Palo Alto Networks

Markus Laaksonen

mlaaksonen@paloaltonetworks.com

paloalto NETWORKS

the network security company™

About Palo Alto Networks

- Palo Alto Networks is the **Network Security Company**
- World-class team with strong security and networking experience
  - Founded in 2005 by security visionary Nir Zuk
  - Top-tier investors
- Builds next-generation firewalls that identify / control 1200+ applications
  - Restores the firewall as the core of the enterprise network security infrastructure
  - Innovations: App-ID™, User-ID™, Content-ID™
- Global footprint: 2,200+ customers in 50+ countries, 24/7 support

Applications Have Changed; Firewalls Have Not

The gateway at the trust border is the right place to enforce policy control

- Sees all traffic
- Defines trust boundary

BUT…applications have changed

- Ports ≠ Applications
- IP Addresses ≠ Users
- Packets ≠ Content

Need to restore visibility and control in the firewall

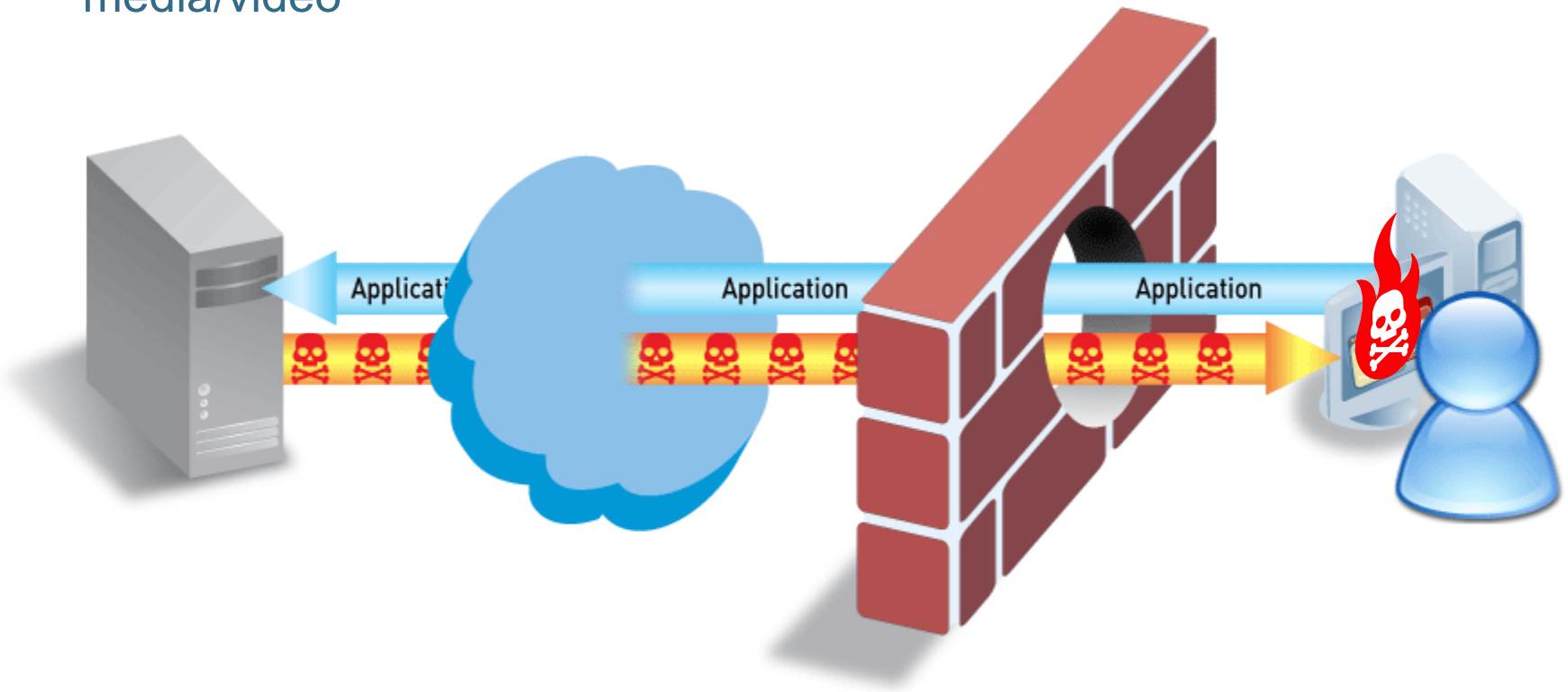
Applications Carry Risk

Applications can be “threats”

