

# The Next Step : Application Aware Network Security

*Palo Alto Networks*



## Agenda

Do you know what's happening on your network?

Do you know 'what' threats are?

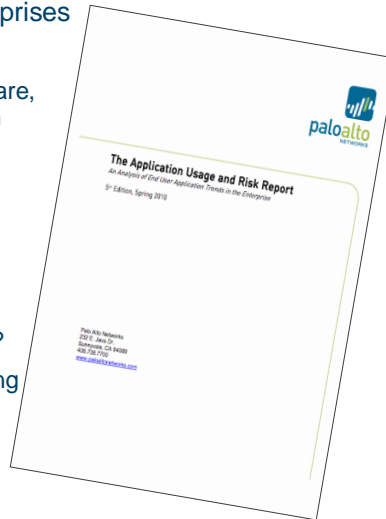
The old approach

What are the 'next' requirements?

Next Step: Real Network Security

# Real Data – What’s on Enterprise Networks

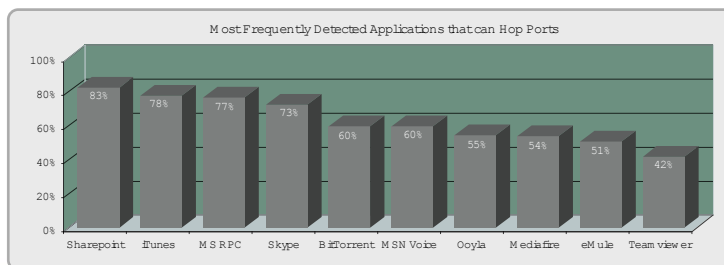
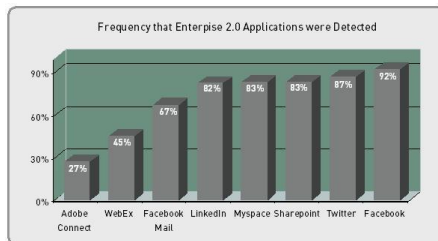
- Application usage assessment of 340 enterprises
  - 1M+ users
  - Across verticals: financial services, health care, manufacturing, government, retail, education
- Looks at
  - Real enterprise traffic
  - How are networks being used?
  - What applications are running on enterprise networks?
  - Which applications are considered high-risk?
  - What are the risks associated with the existing application mix?
  - What threats are on enterprise networks?
- Note: Next edition scheduled for Q3Y10



# Enterprise 2.0 Applications and Risks Widespread

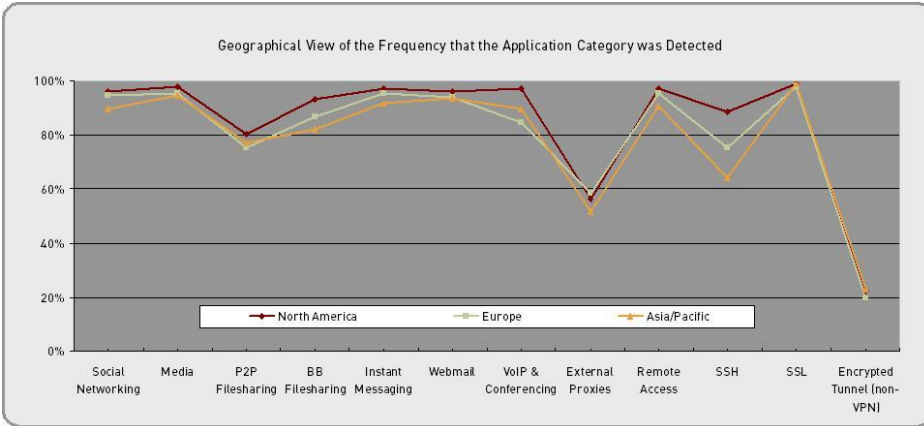
Palo Alto Networks' latest Application Usage & Risk Report highlights actual behavior of 1M+ users across more than 340 organizations

