Palo alto Networks
新一代安全平台及安全解决方案

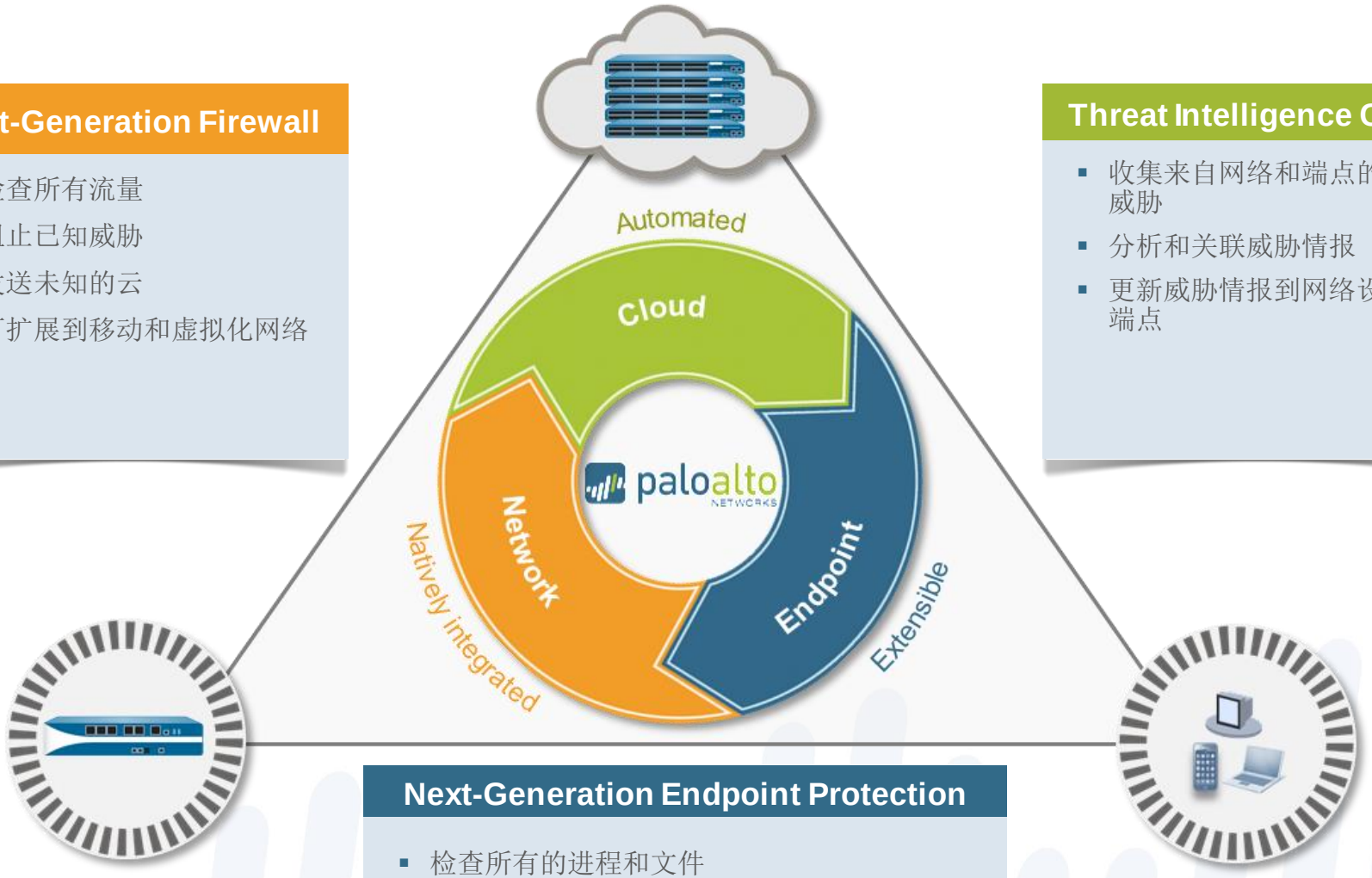
金志勇

paloalto NETWORKS
the network security company™

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

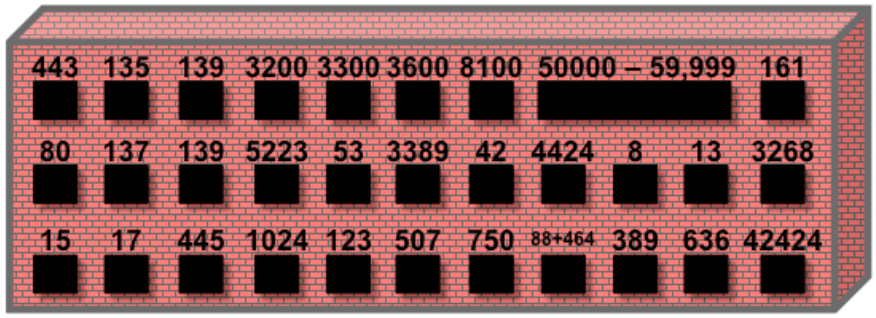
Next-Generation Endpoint Protection

- 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

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
- Palo Alto Networks的下一代网络安全平台
- 企业的下一代网络安全应当如何考虑

什么样的安全防护才是您想要的？



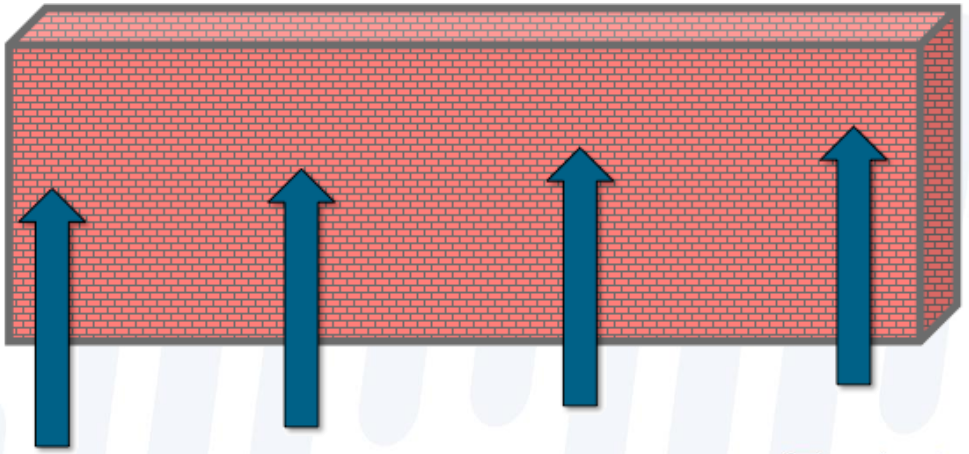
SharePoint
80, 443, 135, 137, 139

SAP
3200, 3300, 8000, 3600, 8100, 50013, 50014, 65000

Lync
443, 3478, 5223, 50,000-59,999

Active Directory
3389, 53, 42, 8, 13, 15, 17, 137, 138, 139, 445, 1025, 123, 507, 750, 88+464, 389, 636, 3268, 445, 161, 162, 42424, 691, 1024-65535

网络任何位置保持高标准的应用安全水平



SharePoint SAP Lync Active Directory

 ©2014, Palo Alto Networks. Confidential and Proprietary.