- P2P file sharing, tunneling applications, anonymizers, media/video

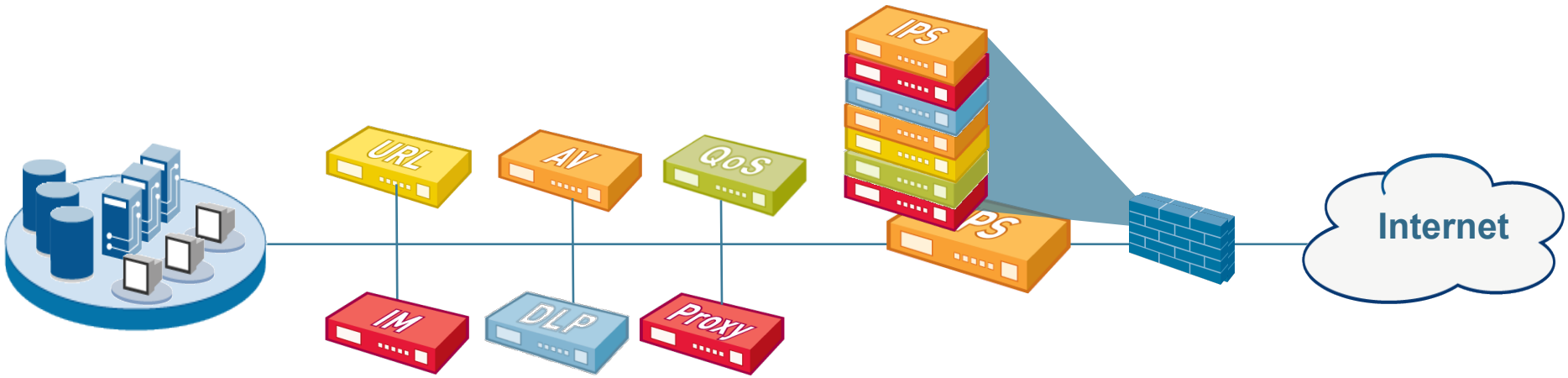
Applications carry threats

- SANS Top 20 Threats – majority are application-level threats



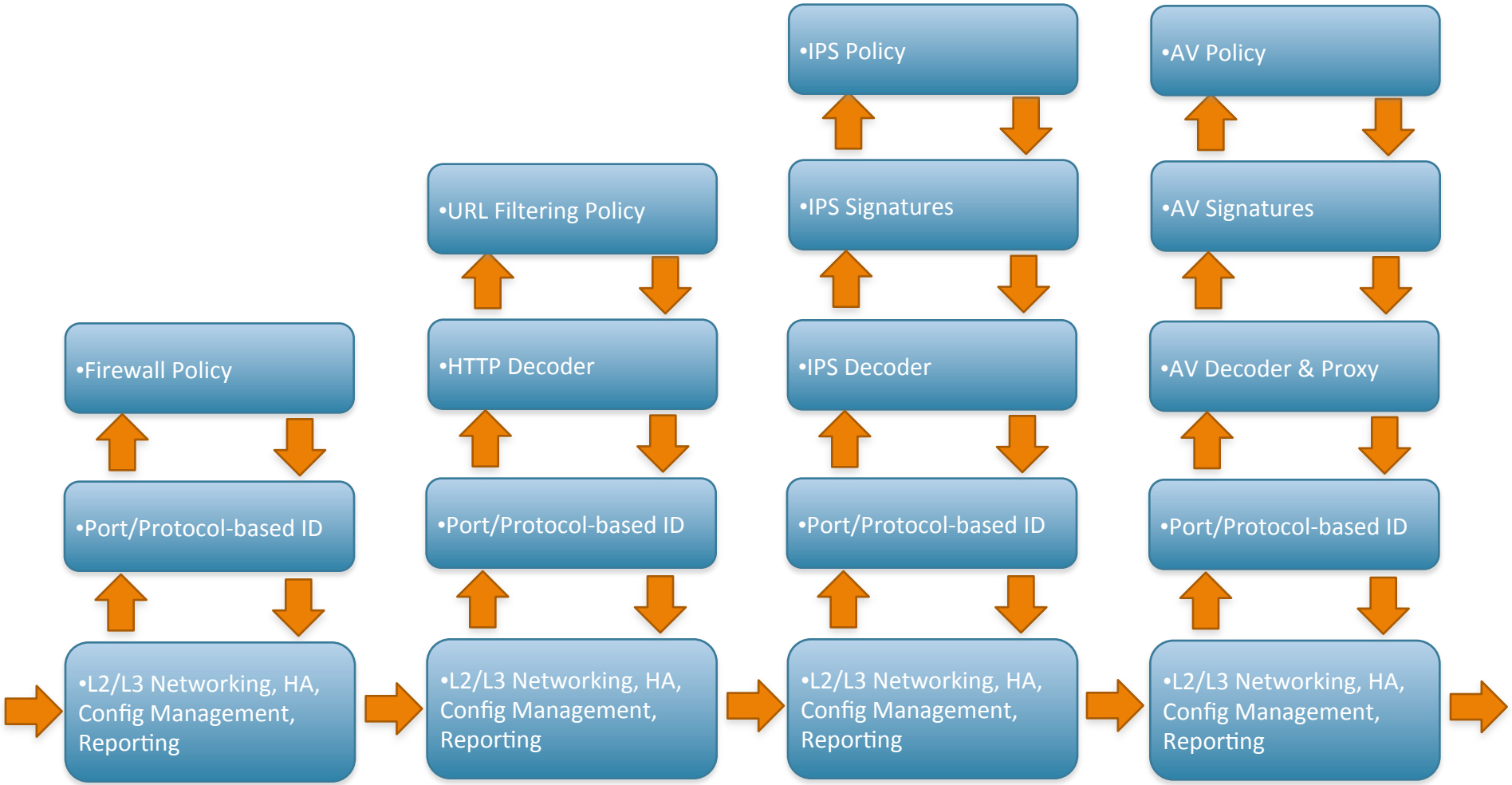
Applications & application-level threats result in major breaches – Pfizer, VA, US Army

