# PALO ALTO NETWORKS APPROACH TO INTRUSION PREVENTION

## Today's Threat Landscape

Organizations today must take advantage of critical business applications to drive growth. However, the threat landscape is constantly changing, with sophisticated, new cyberattacks launching with growing frequency across network, cloud and software-as-a-service environments. Organizations need to protect themselves against the risks of financial and brand damage as well as theft of assets.

Traditionally, organizations have deployed multiple single-purpose security systems to address specific types of threats. These disparate systems might include network antivirus, DNS protection, SSL decryption, sandboxes and intrusion prevention systems, or IPS, for different types of traffic. These products are often cobbled together with a central manager or bolted into a single unified threat management box, or UTM. Organizations build and deploy these single-purpose systems separately, with each offering requiring its own hardware and management. As each tool must scan traffic separately, intelligence gathered from the first step is not shared with subsequent steps, creating gaps in protection. Without native integration, turning on all security features can slow down traffic. Further, these tools are often merely raise alarms instead of actually preventing successful attacks, leaving security personnel inundated with alerts and struggling to respond quickly to critical threats.

## Palo Alto Networks Approach

Threat prevention must be done across multiple layers, everywhere on the network. It must keep pace with the changing threat landscape, allow for high throughput, and be inclusive of all traffic regardless of port, protocol or encryption. It must also focus on prevention to automatically stop threats instead of generating alerts and noise that security teams may never investigate. With these key tenets in mind, Palo Alto Networks Threat Prevention service is a natively integrated part of our Security Operating Platform that protects organizations across the entire attack lifecycle, delivering:

- **Comprehensive protection** against known and unknown attacks – server-side, client-side, exploit kits and phishing – including those that use network evasion techniques
- **Broad visibility and granular control** across your entire network
- **Consistent, simplified policy management** wherever your apps are deployed – hardware servers, virtual environments, clouds or containers
- **Automated threat intelligence** to prevent successful attacks
- **High-throughput, low-latency performance** to zero in on critical threats

## Comprehensive Protection

It's critical to identify and stop threats once they've entered your network, but it's just as important to stop them from entering in the first place by reducing your attack surface. Palo Alto Networks Threat Prevention service helps you do this through features you can easily work into policy to reduce your exposure, such as native SSL Decryption and file blocking.

### *IPS Vulnerability Protection*

Vulnerability exploits are the initial steps in the attack lifecycle for breaches, infections, ransomware and cryptomining malware. In 2017, the number of vulnerabilities reported increased by 128 percent, and 2018 will see this increase even more. This makes vulnerability protection an essential part of security.

Our IPS vulnerability protection blocks remotely exploitable network vulnerabilities, including buffer overflows, code execution vulnerabilities and port scans. Vulnerability-based signatures deliver network patching while creating a wide range of protections for client-side, server-side and ICS/SCADA vulnerabilities, as well as the internet of things. Using the industry's best exploit kit protection, Palo Alto Networks stops threats that may attempt to automatically exploit multiple vulnerabilities at once when an unsuspecting user does something as simple as visit a website. Additional capabilities, such as invalid or malformed packet blocking, IP defragmentation, and TCP reassembly, protect you from attackers' evasion and obfuscation methods. Measures are also in place to address cross-site scripting, SQL injection and brute force attacks.

Palo Alto Networks generates all signatures in-house, without any third-party content, for the most effective protection. Vulnerability-based signatures are updated at least twice a week and as needed for critical, newfound vulnerabilities or exploit kit modifications. Palo Alto Networks WildFire® malware prevention service subscribers receive these updates in as few as five minutes once new threats are discovered. Threat signatures are applied, with no dependence on port, for inbound and outbound application traffic. This means that instead of having to decide on a port that an IPS signature works on, the vulnerability-based signature automatically covers the vulnerability per profile, in stark contrast to legacy security devices that rely solely on ports. Further, policy-based SSL Decryption ensures that IPS functionality is applied to encrypted traffic.

### *Anti-Malware Protection*

A stream-based engine that blocks in-line at very high speeds detects known malware and unknown variations of known malware families. IPS and anti-malware protection address multiple threat vectors with one service, rather than requiring an organization to buy and maintain separate IPS and proxy-based products from legacy security vendors. Unlike legacy products that focus on hash-based detection, our offerings block thousands of malware variants with a single signature.

