Palo alto Networks
安全解决方案-ASE培训

金志勇

zhjin@paloaltonetworks.com

paloalto NETWORKS

the network security company™

关于 Palo Alto Networks

- 专业的网络安全公司
  - 世界级团队积累丰富的网络和安全经验
- 2005年成立，NYSE上市公司 PANW
- 下一代企业安全平台
  - 创新性的支持: App-ID™, User-ID, Content-ID, GlobalProtect™, WildFire™
  - 恢复防火墙在企业网安全架构的核心位置
  - 野火威胁检测云安全、端点检测安全
- 全球客户：20000+在100多个国家的客户，50% Fortune 100公司使用我们产品

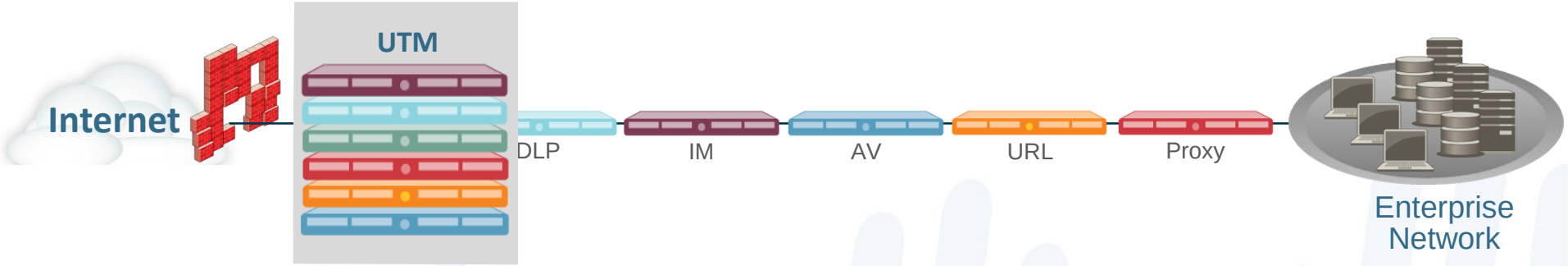
paloalto NETWORKS

众多第三方机构得出相同的结论

- Gartner 企业级网络防火墙魔力象限
  - Palo Alto Networks领先于市场
- Forrester IPS 市场表现
  - 强大的IPS解决方案，展示了有效的整合
- 《网络世界》的评测
  - 至今最严苛的NGFW测试，验证其持续的性能表现
- NSS 测试
  - IPS: Palo Alto Networks NGFW面对竞争厂商的独立IPS设备测试，获得 NSS Recommended
  - Firewall: 传统基于端口的防火墙测试；NSS 推荐
  - NGFW: FW + IPS测试；NSS 推荐

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**



paloalto NETWORKS

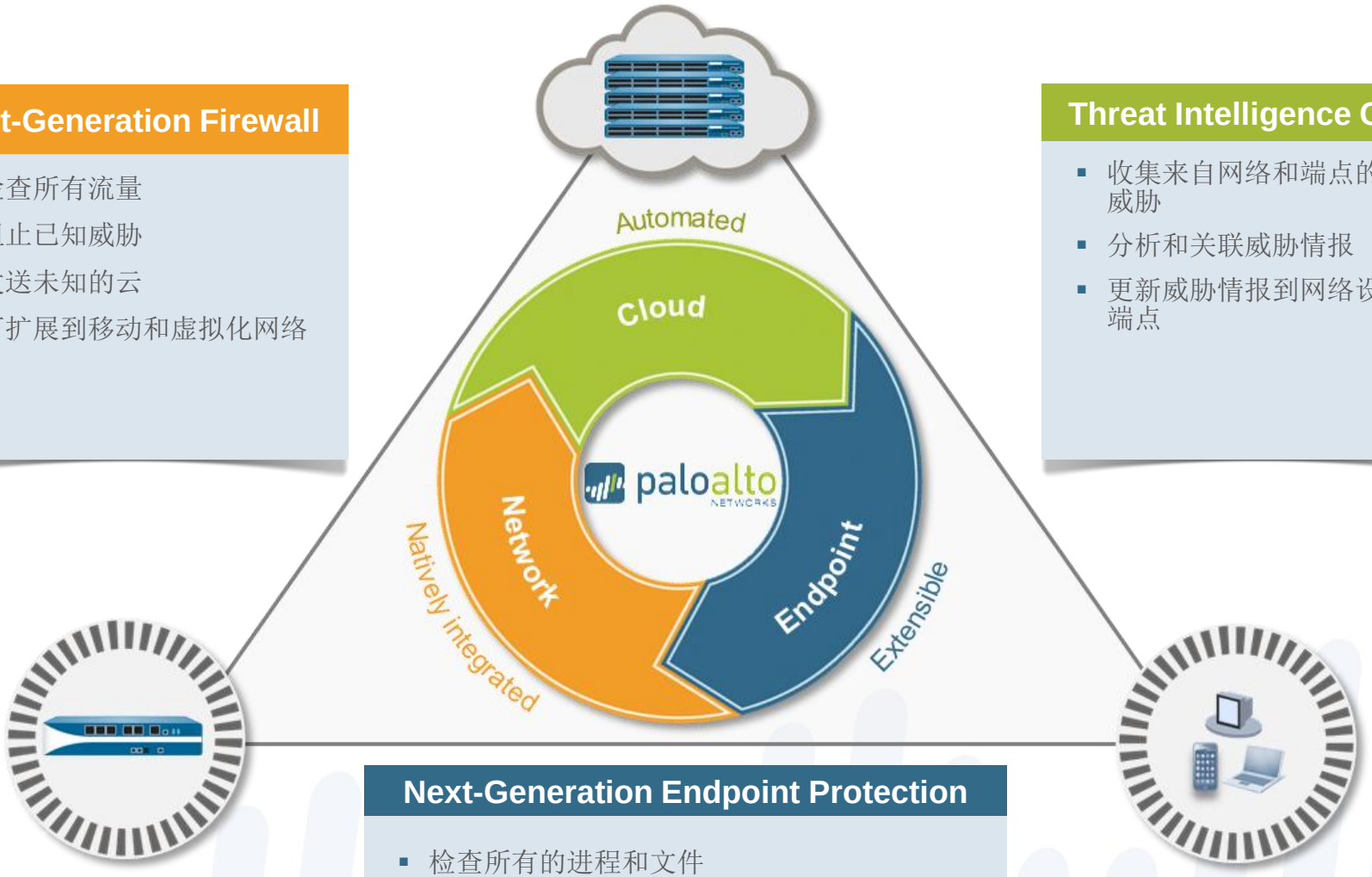
Palo Alto Networks 下一代企业安全平台

Next-Generation Firewall

- 检查所有流量
- 阻止已知威胁
- 发送未知的云
- 可扩展到移动和虚拟化网络

Threat Intelligence Cloud

- 收集来自网络和端点的潜在威胁
- 分析和关联威胁情报
- 更新威胁情报到网络设备和端点



Next-Generation Endpoint Protection

- 检查所有的进程和文件
- 防止所有已知和未知的攻击
- 云集成，从而防止已知和未知的恶意软件

平台组成特点？

独特的集成性	闭环架构	集中管理
多种功能的操作 内部集成系统	自动发布新的 ‘未知’自威胁 即刻的防御	单一的架构管理 和功能模块之间 紧密关联互动

paloalto networks.

What we do

Palo Alto Networks 拥有唯一 企业安全平台

能够 安全的启用所有的应用
通过 颗粒化的用户控制
并 阻止已知和未知的网络威胁
对于 *使用任何网络的 任何终端上的* 所有用户

有别于 传统的防火墙, **UTM's**, *和*
不同的独立点式安全产品

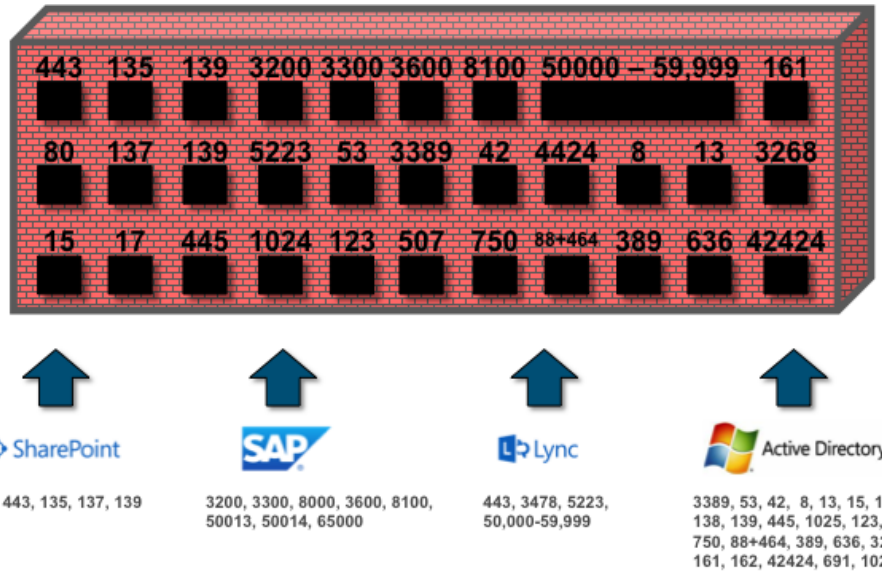
他们 提供有限的控制对于某些应用程序和

某些网络威胁

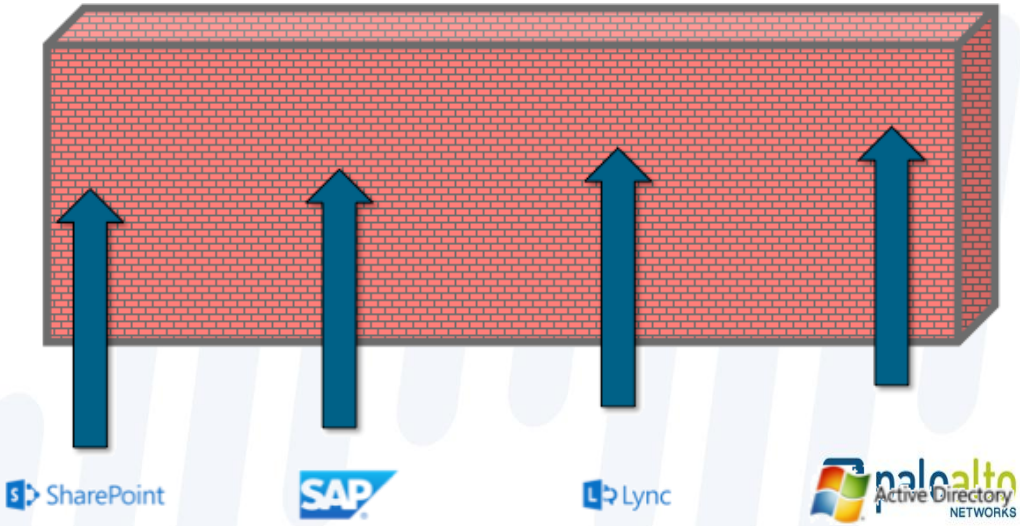
主要议题

- 颠覆传统的下一代防火墙设计
- 针对现代威胁的防护
- 重要场景（数据中心，BYOD）
- 其他议题

什么样的安全防护才是您想要的？



网络任何位置保持高标准的应用安全水平



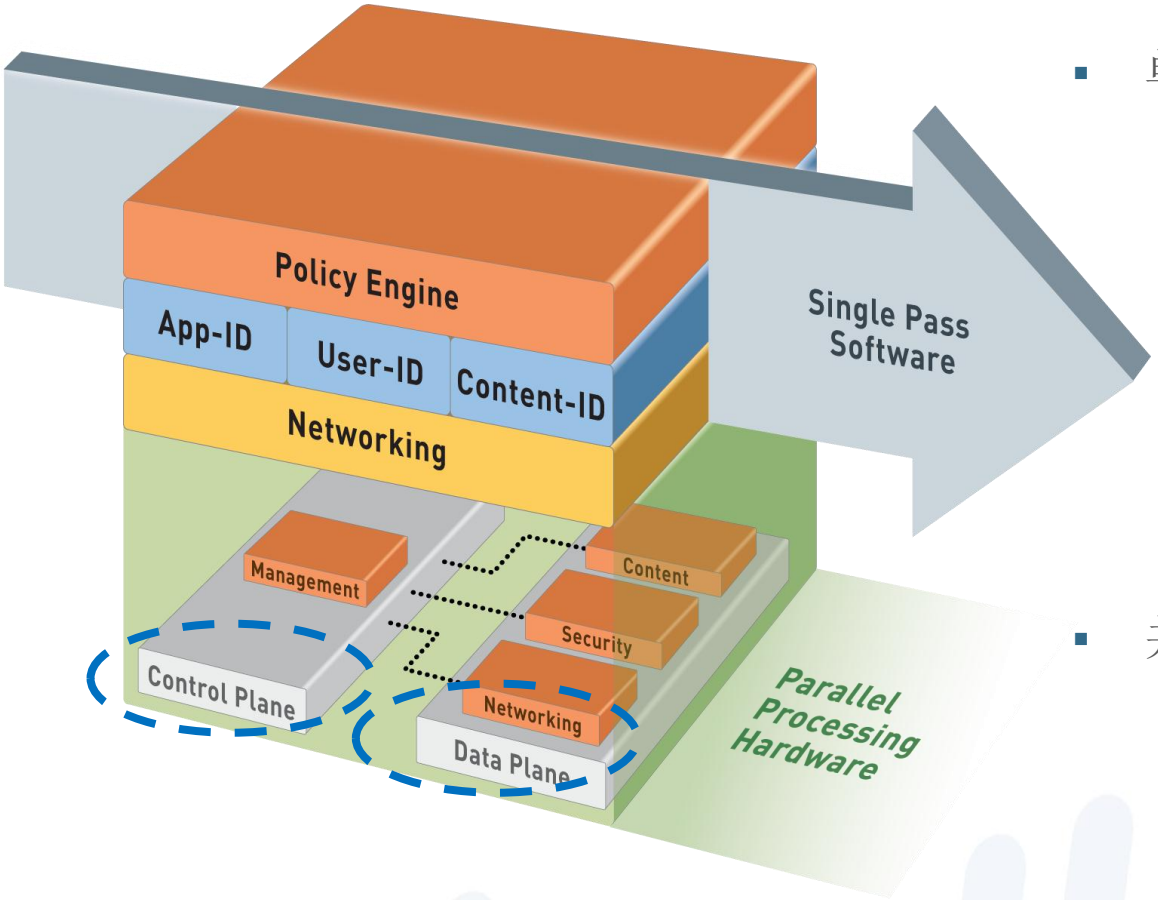
颠覆传统的
下一代防火墙设计

重新定义了“防火墙”