- Enterprise 2.0 applications – like Twitter, Facebook, and Sharepoint – continue to rise for both personal and business use. Facebook and Google extend dominance outside of core applications
- Tunneling and port hopping are common
- Bottom line: all had firewalls, and most had IPS, proxies, & URL filtering – but none of these organizations could control what applications ran on their networks



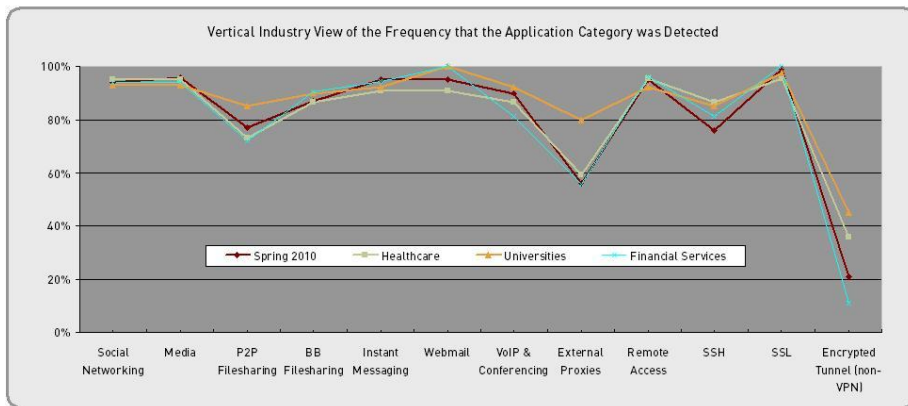
## Geographically – Usage is Universal

- Users: High speed access and a desire to use whatever application they want...



## An Industry View – Universal Use Continues

- Financial services, universities and healthcare all show similar usage patterns



## Network Threats: Today's Thinking

- When talking about network threats, the following threats come into mind:
  - Viruses
  - Spyware
  - Exploits/Intrusions
  - Worms
  - Bots
  - Trojans
  - Etc.
- But these are not threats...

!!! These are technologies and mechanisms which can carry threats !!!

## Network Threats: The Real Threats

- From the business's perspective, network-born threats include:
  - Data loss
  - Productivity loss
  - Increasing operations costs (e.g., helpdesk overload)
  - Non-compliance with regulations
  - Business continuity
  - Bad PR
- These threats can be introduced by viruses, spyware and exploits but through other mechanisms as well

!!! Uncontrolled applications carry risks of all the threats in the list above !!!

## Applications' Double Threat

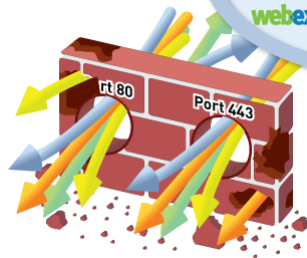
- Applications bring threats:
  - Data loss
  - Productivity loss
  - Increasing operations costs (e.g., helpdesk overload)
  - Non-compliance with regulations
  - Business continuity
  - Bad PR
- Applications also carry traditional threat vectors
  - Viruses, Spyware, Exploits
- When allowing an application to be used, its traffic needs to be secured
  - Scan for Viruses, Spyware, Exploits, Data Loss, etc.

## What the Analysts Say...

- Gartner Group
  - "The days when port = protocol = application are behind us. An increasing percentage of enterprise network traffic is being funneled through a few well-known ports, more port-hopping or dynamic application content, such as Web 2.0. In many cases, traffic is being encrypted."
- Forrester Research
  - Firewalls must go beyond port/protocol identification to deliver visibility and control of applications—in particular those encrypted with SSL—to provide granular visibility and control over all traffic rather than a percentage of it." -- *Rob Whiteley*

