SECURITY OPERATING PLATFORM AND ARCHITECTURE

EDU-210 Version A
PAN-OS® 9.0

PREVENTION EVERYWHERE

- Security platform overview
- Next-generation firewall architecture
- Zero Trust security model
- Firewall offerings

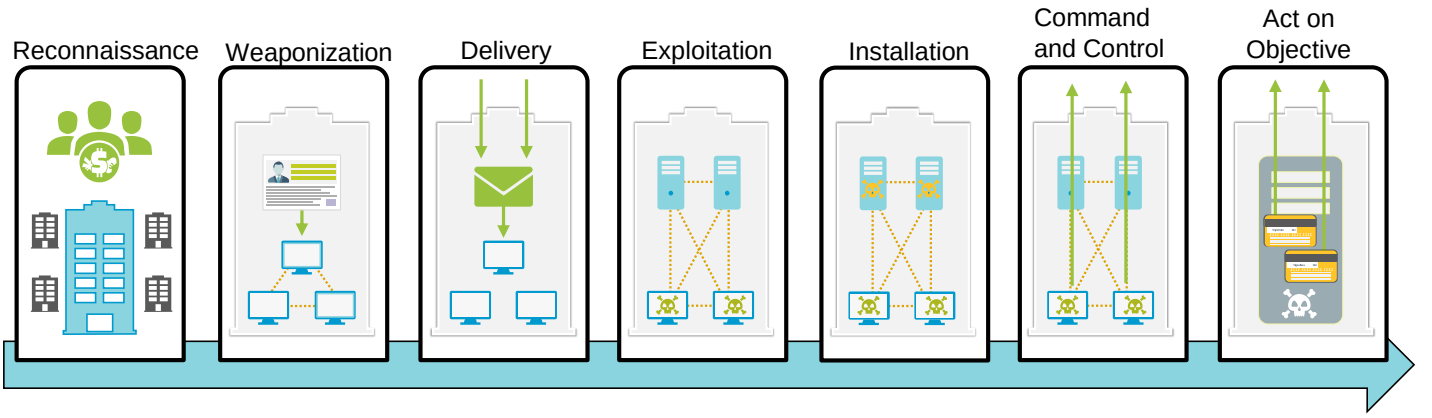
Learning Objectives

After you complete this module, you should be able to:

- Describe the characteristics of the Security Operating Platform
- Describe the single-pass architecture
- Describe the Zero Trust security model and how it relates to traffic moving through your network

After you complete this module, you should be able to:
- Describe the characteristics of the Security Operating Platform
- Describe the single-pass architecture
- Describe the Zero Trust security model and how it relates to traffic moving through your network

Cyber-attack Lifecycle

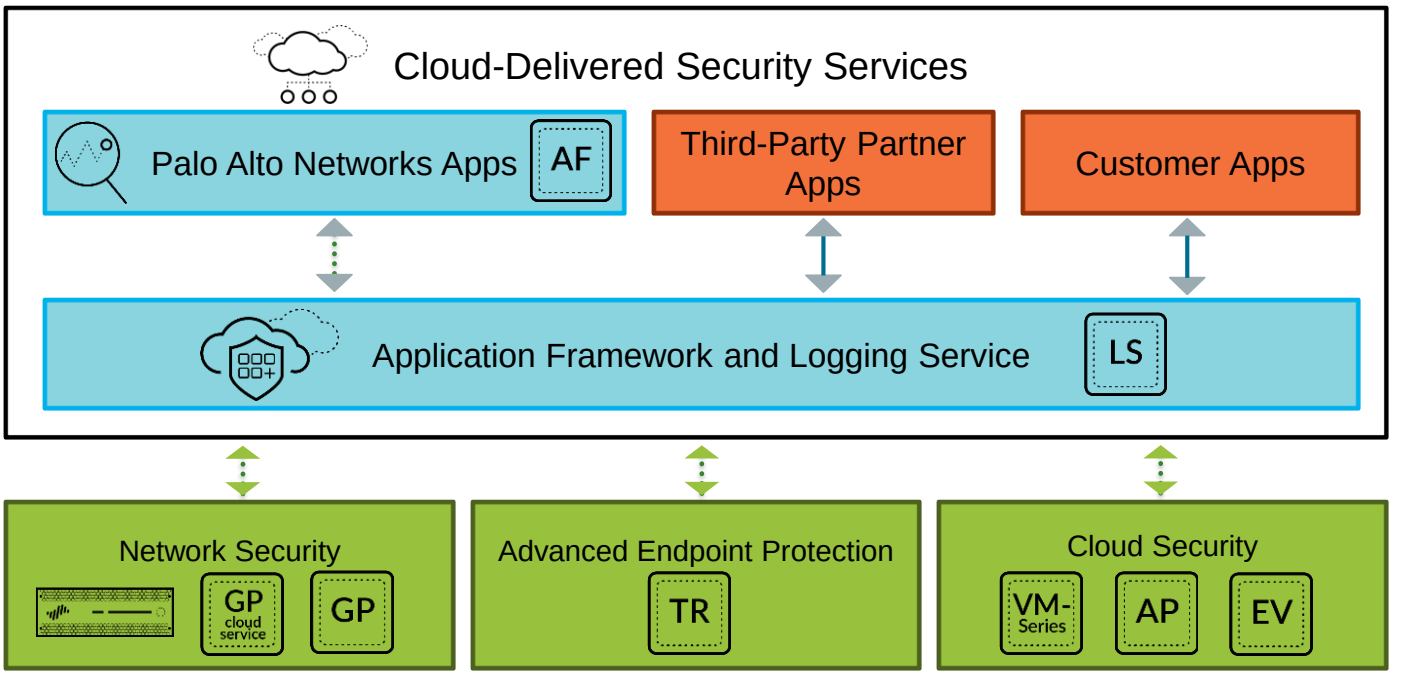


Stop the attack at any point!