paloalto NETWORKS

the network security company™

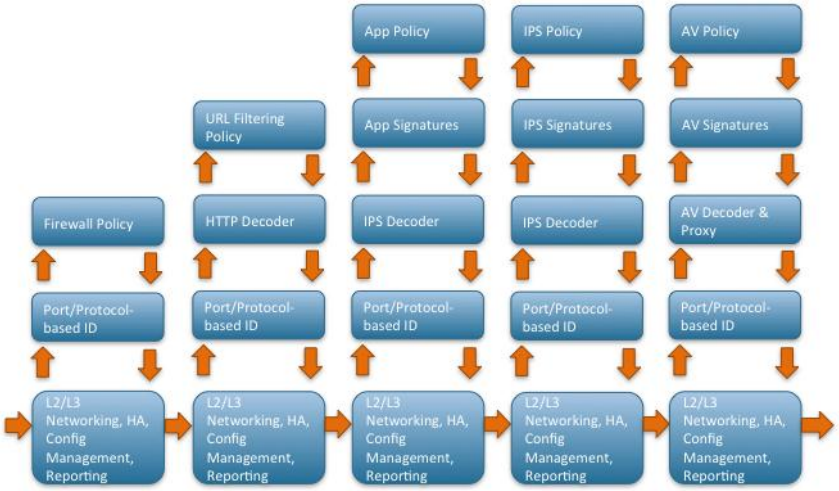
单通道&并行处理™ (SP3) 系统架构-保障高性能低延时



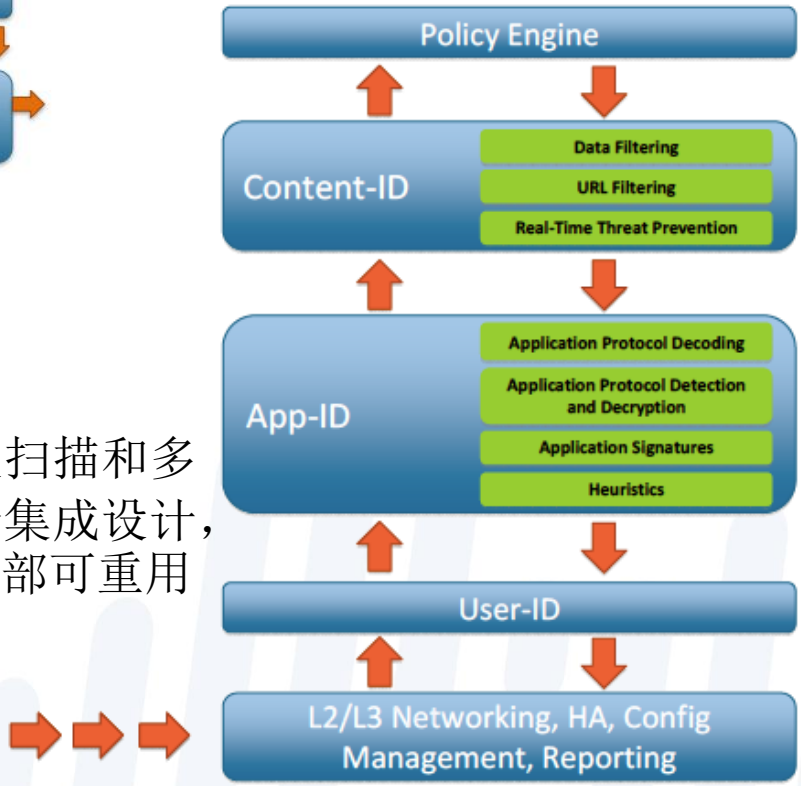
- 单通道处理
  - 数据包一次操作
    - 流量分类 （应用识别)
    - 用户/组 对应
    - 内容扫描 – 病毒，间谍软件，等威胁
  - 而且仅仅执行单一策略
- 并行处理技术
  - 特定功能的并行处理硬件引擎
  - 独立的数据/控制平面

高达120Gbps(App-ID)，微秒级低延时

采用与传统厂商不同的扫描方式

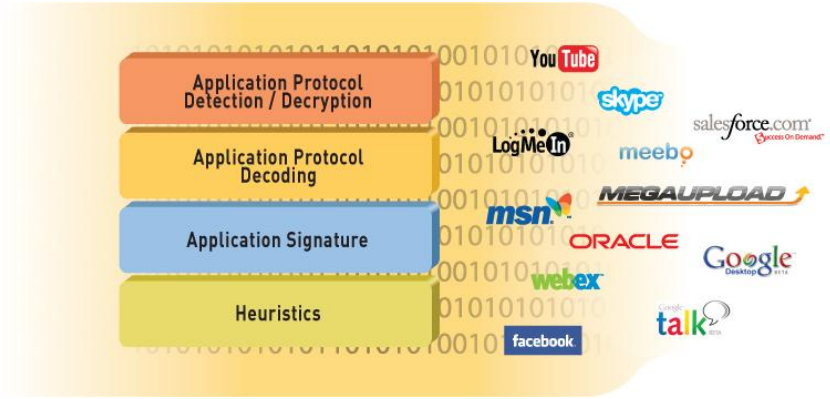


不同于UTM多次重复扫描和多重日志记录，采取全集成设计，识别的应用信息在内部可重用

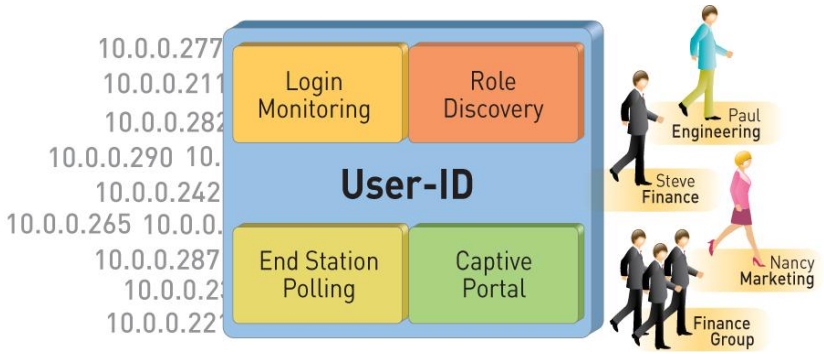


NGFW最核心的差别
识别技术—提升现有安全

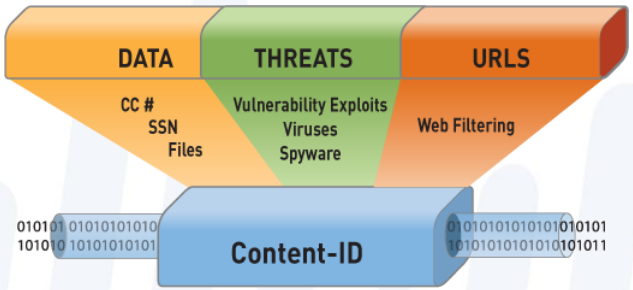
App-ID™
识别应用—提升端口识别



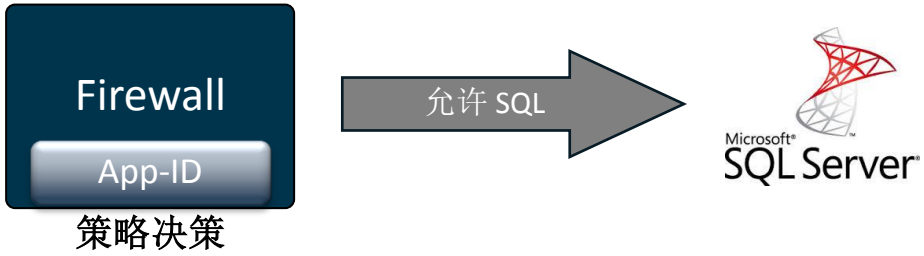
User-ID™
识别用户—提升基于IP控制



Content-ID™
扫描内容威胁—综合防护IPS，病毒，现代威胁



App-ID：采用应用协议而非服务端口进行控制

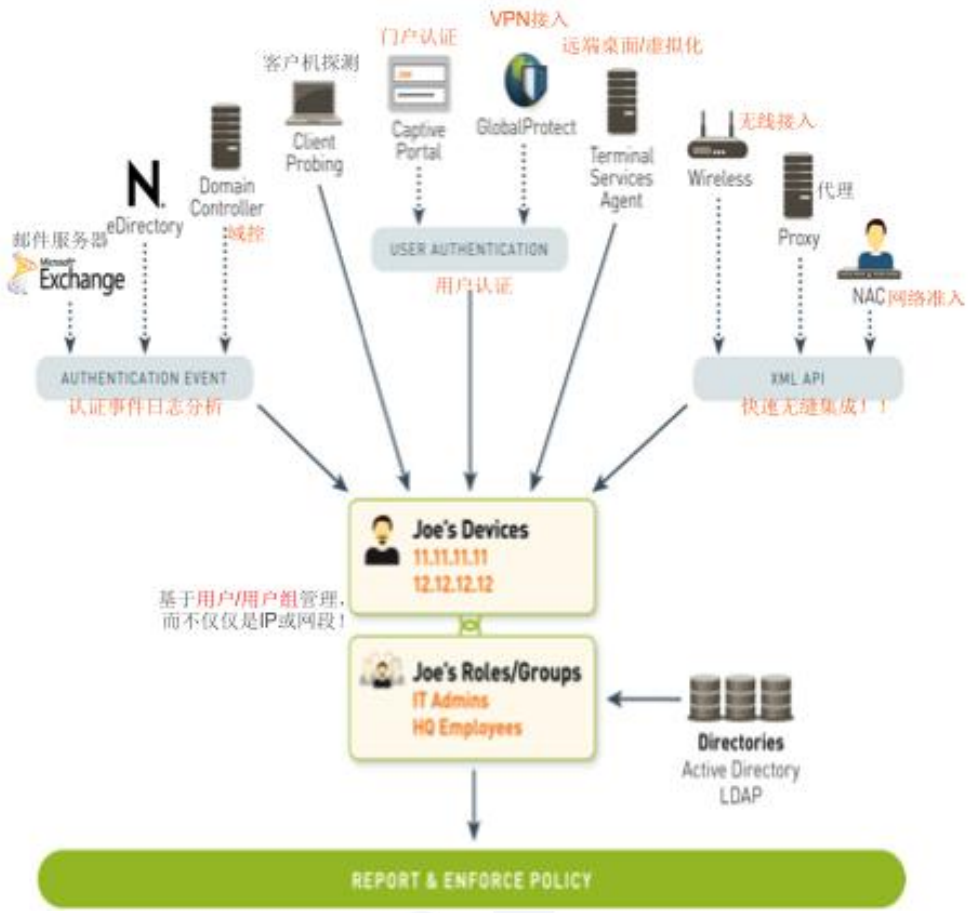


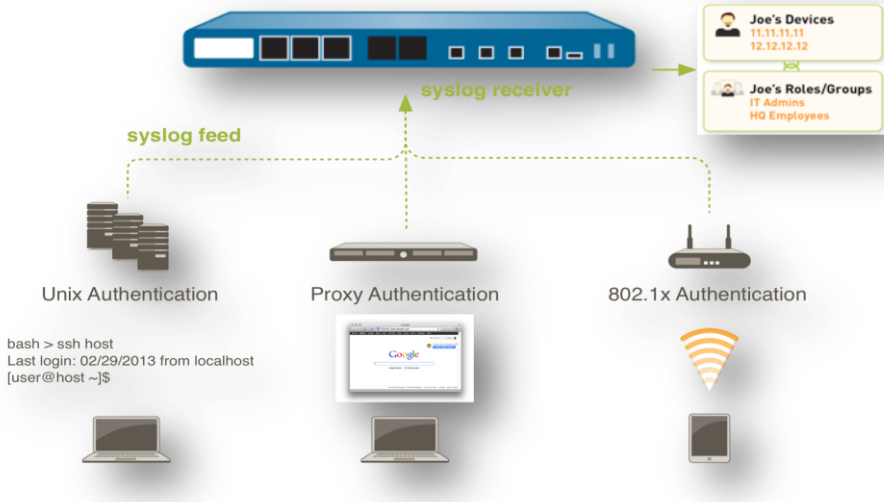
策略决策

paloalto NETWORKS

User-ID基于用户角色的识别与控制

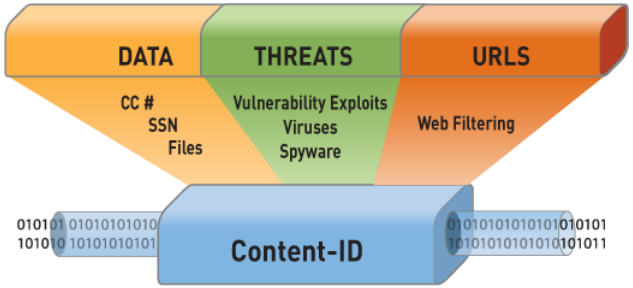
全网基于用户策略



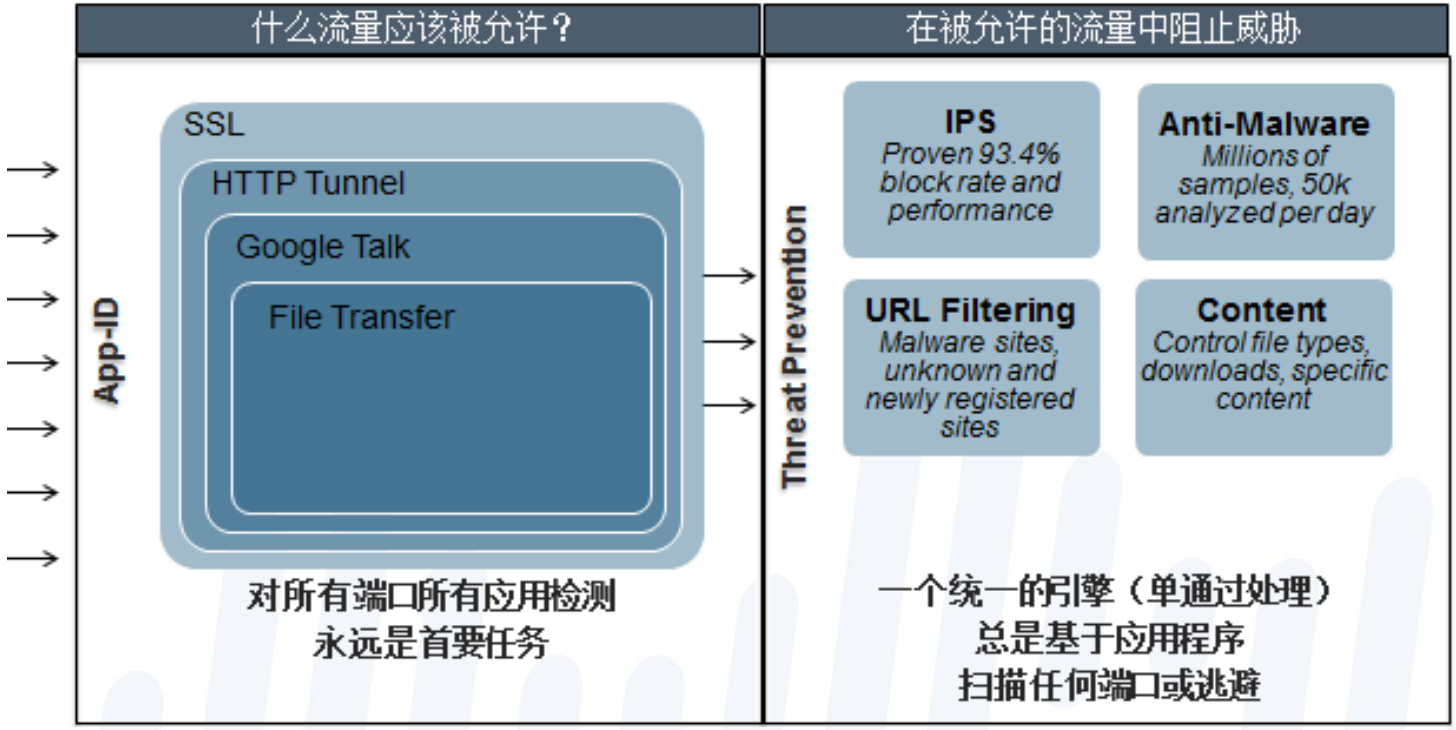


- Syslog接收器可以与大量现有无线控制器，代理，NAC准入方案整合
  - 原生支持BlueCoat Proxy, Citrix Access Gateway, Aerohive AP, Cisco ASA, Juniper SA NetConnect, Juniper Infranet Controller
- 借助XML API仍可与其他方案结合

