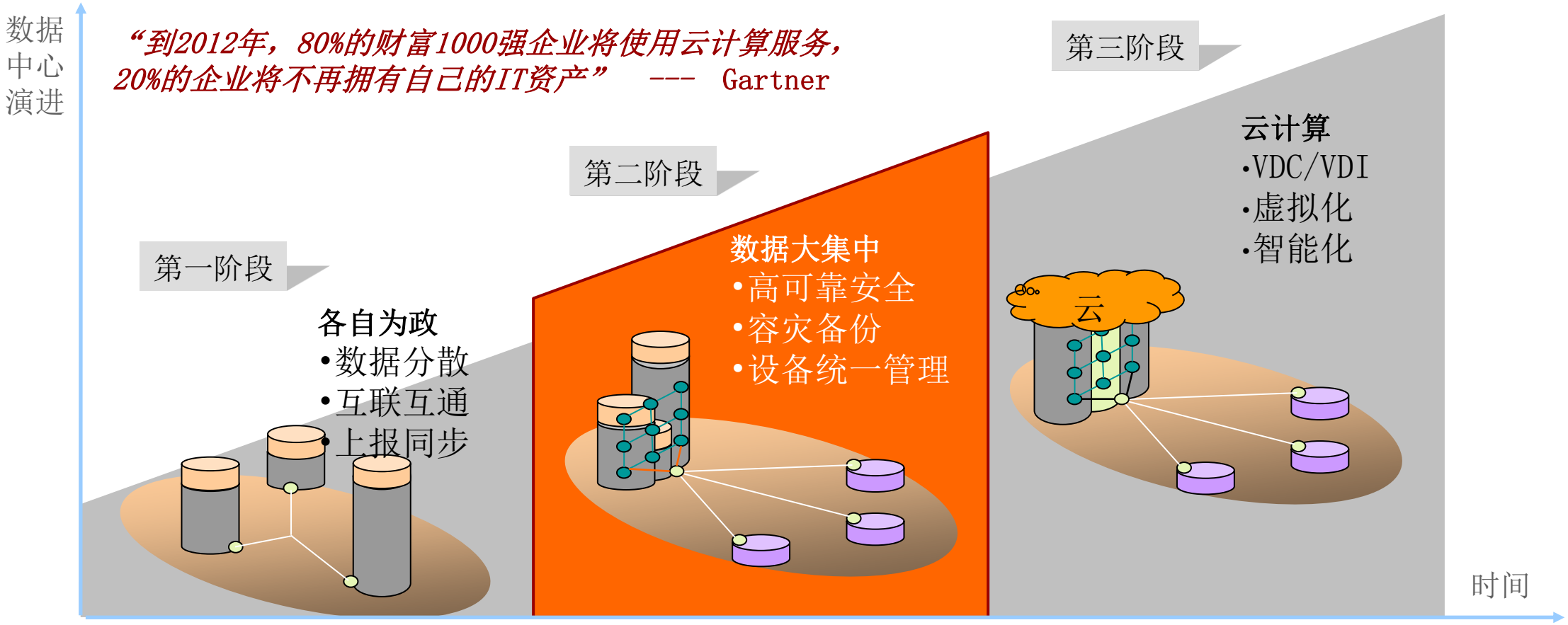
华为USG9500系列高端防火墙 主打胶片

内容

- **云计算时代的安全问题**
- 华为高性能综合业务安全网关
- 应用场景分析
- 案例分享

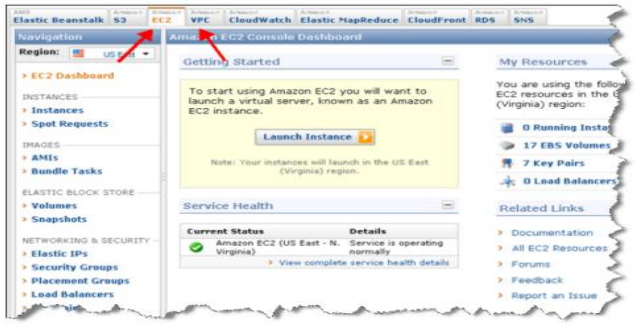
云计算的时代已经到来



“云计算”是下一代数据中心的平台，具备以下特征：

- 新颖的商业服务模式：IaaS（基础设施即服务）、PaaS（平台即服务）、SaaS（软件即服务）
- 无限扩展的计算资源：IT资源通过网络可随时获取、按需使用、易于扩展
- 革新性的IT&CT技术：虚拟化、分布式计算、智能化、自动化

云计算实践遇到的问题



亚马逊从2010年5月连续发生4次故障，以及2011年4月和8月分别发生两次故障，以下是中断4天的Web界面

CSDN客户调研云计算存在的问题TOP2均为安全问题：

- **基础设计安全：**云计算的网络基础设计安全为为云计算的核心安全要素之一
- **数据访问安全：**安全接入、数据访问安全等

对安全问题的忽视，已成为云计算发展的瓶颈

数据中心/云中心安全挑战

云计算

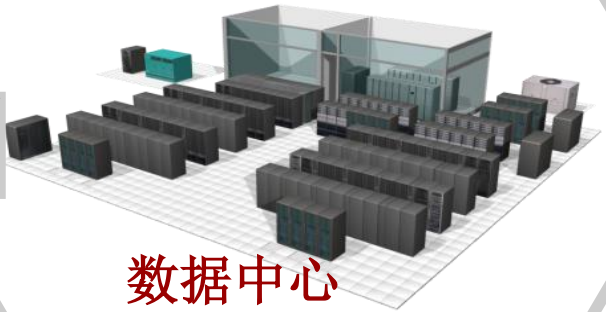
虚拟化

安全边界性能瓶颈问题

虚拟化主机安全隔离与运营支撑问题

数据大集中