### *Command-and-Control Protection*

Anti-spyware capabilities detect and stop outbound command-and-control, or C2, communications from systems that may have been compromised by known malware families, web shells or remote access Trojans. This allows your organization to quickly identify, down to the user, systems that are potentially infected or communicating with unauthorized outside servers. Identifying infected users as quickly as possible is crucial to help protect your organization against potential breaches as well as prevent secondary downloads and data from leaving your organization. Palo Alto Networks utilizes threat intelligence from WildFire to automatically generate payload-based C2 signatures, providing research-grade C2 protections at machine speed.

Our DNS C2 signatures also use machine learning-based techniques to help discover new threats and block them before users are affected. We identify malicious domains that are parts of larger phishing or malware campaigns as soon as they become active, providing much broader coverage than traditional methods. We also deliver network-based protection for phishing attacks, preventing them before they reach end users. By targeting the network patterns of phishing attacks, we can even prevent attacks that have never been seen before.

### *Automated Security Actions*

Instead of manually responding to alerts and attacks, Palo Alto Networks next-generation firewalls deliver multiple methods of automated response, including granular log forwarding as well as first- and third-party actions. These powerful capabilities allow security operations teams to quickly and automatically act, quarantine, and affect policy to control potential infections and risky situations, including stronger security policies and controls, such as automatic multi-factor authentication.

## Broad Visibility and Granular Control

Palo Alto Networks Threat Prevention service uses App-ID™ and User-ID™ technologies to protect against spyware and application-layer exploits as well as provide useful, correlated reporting. App-ID classifies applications and governs per policy regardless of port, protocol, encryption or evasive techniques. User-ID adds further control, enabling organizations to use enterprise directory user and group information in policy. Incident response teams benefit from being able to immediately determine which systems are under attack or which users are potentially infected, rather than guessing based on IP addresses. Giving policy control over applications and users to IT and security staff vastly simplifies network security policy creation and management. User-ID also makes it easy to create policies tied directly to users. This further segments networks and delivers policies as simple as “Users in Accounts Payable are not allowed to download highly risky Portable Executable (PE) or Screen Saver .SCR files.”

## Securing Google Cloud Deployment Scenarios

Palo Alto Networks Content-ID™ technology integrates all the key IPS and network threat scanning techniques into a stream-based scanning engine. It also includes the ability to scan for certain types of confidential data, such as credit card numbers or custom regular expressions, in the same engine. It detects vulnerability exploits, buffer overflows, denial-of-service attacks and port scans – along with confidential data like credit card numbers – by scanning the traffic only once, using proven threat detection and prevention mechanisms, including:

- **Protocol anomaly-based protection** to detect protocol usage that does not comply with the IETF’s Request-for-Comments compliance requirements, such as the use of overlong uniform resource identifiers or FTP login credentials.
- **Stateful pattern matching** to detect attacks across more than one packet, considering elements such as arrival order and sequence.
- **Statistical anomaly detection** to prevent rate-based denial-of-service attacks.
- **Heuristic-based analysis** to detect anomalous packet and traffic patterns, such as port scans and host sweeps.
- **Other attack protection capabilities**, such as blocking invalid or malformed packets, IP defragmentation and TCP reassembly, to protect against evasion and obfuscation methods employed by attackers.
- **Scanning encrypted traffic and compressed content** for threats with Palo Alto Networks next-generation firewalls. Given the amount of inbound and outbound SSL-encrypted traffic in organizations’ networks today, this is critical.

### Consistent, Simplified Policy Management

For the most comprehensive protection, modern distributed networks need consistent policies to be applied across the corporate perimeter, data center, public and private clouds, SaaS applications, and remote users.

Palo Alto Networks Threat Prevention policies are applied as an extension of your firewall policies, making it easy to adopt security best practices. This allows you to radically simplify rule administration through application- and user-based policy while enabling your staff to focus on business priorities. A single interface houses, correlates and manages all logs, and all policies are consistently distributed across the network.

### Automated Threat Intelligence

Generating and consuming high-quality threat intelligence is important, but automatically turning that intelligence into protection is a necessity. Modern IPS must be able to automatically take advantage of threat intelligence to keep up with the speed of attacks. Our Threat Prevention service leverages detailed logs of all threats, which are housed in the same management interface and shared among all prevention mechanisms to provide context.

Palo Alto Networks technologies do not operate in silos; each element shares threat intelligence and protection information across the entire Security Operating Platform. Intelligence gathered from Palo Alto Networks Telemetry, URL Filtering, WildFire, IP feeds and passive DNS research all work together to improve your protection.

