Next-Generation Security Platform and Architecture

Academy Courseware

PAN-OS® 8.0

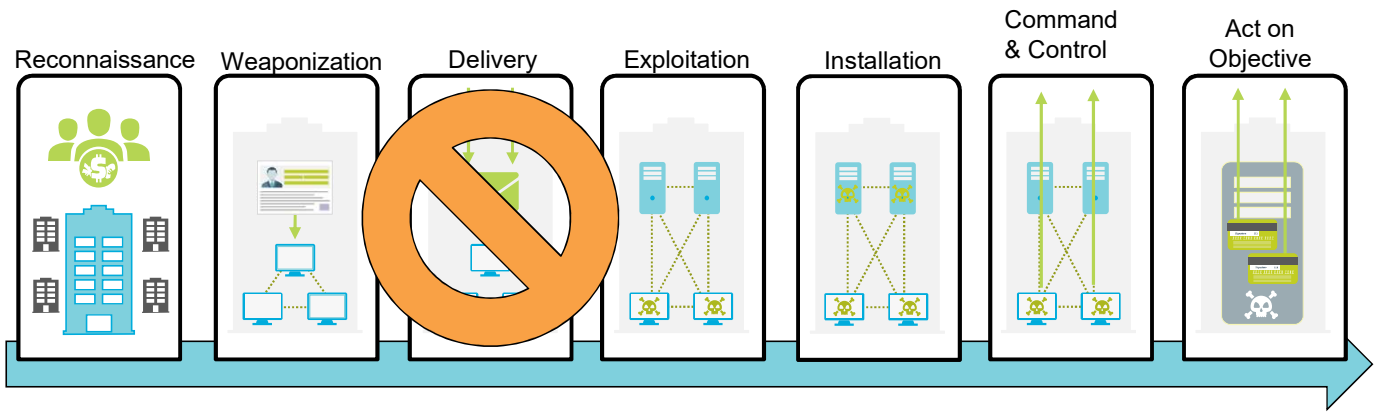
Courseware Version B

Agenda

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

Security Platform Overview

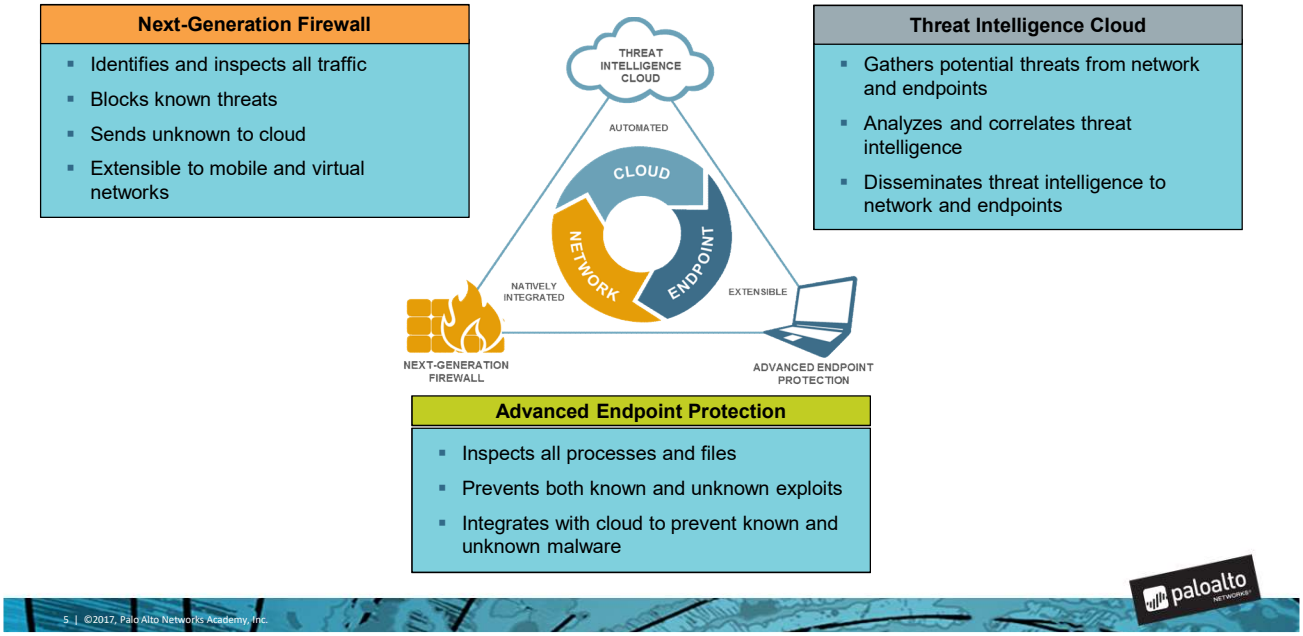
Cyber Attack Lifecycle



Stop the attack at any point!