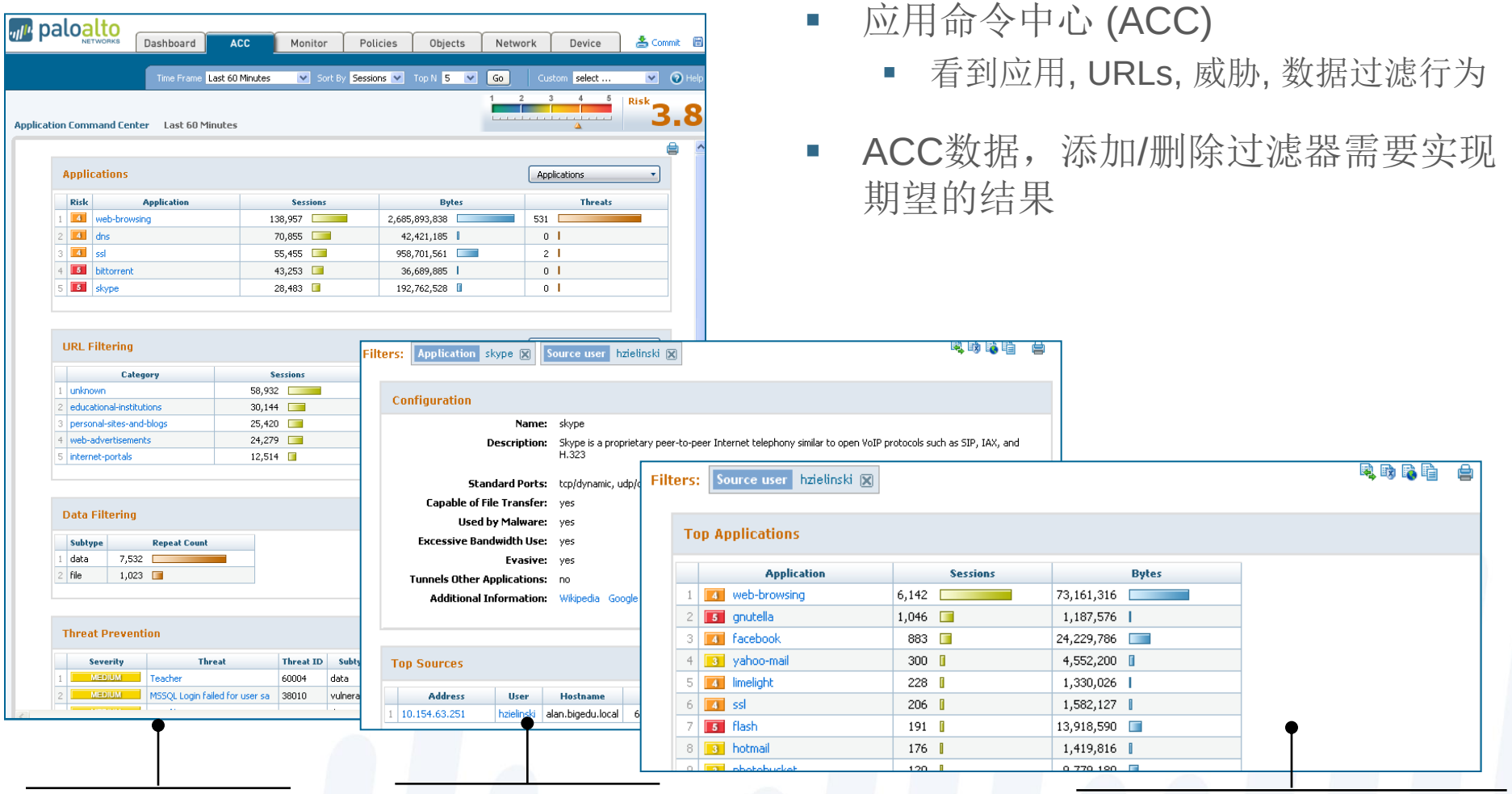
Content-ID: 应用的内容保护



- 主要区别
  - 和流量分类引擎（App-ID）紧密关联
  - 始终检测基于应用程序和用户的威胁
  - 端口和协议无关的
  - 基于流扫描的引擎，统一的签名格式=通过一次处理→检测和拦截各种形式的威胁



应用程序，用户和内容的可视性



- 应用命令中心 (ACC)
  - 看到应用, URLs, 威胁, 数据过滤行为
- ACC数据，添加/删除过滤器需要实现期望的结果

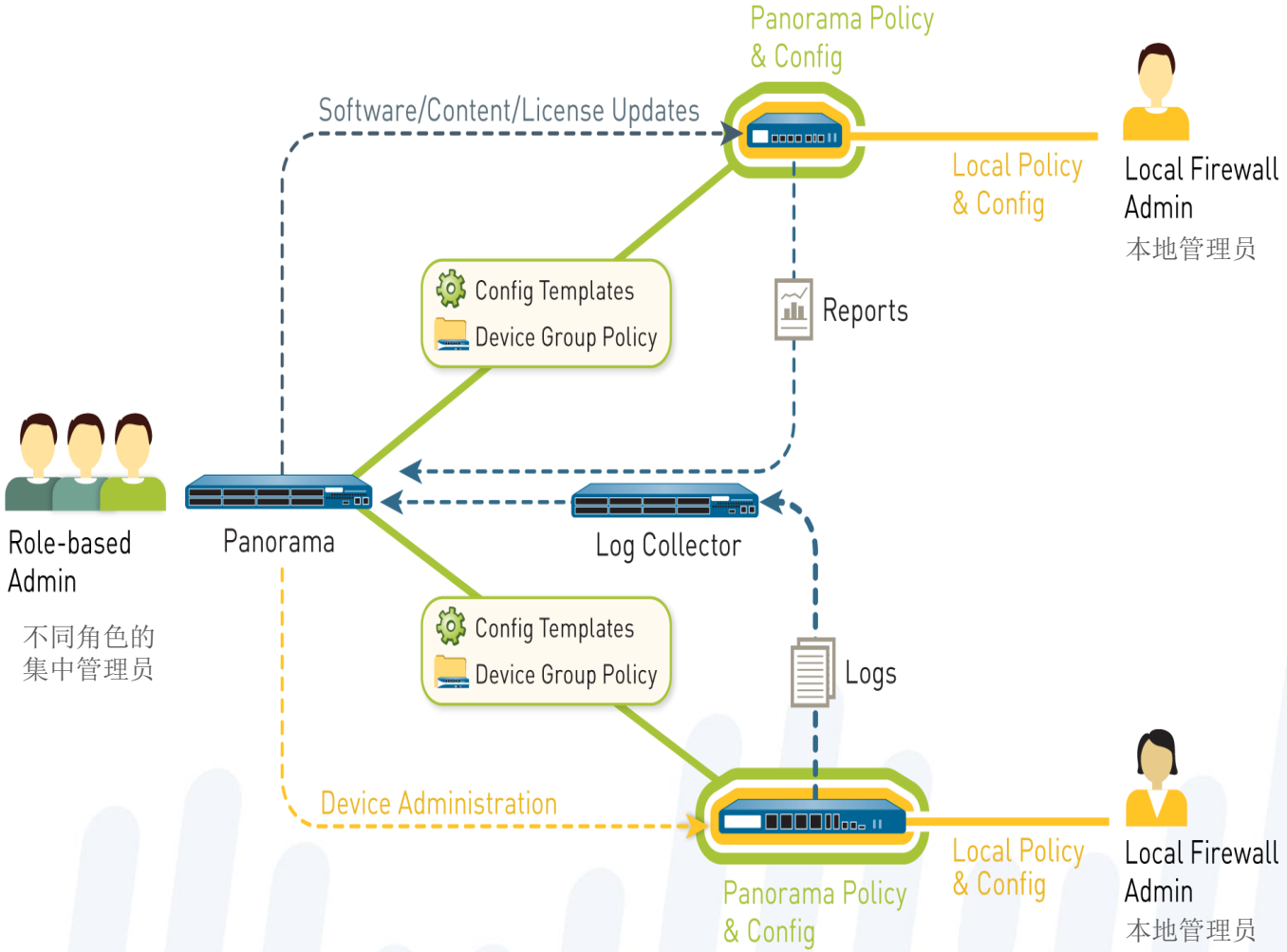
Skype过滤

在Skype上进行筛选和某用户关联

删除Skype扩大对某用户过滤范围

有效管理越来越多的设备

Panorama —— 集中管理！集中日志！集中报表！



主要议题

- 颠覆传统的下一代防火墙设计
- 针对现代威胁的防护
- 重要场景（数据中心，BYOD）
- 其他议题

当前安全问题

- 当今网络攻击者正利用日益成熟逃避战术
- 依赖多项分离的安全技术进行威胁检测和预防，使企业容易发生风险
- 攻击量的迅速加大，更加重了人数有限的安全专家们的负担

高级持续威胁的五大步骤

1 吸引/引诱用户

2 攻击与渗透

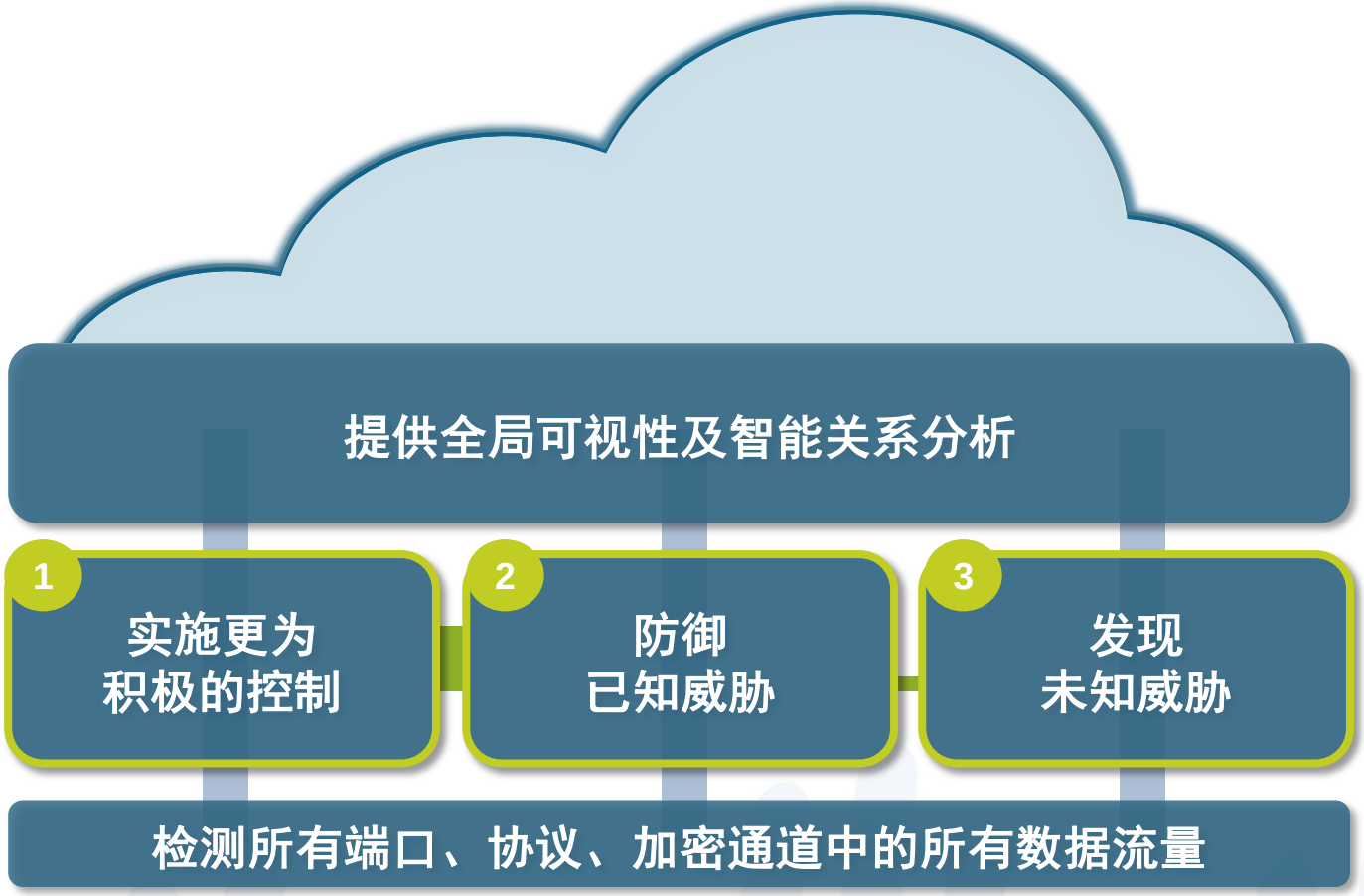
3 下载/上传后门程序

4 建立回传通道

5 浏览窃取资料

paloalto NETWORKS

系统化的方法可使企业网络更安全



实施更为积极的安全控制

细粒度的控制减少攻击面

- 高风险应用程序和协议
- 来自可疑域名或URL网址的文件
- 加密的或自定义的流量

858

应用程序可以传递文件

34%

应用程序使用SSL

17%

应用程序采用跳端口技术

防御已知威胁

通过不断开发的特征签名
阻止已知有害内容

- 漏洞攻击
- 已知有害程序和变种
- 恶意网站域名，网址及DNS
- 命令与控制 (C2或C&C)

