Palo Alto Networks Stallion Spring Seminar -Tech Track

Peter Gustafsson, June 2010

paloalto NETWORKS

the network security company™

About Palo Alto Networks

paloalto 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 1000+ applications
  - Restores the firewall as the core of the enterprise network security infrastructure
  - Innovations: App-ID™, User-ID™, Content-ID™
- Global footprint: 1,000+ customers in 50+ countries, 24/7 support

InformationWeek 50 STARTUP

TiE 50 2009 TOP STARTUPS WINNER

BEST OF INTEROP GRAND PRIZE 2008 Presented by InformationWeek

SC MAGAZINE AWARDS 2009 Honored in the U.S.

BEST OF THE NEW DATA CENTER

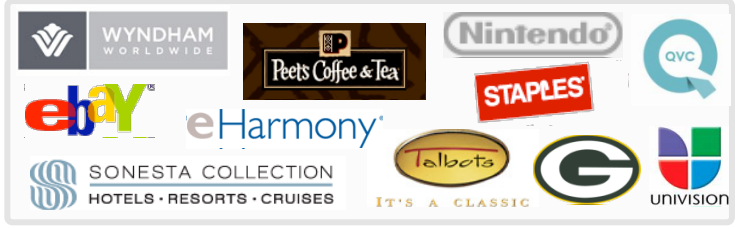
Over 1,000 Organizations Trust Palo Alto Networks

Health Care

Financial Services

Government

Media / Entertainment / Retail



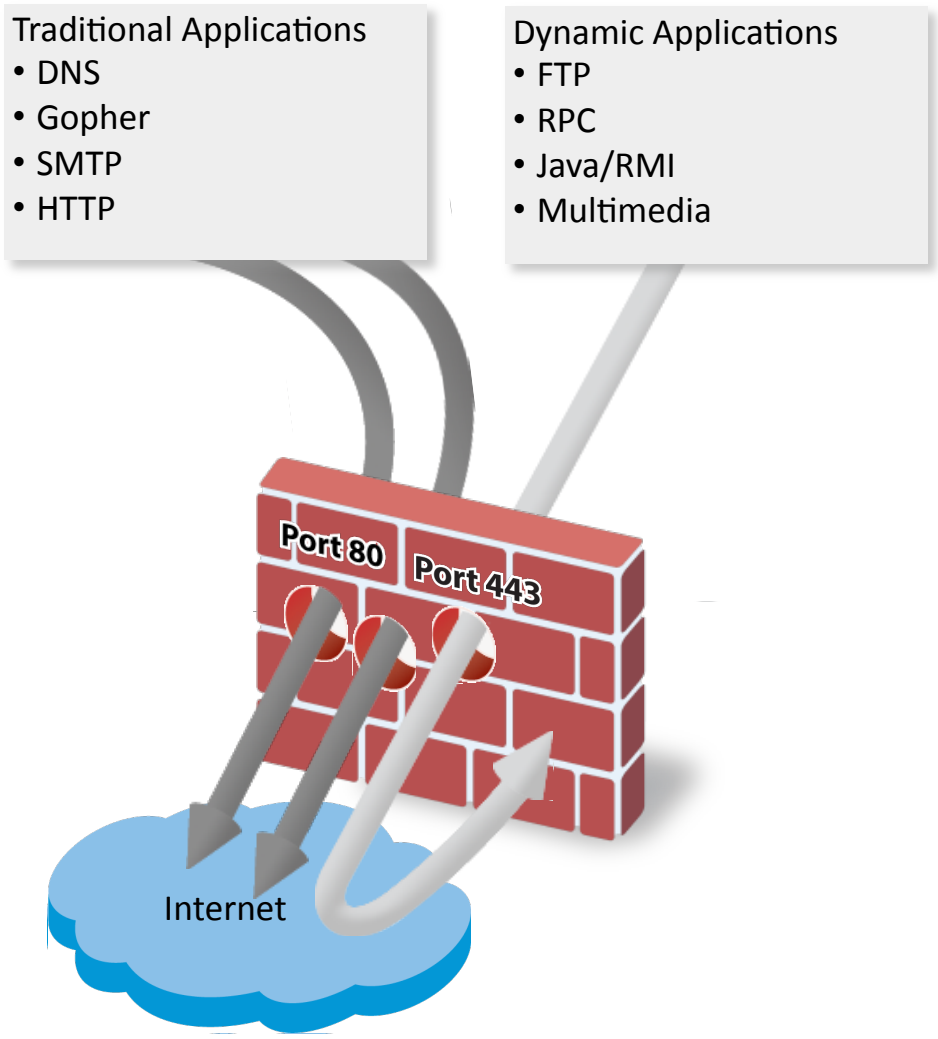
Service Providers / Services

Mfg / High Tech / Energy

Education

paloalto NETWORKS

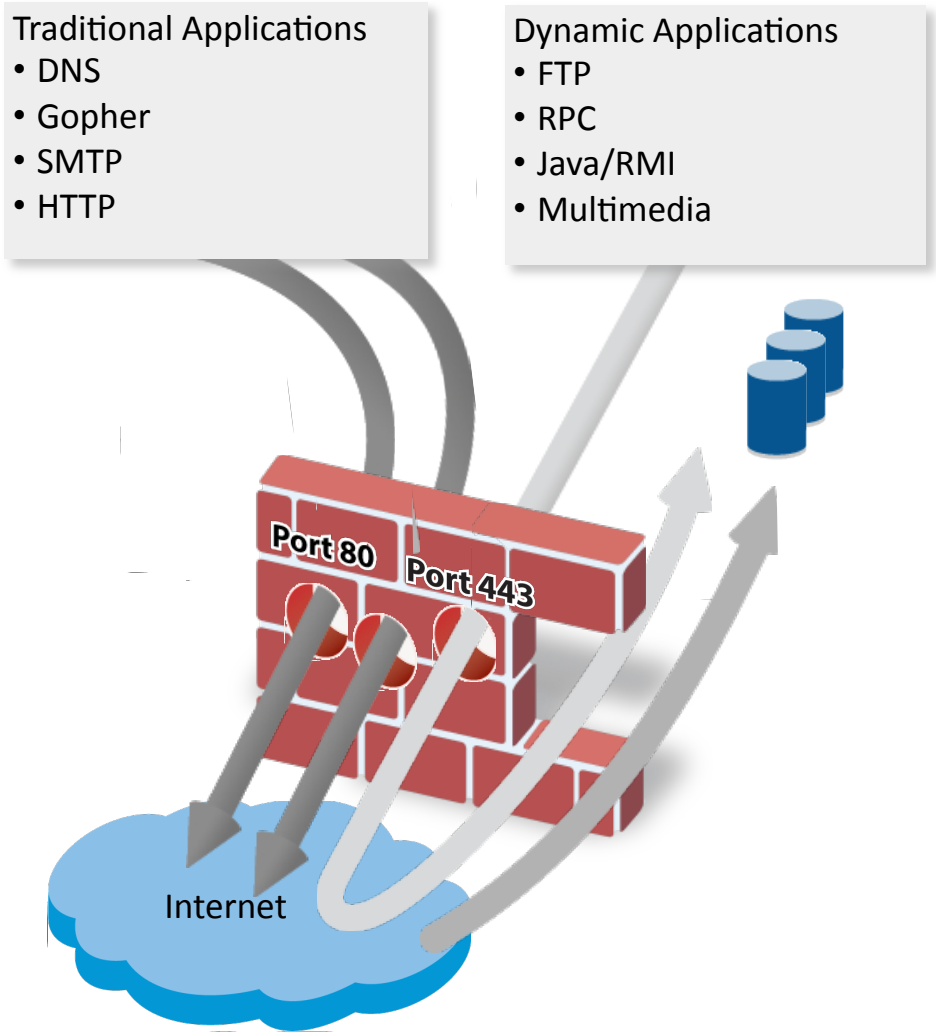
History of the Firewall: Security v1.0 Packet Filters