Technology Sprawl & Creep Are Not The Answer



- "More stuff" doesn't solve the problem
- Firewall "helpers" have limited view of traffic
- Complex and costly to buy and maintain
- Putting all of this in the same box is just slow

Traditional Multi-Pass Architectures are Slow



The Right Answer: Make the Firewall Do Its Job

New Requirements for the Firewall

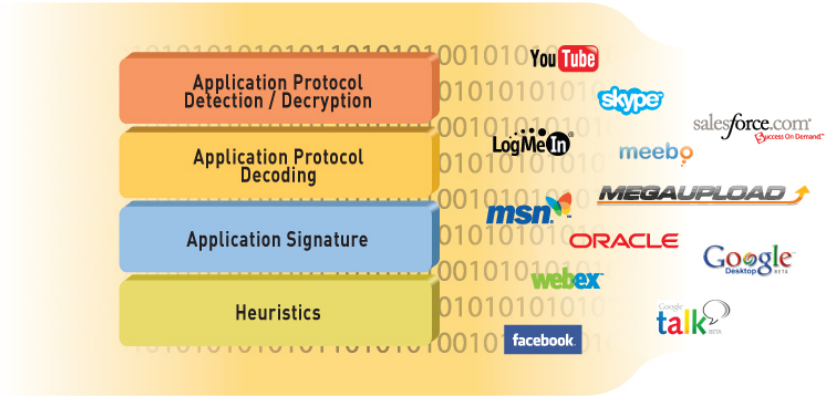
1. Identify applications regardless of port, protocol, evasive tactic or SSL
2. Identify users regardless of IP address
3. Protect in real-time against threats embedded across applications
4. Fine-grained visibility and policy control over application access / functionality
5. Multi-gigabit, in-line deployment with no performance degradation