入侵、DDoS攻击防护影响正常业务问题



数据中心

安全故障问题

突发灾难

多租户服务

怎样提供灵活的安全服务

如何实现应用的管理控制

多系统多业务

内容

- 云计算时代的安全问题
- 华为高性能综合业务安全网关
- 应用场景分析
- 案例分享

云计算数据中心安全诉求

- 海量处理能力
- 虚拟化应用
- 丰富业务识别
- 深度的应用安全

客户诉求

客户抱怨

- 宣称性能高，无法满足实际应用
- 无法支撑虚拟化应用
- 无法实现应用安全
- 应用无法实现掌控

USG9500云数据中心防火墙

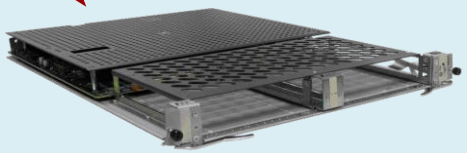
- 海量性能，T级能力
- 虚拟化，动态安全
- 精细化应用管控，深度安全

云的力量：海量性能，T级能力

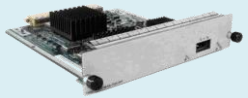
领先架构 | 领先性能 | 最高可靠性

高性能接口板：

20G



LPUF-21母板(20Gbps能力)



1 x 10G POS(1/2宽)

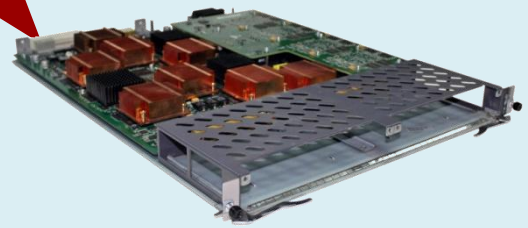
1 x 10GE(1/2宽)

4 x10 GE 光(全宽，收敛50%)

12 x GE 光(1/2宽)

12 x GE 电(1/2宽)

40G



LPUF-40母板(40Gbps能力)