In addition, Palo Alto Networks DNS-based analysis protects your organization against rapidly evolving malware networks and malicious websites. Passive DNS monitoring feeds into our database of malicious domains for use in generating protections across our global customer base. Through functions such as dynamic address groups and selective multi-factor authentication, the Security Operating Platform can automatically update protection while automating SOC workflows for your analysts. We use global threat intelligence from WildFire and third-party feeds to automatically discover unknown malware and deliver protection to our entire customer base, continuously securing you against the latest advanced threats while allowing your incident response teams to focus on what truly matters.

Furthermore, our Unit 42 threat research team applies human intelligence to identify critical zero-day vulnerabilities in Adobe, Microsoft, Android® and other crucial ecosystems in addition to providing timely coverage for other vulnerabilities. By proactively identifying these vulnerabilities, developing protections for our customers and sharing intelligence with the security community, we neutralize the weapons attackers are using to threaten users and compromise networks.

### High-Throughput, Low-Latency Performance

Palo Alto Networks next-generation firewalls are based on a unique Single-Pass Parallel Processing Architecture that enables high-throughput, low-latency network security, even during content and threat scanning. Palo Alto Networks solves the performance problems IPS has struggled with in the past by combining two complementary components for this architecture.

#### *Single-Pass Software*

Palo Alto Networks single-pass software performs networking functions, policy lookup, application identification and decoding, and threat and content scanning operations only once per packet. This significantly reduces the amount of processing overhead required to perform multiple functions in one security device. This method of traffic processing enables high throughput and low latency with all security functions active. It also offers the benefits of a single, fully integrated policy for simple, easy management of enterprise network security.

#### *Parallel Processing Hardware*

Palo Alto Networks next-generation firewalls use parallel processing to ensure that the single-pass software runs fast. First, Palo Alto Networks engineers designed separate data and control planes. This separation means heavy utilization of one won't negatively affect the other. The second important element of the parallel processing hardware is the use of discrete, specialized processing groups that work in harmony to perform networking, security, content and threat scanning, and management functions.

Unique in network security, the combination of single-pass software and parallel processing hardware enables Palo Alto Networks next-generation firewalls to achieve incredible levels of performance.

### Third-Party Validation

Palo Alto Networks has received a "Recommended" rating over the last two years in the NSS Labs® Next Generation Intrusion Prevention System (NGIPS) Group Test. In the 2018 test, we blocked 99.8 percent of exploits and stopped 100 percent of evasions tested.[1] NSS Labs has also given Palo Alto Networks "Recommended" ratings in its most recent Next Generation Firewall, Data Center Security Gateway and Breach Prevention Systems tests.

Palo Alto Networks did not participate in the 2018 Gartner Magic Quadrant™ for Intrusion Detection and Prevention Systems because Gartner excluded products and vendors for this Magic Quadrant if they were sold only as features of an NGFW or UTM platform. In its report, Gartner states that "while the stand-alone IDPS market is forecast to start shrinking from 2017, the technology itself is more widely deployed than ever before on various platforms and in multiple form factors. The technology is increasingly ubiquitous in technology like NGFW and UTM."[2] In addition, Gartner includes IPS capabilities as part of its Magic Quadrant for Enterprise Network Firewalls, in which Palo Alto Networks has been a Leader seven consecutive times.[3]

## Conclusion

Our Threat Prevention service inspects all traffic for threats. Regardless of port, protocol or encryption, everything is inspected – nothing gets swept under the rug. Threat Prevention looks for threats at all points within the cyberattack lifecycle, not just when threats first enter the network, providing layered defense founded in the Zero Trust model, with prevention at all points. Crucially, it does all this with no network performance degradation, using a single-pass architecture that scans traffic only once as it passes through the firewall.

The Palo Alto Networks Security Operating Platform was built from the ground up around a prevention-first approach, with threat information shared across security functions, and designed to operate in increasingly mobile, modern networks without compromising performance. By combining network, cloud and endpoint security with advanced threat intelligence, we safely enable all applications while automatically blocking cyberthreats at every stage of the attack lifecycle.

1. "Next Generation Intrusion Prevention System (NGIPS) Group Test," NSS Labs, September 20, 2018, https://www.nsslabs.com/company/news/press-releases/nss-labs-announces-2018-next-generation-intrusion-prevention-group-test-results.
2. Gartner, Magic Quadrant for Intrusion Detection and Prevention Systems, Craig Lawson, Claudio Neiva, 10 January 2018.
3. Gartner, Magic Quadrant for Enterprise Network Firewalls, Adam Hils, Jeremy D'Hoinne, Rajpreet Kaur, 4 October 2018.



3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com


approach-to-intrusion-prevention-wp-121218