The 10 Critical Security Functions

1. Identify and control applications regardless of port, protocol, evasive tactic or encryption

   Legitimate application developers and hackers alike share a common goal: to get their applications through firewalls. They have done an excellent job of this by taking advantage of the fact that traditional firewalls use port and protocol as the indicator of application. So, they simply write their applications to use commonly open ports and protocols (e.g., TCP port 80, 443), or they dynamically discover open ports. Applications such as Skype®, SharePoint®, Box, or Facebook® all look like HTTP or HTTPS to traditional firewalls. Networks that rely on this legacy technology are effectively wide open. The Palo Alto Networks solution is not port-based. Our exclusive App-ID™ technology enables you to directly configure policy based on applications and users. The reporting capability associated with this technology provides true visibility into application usage. This enables MSOs to secure the network and offer differentiated services, and they can leverage it to gain visibility into OTT traffic.

2. Apply a positive security model

   Positive security controls mandate that anything not explicitly allowed is denied. A negative model is just the opposite, allowing everything that is not explicitly prohibited. Given that virtually all threats start as unknowns, a negative control model is doomed to fail. Legacy port-based firewalls can deliver positive security controls (i.e., deny all, except traffic to specified ports and destinations), but they only look at the packet header. In contrast, IPS devices look at the packet contents, but they apply negative controls. They allow all traffic that does not match a signature in the database. As legacy vendors incorporated IPS functions into their firewalls, their application control functions were embedded into the IPS because their firewall function was unable to look beyond the header. As a result, these so-called next-generation solutions cannot apply positive security controls at the application level. The Palo Alto Networks firewall is fundamentally different in that firewall policy is configured based on application — unknown applications (or unknown sub-functions of allowed applications, or misuse of an allowed application) can be stopped automatically. This is a critical difference because unknown applications, and the misuse or exploitation of known applications, are primary vectors for attacks on today’s networks.

3. Decrypt outbound SSL and control SSH

   Visibility and control must also be applied to encrypted traffic, which comprises a growing proportion of traffic overall. The MSO security team may have a large and growing blind

spot with respect to the visibility and control of SSL and SSH. However, flexibility is needed. The Palo Alto Networks next-generation firewall has the flexibility to leave some SSL-encrypted traffic alone (e.g., Web traffic from financial services or health care organizations), while other types (e.g., SSL on non-standard ports, HTTPS from unclassified websites in Eastern Europe) can be decrypted via policy. It also provides visibility and control over SSH, which is easily configured by end users for non-authorized purposes (e.g., application tunneling, remote desktop). SSH is also commonly used by high-privilege users, so control and visibility is an important security capability.

4. Control application function

   Applications typically offer multiple functions, some of which an MSO may need to prohibit for security or regulatory reasons. For example, conferencing applications often allow remote desktop sharing and file transfer capabilities. The Palo Alto Networks platform continually classifies each application, monitoring for changes that may indicate a different function is being used. It detects when a different function or feature is introduced in the session, notes it within the state tables, and performs a policy check. This continual state tracking to understand the different functions of each application and their associated risks is a critical element of visibility, control and security.

5. Safely enable new applications

   A wide range of applications enable your business and the business of your customers. The applications may be hosted internally or in the cloud. Whether hosted by SharePoint, Box.net, Google® Docs™, Microsoft® Office 365™, or even an extranet application hosted by a partner, many organizations have a requirement to use an application that may use non-standard ports, SSL or can share files. These applications are essential to the business, but they can also act as a cyber threat vector. The tendency to use non-standard ports is highly accentuated in the world of malware. Safe enablement means allowing an application but constantly scanning it for threats. Applications communicate over a combination of protocols (e.g., SharePoint uses CIFS, HTTP and HTTPS). The Palo Alto Networks platform identifies the “The benefit of using a positive security model is that new attacks will be prevented. The negative model can be quite tempting..., however a negative model means you’ll never be sure you’ve addressed everything. You’ll also end up with a long list of negative signatures that has to be maintained.” Source: owasp.org “Palo Alto (sic) is the only single device that can give you the insights, the reports and the flexibility that we require. We needed a next generation firewall to do it at gigabytes speed.” — Networx Australia Palo Alto Networks | Solution Brief 2 application (regardless of port or encryption) and enables policy control over the functions you want to allow or deny. It continually scans the allowed

components for threats and misuse: exploits, viruses/malware, spyware, and confidential, regulated or sensitive information.