- Background
- Appeared mid 1980's
- Typically embedded in routers
- Classify individual packets based on port numbers

- Challenge
- Could not support dynamic applications

Security v1.0 Response: Rip Holes in Firewall



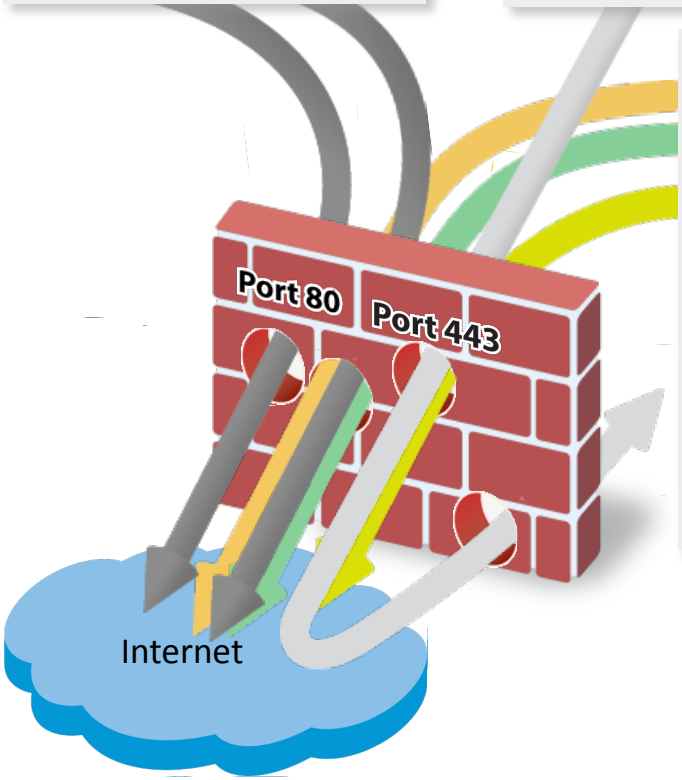
- Background
- Appeared mid 1980's
- Typically embedded in routers
- Classify individual packets based on port numbers

- Challenge
- Could not support dynamic applications
- Flawed solution was to open large groups of ports
- Opened the entire network to attack

Security v1.5: Stateful Inspection

Traditional Applications
- DNS
- Gopher
- SMTP
- HTTP

Dynamic Applications
- FTP
- RPC
- Java/RMI
- Multimedia



Evasive Applications
- Encrypted
- Web 2.0
- P2P
- Instant Messenger
- Skype
- Music
- Games
- Desktop Applications
- Spyware
- Crimeware

- Background
- Innovation created Check Point in 1994
- Used state table to fix packet filter shortcomings
- Classified traffic based on port numbers but in the context of a flow

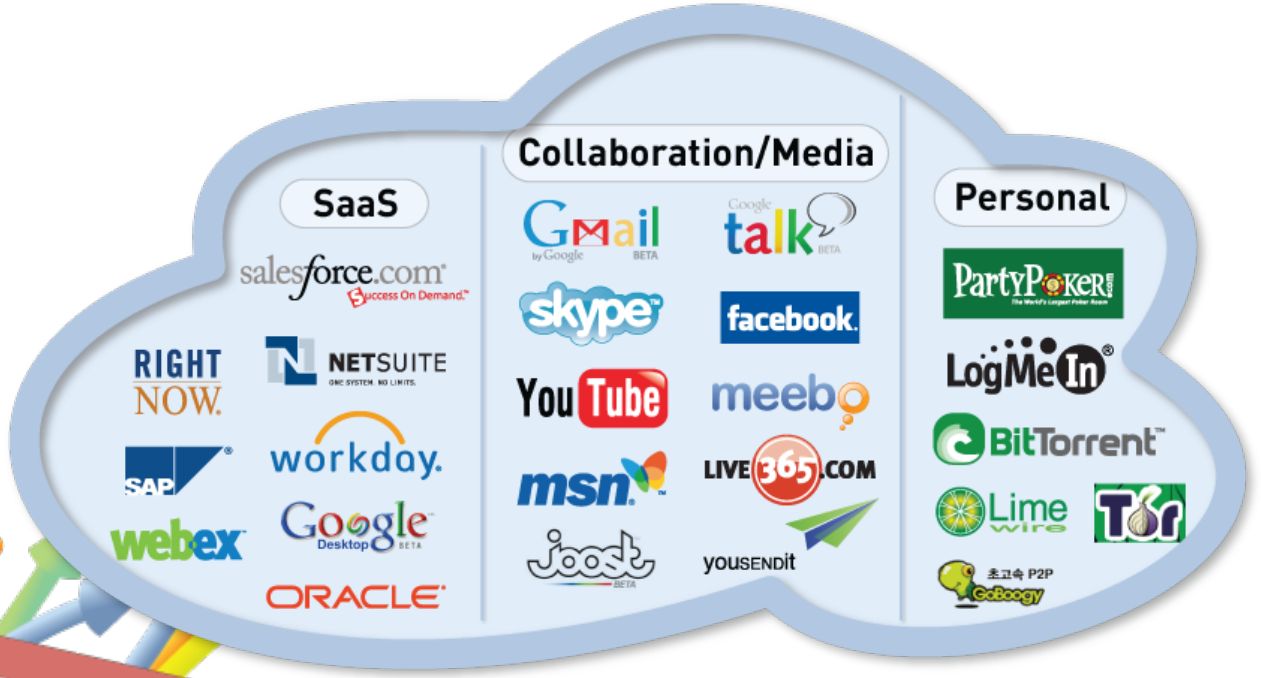
- Challenge
- Cannot identify Evasive Applications
- Embedded throughout existing security products
- Impossible to retroactively fix

