

Palo Alto Networks 技术对比



Agenda

- CHECKPOINT

Palo Alto Networks 概况

NYSE SYMBOL: PANW

Corporate highlights

Founded in 2005; first customer shipment in 2007

Safely enabling applications

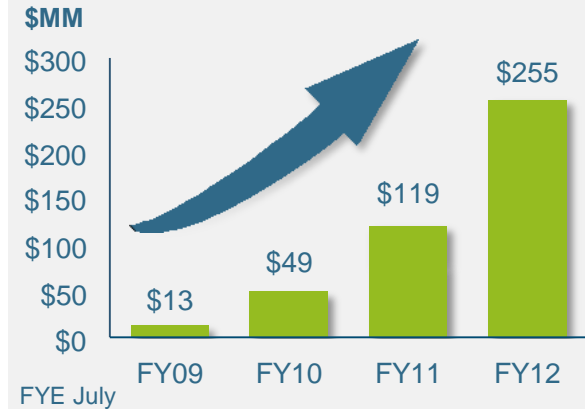
Able to address all network security needs

Exceptional ability to support global customers

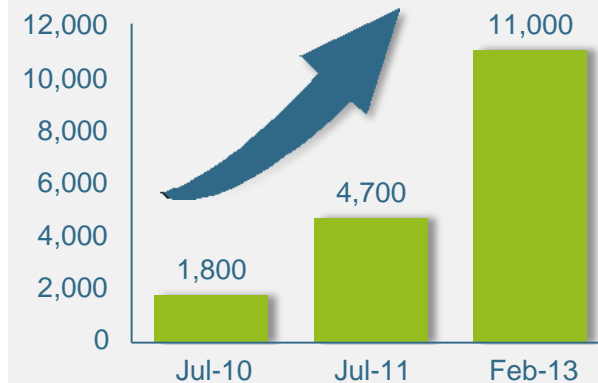
Experienced technology and management team

