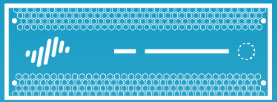
SECURITY OPERATING PLATFORM AND ARCHITECTURE



EDU-210 Version A
PAN-OS® 9.0

PREVENTION EVERYWHERE

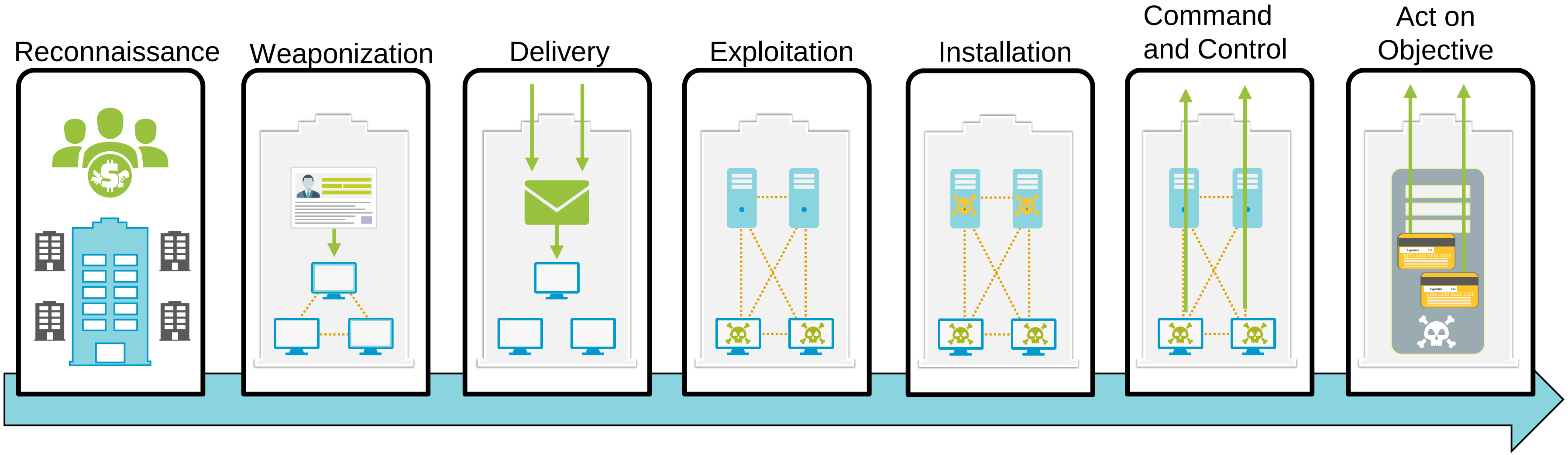
- Security platform overview
- Next-generation firewall architecture
- Zero Trust security model
- Firewall offerings

