Palo Alto Networks
技术对比

paloalto NETWORKS

Agenda

- CHECKPOINT

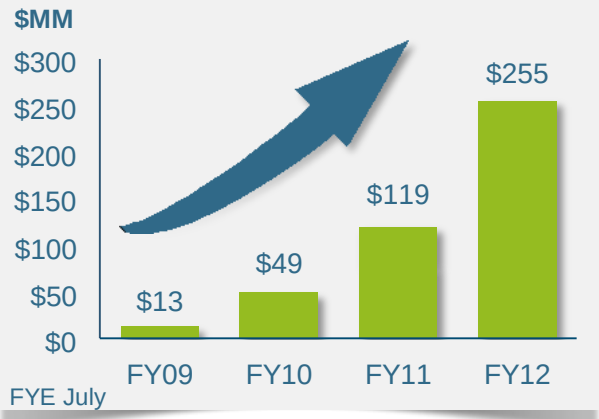
Palo Alto Networks 概況

NYSE SYMBOL: PANW

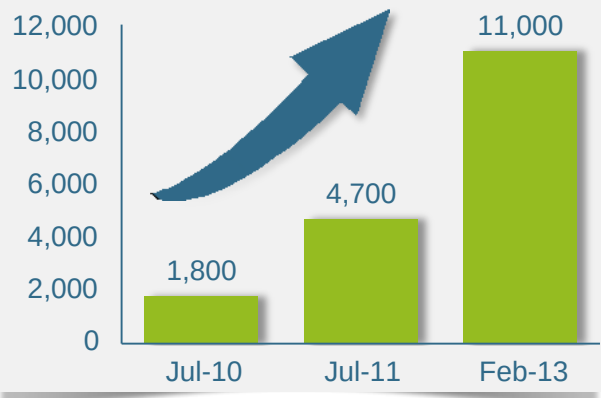
Corporate highlights

- Founded in 2005; first customer shipment in 2007
- Safely enabling applications
- Able to address all network security needs
- Exceptional ability to support global customers
- Experienced technology and management team
- 1,000+ employees globally

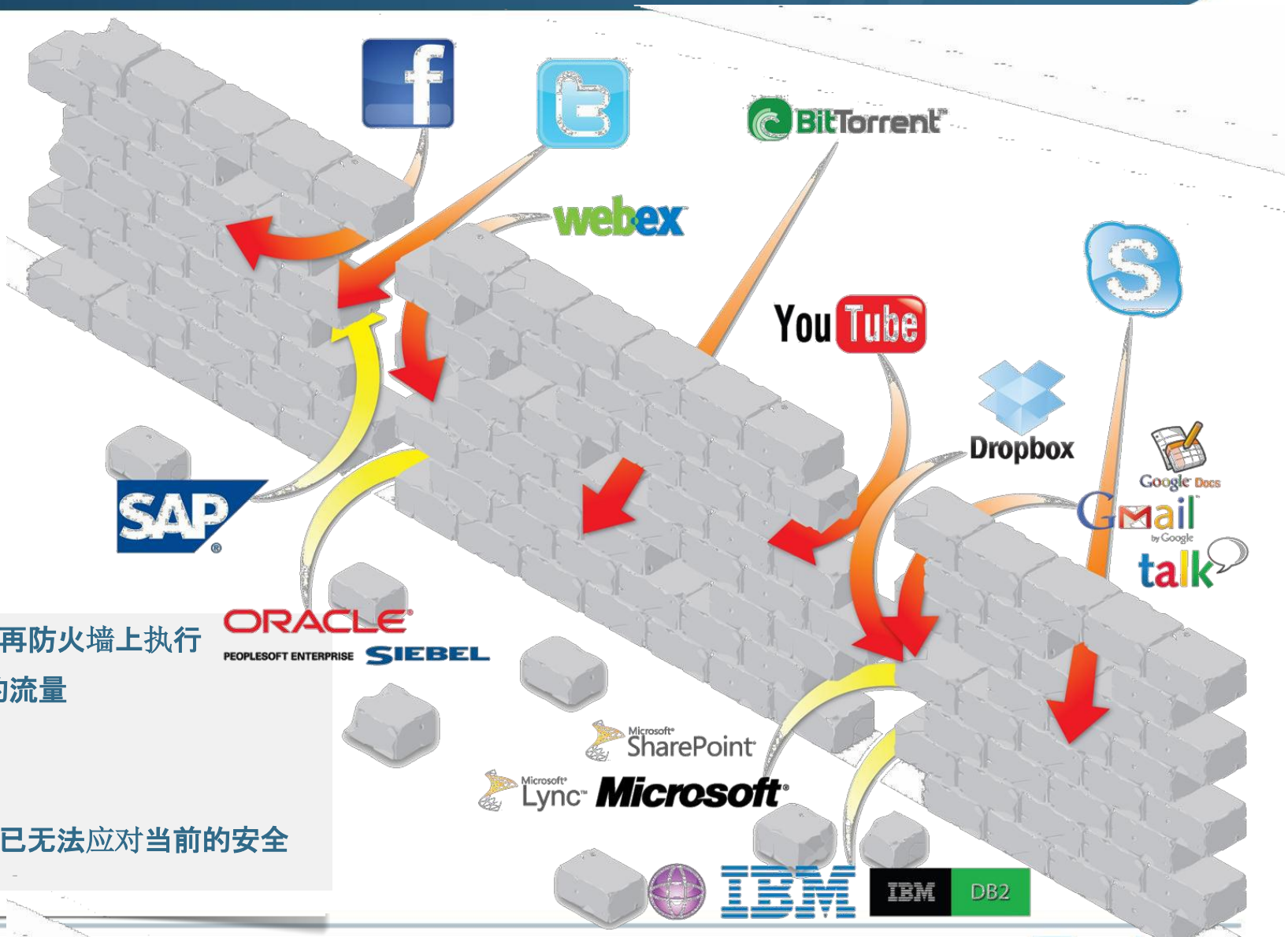
Revenue



Enterprise customers



应用在改变，防火墙却依旧...