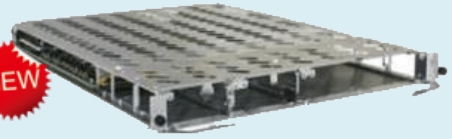
4 x10 GE 光(1/2宽，收敛50%)

20 x GE 光(1/2宽)

2 x 10GE(1/2宽)

100G

NEW



LPUF-101母板(100Gbps能力)

NEW

5 x10GE SFP+(1/2宽)

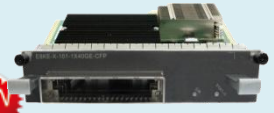
NEW

4 x10 GE SFP+(1/4宽,收敛)

NEW

24x 1GE SFP(1/2宽)

NEW



1x40GE CFP(1/2宽)

NEW

LPUI-101接口板
(1端口100GBase-CFP集成线路处理板)

云的力量：海量性能，T级能力

领先架构 | 领先性能 | 最高可靠性

业界首款超百G性能安全业务处理板

单槽位最大160Gbps

SPU业务处理板

- 单槽位**40Gbps起步**，可扩展至**160Gbps**
- 全新**高密度多CPU多核**设计，**灵活线性扩展**，节省**75%**槽位数
- 专业的 **NAT/IPS/VPN等**安全特性支持
- **虚拟化特性**，管理/带宽/会话虚拟化定制，专为数据中心环境定制