每天发布超过

6,200个特征签名

1个特征签名最多阻挡

1,800种威胁变种

paloalto NETWORKS

发现未知威胁

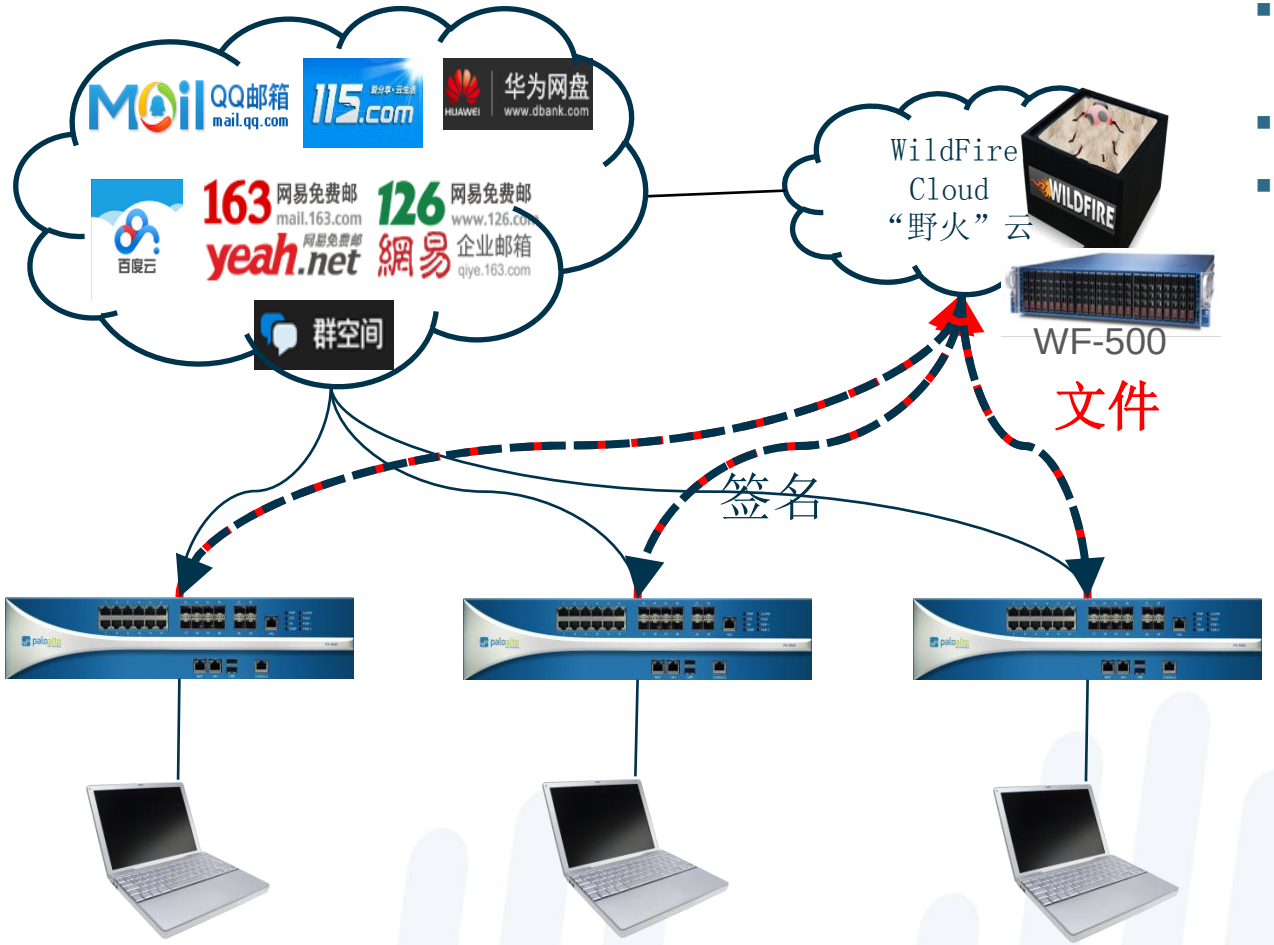
自动威胁防御

- 下一代防火墙在线部署控制
- 接近实时的特征签名更新
- 破坏威胁传递和回传（反恶意软件，域名，网址，命令与控制）

全球分析信息共享与威胁研究

威胁防护新补充—未知恶意软件分析

WildFire “野火” — Palo Alto Networks 的新措施



- WildFire 野火云分析中心
  - 基于沙盒技术作超过100种行为分析
  - 产生详细分析报告
  - 发现新的恶意软件和后门流量，加到签名库

❶互联网下载可疑文件

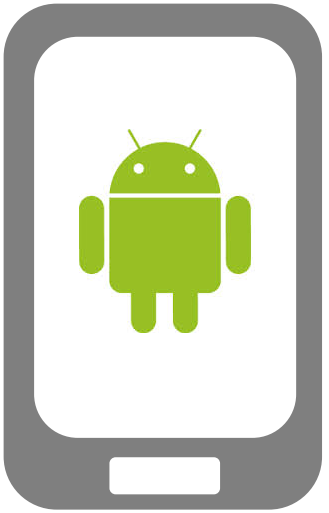
❷转到WildFire作行为分析

❸所有客户得到保护

WildFire持续创新，扩大覆盖面

恶意软件和攻击代码检测 NEW

移动恶意软件 NEW



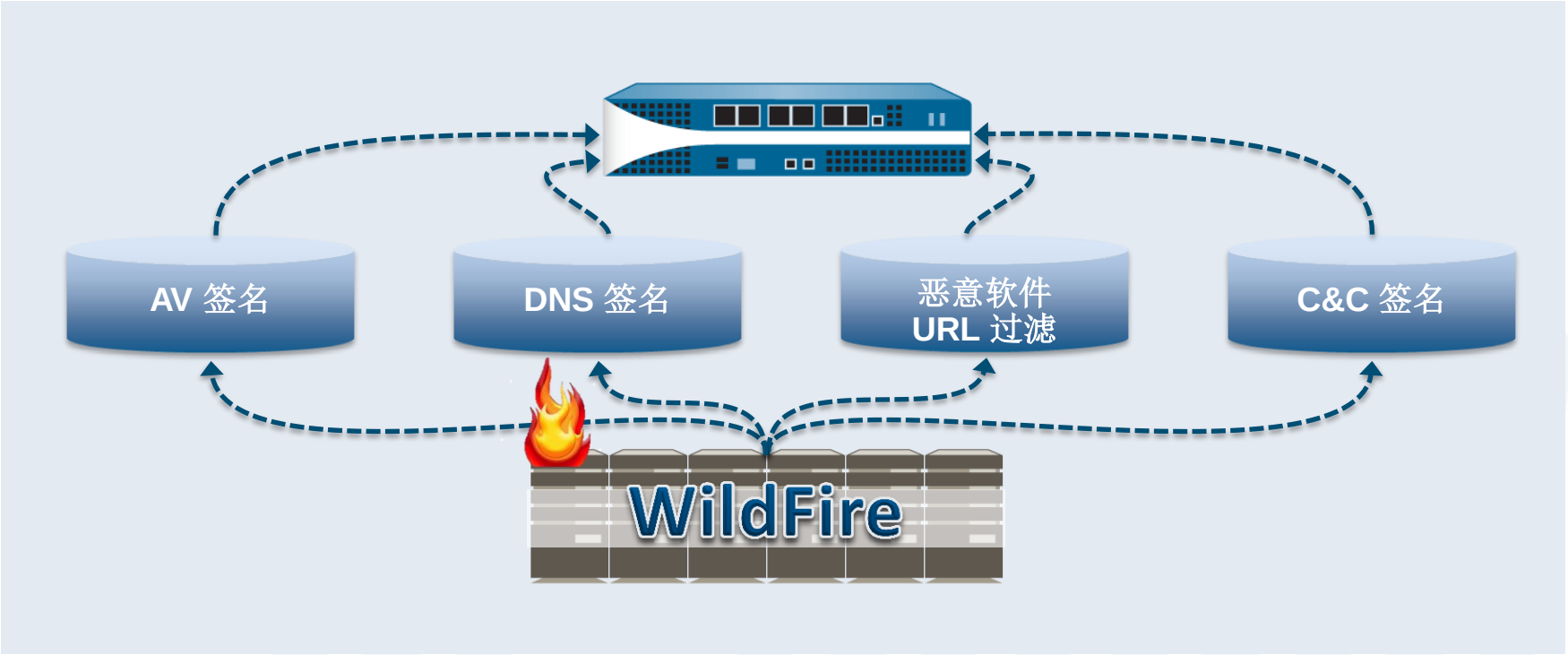
静态文件分析
和Android模拟器
中的动态分析相结合

同步在多个操作系统中执行 NEW

paloalto NETWORKS

WildFire与设备全面集成，生成多种有效签名

- 基于实际行为进行判断来执行未知文件发现恶意软件
- 威胁预防所有阶段结果的反馈
- 阻止新的威胁，而不是仅仅检测



APT与现代威胁防护

paloalto NETWORKS

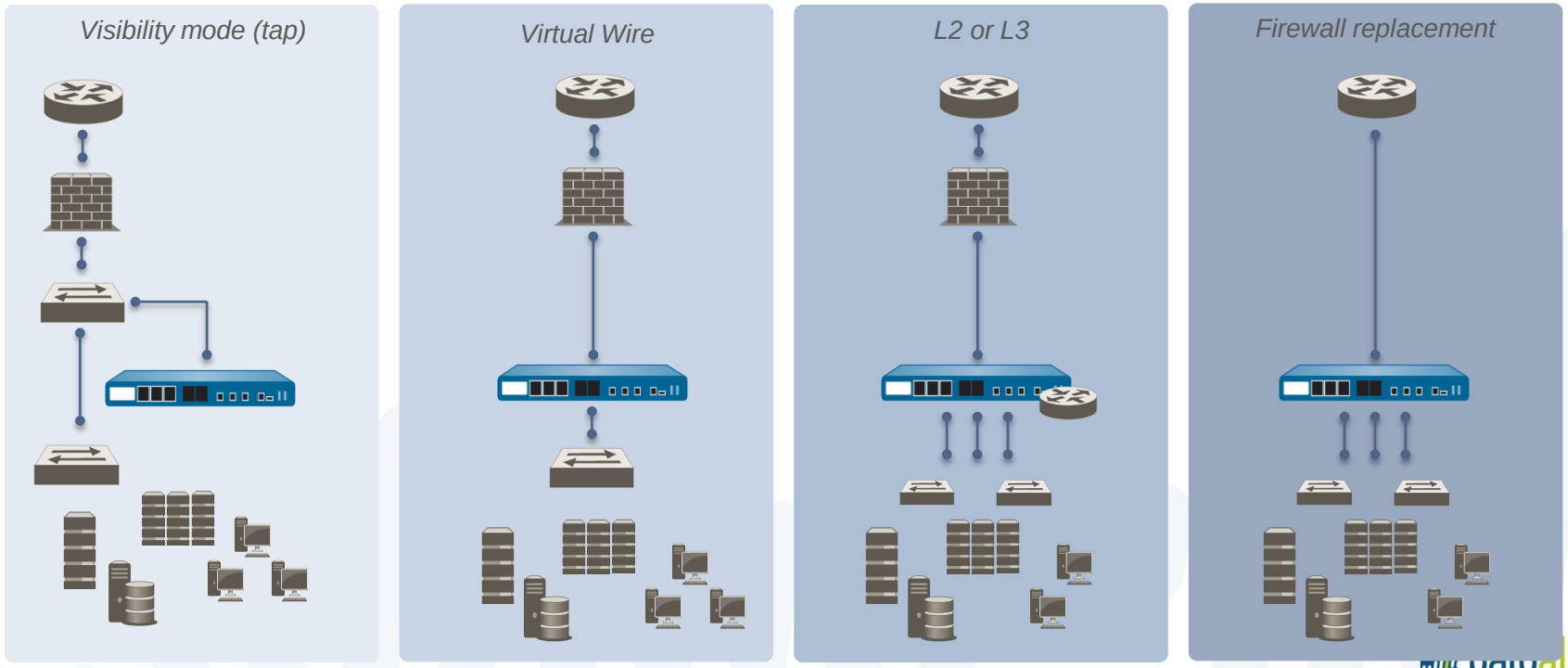
	1	2	3	4	5
	吸引/引诱 最终用户	攻击 与渗透	下载 后门程序	建立 回传通道	浏览 与窃取
App-ID	阻挡高风险应用			阻挡使用非标准端口的命令与控制通讯	
URL	阻挡已知恶意网站链接			阻断恶意软件及恶意快速变动域名	
IPS		阻断攻击与渗透			协调特征签名，攻击源，行为分析等多种智能手段，检测和阻断主动攻击
Spyware				阻止间谍软件，命令与控制流量	
AV			阻挡恶意软件		
Files			防御随看下载行为		
WildFire			检测未知恶意软件	阻止新的命令与控制通讯	

威胁防护许可

Palo Alto Networks 灵活部署

无需替换现有防火墙的部署，即可利用WildFire 野火和Threat Prevention威胁防御获得APT的检测与防护

- ✓ 无需像传统防火墙一样部署就可以开启WildFire野火或其他威胁防护功能
- ✓ 灵活的TAP，虚拟线或三层混合部署模式，可适用于任何现有网络架构，将文件发送至WildFire进行分析
- ✓ 公有或私有云架构其扩展性可满足任何网络规模的分析需求



主要议题

- 颠覆传统的下一代防火墙设计
- 针对现代威胁的防护
- 重要场景（数据中心，BYOD）
- 其他议题

安全性能需求

应用程序级攻击日益复杂化，更大的带宽需要可扩展的高性能安全

Internet Gateway	• 确保所有用户在所有设备上安全
Data Center	• 确保所有的应用程序，控制所有用户访问与设备
Network Segmentation	• 保护内部资源

paloalto NETWORKS

关键场景

数据中心的安全

paloalto NETWORKS

the network security company™

为什么要用于数据中心?

- 大的项目:
  - 高端防火墙与HA
  - 捆绑威胁许可证
  - 更好的利润
- 许多IT规划需要安全
  - 服务器虚拟化
  - VDI（虚拟桌面基础架构）
  - 网络分割
  - 公共网站
  - 外部网络

- Palo Alto Networks 相关技术从 App-ID 到 WildFire, 真正解决客户的问题

paloalto NETWORKS

影响数据中心
应用程序的复杂性和用户访问

微软推荐开放的Lync端口

Port	Protocol	Direction	Usage
443	STUN/TCP	Outbound	Audio, video, and application sharing sessions
443	PSOM/TLS	Outbound	Data sharing sessions
3478	STUN/UDP	Outbound	Audio and video sessions
5223	TCP	Outbound	Lync Mobile push notifications
50000-50019	RTP/UDP	Outbound	Audio
50020-50039	RTP/UDP	Outbound	Video
50040-50059	UDP	Outbound	Application sharing and file transfer

随机的，不连续的通讯端口和协议

…… 分布式网络访问具有不同的安全风险

paloalto NETWORKS

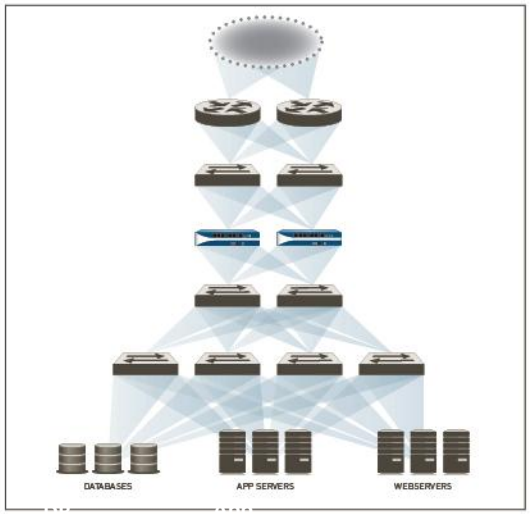
影响数据中心
通过应用程序和用户的高层攻击

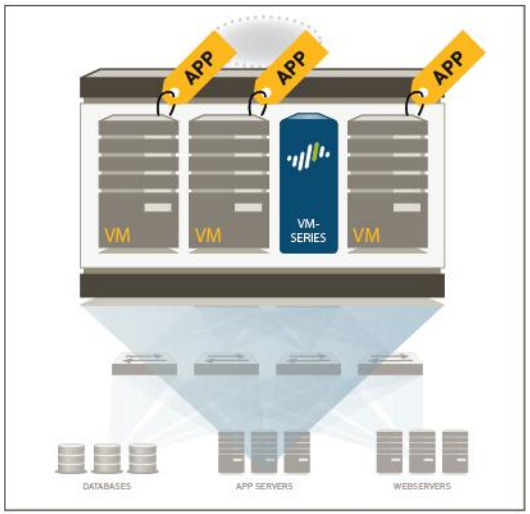
- 10 out of 1,395 applications = 97% of the exploit logs
- 9 of these are business critical, running in your datacenter
- 2,016 unique exploits, ~60M exploit logs

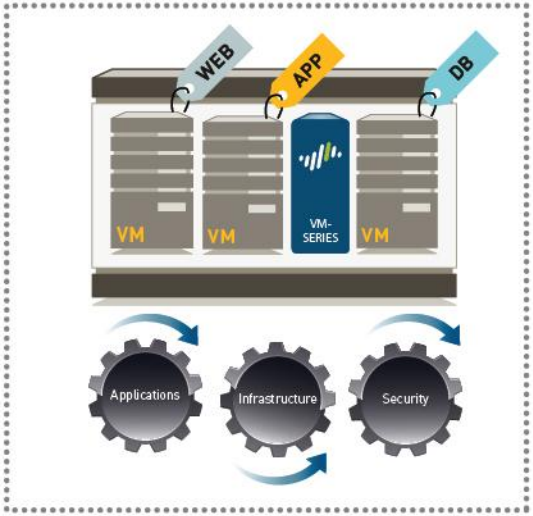
paloalto NETWORKS

影响数据中心

整合，虚拟化和云计算





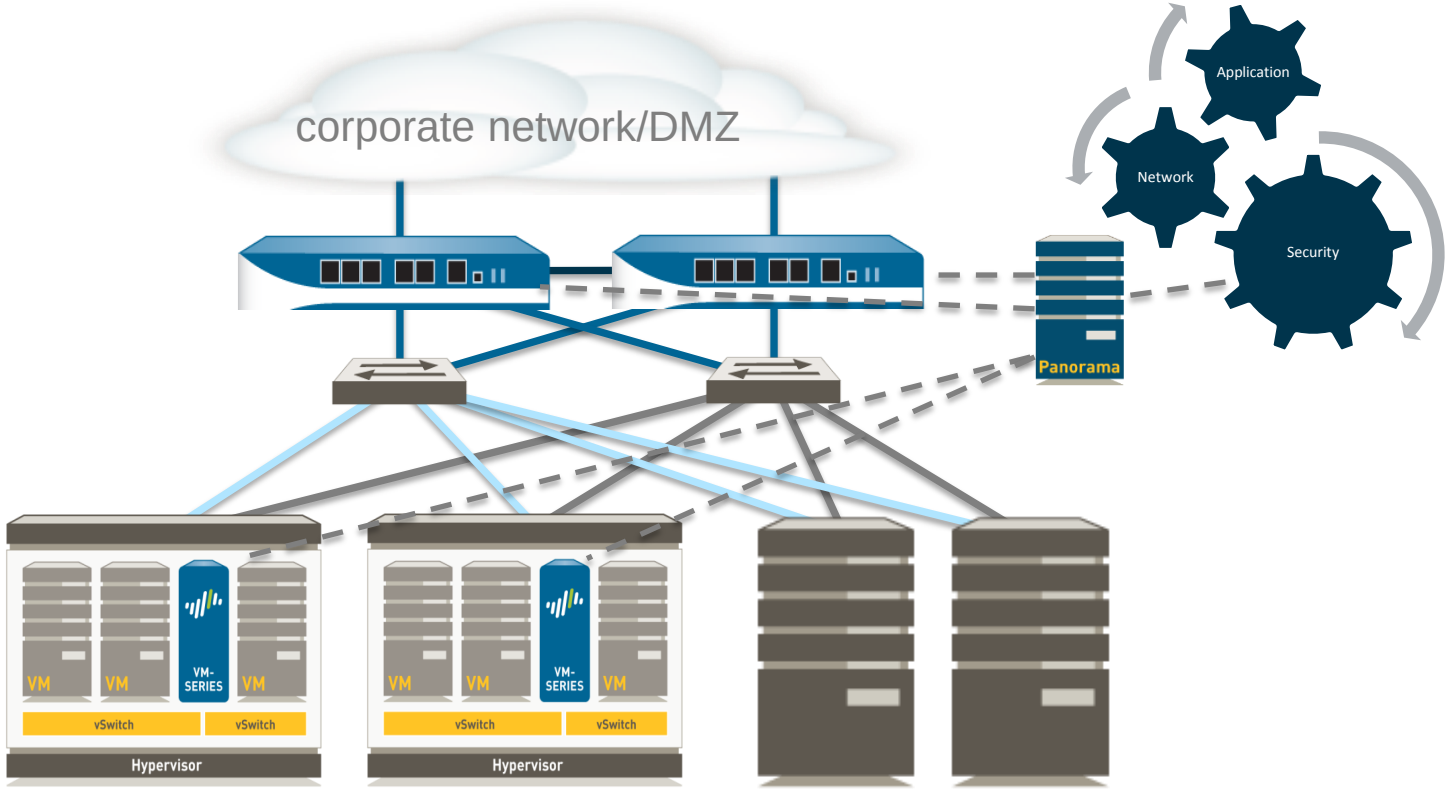


传统数据中心	虚拟数据中心	云（私有/公共）
• 专用应用程序服务器	• 每个服务器多个应用	• IT 即服务
• 服务器使用率 = 15%	• 提高运营效率	• 按需服务
• 横跨流量	• 提高服务器利用率	• 自动化和编排化

