

# Comparing Palo Alto Networks With UTM Products

## OVERVIEW

The Palo Alto Networks next-generation firewall classifies traffic from an application-centric perspective, thereby allowing organizations to accurately identify and control applications flowing in and out of the network regardless of port or protocol. The knowledge of exactly which application is traversing the network is then used as the basis for all security decisions including access control, SSL decryption, threat prevention, and URL filtering.

Due to the fact that the Palo Alto Networks firewall can perform traditional firewall functions, and is also capable of blocking threats and controlling web usage, logical comparisons to Unified Threat Management (UTM) offerings are made. The key differences between UTM solutions and Palo Alto Networks can be summarized as follows:

- **Application-Centric Traffic Classification:** Palo Alto Networks classifies traffic by actual application regardless of port or protocol, enabling granular visibility and control over applications traversing the network. UTM offerings classify traffic from a port and protocol perspective, which is ineffective when faced with new applications that are equipped with increasingly sophisticated security evasion techniques, such as dynamic port hopping, application emulation and SSL encryption.
- **Simplified Policy Management:** Palo Alto Networks application control and threat prevention policies are implemented from a single, centralized policy table. UTM solutions use different management interfaces accessing multiple policy tables resulting in complex and cumbersome policy control.
- **High Performance:** Through a combination of custom hardware, function specific processing and innovative software design, the Palo Alto Networks firewall delivers high performance, low latency throughput, even with all security functionality turned on. Current UTM offerings suffer from latency and throughput slowdowns as each different function is enabled, rendering many of them unusable.

## ABOUT THE PALO ALTO NETWORKS FIREWALL

The Palo Alto Networks next-generation firewall has been built from the ground up to address changes in the application landscape that have new applications using increasingly sophisticated security evasion techniques such as dynamic or random port numbers, application emulation and SSL encryption. The application development process of port/protocol = application is no longer followed which means that existing security solutions that rely on port/protocol to identify traffic are no longer effective.

The enabling technology in the Palo Alto Networks firewall is called App-ID™, a new traffic classification technique that uses the application content to accurately identify the application, irrespective of protocol, port, SSL encryption or evasive tactic employed. The App-ID classification engine uses a combination of application decoders, application signatures and SSL decryption to identify more than 500 applications. The application identity is then used as the basis of all security decisions. With the application identity, the policy engine performs a lookup to determine what actions to take—allow, block, mark, scan for threats, and more.

## ABOUT UTM PRODUCTS

UTM solutions were born as security vendors began bolting feature add-ons such as Intrusion Prevention and Antivirus to their stateful firewalls in an effort to address threat evolution. Traffic flowing through a UTM is first classified by the stateful firewall using port and protocol. Based on this classification, which is often inaccurate, a policy lookup decides whether or not the traffic is sent off to the other scanning engines to look for application exploits (IPS) or viruses/Trojans (AV) or some other type of threat.

In general, UTM products do not try to perform their functions any better than they would be on standalone devices, but rather are simply trying to provide convenience to the customer by integrating multiple functions into one device. In almost all cases, though, UTMs have built a reputation of being inaccurate, hard to manage, and performing poorly when services are enabled, relegating them to environments where the value of device consolidation outweighs the downside of lost functionality, manageability or performance.

## COMPARISON DETAILS

Palo Alto Networks and UTM solutions are both designed to protect the network against a wide range of attacks, however, there are several significant differences in how they achieve that protection.

- Application-centric vs Port-centric Classification:** As the threat landscape rapidly evolved, security vendors began bolting feature add-ons such as Intrusion Prevention, and Antivirus to their stateful firewalls and UTM solutions were born. Unfortunately, the underlying stateful inspection classification engine wasn't enhanced, so UTMs continue to see traffic by port and protocol, rendering the firewall ineffective at controlling applications. It also means that applications can be mis-identified, allowing them to bypass the other security engines. IPS or DPI (Deep Packet Inspection) add-ons are threat oriented, looking only for bad traffic and do not address the traffic classification problem.

All of the Palo Alto Networks functionality has been developed as a tightly integrated solution that leverages the application identity across all security policy decisions including, access control, threat prevention and SSL decryption. The identity of the application is not only used for access control, but it also determines where a file transfer may start and stop within a specific instant messaging application such as AIM, thereby enabling broader application of malware and threat detection.

- Simplified Policy Management:** The typical UTM product simply takes AV, IPS or other functionality as it exists on stand-alone platforms and copies it as another layer to the base product. While this can provide some cost savings, it does nothing to improve the solution nor optimize it for network-based security. Instead, security policy management becomes cumbersome because each functional "silo" has its own policy table. Use of separate policy tables makes management a complex task and it also means that there is no ability to share what each threat mechanism "learns" about traffic when building the security policy. In some cases, the management interfaces are merely re-branded versions of the vendor supplied solution with a completely different look and feel. If the policy management goal is application visibility and control, UTM offerings will fall woefully short because the port-centric traffic classification does not supply the policy engine with accurate application identity.

With its fully integrated capabilities and App-ID classifying traffic by application instead of port, policy management with Palo Alto Networks is a single, streamlined function. A single policy determines the matching criteria for the traffic, including source/destination zone and IP address, source user or user group, and application or application category. Based on the match, the policy can allow or block the application, and can also determine how to scan the traffic for viruses, spyware, vulnerabilities, file types, and URLs—all through a single policy entry.

- Performance:** Many of the functions that UTMs integrate were originally designed to run on dedicated, general purpose processors and often in different parts of the network (such as on an email server). Additionally, to save cost, most UTMs will share one CPU across multiple functions, resulting increasingly poor performance as each service is enabled. Traffic must flow through multiple scanning engines resulting in increased latency. In the case of AV, most of the UTM solutions use a proxy or file-based AV solution which requires that the entire file be loaded into memory before it is scanned, adding significant amounts of latency to the traffic flow.

The Palo Alto Networks firewall has been designed to deliver low latency, high performance throughput with all security services enabled. Performance is achieved through a purpose-built platform with function-specific processing and dedicated memory for networking, security, threat prevention and management. Virus, spyware, vulnerability detection and file blocking are all performed in a single engine (FlashMatch™), which is run on an advanced processor, not a general purpose CPU. FlashMatch is a stream-based threat prevention engine that scans for viruses, spyware, and application exploits in a single pass through the use of a uniform signature format. The stream-based architecture of FlashMatch means that scanning is performed inline, as soon as the first packet hits the scan engine. The combination of dedicated processing, single pass scanning and stream-based architecture means that latency is minimized and throughput maximized.

## SUMMARY

The Palo Alto Networks firewall and UTM solutions are both designed to perform firewall functions as well as block a wide range of threats. The key items that differentiate Palo Alto Networks from UTM offerings are in how the protection is achieved in terms of traffic classification, policy management and performance.