The Cyber-attack Lifecycle is a sequence of events that an attacker goes through to infiltrate a network and exfiltrate data from it. A block of just one stage in this lifecycle will protect a company's network from attack. This Cyber-attack Lifecycle model illustrates how Palo Alto Networks views each stage in the lifecycle:

1. Reconnaissance: Attackers carefully plan their attacks, just as burglars and thieves do. They research, identify, and select targets, often using phishing tactics or extracting public information from an employee's LinkedIn profile or from corporate websites. These criminals also scan for network vulnerabilities and services or applications that they can exploit.
2. Weaponization and Delivery: Next, the attackers determine which methods to use in order to deliver malicious payloads. They may choose to embed intruder code within seemingly innocuous files such as a PDF or Word document or email message. Or, for highly targeted attacks, attackers may craft deliverables to attract the specific interests of an individual.
3. Exploitation: An attacker now deploys an exploit against a vulnerable application or system, typically using an exploit kit or weaponized document. Deploying an exploit allows the attack to gain an initial entry point into the organization.
4. Installation: Attackers will seek to establish privileged operations, such as maintaining access, persistence, and escalating privileges.
5. Command and Control: Attackers establish a command channel back through the internet to a specific server so that they can communicate and pass data back and forth between infected devices and their own infrastructure.
6. Act on the Objective: Now that an attacker has persistence and ongoing communication, they will act upon their motivations in order to achieve their goal. Their motivation could be data exfiltration, destruction of critical infrastructure, to deface web property, or to create fear or the means for extortion.

Security Operating Platform



The Palo Alto Networks Security Operating Platform is a prevention-focused architecture that provides visibility into all traffic and is natively integrated in such a way that no gaps exist and context is provided so you have to react only to the threats that are critically important. The Security Operating Platform is highly automated to reduce or remove manual response and enables you to drive seamless policy throughout your organization to reduce your attack surface and eliminate unnecessary risk. The platform safely enables all applications through granular use of controls and prevention of known and unknown cyberthreats for all users on any device across any network.

Application Framework and Logging Service
Apps can be created and developed on a common application framework to rapidly build and deliver cloud-based security services with no additional infrastructure or on-premises hardware changes. Apps are delivered from the cloud to extend the capabilities of the platform, including the ability to effortlessly collaborate between different apps, share threat context and intelligence, and drive automated response and enforcement. The Logging Service functions as the central cloud-based repository for all application data and logs so that you do not need to plan for additional processing power and storage.

Network Security
Palo Alto Networks Security Operating Platform firewalls are designed to safely enable applications and prevent modern threats. The firewall can identify all network traffic based on applications, users, content, and devices, and lets you express your business policies in the form of easy-to-understand security rules.

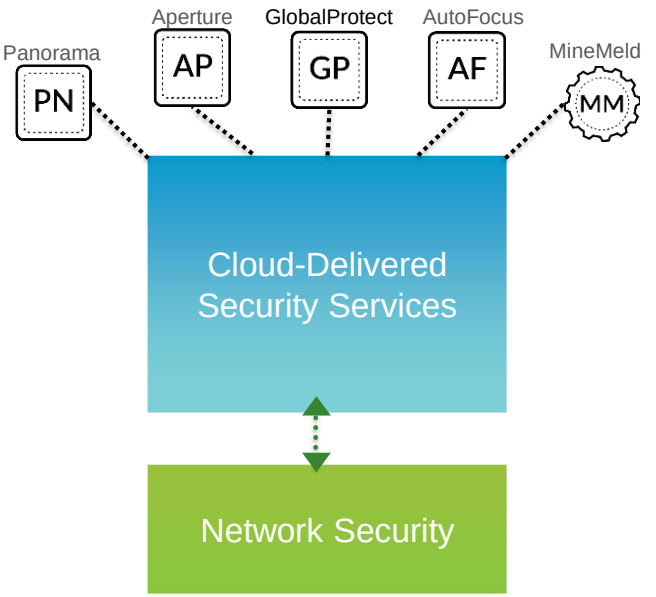
Advanced Endpoint Protection
Traps Advanced Endpoint Protection provides multi-method prevention, a proprietary combination of malware and exploit prevention methods that pre-emptively block both known and unknown threats directly on an endpoint.

Cloud Security

The Palo Alto Networks VM-Series firewall is a virtualized form of the Palo Alto Networks Security Operating Platform firewall. The VM-Series firewalls are designed for use in a virtualized or cloud environment to identify all network traffic based on applications, users, content, and devices.

Security Operating Platform (Cont.)

- Panorama: Management and reporting
- Aperture: Software-as-a-service (SaaS) security
- GlobalProtect: Extend platform externally
- AutoFocus: Threat intelligence that can be acted on
- MineMeld: Aggregate threat intelligence



Panorama
Panorama network security management provides consolidated policy creation and centralized management. It allows for the implementation and control of firewalls centrally with an efficient rulebase, and it adds insight into network-wide traffic and threats.