paloalto NETWORKS

Identification Technologies Transform the Firewall

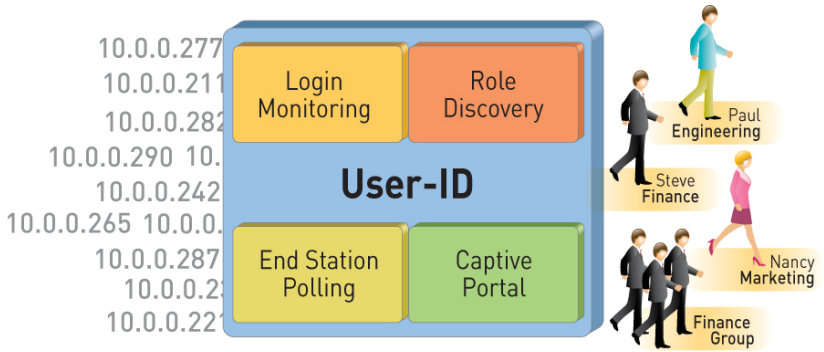
App-ID™

Identify the application



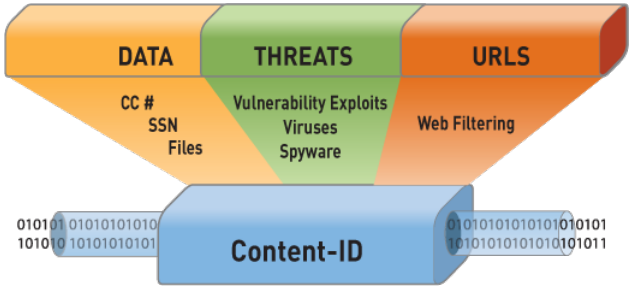
User-ID™

Identify the user



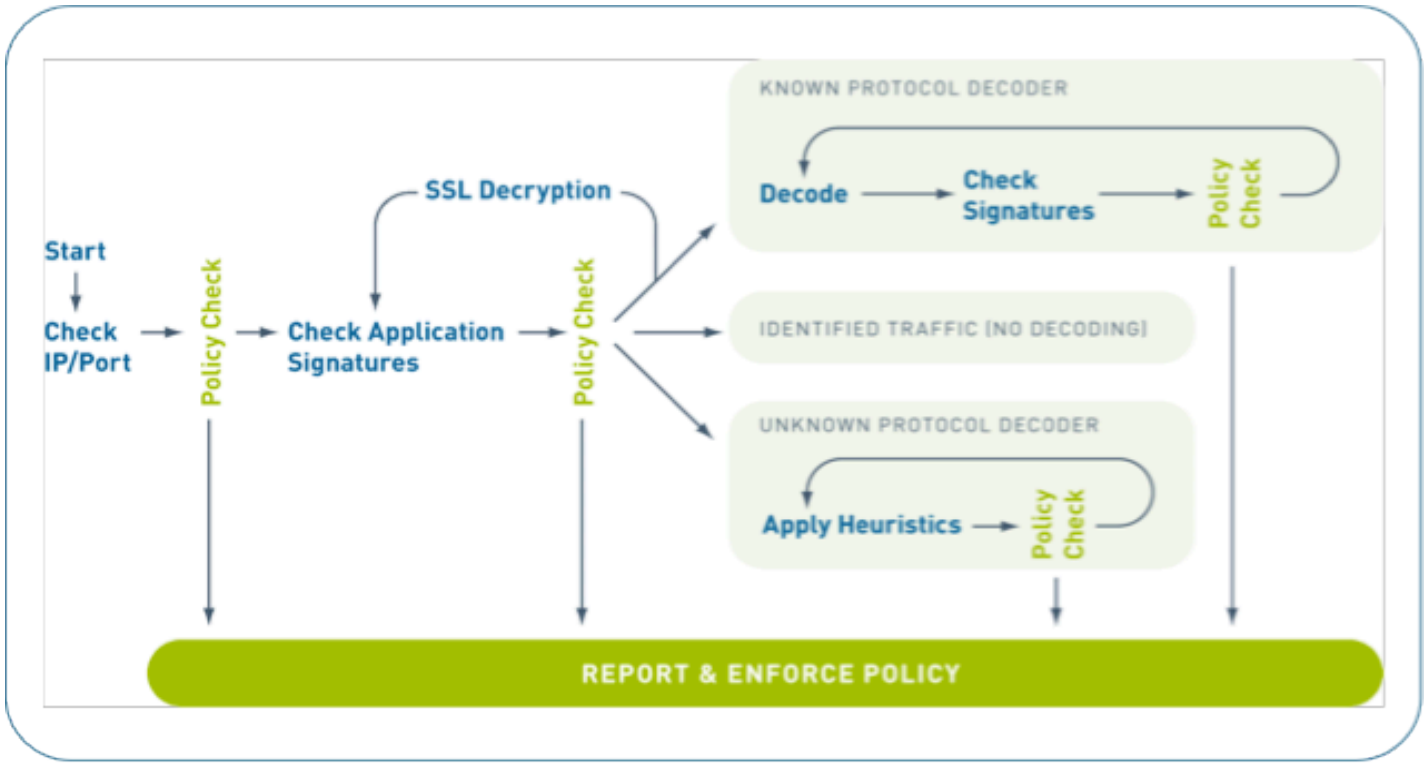
Content-ID™

Scan the content



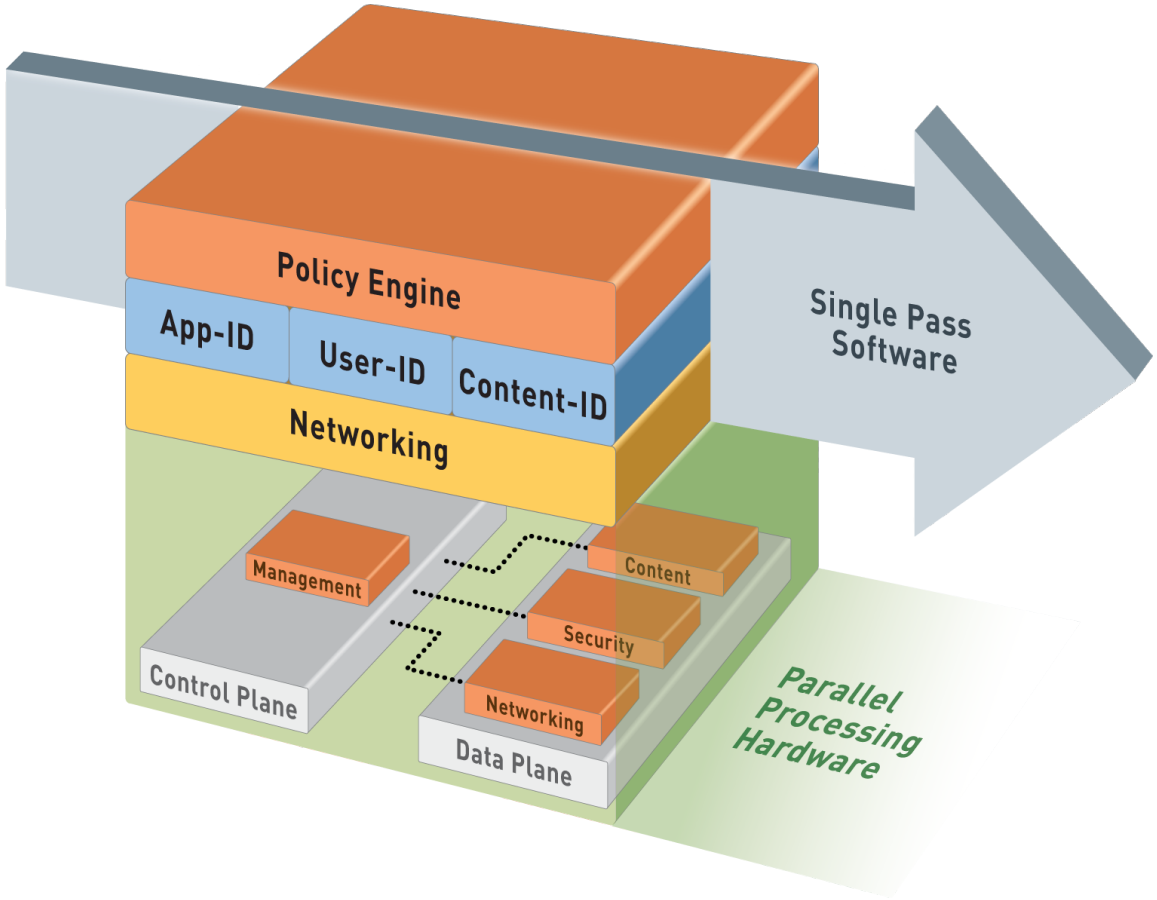
App-ID is Fundamentally Different

- Always on, always the first action
- Built-in intelligence
- Sees all traffic across all ports
- Scalable and extensible



Much more than just a signature….

