per-rule basis. When this is done, an additional 1M URLs can be cached on-box.
- File and data filtering: Taking full advantage of the in-depth analysis performed by App-ID, the Content-ID engine enables administrators to implement data filtering policies to reduce the risks associated with unauthorized file and data transfer. Files based on type (as opposed to looking only at the file extension) and confidential data patterns (credit card and social security numbers) can be detected and blocked based on policy. This includes granular per-application control.

Below are examples of functions that can be achieved with PAN firewalls by utilizing Content-ID technology:

- Identify the URL accessed that resulted in the download of a virus and list the name of the file containing the virus as well as the user who downloaded it
- Block attachments in Gmail and Yahoo Mail, but allow them for Outlook Web Access
- Identify the user who tried to upload a file containing social security numbers within a zipped file over FTP
- Inspect SSL encrypted traffic for browsing to blogging sites unless it sourced from members of the marketing or legal groups
- Generate a report for a user that contains all the applications they've used, URL categories they've accessed, web sites they've visited, and every URL accessed yesterday

### **Single Pass Architecture (SP3)**

Performance has historically been an issue with devices that perform multiple security functions. These types of devices are categorized as Unified Threat Management (UTM) platforms in many cases. The issue with UTM devices is they are really several different engines that have been bolted together rather than having been purposefully built from the ground up to provide this type of functionality. The result is that traffic is parsed, decoders are applied, state is maintained, etc for each individual function. This is extremely resource intensive so degradation of 90% or more is not uncommon when all features are enabled on these UTM platforms. It's very difficult to make the fundamental changes in how UTM products work in order to address this issue.

The founders of PAN realized that such inefficiencies could not exist in next-generation firewalls so they developed the "Single-Pass Parallel Processing" (SP3) architecture. This unique approach to integrating software and hardware simplifies management, streamlines processing, and maximizes performance. The single pass software performs policy lookup, application identification and decoding, user mapping, and content scanning (viruses, spyware, IPS) once on a given set of traffic. The software is tied directly to a parallel processing hardware platform that uses function specific processors for networking, security, threat prevention and management to maximize throughput and minimize latency.

### **Summary**

The Palo Alto Networks Next Generation Firewall provides the functionality required in today's firewalls and much more. It provides features that are not available in any other platform. It should be noted that the purpose of this document was to differentiate the PAN firewall from other traditional firewalls and UTM devices so many basic features such as IPSec VPN, NAT, SSL VPN, etc. were not covered here, but are certainly supported. Lastly, it should also be pointed out that the PAN device supports many deployment scenarios. As a result it can and is deployed in several ways ranging from tap mode for visibility only to inline layer 3 mode for typical firewall deployments. In any case, you can now regain visibility into what is running on your network and control it if you so desire. Its time that we fix the problem with enterprise security and that's the firewall.