6. Enable application visibility and control for all users and devices

   The MSO workforce is increasingly mobile, working from laptops, smartphones and tablets. Whether working from a coffee shop, home or a customer location, users need to connect to their applications. Regardless of where the user is, or even where the employed application might be, the same standard of policy control should apply. The GlobalProtect™ mobile security service in the Palo Alto Networks platform delivers consistent visibility, security and policy control over traffic, regardless of where the user is. It has the flexibility to apply policies that are adapted to the user, location, endpoint and application. For example, some organizations might want employees to use Skype when on the road, but not inside headquarters, where others might have a policy that says, if outside the office, users may not download salesforce.com attachments, unless they have hard disk encryption turned on. Securely enabling the mobile workforce is a key business value that MSOs can leverage for both their internal workforce and business services subscribers.

7. Make network security simpler

   MSOs struggle with incorporating more information feeds, policies and management into overloaded security processes and people. The more distributed the policy is (e.g., port-based firewall allows port 80 traffic, IPS looks for and blocks threats and applications, secure Web gateway enforces URL filtering), the harder it is to manage that policy. Typical port-based firewall installations have rule bases that include thousands of rules. Business is based on applications, users and content — not ports and protocols. Palo Alto Networks Next-Generation Firewall policy control, reporting and event logging are based on application (App-ID™), content (Content-ID™) and user (User-ID™). The concept is simple and straightforward: build policies based on who the user is (user identity and job role), and specify which applications and sub-functions they are permitted in the context of their job role, endpoint and location.

8. Deliver the same throughput and performance with application control fully activated

   MSOs cannot afford to compromise between performance and security. The Palo Alto Networks Next-Generation Firewall maintains performance even with all of the security functions enabled because of its unique “single-pass” inspection architecture. Traffic is inspected once and processed in parallel for all security elements (e.g., application, user, content, malware, URL filtering). Competing solutions typically employ multi-bladed architectures, which require each security function to perform its own inspection. The result

is throughput degradation of over 90 percent in many cases. It is critical that performance and security both scale to the high throughput needs of MSOs.

9. Provide a platform for managed services

   According to IDC, the managed security services is over $15 billion and will grow at a compound annual rate of 12 percent for the next several years. Businesses of all sizes are struggling to secure their assets while enabling mobility for their users, BYOD and cloud-based applications. Recognizing that they do not have the core competency and resources to adequately do this on their own, they are looking to their network providers to provide these services. MSOs are in an excellent position to move up the customer value chain by offering managed security services in either a hosted model, CPE model or both. Because of its tightly integrated but modular suite of capabilities, Palo Alto Networks is the ideal platform for delivering managed services.

10. Enable security for NFV/SDN deployments

    The explosive growth of virtualization and cloud computing introduces new security challenges that are difficult or impossible for legacy firewalls to effectively manage. Simply having a platform that can run on a VM does not enable the benefits of NFV/SDN. The security functions need to be dynamically and automatically instantiated in concert with new instances of applications and servers. Static firewall policies based on IP addresses, ports and protocols are incompatible with SDN environments where VM-toVM traffic flows are dynamically and automatically instantiated. Key capabilities in the Palo Alto Networks NGFW, such as dynamic address groups, enable fully automated orchestration of virtualized security. The Palo Alto Networks NGFW VM-Series supports open source technology platforms (e.g., KVM and OpenStack®) and VMware® NSX™. This is a critical enabling technology for MSO adoption of NFV/SDN. “Regardless of which ... 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.