Aperture
Aperture is a SaaS-based service that protects cloud-based applications such as Box, Salesforce, and Dropbox by managing permissions and scanning files for external exposure and sensitive information. Aperture is focused on data loss prevention (DLP) for Personally Identifiable Information (PII), payment card industry (PCI) information, and other sensitive data.

GlobalProtect
GlobalProtect network security for endpoints safeguards the mobile workforce by inspecting all traffic using the organization's next-generation firewalls that are deployed as internet gateways, whether at the perimeter, in the DMZ, or in the cloud. Laptops, smartphones, and tablets with the GlobalProtect app automatically establish a secure SSL/IPsec VPN connection to the next-generation firewall with the best performance for a given location, thus providing the organization with full visibility of all network traffic, for applications, and across all ports and protocols. The organization that eliminates the blind spots in mobile workforce traffic maintains a consistent view into applications.

AutoFocus
AutoFocus is a hosted security service that is part of the Threat Intelligence Cloud. AutoFocus gives security operations and analysis teams direct access to all of the threat intelligence Palo Alto Networks gathers from customers, open source feeds, and the Unit 42 threat research team. Security teams then can focus their efforts on the most important attacks and understand the most critical elements of those attacks via the globally correlated analysis.

MineMeld

MineMeld allows you to aggregate threat intelligence across public, private, and commercial intelligence sources. MineMeld natively integrates with the Palo Alto Networks Security Operating Platform to automatically create new prevention-based controls for URLs, IP addresses, and domain intelligence derived from all sources providing data to MineMeld. After the indicators are collected, MineMeld can filter, unduplicate, and consolidate metadata across all sources, which allows security teams to analyze a more actionable set of data that has been enriched from multiple sources.

Security platform overview

Next-generation firewall architecture

Zero Trust security model

Firewall offerings

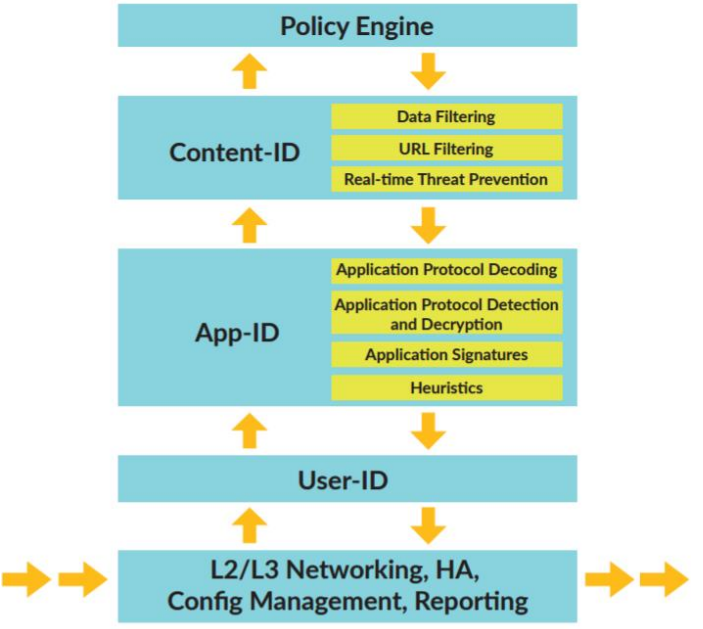
Palo Alto Networks Single-Pass Architecture

Single pass:

- Operations per packet:
  - Traffic classification with App-ID technology
  - User or group mapping
  - Content scanning: threats, URLs, confidential data
- One single policy (per type)

Parallel processing:

- Function-specific parallel processing hardware engines
- Separate data and control planes

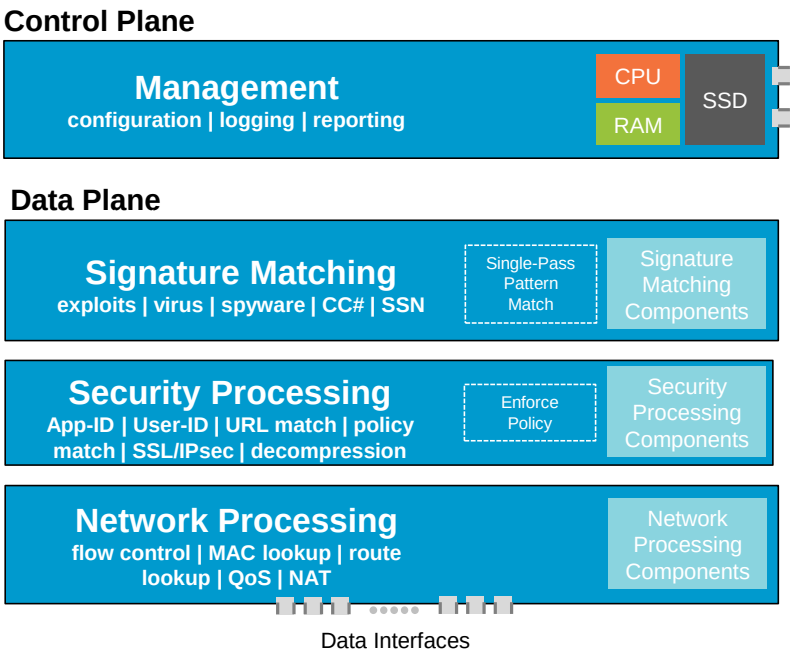


The Palo Alto Networks firewall allows you to specify Security policy rules based on a more accurate identification of each application seeking access to your network. It is unlike traditional firewalls that identify applications only by protocol and port number. It uses packet inspection and a library of application signatures to distinguish between applications that have the same protocol and port, and to identify potentially malicious applications that use non-standard ports.