paloalto NETWORKS

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

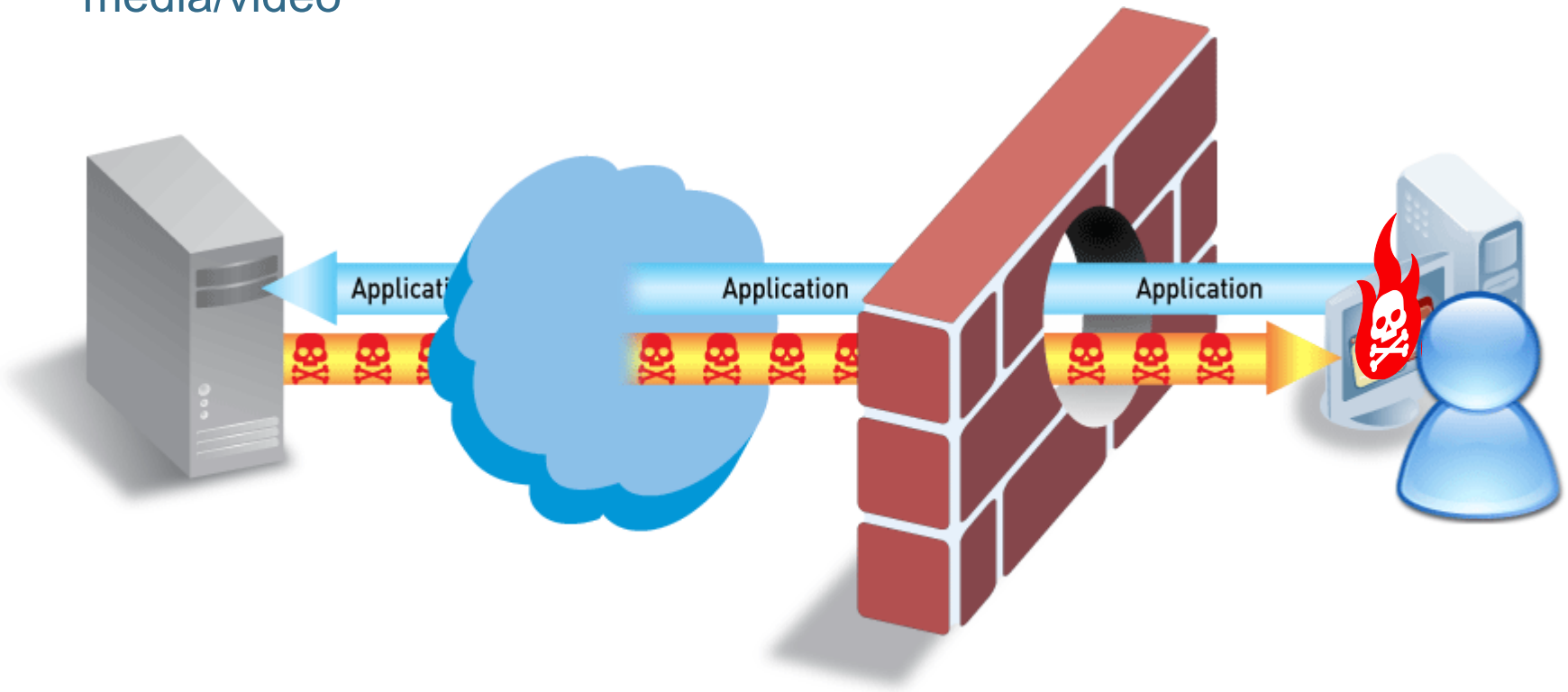
Applications Carry Risk

Applications can be “threats”

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

Applications carry threats

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

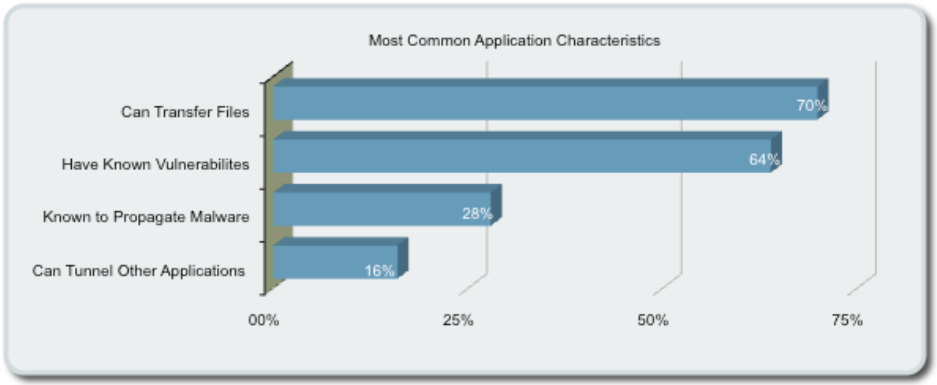


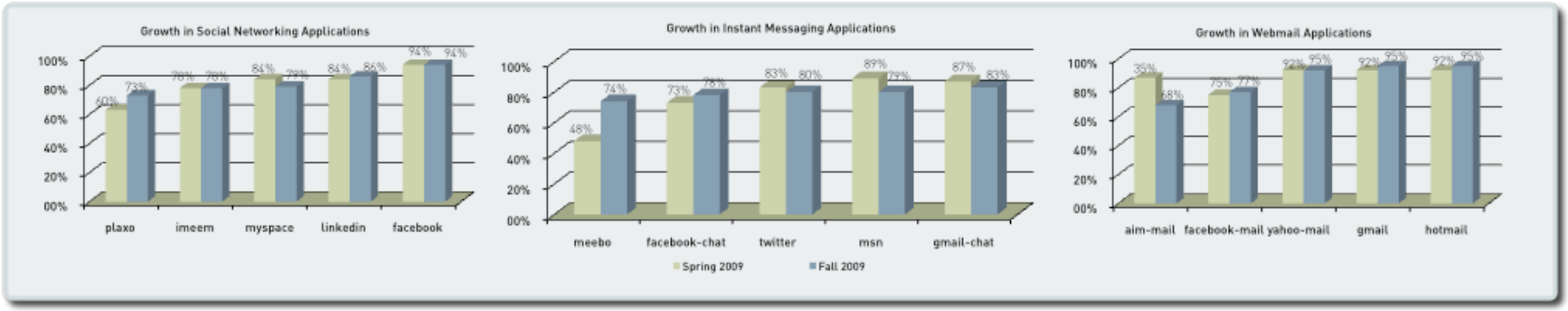
Applications & application-level threats result in major breaches – Pfizer, VA, US Army