The Cyber Attack Lifecycle is a sequence of events that an attacker goes through to successfully infiltrate a network and exfiltrate data from it. The good news is that blocking just one stage in this lifecycle is all that is needed to 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: Just like burglars and thieves, attackers carefully plan their attacks. They research, identify, and select targets, oftentimes using phishing tactics or extracting public information from an employee's LinkedIn profile or corporate websites. These criminals also scan for network vulnerabilities and services or applications they can exploit.
2. Weaponization and Delivery: Next, the attackers determine which methods to use. They may choose to embed intruder code within seemingly innocuous files like a PDF or Word document or email message. Or, for highly-targeted attacks, attackers may craft deliverables to catch specific interests of an individual.
3. Exploitation: Once attackers gain access "inside" an organization, they can activate attack code on the victim's host and ultimately take control of the target machine.
4. Installation: Attackers will seek to establish privileged operations, a root kit, escalate privileges, and to establish persistence.
5. Command and Control: Attackers establish a command channel back through the internet to a specific server so they can communicate and pass data back and forth between infected devices and their server.
6. Act on the Objective: Attackers may have many different motivations for attack, and it's not always for profit. Their reasons could be data exfiltration, destruction of critical infrastructure, to deface web property, to create fear, or to extort.



The Palo Alto Networks platform is a prevention-focused architecture that provides visibility into all traffic, is natively integrated in such a way that no gaps exist and context is delivered so you only have to react to the threats that are critically important, 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.

NGFW

Palo Alto Networks next-generation firewalls are designed to safely enable applications and prevent modern threats. The Palo Alto Networks approach identifies 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.

Threat Intelligence Cloud

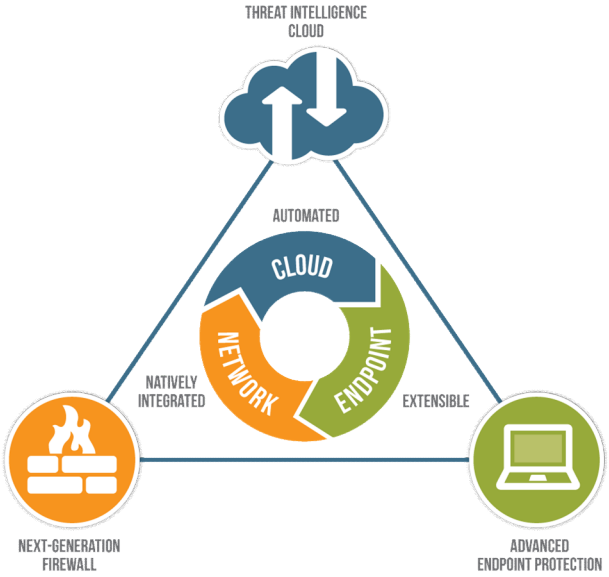
The Threat Intelligence Cloud correlates global, community-driven threat intelligence from multiple sources across networks, endpoints, and clouds to immediately halt threats from spreading.

Advanced Endpoint

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.

Next-Generation Security Platform (Cont.)

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



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

AutoFocus
AutoFocus is a hosted security service. It is part of the Threat Intelligence Cloud. AutoFocus gives security operations and analysis teams direct access to all 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.

Aperture
Aperture service 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.

Next-Generation Firewall Architecture

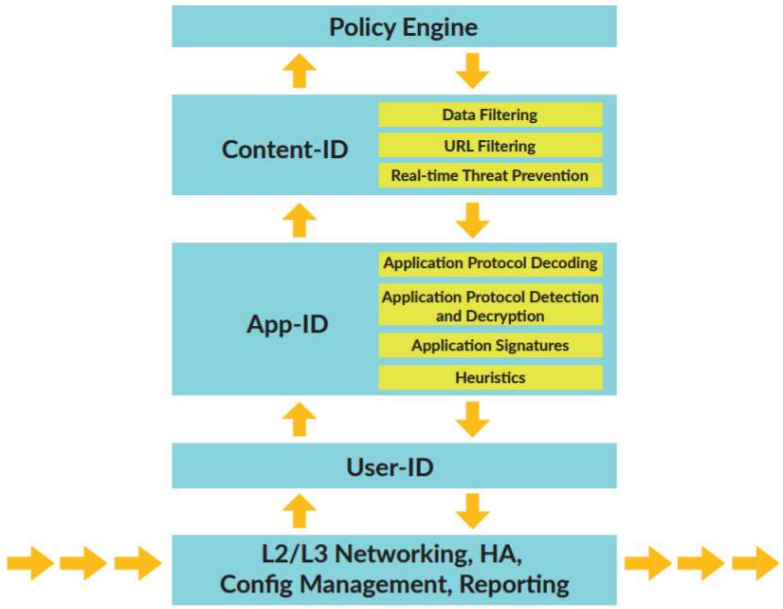
Palo Alto Networks Single-Pass Architecture

Single pass:

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

Parallel processing:

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

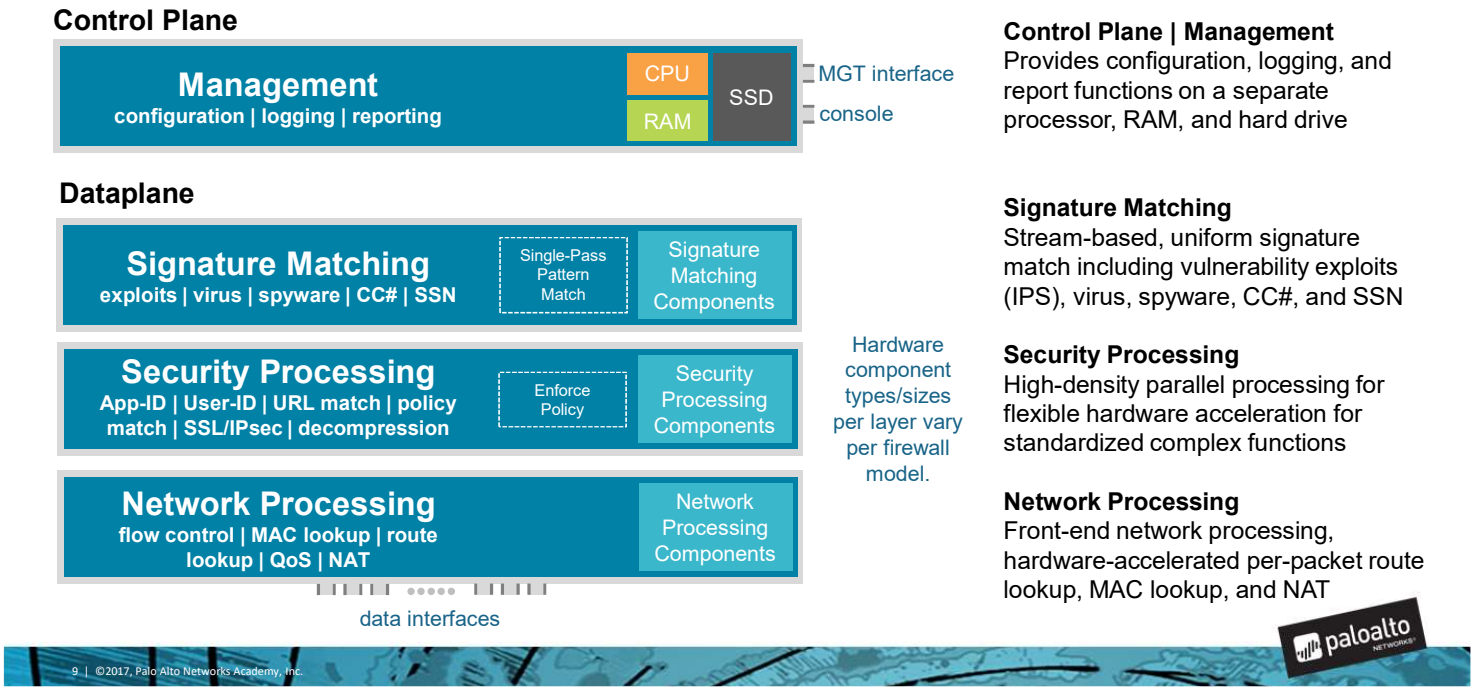


The Palo Alto Networks firewall allows you to specify Security policy rules based on a more accurate identification of each application seeking access to your network. It is unlike traditional firewalls that identify applications only by protocol and port number. It uses packet inspection and a library 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 of 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 turn on advanced features such as scanning for viruses and malware without slowing the firewall's performance.

Palo Alto Networks Firewall Architecture



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

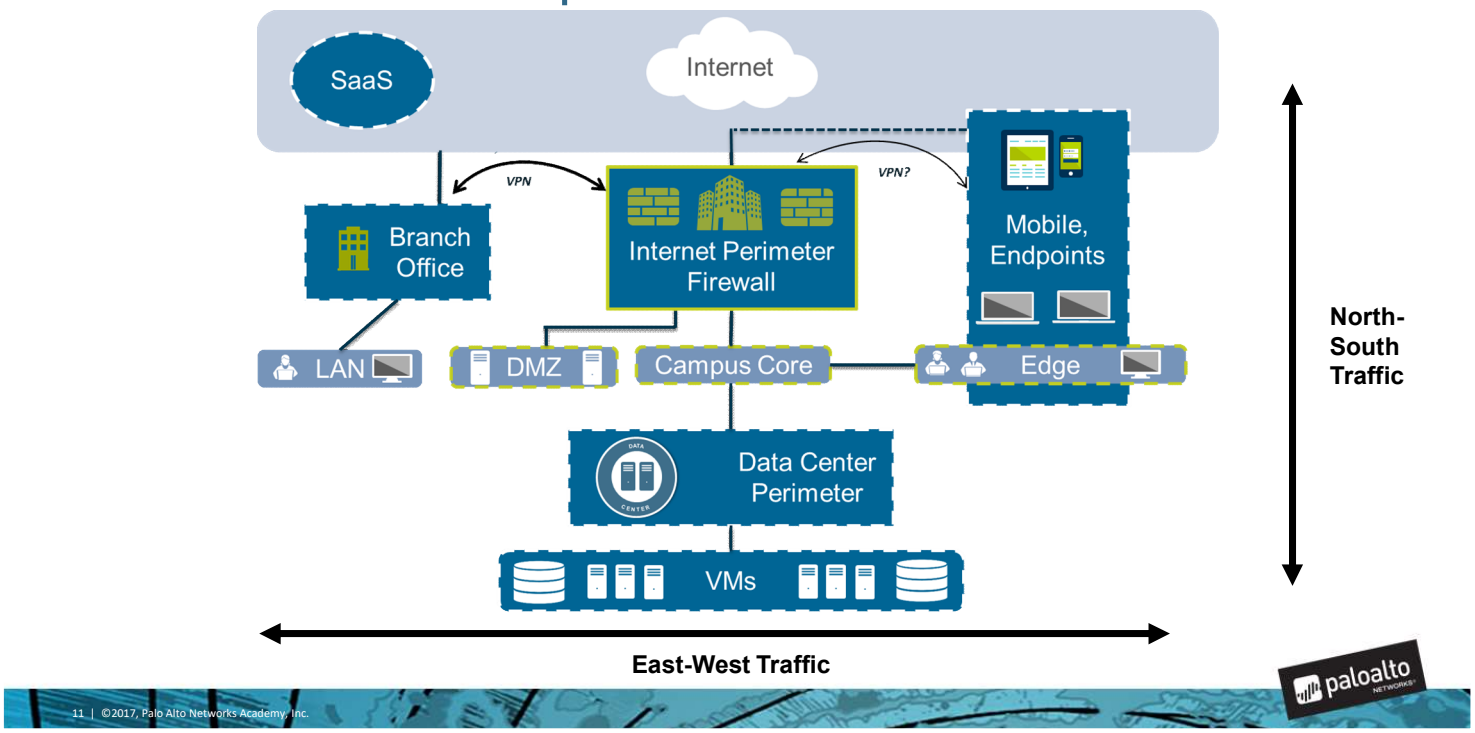
On the higher-end hardware models, the dataplane contains three types of processors that are connected by high-speed 1Gbps busses:

- Signature Match Processor scans traffic and detects:
  - Vulnerability exploits (Intrusion Prevention System)
  - Viruses
  - Spyware
  - Credit card numbers
  - Social Security numbers
- Security Processors: Multicore processors that handle security tasks such as Secure Socket 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.

Zero Trust Security Model

Data Flows in an Open Network



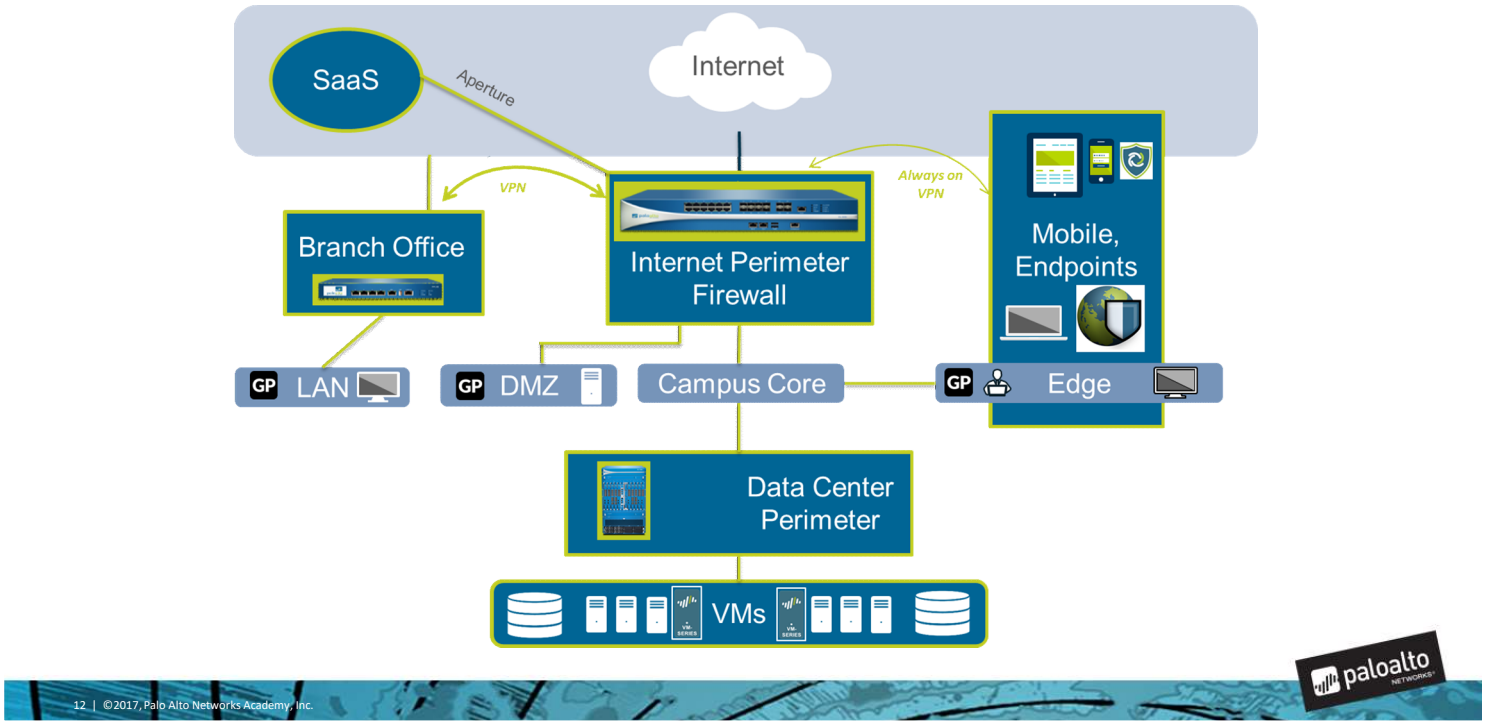
The constant cyberattacks against organizations show that perimeter security strategies alone are not effective. Without true visibility, IT and network security teams cannot control the users and applications traversing the network. Limited visibility results in organizations being vulnerable to attacks 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 datacenter.