The strength of the Palo Alto Networks firewall is its Single-Pass Parallel Processing (SP3) engine. Each current protection feature in the device (antivirus, spyware, data filtering, and vulnerability protection) uses the same stream-based signature format. As a result, the SP3 engine can search for all these risks simultaneously.

The advantage of providing a stream-based engine is that the traffic is scanned as it crosses the box with a minimal amount of buffering. This speed allows you to enable advanced features, such as scanning for viruses and malware, without slowing the firewall's performance.

Palo Alto Networks Firewall Architecture



Hardware component types and sizes per layer vary per firewall model.

Control Plane | Management
Provides configuration, logging, and reporting functions on a separate processor, RAM, and hard drive

Signature Matching
Stream-based, uniform signature match including vulnerability exploits (IPS), virus, spyware, CC#, and SSN

Security Processing
High-density parallel processing for flexible hardware acceleration for standardized complex functions

Network Processing
Front-end network processing, hardware-accelerated per-packet route lookup, MAC lookup, and NAT

Palo Alto Networks has processors dedicated to specific security functions that work in parallel. These components can be implemented in hardware or software.

On the higher-end hardware models, the data plane contains three types of processors that are connected by high-speed 1Gbps busses:

- Signature Match Processor scans traffic and detects:
  - Vulnerability exploits (Intrusion Protection System)
  - Viruses
  - Spyware
  - Credit card numbers
  - Social Security numbers
- Security Processors: Multicore processors that handle security tasks such as Secure Sockets Layer decryption
- Network Processor: Responsible for routing, Network Address Translation, and network-layer communication

On the higher-end hardware models, the control plane has its own dual core processor, RAM, and hard drive. This processor is responsible for tasks such as management UI, logging, and route updates.