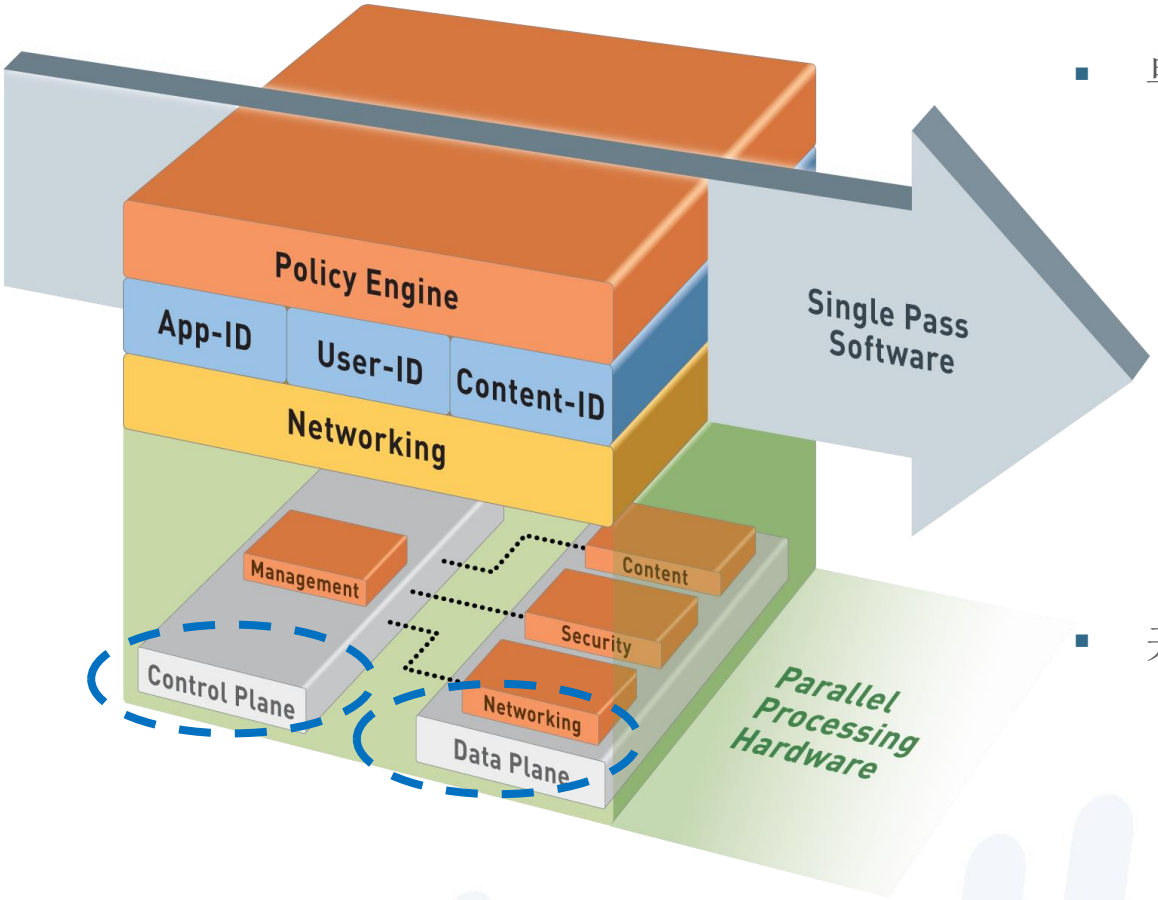
颠覆传统的
下一代防火墙设计

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

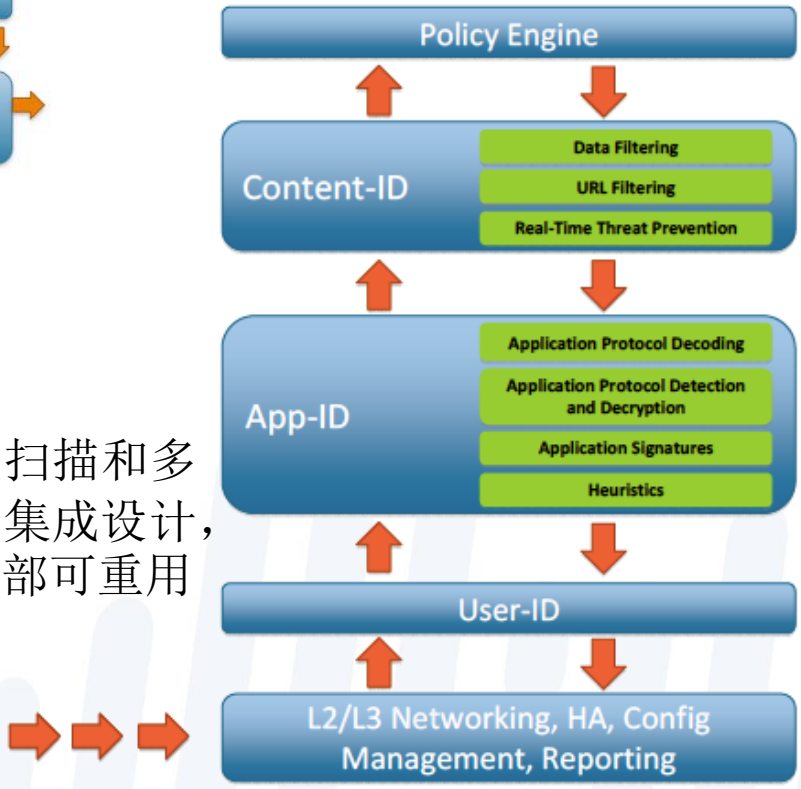


- 单通道处理
  - 数据包一次操作
    - 流量分类 （应用识别)
    - 用户/组 对应
    - 内容扫描 – 病毒，间谍软件，等威胁
  - 而且仅仅执行单一策略
- 并行处理技术
  - 特定功能的并行处理硬件引擎
  - 独立的数据/控制平面