## 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

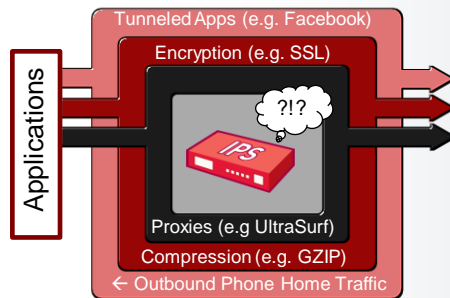
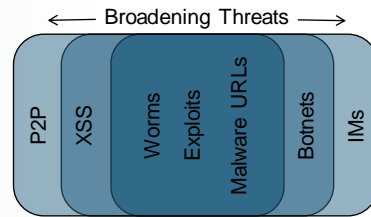
## Traditional FW is Not Protecting the Network

- **Fundamentally Limited Identification Capability**
  - Classifies traffic based on port numbers in the context of a flow (Stateful Inspection)
- **Fails to Understand Applications and Vectors**
  - No way to identify evasive applications and/or contexts
- **Limitations on Traditional FW (architecture)**
  - Impossible to retroactively fix
  - Fix Requires new foundations
- **Fails to Understand Users**
  - Typically only 5-tuple
  - Does not understand all layers of the OSI model
- **Is however deployed at the best spot in the network to see all.**

## The Threat Landscape Has Changed, IPS Has Not

- **The scope of threats has broadened**

- No longer limited to vulnerability exploits
- Malware, botnets, applications, dangerous URLs all form the threats vectors



- **Applications revolutionized the transmission vector**

- Threats use apps to hide, circumvent (encryption, compression, evasion)
- This has created a new generation of “dark” threat vectors
- Largely ignored by IPS solutions today

## Traditional IPS is Not Protecting the Network

- **Fundamentally Reactive Approach**

- Waits for attacks to happen – does nothing to proactively reduce the exposure

- **Fails to Understand Applications and Vectors**

- Catches only a few “bad” apps as threats, most apps are missed
- Misses threats hidden by apps (SSL, compression, protocol in protocol, etc)
- No concept of grey areas – response is kill or allow, no enablement

- **Limitations on Threat Detection**

- Spotty coverage beyond traditional vulnerability exploits (Malware URLs, botnets, XSS)
- Typically can't enable all IPS protections due to performance limitations

- **Fails to Understand Users**

- Typically only inspects inbound traffic due to poor performance (misses phone home)
- Does not see user in IPS context (John was infected vs. 192.168.10.25 was infected)

# Traditional Systems Have Limited Understanding

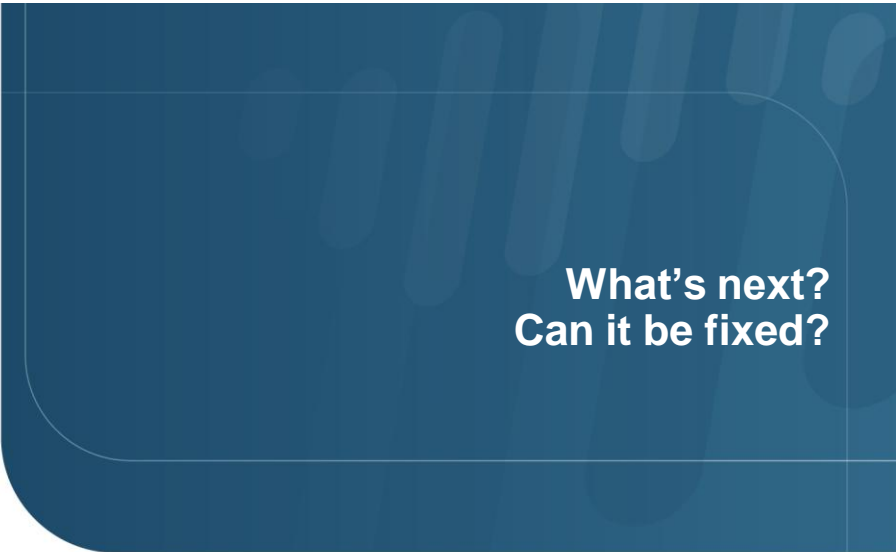
Applications	
Risk	Application
1	web-browsing
2	dns
3	ssl
4	bittorrent
5	unknown-udp
6	msrpc
7	netbios-ns
8	limelight
9	smtp
10	neonet
11	slp
12	grutella
13	flash
14	photobucket
15	hotmail
16	unknown-tcp
17	emule
18	facebook
19	yahoo-mail
20	ntp
21	mssql-db
22	myspace
23	youtube
24	mssql
25	web-crawler