Single-Pass Parallel Processing™ (SP3) Architecture



Single Pass

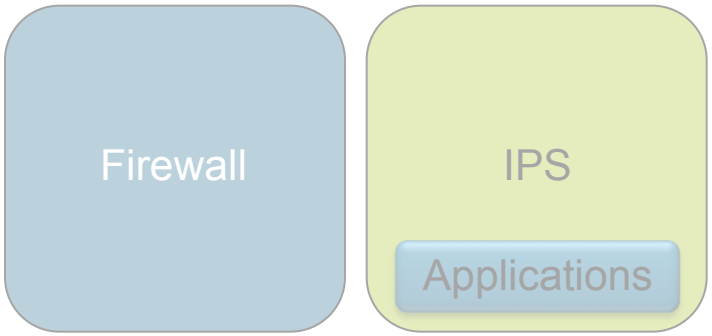
- Operations once per packet
  - Traffic classification (app identification)
  - User/group mapping
  - Content scanning – threats, URLs, confidential data
- One policy

Parallel Processing

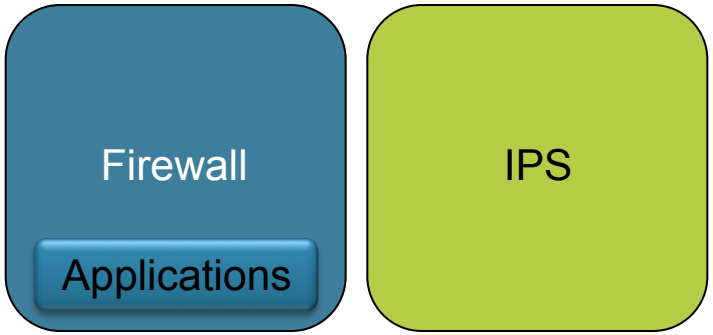
- Function-specific parallel processing hardware engines
- Separate data/control planes

Up to 10Gbps, Low Latency

Why It Has To Be The Firewall



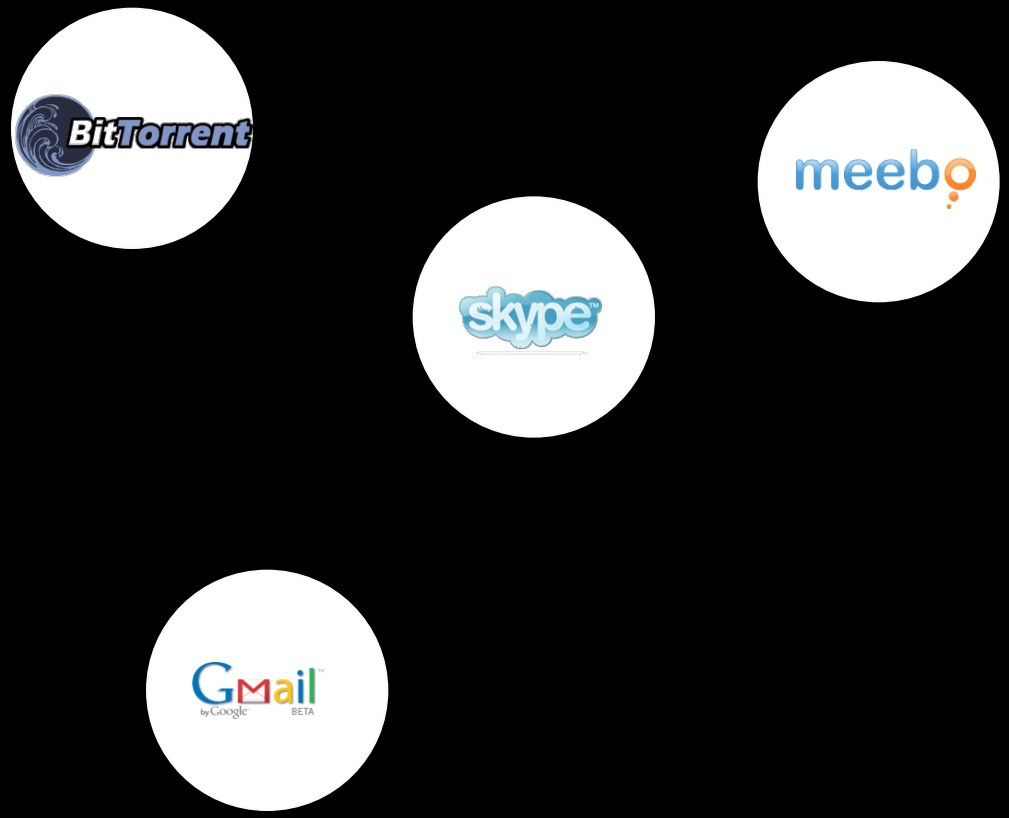
1. Path of least resistance - build it with legacy security boxes
2. Applications = threats
3. Can only see what you expressly look for



