Comparing Palo Alto Networks with Web Application Firewalls

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. The knowledge of which application is traversing the network and who is using it is then be used to create firewall security policies, including access control, SSL decryption, threat prevention, and URL filtering. Every corporation needs a firewall.

In contrast, a Web Application Firewall (WAF) is designed to look at web applications, monitoring them for security issues that may arise due to possible coding errors. The only similarities between the two solutions is the fact that they use the term firewall in the name. Only those corporations that feel they have coding issues in their web applications need a WAF.

Key attributes of Palo Alto Networks next generation firewall:

- Designed to be a primary firewall, identifying and controlling applications users and content traversing the network.
- App-ID: Identifies and controls more than 900 applications of all types, irrespective of port, protocol, SSL encryption or evasive tactic.
- User-ID: Leverages user data in Active Directory (as opposed to IP addresses) for policy creation, logging and reporting.
- Content-ID: Blocks a wide range of malware, controls web activity and detects data patterns (SSN, CC#) traversing the network.
- Logging and reporting: All application, user and threat traffic is logged for analysis and forensics purposes.
- Performance: Designed to act as the primary firewall for enterprises of all sizes which dictates that it deliver high performance throughput under load. Palo Alto Networks uses a combination of custom hardware, function specific processing and innovative software design to deliver high performance, low latency throughput.

Key attributes of Web Application Firewalls:

- Designed to compensate for insecure coding practices – only those companies that use web applications and are concerned that their code is insecure need to buy a WAF.
- Looks specifically for security flaws in the application itself, ignoring the myriad of attacks that may be traversing the network.
- Highly customized for each environment – looking at how the web application is supposed to act and acting on any odd behavior.
- Looks only at the specific L7 fields of a web application – they do not look at any of the other layers in the OSI stack.
- Current WAF offerings are designed to look only at a very small subset of the application traffic and as such, cannot address the performance requirements of a primary firewall.

SUMMARY

Palo Alto Networks next generation firewalls and WAF solutions are both firewalls in the sense that they can allow or deny traffic, but that is where the similarities end.

paloalto NETWORKS

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