Traffic protection from external locations where the egress point is the perimeter is commonly referred to 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/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



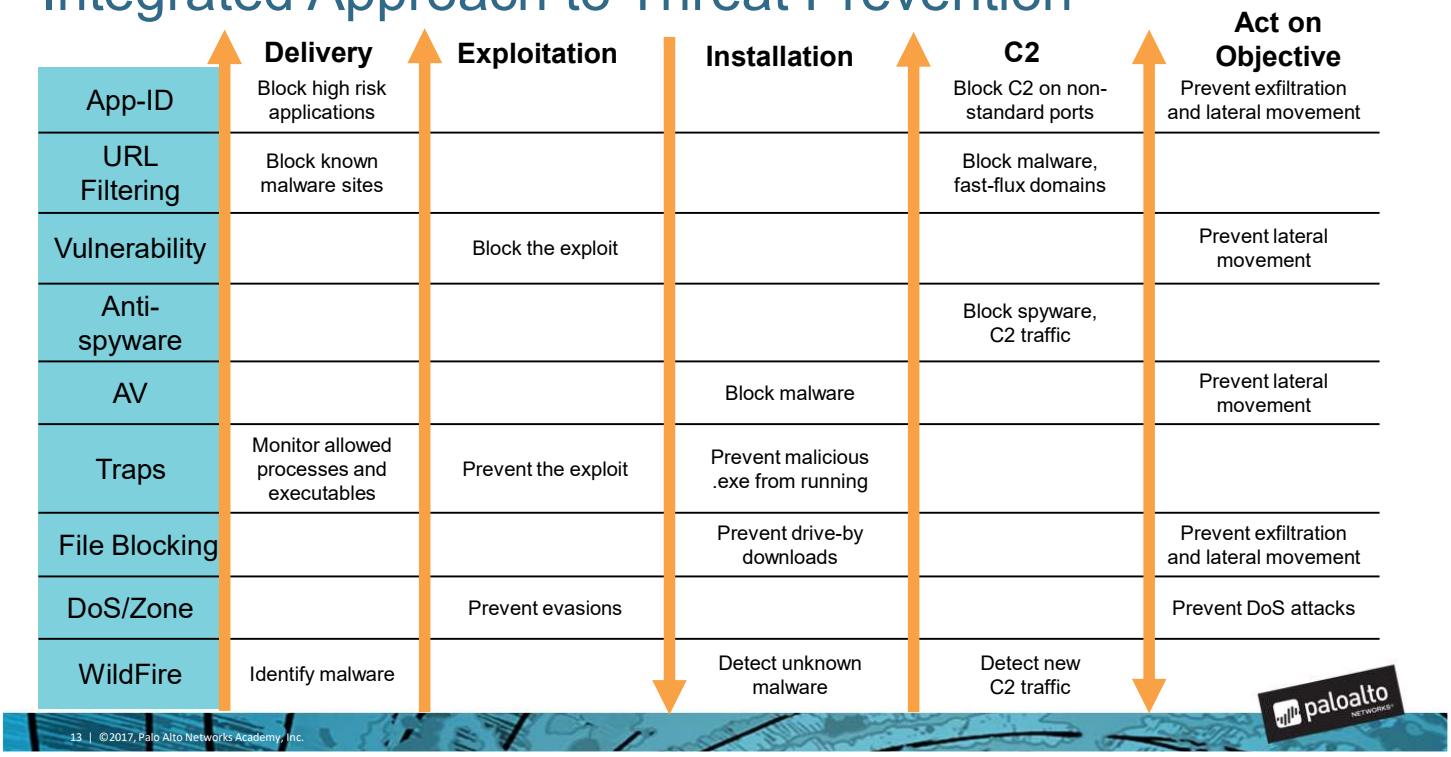
Zero Trust is an alternative security model that addresses the shortcomings of failing perimeter-centric strategies by removing the assumption of trust. With Zero Trust there is no default trust for any entity (including users, devices, applications, and packets), regardless of what it is and its location 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. This way Security policy can be enforced regardless of the point of origin and the communications traffic associated.

Trust boundaries need to do more than just provide initial authorization and access control levels of enforcement. To "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 include the following:

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

Public Cloud Security

Public Cloud Security Overview

- Protect your public cloud deployment just as you would your data center.