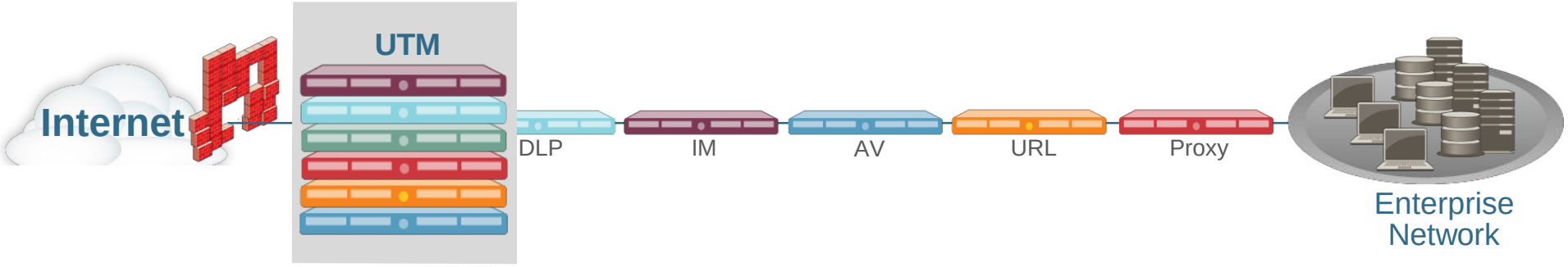


- 网络安全策略再防火墙上执行
  - 看到全部的流量
  - 定义边界
  - 访问控制
- 传统防火墙早已无法应对当前的安全需求

paloalto NETWORKS

传统解决方法并没有任何帮助

- 更多的设备并不能解决问题
- 防火墙“帮手”只能看到有限的流量
- 购买/维护成本较高并且较复杂
- 并没有解决应用控制、安全防护等问题



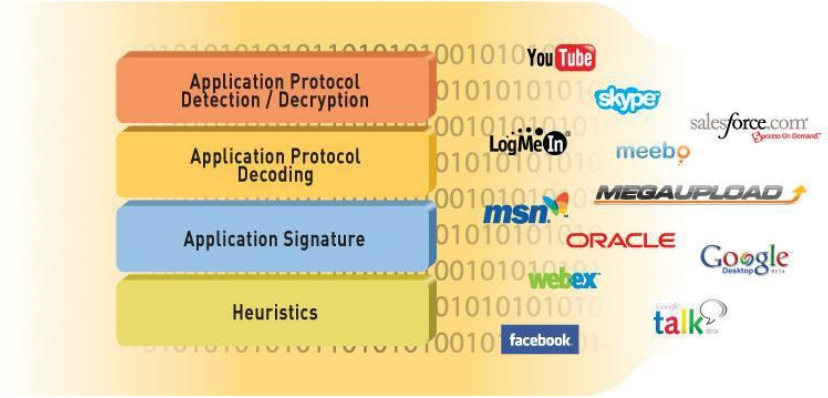
答案？ 让防火墙做自己的事情

1. 并非基于端口、协议，全流量应用识别，即便是逃逸流量或SSL加密流量
2. 并非基于IP、地理位置或设备，对最终用户进行识别和控制
3. 阻断已知和未知的潜在威胁流量
4. 灵活细腻的可视性及策略控制
5. 高性能、低延时，基于用途设计的专业硬件确保功能全开性能不下降