高达120Gbps(App-ID)，微秒级低延时

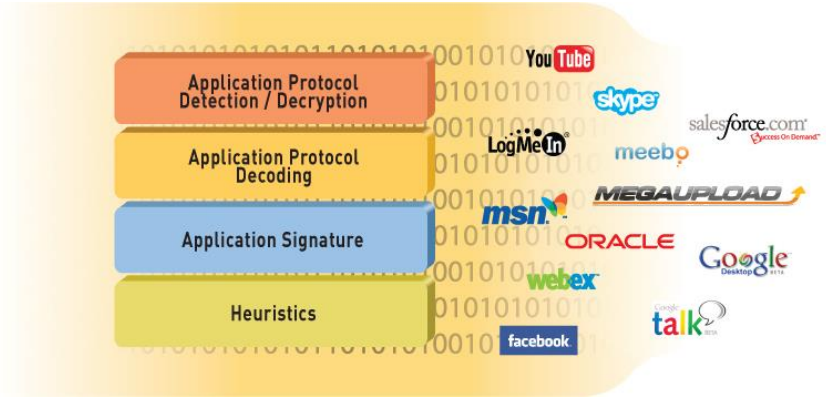
采用与传统厂商不同的扫描方式

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

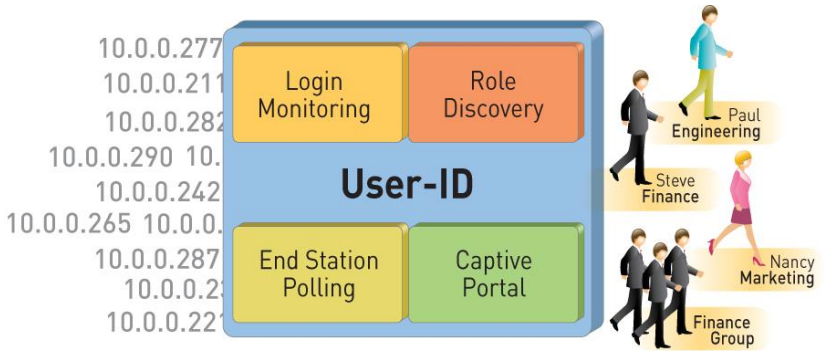


NGFW最核心的差别
识别技术—提升现有安全

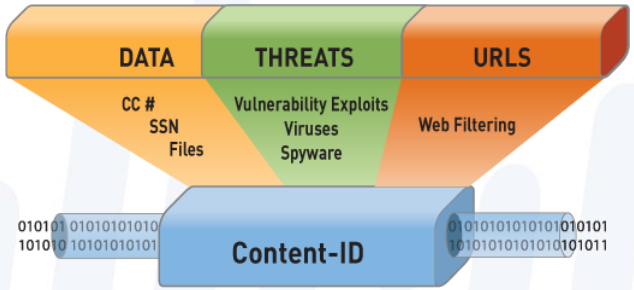
App-ID™
识别应用—提升端口识别



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

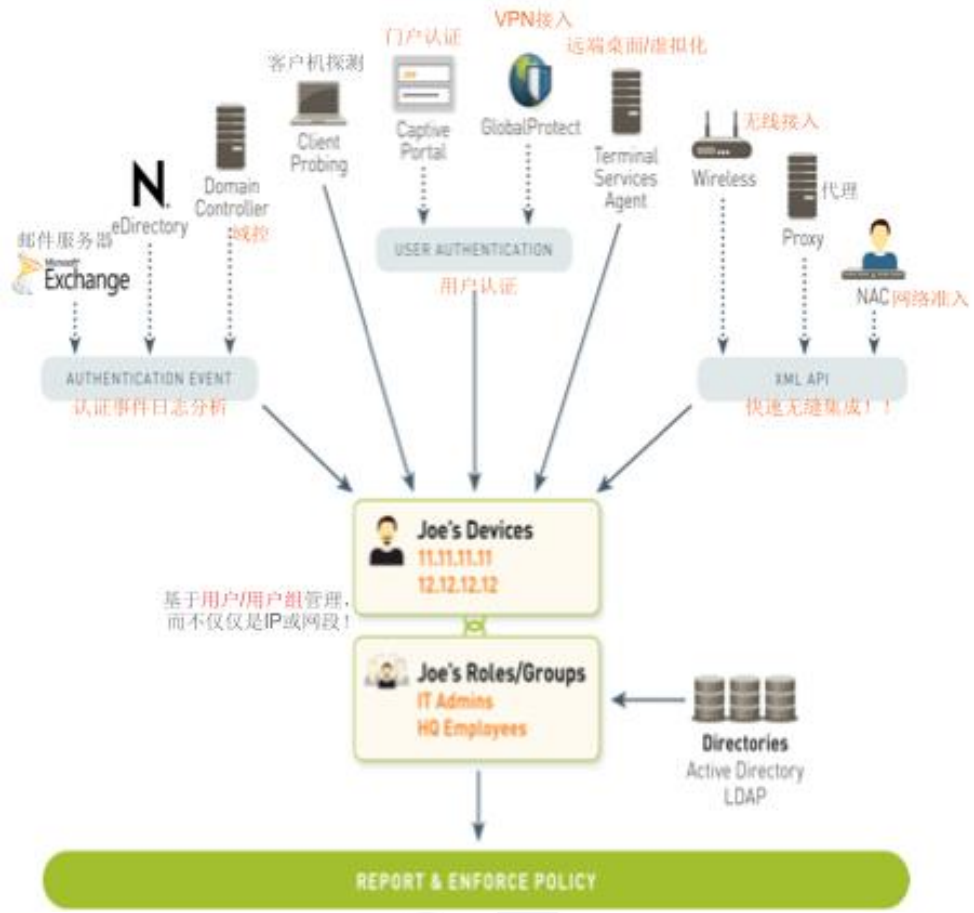


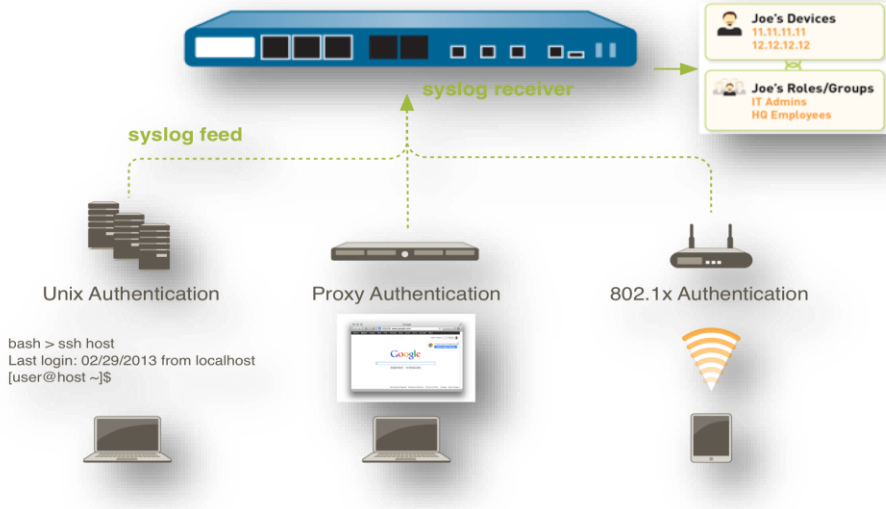
App-ID：采用应用协议而非服务端口进行控制

策略决策

User-ID基于用户角色的识别与控制

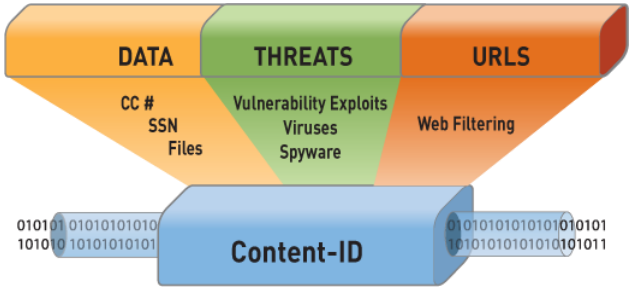
全网基于用户策略



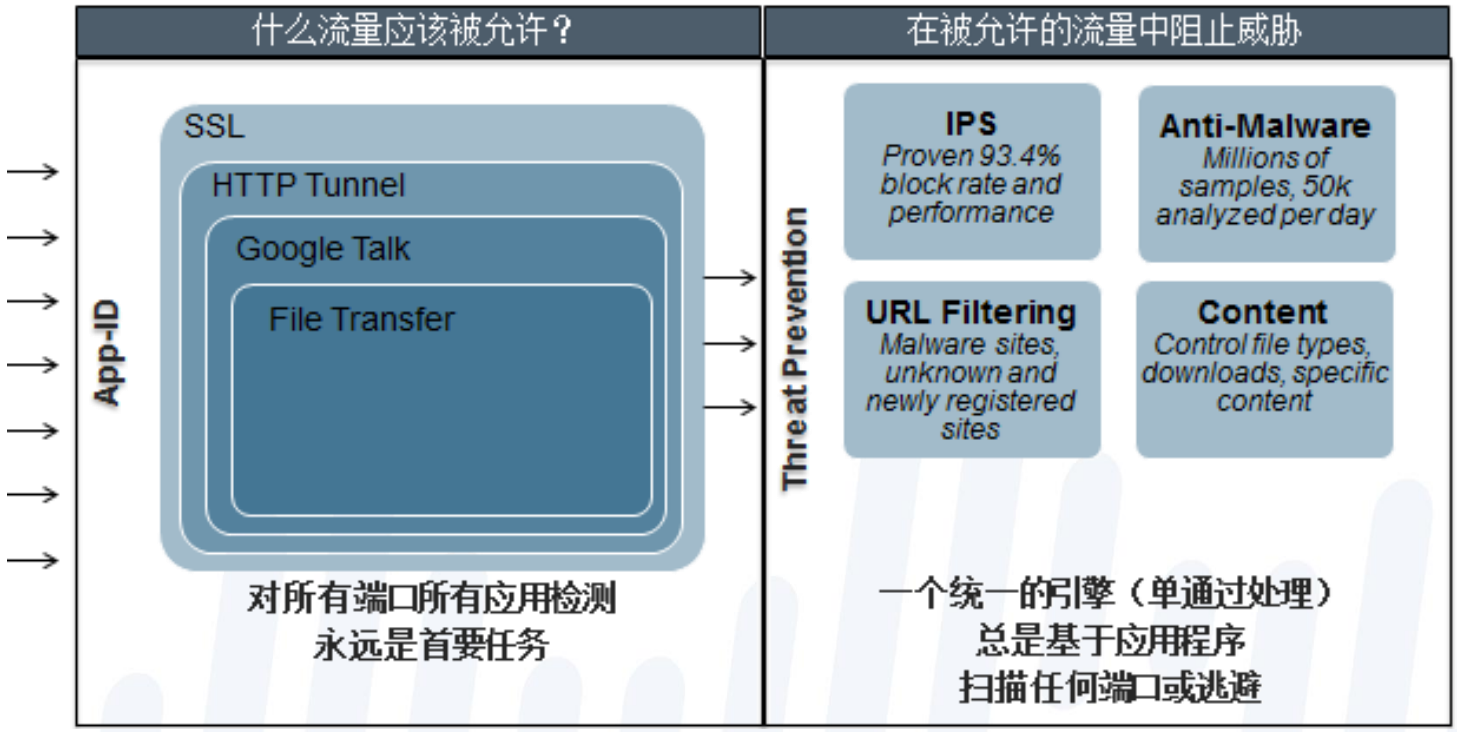


- Syslog接收器可以与大量现有无线控制器，代理，NAC准入方案整合
  - 原生支持BlueCoat Proxy, Citrix Access Gateway, Aerohive AP, Cisco ASA, Juniper SA NetConnect, Juniper Infranet Controller
- 借助XML API仍可与其他方案结合

Content-ID: 应用的内容保护



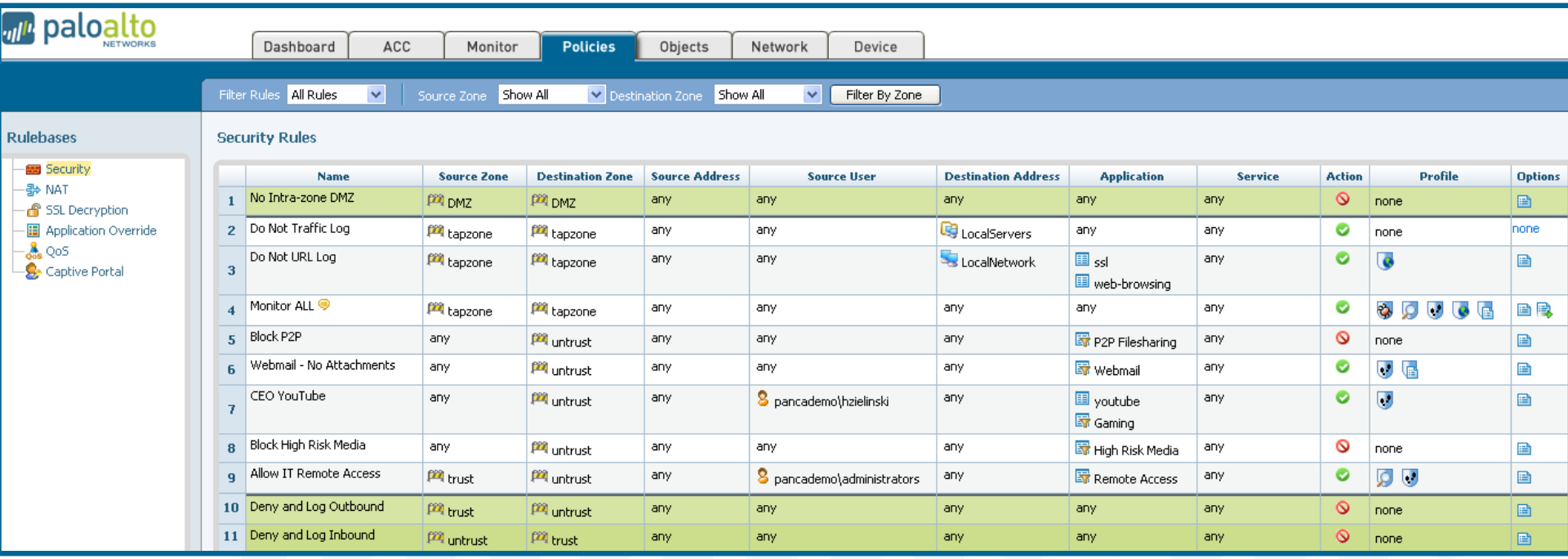
- 主要区别
  - 和流量分类引擎（App-ID）紧密关联
  - 始终检测基于应用程序和用户的威胁
  - 端口和协议无关的
  - 基于流扫描的引擎，统一的签名格式=通过一次处理→检测和拦截各种形式的威胁