Hybrid	Segmentation	Internet Gateway	Remote Access
Securely deploy applications in your data center or in the cloud	Separate data and applications for compliance and security	Protect internet-facing applications	Consistent policy on the network, in the cloud, on devices

Automated Deployment and Centralized Management

- Automate firewall deployments with bootstrapping; dynamically update Security policy to ensure security keeps pace with workload changes
- Manage all aspects of the VM-Series – from configuration to policy to reporting – from a centralized location
- Enforce policy consistency across both virtualized and physical form-factor firewalls

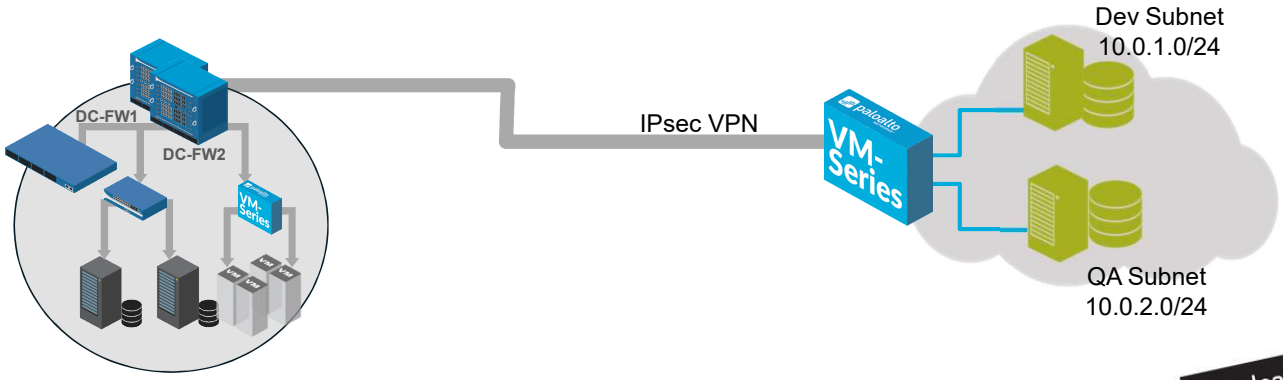
Cloud deployments have additional security challenges to overcome compared to traditional deployments:

- Traffic visibility is more limited.
- The built-in security tools are outdated and/or inconsistent.
- Process management is cumbersome.

Note: SaaS security is achieved with Aperture.

Hybrid Cloud: Quick Way to Get Started

- Extend the corporate data center into the public cloud:
  - Application dev/test/product projects are common…
- IPsec VPN protects the connection and contents.
- VM-Series NGFW features protects the content.

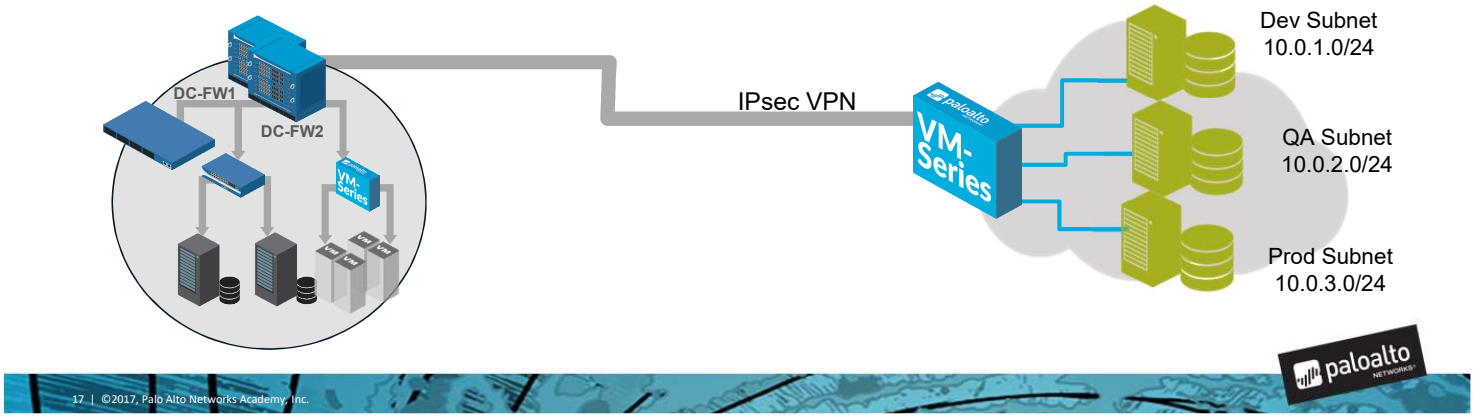


Hybrid cloud use case: Palo Alto Networks as the bridge between public and private cloud:

- Leverages existing VPN functionality
- DNAT not needed
- Operate perfectly *in front* of an internal Elastic Load Balancing (ELB) group

Application Segmentation: Expands upon Hybrid

- Maintain separation between data and applications for security and compliance
- Control which applications can communicate with each other
- Protect traffic within the VPC/vNet and traversing each subnet
- Prevent threats from moving laterally