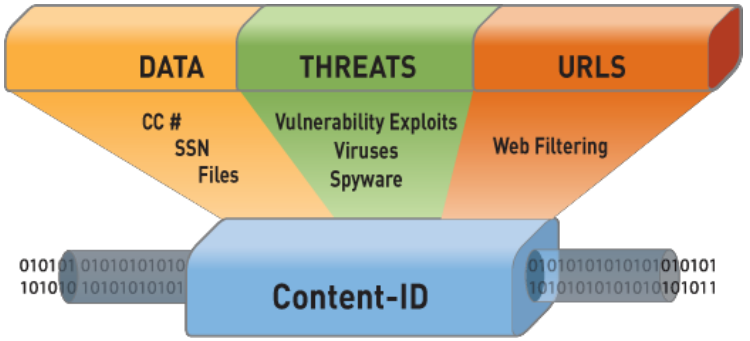
paloalto NETWORKS

Palo Alto Networks' Technology Makes This Possible

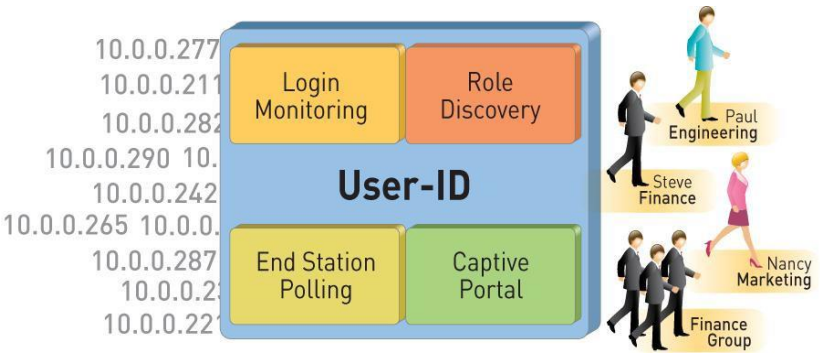
App-ID



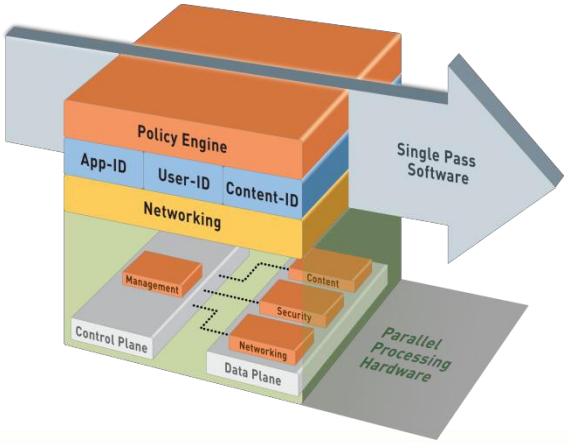
Content-ID



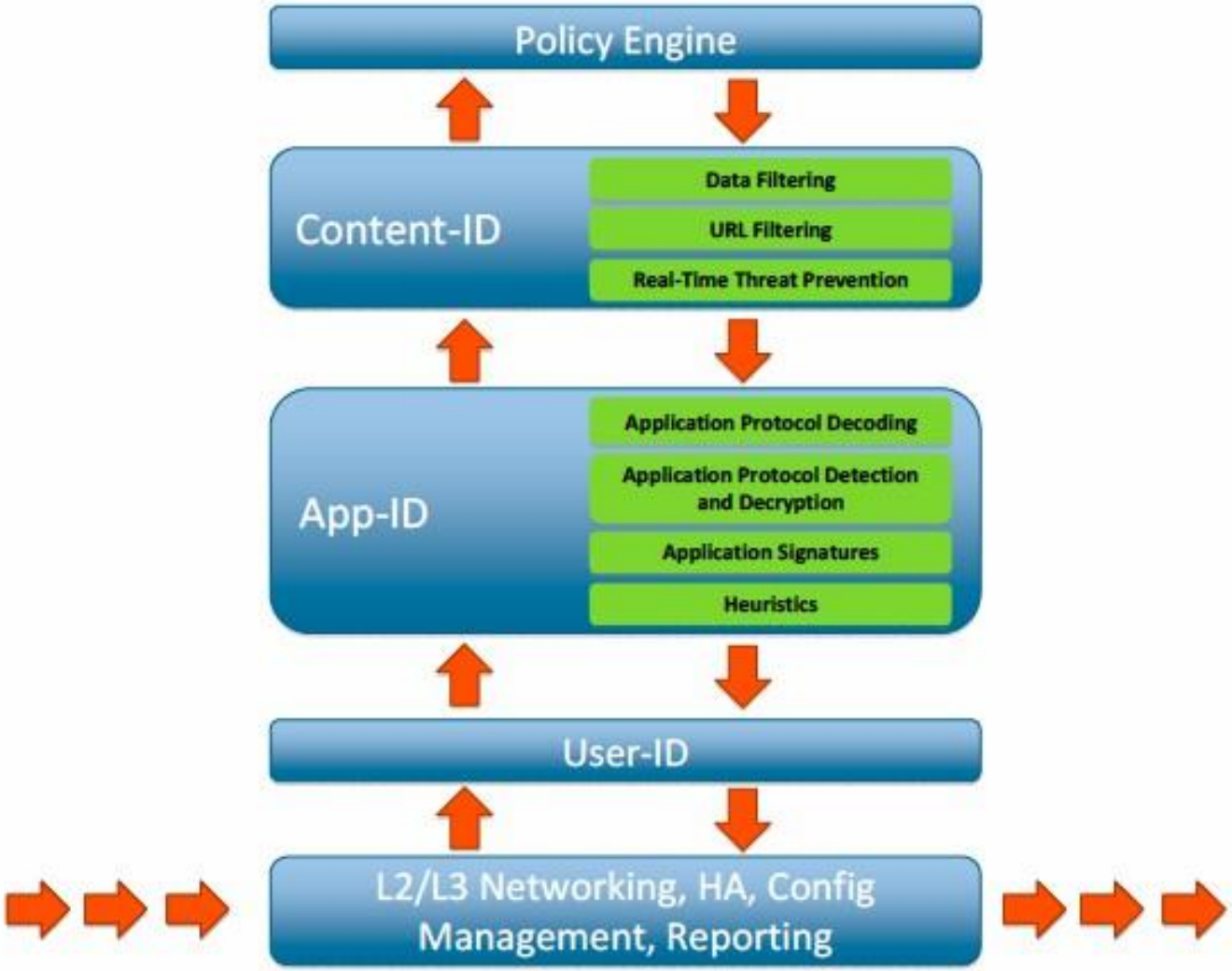
User-ID



SP3 Architecture

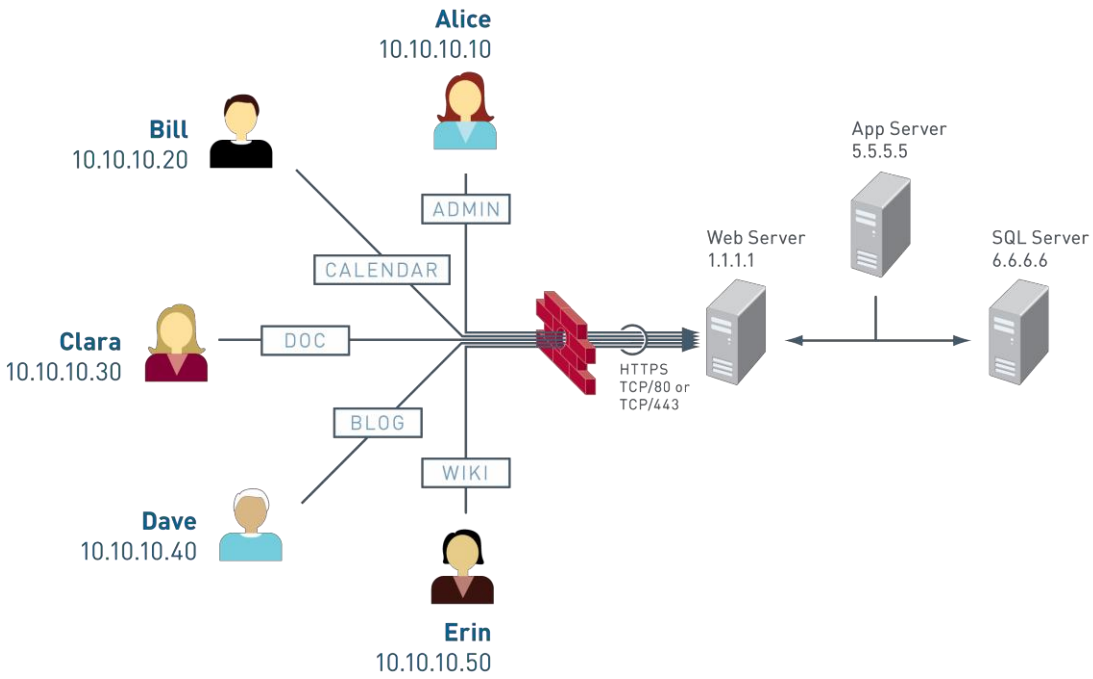


无需多次扫描，所有检查一次完成



SharePoint

- A Microsoft Collaboration Suite
- Based on IIS, SQL and ASP.net – represents risks
- Often deployed without IT help
- Uses port 80 or 443 for all functions – looks like web browsing