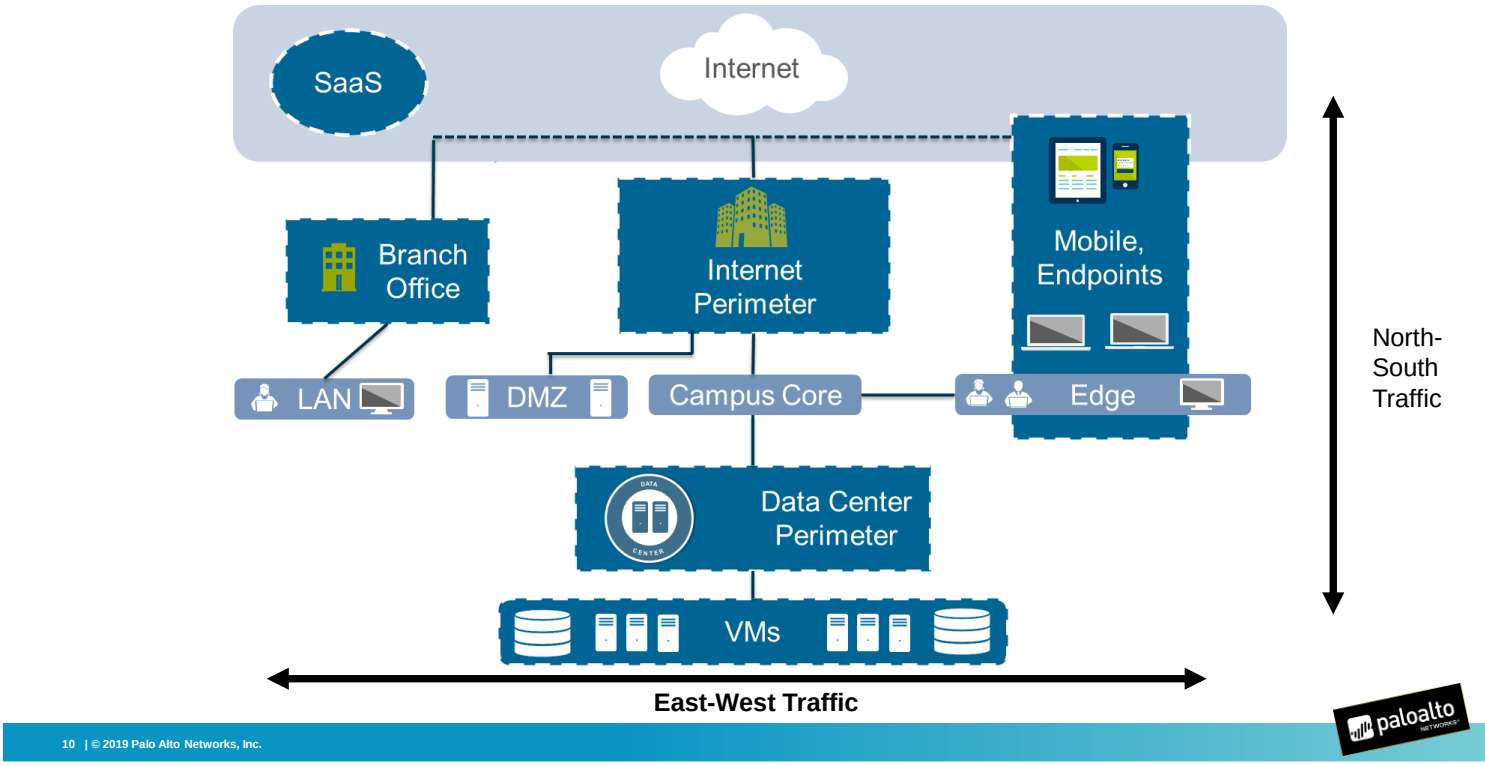
Security platform overview

Next-generation firewall architecture

Zero Trust security model

Firewall offerings

Data Flows in an Open Network



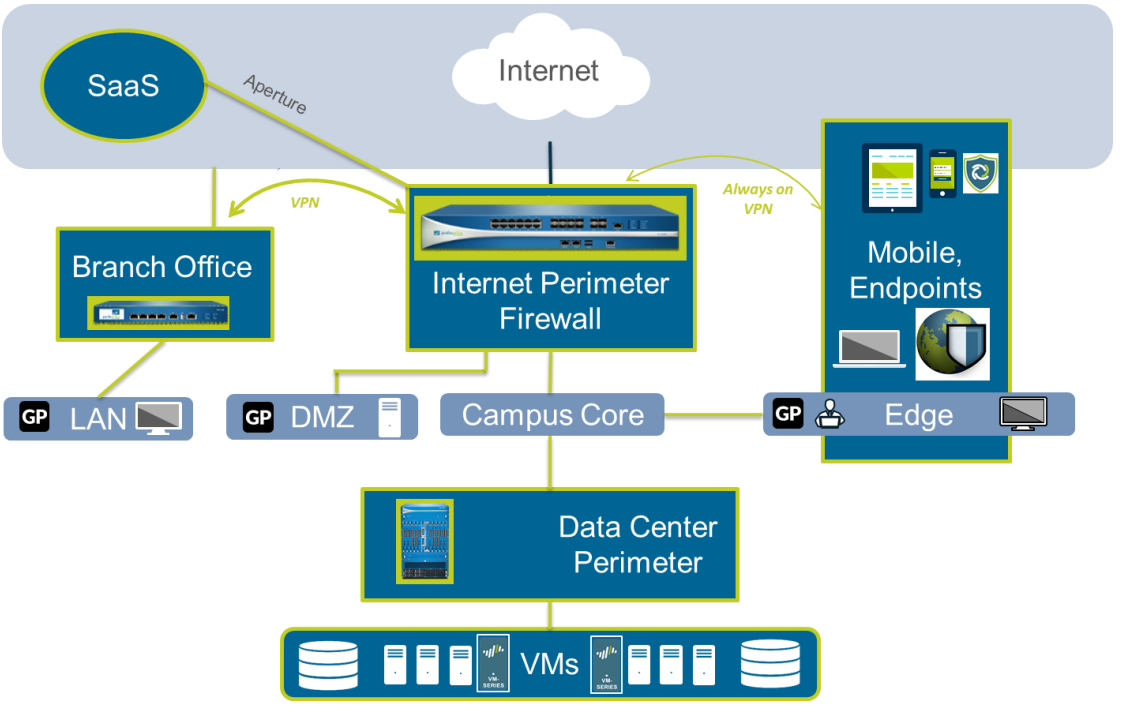
The constant cyberattacks against organizations show that perimeter security strategies alone are not effective. If IT and network security teams have no true visibility, they cannot control the users and applications traversing the network. The lack of full visibility means that organizations are vulnerable to attacks from both within the organization and from the public internet. In the majority of breaches, hackers first infiltrated an end-user device before moving into the data center.

Protection is needed from traffic that enters the network from external locations where the egress point is the perimeter (known as “north-south” traffic). Protection also is needed for traffic within the network because that is where the malicious lateral movement techniques will take place. This traffic is referred to as “east-west” traffic.

The primary issue with perimeter security at both the ingress and egress points on the network is the false assumption that the internal traffic taking place within the internal network can be trusted. Vulnerabilities include the following situations:

- Remote employees and mobile users are treated as internal traffic.
- Wireless users, partner connections, or guest users introduce new ingress points into the network.
- Remote offices may need to be considered as providers of untrusted traffic because of where they are located (regions of instability, or rogue nations or countries).
- Internal employees unintentionally present a security threat (USB keys, file downloads, and transfers).