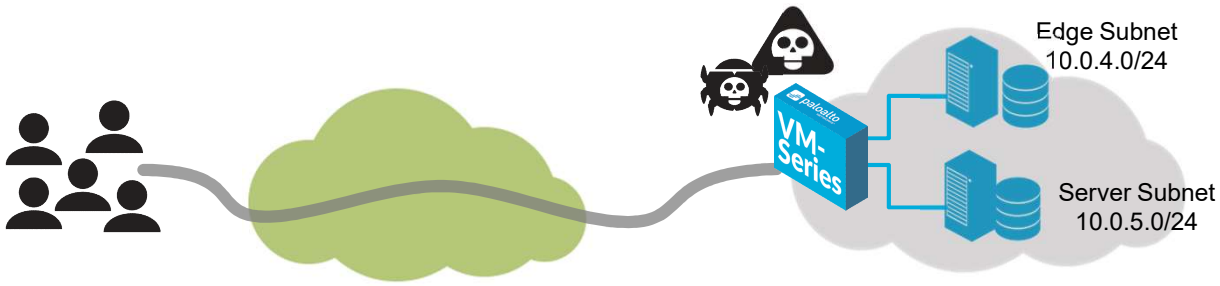


Inter-VPC use case with no Internet-sourced traffic: Zero-Trust security in the cloud:

- Security maintained as cloud resources scale out
- Operate perfectly *in front* of an internal ELB group

Internet-Facing Applications: Leverage Perimeter Controls

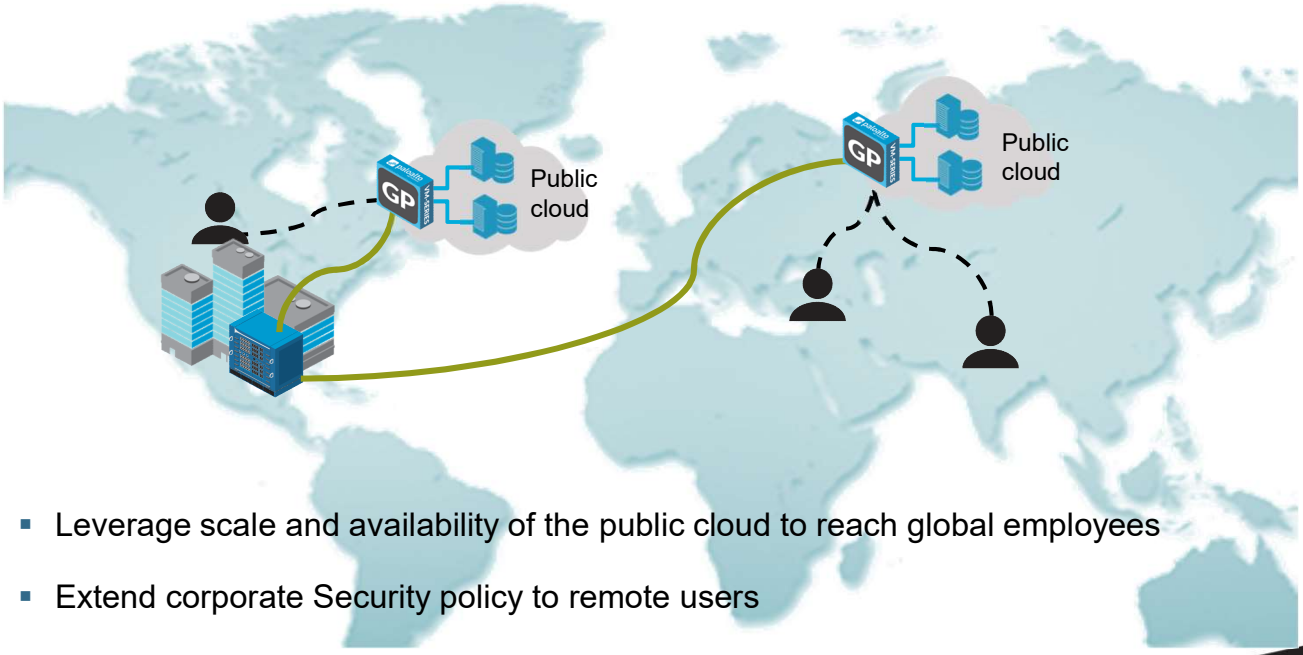
- Traditional perimeter security strengths apply:
  - Visibility: Classify all traffic based on application identity
  - Control: Enable those applications you want, deny those you don't
  - Protect: Block known and unknown threats
  - Authorize: Grant access based on user identity



ELB groups provide a limited feature set compared to current on-premise load balancers. The VM-Series firewall can be used to address these limitations:

- VM-Series: NAT to an internal ELB group
- VM-Series: Should be addressable via an FQDN specifically, because IPs can change anytime