业务灵活性 Vs 节省成本 Vs 安全

paloalto NETWORKS

下一代数据中心保护



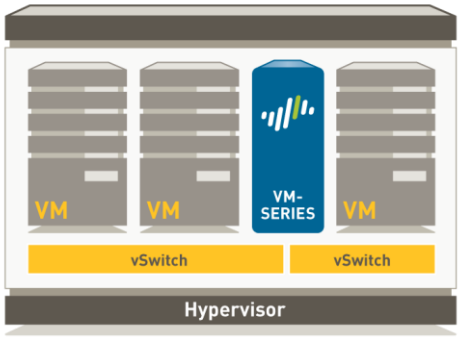
南北（物理）和东西（虚拟）流量分割

通过动态地址组跟踪虚拟应用程序配置和变更

通过REST的API，自动化和业务流程的支持

虚拟化部署的选择

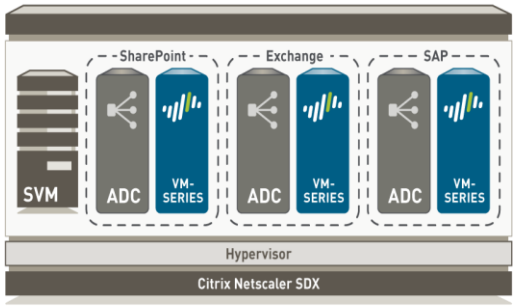
VM-Series for VMware vSphere (ESXi)



- VM-100, VM-200, VM-300 在VMware ESXi平台上作为虚拟客户机部署
- 作为虚拟网络配置的一部分，提供东—西向流量检测

New

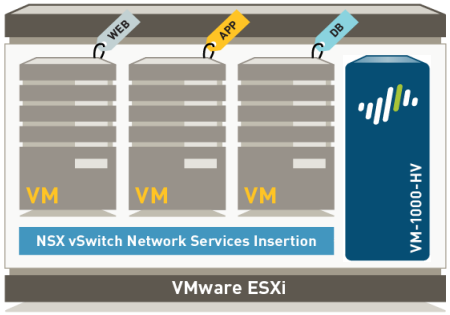
VM-Series for Citrix NetScaler SDX



- VM-100, VM-200, VM-300在 Citrix NetScaler SDX平台上作为虚拟客户机部署
- 为多客户及Citrix XenApp/XenDesktop部署提供整合的ADC及安全服务

独有！

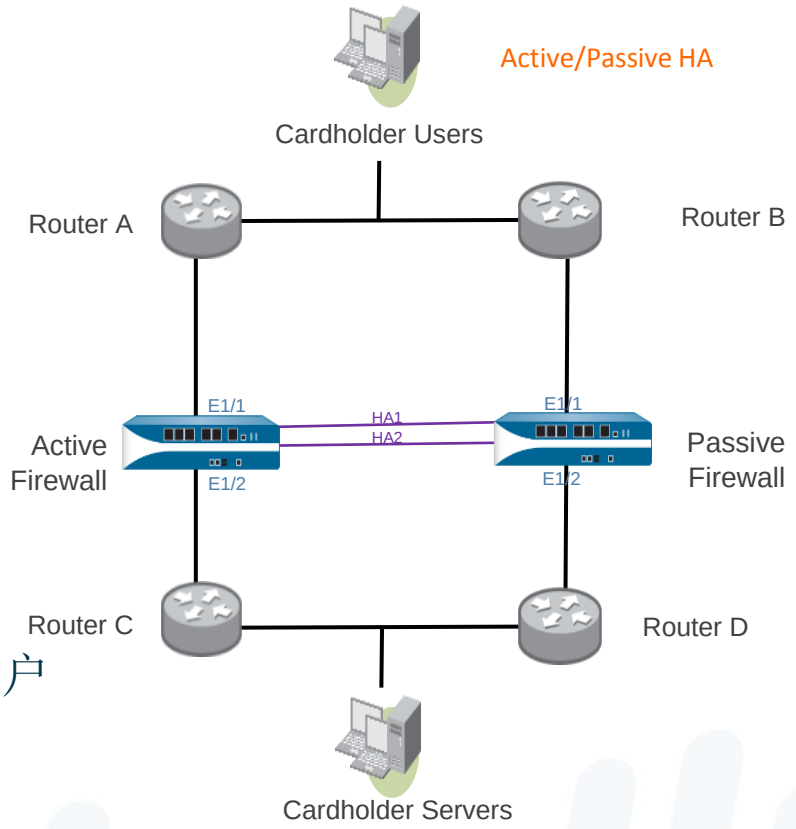
VM-Series for VMware NSX



- VM-Series for NSX 与VMware NSX和Panorama集中平台一同作为服务部署
- 东—西向流量检测的理想方式

通过 Palo Alto Networks实现网络分割

- 很多的原因需要实现网络分割:
  - 降低合规范围
    - PCI 和 HIPAA 规则
  - 降低攻击范围
    - 隔离脆弱或老的系统
  - 限制数据泄露
    - 限制用户对敏感数据的访问.
- 真正的分割要求防火墙能够理解应用程序，用户和内容。



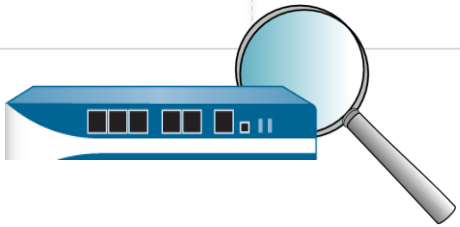
大型企业 “Zero Trust” 机会

全球合作伙伴，承包商和收购

知识产权数据

国家利益

办公室和国家之间的用户移动性

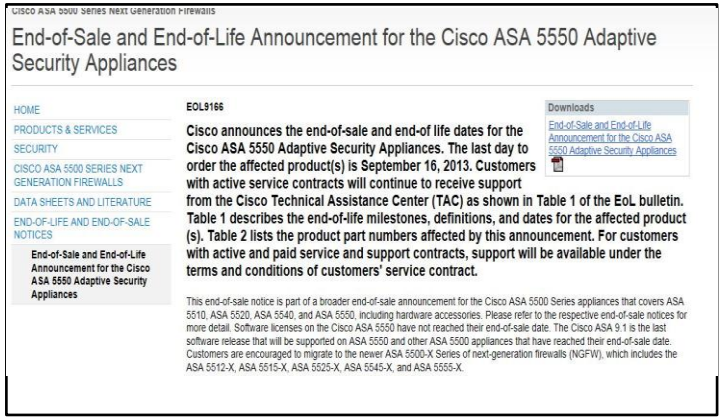


- 大，全球企业网络安全的挑战 - 全球化，流动性，针对智能数据攻击。
- 大型企业 “segmentation” 机会:
  - ESPN with Disney
  - Disney (each movie is its entity)
  - Autodesk
  - Microsoft

paloalto NETWORKS

Conversation triggers and opportunities

- 数据中心防火墙更新机会
  - Cisco ASA
  - Cisco FWSM
  - Juniper SRX
- 项目
  - DC consolidation (Cisco Cat 6K - Nexus)
  - Virtualization projects
  - Private cloud projects
  - Zero Trust network segmentation
  - B2B Partner Extranet
  - Public Websites


Cisco ASA 5500 Series Next Generation Firewalls

End-of-Sale and End-of-Life Announcement for the Cisco ASA 5550 Adaptive Security Appliances

HOME
PRODUCTS & SERVICES
SECURITY
CISCO ASA 5500 SERIES NEXT GENERATION FIREWALLS
DATA SHEETS AND LITERATURE
END-OF-LIFE AND END-OF-SALE NOTICES
End-of-Sale and End-of-Life Announcement for the Cisco ASA 5550 Adaptive Security Appliances

EOL9166

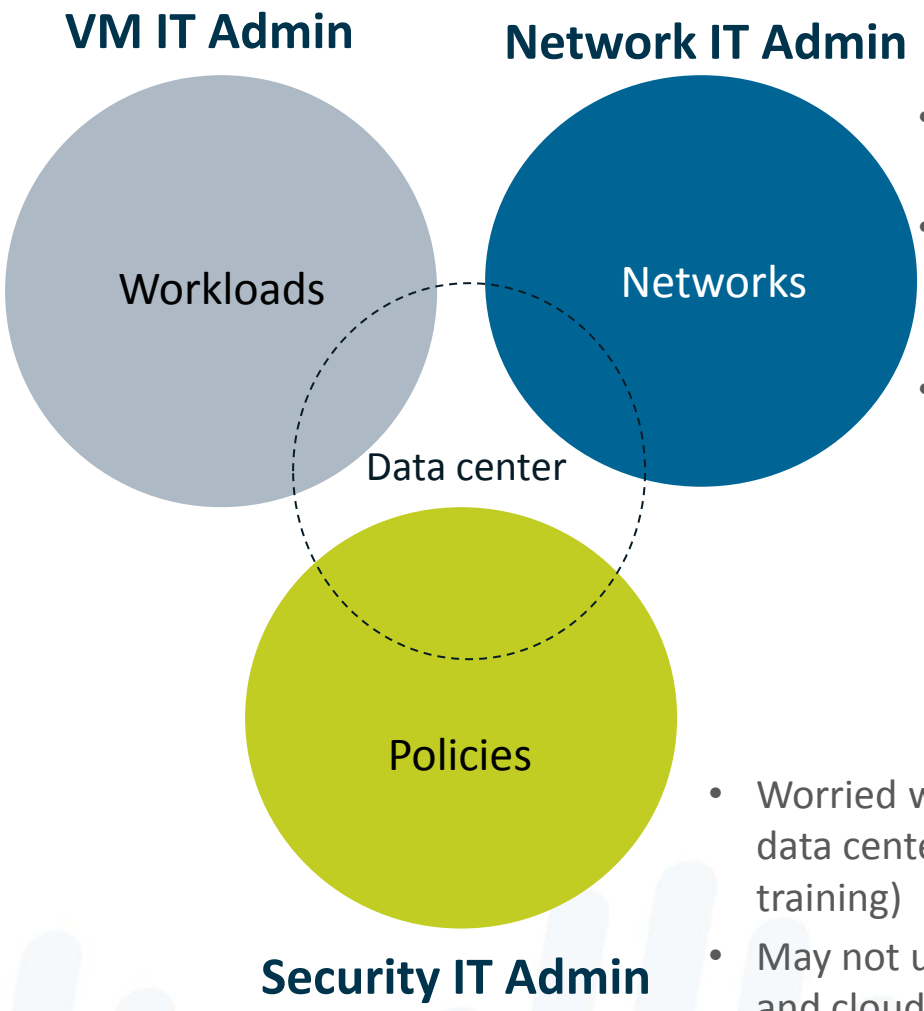
Cisco announces the end-of-sale and end-of life dates for the Cisco ASA 5550 Adaptive Security Appliances. The last day to order the affected product(s) is September 16, 2013. Customers with active service contracts will continue to receive support from the Cisco Technical Assistance Center (TAC) as shown in Table 1 of the EoL bulletin. Table 1 describes the end-of-life milestones, definitions, and dates for the affected product (s). Table 2 lists the product part numbers affected by this announcement. For customers with active and paid service and support contracts, support will be available under the terms and conditions of customers' service contract.

This end-of-sale notice is part of a broader end-of-sale announcement for the Cisco ASA 5500 Series appliances that covers ASA 5510, ASA 5520, ASA 5540, and ASA 5550, including hardware accessories. Please refer to the respective end-of-sale notices for more detail. Software licenses on the Cisco ASA 5550 have not reached their end-of-sale date. The Cisco ASA 9.1 is the last software release that will be supported on ASA 5550 and other ASA 5500 appliances that have reached their end-of-sale date. Customers are encouraged to migrate to the newer ASA 5500-X Series of next-generation firewalls (NGFW), which includes the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X.

