

# Architecture

*SE Boot Camp*

*PAN-OS 8.0*

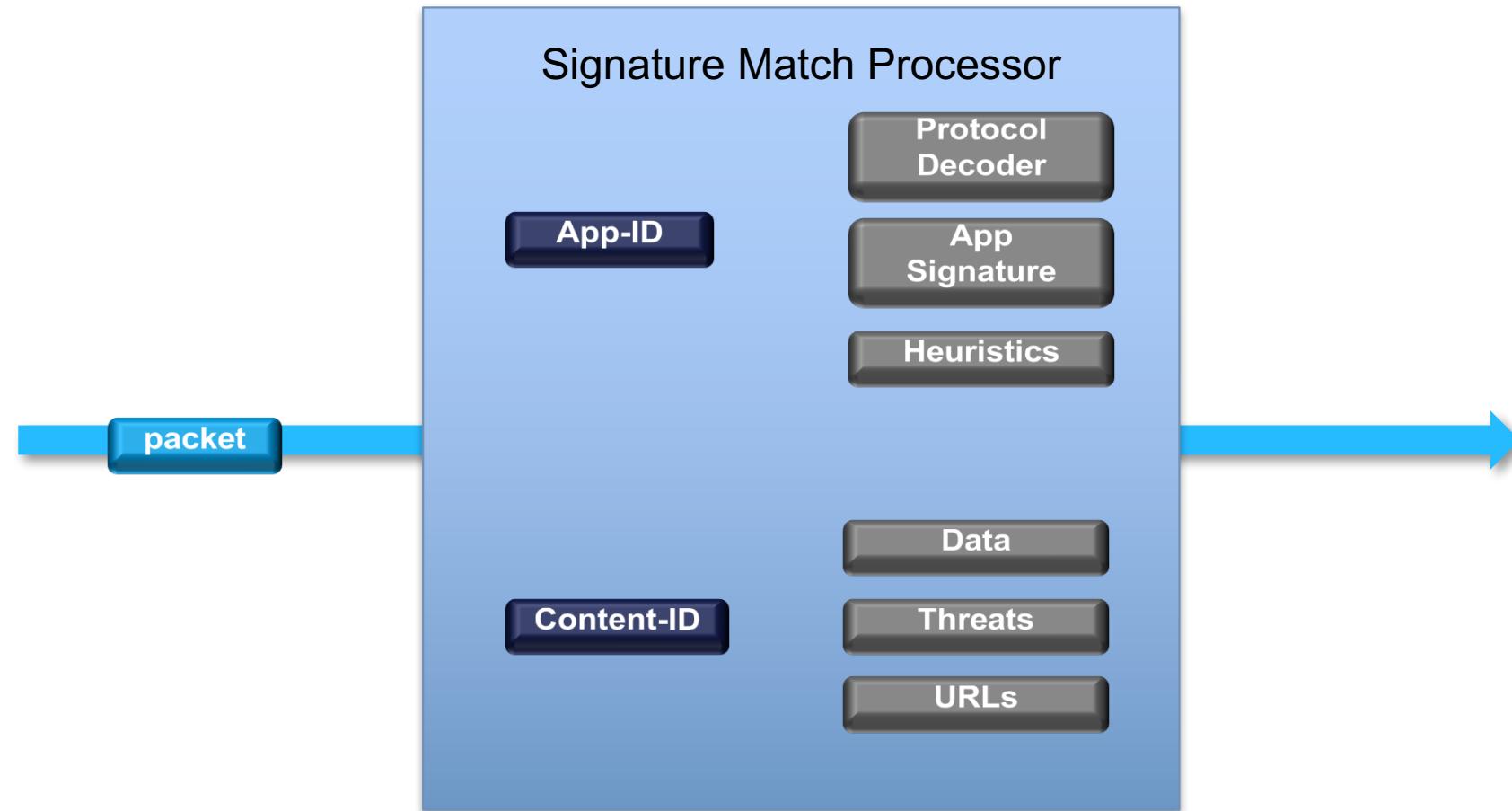


# Agenda

- Single Pass Architecture
- General Architecture
- Flow Logic
- Firewall Models

# General Architecture

# Single Pass Architecture



# Palo Alto Networks Firewall Architecture



## Control Plane | Management

Provides configuration, logging, and report functions on a separate process, RAM, and hard drive

## Signature Matching

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

## Security Processing

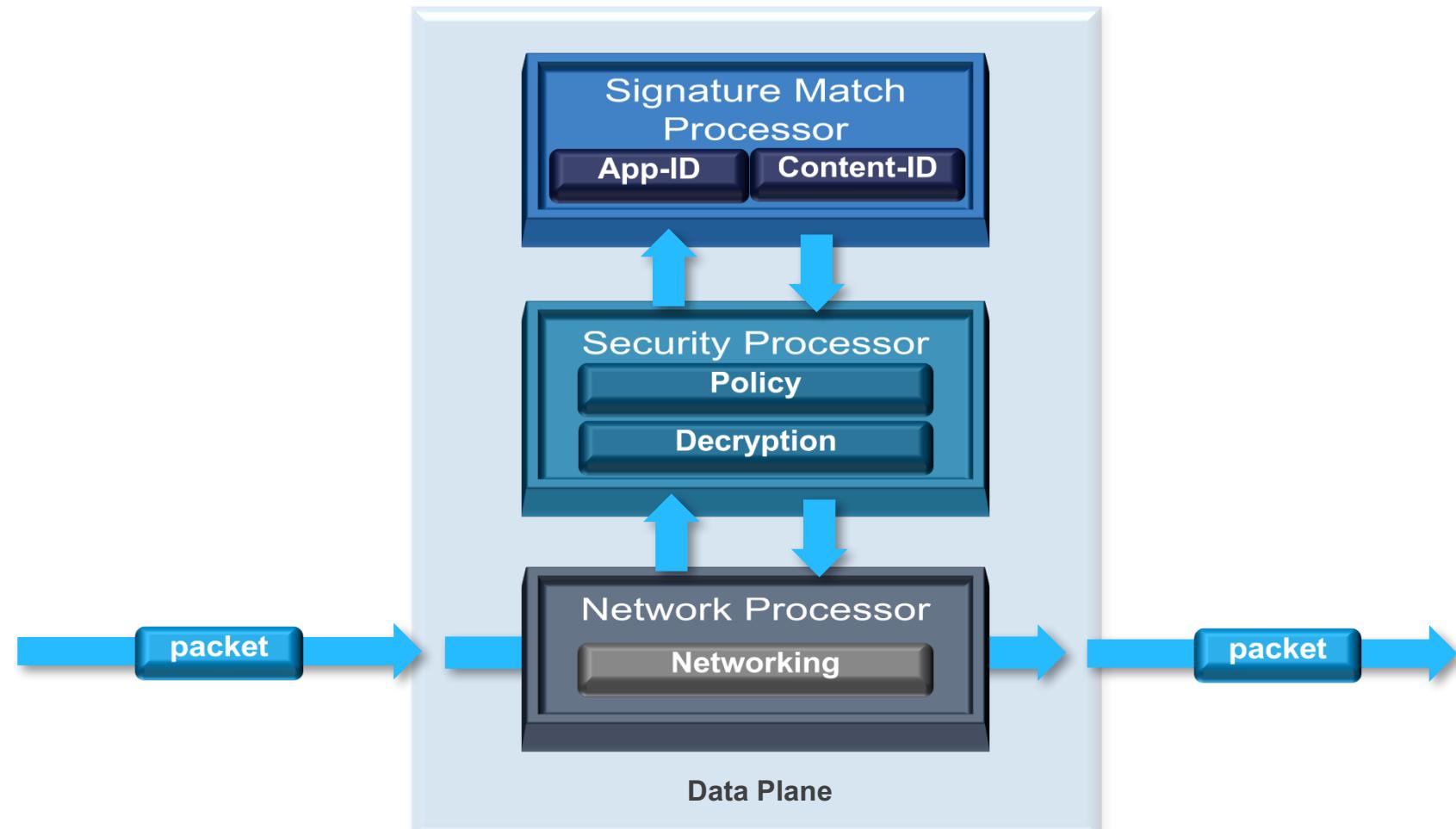
High-density parallel processing for flexibility hardware-acceleration for standardized complex functions