GlobalProtect: Extend Security to All Users/Devices



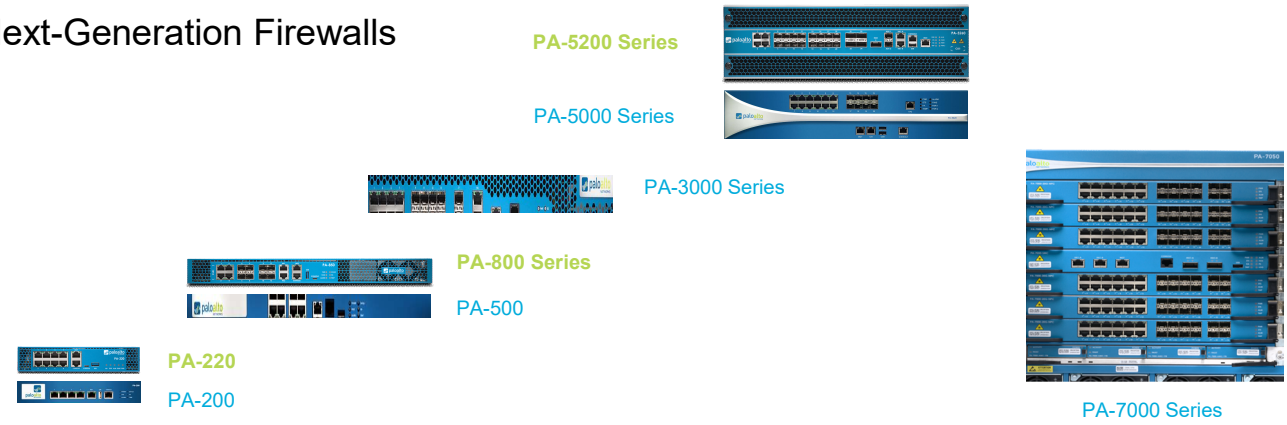
- Leverage scale and availability of the public cloud to reach global employees
- Extend corporate Security policy to remote users

GlobalProtect network security provides load balancing functionality natively, even in the cloud.

Firewall Offerings

Physical Platforms

Next-Generation Firewalls



Panorama

The PA-220, PA-800, and PA-5200 Series are next-generation hardware, released with PAN-OS® 8.0.

The PA-7050 and 7080 are chassis architecture.

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, refer to the following site: https://paloaltonetworks.com/comparefirewalls.

VM-Series Models and Capacities (PAN-OS® 8.0)

Performance and Capacities	VM-700	VM-500	VM-300	VM-100	VM-50
Firewall throughput (App-ID enabled)	**20Gbps**	**10Gbps**	**4Gbps**	**2Gbps**	**200Mbps**
Threat prevention throughput	**10Gbps**	**5Gbps**	**2Gbps**	**1Gbps**	**100Mbps**
Max sessions	10,000,000	2,000,000	800,000	250,000	50,000
Dedicated CPU cores	2, 4, 8, 16	2, 4, 8	2, 4	2	2
Dedicated memory (minimum)	48GB	16GB	9GB	6.5GB	4.5GB
Dedicated disk drive capacity (minimum)	60GB	60GB	60GB	60GB	32GB

As of PAN-OS® 8.0, the VM-Series firewalls now 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 premise equipment (CPE) and network tenant environments, improved performance and efficiency for perimeter and east-west data-center traffic, and maximized performance to support network function virtualization (NFV).

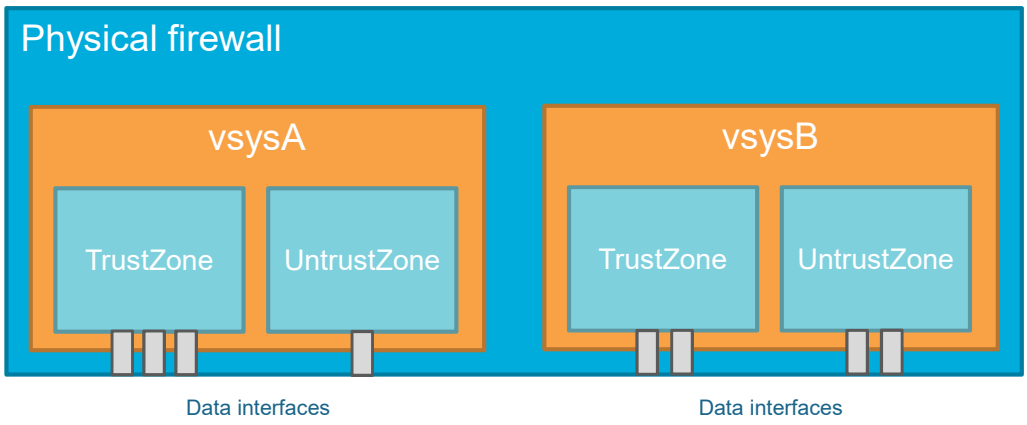
All VM-Series firewalls use a unified licensing system, which is platform-agnostic. For example, a VM-100 perpetual license can be used to license a VM running on Hyper-V or in AWS.

Supported Environments	**VM-Series Models**
VMware ESXi	**All**
KVM/OpenStack	**All**
Hyper-V	**All**
VMware NSX	**VM 100 through 500**
AWS	**VM 100 through 700**
Microsoft Azure	**VM 100 through 700**

- New sessions per second (all models): 8,000
- IPsec VPN throughput (all models): 250Mbps

Virtual Systems

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



Virtual systems are separate, logical firewall instances within a single physical Palo Alto Networks firewall. Rather than using 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 (vsys) is an independent, separately managed firewall with its traffic kept separate from the traffic of other virtual systems.

A virtual system 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. By using 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-3000, PA-5000, and PA-7000 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-3000 Series firewalls, and to create more than the base number of virtual systems supported on a platform.

Questions?