Application Visibility and Control: In the Firewall vs. Next to the Firewall

How Next-Generation Firewalls are Different From UTM and IPS-based Products

May 2010

Palo Alto Networks
232 E. Java Drive
Sunnyvale, CA 94089
408-738-7700
www.paloaltonetworks.com

Enterprises Need Application Visibility and Control

In a world where social networking and cloud-based applications dominate business application discussions, the need for application visibility and control has never been greater. A growing number of Internet-savvy employees are accessing any business and personal applications they want in order to be more productive and stay connected. The benefits may be clear, but there are also security risks, which is why many enterprises are demanding that their security infrastructure help them regain visibility and control over the applications traversing the network.

Gartner has highlighted application visibility and control as a critical requirement for next-generation firewalls. Today, many security vendors are weaving the terms “next-generation” and “application control” into marketing messages for their existing port-based offerings. Interestingly, these vendors are incumbents in many enterprises, yet these same enterprises are still seeking application visibility and control.

Next-Generation Firewalls and UTMs Are Not the Same

Palo Alto Networks is the only firewall that can classify traffic by application – with App-ID™. Identifying the application is the very first task that is executed when traffic hits the firewall and the basis of all other functions. Incumbent offerings utilize stateful inspection to classify traffic and attempt to identify applications secondarily using an add-on, UTM-style feature (typically an intrusion prevention system, or IPS). The architectural differences between a next-generation firewall and a unified threat management (UTM) system are significant, and deeply impact function.

Performing application identification in the firewall takes advantage of two firewall attributes:

1. The firewall is the only security component that sees all traffic
2. The firewall is the right place to perform policy control
    - It uniquely uses a positive control model
    - It defines the trust boundary

This has serious implications, with the major differences relating to visibility and control.

Visibility: Turning On the Lights vs. Using a Flashlight

A firewall must classify all traffic, across all ports—it is the whole point of a firewall. An IPS (or UTM using IPS to identify applications) only sees patterns it is expressly looking for, typically only on certain specified ports. The resulting benefit of doing this in the firewall: the administrator has a clear and comprehensive picture of all of the applications on the network. Armed with this information, administrators can make more informed enablement decisions. It’s like turning on the lights in a dark room – suddenly everything is illuminated and easily seen, and administrators can act on it. With a traditional firewall + IPS or other add-ons, administrators are not given this level of detail. They only know what they have configured the IPS to look for. It’s very much like using a flashlight in a dark room – you only have limited visibility into the small area you are focused on.

Control: Safe Enablement vs. Blindly Blocking

A next-generation firewall is designed to enable and control application access, and, if need be, hand it off to be scanned for threats by an IPS. The benefit of doing application identification and control in the firewall: safe enablement of applications. Organizations can

allow, deny, allow for certain groups, allow certain functions, allow but shape, or allow but scan for threats or confidential data. In contrast, an IPS's control model is negative, and terminal - meaning that an IPS can only block, which is insufficient for application control. With an IPS or UTM, an organization can only blindly block – i.e., "find it and kill it."

The Numbers Game

The number of applications identified by the security infrastructure is obviously very important. That said, where applications get identified is more important (firewall vs. add-on), as highlighted above. There are other elements to consider as well: quality, accuracy, and richness of the identification. A simple IPS signature that identifies a single version of a single client is not comparable to a more sophisticated, firewall-based technology like Palo Alto Networks App-ID™. App-ID™, for a given application, may consist of multiple signatures and heuristics. For example, Palo Alto Networks has one BitTorrent App-ID™, which identifies all BitTorrent traffic, regardless of client or client version. Other vendors have a signature listed for each version of each BitTorrent-compatible client - which looks good on paper, but ultimately doesn't matter.

What does matter is that by using a next-generation firewalls' positive security model, organizations can enforce a policy that only enables certain applications, regardless of port, protocol, or SSL encryption. For enabled applications, organizations can then add additional security steps – like scanning for threats or confidential data.

In contrast, using a stateful inspection firewall plus an IPS to identify and control applications, IT organizations must rely on simple signatures, but applications' port-agility and SSL-encryption can render those signatures useless – "find it and kill it" only works when you can find it. Everything else gets through. And that means the ability to effectively control applications is very limited.

Bottom line: if the firewall uses stateful inspection to classify traffic, it isn't a next-generation firewall. If it isn't a next-generation firewall, it doesn't really change anything for your network security.