Enterprise 2.0 Applications and Risks Widespread

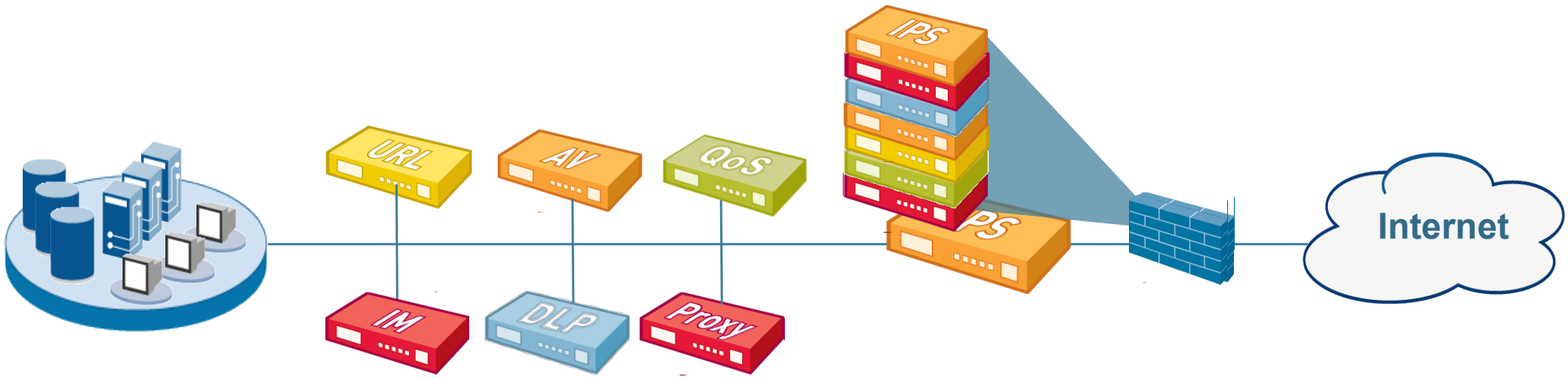
- Palo Alto Networks' Application Usage & Risk Report highlights actual behavior of 1M+ users across more than 200 organizations
  - Enterprise 2.0 applications – Twitter, Facebook, Sharepoint, and blog/wiki applications – both frequency and use skyrocketing – for both personal and business use. Facebook extends social networking dominance to IM and webmail
  - Bottom line: despite all having firewalls, and most having IPS, proxies, & URL filtering – none of these organizations could control what applications ran on their networks

Applications carry risks: business continuity, data loss, compliance, productivity, and operations costs