Data Flows Secured by Palo Alto Networks Solution



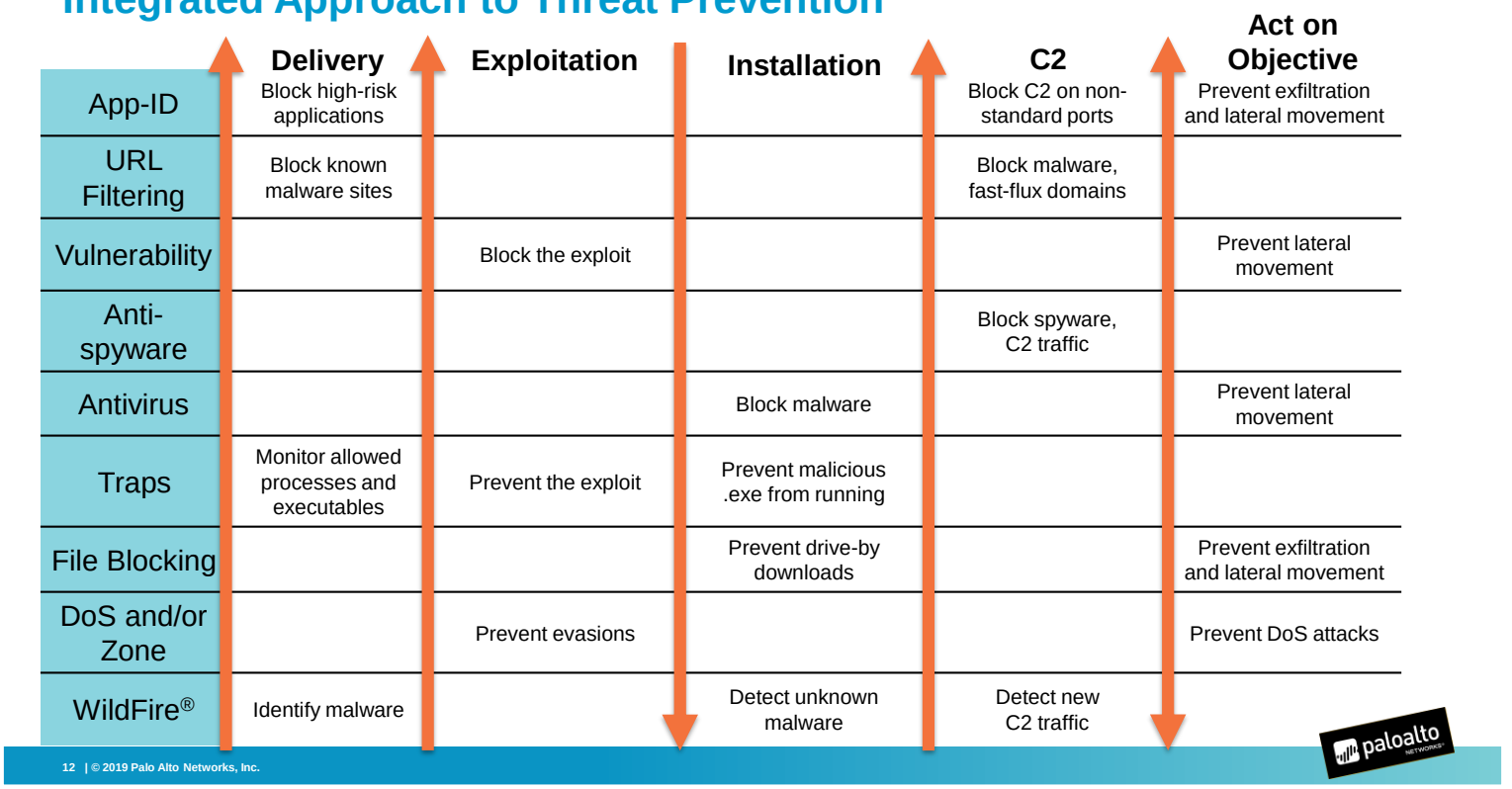
Zero Trust is an alternative security model that addresses the shortcomings of failing perimeter-centric strategies by removing the assumption of trust. With Zero Trust there is no default trust for any entity (including users, devices, applications, and packets), regardless of what it is and its location on or relative to the corporate network.

Zero Trust is a promising alternative model for IT security to follow. It is intended to remedy the deficiencies with perimeter-centric strategies and the legacy devices and technologies used to implement them by promoting “never trust, always verify” as a guiding principle. This approach differs substantially from conventional security models that operate on the basis of “trust but verify.”

The implications for these two changes are, respectively:

- The need to establish trust boundaries that effectively compartmentalize different segments of the internal computing environment.
- The general idea is to move security functionality closer to the different pockets of resources that require protection. Thus Security policy can be enforced regardless of the point of origin and the communications traffic associated.

Trust boundaries need to do more than provide only initial authorization and access-control levels of enforcement. The concept of “always verify” also requires the continuous monitoring and inspection of the associated communications traffic in search of subversive activities.



Palo Alto Networks next-generation firewalls offer a range of threat prevention functionalities that together offer an integrated approach against prevalent threats.

Threat prevention capabilities of the Palo Alto Networks next-generation firewall are the following:

- Application identification
- User identification
- URL filtering
- Vulnerability protection
- Anti-spyware
- Antivirus
- Traps
- File blocking
- DoS protection
- Zone protection
- WildFire advanced malware protection

Each function protects against specific types of threats and is configured in the zone settings and the Security Profiles, and then is applied to the various rules of the Security policy. This integrated protection will safeguard against threats and also provide application visibility and control over the network.