1. Most difficult path - can't be built with legacy security boxes
2. Applications = applications, threats = threats
3. Can see everything

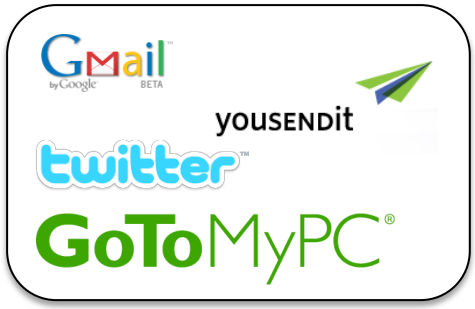
Traffic decision is made at the firewall
No application knowledge = bad decision

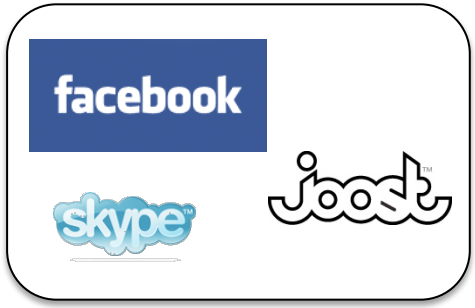
What You See…with non-firewalls



What You See with With A Firewall

Your Control With a Firewall

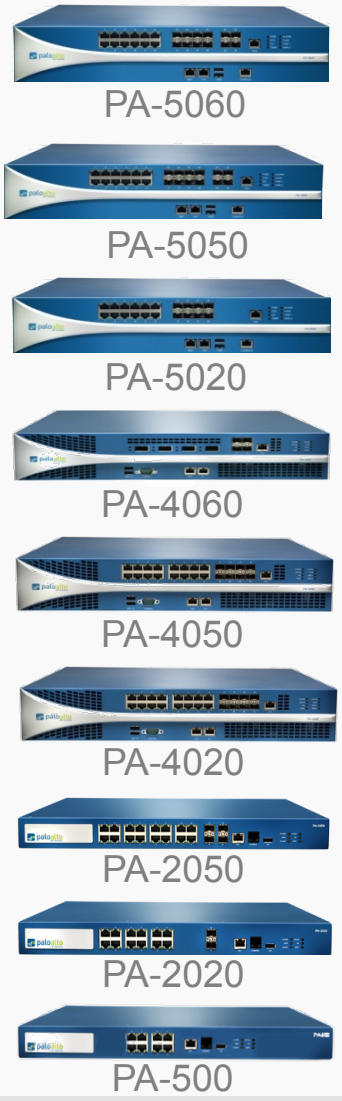




PAN-OS Core Firewall Features

Visibility and control of applications, users and content complement core firewall features

- Strong networking foundation
  - Dynamic routing (BGP, OSPF, RIPv2)
  - Tap mode – connect to SPAN port
  - Virtual wire (“Layer 1”) for true transparent in-line deployment
  - L2/L3 switching foundation
  - Policy-based forwarding
- VPN
  - Site-to-site IPSec VPN
  - SSL VPN
- QoS traffic shaping
  - Max/guaranteed and priority
  - By user, app, interface, zone, & more
  - Real-time bandwidth monitor
- Zone-based architecture
  - All interfaces assigned to security zones for policy enforcement
- High Availability
  - Active/active, active/passive
  - Configuration and session synchronization
  - Path, link, and HA monitoring
- Virtual Systems
  - Establish multiple virtual firewalls in a single device (PA-5000, PA-4000, and PA-2000 Series)
- Simple, flexible management
  - CLI, Web, Panorama, SNMP, Syslog



Palo Alto Networks Next-Gen Firewalls

PA-5060

20 Gbps FW/10 Gbps threat prevention/4,000,000 sessions

4 SFP+ (10 Gig), 8 SFP (1 Gig), 12 copper gigabit

PA-5050

10 Gbps FW/5 Gbps threat prevention/2,000,000 sessions

4 SFP+ (10 Gig), 8 SFP (1 Gig), 12 copper gigabit

PA-5020

5 Gbps FW/2 Gbps threat prevention/1,000,000 sessions

8 SFP, 12 copper gigabit

PA-4060

10 Gbps FW/5 Gbps threat prevention/2,000,000 sessions

4 XFP (10 Gig), 4 SFP (1 Gig)

PA-4050

10 Gbps FW/5 Gbps threat prevention/2,000,000 sessions

8 SFP, 16 copper gigabit

PA-4020

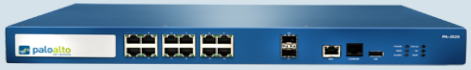
2 Gbps FW/2 Gbps threat prevention/500,000 sessions