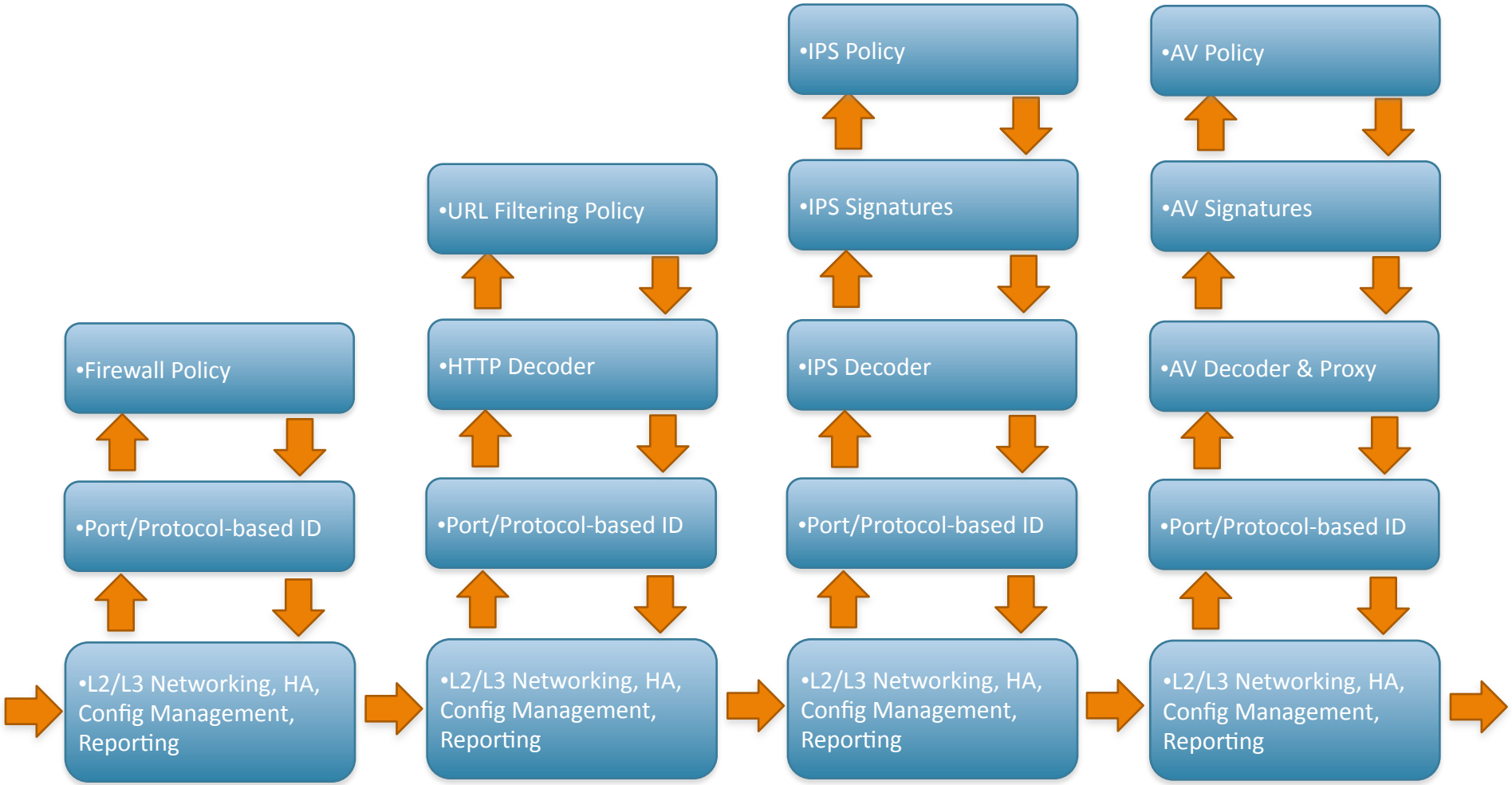


Technology Sprawl & Creep Are Not The Answer



- "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

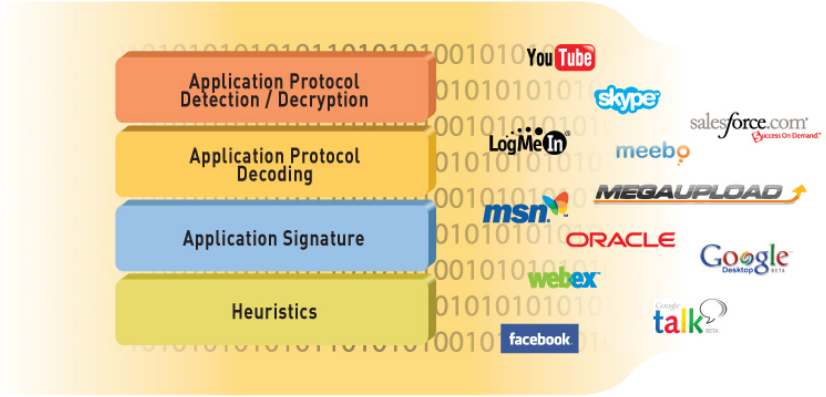
New Requirements for the Firewall

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

Identification Technologies Transform the Firewall

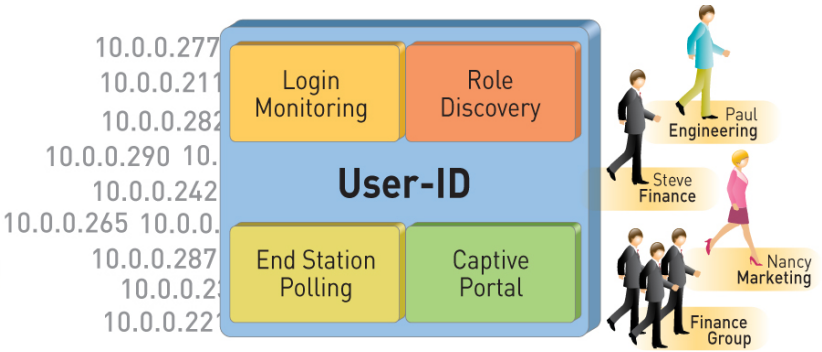
App-ID™

Identify the application



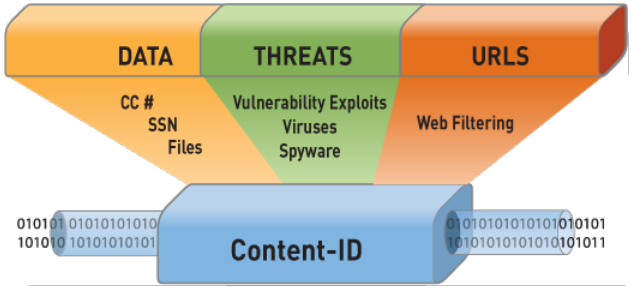
User-ID™

Identify the user

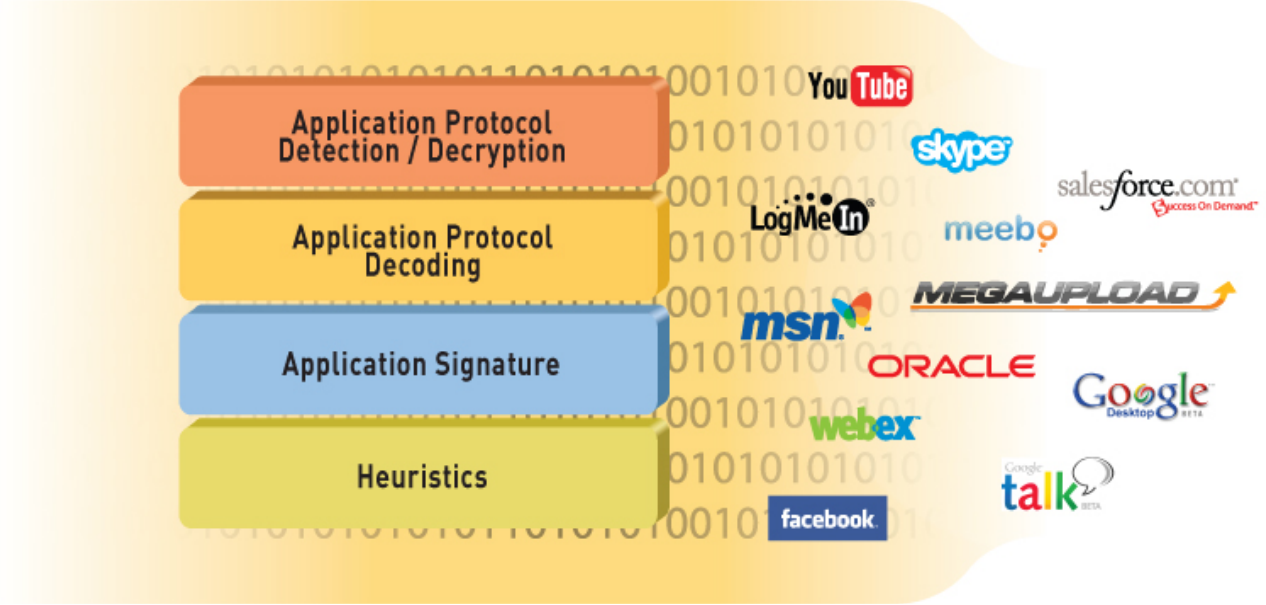


Content-ID™

Scan the content

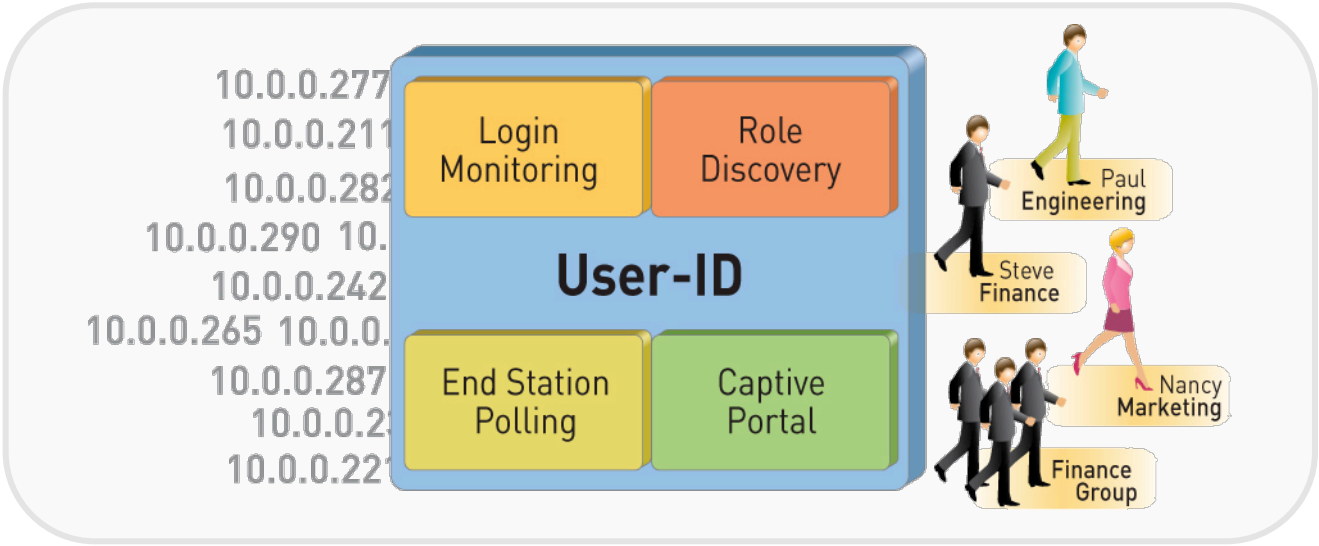


App-ID: Comprehensive Application Visibility



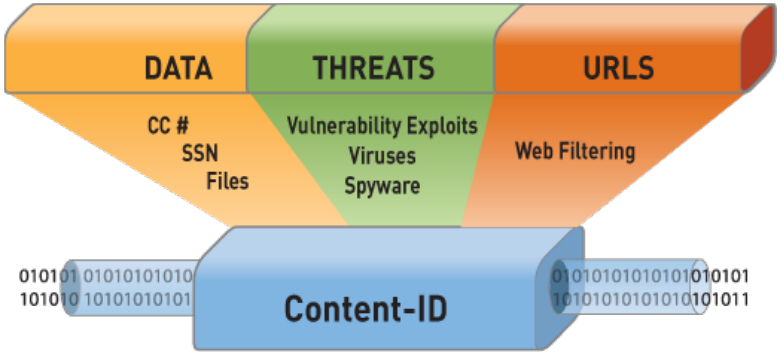
- Policy-based control more than 1000 applications distributed across five categories and 25 sub-categories
- Balanced mix of business, internet and networking applications and networking protocols
- 3 - 5 new applications added weekly
- App override and custom HTTP/SSL applications address internal applications