	Palo Alto Networks	UTM (FW + IPS)	Impact
Primary traffic classification mechanism	App-ID™: the application identity is determined irrespective of the port, protocol, or SSL encryption.	Stateful inspection: by port and network protocol. Application protocol is (often wrongly) assumed	**UTM:** Applications adhere to neither port nor protocol associations. Classification by port is ineffective, offers no visibility and poor control. **Palo Alto Networks:** App-ID™ enables comprehensive visibility and fine-grained control.
Primary security policy element	The application's identity.	Port numbers and protocols believed to be associated with specific traffic.	**UTM:** Allow port 80, block port 5605. Effectively, this policy blocks nothing because ports can no longer enable appropriate levels of control. **Palo Alto Networks:** The actual identity of the application is used in policy: e.g., allow Gmail, block BitTorrent and UltraSurf.
Application identity visibility	Complete picture of all application traffic is displayed graphically; used as primary policy element; viewed in logging and reporting.	Limited to IPS log filtering and reporting.	**UTM:** Log viewing is an "after the fact exercise" providing data too late. The data is incomplete, because it only reflects the applications expressly searched for. **Palo Alto Networks:** The application identity – what it does, how it works, and who is using it – is the primary policy element.
Application control model	Positive control: allow only what has been configured, block all else – ideal for enabling secure use.	Negative control: Block what has been configured, allow all else – cumbersome to enable secure use.	**UTM:** Coarse-grained model forces IT admins to say "No" too often. **Palo Alto Networks:** Employees are given more application freedom, with IT ensuring "safe enablement" to improve the company bottom line while protecting the network.
Enterprise directory services integration	Displayed graphically; as a policy element; in logging and reporting.	Integration is for authentication purposes only; or it is limited to secondary policy element.	**UTM:** Using IP addresses in lieu of users and groups makes positive control of applications nearly impossible. **Palo Alto Networks:** Able to enable applications is based on users and groups in addition to, or regardless of, IP address.
Visibility and control of SSL traffic (inbound and outbound)	Yes.	No.	**UTM:** Typically, all SSL traffic is uncontrolled, un-scanned, and invisible to traditional security infrastructure – and IT administrators. **Palo Alto Networks:** Incorporates policy-based decryption and inspection of SSL traffic (both inbound and outbound), ensuring total visibility.

Some Specific Examples: Google Talk, SharePoint, and Ultrasurf

Application visibility and control must enable organizations to specify what to allow, not just what to block. The best way to demonstrate the value of using the firewall as the controlling element is with examples. Let's pick three applications and policy responses that organizations might have to contend with – block Google Talk, block Ultrasurf, and allow SharePoint.

1. Let's start with Google Talk. It seems it should be easy for an IPS to have a signature to identify Google Talk, allowing an admin to block Google Talk. It could also have signatures to block Google Talk Gadget, Gmail Chat, and Google Talk File Transfer. However, there are two potential challenges – first, the port agility of some of these applications (IPS engines still use port to determine which decoder to use, and signatures are written for specific decoders) renders application identification spotty – administrators have to specify all of the ports to search on. Second, Gmail defaults to SSL-encrypted now, and most IPSs are not capable of decrypting outbound SSL – so Gmail Chat works just fine, despite whatever policy is in place on the UTM. Palo Alto Networks App-ID™ includes an ability to decrypt SSL, coupled with identifying the application. In this case, that includes controlling file transfers over Gmail as well as Gmail Talk (a special implementation of Google Talk embedded in Gmail).

2. Block UltraSurf. Anyone who knows what UltraSurf does would likely want to block it as it allows the user to tunnel any other internet application through an encrypted tunnel capable of traversing traditional firewalls, proxies, and IPS systems. Here the biggest challenge is the way UltraSurf uses a proprietary implementation of SSL to bypass protocol decoding and signature detection, so the IPS approach cannot identify and block UltraSurf. Put another way, "find it and kill it" only works when you can find it. And since UltraSurf can be used to tunnel just about any application, all other application controls are rendered useless. Palo Alto Networks' App-ID™ uses its heuristics engine to identify UltraSurf, and to keep up with UltraSurf's often changing evasion tactics.

3. Allow SharePoint. IPS systems are designed to block, not allow, so it isn't possible to safely "allow SharePoint". Instead you need to block everything else. But how do you do this unless you know every application on the market and you have a management interface to then allow you to easily select "everything but SharePoint". Neither of these is available nor will it likely ever be available given the rate of new applications arriving on the market. Palo Alto Networks App-ID™ makes it very easy to safely allow SharePoint. You don't even need to know what ports it uses. You can further control functions within SharePoint (SharePoint, SharePoint Admin, SharePoint Blog Posting, SharePoint Calendar, SharePoint Documents, and SharePoint Wiki), including limiting them to certain users, such as SharePoint Admin limited to IT administrators. And you can ensure it is "safe" by scanning for threats that may be targeting any of SharePoint components (e.g., SQL Server, IIS).