1,000+ employees globally

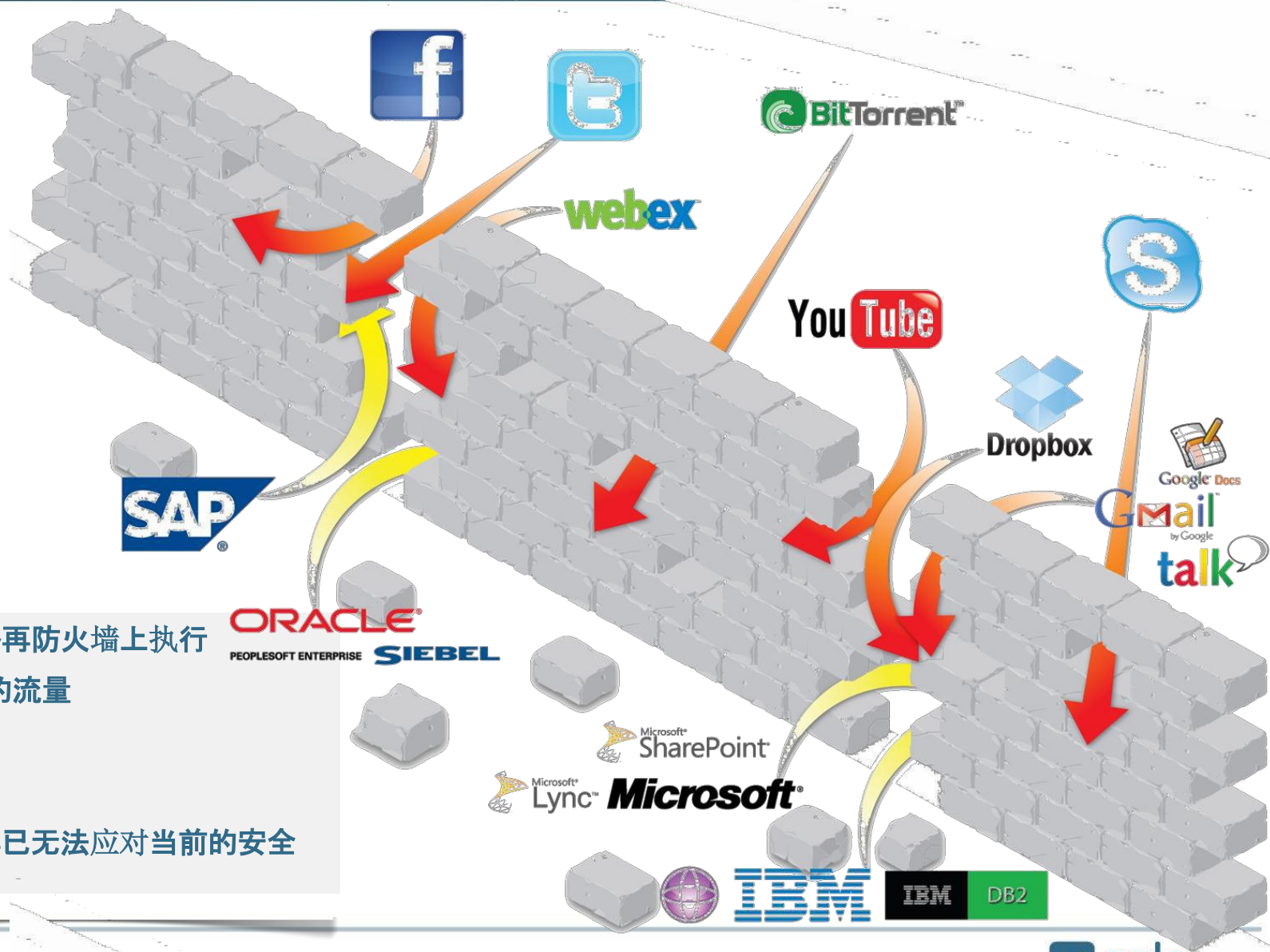
Revenue



Enterprise customers



应用在改变，防火墙却依旧...