User-ID: Enterprise Directory Integration



- Users no longer defined solely by IP address
  - Leverage existing enterprise directory services (Active Directory, LDAP, eDirectory) without desktop agent rollout
  - Identify Citrix users and tie policies to user and group, not just the IP address
- Manage and enforce policy based on user and/or group
- Understand user application and threat behavior based on username, not just IP
- Investigate security incidents, generate custom reports
- XML API enables integration with other user repositories

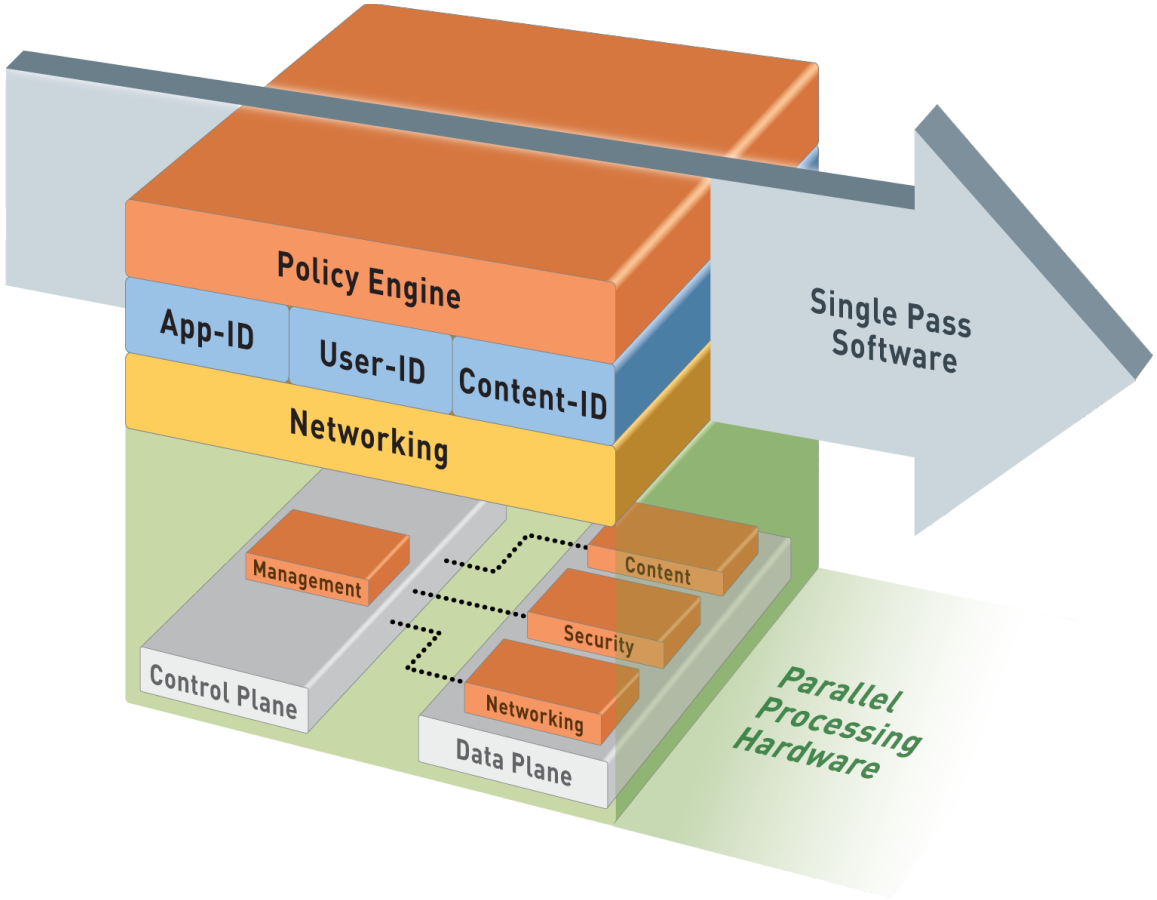
Content-ID: Real-Time Content Scanning



Detect and block a wide range of threats, limit unauthorized data transfer and control non-work related web surfing

- Stream-based, not file-based, for real-time performance
  - Uniform signature engine scans for broad range of threats in single pass
  - Vulnerability exploits (IPS), viruses, and spyware (both downloads and phone-home)
- Block transfer of sensitive data and file transfers by type
  - Looks for CC # and SSN patterns
  - Looks into file to determine type – not extension based
- Web filtering enabled via fully integrated URL database
  - Local 20M URL database (78 categories) maximizes performance (1,000's URLs/sec)
  - Dynamic DB and customizable categories adapts to local, regional, or industry focused surfing patterns

Single-Pass Parallel Processing™ (SP3) Architecture



Single Pass

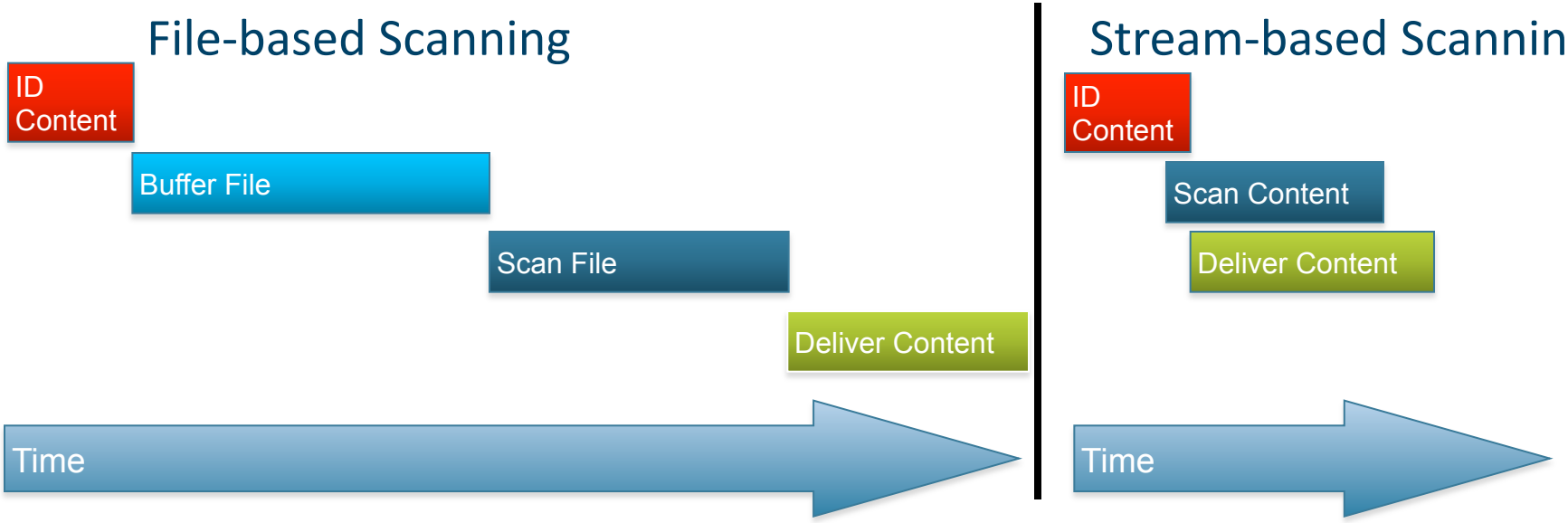
- Operations once per packet
  - Traffic classification (app identification)
  - User/group mapping
  - Content scanning – threats, URLs, confidential data
- One policy