灵活的策略控制响应

- 直观式策略编辑器可利用灵活策略响应执行适当的使用策略

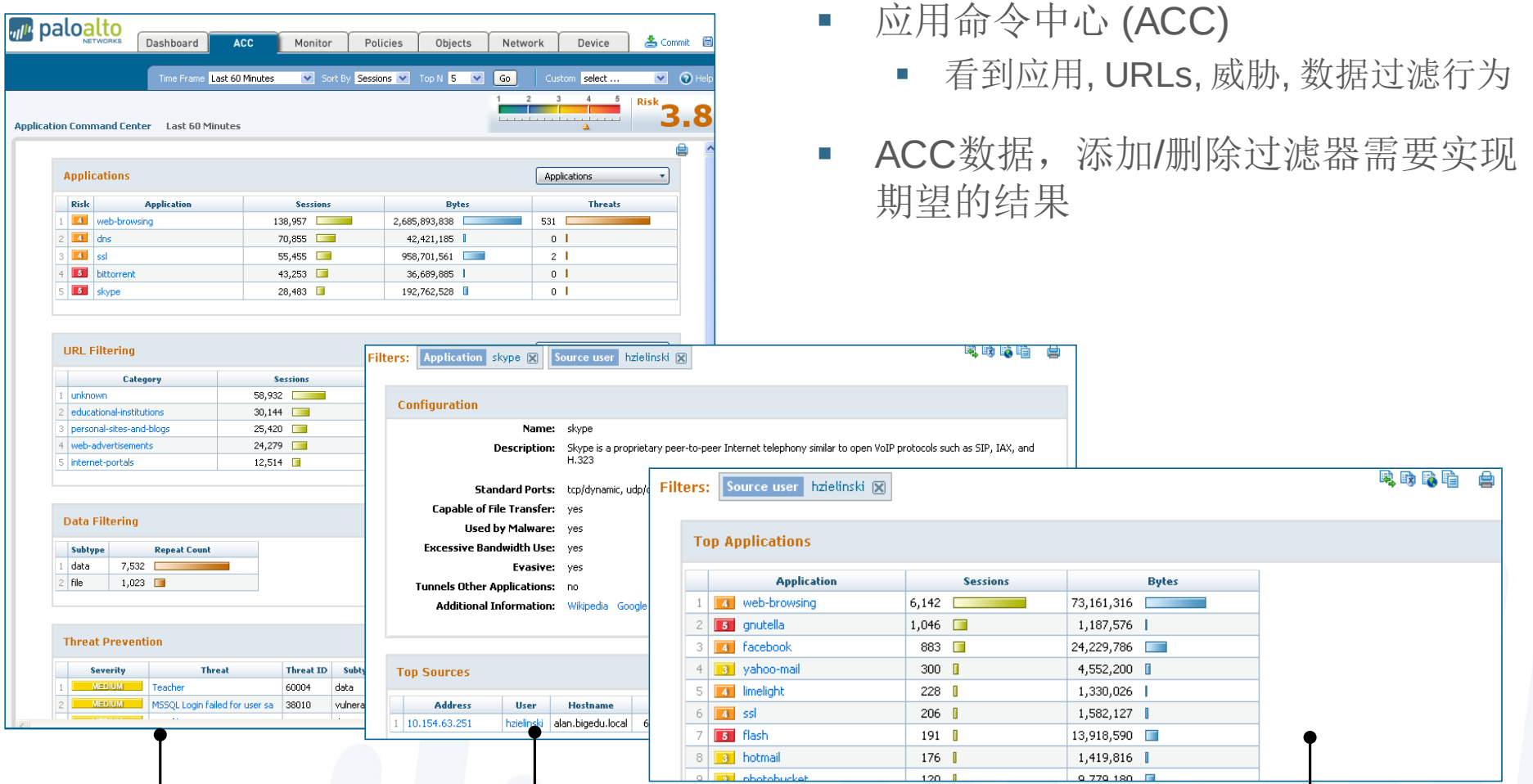
• 允许或拒绝个别应用程序的使用	• 允许但应用IPS策略，进行病毒与间谍软件扫描
• 根据类、子类、技术或特性控制应用程序	• 应用流量整形（保障型、优先型与最高整形能力）
• 解密并检查SSL	• 允许AD中的某类用户或群组
• 允许或阻止某类应用功能	• 控制过多网络浏览
• 根据调度允许流量通过	• 查看、警惕或阻止文件或数据传输



	Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action	Profile	Options
1	No Intra-zone DMZ	DMZ	DMZ	any	any	any	any	any		none	
2	Do Not Traffic Log	tapzone	tapzone	any	any	LocalServers	any	any		none	none
3	Do Not URL Log	tapzone	tapzone	any	any	LocalNetwork	ssl web-browsing	any			
4	Monitor ALL	tapzone	tapzone	any	any	any	any	any			
5	Block P2P	any	untrust	any	any	any	P2P Filesharing	any		none	
6	Webmail - No Attachments	any	untrust	any	any	any	Webmail	any			
7	CEO YouTube	any	untrust	any	pancademo\hzielinski	any	youtube Gaming	any			
8	Block High Risk Media	any	untrust	any	any	any	High Risk Media	any		none	
9	Allow IT Remote Access	trust	untrust	any	pancademo\administrators	any	Remote Access	any			
10	Deny and Log Outbound	trust	untrust	any	any	any	any	any		none	
11	Deny and Log Inbound	untrust	trust	any	any	any	any	any		none	