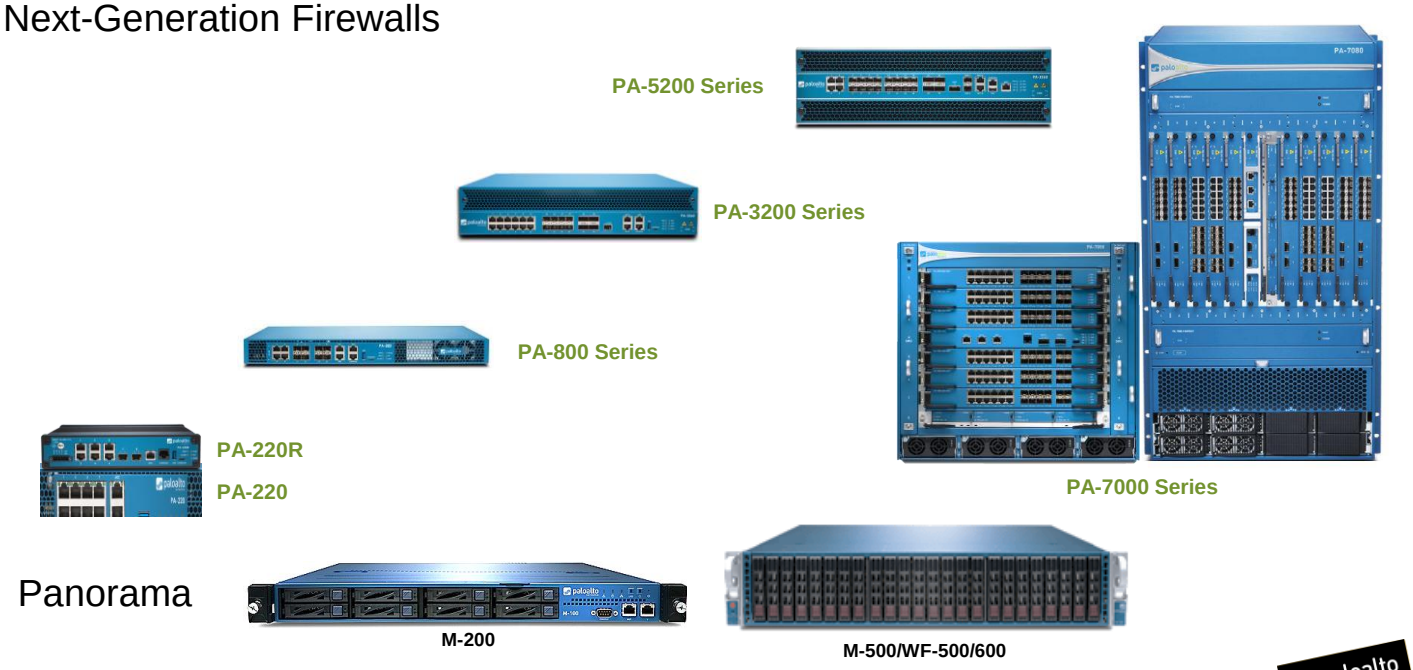
Security platform overview

Next-generation firewall architecture

Zero Trust security model

Firewall offerings

Physical Platforms



The PA-220, PA-800, PA-3200 Series, and PA-5200 Series are next-generation hardware. With the release of PAN-OS® 8.1, the PA-5280 firewall was released. The PA-5280 firewall is identical to the PA-5260 firewall except that the PA-5280 now has double the data-plane memory, which doubles the session capacity of the PA-5260 firewall.

The PA-7050 and PA-7080 are chassis architecture. With the release of PAN-OS 9.0, three new chassis cards were introduced: Network Processing Card, Switch Management Card, and the Dedicated Logging Card. The Network Processing Card, or NPC, is dedicated to executing all packet-processing tasks, including networking, traffic classification, and threat prevention. The Switch Management Card, or SMC, oversees all traffic and executes all management functions, using a combination of three elements: the First Packet Processor, a high-speed backplane, and the management subsystem. The Dedicated Logging Card creates a dedicated subsystem to manage the high volume of logs the PA-7000 Series generates. Two log cards are available: the Log Processing Card, or LPC, and the Log Forwarding Card, or LFC. The LPC offloads logging-related activities and the LFC is a dedicated card for exporting log messages. For more information about the new hardware, see https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-release-notes/pan-os-9-0-release-information/features-introduced-in-pan-os-9-0/hardware-features.html#.

Also with the release of PAN-OS 9.0, a new K2-series firewall was introduced. The K2-series firewall is a 5G-ready firewall designed for service provider mobile network deployments with 5G and internet of things, or IoT, security requirements. The K2-series enables mobile network operators to gain complete visibility and control across all layers, and it takes full advantage of automated cloud-based threat intelligence.

The operating system is consistent across all platforms, so the look-and-feel of the interface is the same.

To compare the capabilities of the various firewall models, see https://paloaltonetworks.com/comparefirewalls.

VM-Series Models and Capacities

Performance and Capacities	VM-700	VM-500	VM-300	VM-100/ VM-200	VM-50 /Lite
Firewall throughput (App-ID enabled)	**16Gbps**	**8Gbps**	**4Gbps**	**2Gbps**	**200Mbps**
Threat prevention throughput	**8Gbps**	**4Gbps**	**2Gbps**	**1Gbps**	**100Mbps**
New sessions per second	120,000	60,000	30,000	15,000	3,000
Dedicated CPU cores	2, 4, 8, 16	2, 4, 8	2, 4	2	2
Dedicated memory (minimum)	56GB	16GB	9GB	6.5GB	4.5GB/4GB
Dedicated disk drive capacity (minimum)	60GB	60GB	60GB	60GB	32GB

The VM-Series firewalls support a wider range of deployment scenarios and higher volumes of traffic when compared to previous versions of PAN-OS software.