Learning Objectives

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

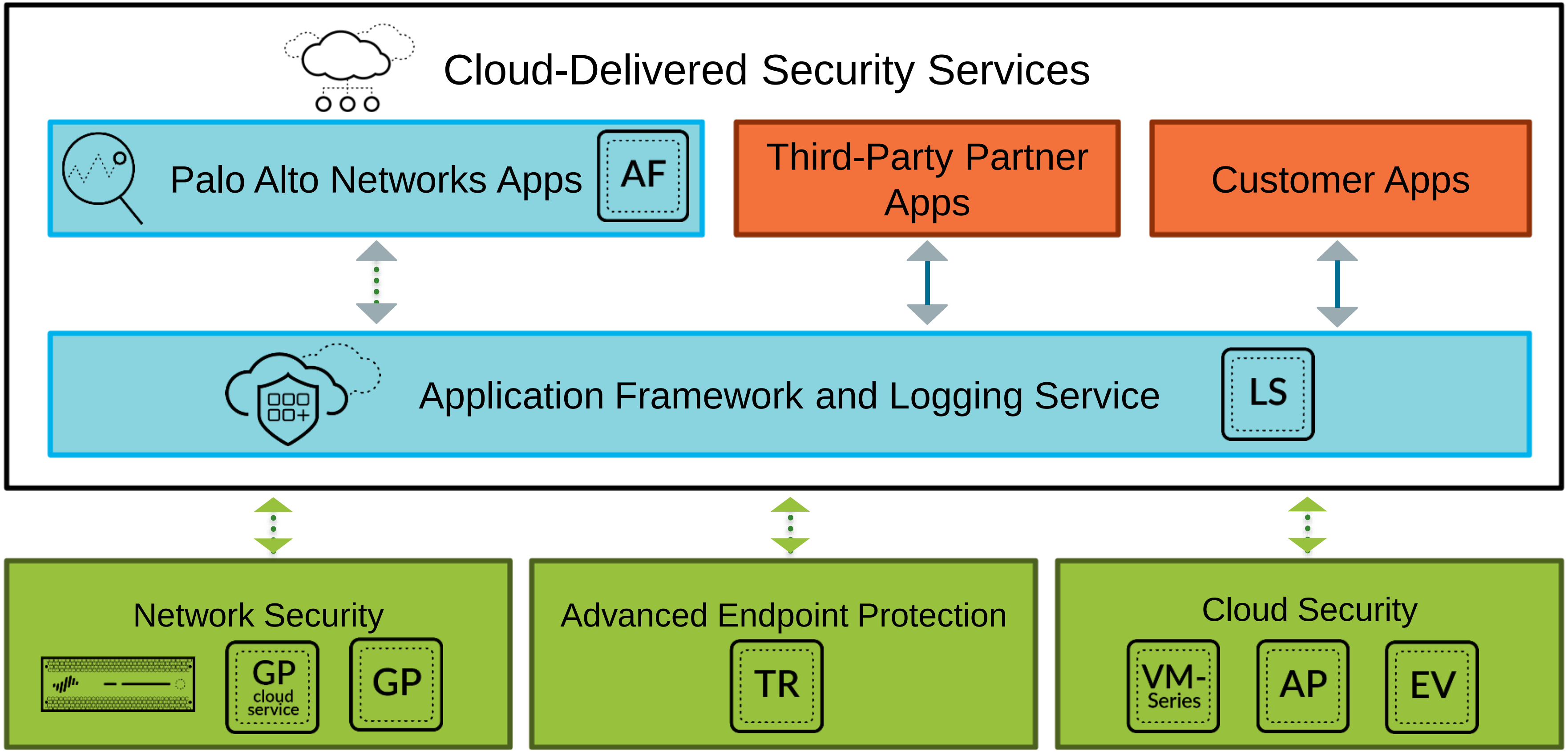
- Describe the characteristics of the Security Operating Platform
- Describe the single-pass architecture
- Describe the Zero Trust security model and how it relates to traffic moving through your network

Cyber-attack Lifecycle



Stop the attack at any point!

