Summary: NetworkWorld PA-5060 and PAN-OS 4.0 Product Review

SCORECARD

Product	Palo Alto-5060
Intrusion prevention (10%)	4
Anti-malware (10%)	4
VPN features/ functions (10%)	3.5
Routing (5%)	4
IPv6 (5%)	4
Hardware architecture (5%)	4.5
Management (15%)	4
Power (5%)	3.5
Next Gen Firewalls (25%)	4
Performance (10%)	4
Total	4

SCORING KEY: 5: EXCEPTIONAL; 4: VERY GOOD; 3: AVERAGE; 2: BELOW AVERAGE; 1: SUBPAR OR NOT AVAILABLE

The recent (8/22/2011) NetworkWorld review of the PA-5060 running PAN-OS 4.0 is a great result, we are very happy with the functionality and performance aspects of the review. The performance tests are the most strenuous the reviews team has ever seen in the nearly 10 years of firewall product reviews. Likewise, the functionality tests focused on what next-generation firewalls were designed to do: securely enable applications. In total, there are four articles on the NWW site – the direct links are below:

Functionality: http://www.networkworld.com/reviews/2011/082211-palo-alto-test-249389.html
Performance: http://www.networkworld.com/reviews/2011/082211-palo-alto-performance-test-249383.html
How it was tested: http://www.networkworld.com/reviews/2011/082211-palo-alto-performance-test-how-249388.html
NGFW Defn http://www.networkworld.com/reviews/2011/082211-palo-alto-next-gen-test-249395.html

We are very pleased with this review as it does several things:

1) It validates that our stature as an enterprise firewall
2) It points out one of our long standing key strengths – the visibility into network traffic.
3) It highlights our unique feature set as something that cannot be found in other firewall or gateway security offerings.

A summary of the positive (there were many) and negative (a few) points are below.

Overall

- *"…its application awareness makes it even better suited as an outbound firewall, giving extended visibility into what is happening, and fine-grained control over what is allowed."*
- *"Our overall conclusion is that the PA-5060 has more than most managers would need to effectively control outbound application usage in enterprise networks."*

Visibility

- *"The Palo Alto Networks PA-5060 has so many good reporting and visibility tools that it's easy to forget that it's a fire wall."*
- *"The main starting point for viewing your traffic is the PA-5060's Application Command Center…this view alone [ACC] will likely be an eye-opener for most network managers, as most of these data are not available in traditional visibility tools."*

Workflow

- *"To get deeper [visibility], the PA-5060 has a pastiche of additional tools. The most useful include log analyzers and periodic reporting tools. Jumping between the Application Control Center and the detailed log analysis tools is easy, because once you've narrowed down what you want to look at in the Application Control Center, the filter is automati cally passed over into the log analyzer."*
- On converting a 182 rule ScreenOS policy, *"The job was easier than we had imagined, because Palo Alto has fixed one of our long-standing design complaints about the Juniper firewall: the inability to put more than one security zone in a single firewall rule. The PA-5060 supports rules with more than one security zone, which let us shrink our policy down by a third."*

Secure enablement

- *"Unlike some firewalls where the UTM features are system-wide or apply to all traffic, we found the ability to tie different threat protection profiles to different sets of traffic both intuitive and useful."*
- On the subject of applying threat prevention profiles to applications, *"This [the profiles] would let you apply, for example, one set of DoS protections to seldom-used Web servers and a different set to heavily-used ones. Or, you could apply different IPS signatures for incoming traffic than for outgoing."*

Threat prevention

- Using a Mu Dynamics test bed, *"The PA-5060 did better in this test [than the previously tested PA-4020], blocking 90% of the attacks in the client-to-server direction and 93% of the attacks in the server-to-client direction."*

Summary: NetworkWorld PA-5060 and PAN-OS 4.0 Product Review

Performance

- Firewall throughput: As we stated earlier, the performance tests are the most strenuous the reviews team has ever seen in the nearly 10 years of firewall product reviews. That said, the PA-5060 achieved 18.7 Gbps of static (512kb) HTTP throughput and 17 Gbps of mixed HTTP throughput (table 1) - these are spectacular results. We collaborated with NWW on the agreed upon test criteria which used HTTP with a mix of payloads as well as static HTTP traffic (10kb and 512kb response sizes).

  To clarify the significance of these results, it is important to look at how firewall performance has been tested in the past. Normally, firewall testing is done using UDP and large packets (1,518 kb). The results are a favorable but unrealistic (datasheet) performance number.

HTTP mixed payload breakdown (Table 1)	
1 x 32k image/gif	1 x 1024k application/octet-stream (pdf)
1 x 1k, 2 x 192 text/html	1 x 1216k application/x-zip
1 x 64k, 1 x 128k, 1 x 384k image/jpg	1 x 1536k application/octet-stream (exe)

- Consistent threat prevention throughput: The PA-5060 delivered 13 Gbps (DSRI enabled) and 5 Gbps with full scanning in both directions. From the review, "*Regardless of which UTM features we enabled - intrusion prevention, antispyware, antivirus, or any combination of these - results were essentially the same as if we'd turned on just one such feature. Simply put, there's no extra performance cost, beyond the initial sharp drop in rates, for layering on multiple types of traffic inspection.*"

- SSL decryption throughput: The PA-5060 delivered nearly 1 Gbps SSL decryption.

As with any review, there are a few negatives:

- We are not a UTM: The reviewer uses UTM liberally, but does so as a descriptive term of a security device that does many things. From the review, *"Next-generation firewall vendors don't like the term "UTM" (Unified Threat Management) very much because UTM products have been unfairly painted as only appropriate for small businesses. However, next-generation firewalls need threat mitigation features just as much as UTM firewalls do. While the buzzword police fight out the differences and split hairs, we tested the PA-5060's UTM features, including intrusion prevention (IPS), anti-malware and URL filtering."*

- User-ID: The statement, *"Gathering user identification information is hard"* acknowledges (correctly) that identifying users in heterogeneous environments is challenging – it is not an indictment of our User-ID feature. The reviewer did not attempt anything beyond basic Active Directory events and captive portal.

- SSL performance with full threat prevention enabled. The 100 and 118 Mbps of SSL decryption with full threat inspection enabled is the result of a test-tool configuration issue plus a bug found in PAN-OS that has been fixed (in PAN-OS 4.0.4). Running the exact same test internally resulted in performance of 1.2 Gbps even with full threat scanning enabled.

- No information on PDF exploit evasion. The PDF exploit evasion is an evasion tactic and the results are exactly what should have happened – the administrator was warned of the tactic.