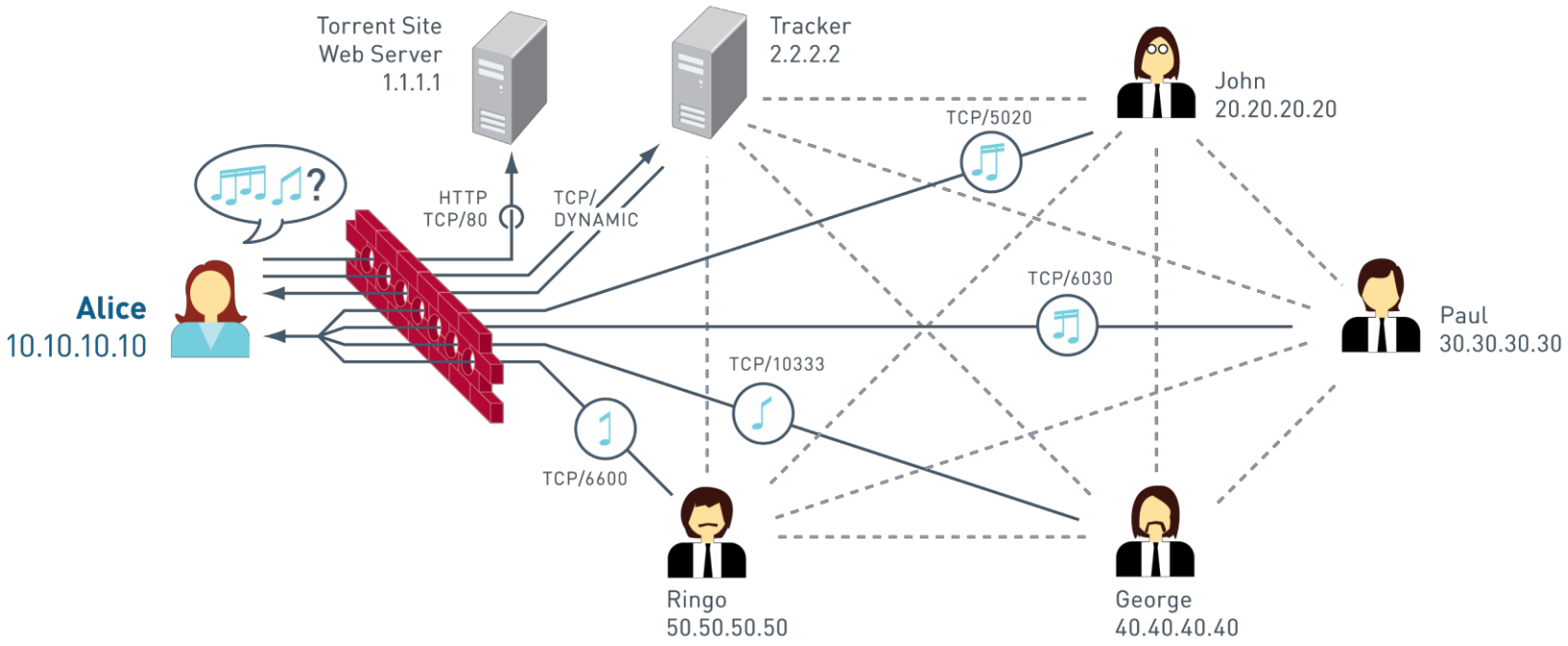


What they see: SharePoint

As seen by the network security infrastructure	
STATEFUL INSPECTION	TCP/80 (HTTP) or TCP/443 (HTTPS)
PROXY	Web session or SSL connection
URL FILTERING	Category: Unknown
IPS	Invisible
APP-ID	SharePoint SharePoint Administration SharePoint Documents SharePoint Wiki SharePoint Blogging SharePoint Calendar

BitTorrent

- Facilitates large file transfer - Binary downloads (business) or music (personal)
- Can hop from port to port, use port 80 – now usually encrypted (proprietary)

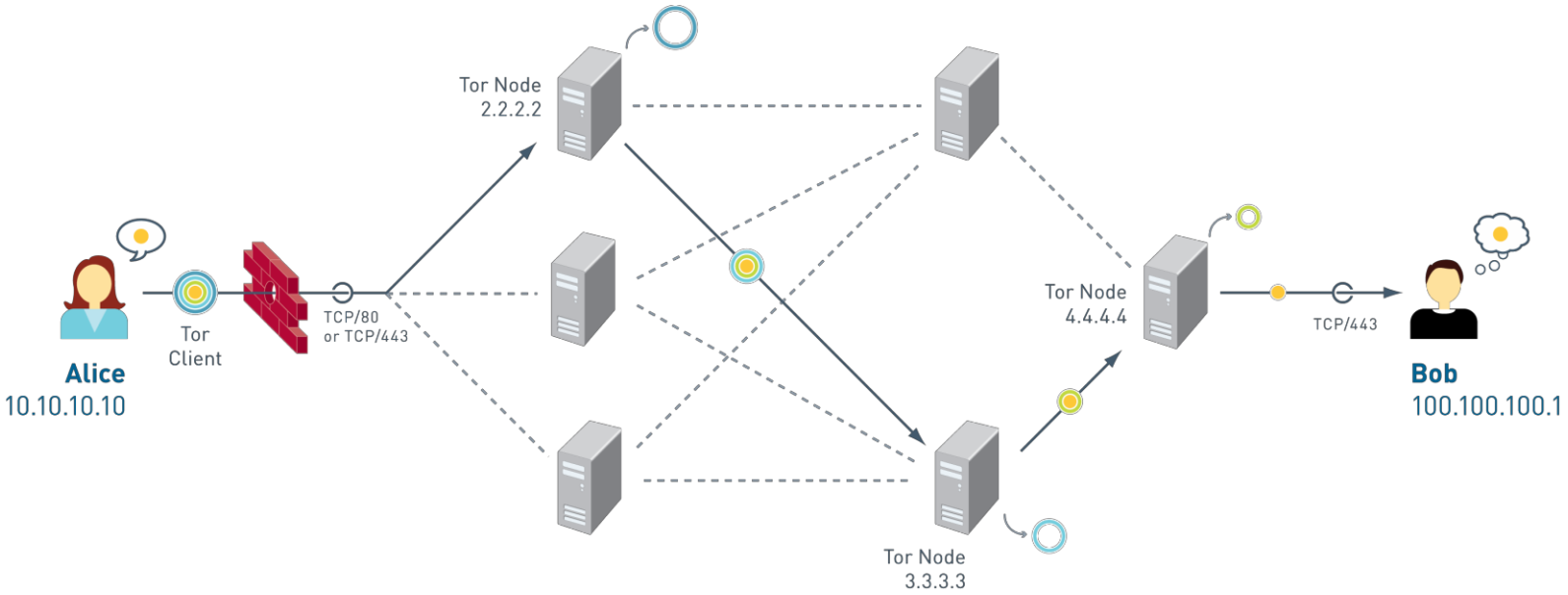


What they see: BitTorrent

As seen by the network security infrastructure	
STATEFUL INSPECTION	TCP/80 (HTTP) or TCP/443 (HTTPS) for torrent file download from web server Torrent file specified IP and TCP port for information about peers from tracker Multiple TCP sessions such as TCP/6600 for content download
PROXY	Some torrent file download URL Nothing for P2P traffic
URL FILTERING	Category: P2P (for well known torrent sites), Unknown (for other web servers)
IPS	May see as a threat and can only block it
APP-ID	BitTorrent