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



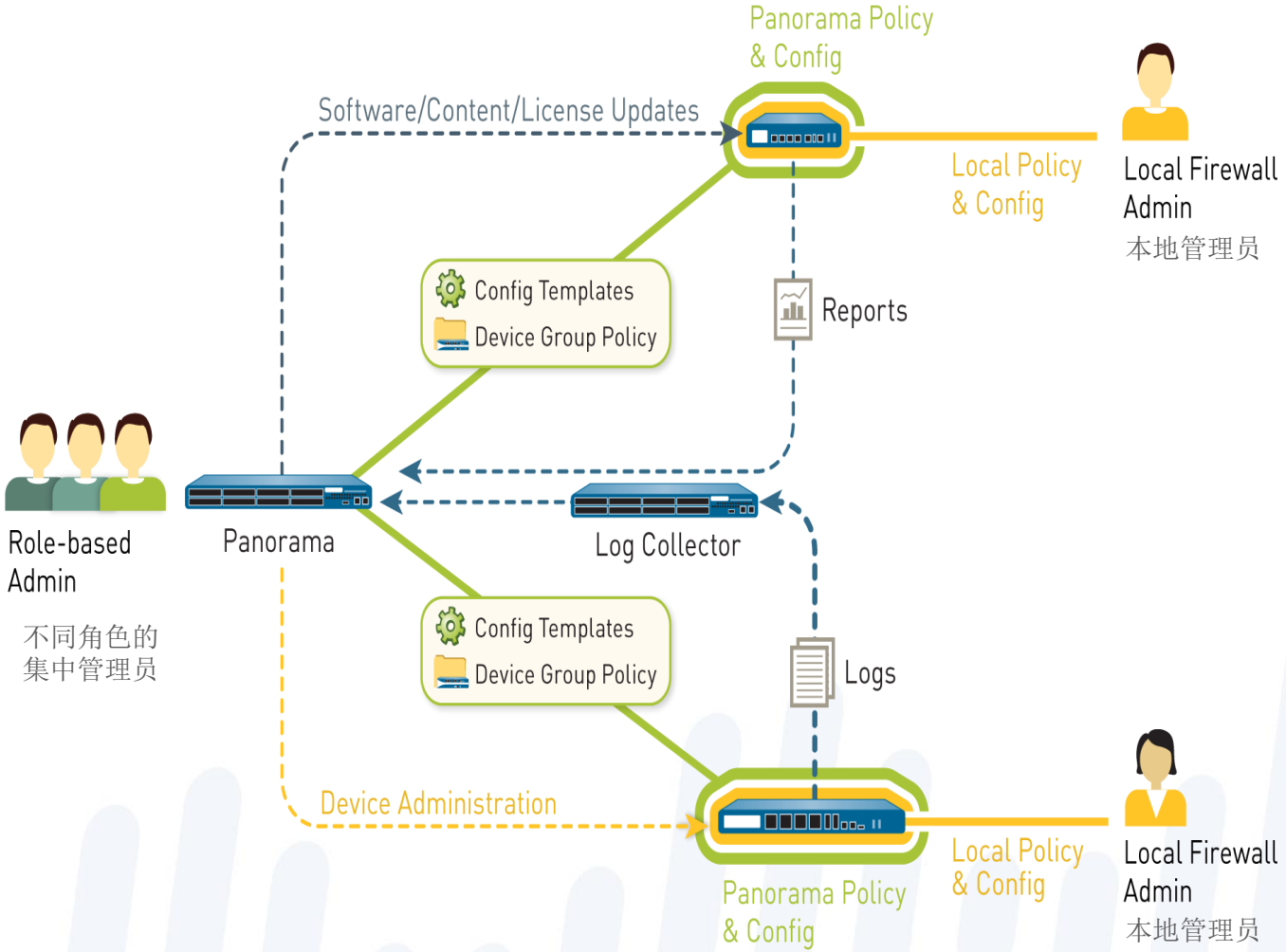
Skype过滤

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
- Palo Alto Networks的下一代网络安全平台
- 企业的下一代网络安全应当如何考虑

APT与现代威胁防护

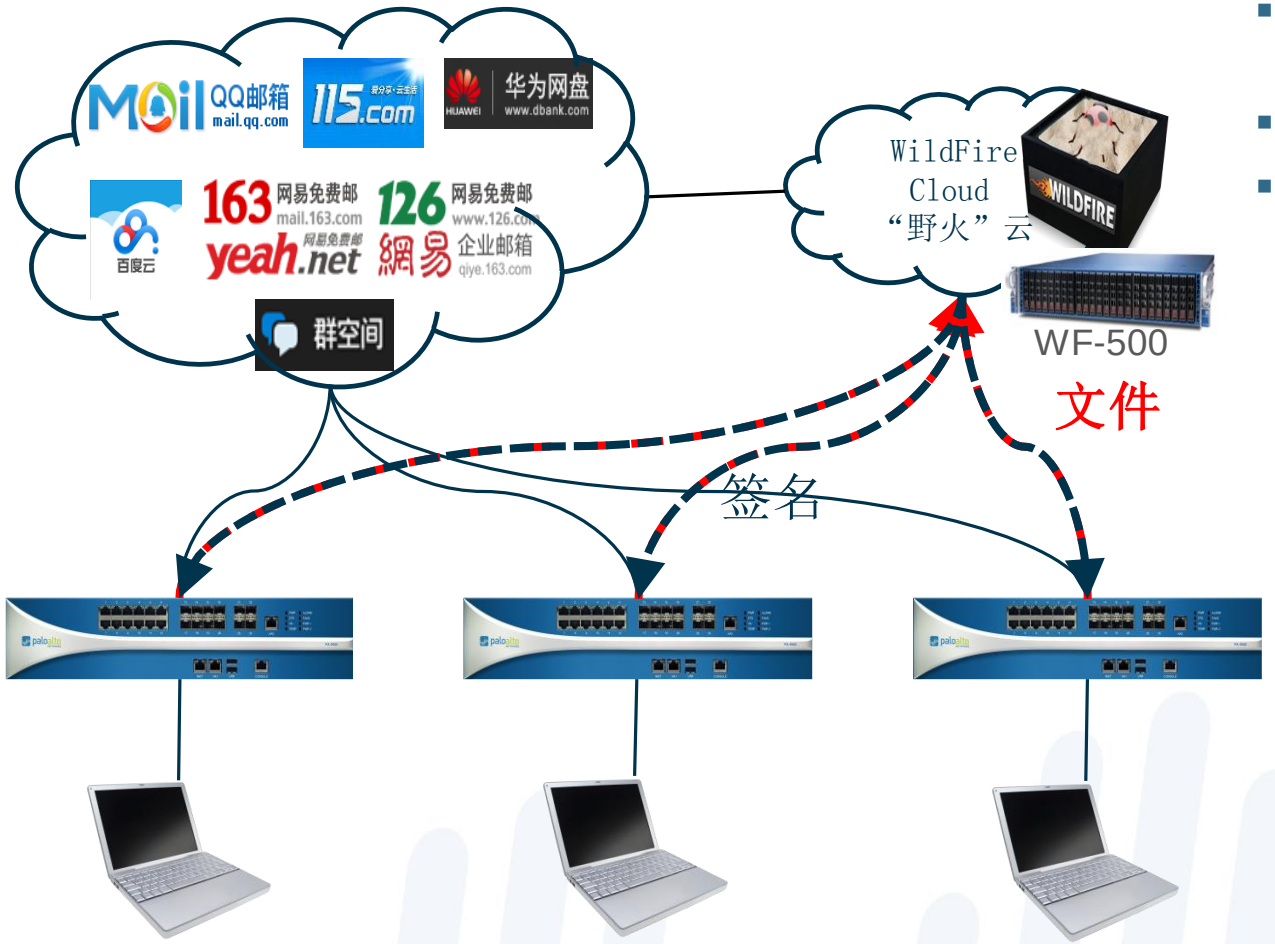
paloalto NETWORKS

	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

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

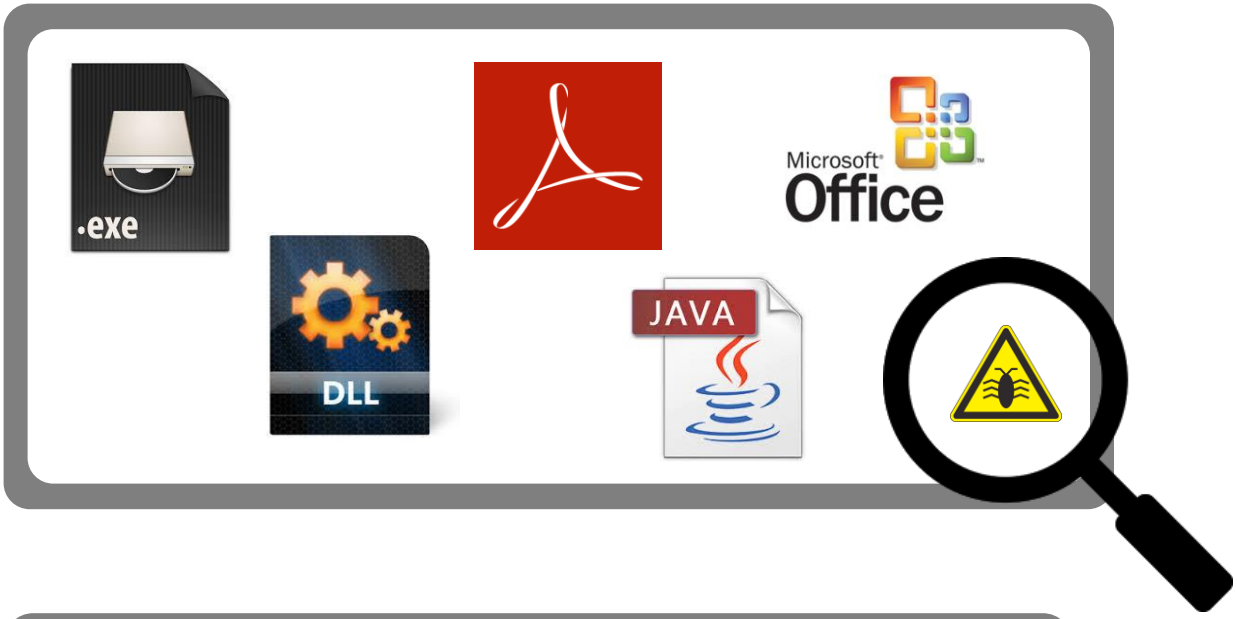
❶互联网下载可疑文件

❷转到WildFire作行为分析

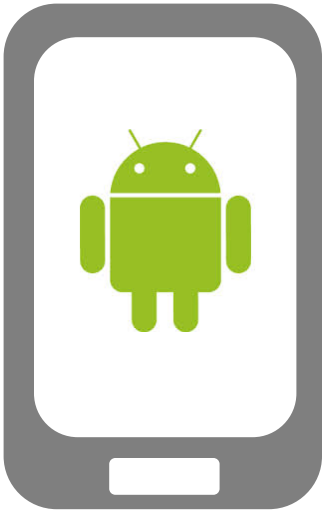
❸所有客户得到保护

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

阻断“未知后门程序”上传到门户/交易网站

对恶意脚本地址尝试访问暴露出隐藏的已注入木马

WildFire检测未知恶意软件（续）—阻断“未知后门程序”

This virtual machine is configured with the following software: **Windows XP SP2**.