## Network Processing

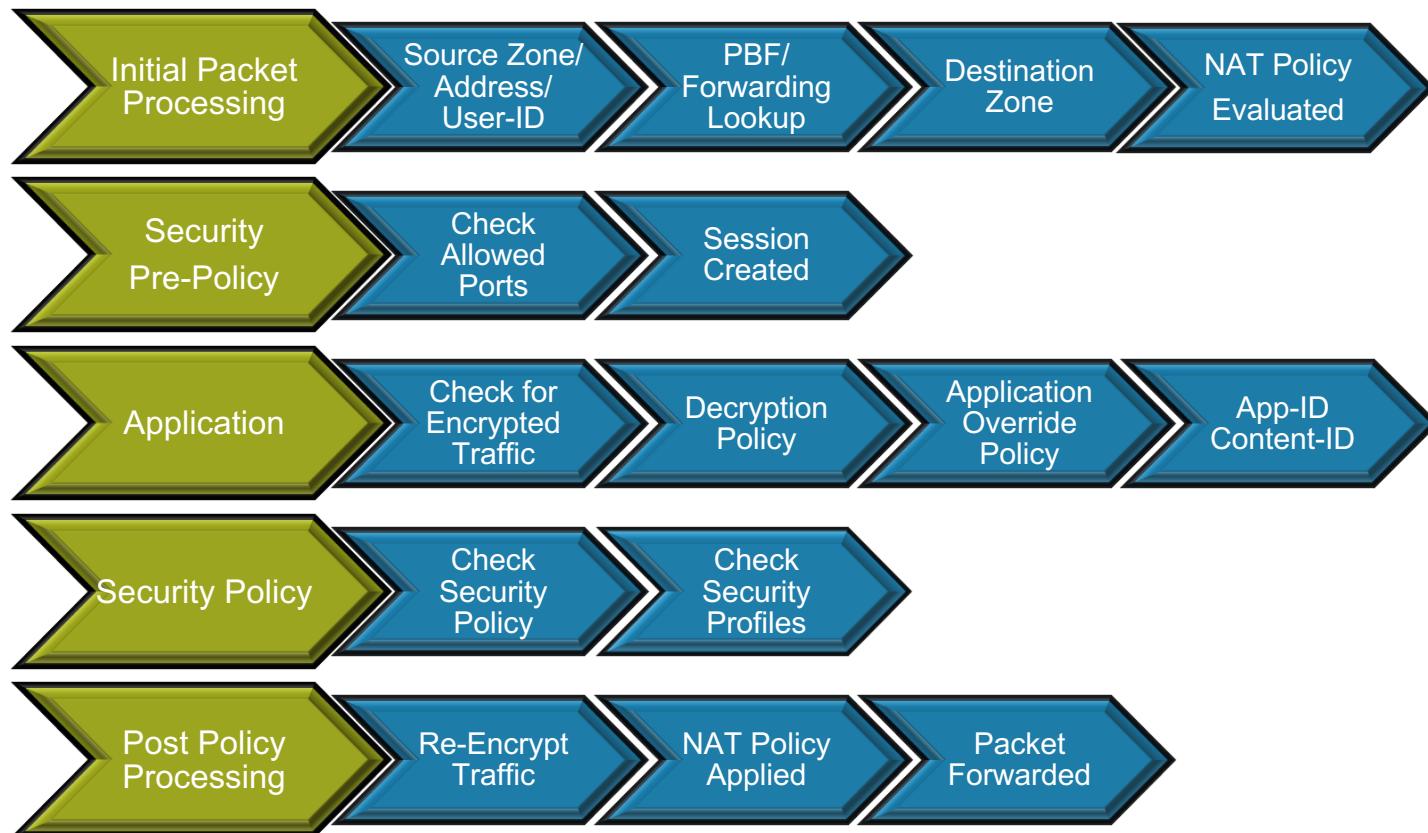
Front-end network processing, hardware accelerated per-packet route lookup, MAC lookup, and NAT

Components can be implemented in hardware or virtually

# Processing Flow



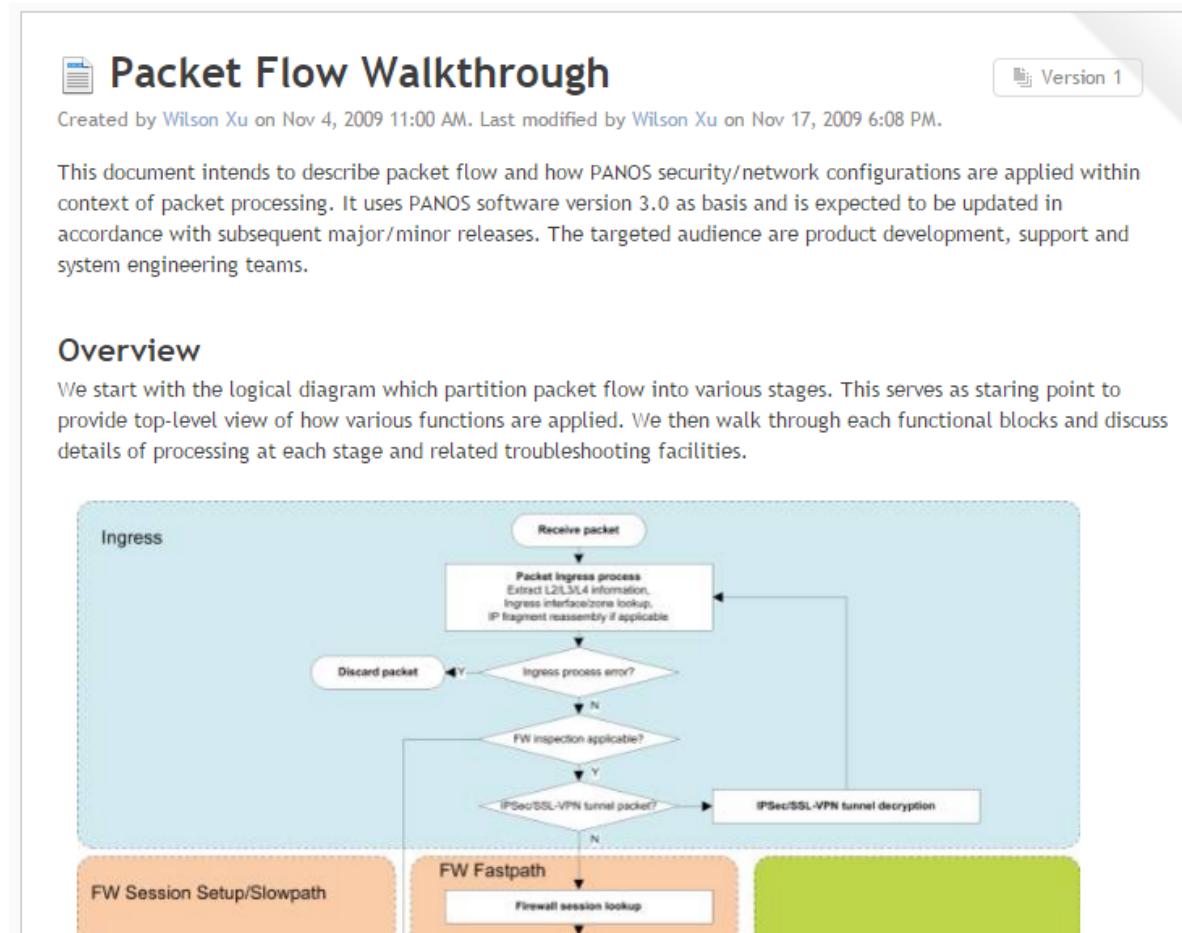
# Flow Logic of the Next-Generation Firewall



# Detailed Packet Flow Walkthrough

Excellent reference document for the packet flow, written by our VP of Engineering Wilson Xu:

<https://intranet.paloaltonetworks.com/docs/DOC-1964>

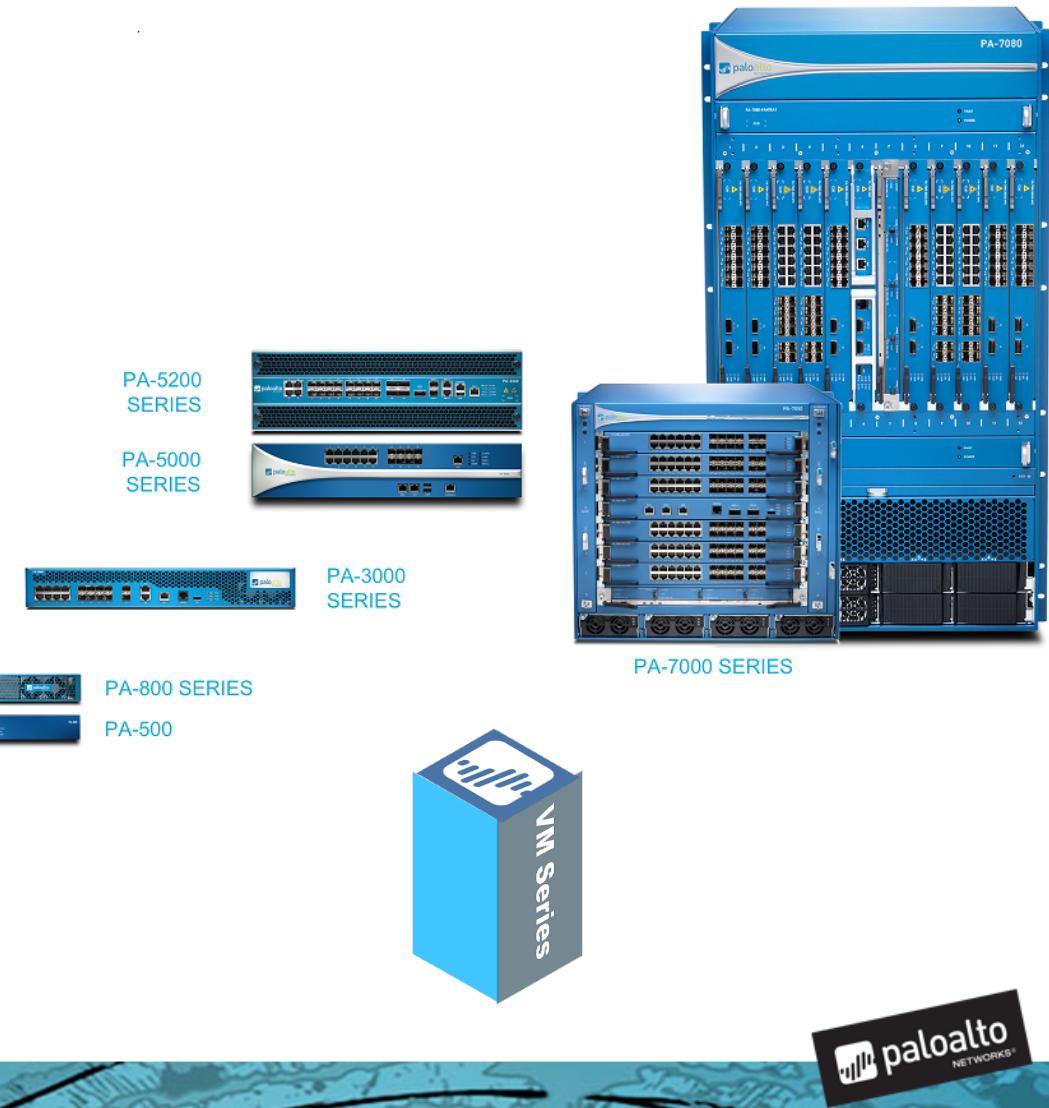


# Firewall Models

# Firewall Platforms

## Current Platforms

- PA-200
- PA-220
- PA-500
- PA-800
- PA-3000 Series
- PA-5000 Series
- PA-5200 Series
- PA-7000 Series
- VM-Series



## End-of-Sale Platforms

- PA-2000 Series
- PA-4000 Series

# Product Summary Specsheets

<https://paloaltonetworks.com/resources/datasheets/product-summary-specsheet.html/>

The screenshot shows the 'Product Summary Specsheets' page on the Palo Alto Networks website. The top navigation bar includes the Palo Alto Networks logo, user information ('Logged in as: Calvin Mangubat'), a 'Get Support' button, a search icon, language selection ('EN'), and a 'MENU'. The breadcrumb navigation shows 'Home > Resources > Resource Center > Product Summary Specsheets - Palo Alto Networks'. The main title 'Product Summary Specsheets' is displayed over a background image of a network mesh. On the left, there's a large orange 'DOWNLOAD' button with a red oval highlighting it, followed by download statistics ('71760 downloads') and a rating ('39'). Below this, the date 'May 04, 2017 at 03:45 PM' and the text 'Key features, performance capacities and spec' are visible. To the right, a table titled 'Platform Specifications and Features Summary' compares six products: PA-7080 System, PA-7050 System, PA-5260, PA-5250, PA-5220, PA-3260, PA-3250, and PA-5220. The table includes sections for 'Performance and Capacities' and 'Hardware Specifications'. The bottom of the page features a blue footer with the Palo Alto Networks logo and the text '11 | © 2016, Palo Alto Networks, Inc.'