	华为		业界平均
最大吞吐量	160Gbps	4X	40Gbps
最大并发连接	160M	2X	80 M
最大新建连接	2 M/s	5X	0.4 M/s

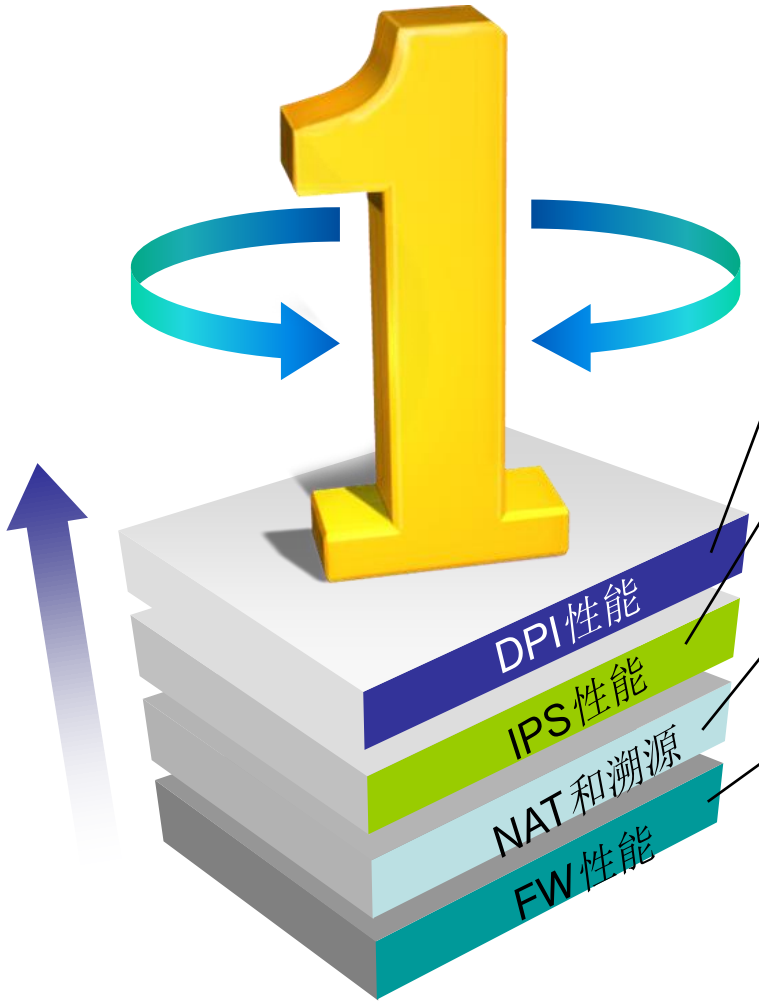
单CPU防火墙业务子卡
(1/2宽,40Gbps性能）

双CPU防火墙业务子卡
(1/2宽,80Gbps性能）

IPS业务子卡
(1/2宽,20Gbps性能）

云的力量：海量性能，T级能力

领先架构 | 领先性能 | 最高可靠性

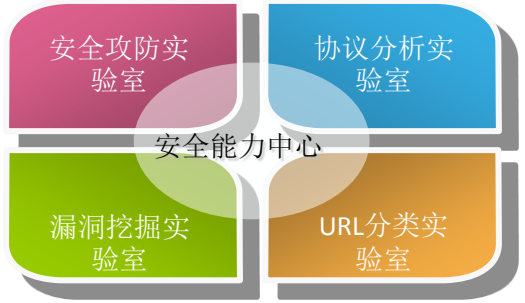


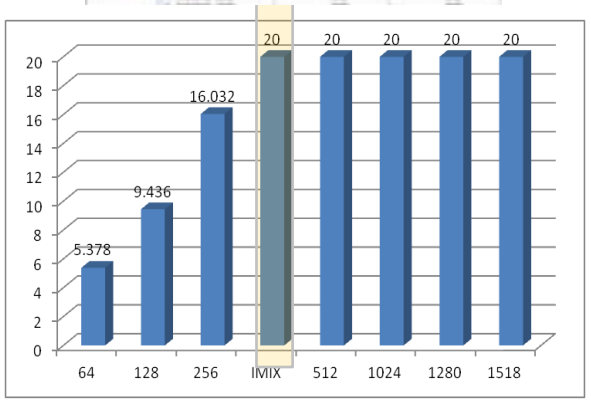
1200多种应用协议识别能力
可识别IM、P2P、视频、游戏等主流应用，基于时间、应用、链路等多维度的流量QoS，可视化管理网络。