Security Operating Platform



Cloud-Delivered Security Services

Palo Alto Networks Apps

Third-Party Partner Apps

Customer Apps

Application Framework and Logging Service

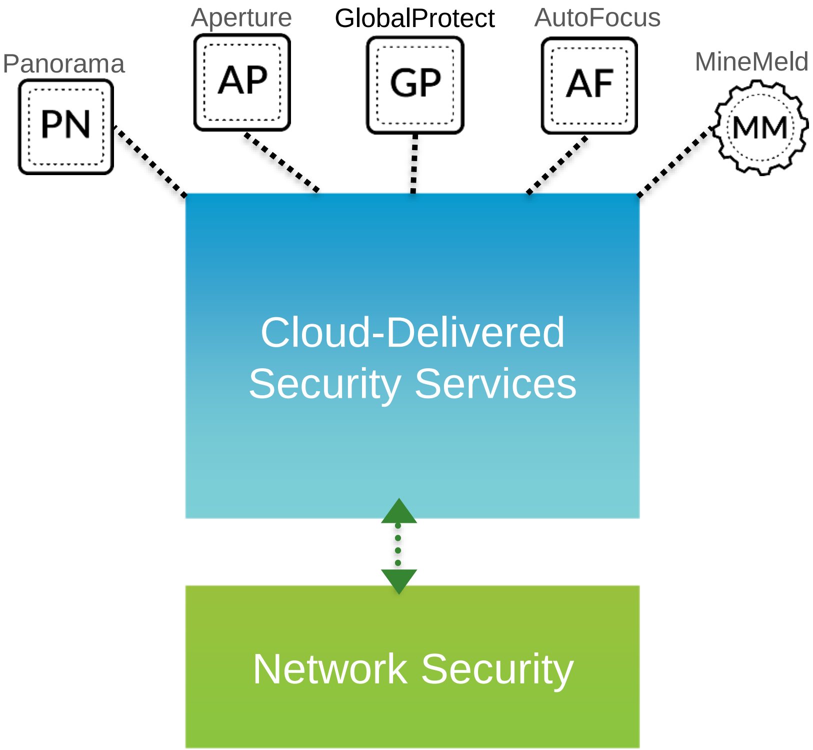
Network Security

Advanced Endpoint Protection

Cloud Security

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



Security platform overview

Next-generation firewall architecture

Zero Trust security model

Firewall offerings

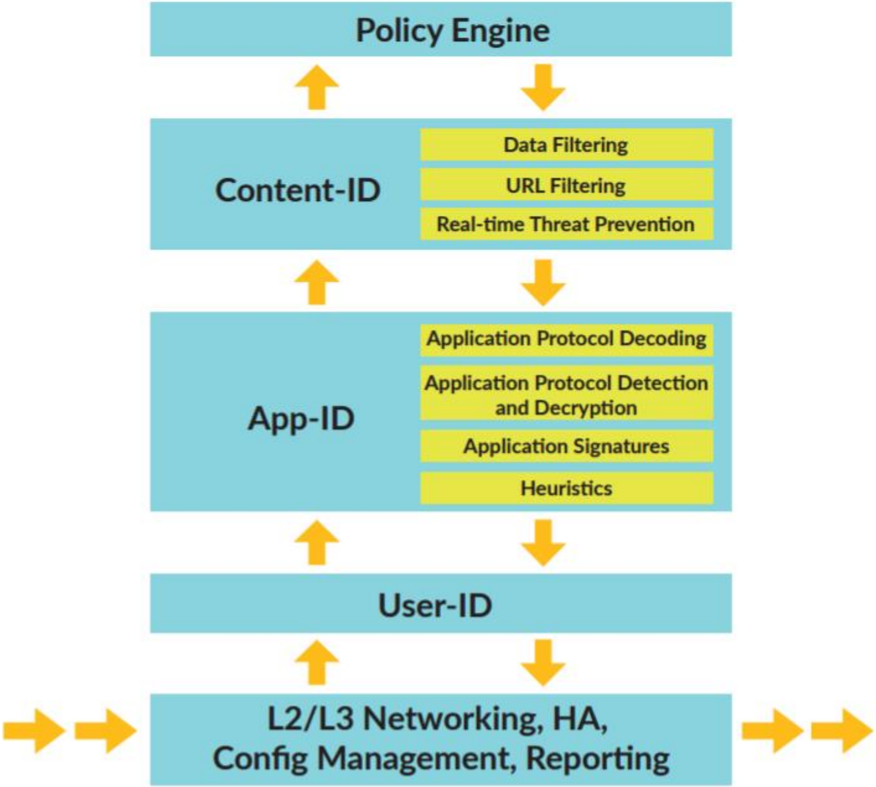
Palo Alto Networks Single-Pass Architecture

Single pass:

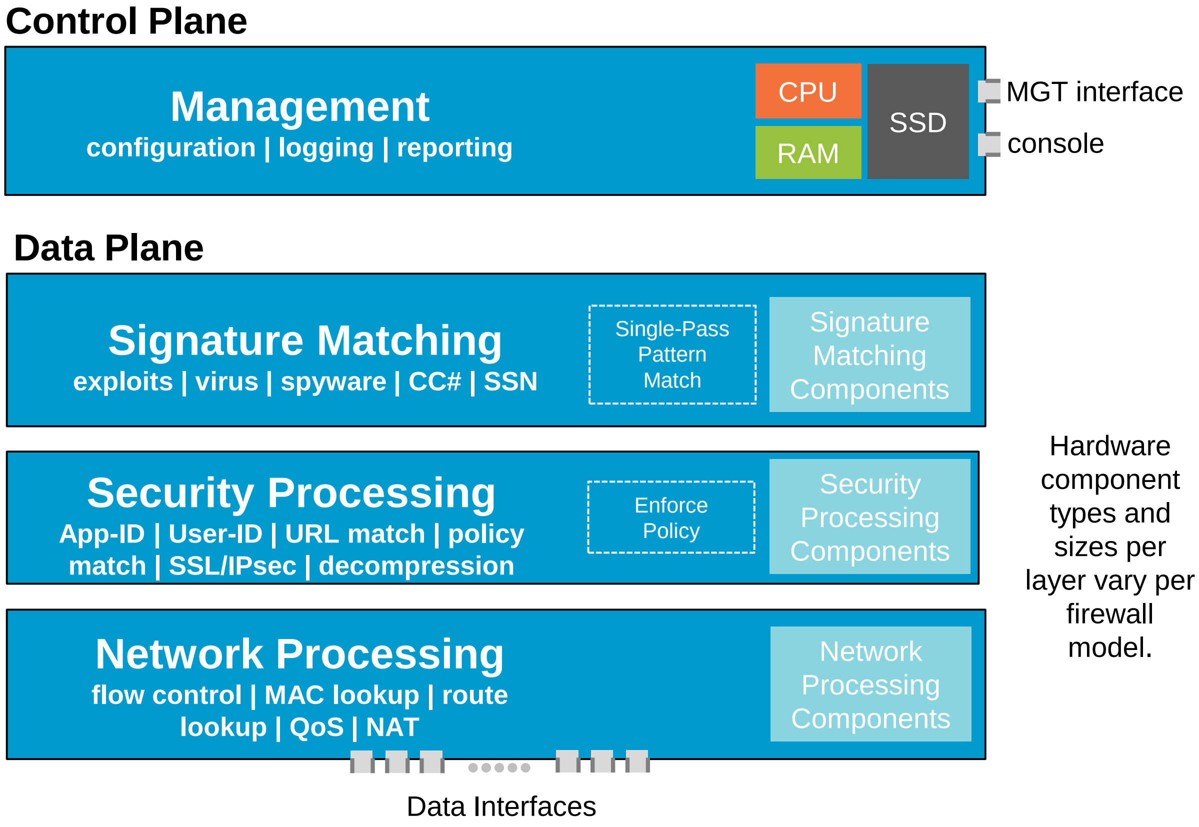
- Operations per packet:
  - Traffic classification with App-ID technology
  - User or group mapping
  - Content scanning: threats, URLs, confidential data
- One single policy (per type)

Parallel processing:

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


Policy Engine
Content-ID
Data Filtering
URL Filtering
Real-time Threat Prevention
App-ID
Application Protocol Decoding
Application Protocol Detection and Decryption
Application Signatures
Heuristics
User-ID
L2/L3 Networking, HA, Config Management, Reporting

Palo Alto Networks Firewall Architecture


Control Plane
Management
configuration | logging | reporting
CPU
RAM
SSD
MGT interface
console
Data Plane
Signature Matching
exploits | virus | spyware | CC# | SSN
Single-Pass Pattern Match
Signature Matching Components
Security Processing
App-ID | User-ID | URL match | policy match | SSL/IPsec | decompression
Enforce Policy
Security Processing Components
Network Processing
flow control | MAC lookup | route lookup | QoS | NAT
Network Processing Components
Data Interfaces