8 SFP, 16 copper gigabit

PA-2050

1 Gbps FW/500 Mbps threat prevention/250,000 sessions

4 SFP, 16 copper gigabit



PA-2020

500 Mbps FW/200 Mbps threat prevention/125,000 sessions

2 SFP, 12 copper gigabit

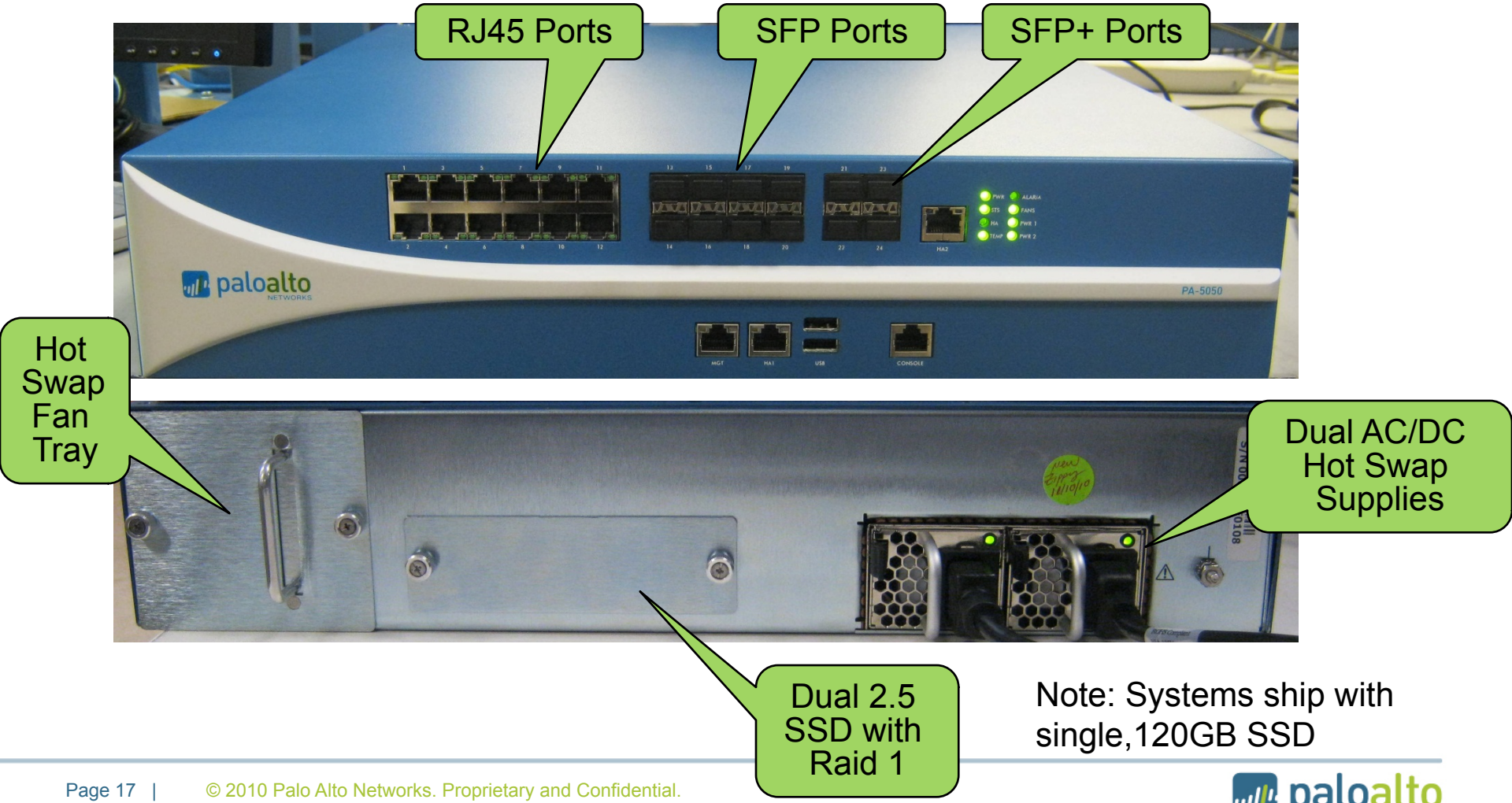
PA-500

250 Mbps FW/100 Mbps threat prevention/50,000 sessions

8 copper gigabit

PA-5000 Series

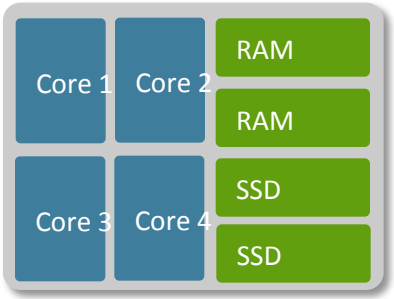
- A picture is worth a thousand words…



Note: Systems ship with single,120GB SSD

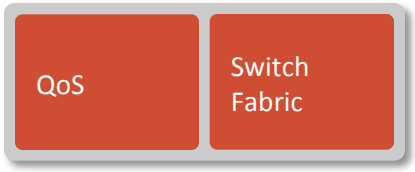
PA-5000 Series Architecture

- Quad-core mgmt
- High speed logging and route update
- Dual hard drives



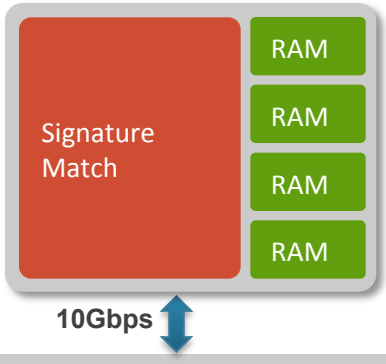
Control Plane

- 80 Gbps switch fabric interconnect
- 20 Gbps QoS engine

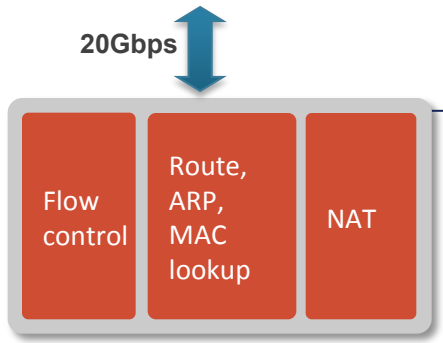


Switch Fabric

Signature Match HW Engine
- Stream-based uniform sig. match
- Vulnerability exploits (IPS), virus, spyware, CC#, SSN, and more