Some port-based apps caught by firewalls (when well-behaved)

Some web-based apps caught by URL filtering or proxy

Some evasive apps caught by IPS

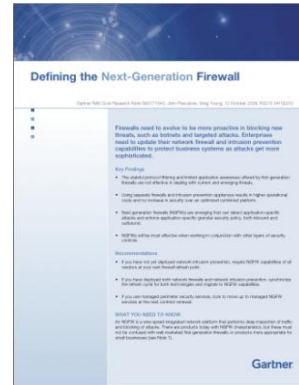
None give a comprehensive view of what is going on in the network



## What are the NGFW Requirements

### “Defining the Next-Generation Firewall,”

- ✓ **Application Awareness and Full Stack Visibility**  
Identify and control applications – App-ID
- ✓ **Integrated Rather Than Co-Located IPS**  
Include full IPS, without compromising performance – Content-ID
- ✓ **Extra-Firewall Intelligence to Identify Users**  
Bring users and groups into the firewall policy – User-ID
- ✓ **Standard First-Generation Firewall Capabilities**  
Packet filtering, state, flexible NAT, IPSec, SSL VPNs, etc.
- ✓ **Support “bump in the wire” Deployments**  
Multiple options for transparent deployment behind existing firewalls



## New Requirements for Intrusion Prevention

- **Control the Threat Vector**
  - By first controlling which applications run on the network, organizations greatly reduce their attack surface
- **Scan Allowed Application Traffic for Threats**
  - Identify and stop threats
  - Scan inside SSL and compressed content
  - Stop leaks of confidential data (e.g., credit card #)
- **High performance**
  - Multi-Gbps, low latency
  - Even when scanning both client and server traffic – a requirement for threats that come in over Internet applications to desktops
- **Solid research and support – rapid deployment of new protections**

# Can't IPS Block Applications?

- Blocking applications, even if possible, is not the right answer
  - Yes, there are harmful applications that need to be blocked
  - Controlling those applications however does make much more sense
- Many “Web 2.0” applications are useful (port 80/443)
  - Enhancing productivity
    - *The application itself might not always be business related though...*
  - Giving competitive advantage to the business
  - Employee retention and productivity
    - *Happy and motivated*
    - *Comfort zone*
- Some applications are good but have bad features
- IPS cannot
  - Explicitly allow good traffic (can only block bad traffic)
    - *Negative Enforcement Model*
  - Identify users
  - Identify which feature within the application is being used



# What is NOT a NGFW

## In “Defining the Next-Generation Firewall,” Gartner Also Describes What an NGFW is NOT!

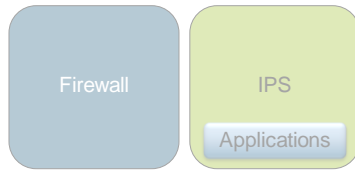
- ✓ UTM devices are not next-generation firewalls
- ✓ DLP devices are not next-generation firewalls
- ✓ Secure web gateways are not next-generation firewalls
- ✓ Email security gateways are not next-generation firewalls

### Gartner’s Recommendations

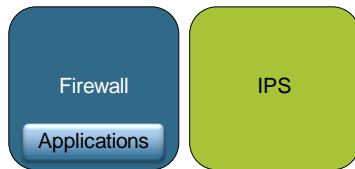
- Move to next-generation firewalls at the next refresh opportunity – whether for firewall, IPS, or the combination of the two.