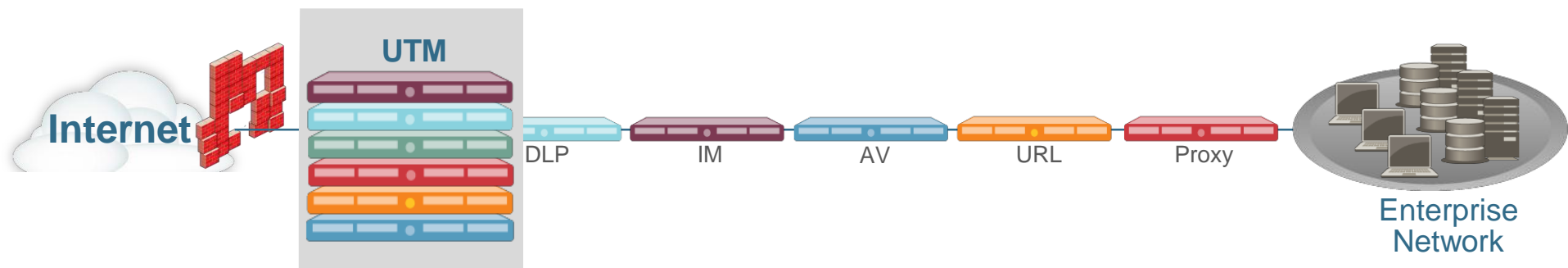
网络安全策略再防火墙上执行

- 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

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



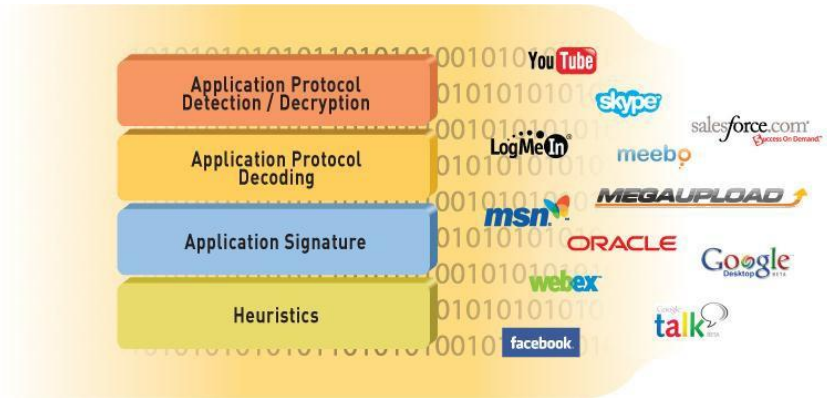
答案？ 让防火墙做自己的事情

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