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



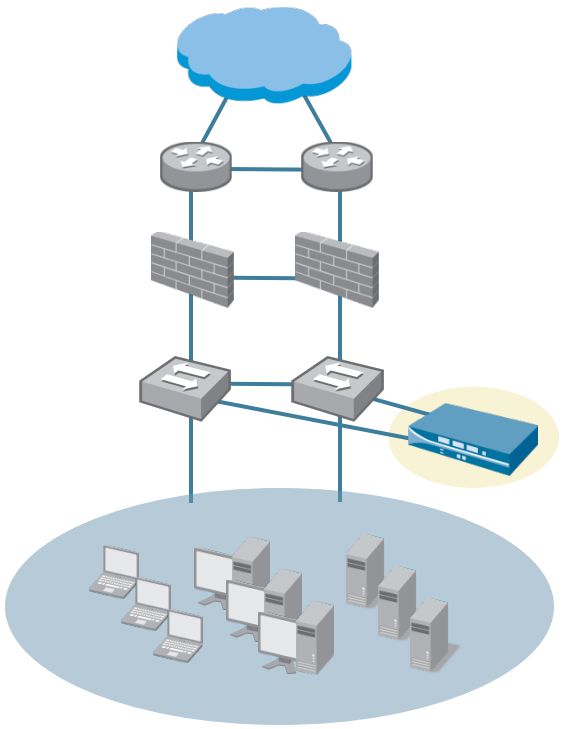
Data Plane

Network Processor
- 20 Gbps front-end network processing
- Hardware accelerated per-packet route lookup, MAC lookup and NAT

paloalto NETWORKS

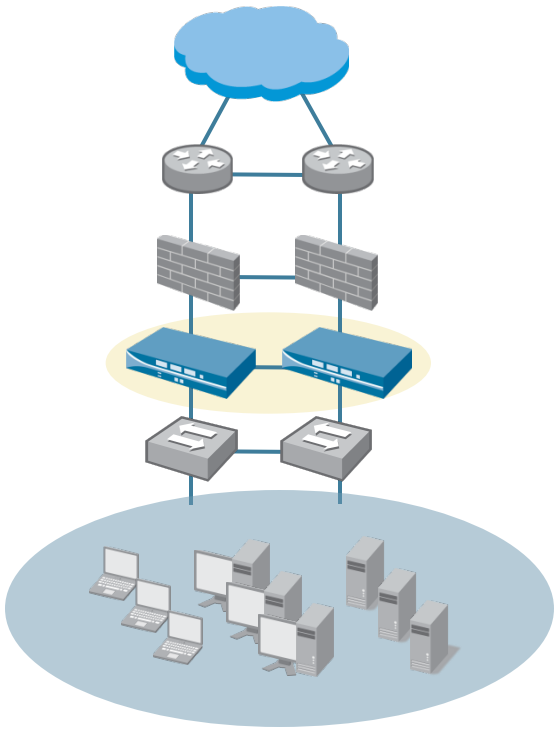
Flexible Deployment Options

Visibility



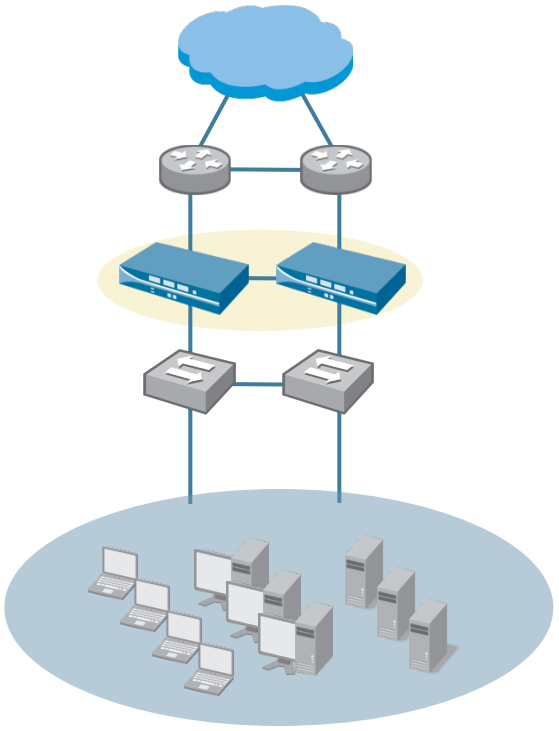
- Application, user and content visibility without inline deployment

Transparent In-Line



- IPS with app visibility & control
- Consolidation of IPS & URL filtering

Firewall Replacement



- Firewall replacement with app visibility & control
- Firewall + IPS
- Firewall + IPS + URL filtering

Thank You