高性能的IPS插卡，专业应用层入侵防御能力，微软MAPP合作伙伴，可获取最新僵尸、木马、蠕虫知识库信息

完整的NAT溯源方案
完整的NAT+URL+用户日志
Syslog和二进制日志格式
满足公安部监管需要

整机IMIX吞吐量960G
整机新建连接1200万
整机并发连接9.6亿





注：IMIX模型，采用三类包按下面比例混合64B：594B：1518B=61:24:15

云的力量：海量性能，T级能力

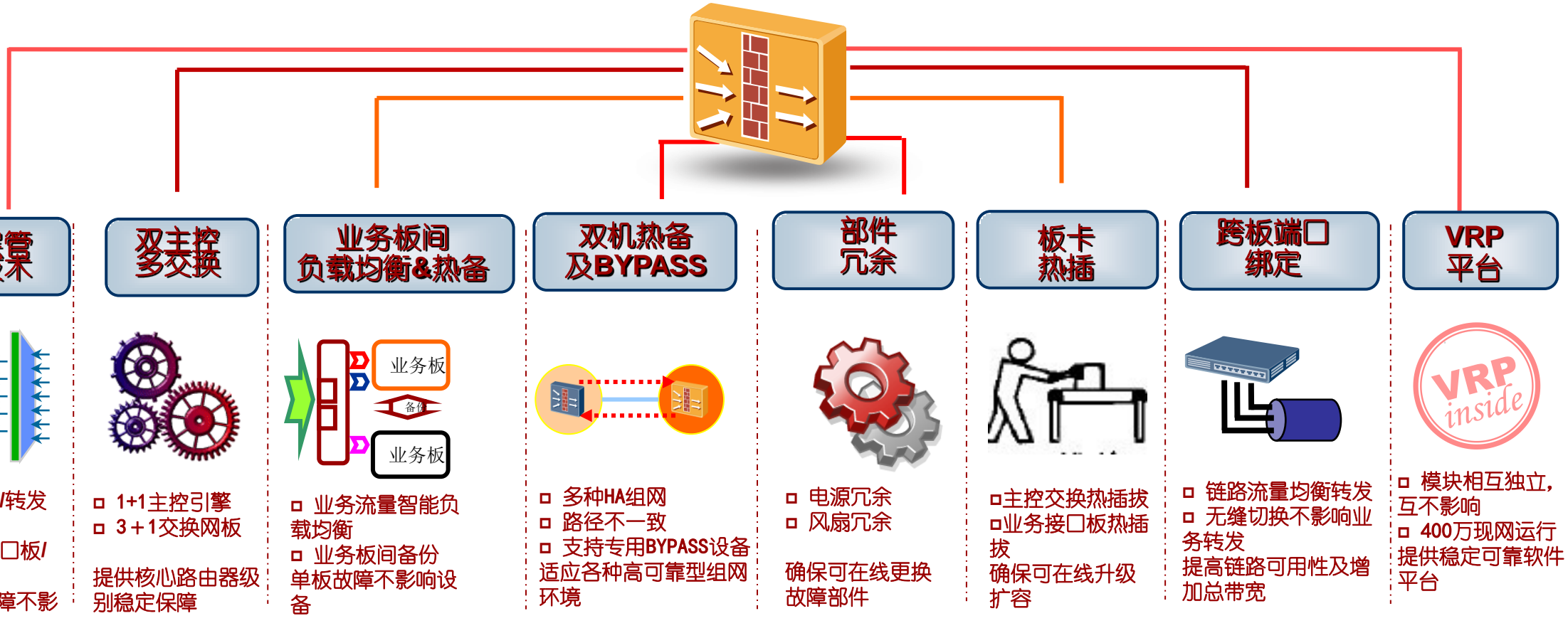
领先架构 | 领先性能 | 最高可靠性

型号	USG9520（4U直流、5U交流）	USG9560（14U）	USG9580（32U）
*吞吐	最大960Gbps		
*并发	最大9.6亿		
*新建	最大1200万/秒		
特性	FW: ASPF/anti-DDoS/NAT/PAT/virtual FW/SA VPN: IPSec/GRE/L2TP/IKEv2 路由: RIP/OSPF/BGP/static routing/I GMP/source address routing IPS: traffic reassembly/signature-based IPS/protocol anomaly detection/automatic upgrade		
接口	Ethernet: 4x10G，2x10G, 1x 10G, 20 x GE O, 12 x GE O/E, 5 x 10GE,24 x 1GE,1 x 40GE POS：1 x 10GPOS 单板最大接口数量4；单板最大千兆接口数量48个		