Platform Specifications and Features Summary					
Performance and Capacities <sup>1</sup>	PA-7080 System <sup>2</sup>	PA-7050 System <sup>2</sup>	PA-5260	PA-5250	PA-5220
Firewall throughput (App-ID)	200 Gbps	120 Gbps	72.2 Gbps	35.9 Gbps	18.5 Gbps
Threat prevention throughput	100 Gbps	60 Gbps	30 Gbps	20.3 Gbps	9.2 Gbps
IPSec VPN throughput	80 Gbps	48 Gbps	21 Gbps	14 Gbps	5 Gbps
New sessions per second	1,200,000	720,000	458,000	348,000	169,000
Max sessions	40,000,000/80,000,000 <sup>3</sup>	24,000,000/48,000,000 <sup>3</sup>	32,000,000	8,000,000	4,000,000
Virtual systems (base/max <sup>4</sup> )	25/225	25/225	25/225	25/125	10/20
Hardware Specifications	PA-7080 System	PA-7050 System	PA-5260	PA-5250	PA-5220
Interfaces supported NPC option 1 <sup>4</sup>	Up to (20) QSFP+, (120) SFP+	Up to (12) QSFP+, (72) SFP+	(4) 100/1000/10G Cu, (16) 1G/10G SFP/SFP+, (4) 40G/100G QSFP28	(4) 100/1000/10G Cu, (16) 1G/10G SFP/SFP+, (4) 40G/100G QSFP28	(4) 100/1000/10G Cu, (16) 1G/10G SFP/SFP+, (4) 40G QSFP+
Interfaces supported NPC option 2 <sup>4</sup>	Up to (120) 10/100/1000, (80) SFP, (40) SFP+	Up to (72) 10/100/1000, (48) SFP, (24) SFP+	(2) 10/100/1000 Cu, (1) 10/100/1000 out-of-band management, (1) RJ45 console	(1) 40G/100G QSFP28 HA	(1) 40G QSFP+ HA
Management I/O	(2) 10/100/1000, (2) QSFP+ high availability, (1) 10/100/1000 out-of-band management, (1) RJ45 console	9U, 19" standard rack or 14U, 19"	3U, 19" standard rack		
Rack mountable?	19U, 19" standard rack				

# Product Comparison URL

Beyond the datasheets, this is the best publicly-accessible place to go to get detailed capabilities of all the platforms:

<https://www.paloaltonetworks.com/products/product-selection.html>

The screenshot shows the Palo Alto Networks product comparison interface. At the top, there's a navigation bar with the Palo Alto Networks logo, user information (Calvin Mangubat), support links, and a search bar. Below the navigation, the page title is "Compare Firewalls". On the left, there are three main filter categories: "Performance", "Current Filters", and "Viewing all results". Under "Performance", there are three sections: "APP-ID FIREWALL THROUGHPUT", "THREAT PREVENTION THROUGHPUT", and "CONNECTIONS PER SECOND". Each section has a list of performance ranges with their respective counts in parentheses. To the right of these filters, there are three product cards for the PA-7080, PA-7050, and PA-7000-20GQXM-NPC firewalls. Each card includes a thumbnail image of the hardware, the model name, a brief description of its key features, and a "Compare" button.

Model	App-ID firewall throughput	Threat prevention throughput	Connections per second	Max sessions (IPv4 or IPv6)
PA-7080	200 Gbps 100 Gbps	1,200,000	80,000,000	
PA-7050	120 Gbps 60 Gbps	720,000	48,000,000	
PA-7000-20GQXM-NPC	20 Gbps 10 Gbps	120,000	8,000,000	

## Multi-Data Plane Firewalls

# PA-5200 SERIES

- New advanced architecture delivers up to 72 Gbps\* App-ID and 30 Gbps\* Threat Prevention performance
- Up to 32M sessions; 3.2M SSL decrypt session capacity
- Higher 10G port density, 40G and 100G interface support for diverse deployments



\* Performance specs with new platforms based on testing using HTTP traffic with 64K transaction sizes to get a mix of packet sizes on a common application protocol.

# PA-5200 SERIES SPECIFICATIONS

PA-5260



- 72.2 Gbps App-ID
- 30 Gbps Threat Prevention
- 21 Gbps IPSec VPN
- 32,000,000 sessions
- (4) 40G/100G QSFP28
- (16) 1G/10G SFP/SFP+
- (4) 100/1000/10G Copper

PA-5250



- 35.9 Gbps App-ID
- 20.3 Gbps Threat Prevention
- 14 Gbps IPSec VPN
- 8,000,000 sessions
- (4) 40G/100G QSFP28
- (16) 1G/10G SFP/SFP+
- (4) 100/1000/10G Copper