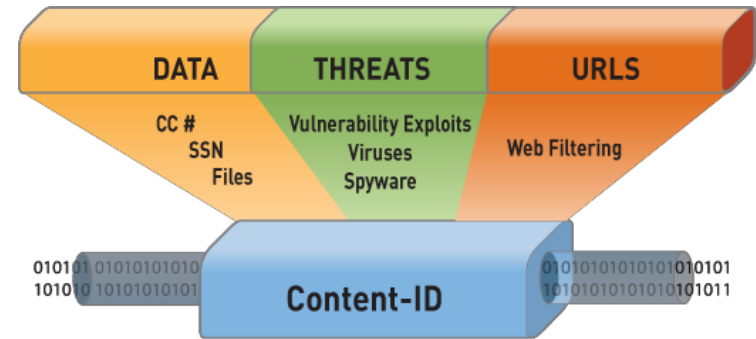


Palo Alto Networks' Technology Makes This Possible

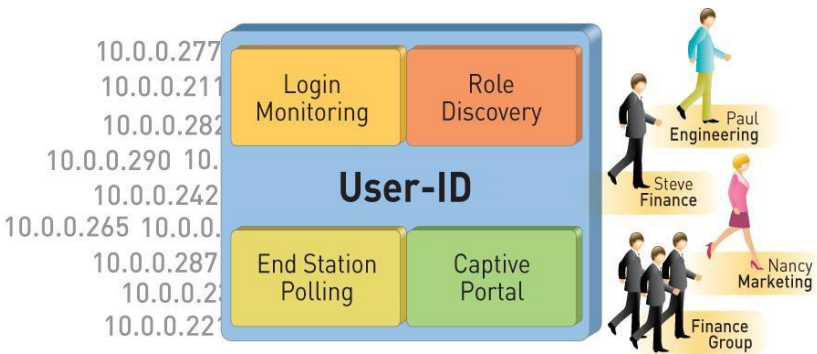
App-ID



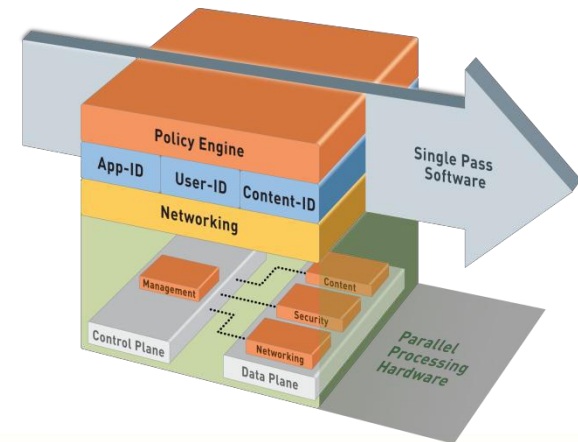
Content-ID



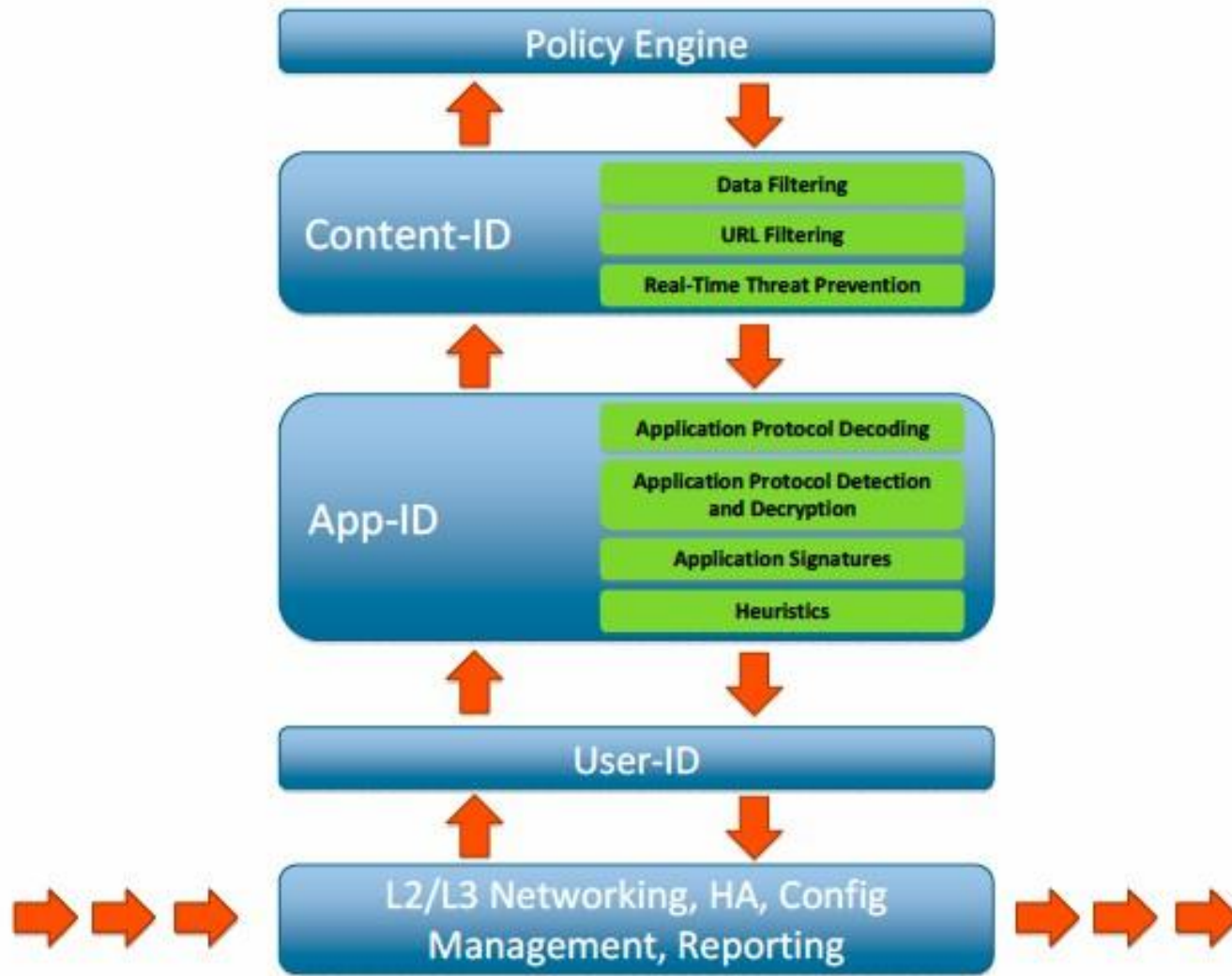
User-ID