These enhancements enable three broad use cases: optimized resources for customer premises equipment (CPE) and network tenant environments, improved performance and efficiency for perimeter and east-west data-center traffic, and maximized performance to support network functions virtualization (NFV).

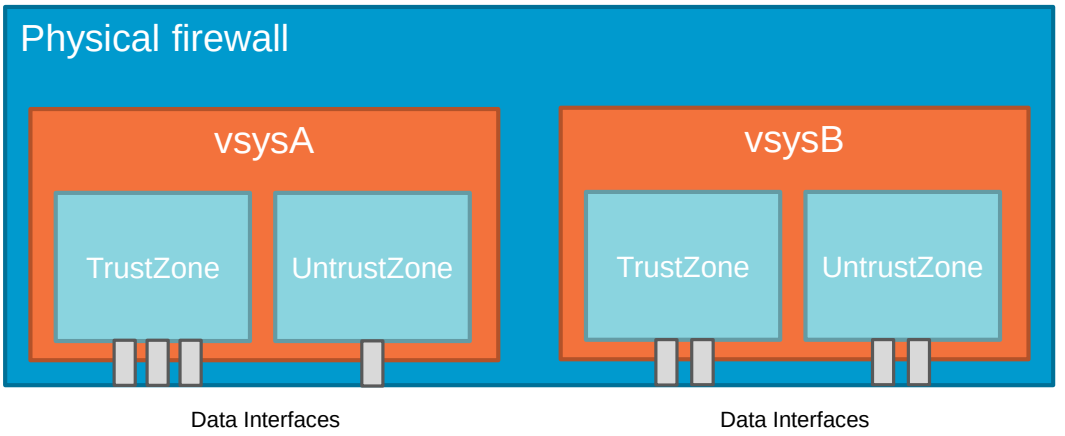
With the release of PAN-OS 8.1, a new, smaller VM was introduced. The VM-50 Lite provides an alternative for environments where hardware resources are constrained. The VM-50 Lite requires 4GB of memory instead of the 4.5GB required by the standard VM-50. The VM-50 Lite uses the same license as the standard VM-50 but changes to a VM-50 Lite when you lower the amount of allocated memory.

The VM-Series firewall can be deployed either on-premises or in a public cloud. A VM-Series firewall can be deployed on either the Alibaba Cloud, Amazon Web Services, Google Cloud Platform, Microsoft Azure, or Oracle Cloud to protect your cloud perimeter and your east-west traffic.

All VM-Series firewalls use a unified licensing system that is platform-agnostic. For example, a VM-100 perpetual license can be used to license a VM running on Hyper-V or in AWS.

Virtual Systems

- Separate, logical firewalls within a single physical firewall
- Creates an administrative boundary
- Use case: multiple customers or departments



Virtual systems, or vsys, are separate, logical firewall instances within a single physical Palo Alto Networks firewall. Rather than use multiple firewalls, managed service providers and enterprises can use a single pair of firewalls (for high availability) and enable virtual systems on them. Each virtual system is an independent, separately managed firewall with its traffic kept separate from the traffic of other virtual systems.

A vsys consists of a set of physical and logical interfaces and subinterfaces, virtual routers, and security zones. You choose the deployment mode(s) (any combination of Virtual Wire, Layer 2, or Layer 3) of each virtual system. When you use virtual systems, you can segment any of the following:

- Administrative access
- The management of all policies (Security, NAT, QoS, Policy-based Forwarding, Decryption, Application Override, Authentication, and DoS Protection)
- All objects (such as Address objects, application groups and filters, dynamic block lists, Security Profiles, Decryption Profiles, and Custom objects)
- User-ID
- Certificate management
- Server Profiles
- Logging, reporting, and visibility functions

Virtual systems are supported on the PA-3x00, PA-5x00, and PA-7x00 Series firewalls. Each firewall series supports a base number of virtual systems; the number varies by platform. A Virtual Systems license is required to support multiple virtual systems on the PA-3x00 Series firewalls, and to create more than the base number of virtual systems supported on a platform.

Module Summary

Now that you have completed this module, you should be able to:

- Describe the characteristics of the Security Operating Platform
- Describe the single-pass architecture
- Describe the Zero Trust security model and how it relates to traffic moving through your network

Now that you have completed the module, you should be able to:

- Describe the characteristics of the Security Operating Platform
- Describe the single-pass architecture
- Describe the Zero Trust security model and how it relates to traffic moving through your network

Questions?

Review Questions

1. Which four models are the Palo Alto Networks next-generation firewall models? (Choose four.)
   a. PA-200 Series
   b. PA-2000 Series
   c. PA-300 Series
   d. PA-3200 Series
   e. PA-400 Series
   f. PA-5000 Series
   g. PA-7000 Series
2. Which two planes are found in Palo Alto Networks single-pass platform architecture? (Choose two.)
   a. control
   b. single pass
   c. data
   d. parallel processing
3. True or false? The strength of the Palo Alto Networks firewall is its Single-Pass Parallel Processing (SP3) engine.
   a. true
   b. false
4. Which new firewall model was introduced with PAN-OS 8.1 with double the data-plane memory?
   a. PA-5260
   b. PA-5270
   c. PA-5280
   d. PA-5290

PROTECTION. DELIVERED.

Answers to Review Questions

1. a, d, f, g
2. a, c
3. a (true)
4. c

This page intentionally left blank