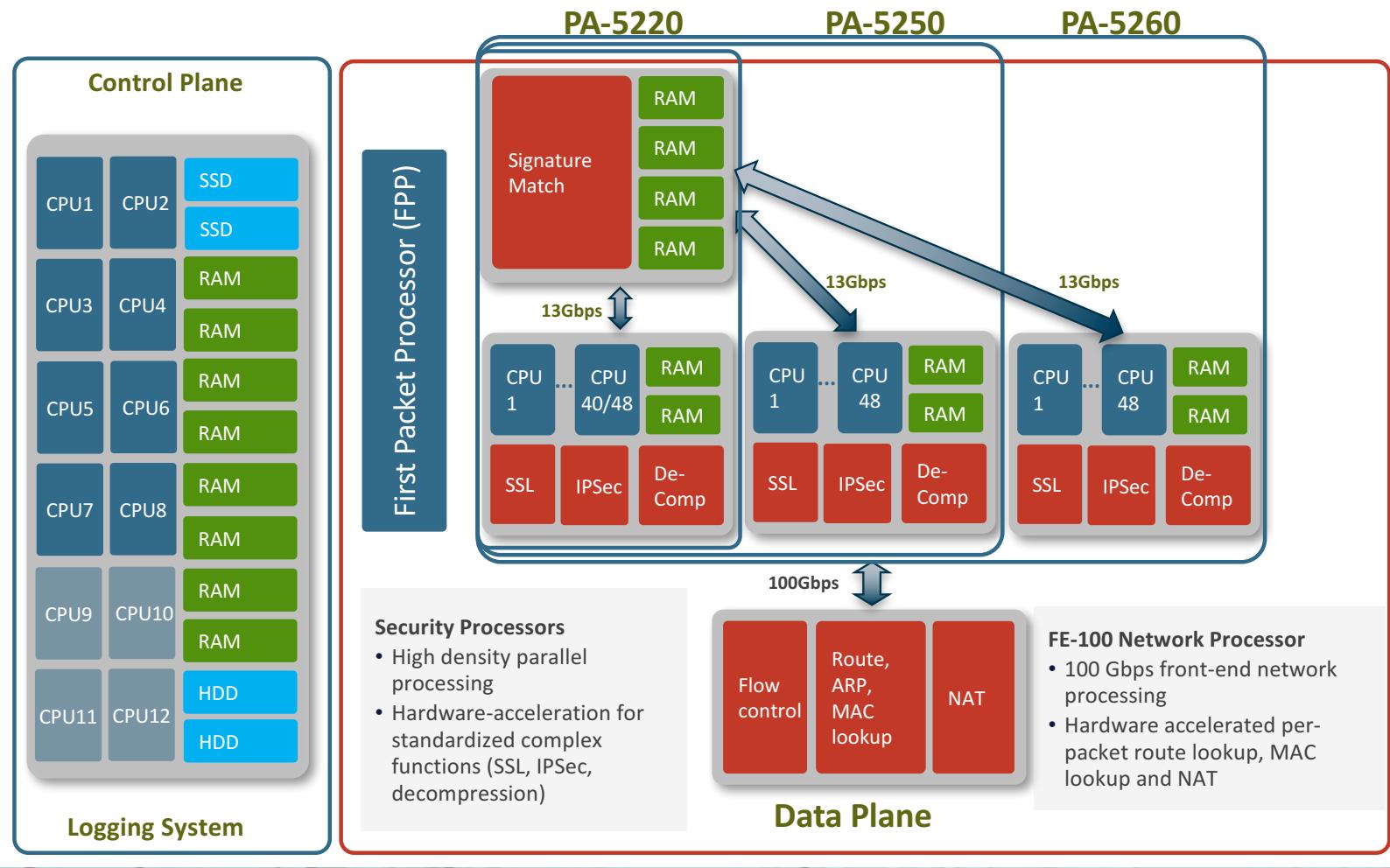
PA-5220



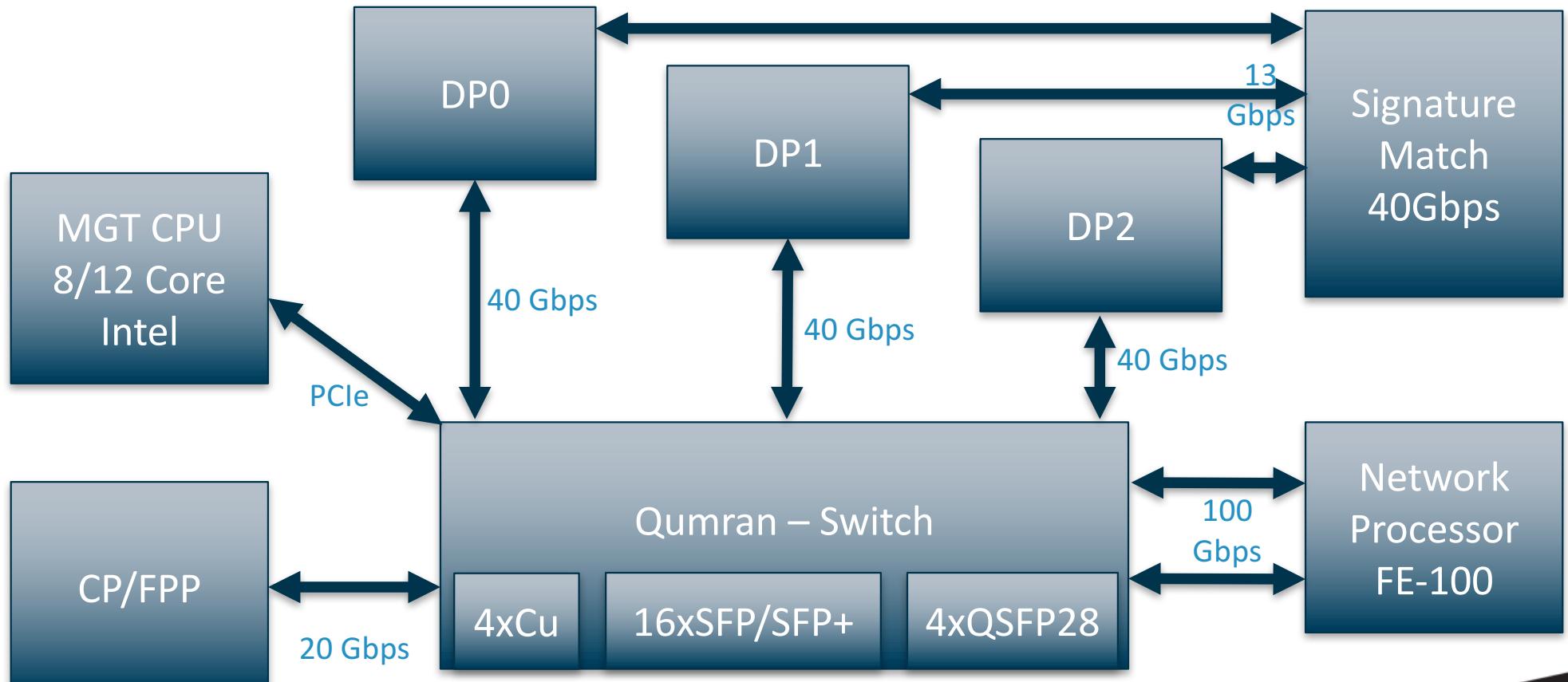
- 18.5 Gbps App-ID
- 9.2 Gbps Threat Prevention
- 5 Gbps IPSec VPN
- 4,000,000 sessions
- (4) 40G QSFP+
- (16) 1G/10G SFP/SFP+
- (4) 100/1000/10G Copper

- Hot swappable fans, power supplies
- Dual SSD system drives (240GB) and dual HDD logging drives (2TB)
- Dedicated HA and management interfaces
- 3U, 2 and 4 post rackmount units
- Front to back airflow with replaceable filters
- NEBS Level 3 Certified

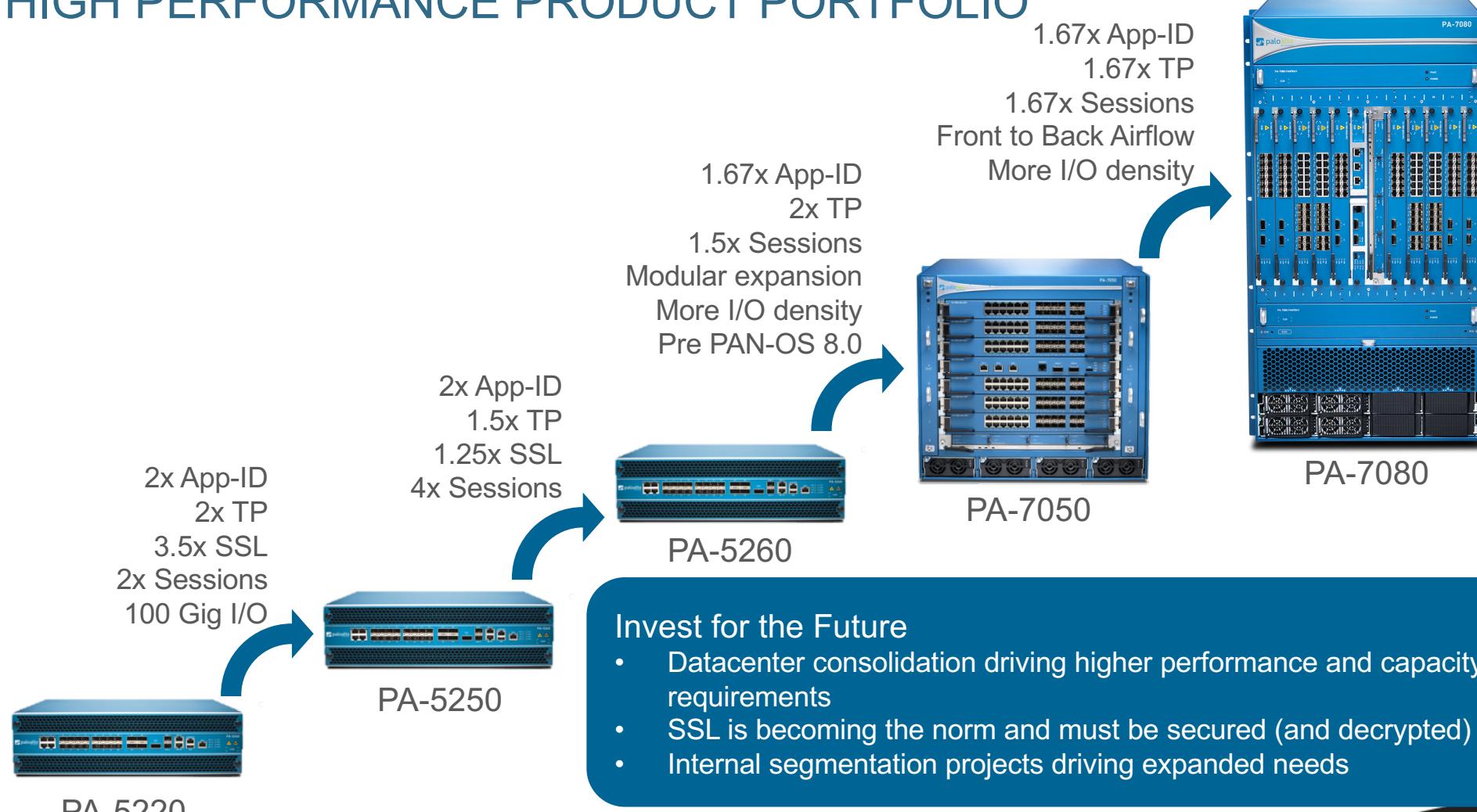
# PA-5200 Series Architecture



# PA-5200 Architecture



# HIGH PERFORMANCE PRODUCT PORTFOLIO



# POSITIONING: PA-7000 SERIES AND PA-5200 SERIES



Lead with PA-7000 Series when the customer needs:

## Highest performance and capacity

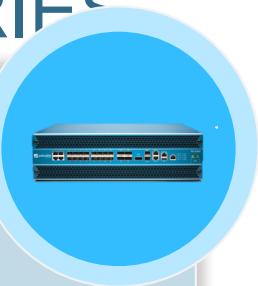
- Beyond 72 Gbps App-ID or 30 Gbps Threat Prevention or above 30M concurrent sessions

## Investment protection

- NPCs allow you to continue increasing capacity and performance

## Disruption free scaling of resources

- Scale without any downtime by adding more NPCs



Lead with PA-5200 Series when the customer needs:

## Compact form factor

- Performance up to 72 Gbps App-ID or 30 Gbps Threat Prevention
- Power and cooling constraints

100G I/O connectivity due to new/refresh data center projects

Ultimately Customer Requirements Drive the Choice

## NEAR-TERM FACTORS TO CONSIDER

	PA-7000 Series	PA-5200 Series	PA-5000 Series
40G and 100G Interfaces	40G interfaces	40G and 100G interfaces	✗
Modular scalability	✓	✗	✗
Front to back airflow	✓	✓	✗
FIPS and CC certification	✓	Not yet	✓
Pre PAN-OS 8.0 deployments	✓	✗	✓

# PA-5260 COMPETITIVE COMPARISON: REFERENCE DATA

Appliance	L3/L4 Firewall Throughput (Gbps)	Next-Generation Firewall Throughput (Gbps)	Threat Prevention Throughput (Gbps)	Max Concurrent Sessions	Ports	List Price	\$/Gbps of Threat Prevention Throughput
PA-5260	N.A.	72 (App-ID enabled)	30	32	4xCu10G, 16xSFP/+ 4x40G/100G	\$180,000	\$6,000
FortiGate 3815D	320	17 (App Control and IPS enabled)	12	95	10x10G + 4x100G	\$250K	<b>\$20,800</b>
FortiGate 3700D	160	14 (App Control and IPS enabled)	12	50	20 SFP/+, 4x40G	\$100K	<b>\$8,300</b>
Cisco Firepower 4150 or 9300 with SM-24 Module	75	30 (App Control enabled)	24	30	8xSFP+ Optional 2x 8xSFP+ or 4x40	\$250K+ Optional ports	<b>\$10,400</b>
Check Point 23800	128	27 (App Control and IPS enabled)	11	12.8-51.2	Flexible, no 100Gbps	\$150K – \$185K	<b>\$15,200</b>