Downloads
End-of-Sale and End-of-Life Announcement for the Cisco ASA 5550 Adaptive Security Appliances

Saying the right things to the right people

- The evolution of the “Server Guy” (Windows)
- Can deploy 1000 servers in a single click
- Afraid that security will take away the “Easy Button”



- Owns data center budget for switch refresh
- Wants security solutions that work best with the networking infrastructure
- Afraid that security will impact network performance, availability, uptime

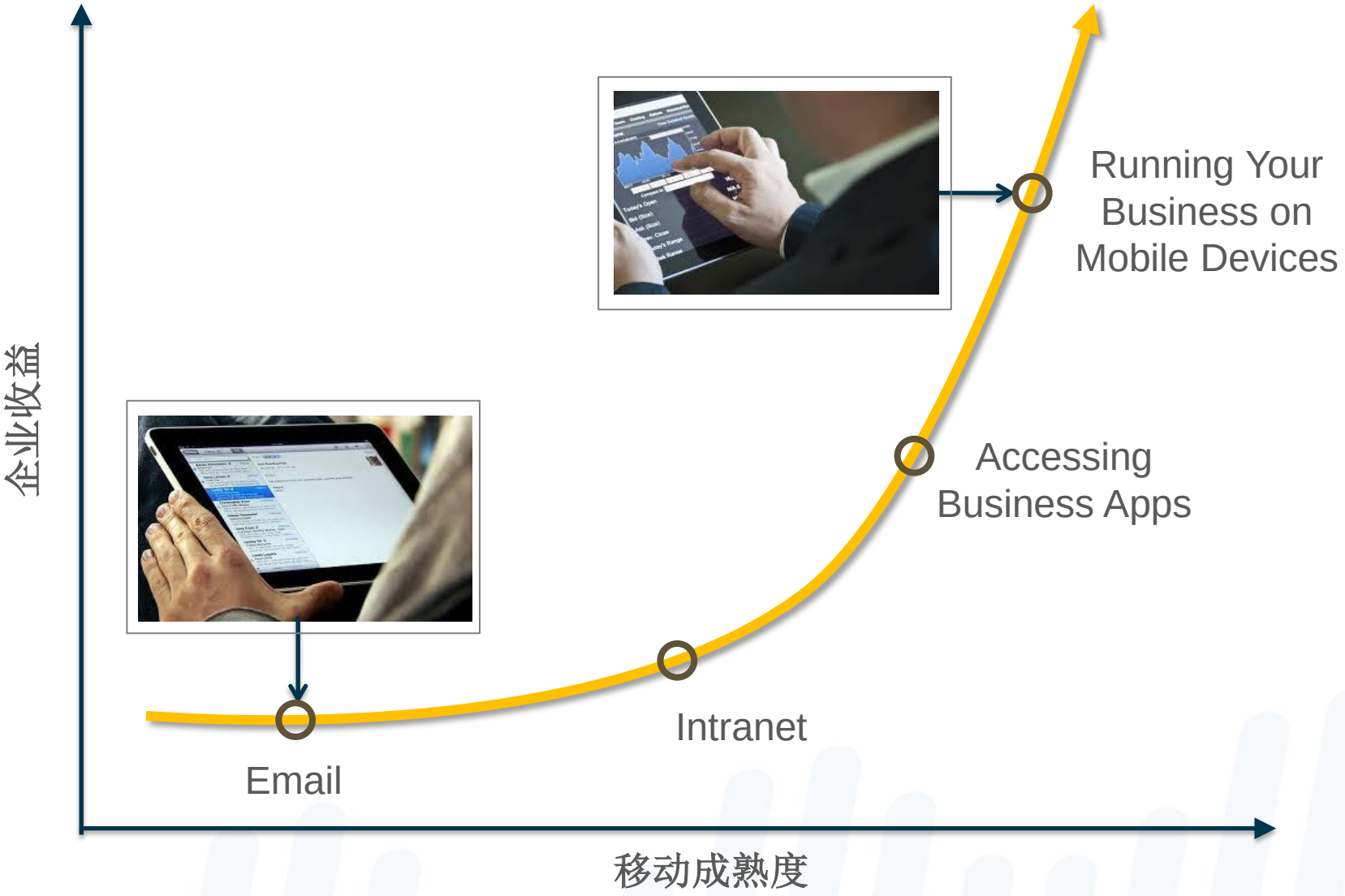
- Worried we’re unproven in the data center (operations, support, training)
- May not understand virtualization and cloud security challenges

paloalto NETWORKS

应用场景
BYOD

paloalto NETWORKS
the network security company™

‘解锁’移动终端的潜力取决于安全



移动安全的现有方法是失效

途径	面临的风险
阻止移动设备	人们仍然会使用移动设备，只是没有你的控制
希望现有的安全保护移动设备	不知道现有措施是否将对移动设备有效
使用像ActiveSync的基本的移动安全	没有解决移动的威胁，不能确保安全使用应用和数据

paloalto NETWORKS

新的方法来安全地使移动设备

管理设备	保护设备	控制数据
使用正确的安全设置来配置设备，确保设备安全启用。通过配置常见的配置来简化部署和设置，例如电子邮件的帐户设置以及诸如证书等凭据。	保护移动设备免受攻击和恶意软件侵害。数据在有漏洞的设备上不会安全。 • 保护设备免受感染，也可以保护机密数据和未经授权的网络访问	控制对数据的访问权限以及控制数据在应用程序之间的移动 • 通过应用程序，用户和设备状态控制访问 • 扩展设备数据移动控制，以确保数据保留在“业务应用”范围内

GlobalProtect移动安全解决方案

GlobalProtect
移动安全管理（MSM） NEW

提供设备管理，
恶意软件检测，
设备状态

GlobalProtect Gateway

基于的应用程序，用户，内容和设备状态
提供移动威胁防护和策略实施

GlobalProtect App（客户端）

启用设备管理，提供设备状态信息，并建立安全连接

管理设备

GlobalProtect
移动安全管理（MSM）

NEW

GlobalProtect App
（客户端）

管理设备的设置

- 强制执行安全设置，如密码
- 限制了设备的功能，如摄像头
- 配置帐户，如电子邮件，VPN，Wi-Fi设置

监控设备状态

- 监测和报告设备状态策略执行，如:
  - 白名单/黑名单的应用程序
  - Rooted/越狱

执行关键操作

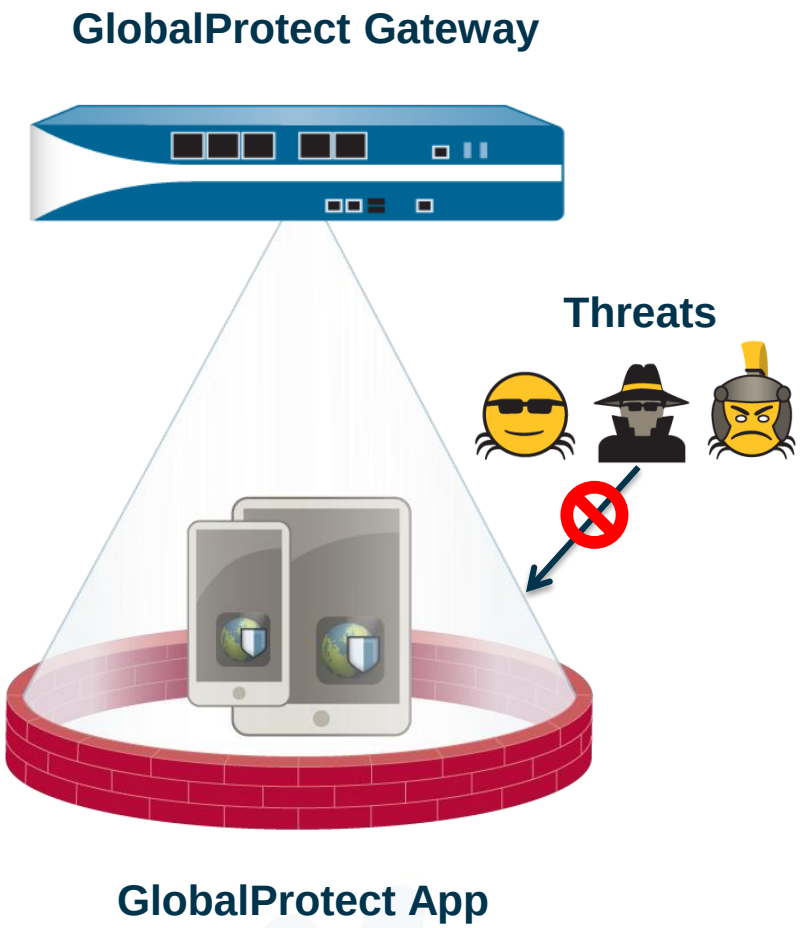
- 例如：锁定，解锁，擦除，发送消息

检测Android恶意软件

- 对恶意软件的检测和反应

paloalto NETWORKS

保护设备



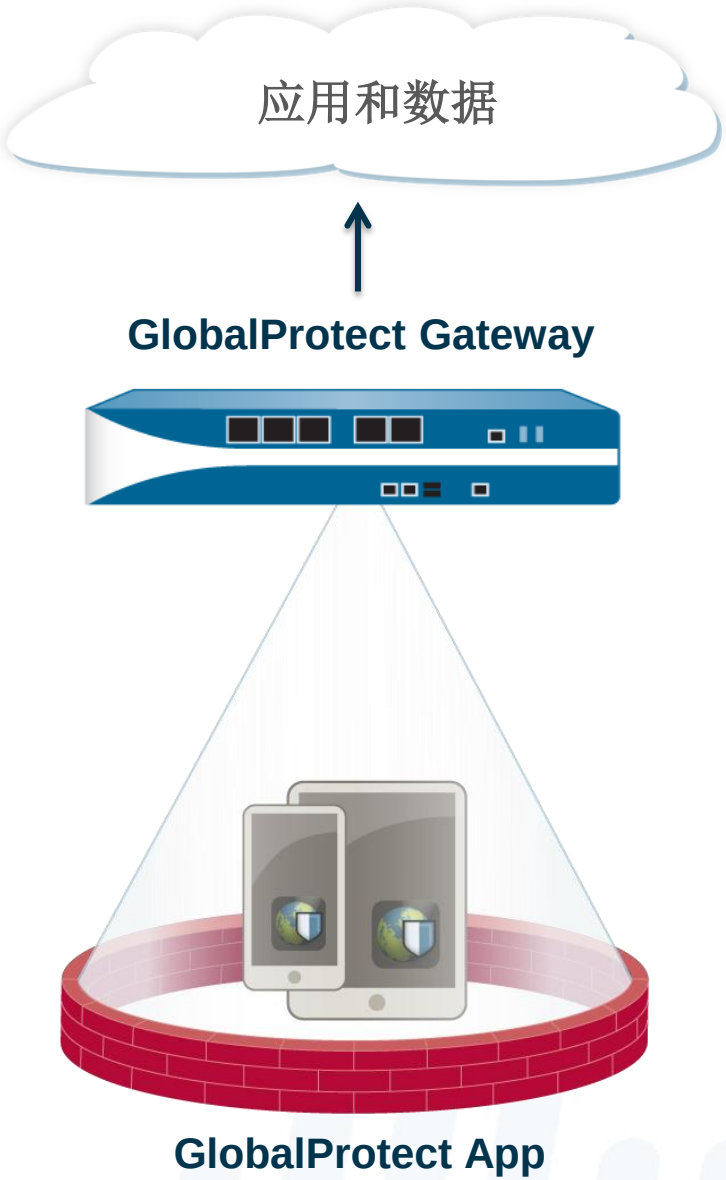
一致的安全无处不在

- IPsec/ SSL VPN和下一代安全平台建立连接，策略执行，无论该设备位于何位置

移动威胁防护

- 漏洞（IPS）和恶意软件（AV）保护移动威胁
- URL过滤保护，防止恶意网站
- 野火-高级移动威胁静态和动态分析

控制数据



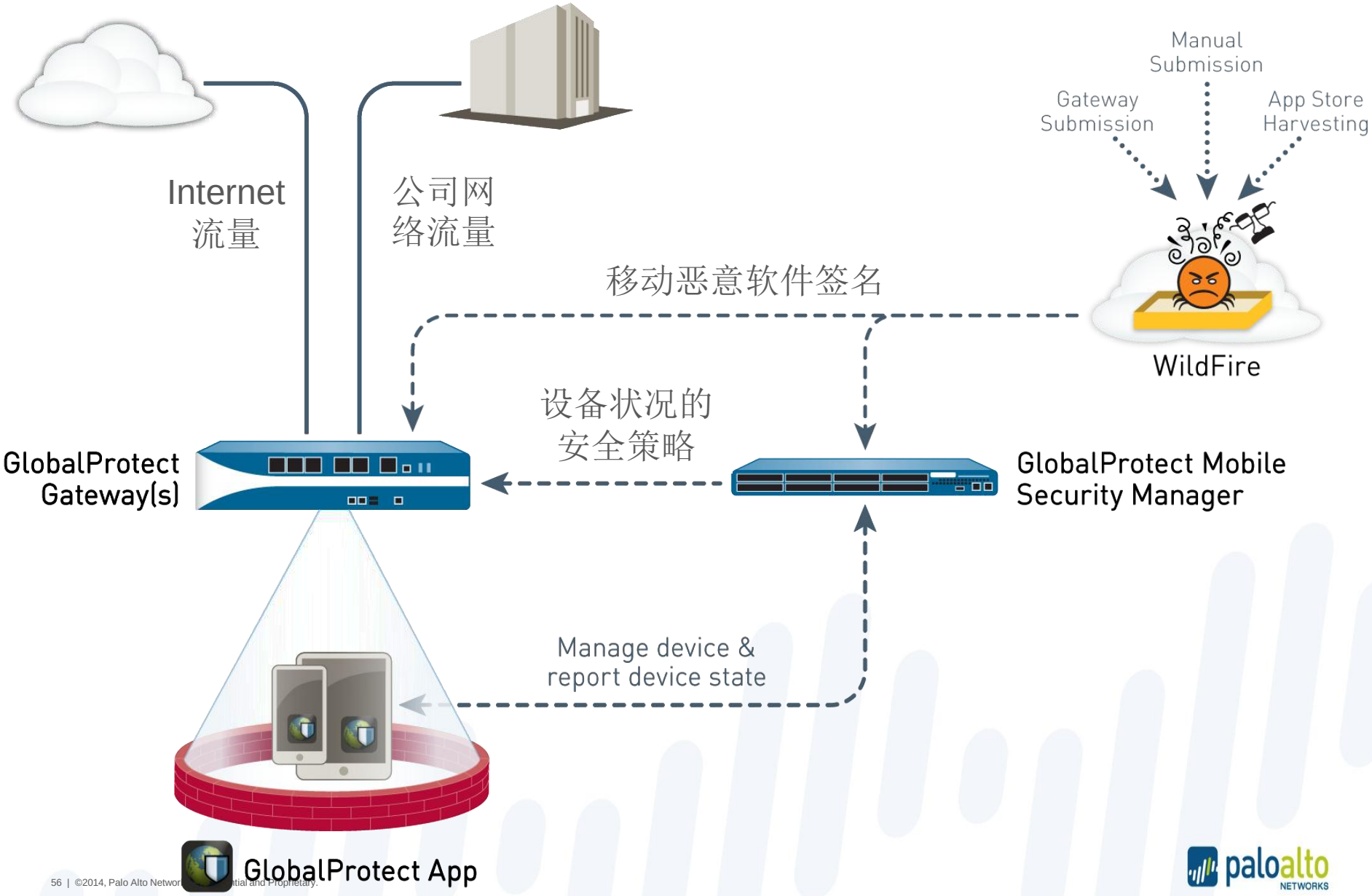
应用程序和数据的访问控制

- 细粒度的策略决定哪些用户和设备可以访问敏感的应用程序和数据
- 根据应用，用户，内容，设备和设备状态进行控制和可视性
  - 识别设备类型，如IOS，Android的，在Windows，Mac设备
  - 识别设备的所有权，如个人（BYOD）或公司发行的
  - 确定设备状态，如Rooted/越狱
- 基于内容和文件类型阻挡及控制

在设备上的应用之间的控制数据移动

- 解决方案提供对于数据保护未来进一步的发展基础

真正的BYOD解决方案



Palo Alto Networks 移动安全

唯一解决方案，集成了多种技术 - VPN，策略，威胁预防，管理

独特的能力，能够通过野火，IPS和应用策略保护设备

完整的安全平台，在网络中保护所有的流量，设备，应用程序和数据


paloalto
NETWORKS
the network security company™

主要议题

- 颠覆传统的下一代防火墙设计
- 针对现代威胁的防护
- 重要场景（数据中心，BYOD）
- 其他议题

企业级下一代防火墙安全

网络边界

- 防火墙上的应用可视化和控制
  - 所有应用，所有端口，每时每刻
- 威胁防御
  - 已知威胁
  - 未知/有针对性恶意软件
- 简化安全基础架构

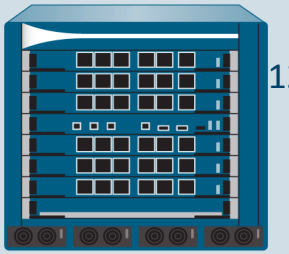
数据中心

- 网络分割
  - 基于应用和用户，而非端口及IP
- 简单，灵活的网络安全
  - 可与各类数据中心设计集成
  - 高可用性，高性能
- 威胁防御

分布式企业环境

- 各地的网络安全保持一致水准
  - 总部/分公司/远程及移动用户
- 逻辑边界
  - 策略随应用和用户生效，而非地理区域
- 集中管理

Palo Alto Networks 下一代防火墙主力机型



PA-7050

120 Gbps FW/60 Gbps TP
24 million sessions

24 SFP+ (10 Gig)
48 SFP (1 Gig)
72 copper gigabit

PA-5050/5060

10/20 Gbps FW/
5/10 Gbps threat prevention/
2million/4million 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