## 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
4. Can't "allow, but..."



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

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



## Important buzzwords in IPS context

- Zero-day attack detection:
  - Often in reference to anomaly-based detection
  - Sometimes in reference to advanced notice from Microsoft for super-Tuesday vulnerability announcements
  - Reality
    - *Mostly advance notice of threat*
      - prepped signature available at no delay by official announcement of threat
    - *Variant of existing threat*
      - covered with an existing signature, covering the vulnerability
- Protocol anomaly detection:
  - Anomaly-based detection in how the protocol is being used
  - Often used to detect buffer overflow attacks
  - Reality
    - *Almost NO effectiveness as majority of applications deviate from the protocol...*
- Traffic anomaly detection:
  - Traffic pattern anomalies with manual or automatic policy responses
  - Reality
    - *Prone to false positives as no network is the same*
    - *Often the (D)DoS mechanism*

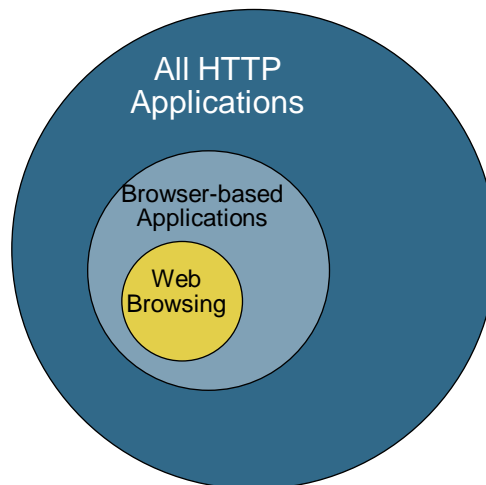


## Can Proxies Block Applications?

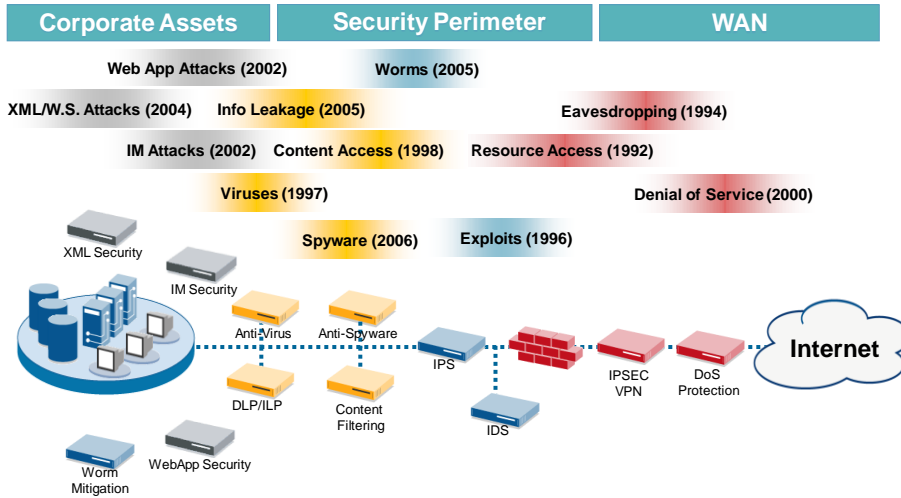
- Proxies cannot run at multi-gig
- High latency
  - Buffer/proxy files before scanning for viruses, spyware or URLs
- Cannot support millions of concurrent connections
  - Session management in both directions (client and server)
- Proxies only work for 'proxied' applications
  - Cannot build a proxy for 100's of modern applications
  - Applications essentially are broken
  - A small change in the application (update/upgrade) often breaks the proxy
- Do you want to block or protect applications?