# PA-5000 Series



- Multiple Security Processors
- DP Processing
  - Sessions are distributed across DP processors
  - DP0 is in charge of choosing a DP for processing a given flow
  - Sessions can be processed by any DP (except some that must be on DP0)
    - Tunnel sessions
    - Predict sessions
    - Host-bound sessions
    - Non TCP/UDP sessions

# PA-5000 Series Specs



## PA-5020

- **5 Gbps FW**
- **2 Gbps threat prevention**
- 2 Gbps IPSec VPN
- 5,000 SSL VPN Users
- 1,000,000 sessions
- Up to 20 VSYS
- (8) SFP (1 Gig) I/O
- (12) 10/100/1000
- DP0, DP1



## PA-5050

- **10 Gbps FW**
- **5 Gbps threat prevention**
- 4 Gbps IPSec VPN
- 10,000 SSL VPN Users
- 2,000,000 sessions
- Up to 125 VSYS
- (4) SFP+ (10 Gig) I/O
- (8) SFP (1 Gig) I/O
- (12) 10/100/1000
- DP0, DP1

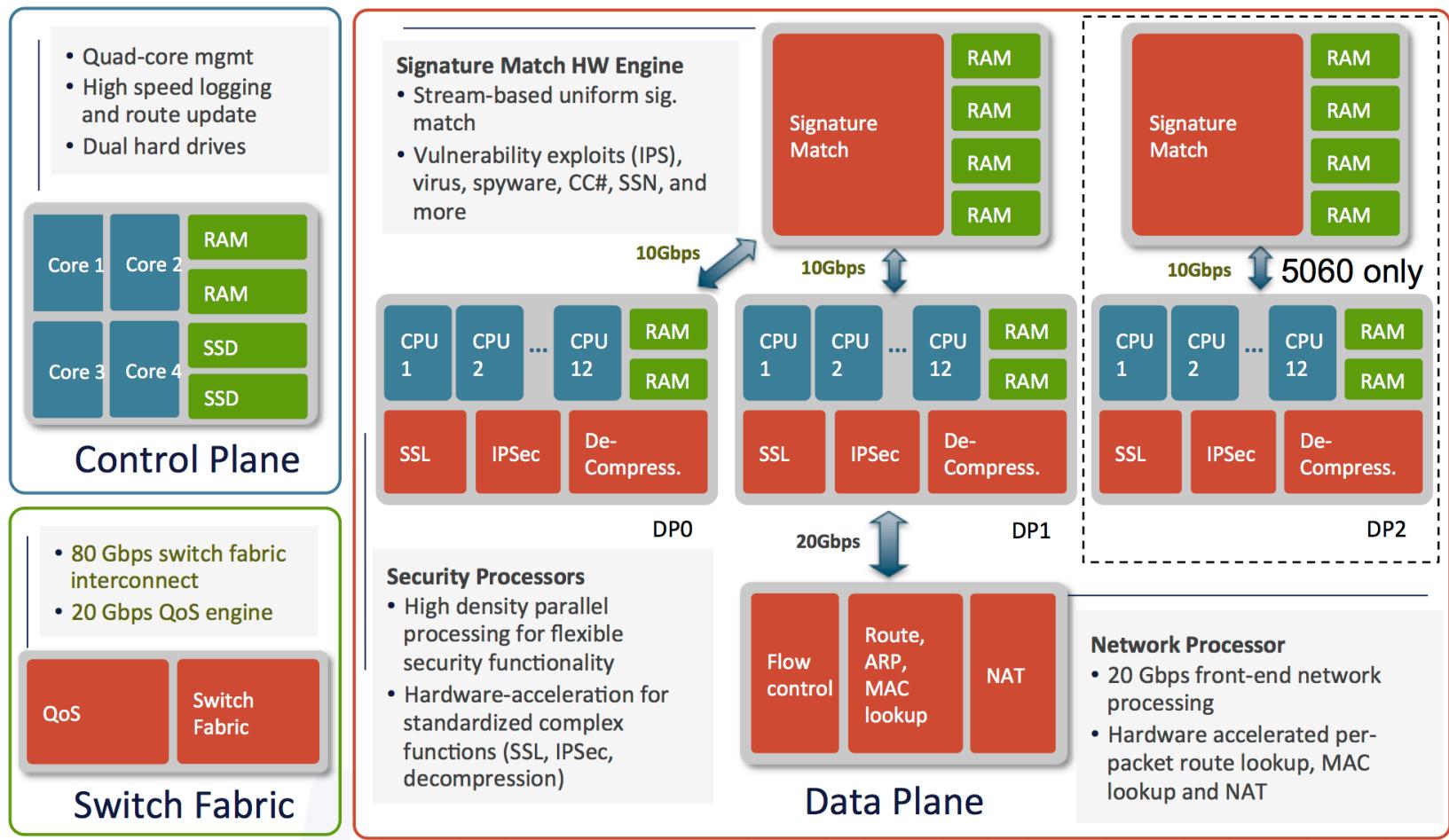


## PA-5060

- **20 Gbps FW**
- **10 Gbps threat prevention**
- 4 Gbps IPSec VPN
- 20,000 SSL VPN Users
- 4,000,000 sessions
- Up to 225 VSYS
- (4) SFP+ (10 Gig) I/O
- (8) SFP (1 Gig) I/O
- (12) 10/100/1000
- DP0, DP1, DP2

- Hot swappable fans, power supplies
- Dual, solid state hard drives (SSD), field replaceable (not hot swap)
- Dedicated HA and management interfaces
- 2U standard rack mount form factor
- PAN-OS 4.0 and later