Tor

- Ensures message privacy through encryption and random paths
- Client server application that uses 80 or 443
- Most uses are non-business related

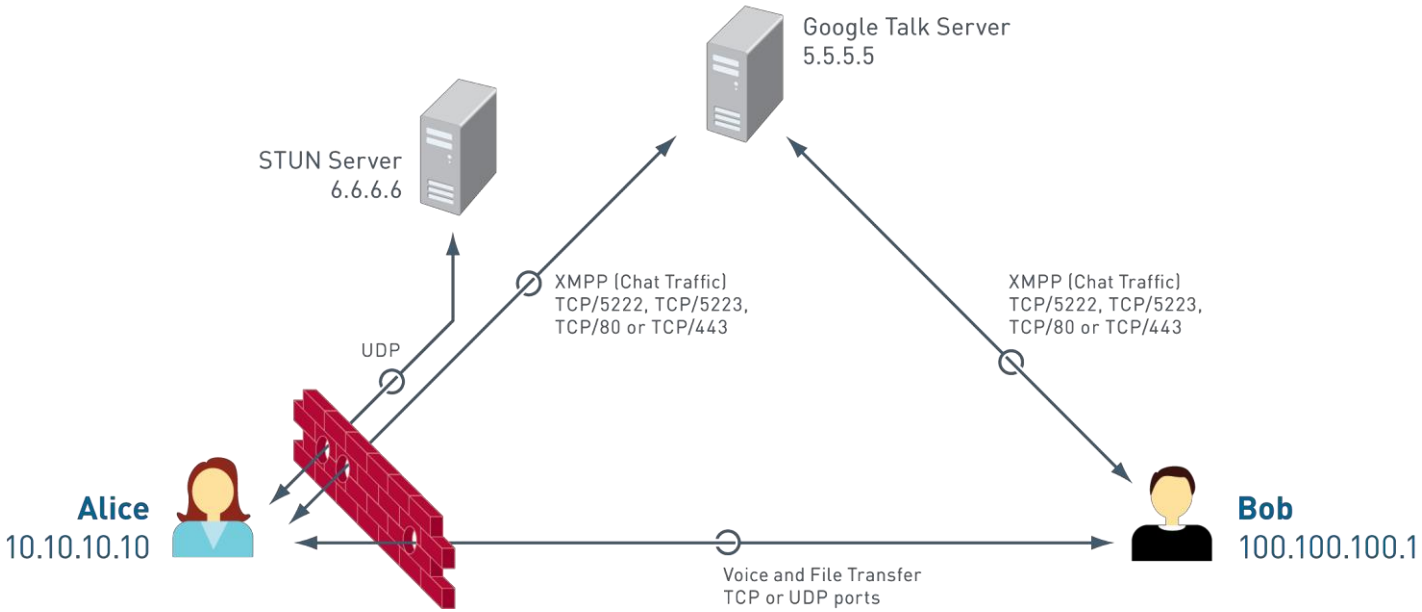


What they see: Tor

As seen by the network security infrastructure	
STATEFUL INSPECTION	TCP/80 (HTTP) or TCP/443 (HTTPS)
PROXY	Web session or SSL connection
URL FILTERING	Category: Unknown
IPS	Invisible or may see as a threat and can only block it
APP-ID	Tor

Google Talk

- IM, VoIP and file transfer application – both personal and business use
- Uses either dedicated ports or port 80 if blocked – looks like web browsing