SP3 Architecture

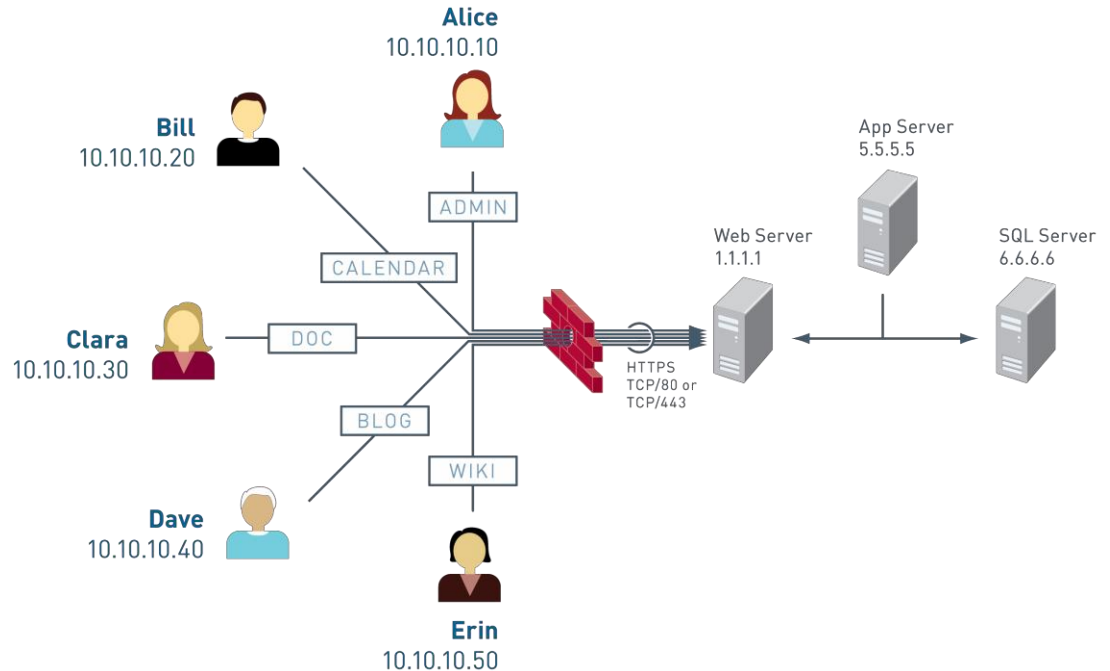


无需多次扫描，所有检查一次完成



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



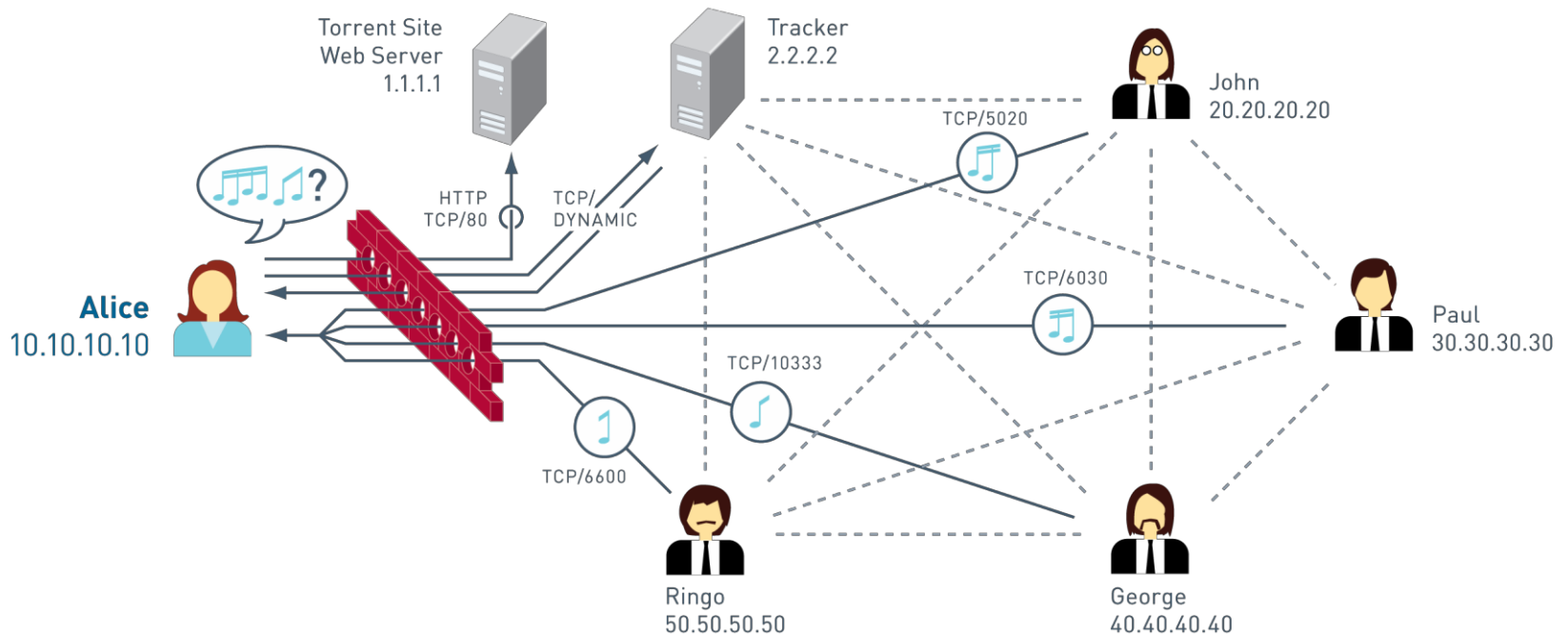
What they see: SharePoint

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)