## HTTP: Universal Application Protocol

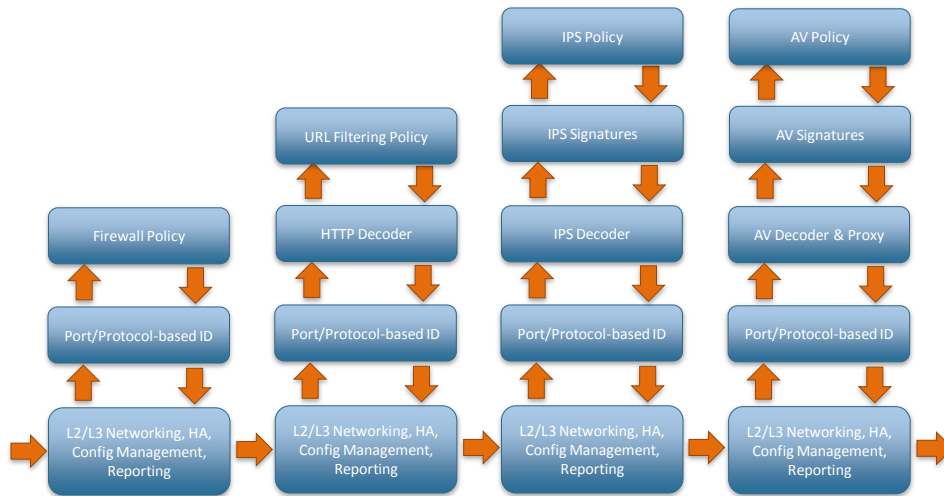
- HTTP is > 50 % of enterprise bandwidth
- Most HTTP traffic is client/server -- proxies cannot deal with it
- Less than half of the HTTP traffic are Browser-based applications -- some work with proxies and some don't
- Web browsing is not even 25% of the HTTP traffic



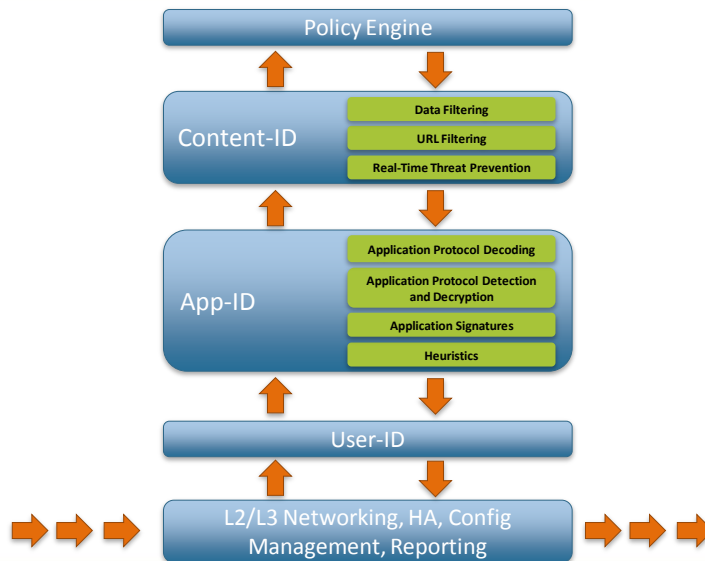
# The Traditional Approach to Network Security



# The "UTM" Approach



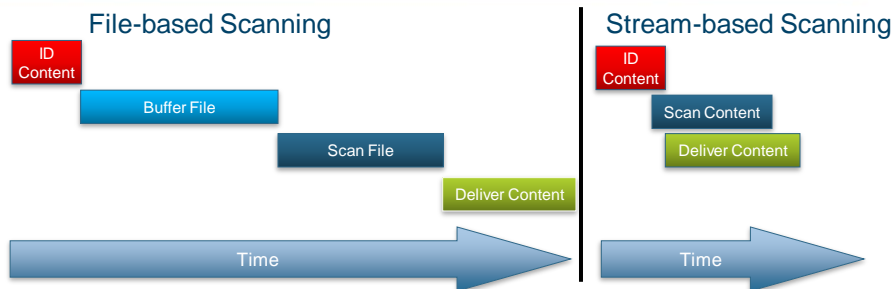
## A Better Approach...