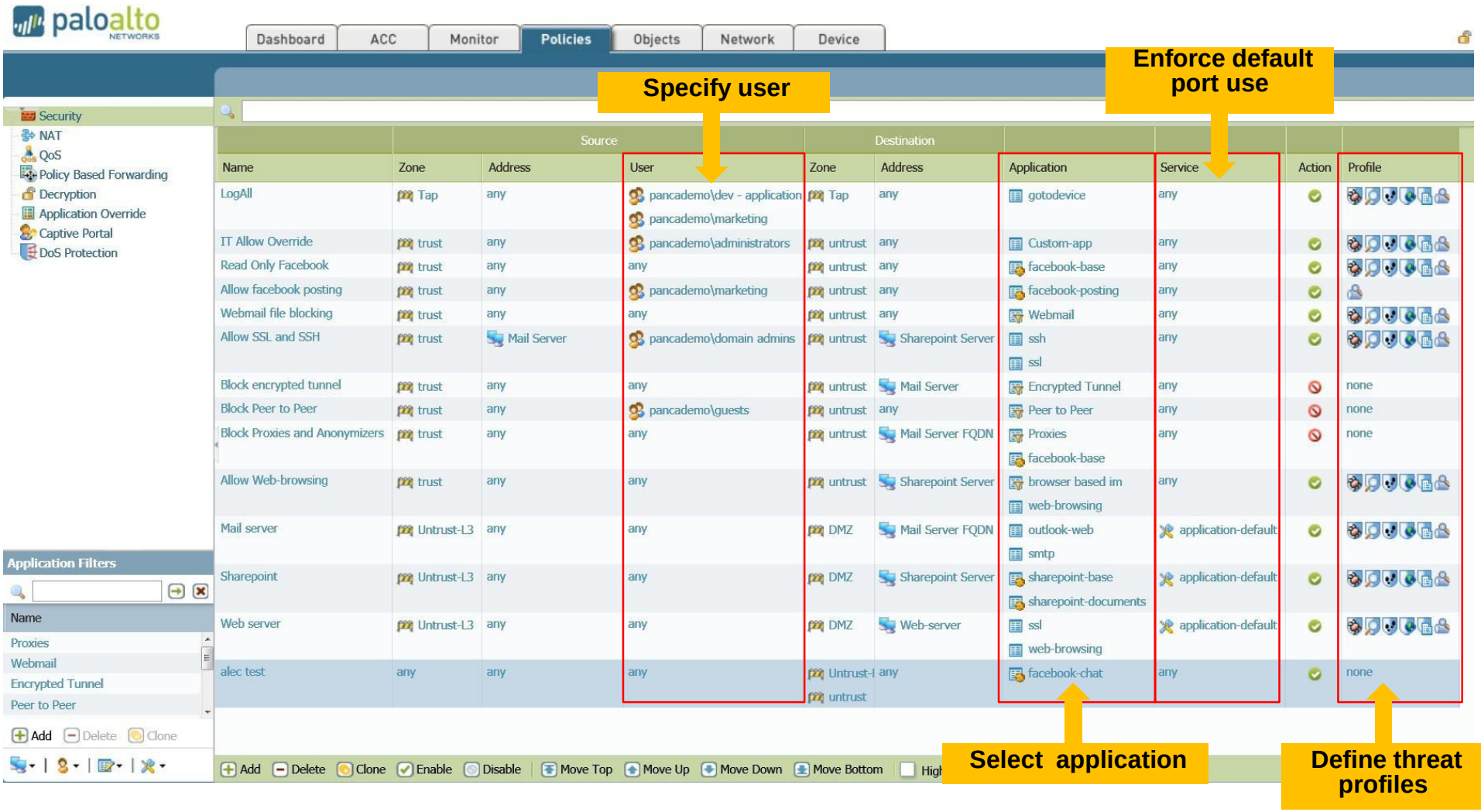
What they see: Google Talk

As seen by the network security infrastructure	
STATEFUL INSPECTION	TCP/5222 or TCP/5223 (Jabber) TCP/80 (HTTP) or TCP/443 (HTTPS) UDP port (for STUN) Dynamic TCP or UDP port (for media)
PROXY	Not handled by proxy
URL FILTERING	Category: Unknown
IPS	May see as a threat and can only block it
APP-ID	Google Talk Gtalk File Transfer Gtalk Voice Gbridge

App-ID仅仅是开始…

1. 鉴别和管理未知流量(unknown)
2. 通过应用识别有效的提高IPS效率
3. 基于App-ID例外防病毒扫描
4. 根据预定义的应用配置文件拦截策略(file blocking)
5. 基于应用转发可疑的可执行文件到云端确认

基于应用的统一策略



我们的研究团队在“发现” 威胁

- 我们的研究团队是“活跃的”
  - 许多的IPS厂家拥有巨大的研究团队来“写签名”
  - 我们的研究团队同样 “发现”零日攻击威胁

Discovering Microsoft Vulnerabilities in the past 4

Palo Alto Networks	McAfee	Tipping Point	Check Point	Sourcefire	Juniper	Cisco
20	7	7	3	1	0	0

Source: OSVDB; as of June 15th 2011

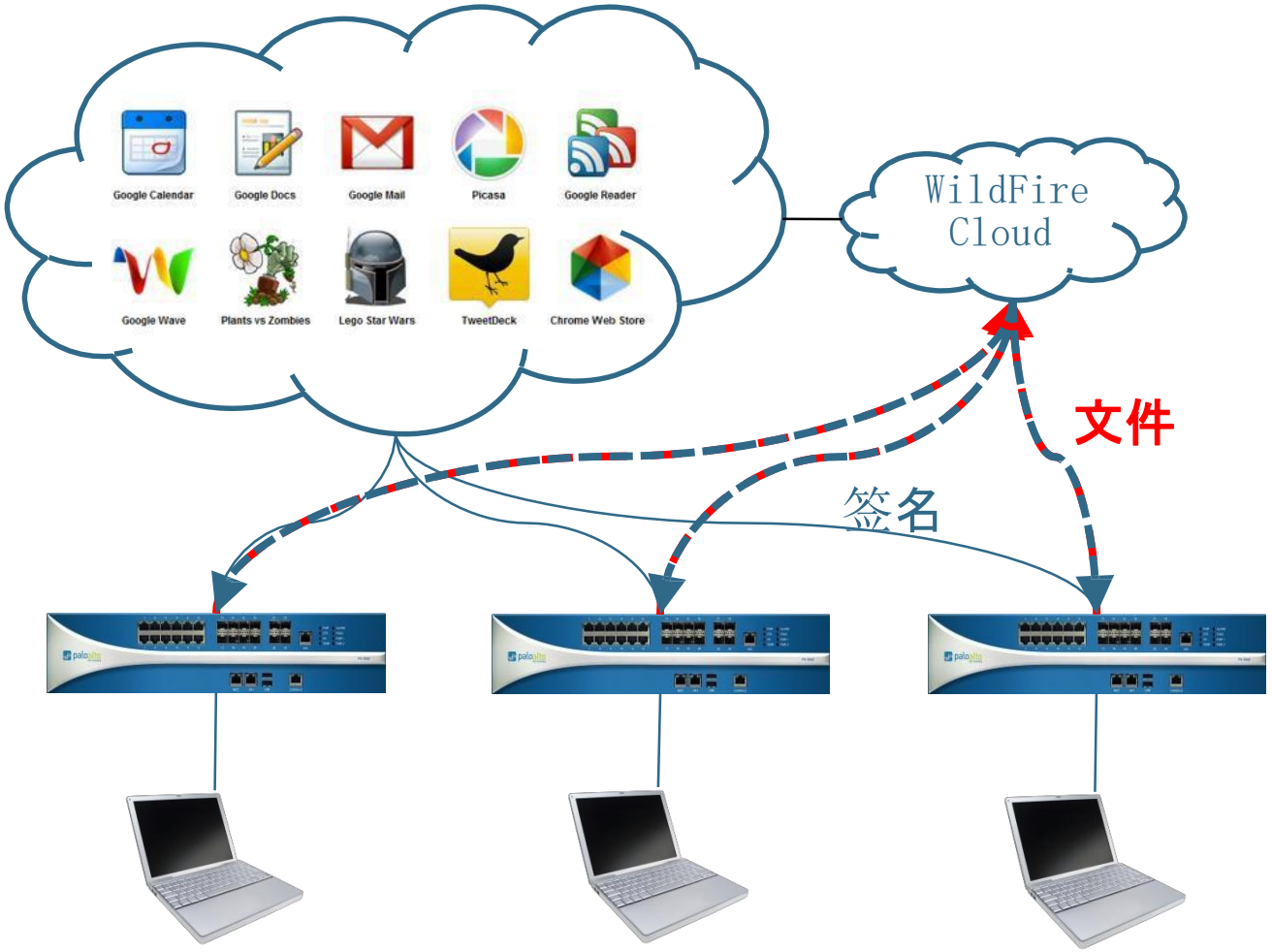
Discovering Adobe Vulnerabilities in the past 4 years

Palo Alto Networks	McAfee	Tipping Point	Check Point	Sourcefire	Juniper	Cisco
14	1	1	0	0	0	0