Parallel Processing

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

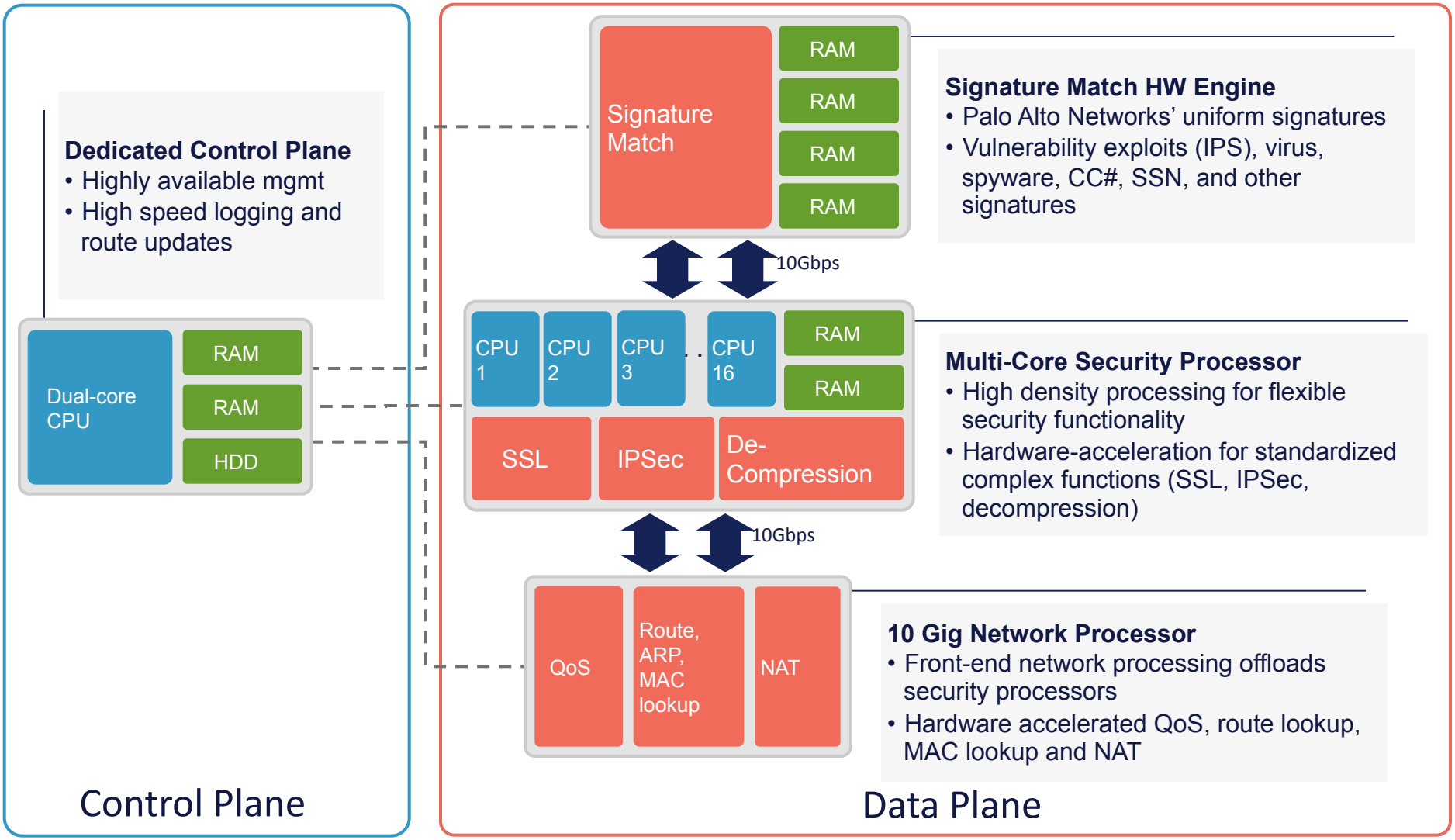
Up to 10Gbps, Low Latency

Content-ID Uses Stream-Based Scanning



- Stream-based, not file-based, for real-time performance
  - Dynamic reassembly
- Uniform signature engine scans for broad range of threats in single pass
- Threat detection covers vulnerability exploits (IPS), virus, and spyware (both downloads and phone-home)

Purpose-Built Architecture: PA-4000 Series



Palo Alto Networks Next-Generation Firewalls

PA-4060

- 10 Gbps FW
- 5 Gbps threat prevention
- 2,000,000 sessions
- 4 XFP (10 Gig) I/O
- 4 SFP (1 Gig) I/O

PA-4050

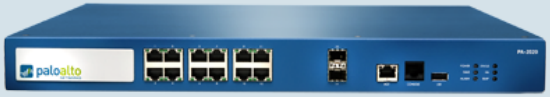
- 10 Gbps FW
- 5 Gbps threat prevention
- 2,000,000 sessions
- 16 copper gigabit
- 8 SFP interfaces

PA-4020

- 2 Gbps FW
- 2 Gbps threat prevention
- 500,000 sessions
- 16 copper gigabit
- 8 SFP interfaces

PA-2050

- 1 Gbps FW
- 500 Mbps threat prevention
- 250,000 sessions
- 16 copper gigabit
- 4 SFP interfaces



PA-2020

- 500 Mbps FW
- 200 Mbps threat prevention
- 125,000 sessions
- 12 copper gigabit
- 2 SFP interfaces

PA-500

- 250 Mbps FW
- 100 Mbps threat prevention
- 50,000 sessions
- 8 copper gigabit

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 / passive
  - Configuration and session synchronization
  - Path, link, and HA monitoring
- Virtual Systems
  - Establish multiple virtual firewalls in a single device (PA-4000 and PA-2000 Series only)
- Simple, flexible management
  - CLI, Web, Panorama, SNMP, Syslog