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

8 SFP, 8 copper gigabit,2SFP+

PA-3050

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

8 SFP, 12 copper gigabit

PA-3020

2 Gbps FW/1 Gbps threat prevention/250,000 sessions

8 SFP, 12 copper gigabit

PA-500

250 Mbps FW/100 Mbps threat prevention/64,000 sessions

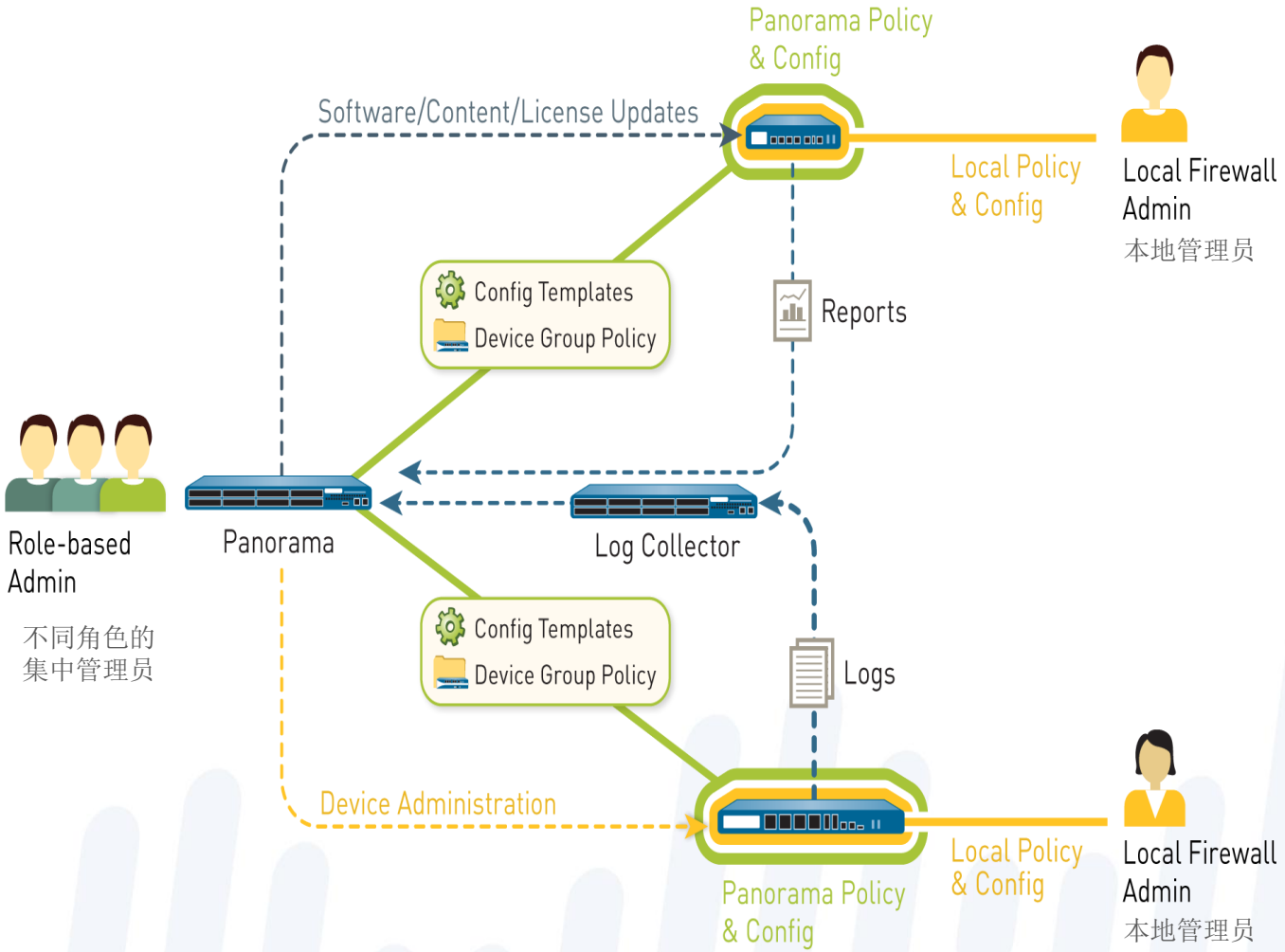
8 copper gigabit

PA-200

100 Mbps FW/50 Mbps threat prevention/64,000 sessions

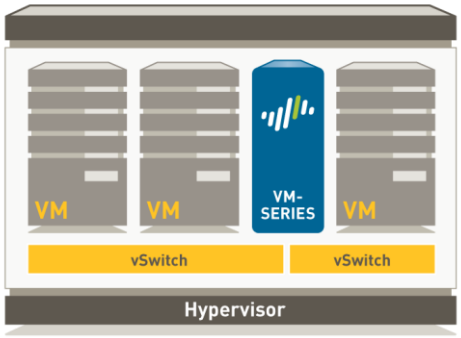
4 copper gigabit

Panorama —— 集中管理！集中日志！集中报表！



虚拟化部署的选择

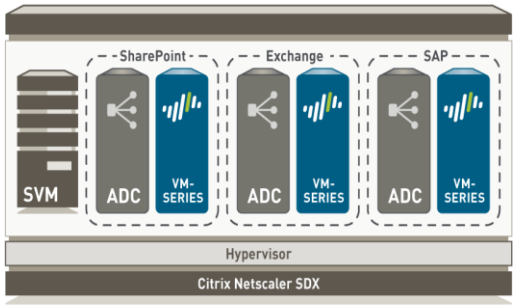
VM-Series for VMware vSphere (ESXi)



- VM-100, VM-200, VM-300 在VMware ESXi平台上作为虚拟客户机部署
- 作为虚拟网络配置的一部分，提供东—西向流量检测

New

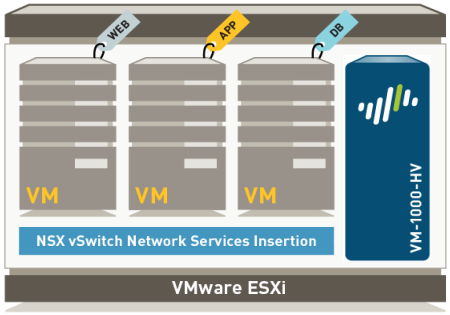
VM-Series for Citrix NetScaler SDX



- VM-100, VM-200, VM-300在 Citrix NetScaler SDX平台上作为虚拟客户机部署
- 为多客户及Citrix XenApp/XenDesktop部署提供整合的ADC及安全服务

独有！

VM-Series for VMware NSX



- VM-Series for NSX 与VMware NSX和Panorama集中平台一同作为服务部署
- 东—西向流量检测的理想方式

AVR 报告
应用可视化风险报告

paloalto NETWORKS

the network security company™

何为 Application Visibility Report (AVR) 报告

- 这是一个执行报告，提出了一段时间的数据总结。
- 它提供了提供手段，是一个安全报告，以及对一个企业的影响的报告

AVR报告/销售流程

- 我们对每一个客户提供一个AVR. 他给我们一个再次和客户讨论的理由，并把我们的解决方案介绍给高层领导
- 首次设备安装后，我们第一次安装后，我们安排一个星期后跟进。我们回答问题，并在交谈中收集统计资料。
- 我们会安排AVR的回报（在测试结束后）.也给我们一个尽快结束测试的理由。

AVR 产生

- Tap Mode 安装或其他模式都可以
- 通过图形界面device->Support->Stats Dump File获得测试数据
- 登陆 https://avr.paloaltonetworks.com/
  - 授权认证的渠道商可以进入，SI可以让渠道商生成此报告
  - 进入后，上传此测试数据文件，点击 “create report”
  - 执行报告向导操作（如选择语言-中文，用户名称，代理商名称等），生成AVR报告
  - PDF形式

AVR 注意事项

- 用户数据会被上传
- 生成的AVR报告是普通模板生成的，很多内容用户未必理解和关心。
- 如果是对安全比较专业的客户建议用‘增强’模板提交报告（而不是用此通用格式提交）

行业解决方案

paloalto NETWORKS

the network security company™

Our evolution

Product

Solutions

Industry

Core

Applied

paloalto NETWORKS

行业相关的App-ID的区别

- 展示我们如何保证客户关心的应用
- 行业的App-ID的展示我们的独特之处更好地
- 我们可以提供极具吸引力的技术演示：
  - 行业了解
  - 基本ACC的演示
  - 和行业相关应用的演示

paloalto NETWORKS

BY INDUSTRY

Cybersecurity impacts every industry in different ways. One constant is the ongoing pressure
new systems, applications, and devices. How can you enable change and deploy innovative
on time and on budget but without compromising your security?

Our network security solutions give you full visibility and control over all traffic based on appli
protocols, users, and content - even in the most remote and specialized corners of your netw
Alto Networks, you can better manage and protect the complex and ever-evolving ecosystem
technologies upon which your industry relies.

On our web site 5 industries

GOVERNMENT

The unabated rise of cyberthreats targeting governments and critical infrastructure has made protecting networks and information systems a strategic priority for governments worldwide. Adopting new applications and innovative technologies to remain competitive is a must, but they bring new vulnerabilities and add complexity and new challenges to your network security.

LEARN MORE >

HEALTHCARE

Like many of your peers in the healthcare industry, you might be going through a technology revolution to improve efficiencies and to satisfy new regulations. Palo Alto Networks can help. Our next-generation firewalls allow you to define and enforce the acceptable use of new technologies and applications on your network. Regardless of the state of your network, you can easily and safely transition to our security platform and rapidly improve your cybersecurity posture.

LEARN MORE >

SCADA & INDUSTRIAL CONTROL

Insufficient security and unpatched, highly vulnerable legacy systems combined with a more sophisticated threat landscape targeting critical infrastructure, has made improving cybersecurity in SCADA/ICS networks more important than ever. Palo Alto Networks unique approach to network traffic control, threat prevention, and central management protects your key infrastructure from cyberthreats and ensures network availability.

LEARN MORE >

EDUCATION

FINANCIAL SERVICES

谢谢！

Q&A

paloalto NETWORKS

the network security company™

与众不同

根本全新的网络安全

App-ID

识别应用

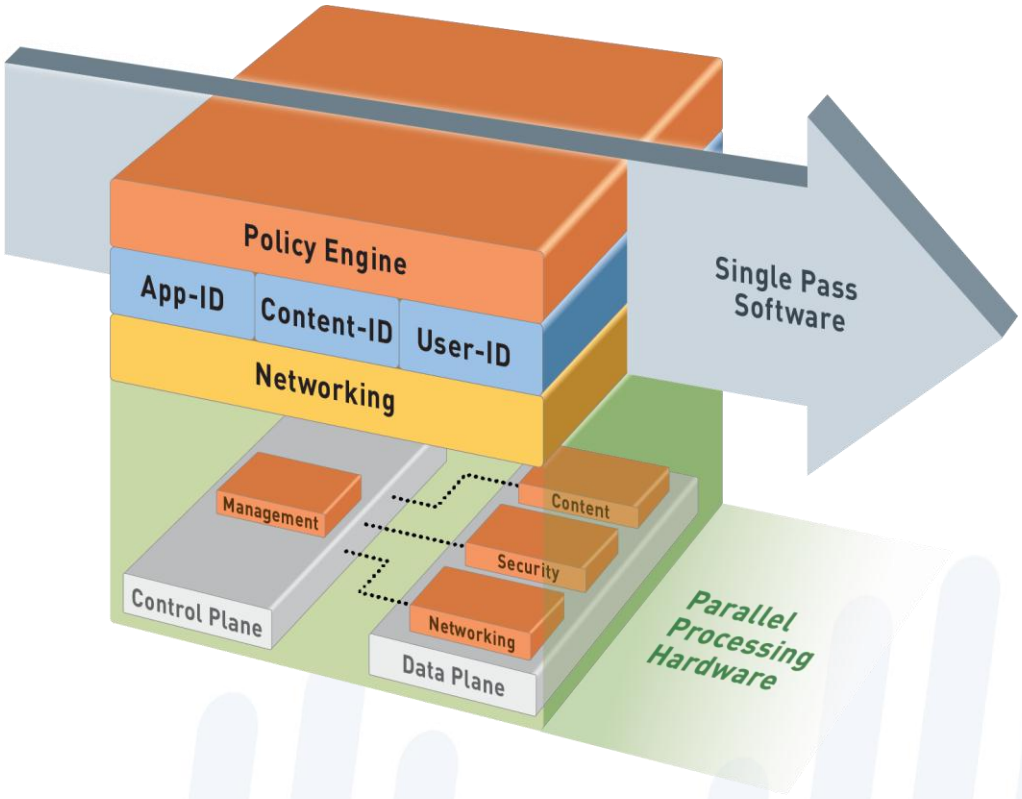
Content-ID

扫描内容

User-ID

识别用户

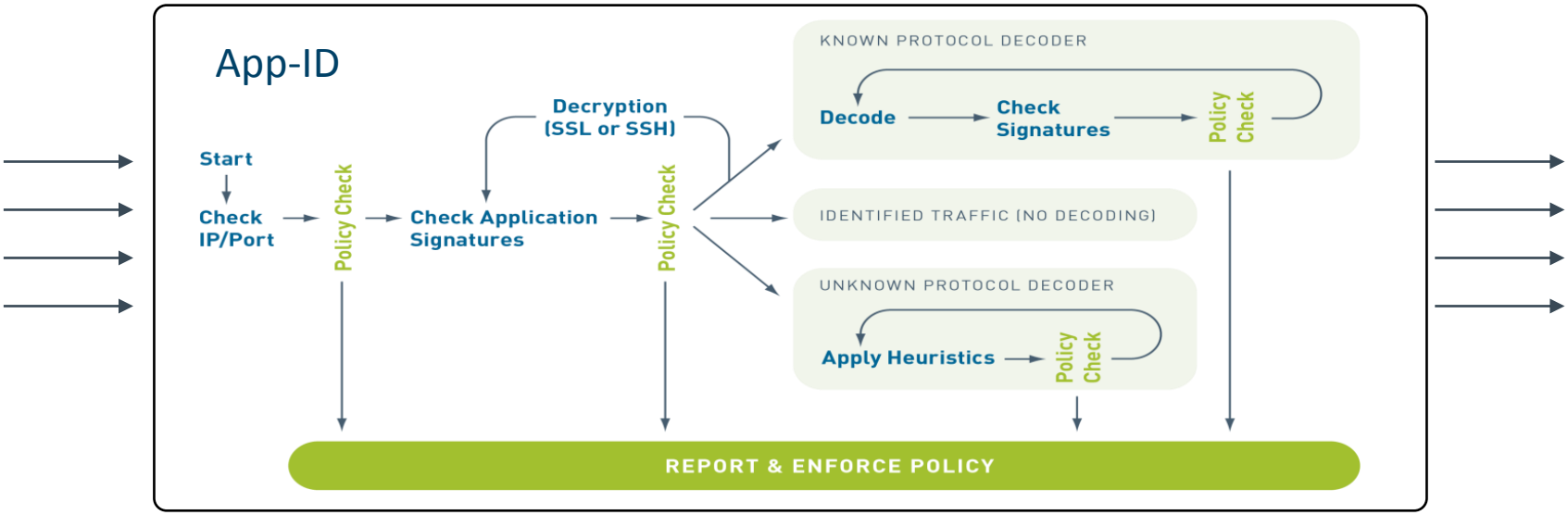
Palo Alto Networks Platform



1
App-ID

App-ID =应用启用

一个单一的分类机制;一个单一的启用策略

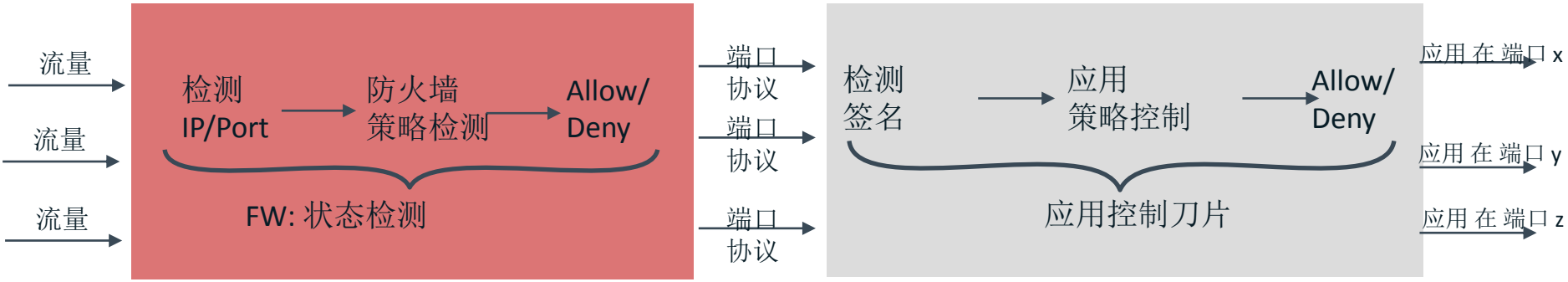


- 总是第一个动作，始终处于启用状态，始终跟踪状态
- 所有的流量，所有的应用程序，所有的端口

首先识别应用程序是安全地启用应用程序的唯一途径

paloalto NETWORKS

状态检测+ 应用控制



过程#1; 防火墙策略决策

过程 #2; 应用策略控制决策

所有其他在此协议中的应用是被允许

附加实现方案面临问题....