BEHAVIORAL SUMMARY

This sample was found to be **malware** on this virtual machine.

Behavior	
Created a file in the Windows folder	创建目录
Created or modified files in the Windows system folder	创建篡改文件
Created or modified files	篡改注册表
Modified Windows registries	派生进程
Spawned new processes	

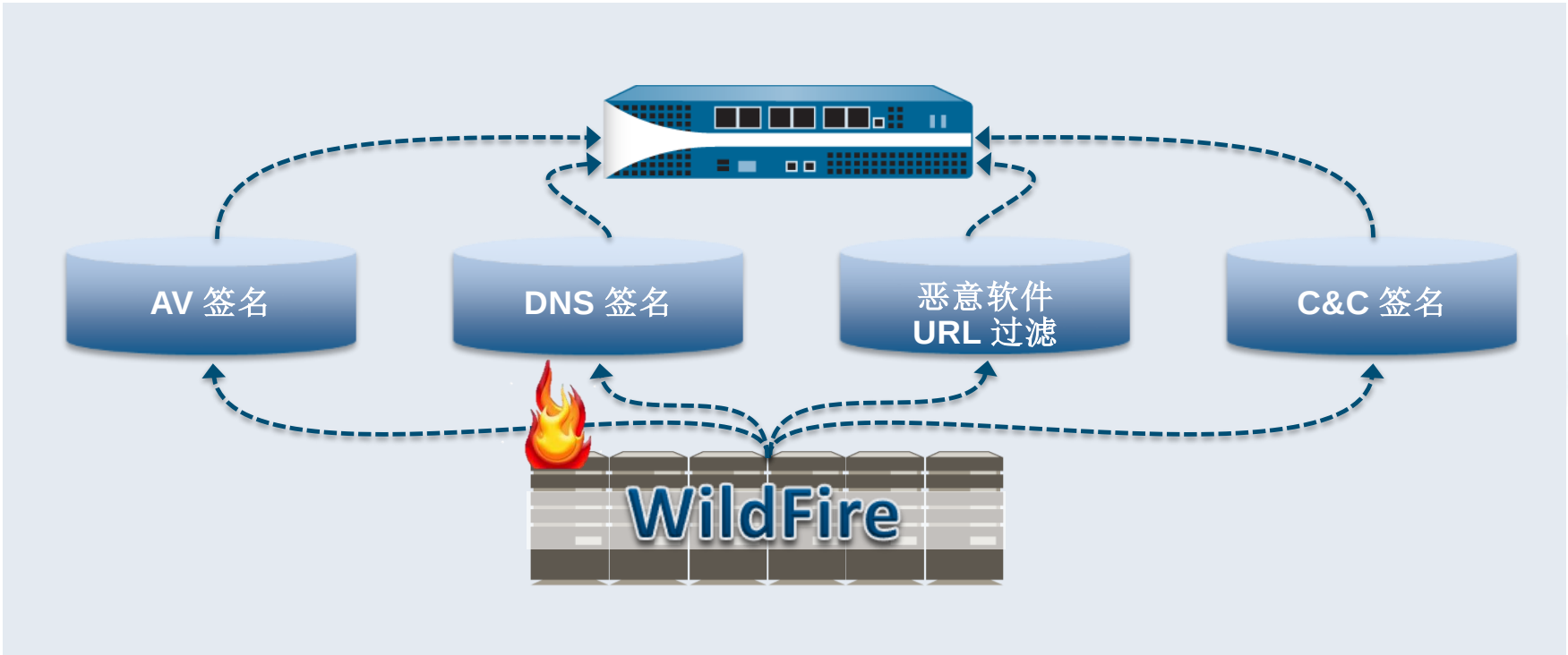
HOST ACTIVITY

REGISTRY ACTIVITY

Registry Key	Action
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Directory	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Paths	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path1\CachePath	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path2\CachePath	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path3\CachePath	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path4\CachePath	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path1\CacheLimit	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path2\CacheLimit	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path3\CacheLimit	Set
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path4\CacheLimit	Set
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cookies	Set

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



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
- Palo Alto Networks的下一代网络安全平台
- 企业的下一代网络安全应当如何考虑

应用场景（网关，数据中心等）

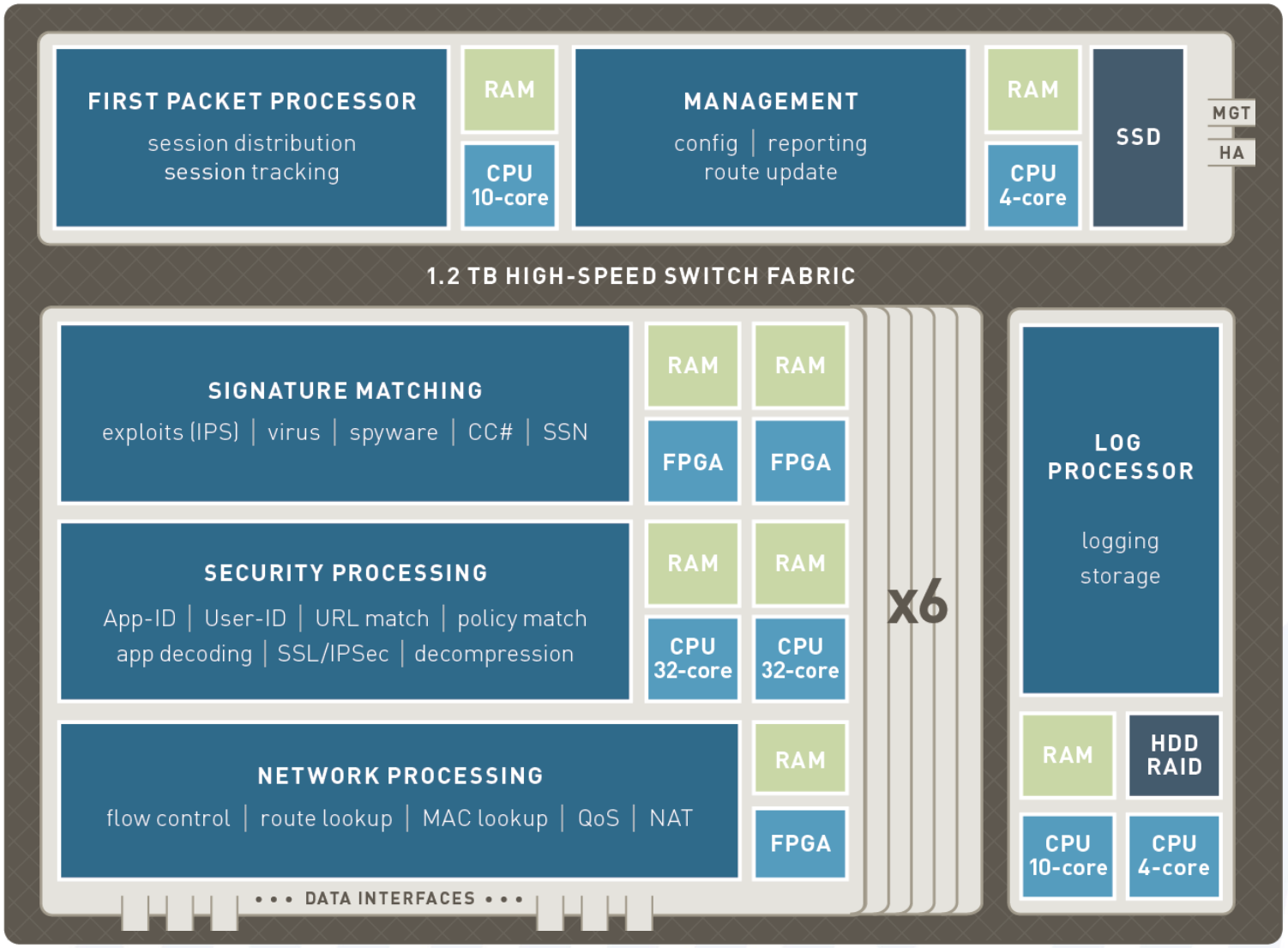
应用程序级攻击日益复杂化，更大的带宽需要可扩展的高性能安全

Internet Gateway	• 确保所有用户在所有设备上安全 • 需求 10+ Gbps
Data Center	• 确保所有的应用程序，控制所有用户访问与设备 • 需求 20+ Gbps
Network Segmentation	• 保护内部资源 • 需求 20-40+ Gbps