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

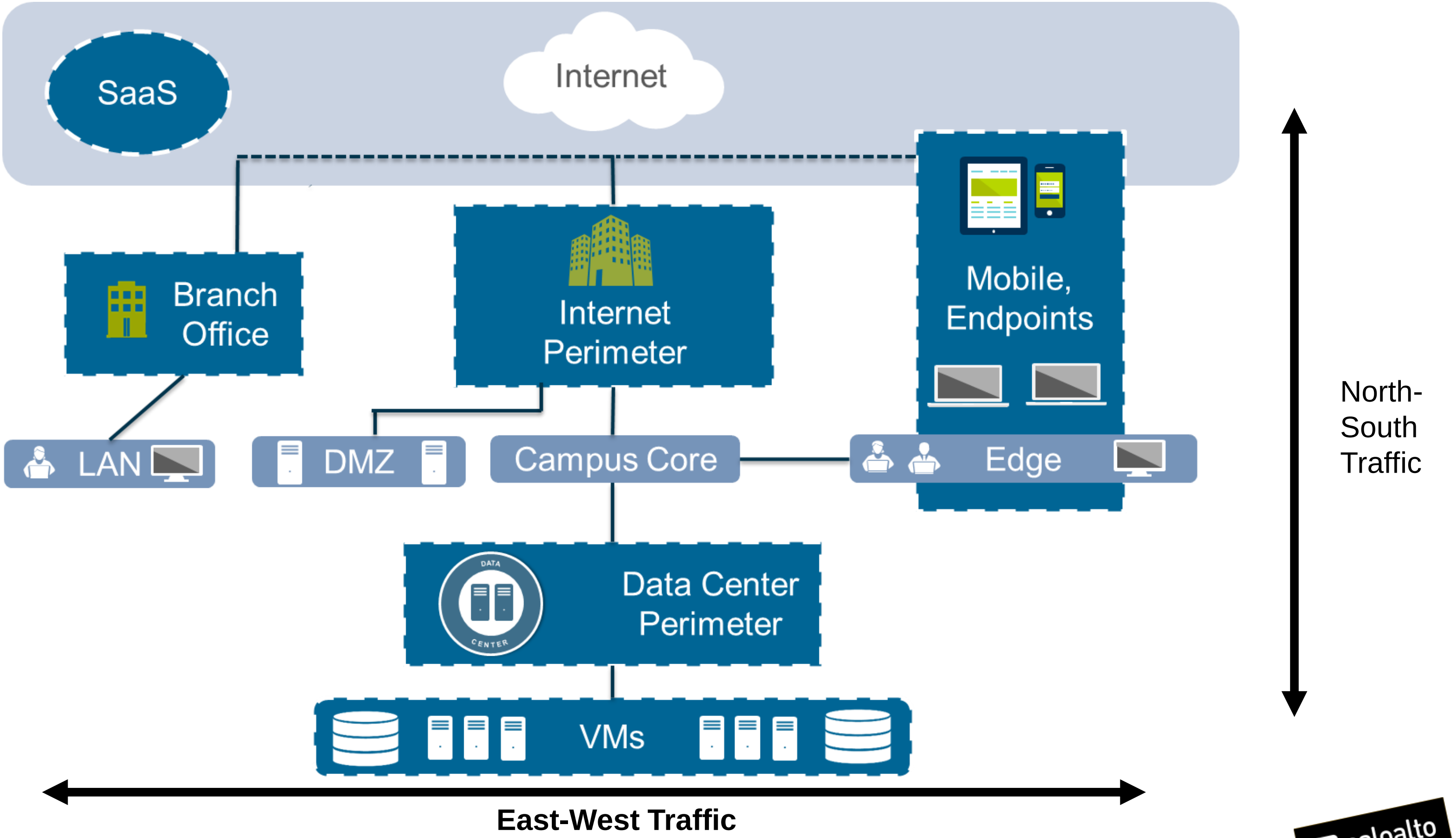
Security platform overview

Next-generation firewall architecture

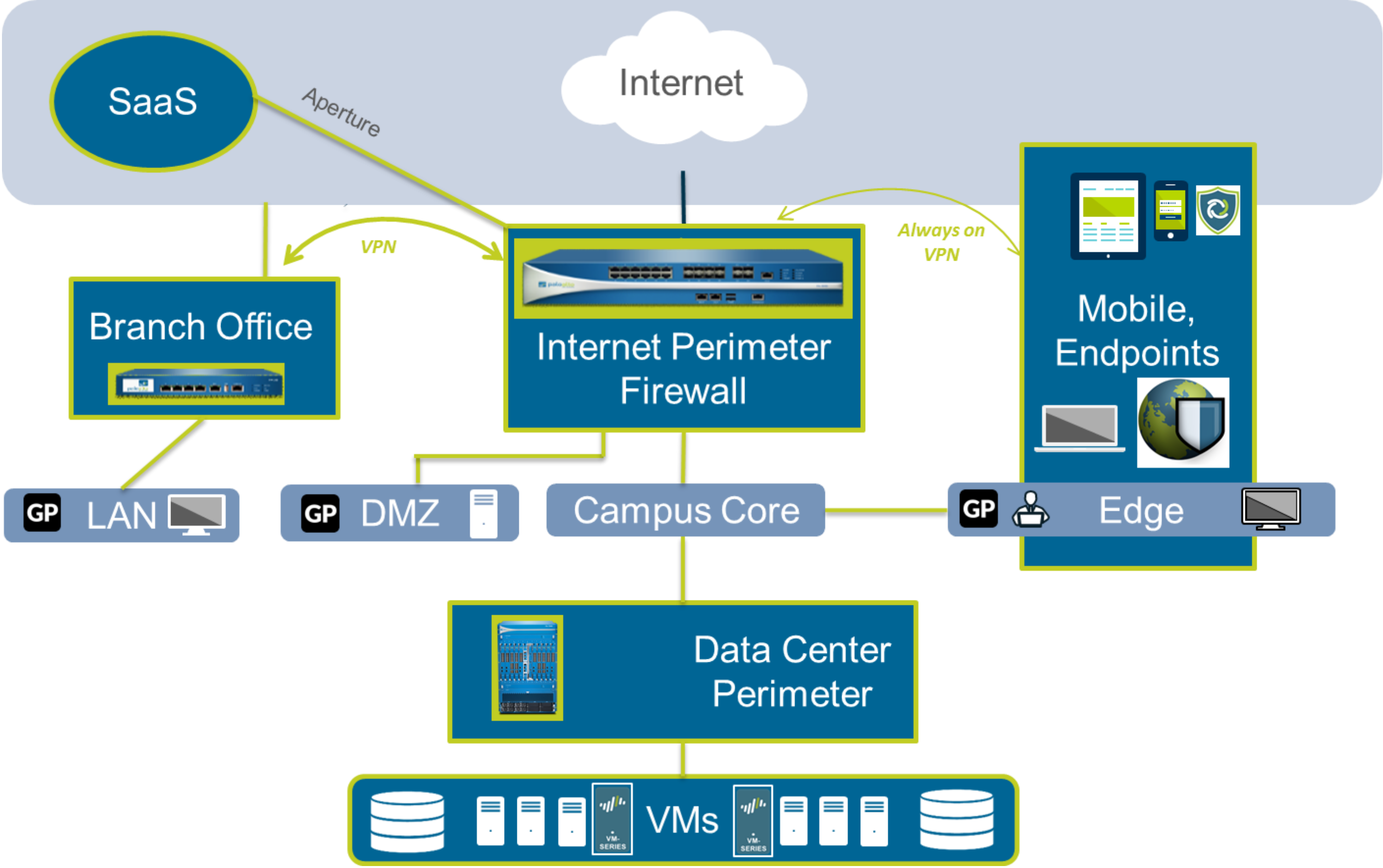
Zero Trust security model

Firewall offerings

Data Flows in an Open Network



Data Flows Secured by Palo Alto Networks Solution



Integrated Approach to Threat Prevention

	Delivery	Exploitation	Installation	C2	Act on Objective
App-ID	Block high-risk applications			Block C2 on non-standard ports	Prevent exfiltration and lateral movement
URL Filtering	Block known malware sites			Block malware, fast-flux domains	
Vulnerability		Block the exploit			Prevent lateral movement
Anti-spyware				Block spyware, C2 traffic	
Antivirus			Block malware		Prevent lateral movement
Traps	Monitor allowed processes and executables	Prevent the exploit	Prevent malicious .exe from running		
File Blocking			Prevent drive-by downloads		Prevent exfiltration and lateral movement
DoS and/or Zone		Prevent evasions			Prevent DoS attacks
WildFire®	Identify malware		Detect unknown malware	Detect new C2 traffic	