# PA-5000 Series Architecture

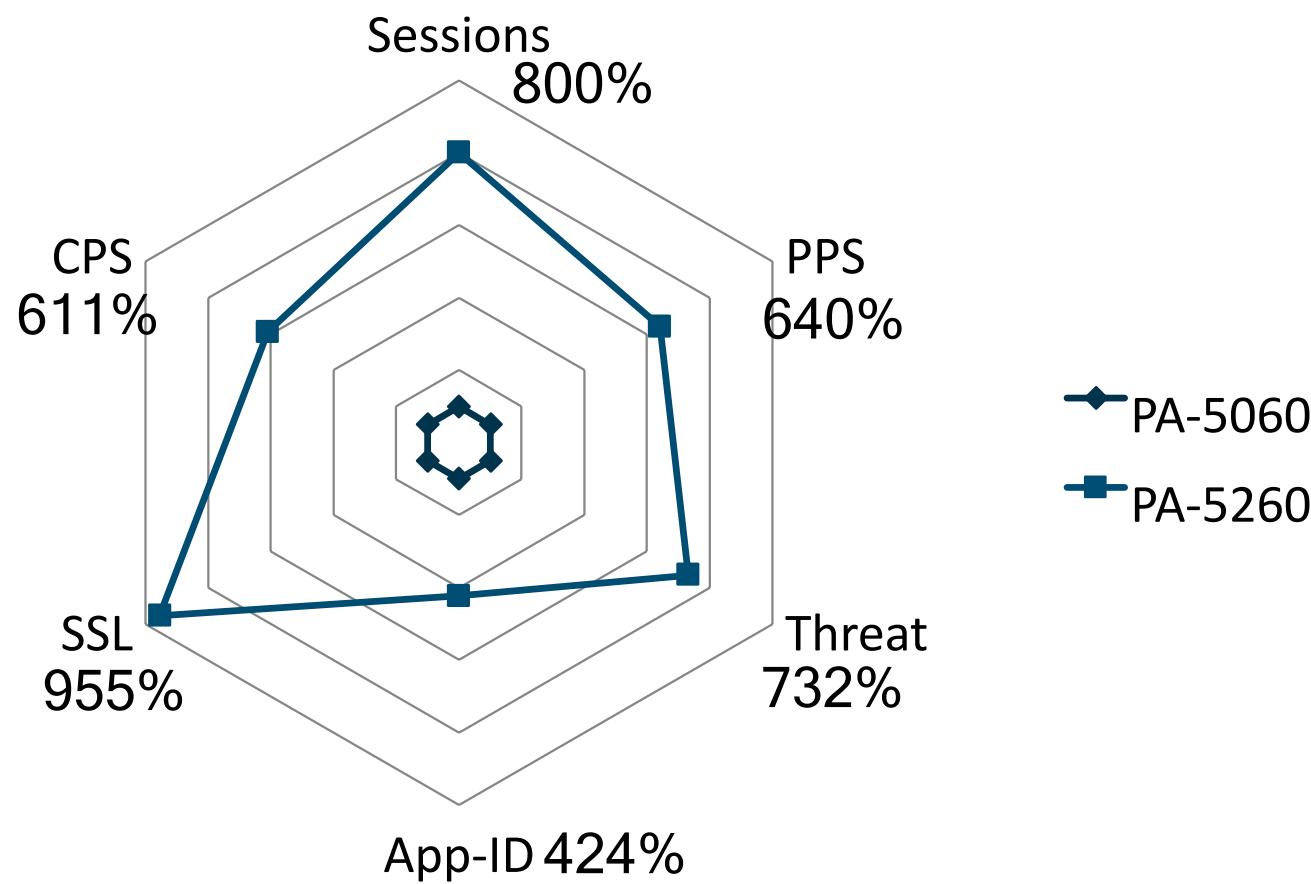


# PA-5200 Series

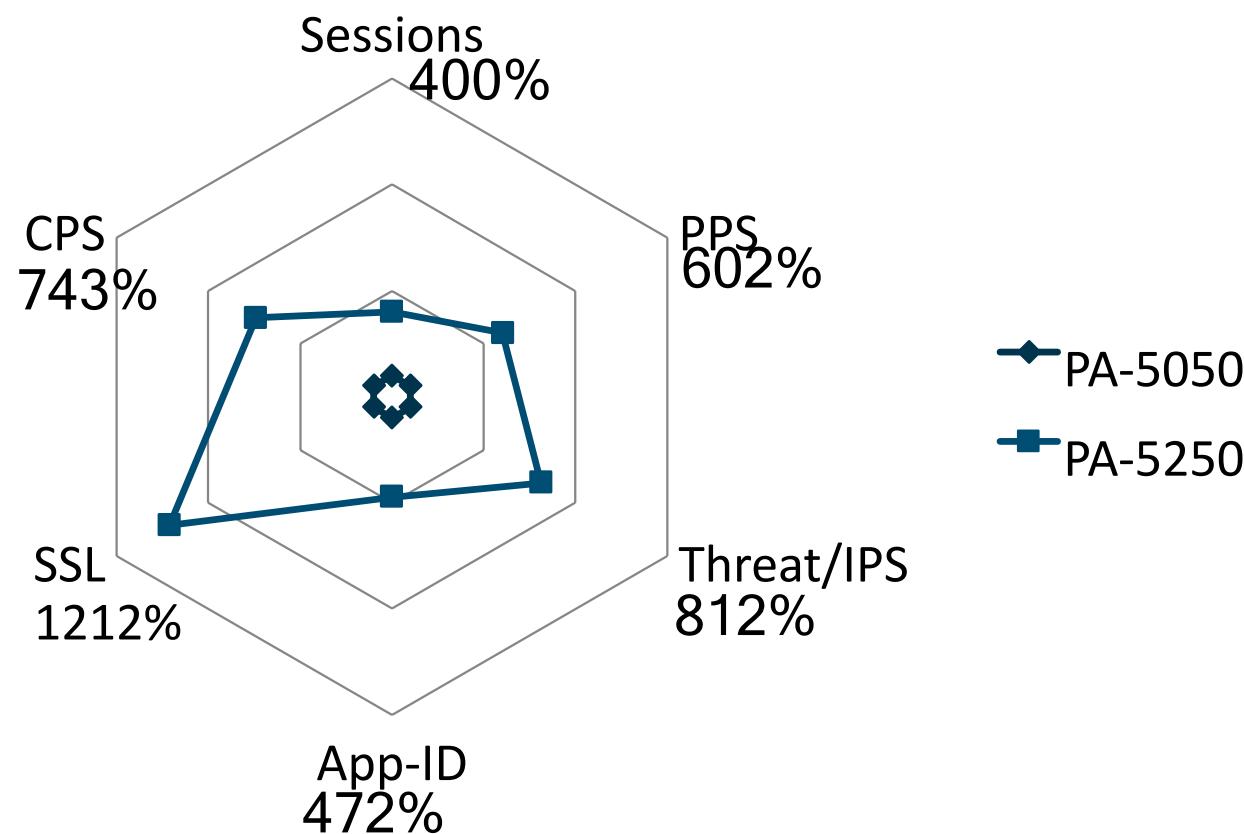
## Performance vs PA-5000 Series

	PA-5260	PA-5060	PA-5250	PA-5050	PA-5220	PA-5020
US List Price	\$180,000	\$130,000	\$100,000	\$70,000	\$50,000	\$40,000
Firewall Gbps (App-ID)	72.2	17.3	35.9	7.6	18.5	3.9
Threat Gbps (DSRI)	67.3	6.8	35	2.8	18.4	3.6
Threat Gbps (Full)	30	3.4	20.3	1.4	9.2	2.1
New sessions per second	458,000	69,500	349,000	37,500	169,000	37,500
Max sessions (M)	32	4	8	2	4	1
Max SSL Sessions (M)	3.2M	90K	800K	47K	400K	15K
SSL Throughput	6.5Gbps	680Mbps	5.1Gbps	425Mbps	1.4Gbps	120Mbps
Packets per Second (M)	73.7	11.4	68.6		33.7	
Avg Latency (uS)	8.7	11	8.5	11	7.9	11