PA-7050: 最快的下一代防火墙

- 安全地启用所有的应用程序，全新一代防火墙功能
- 突破性的应用层性能
- 简单，灵活的机箱架构

可扩展的专用体系结构


FIRST PACKET PROCESSOR
session distribution
session tracking
RAM
CPU
10-core
MANAGEMENT
config | reporting
route update
RAM
CPU
4-core
SSD
MGT
HA
1.2 TB HIGH-SPEED SWITCH FABRIC
SIGNATURE MATCHING
exploits (IPS) | virus | spyware | CC# | SSN
RAM
RAM
FPGA
FPGA
SECURITY PROCESSING
App-ID | User-ID | URL match | policy match
app decoding | SSL/IPSec | decompression
RAM
RAM
CPU
32-core
CPU
32-core
NETWORK PROCESSING
flow control | route lookup | MAC lookup | QoS | NAT
RAM
FPGA
x6
DATA INTERFACES
LOG
PROCESSOR
logging
storage
RAM
HDD
RAID
CPU
10-core
CPU
4-core

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
- Palo Alto Networks的下一代网络安全平台
- 企业的下一代网络安全应当如何考虑

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

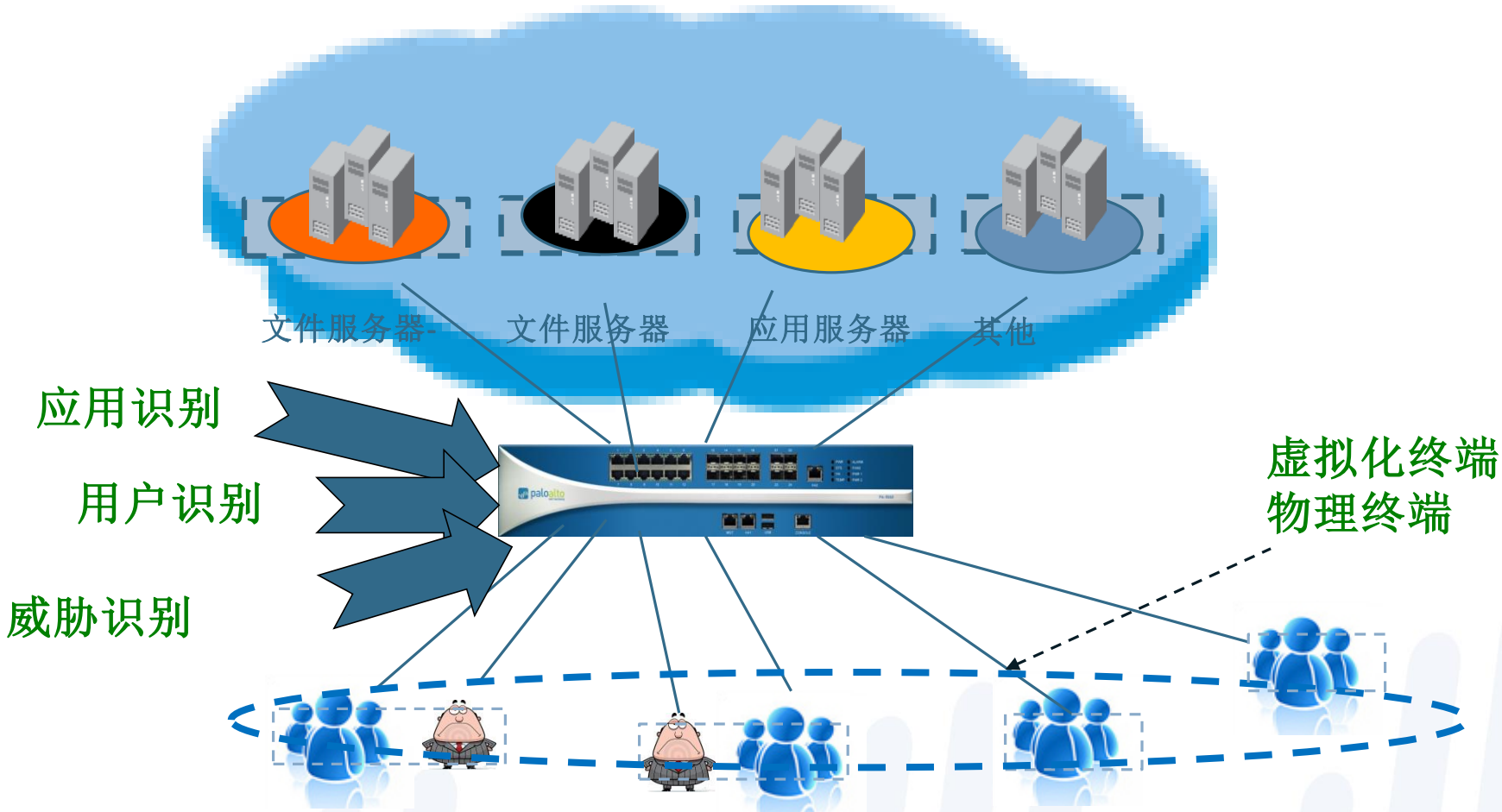
- 网络分割
  - 基于应用和用户，而非端口及IP
- 简单，灵活的网络安全
  - 可与各类数据中心设计集成
  - 高可用性，高性能
- 威胁防御

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

paloalto NETWORKS

关键业务威胁防护 （基于应用/用户）-如关键服务群



- 可以根据不同的终端、用户账号规划对服务区访问权限—基于应用的控制
- 内部不同安全等级服务器隔离（同时—应用、威胁保护）
- 提供基于应用、用户、威胁分析报告

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

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

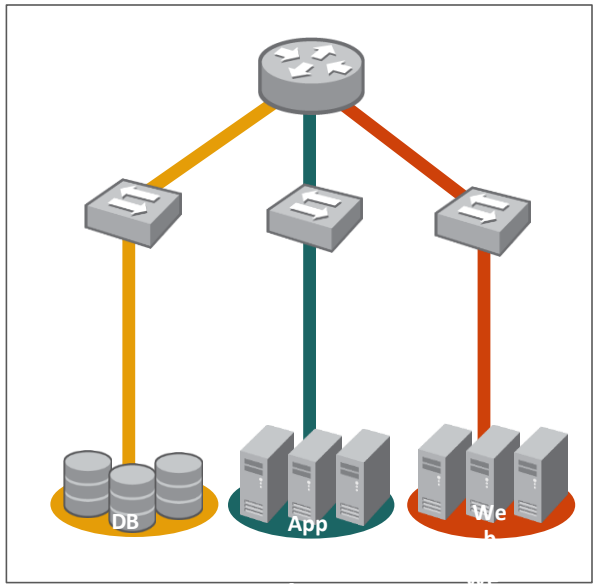
PA-500

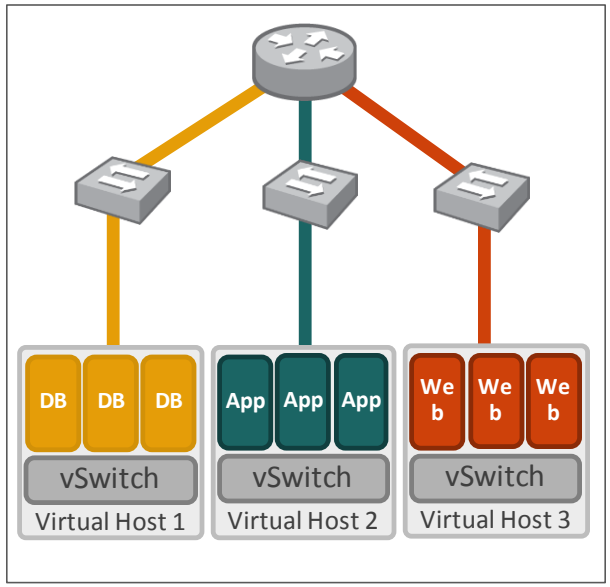
250 Mbps FW/100 Mbps threat prevention/64,000 sessions
8 copper gigabit

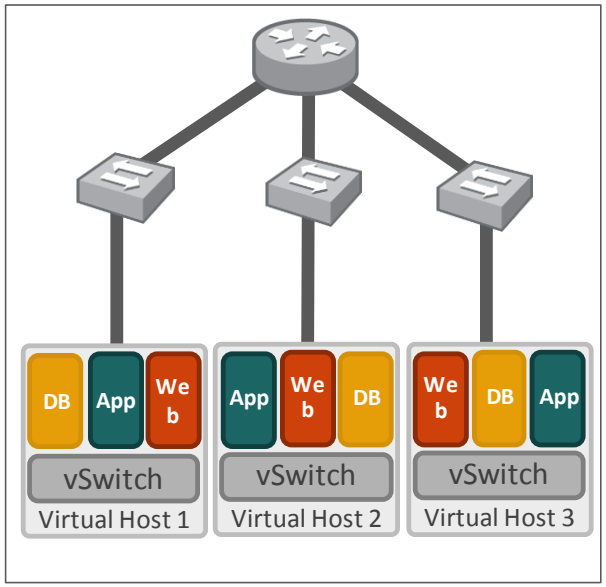
PA-200

100 Mbps FW/50 Mbps threat prevention/64,000 sessions
4 copper gigabit

虚拟化





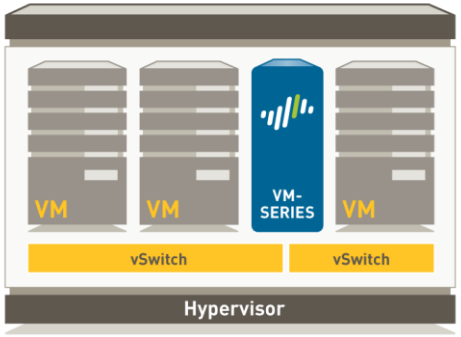


传统数据中心	虚拟数据中心	云（私有/公共）
• 专用应用程序服务器	• 每个服务器多个应用	• IT 即服务
• 服务器使用率 = 15%	• 提高运营效率	• 按需服务
• 横跨流量	• 提高服务器利用率	• 自动化和编排化