Source: OSVDB; as of August 15th 2011

Wildfire: 另一项Palo Alto Networks发明

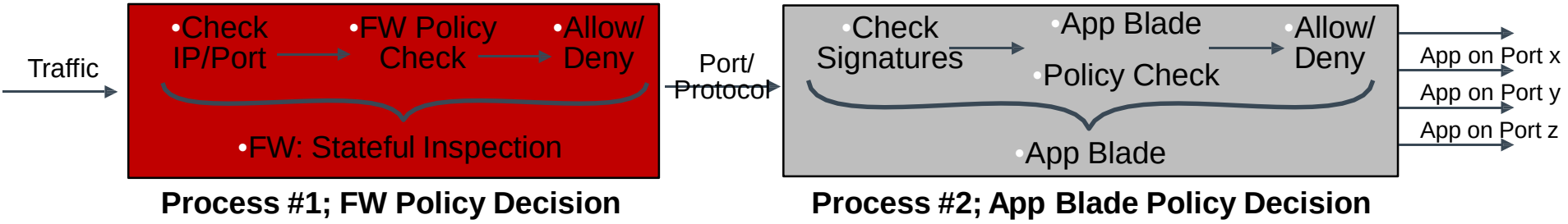
您可以自主决定选择上传什么文件

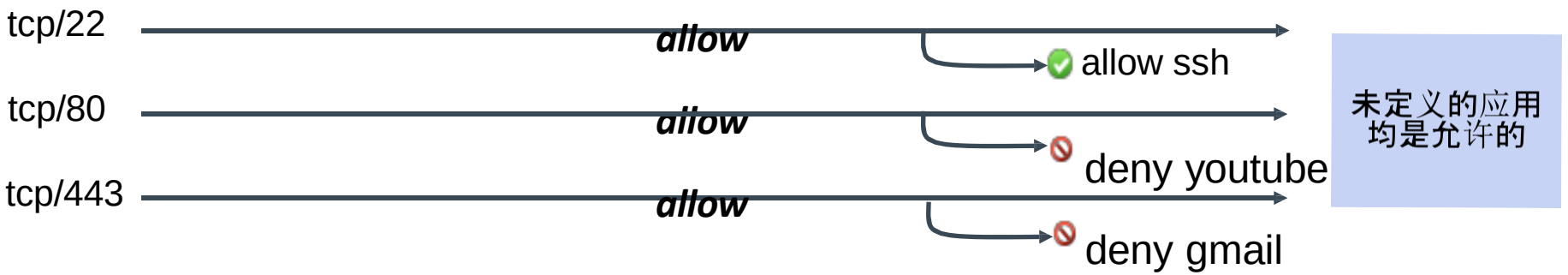


- CHECKPOINT

Check Point FW + App Blade = 2 Processes

两个完全独立的扫描引擎和策略执行





- **Check Point 不能做 ….**
  - 在允许的协议中阻断特定的应用
  - 使用非标准端口的应用(SSH, MySQL, Telnet)
  - 翻墙的应用
  - 策略优先级调整

FW and App 刀片依赖端口

- 防火墙和应用刀片均依赖端口
- 增加了运维负担，容易造成疑惑

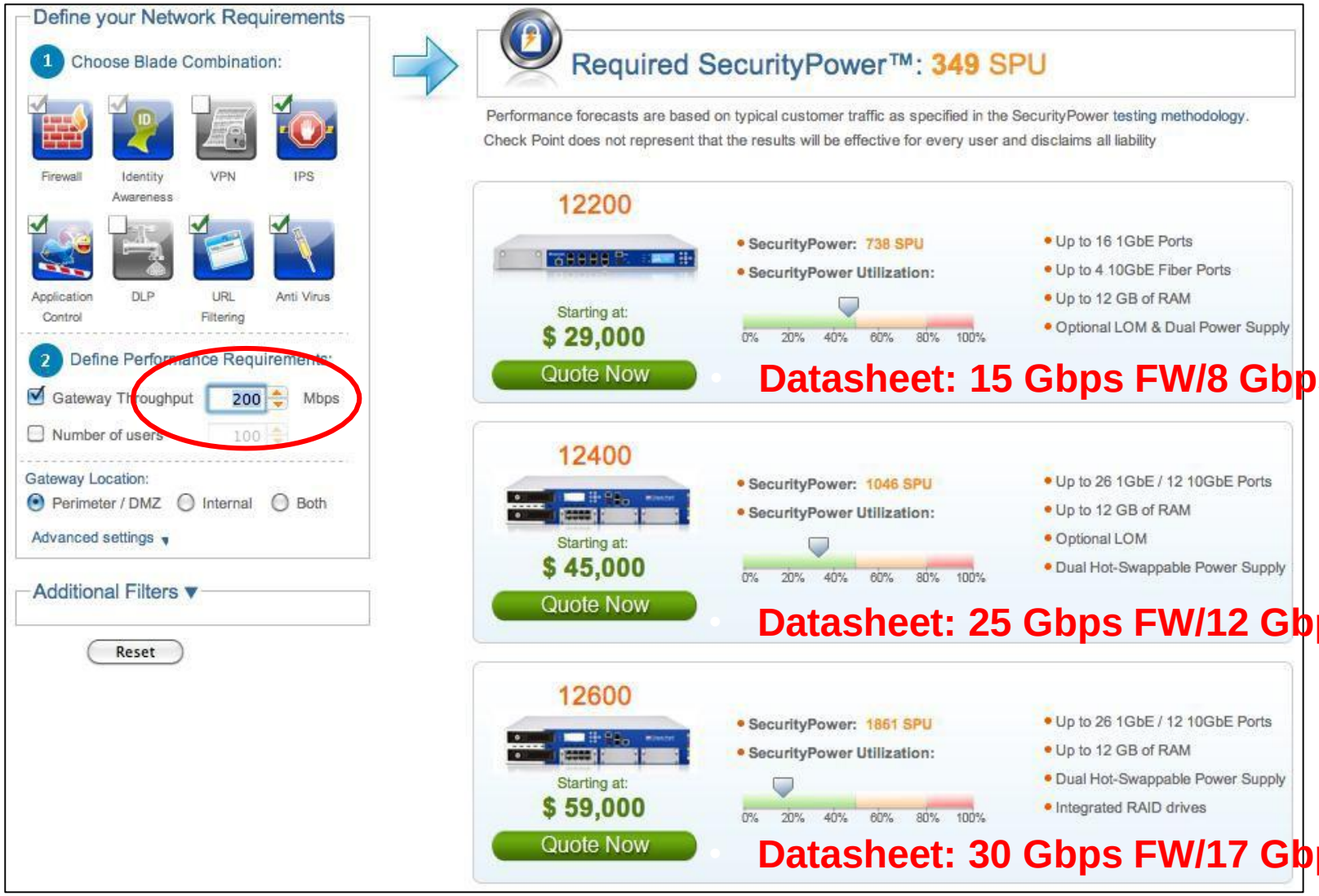
	Port	FW Logs	App Logs	IPS Logs
MySQL	3606 (Default)	Service = TCP,3606	MYSQL	Blank
MySQL	10000	Service = TCP,10000	Blank	Blank
MySQL	1645	Service = TCP datametrics (1645)	Blank	Blank
SMTP	25 (Default)	SMTP	Blank	Blank
SMTP	10000	Service = TCP,10000	Blank	Blank
SMTP	1645	Service = TCP datametrics (1645)	Blank	Blank
Telnet	23 (Default)	telnet	Blank	Blank
Telnet	10000	Service=TCP,10000	Blank	Blank
Telnet	1645	Service = TCP datametrics (1645)	Blank	Blank
SSH	22 (Default)	SSH	OpenSSH	Blank
SSH	10000	service tcp,10000	Blank	SSH detected
SSH	1645	service tcp,10000	Blank	SSH detected
HTTPS	443 (Default)	HTTPS	SSL	SSL detected
HTTPS	10000	Service = TCP,10000	Blank	SSL detected
HTTPS	1645	Service = TCP datametrics (1645)	Blank	SSL detected
HTTPS	25 (SMTP)	Service = TCP SMTP (25)	Blank	SSL detected