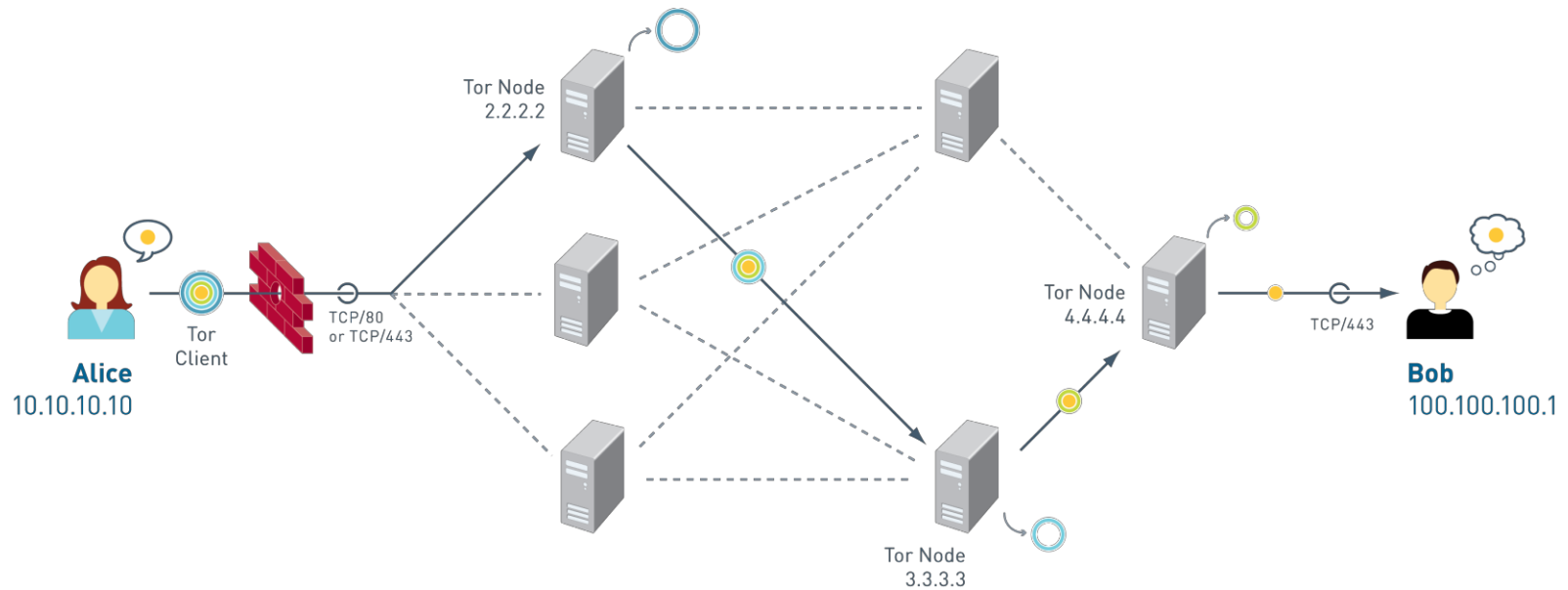
What they see: BitTorrent

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



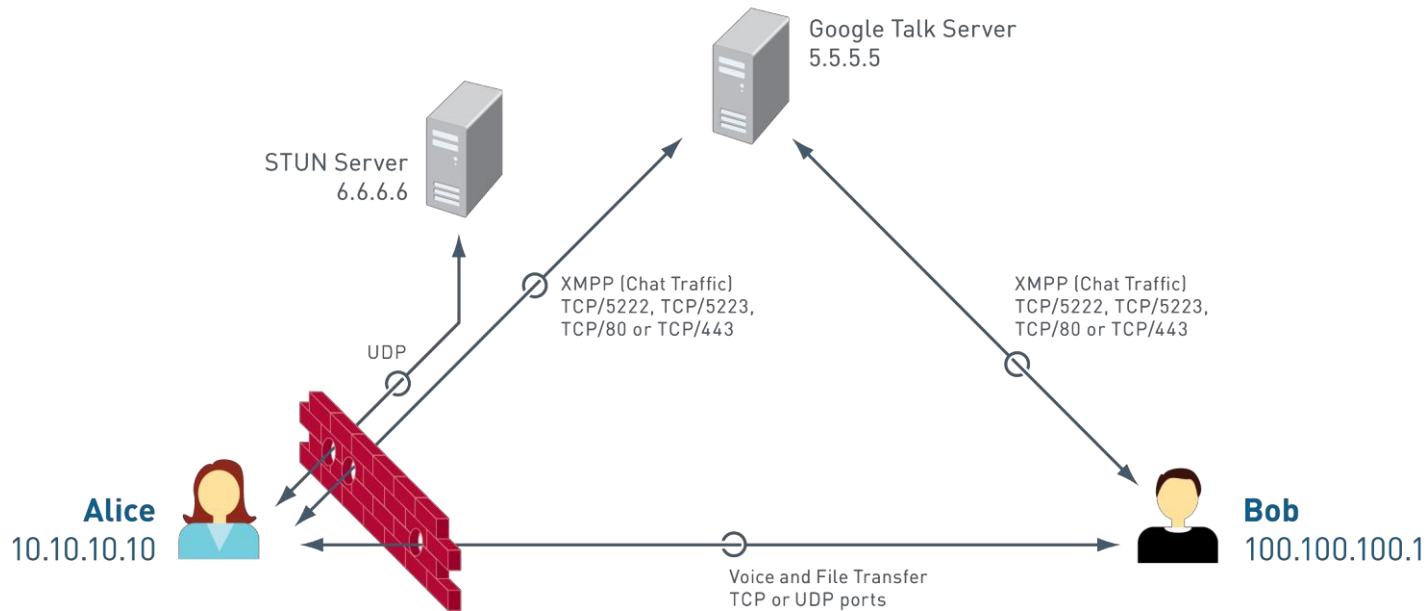
What they see: Tor

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

The screenshot shows the Palo Alto Networks Security Policy configuration page. The interface includes a navigation menu on the left with options like Security, NAT, QoS, Policy Based Forwarding, Decryption, Application Override, Captive Portal, and DoS Protection. The main area displays a table of policies with columns for Name, Zone, Address, User, Zone, Address, Application, Service, Action, and Profile. Annotations in yellow boxes point to specific fields: 'Specify user' points to the User column, 'Enforce default port use' points to the Service column, 'Select application' points to the Application column, and 'Define threat profiles' points to the Profile column. The 'Application Filters' sidebar on the left shows a list of applications including Proxies, Webmail, Encrypted Tunnel, and Peer to Peer.