业务灵活性 Vs 节省成本 Vs 安全

虚拟化部署的选择

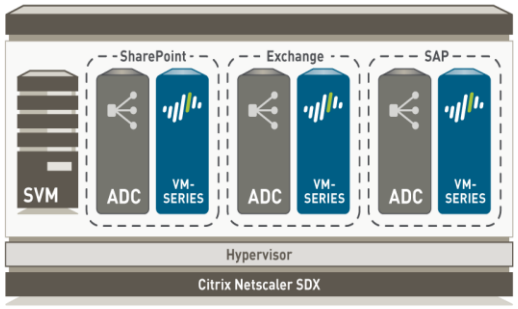
VM-Series for VMware vSphere (ESXi)



- 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

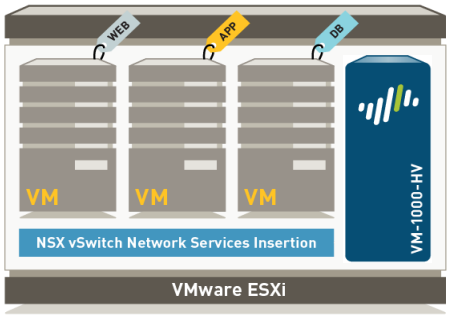
VM-Series for Citrix NetScaler SDX



- 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

Key Takeaway

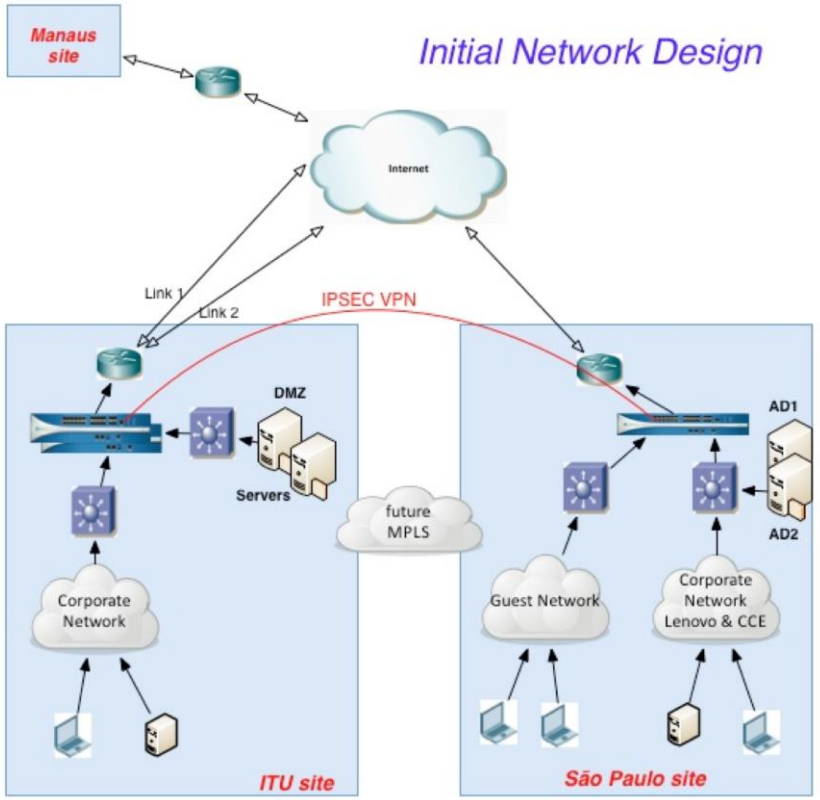
从边界到数据中心

1. 全网流量可视化
2. 全流量威胁防护
3. 基于用户、应用的策略管控
4. 新一代数据中心、虚拟化安全解决方案
5. 丰富的API，支持多样化自定义使用场景
6. 多途径安全接入

联想集团— 技术领先的安全解决方案

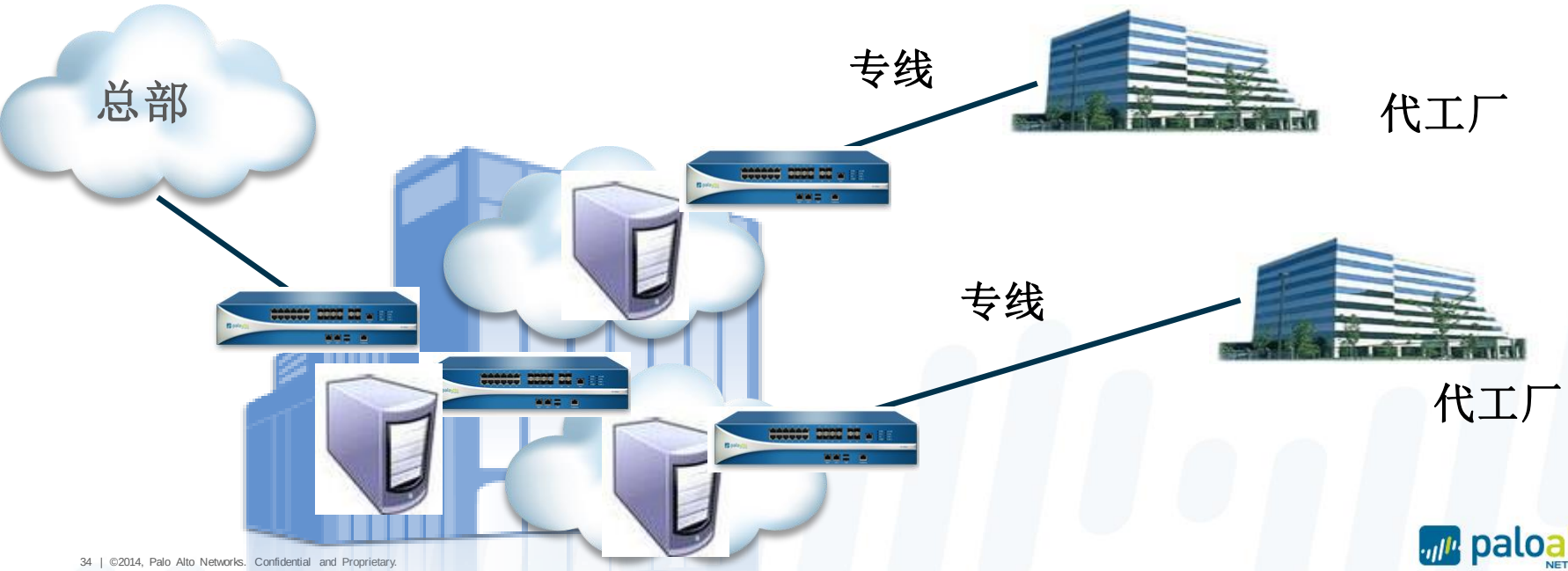
- 联想集团主要生产笔记本电脑、一体机、台式电脑、服务器、手机、平板电脑、打印机、投影机，以及其他移动互联、数码、电脑周边等类商品。收购IBM x86
- 遍布全球的EMC/CCE/IBM分支机构, 需要全方位的互联网边界安全防护；
- 北京/美国/香港/德国数据中心，需求安全隔离，与外界VPN互联，应用与用户控制
- 技术复杂多变，大量Cisco ASA替换， 实施难度大

- PaloAlto Networks
  - 技术领先，测试第一；
  - “All in One “ 解决方案 , PA = NGFW + IPS + URL ， 综合成本低
  - 配置管理简便，减少实施难度
  - 统一集中/分级管理和日志采集分析



苹果中国生产中心
— 世界级生产的核心，安全防护解决方案

- 苹果公司(Apple Inc.)是美国的著名电子设备生产商，全球市值最大的公司之一；其在全世界有大量的代工生产厂，以及区域性的数据中心；
- 苹果公司在上海设有自己的数据中心，为其多个代工生产厂提供服务；
- Paloalto 提供全球的安全服务给苹果公司， 在中国针对其数据中心，提供全面的安全防护服务，针对每个代工厂的数据服务区设置1对安全防护平台，提供NGFW + TP + WF 等全面的安全防护，以及和总部的安全互联和核心服务集群等，设备型号为PA-5060



谢谢！

Q&A

paloalto NETWORKS

the network security company™