Comparing Palo Alto Networks with UTM Products

OVERVIEW

Palo Alto Networks next-generation firewalls enable policy-based visibility and control over applications, users and content using three unique identification technologies: App-ID, User-ID and Content-ID. 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.

Palo Alto Networks is not a UTM. Palo Alto Networks' next-generation firewalls FIX the problem that is plaguing network security – the inability to identify and control the applications running on enterprise networks. By giving control back to IT in the firewall, many network security band-aids can be removed. The only value proposition a UTM provides is to collapse the traditional (broken) network security infrastructure into a single box as a cost savings mechanism.

Specific differences include:

- **Traffic Classification by Application – not Port or Protocol:** 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 security evasion techniques, such as dynamic port hopping, application emulation and SSL encryption.
- **Granularity of Controls:** Palo Alto Networks next-generation firewalls enable fine-grained control over applications from a single, centralized policy table with response options that are more flexible then the traditional all, deny or find it and kill it threat oriented approach. UTM solutions tack on IPS making management cumbersome and ineffective while treating the application like a threat (find it and kill it).
- **Performance:** Palo Alto Networks' single pass parallel process architecture takes a unique approach to integrating software and hardware to simplify management, streamline processing and maximize performance. The single pass software performs its' defined functions only 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. Current UTM offerings are underpowered, often times, utilizing a single, general purpose chip which results in increased latency and throughput bottlenecks as each different function is enabled, rendering many of them unusable.

ABOUT THE PALO ALTO NETWORKS FIREWALL

The Palo Alto Networks next-generation firewall addresses the rapid evolution 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 era where "port/protocol = application" no longer exists, which means that existing security solutions that rely on port/protocol to identify traffic are no longer effective. Palo Alto Networks uses App-ID, a patent-pending traffic classification mechanism that accurately identifies more than 900 applications. The application identity is mapped to the user identity (User-ID) for control, while traffic is inspected for content policy violations (Content-ID). Deployed either as a complement to existing security infrastructure components, or as a primary firewall, Palo Alto Networks takes a traditional, positive approach to security enforcement—deny all traffic except that which is expressly allowed.

ABOUT UTM PRODUCTS

UTM solutions were born as security vendors began bolting Intrusion Prevention and Antivirus add-ons to their stateful firewalls in an effort to reduce the cost of deployment. UTM products do not perform their functions any better than they would be on standalone devices, instead, they provide convenience to the customer by integrating multiple functions into one device. Unfortunately, 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.

SUMMARY

The Palo Alto Networks firewall is designed to address the specific problem presented by the changes in the application landscape. UTM solutions are merely attempting to reduce the cost of deployment without addressing the business and security risks presented by the loss of visibility and control over applications, users and content that IT managers are faced with today.

paloalto NETWORKS

Palo Alto Networks
232 E. Java Dr.
Sunnyvale, CA 94089