*性能最大值均为USG9580满配置测算

云的力量：海量性能，T级能力

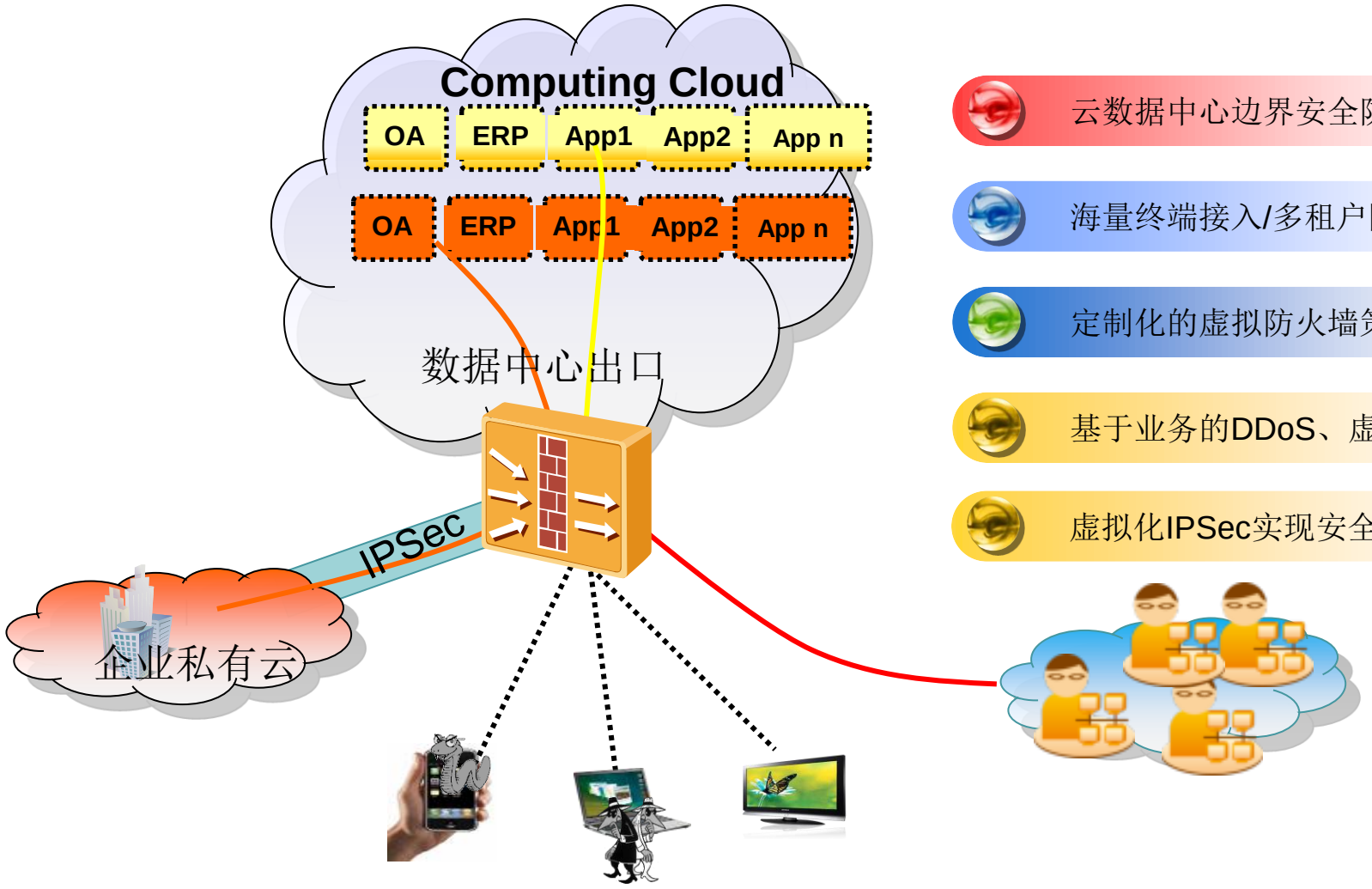
领先架构 | 领先性能 | 最高可靠性



从硬件平台、板卡部件到 组网链路和软件平台&软件管理等，提供多重可靠性技术保证，确保电信99.999%级可靠性

云的敏捷：虚拟化安全，运营管理

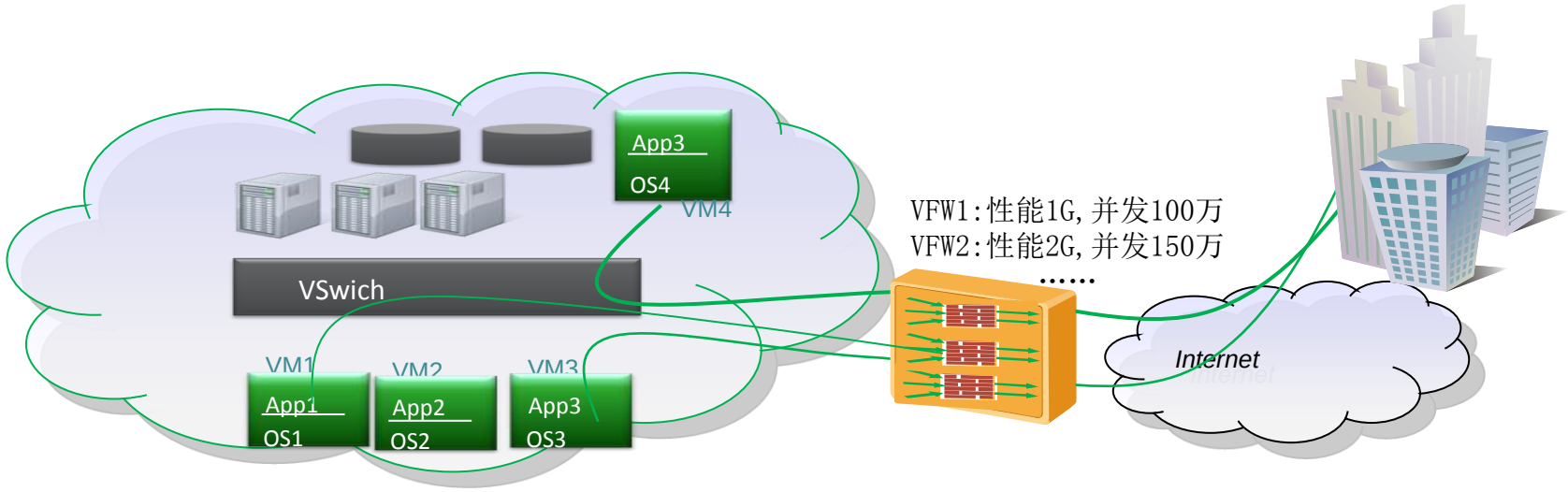
虚拟化安全 | 运营管理



- 云数据中心边界安全防护，960G防护性能满足高性能需求