R75.10 - Firewall, log; Application Blade allow, log; IPS configured to detect and log.

Does Check Point Really Do What We Do?

	Palo Alto Networks	Check Point
使用应用识别技术作为主要的策略判定依据	Yes	No
使用单通道处理机制	Yes	No
使用一个页面进行统一的策略配置	Yes	No
从始至终进行应用识别	Yes	No
针对全端口、全流量执行应用识别	Yes	No
应用、威胁自定制	Yes	No
全功能启用后性能不下降	Yes	No
策略条目数量与性能无关	Yes	No
多AD域支持	Yes	No

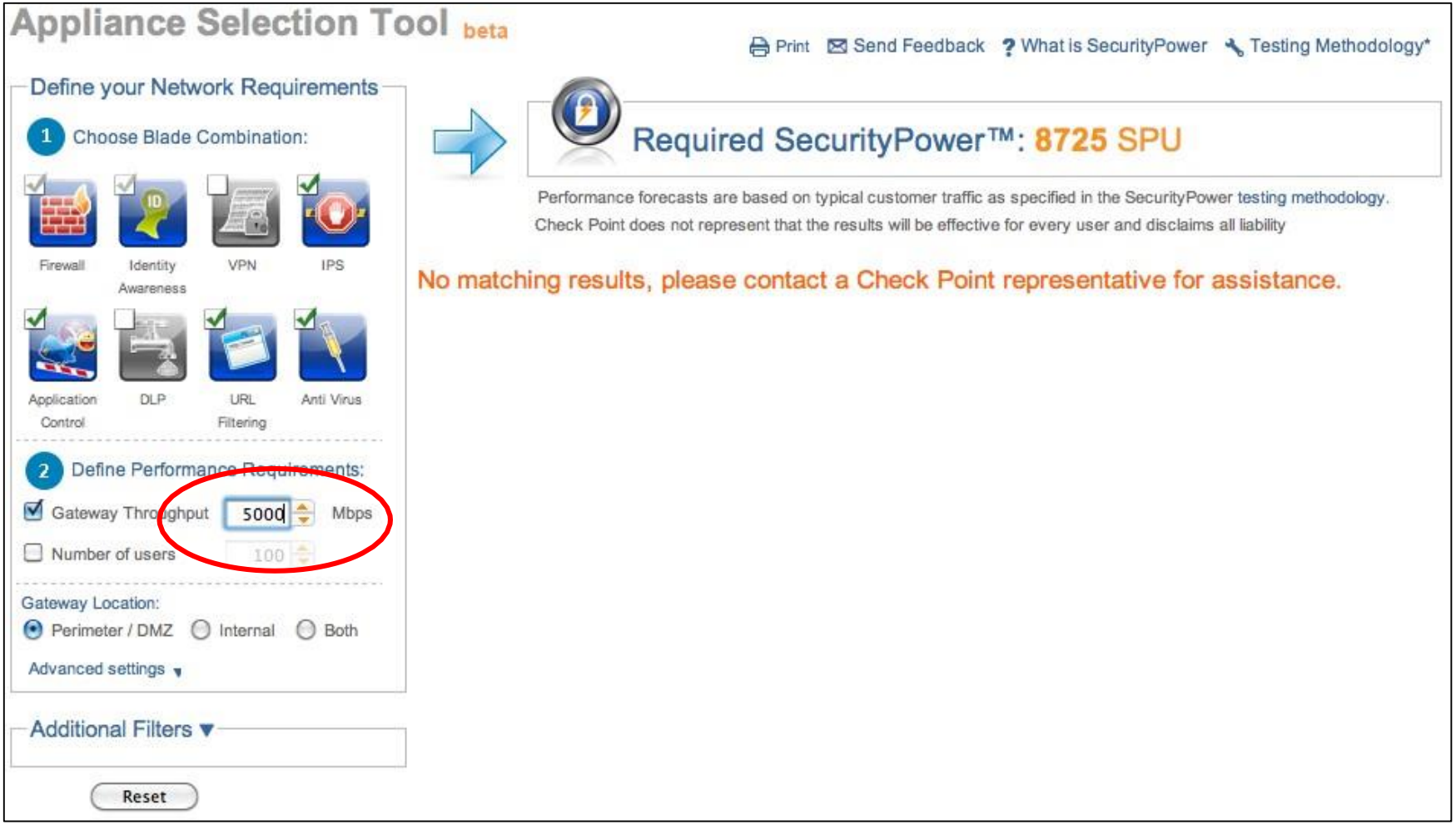
200 Mbps of Throughput: FW, IPS, AppCtrl, AV



500 Mbps of Throughput: FW, IPS, AppCtrl, AV

2 Gbps of Throughput: FW, IPS, AppCtrl, AV

5 Gbps of Throughput: FW, IPS, AppCtrl, AV



Check Point: We do what they do…


paloalto
NETWORKS
the network security company™