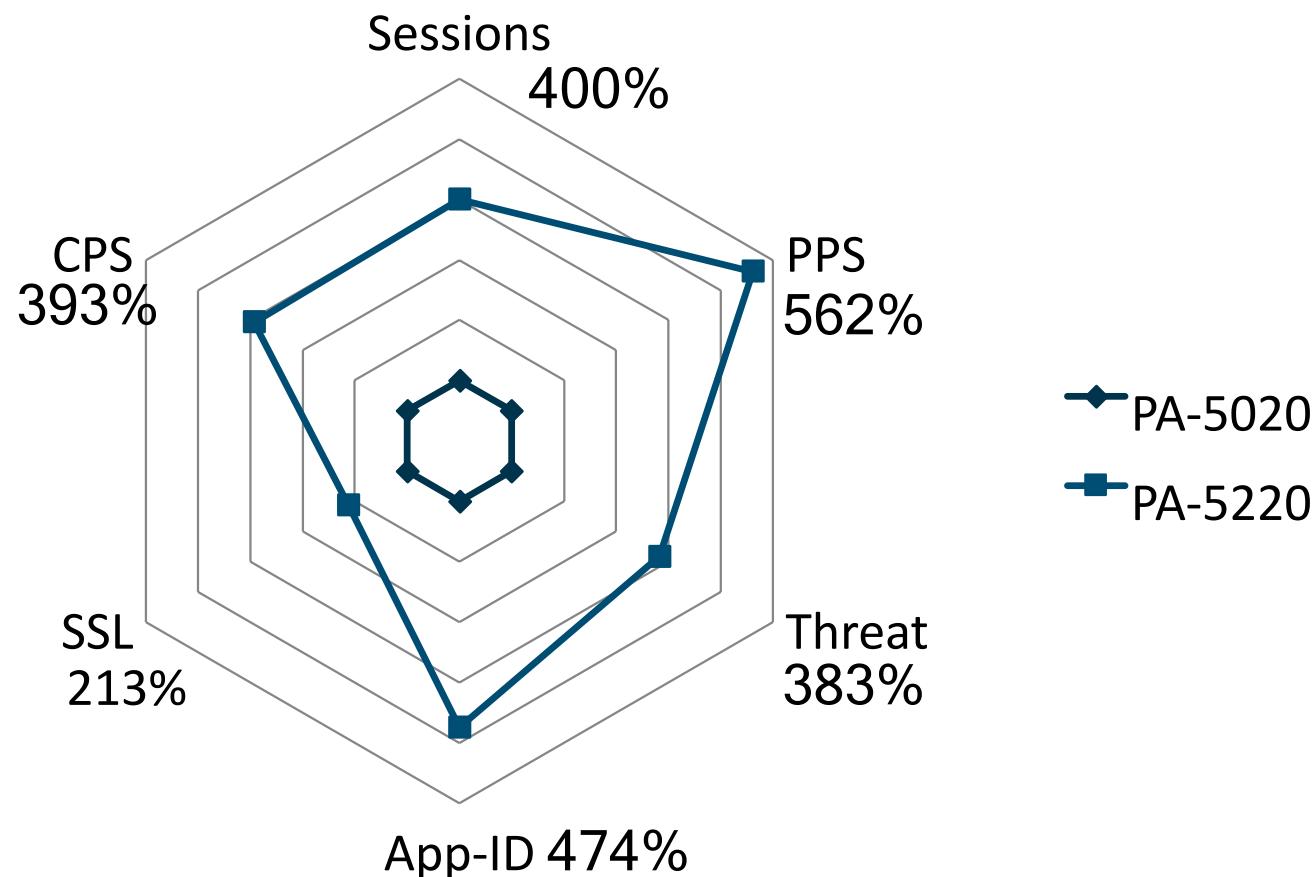
# Radar Map Chart: PA-5260 vs PA-5060



# Radar Map Chart: PA-5250 vs PA-5050



## Radar Map Chart: PA-5220 vs PA-5020



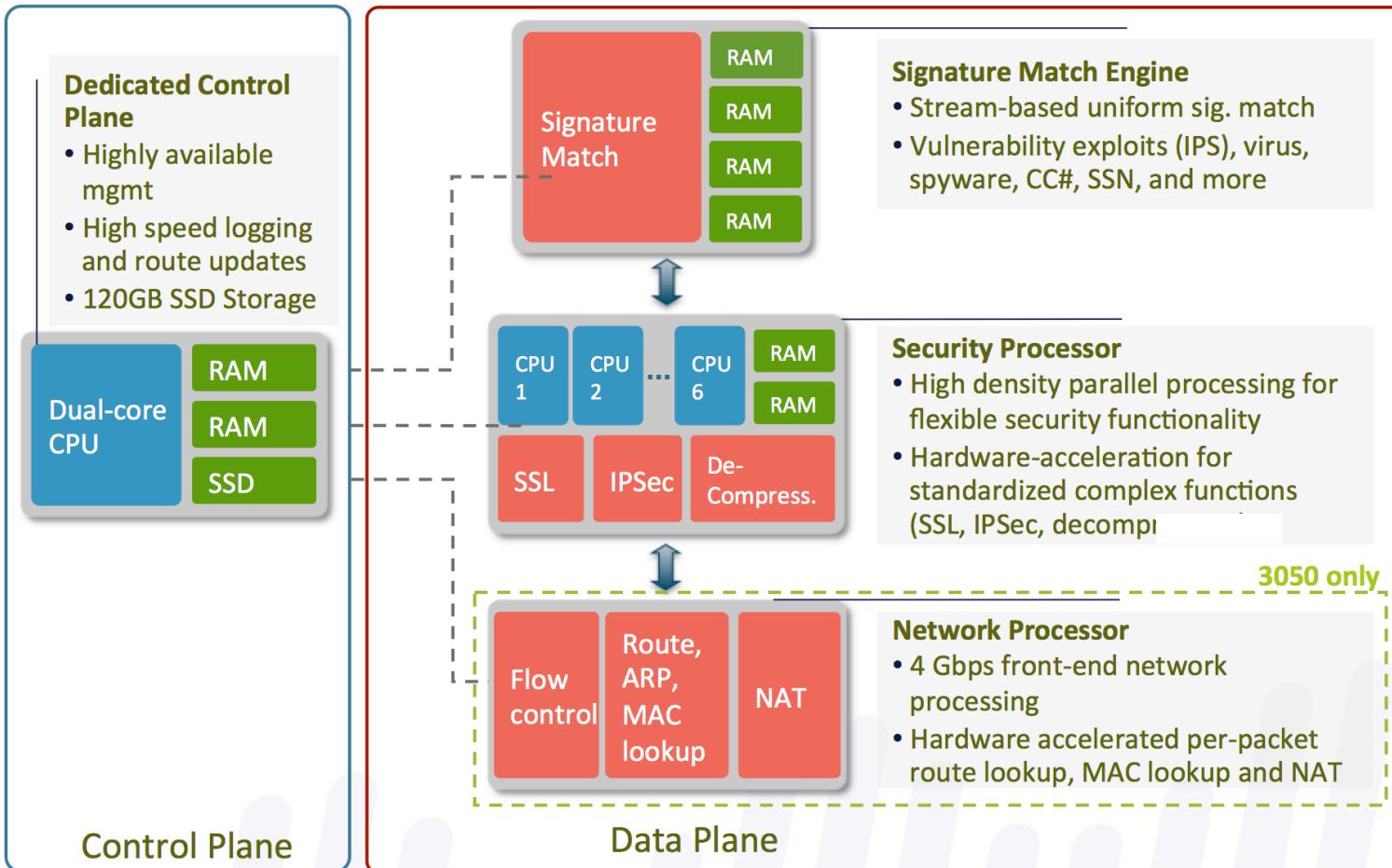
## Single Data Plane Firewalls

# PA-3000 Series

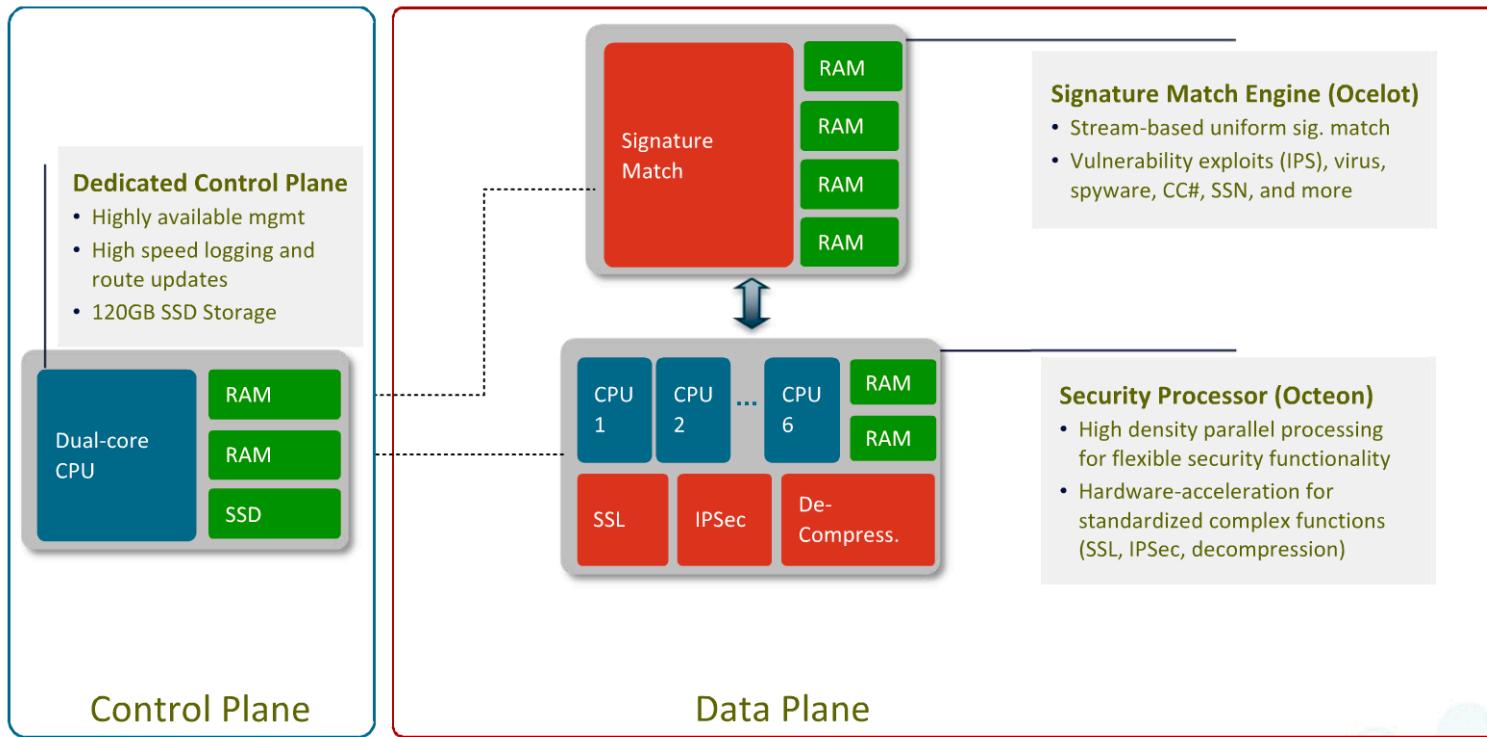


- Mid-size platform for enterprise customers
  - Parallel processing hardware architecture
  - High performance management subsystem
    - Dual core Intel Celeron with 4GB DDR2 memory
  - 120GB SSD storage for high reliability and performance

# PA-3050/3060 Architecture



# PA-3020 Architecture



- On the PA-3020 firewall, the network processing engine has been virtualized into the multi-core security processor

# PA-800 SERIES

- High speed appliances up to 1.9 Gbps (App-ID) and 780 Mbps (Threat)
- High performance management plane leveraging multiple CPU cores and 8GB memory
- Redundant power for additional hardware resiliency (PA-850)
- Flexible I/O for today and tomorrow's network needs; 10G interfaces (PA-850)



# PA-800 SERIES SPECIFICATIONS

PA-850



- 1.9 Gbps App-ID
- 780 Mbps Threat Prevention
- 192,000 sessions
- (4) 10/100/1000 Copper
- (4) SFP, (4) SFP+

PA-820



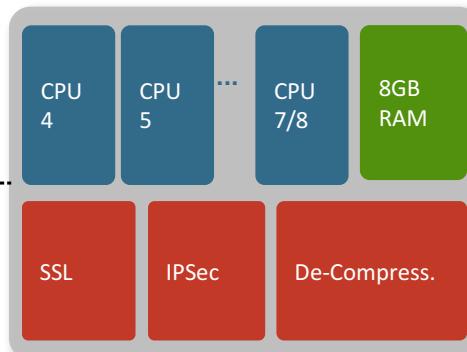
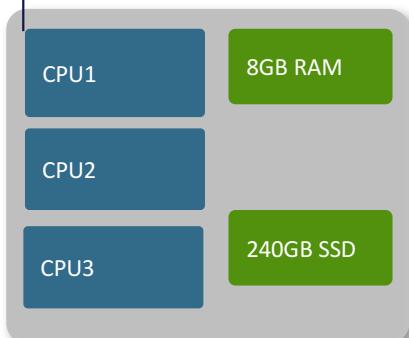
- 940 Mbps App-ID
- 610 Mbps Threat Prevention
- 128,000 sessions
- (4) 10/100/1000 Copper
- (8) SFP

- 1U rackmount chassis
- Dual, hot swap power supplies (PA-850 only)
- 240GB SSD
- Dedicated out-of-band management port
- RJ-45, Micro USB console port
- Dedicated HA interfaces

# PA-800 Series Architecture

## Dedicated Control Plane

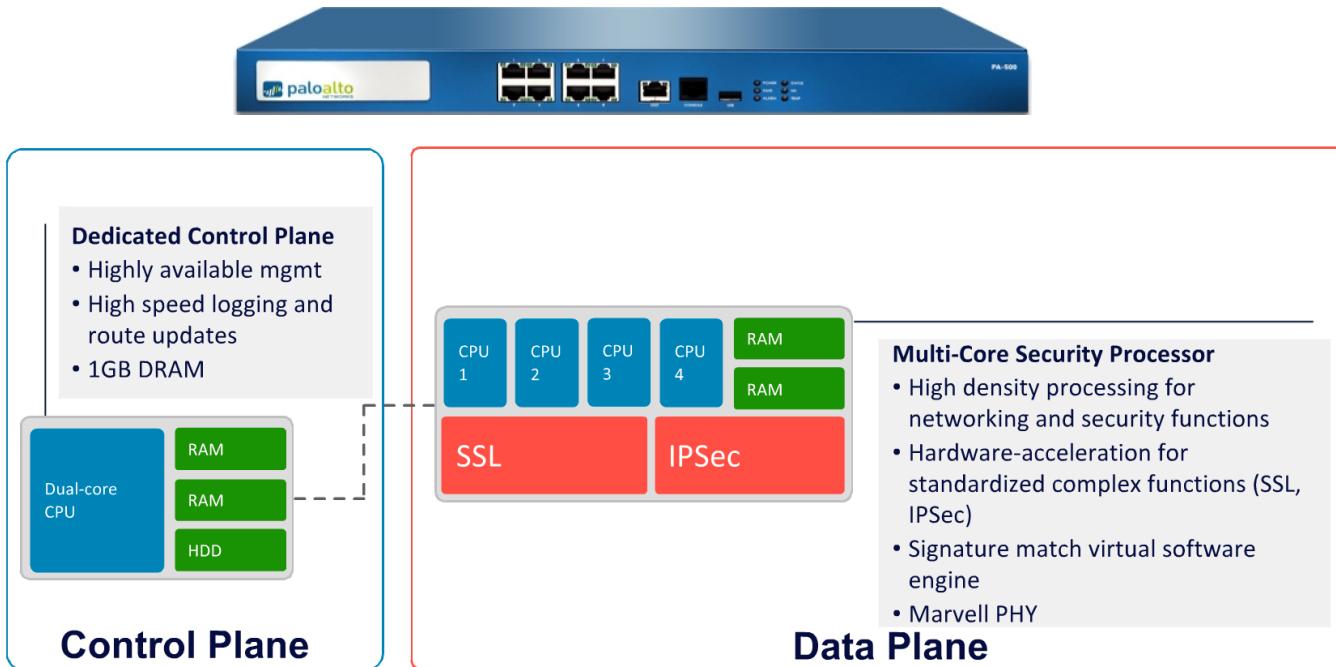
- Highly available mgmt
- High speed logging and route updates
- 240GB SSD Storage



## Security Processor

- High density parallel processing for flexible security functionality
- Hardware-acceleration for standardized complex functions (SSL, IPSec, decompression)