- 海量终端接入/多租户隔离，4096个虚拟防火墙支撑运营
- 定制化的虚拟防火墙策略和资源，实现弹性分配
- 基于业务的DDoS、虚拟化IPS、实现安全虚拟化
- 虚拟化IPSec实现安全安全接入

云的敏捷：虚拟化安全，运营管理

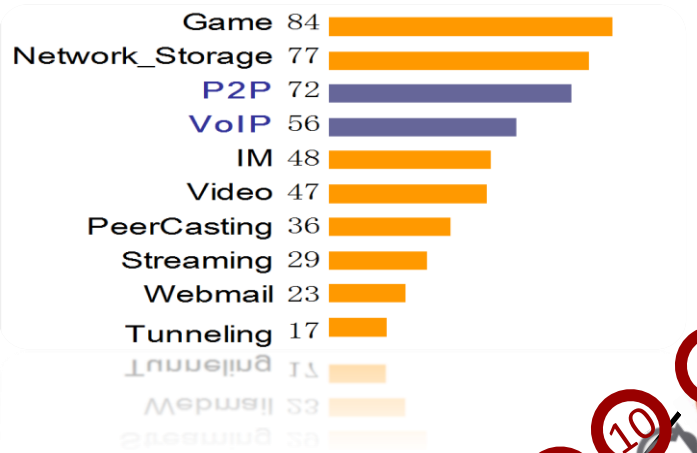
虚拟化安全 | 运营管理



运营配置管理	创建、编辑、切换虚拟系统 虚拟系统管理员权限管理 分配虚拟系统资源
虚系统用户配置管理	虚系统用户配置自己防火墙 支持web、SSH、telnet管理 虚拟用户视图