Name	Zone	Address	User	Zone	Address	Application	Service	Action	Profile
LogAll	Tap	any	pancademo\dev - application pancademo\marketing	Tap	any	gotodevice	any	✓	[Threat Profiles]
IT Allow Override	trust	any	pancademo\administrators	untrust	any	Custom-app	any	✓	[Threat Profiles]
Read Only Facebook	trust	any	any	untrust	any	facebook-base	any	✓	[Threat Profiles]
Allow facebook posting	trust	any	pancademo\marketing	untrust	any	facebook-posting	any	✓	[Threat Profiles]
Webmail file blocking	trust	any	any	untrust	any	Webmail	any	✓	[Threat Profiles]
Allow SSL and SSH	trust	Mail Server	pancademo\domain admins	untrust	Sharepoint Server	ssh ssl	any	✓	[Threat Profiles]
Block encrypted tunnel	trust	any	any	untrust	Mail Server	Encrypted Tunnel	any	✗	none
Block Peer to Peer	trust	any	pancademo\guests	untrust	any	Peer to Peer	any	✗	none
Block Proxies and Anonymizers	trust	any	any	untrust	Mail Server FQDN	Proxies	any	✗	none
Allow Web-browsing	trust	any	any	untrust	Sharepoint Server	facebook-base browser based im web-browsing	any	✓	[Threat Profiles]
Mail server	Untrust-L3	any	any	DMZ	Mail Server FQDN	outlook-web smtp	application-default	✓	[Threat Profiles]
Sharepoint	Untrust-L3	any	any	DMZ	Sharepoint Server	sharepoint-base sharepoint-documents	application-default	✓	[Threat Profiles]
Web server	Untrust-L3	any	any	DMZ	Web-server	ssl web-browsing	application-default	✓	[Threat Profiles]
alec test	any	any	any	Untrust-L3	any	facebook-chat	any	✓	none

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



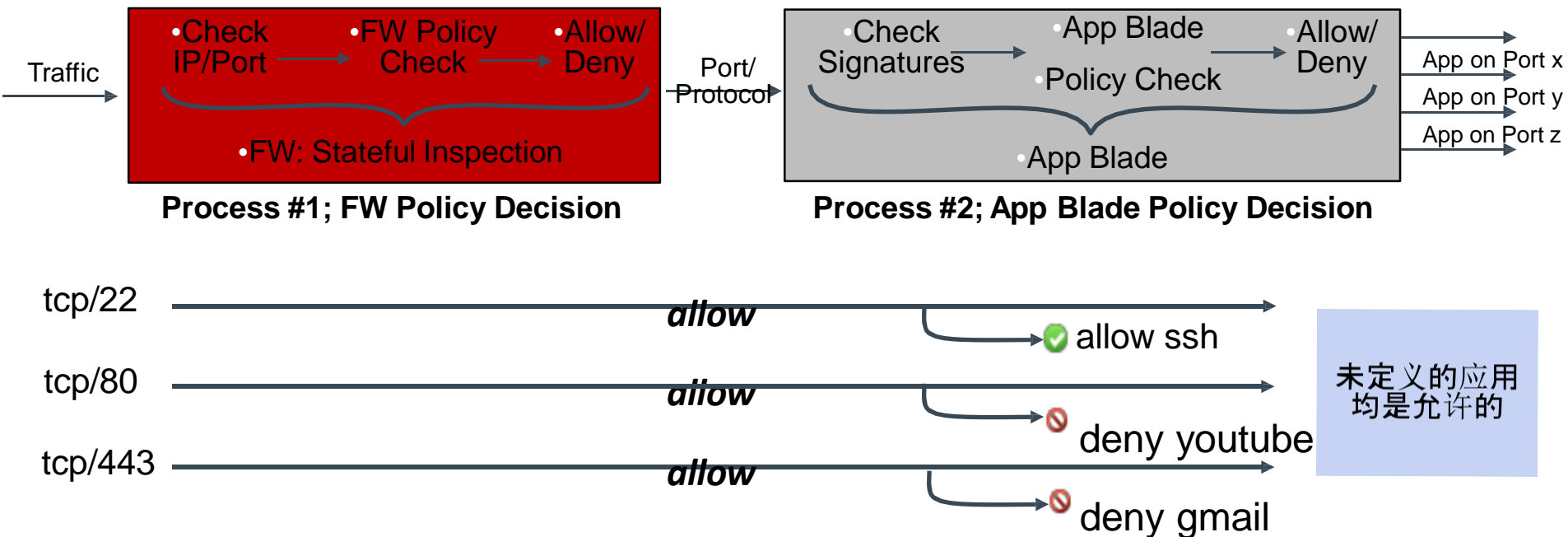
您可以自主决定选择上传什么文件



- 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、威胁自定义	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

Define your Network Requirements

1 Choose Blade Combination:

- Firewall
- Identity Awareness
- VPN
- IPS
- Application Control
- DLP
- URL Filtering
- Anti Virus

2 Define Performance Requirements:

Gateway Throughput **200** Mbps

Number of users: 100

Gateway Location:
 Perimeter / DMZ Internal Both

Advanced settings ▾

Additional Filters ▾

Reset

Required SecurityPower™: 349 SPU

Performance forecasts are based on typical customer traffic as specified in the SecurityPower testing methodology. Check Point does not represent that the results will be effective for every user and disclaims all liability.