# PA-500 Architecture



- No FPGAs / No offload processors
- Network processing and signature match engine virtualized into the multi-core processor
- Ships with 2 GB of RAM

# PA-220

- Delivering full PAN-OS capabilities, in a small desktop footprint, with increased port density
- Built-in resiliency with dual power adapters
- Complete high availability support: active/active and active/passive
- Passive and silent cooling to eliminate noise and increase reliability



# PA-220 SPECIFICATIONS

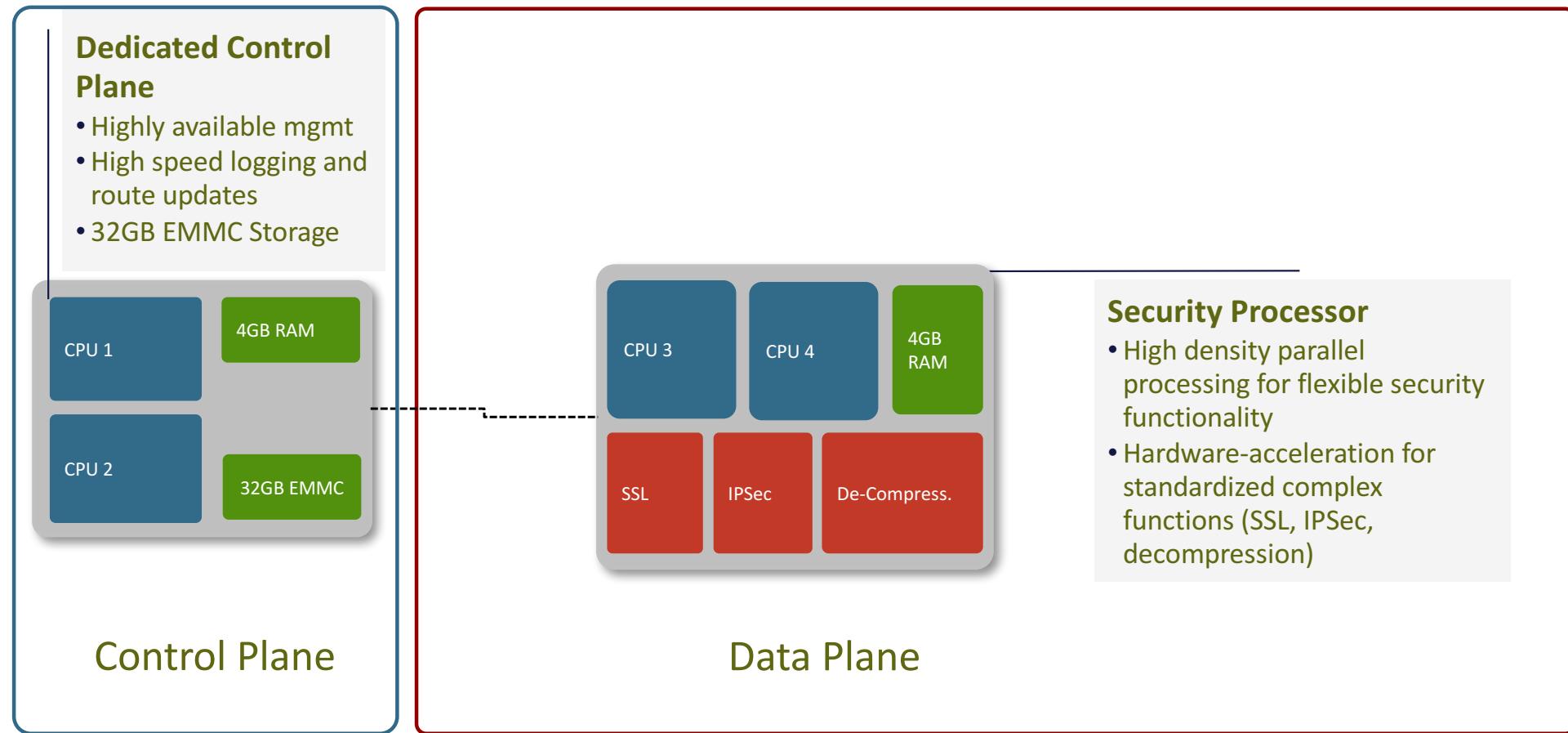
PA-220



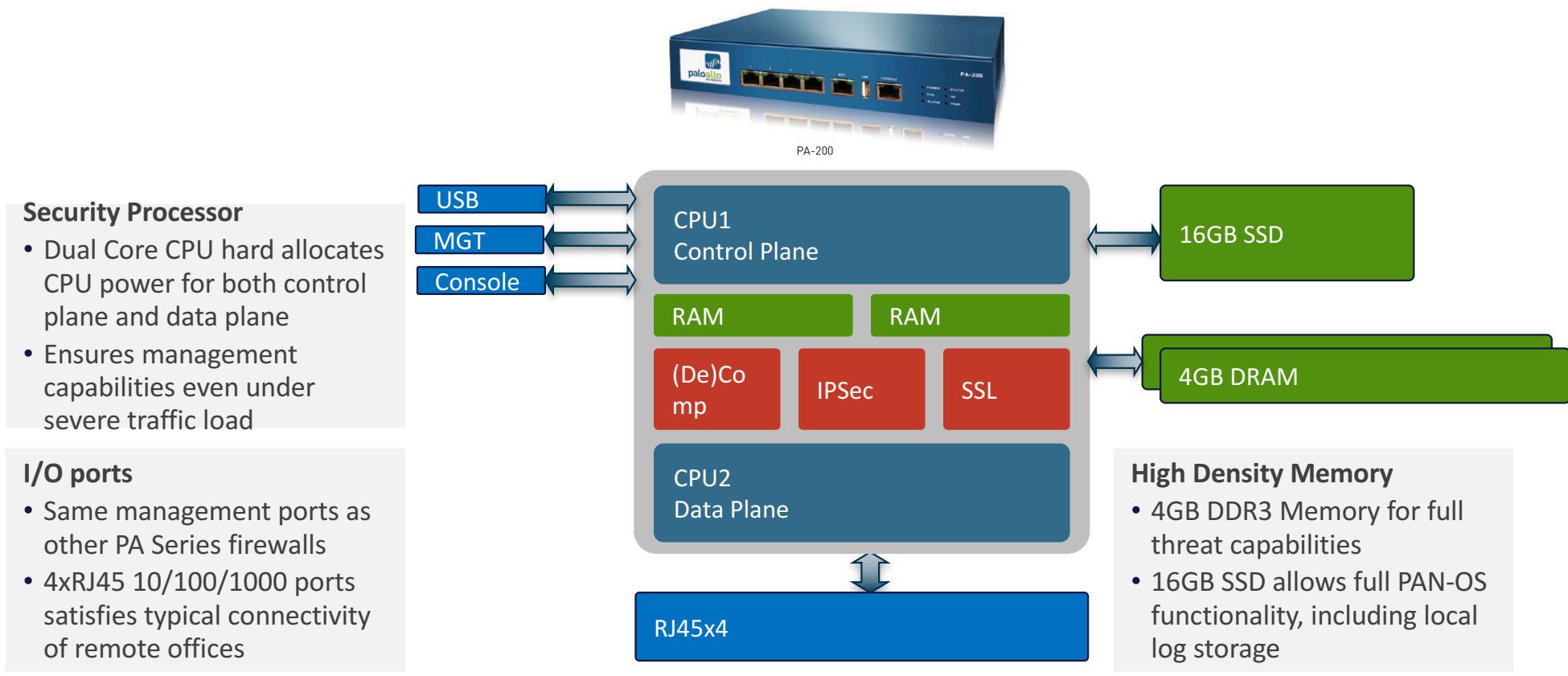
500 Mbps App-ID  
150 Mbps Threat Prevention  
64,000 sessions  
(8) 1G Copper Ethernet ports

- Dual power adapters (optional)
- 32GB solid state storage (EMMC)
- Dedicated out-of-band management port
- RJ-45 and Micro USB console ports
- Complete high availability support (Active/Passive with session sync, and Active/Active)
- Wall-mount or rack-mount desktop form factor

# PA-220 Architecture



# PA-200 Series Architecture



# PA-220, PA-800 Series

## Performance and Capacities Summary

	PA-850	PA-820	PA-500	PA-220	PA-200
US List Price	\$9,500	\$4,500	\$4,500	\$1,000	\$2,000
Firewall Gbps (App-ID)	1.9 Gbps	940 Mbps	712 Mbps	500 Mbps	445 Mbps
Threat Gbps (DSRI)	1.9 Gbps	940 Mbps	660 Mbps	500 Mbps	420 Mbps
Threat Mbps (Full)	780Mbps	610 Mbps	180 Mbps	150 Mbps	80 Mbps
New sessions per sec	9,500	8,300	3,700	4,200	3,200
Max sessions	192,000	128,000	64,000	64,000	64,000
SSL Sessions	19,200	12,800	1,024	6,400	1,024
SSL Throughput	275 Mbps	220 Mbps	38 Mbps	66 Mbps	30 Mbps

# PA-7000 Series



PA-7050



PA-7080

# Additional Architecture Information- Features and Capacities Matrix

- The Features and Capacities matrix is our \*internal\* document that specifies all the various product features and max capacities
- <https://intranet.paloaltonetworks.com/docs/DOC-3950>
- New version of the spreadsheet for each release

More documents in  Product Knowledge Base ▾

 **Features and Capacity, All PAN-OS Releases**  Version 56

Created by Glen Gibson on Jan 20, 2012 2:03 PM. Last modified by Glen Gibson on Jun 1, 2017 7:32 AM.

The below attachments document all features and capacities of the various supported PAN-OS releases in a single location. This document will be the central location for these documents going forward, all other documents associated with 'Features and Capacity' should be considered out of date.

*Please note that the field is allowed to provide pieces of critical information as necessary to customers to address issues/questions, but you are not allowed to transfer this entire document to your partner/customer...*

If you must share something... feel free to share a link to the product comparison tool, which exposes much of what's in the features and capacity spreadsheet on our public website - [Product Comparison tool](#). This tool allows you to export PDF files with the relevant data once you've compared the relevant products. Keep in mind that this tool tracks to the latest feature release of PAN-OS.