Page 27 | © 2010 Palo Alto Networks. Proprietary and Confidential.



## Making Content-Scanning Network-Ready



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

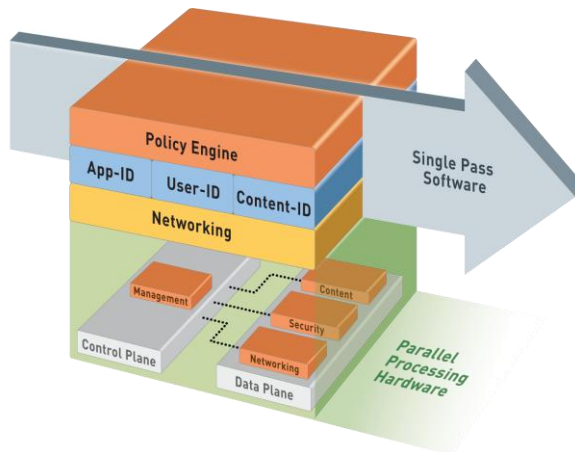
Page 28 | © 2010 Palo Alto Networks. Proprietary and Confidential.



## Single Pass – Parallel Processing

- Common protocol decoding engine, used for all traffic.
  - Pick apart an application stream to determine what the different pieces are
  - That information is then used as the basis for scanning the content for files, data, threats, and URLs
- Stream-based signature engine
  - Replaces several components commonly used in other solutions
    - > *File proxy, signature engine and HTTP decoder are not individually required*
  - Can scan the traffic, real time, only by reassembling packets as needed and only in very small amounts
    - > *vs. a proxy requiring full file before inspection can occur (latency is added)*
  - All traffic can be scanned with a single engine, instead of multiple scanning engines
    - > *Advantage of the uniform signature engine*
- By performing the content scanning task once instead of multiple times, significant processing power is saved as this is one of the most processing-intensive tasks for a security device to perform.

## 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

# How to Manage Next Generation Security



Page 31 |

## Comprehensive View of Applications, Users & Content

The screenshot displays the Palo Alto Networks Application Command Center (ACC) interface. The main view shows 'Application Information' for 'facebook-base'. The interface includes a sidebar with navigation options like 'Applications', 'URLs', and 'Source Filtering'. A 'Top Applications' table is visible at the bottom right of the main view.

Risk	Application	Sessions	Bytes
1	web-browsing	300	2,276,596
2	facebook-base	123	698,546
3	facebook-chat	46	209,009
4	chrs	26	10,454
5	myspace-base	24	605,456
6	mtp	21	3,870
7	myspace-mail	12	208,662
8	flash	10	368,366
9	myspace-im	8	34,896
10	photobucket	4	38,730
11	myspace-video	4	6,214
12	rtmpe	2	10,786
13	pdf	2	16,702
14	http-audio	2	12,402
15	google-analytics	2	2,394

- Application Command Center (ACC)
  - View applications, URLs, threats, data filtering activity
- Add/remove filters to achieve desired result