12200

Starting at: **\$ 29,000**

Quote Now

• SecurityPower: 738 SPU

• SecurityPower Utilization: 

- Up to 16 1GbE Ports
- Up to 4 10GbE Fiber Ports
- Up to 12 GB of RAM
- Optional LOM & Dual Power Supply

Datasheet: 15 Gbps FW/8 Gbps IPS

12400

Starting at: **\$ 45,000**

Quote Now

• SecurityPower: 1046 SPU

• SecurityPower Utilization: 

- Up to 26 1GbE / 12 10GbE Ports
- Up to 12 GB of RAM
- Optional LOM
- Dual Hot-Swappable Power Supply


Datasheet: 25 Gbps FW/12 Gbps IPS

12600

Starting at: **\$ 59,000**

Quote Now

• SecurityPower: 1861 SPU

• SecurityPower Utilization: 

- Up to 26 1GbE / 12 10GbE Ports
- Up to 12 GB of RAM
- Dual Hot-Swappable Power Supply
- Integrated RAID drives

Datasheet: 30 Gbps FW/17 Gbps IPS

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

Appliance Selection Tool beta

[Print](#) [Send Feedback](#) [? What is SecurityPower](#) [Testing Methodology*](#)

Define your Network Requirements

1 Choose Blade Combination:

- Firewall
- Identity Awareness
- VPN
- IPS
- Application Control
- DLP
- URL Filtering
- Anti Virus

2 Define Performance Requirements:

Gateway Throughput Mbps

Number of users

Gateway Location:
 Perimeter / DMZ Internal Both


Advanced settings ▾

Additional Filters ▾

Required SecurityPower™: 728 SPU

Performance forecasts are based on typical customer traffic as specified in the SecurityPower testing methodology. Check Point does not represent that the results will be effective for every user and disclaims all liability.


12600



Starting at: **\$ 59,000**

SecurityPower: 1861 SPU


SecurityPower Utilization:



- Up to 26 1GbE / 12 10GbE Ports
- Up to 12 GB of RAM
- Dual Hot-Swappable Power Supply
- Integrated RAID drives

Datasheet: 30 Gbps FW/17 Gbps IPS

21400



Starting at: **\$ 115,000**

SecurityPower: 2900 SPU

SecurityPower Utilization:



- Up to 37 1GbE/ 12 10GbE Ports
- Up to 24 GB of RAM
- Dual Hot-Swappable Power Supply
- Integrated RAID drives

Datasheet: 50 Gbps FW/21 Gbps IPS

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

Appliance Selection Tool beta

[Print](#) [Send Feedback](#) [? What is SecurityPower](#) [Testing Methodology*](#)

Define your Network Requirements

1 Choose Blade Combination:

Firewall Identity Awareness VPN IPS

Application Control DLP URL Filtering Anti Virus

2 Define Performance Requirements:

Gateway Throughput Mbps

Number of users

Gateway Location:
 Perimeter / DMZ Internal Both

Advanced settings ▾

Additional Filters ▾

[Reset](#)

Required SecurityPower™: 3490 SPU

Performance forecasts are based on typical customer traffic as specified in the SecurityPower testing methodology. Check Point does not represent that the results will be effective for every user and disclaims all liability

61000

Starting at:
\$ 195,000

[Quote Now](#)

SecurityPower: 14600 SPU

SecurityPower Utilization:

0% 20% 40% 60% 80% 100%

- Up to 26 1GbE Ports
- 1U Form Factor
- 3 Expansion Slots
- Management for 2 GWs

Datasheet: 200 Gbps FW/110 Gbps IP

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

Appliance Selection Tool beta

[Print](#) [Send Feedback](#) [? What is SecurityPower](#) [Testing Methodology*](#)

Define your Network Requirements

1 Choose Blade Combination:

<input checked="" type="checkbox"/> Firewall	<input checked="" type="checkbox"/> Identity Awareness	<input type="checkbox"/> VPN	<input checked="" type="checkbox"/> IPS
<input checked="" type="checkbox"/> Application Control	<input type="checkbox"/> DLP	<input checked="" type="checkbox"/> URL Filtering	<input checked="" type="checkbox"/> Anti Virus

2 Define Performance Requirements:

Gateway Throughput Mbps

Number of users

Gateway Location:
 Perimeter / DMZ Internal Both

Advanced settings ▾

Additional Filters ▾

Reset

 **Required SecurityPower™: 8725 SPU**

Performance forecasts are based on typical customer traffic as specified in the SecurityPower testing methodology. Check Point does not represent that the results will be effective for every user and disclaims all liability.

No matching results, please contact a Check Point representative for assistance.

Check Point: We do what they do...





the network security company™