PA-4060


PA-4050

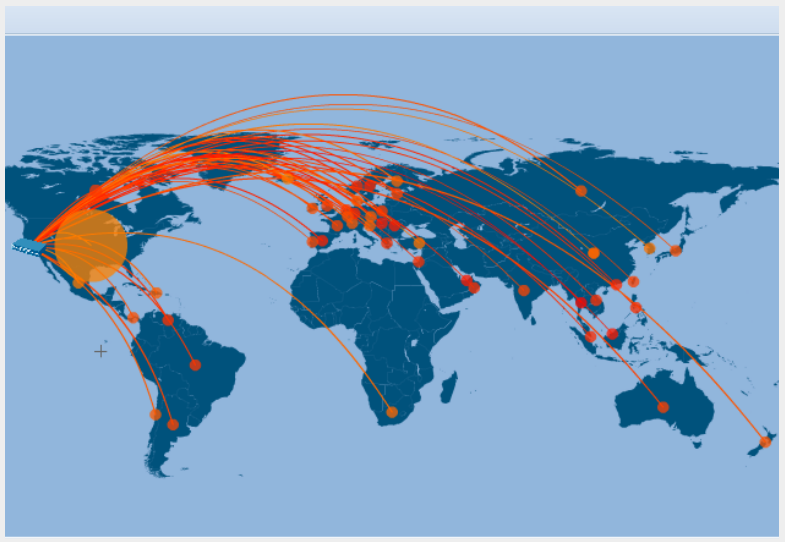

PA-4020


PA-2050


PA-2020


PA-500

Enables Visibility Into Applications, Users, and Content



Category	2	Subcategory	Technology	Risk	Characteristic
116 **business-systems**		8 auth-service	41 browser-based	179 1	107 Vulnerabilities
129 collaboration		13 database	129 client-server	63 2	55 Prone to Misuse
73 general-internet		11 encrypted-tunnel	160 network-protocol	49 3	159 Widely used
49 media		7 erp-crm	4 peer-to-peer	17 4	20 Excessive Bandwidth
218 **networking**		18 general-business		26 5	103 Transfers Files
2 unknown		23 infrastructure			53 Evasive
		116 ip-protocol			46 Used by Malware
		37 management			61 Tunnels Other Apps

Name	Shared	Category	Subcategory	Risk	Technology
3pc	✔	networking	ip-protocol	1	network-protocol
active-directory	✔	business-systems	auth-service	2	client-server
activenet	✔	networking	ip-protocol	1	network-protocol
afp	✔	business-systems	storage-backup	3	client-server
altiris	✔	business-systems	management	1	client-server
apc-powerchute	✔	business-systems	general-business	2	client-server
apple-airport	✔	networking	infrastructure	2	network-protocol
apple-update	✔	business-systems	software-update	3	client-server
argus	✔	networking	ip-protocol	1	network-protocol
aris	✔	networking	ip-protocol	1	network-protocol
asproxy	✔	networking	proxy	5	browser-based
avamar	✔	business-systems	storage-backup	2	client-server
avaya-phone-ping	✔	business-systems	management	2	client-server
avocent	✔	networking	remote-access	3	client-server
avoidr	✔	networking	proxy	5	browser-based
backup-exec	✔	business-systems	storage-backup	3	client-server
backweb	✔	business-systems	erp-crm	1	browser-based
bbn-rcc-mon	✔	networking	ip-protocol	1	network-protocol
beinsync	✔	networking	remote-access	2	client-server

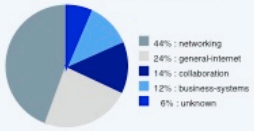
Application and Threat Summary

Apr 09, 2008

Application Usage

Risk Trend

Category Breakdown



Top 5 Applications

Application	Sessions	Bytes
web-browsing	77,859	3,061,989,086
msrpc	46,121	5,220,877,220
icmp	38,103	5,362,784
dns	31,188	11,993,882
skype-probe	28,246	13,009,461

User Behavior

Top 5 Users

User	Sessions	Bytes
paloaltonetwork\binahara	743,869	53,737,432,686
paloaltonetwork\bsi	557,999	1,855,589,371
paloaltonetwork\ycheng	520,748	2,109,032,430
paloaltonetwork\mjacobsen	156,793	4,230,857,356
paloaltonetwork\akaverma	131,483	6,900,749,079

Top 5 URL Categories

Category	Count
unknown	93,844
infrastructure	23,828
news	14,870
computing-and-internet	14,756
advertisements-and-popups	13,643

Top 5 Destination Countries

Destination	Count
Reserved (10.0.0.0 - 10.255.255.255)	3,267,489
United States	1,166,207
Unknown	73,266
France	70,470
China	64,917

paloaltonetwork\binahara

Highest Risk User

Top 5 URL Categories

Category	Count
business	13,790
unknown	10,893
computing-and-internet	3,807
infrastructure	2,784
news	1,985

Top 5 Applications

Application	Sessions	Bytes
skype-probe	957,518	485,701,118
unknown-udp	81,392	20,242,917
ssl	166,063	1,157,247,715
skype	133,752	65,618,460
msrpc	817,743	218,670,488,833

Top 5 Threats

Threat	Count
MiniBug retrieve weather information	6,890
SCAN: Host Sweep	15,956
Ipswitch Mail LDAP Daemon Request Parsing Stack Overflow Vulnerability	216

Threat Types

Top 5 Spyware

Spyware	Count
MiniBug retrieve weather information	377

Top 5 Vulnerabilities

Vulnerability	Count
AWStats Remote Code Execution Vulnerability	7,336
DistCC Daemon Command Execution	5,125
Mediawiki Improper URI Sanitization Remote Command Execution Vulnerability	3,558
HTTP OPTIONS Method	2,482
HTTP SQL Injection Attempt	2,372

Top 5 Viruses

Virus	Count

No matching data found!

Threat

Top 5 Attackers

Address	Count
10.0.0.67	30,365
d9ynymc1.paloaltonetworks.local	21,686
binahara-xp.paloaltonetworks.local	15,956
binahara-xp.paloaltonetworks.local	12,960
pan00097.paloaltonetworks.local	3,888

Top 5 Victims

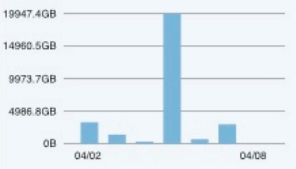
Address	Count
10.0.0.251	34,253
pa-dc-1.paloaltonetworks.local	8,895
pa-dc-2.paloaltonetworks.local	7,823
panserver.paloaltonetworks.local	7,226
panserver2.paloaltonetworks.local	6,095

Top 5 Attacker Countries

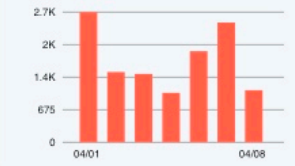
Country	Count
Reserved (10.0.0.0 - 10.255.255.255)	101,082
United States	377

Trends

Bandwidth



Threats



Demo! Cross your fingers…