- 允许的协议中其他应用程序通过
- 使用非标准端口或包括非标准端口(SSL, SSH, MySQL, Telnet)
- 故意逃避的的应用
- 策略的优先级 和 协调一致

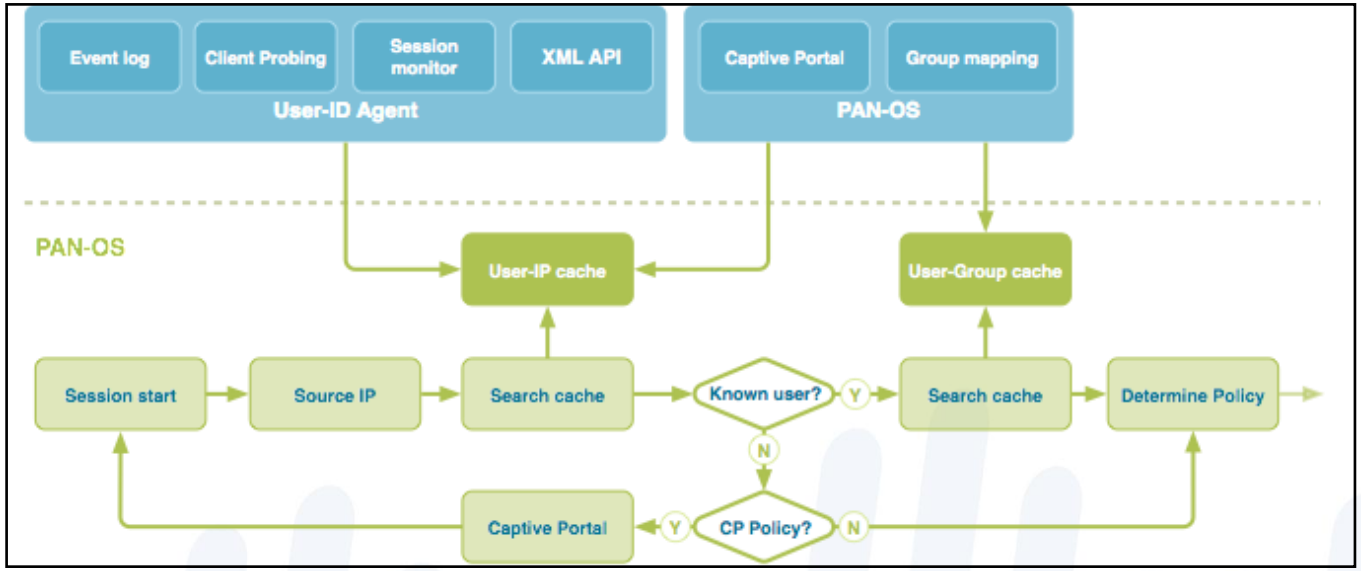
App-ID vs. 其他品牌

	Palo Alto Networks	Cisco	Juniper	Fortinet	Check Point
始终启用 app-ID吗?	Yes	No	No	No	No
缺省针对所有端口吗?	Yes	No	No	No	No
单策略控制吗?	Yes	No	No	No	No
应用 = 正向控制?	Yes	No	No	No	No
统一的策略?	Yes	No	No	No	No
是否对未知应用分类?	Yes	No	No	Yes	No
客户化应用签名?	Yes	No	No	No	No
应用替换?	Yes	No	No	No	No

2
User-ID

User-ID: 所有用户, 所有平台

- 主要区别
  - 支持市场上最广泛的目录系统
  - 单一的，整合在一起代理程序对所有用户目录服务
  - Microsoft Exchange 和 XML API 获得非Windows用户信息
  - XML API 用于和非标准系统客户化集成



User-ID vs. 其他品牌

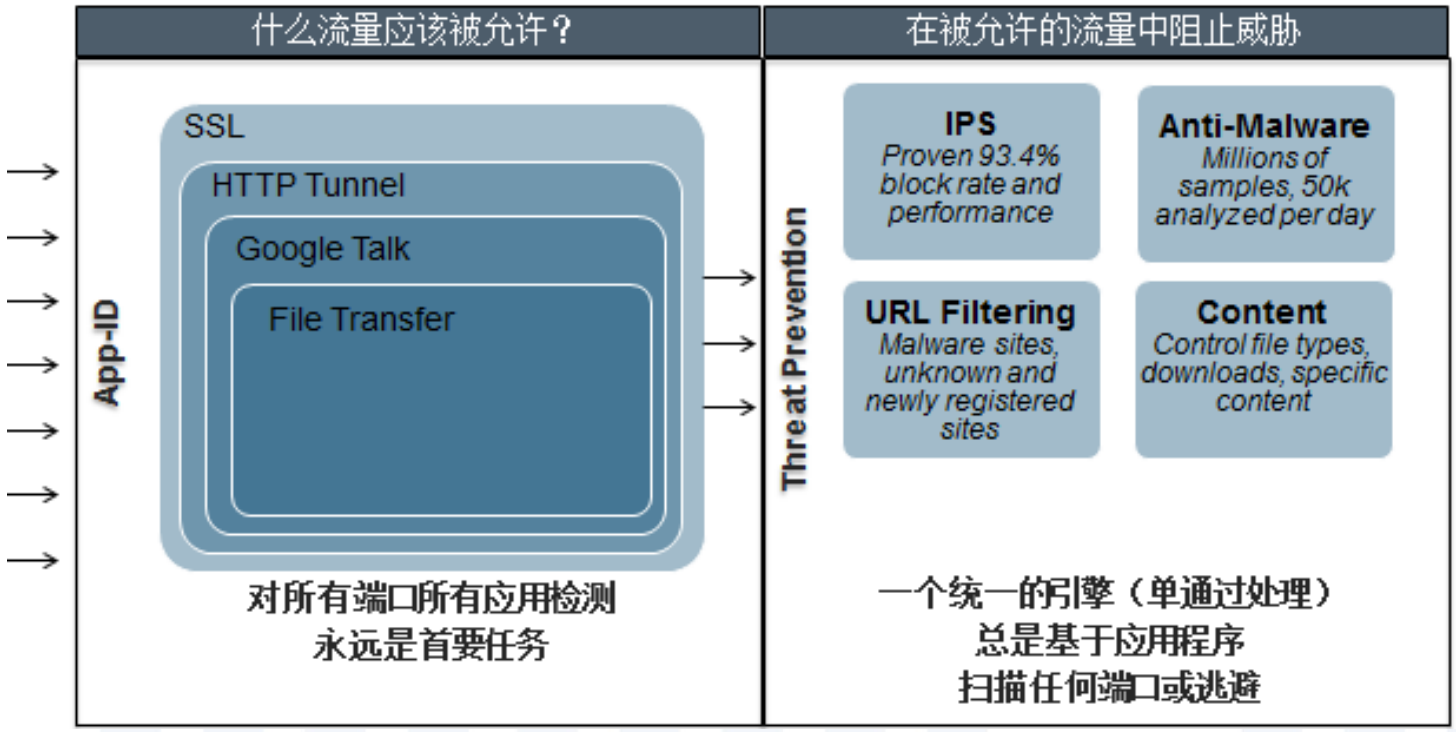
	Palo Alto Networks	Cisco	Juniper	Fortinet	Check Point
Active Directory	Yes	Yes	No	Yes	Yes
LDAP	Yes	No	No	Yes	No
eDirectory	Yes	No	No	No	No
Citrix	Yes	No	No	No	No
Microsoft TSE	Yes	No	No	No	No
Microsoft Exchange	Yes	No	No	No	No
XML API	Yes	No	No	No	No
Proven in production since 2008	Yes	2011	???	2010	2011

paloalto NETWORKS

3
Content-ID

Content-ID: 应用的保护

- 主要区别
  - 和流量分类引擎（App-ID）紧密关联
  - 始终检测基于应用程序和用户的威胁
  - 端口和协议无关的
  - 基于流扫描的引擎，统一的签名格式=通过一次处理→检测和拦截各种形式的威胁



Content-ID vs. 其他

	Palo Alto Networks	Cisco	Juniper	Fortinet	Check Point
威胁策略控制-基于应用	Yes	No	No	No	No
单通过引擎（拆解包）	Yes	No	No	No	No
一次通过阻止 病毒, 漏洞, 间谍软件, 恶意软件	Yes	No	No	No	No
实际性能标称数值匹配	Yes	No	No	No	No

WildFire: 现代恶意软件防护

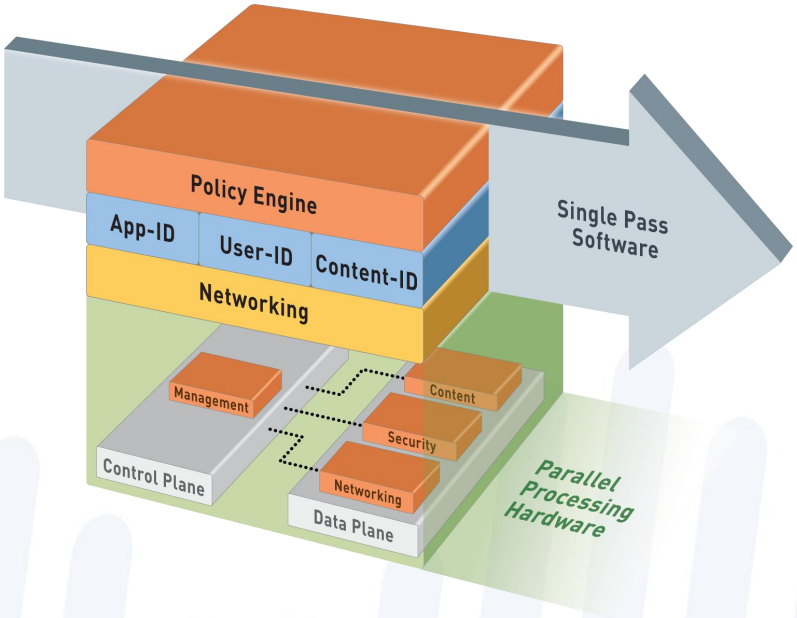
- 主要区别
  - 没有其他的防火墙供应商有类似的东西!

4

规格评估规则

平台：可保证的性能

- 主要区别
  - 一次通过处理的软件，设计用于持续对7层数据进行分析
  - 平台特有设计加速7层的分析
  - 高速背板上的专用功能处理器（安全性，网络，威胁，管理）



不同对 硬件/ 性能 理念 –性能功能评估

	Palo Alto Networks	Others
性能测试理念	向潜在客户提供切合实际的指标	吞吐量最大化
处理	专用功能处理器	通用CPU或 CPU加速的ASIC
深度	7层分析和检测	4层分析和检测
性能标称?	HTTP 64k	UDP 1518 或 512
防火墙策略	启用App-ID	启用状态检测
应用控制性能发布?	Yes	No
应用控制 + 威胁防护性能发布?	Yes	No

paloalto NETWORKS

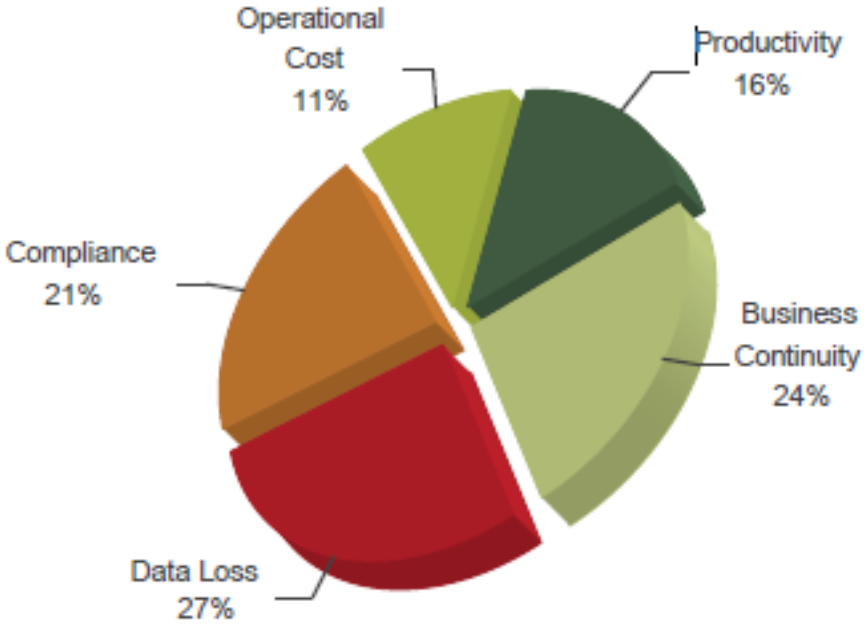
AVR 报告（应用、威胁可视性）

5	ftp	general-internet	file-sharing	client-server	232,193,980	951
5	qq-file-transfer	general-internet	file-sharing	client-server	146,344,787	516
5	bittorrent	general-internet	file-sharing	peer-to-peer	101,735,542	8,347
5	msn-file-transfer	general-internet	file-sharing	peer-to-peer	25,170,896	174
5	flashget	general-internet	file-sharing	peer-to-peer	7,750,952	1,158
5	hotfile	general-internet	file-sharing	browser-based	6,715,750	49
4	qq-download	general-internet	file-sharing	peer-to-peer	3,073,367	893
5	imesh	general-internet	file-sharing	peer-to-peer	2,979,591	63
4	skydrive	general-internet	file-sharing	browser-based	675,168	38
4	4shared	general-internet	file-sharing	browser-based	176,511	3
4	office-live	general-internet	file-sharing	client-server	111,556	4
5	kugoo	general-internet	file-sharing	peer-to-peer	32,680	6
5	webdav	general-internet	file-sharing	browser-based	18,665	6
5	gnutella	general-internet	file-sharing	peer-to-peer	8,082	3
4	web-browsing	general-internet	internet-utility	browser-based	20,648,307,675	543,770
4	flash	general-internet	internet-utility	browser-based	6,798,313,936	18,679
4	mobile-me	general-internet	internet-utility	browser-based	31,107,385	2
5	rss	general-internet	internet-utility	client-server	10,051,799	669
4	apple-appstore	general-internet	internet-utility	client-server	30,507	4
4	atom	general-internet	internet-utility	client-server	21,041	4
5	http-audio	media	audio-streaming	browser-based	592,380,979	1,475
4	itunes	media	audio-streaming	client-server	151,967,582	121
4	pandora-tv	media	audio-streaming	browser-based	82,245	73
5	tudou	media	photo-video	browser-based	1,624,626,968	1,260
5	youku	media	photo-video	browser-based	817,891,676	1,191

paloalto NETWORKS

高风险应用导致的业务风险

- 应用程序文件传输会导致数据泄漏；
- 逃逸或传递其他应用程序的能力可导致合规性的风险；
- 高带宽消耗相当于增加运营成本，
- 而易受恶意软件和漏洞攻击的应用程序可引入业务连续性风险。



最高风险应用程序的业务风险细分。

SharePoint被看到

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

paloalto NETWORKS

谢谢！

Q&A

paloalto NETWORKS

the network security company™