Security platform overview

Next-generation firewall architecture

Zero Trust security model

Firewall offerings

Physical Platforms

Next-Generation Firewalls

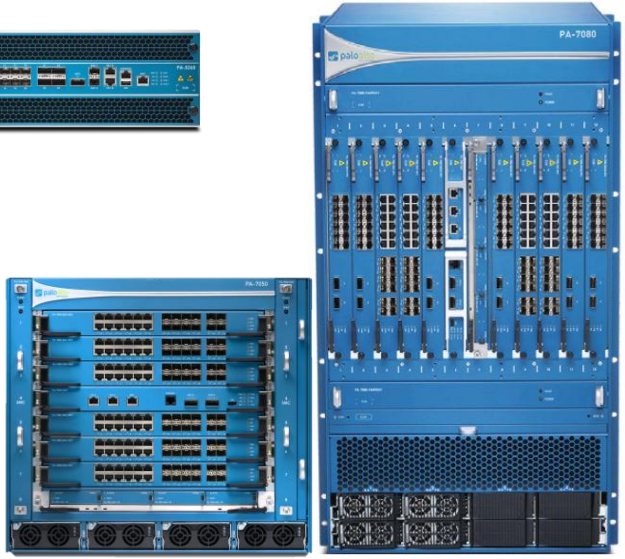
PA-5200 Series

PA-3200 Series

PA-800 Series

PA-220R

PA-220



PA-7000 Series

Panorama

M-200

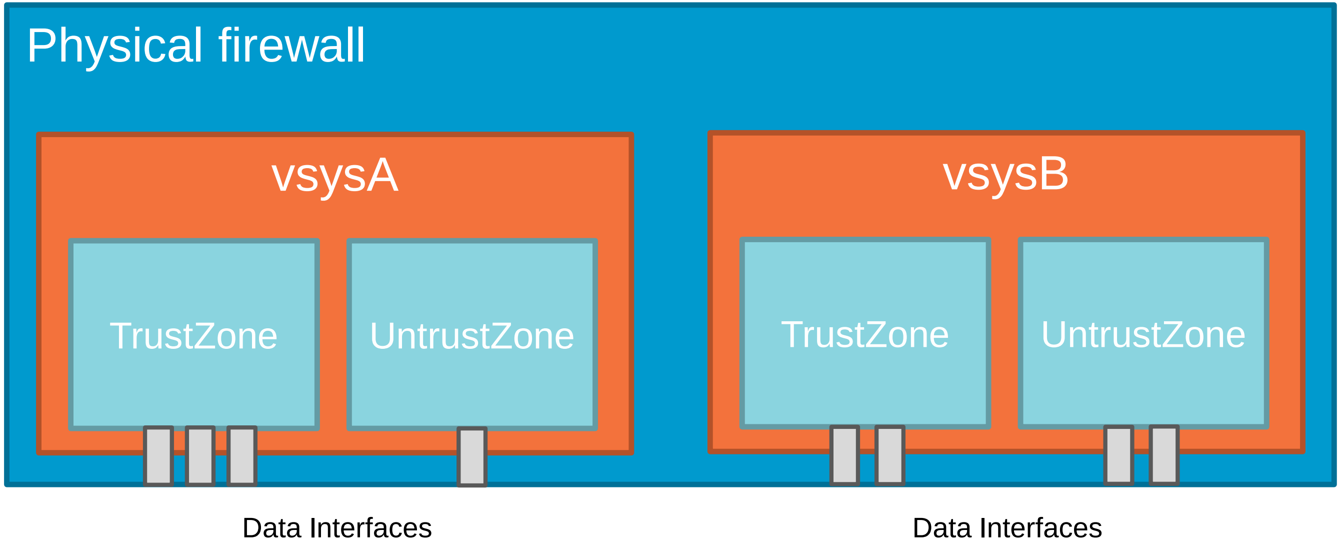
M-500/WF-500/600

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

Virtual Systems

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



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

Questions?

PROTECTION. DELIVERED.

paloalto NETWORKS®

This page intentionally left blank