Filter on Facebook-base

Filter on Facebook-base and user Ellen Cook

Remove Facebook to expand view of Ellen

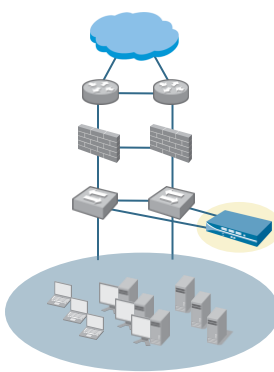
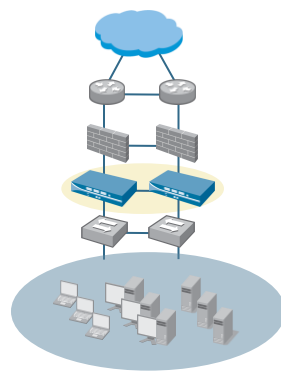
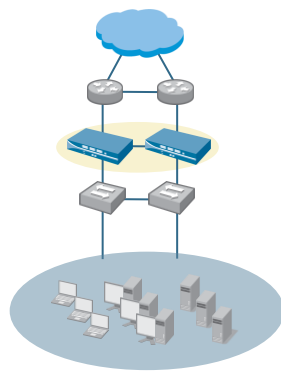


# Palo Alto Networks 'Network Security'

 <p><b>PA-4060</b></p> <ul style="list-style-type: none"> <li>• 10 Gbps FW</li> <li>• 5 Gbps threat prevention</li> <li>• 2,000,000 sessions</li> <li>• 4 XFP (10 Gig) I/O</li> <li>• 4 SFP (1 Gig) I/O</li> </ul>	 <p><b>PA-4050</b></p> <ul style="list-style-type: none"> <li>• 10 Gbps FW</li> <li>• 5 Gbps threat prevention</li> <li>• 2,000,000 sessions</li> <li>• 16 copper gigabit</li> <li>• 8 SFP interfaces</li> </ul>	 <p><b>PA-4020</b></p> <ul style="list-style-type: none"> <li>• 2 Gbps FW</li> <li>• 2 Gbps threat prevention</li> <li>• 500,000 sessions</li> <li>• 16 copper gigabit</li> <li>• 8 SFP interfaces</li> </ul>
 <p><b>PA-2050</b></p> <ul style="list-style-type: none"> <li>• 1 Gbps FW</li> <li>• 500 Mbps threat prevention</li> <li>• 250,000 sessions</li> <li>• 16 copper gigabit</li> <li>• 4 SFP interfaces</li> </ul>	 <p><b>PA-2020</b></p> <ul style="list-style-type: none"> <li>• 500 Mbps FW</li> <li>• 200 Mbps threat prevention</li> <li>• 125,000 sessions</li> <li>• 12 copper gigabit</li> <li>• 2 SFP interfaces</li> </ul>	 <p><b>PA-500</b></p> <ul style="list-style-type: none"> <li>• 250 Mbps FW</li> <li>• 100 Mbps threat prevention</li> <li>• 50,000 sessions</li> <li>• 8 copper gigabit</li> </ul>



# Flexible Deployment Options

<p><b>Visibility</b></p> 	<p><b>Transparent In-Line</b></p> 	<p><b>Firewall Replacement</b></p> 
<ul style="list-style-type: none"> <li>• Application, user and content visibility without inline deployment</li> </ul>	<ul style="list-style-type: none"> <li>• IPS with app visibility &amp; control</li> <li>• Consolidation of IPS &amp; URL filtering</li> </ul>	<ul style="list-style-type: none"> <li>• Firewall replacement with app visibility &amp; control</li> <li>• Firewall + IPS</li> <li>• Firewall + IPS + URL filtering</li> </ul>



## Addresses Three Key Business Problems

- **Identify and Control Applications**
  - Visibility of 1000+ applications, regardless of port, protocol, encryption, or evasive tactic
  - Fine-grained control over applications (allow, deny, limit, scan, shape)
  - Addresses the key deficiencies of legacy firewall infrastructure
- **Prevent Threats**
  - Stop a variety of threats – exploits (by vulnerability), viruses, spyware
  - Stop leaks of confidential data (e.g., credit card #, social security #)
  - Stream-based engine ensures high performance
  - Enforce acceptable use policies on users for general web site browsing
- **Simplify Security Infrastructure**
  - Put the firewall at the center of the network security infrastructure
  - Reduce complexity in architecture and operations



the network **security** company<sup>™</sup>