云的智慧：精细化应用管控

精细化管控 | 专业DDoS防护 | 专业IPS防护 | IPv6安全



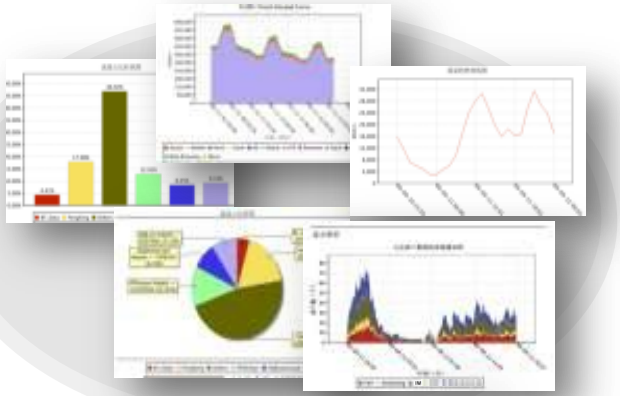
X 阻断

10 限流

20 限流

30 限流

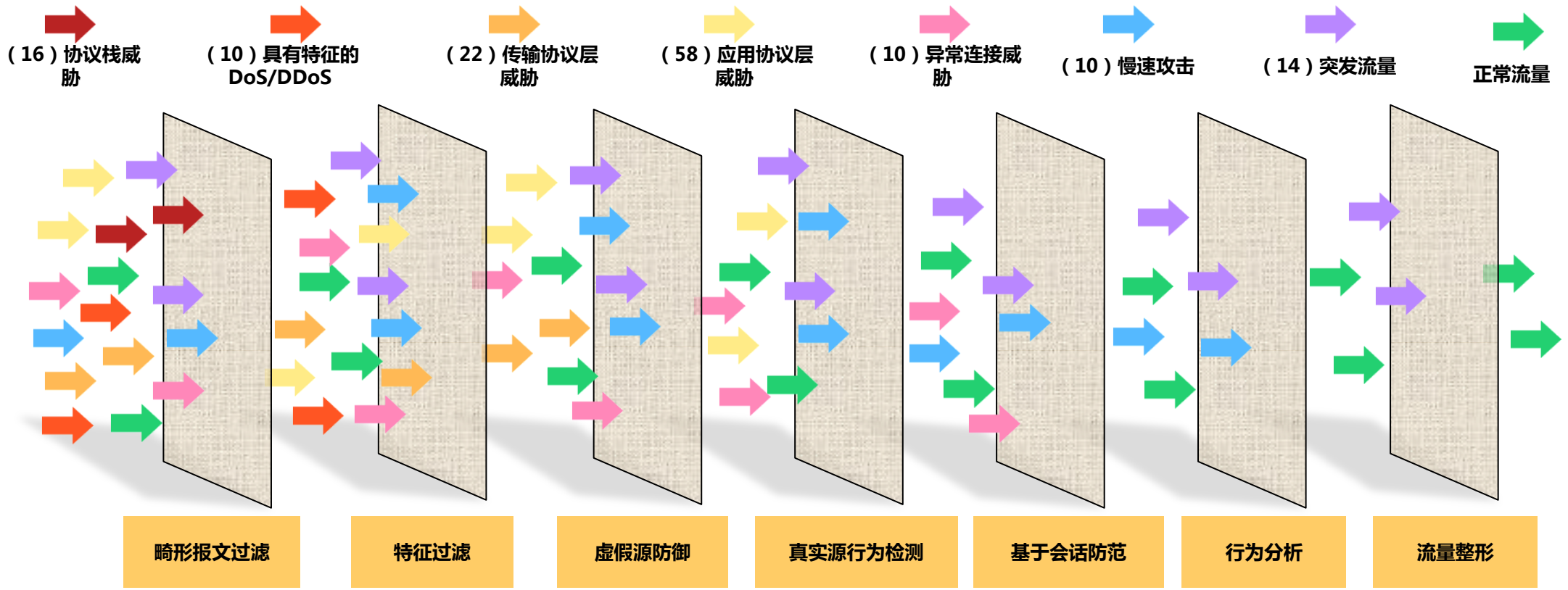
应用识别



报表呈现

云的智慧：深度安全

精细化管控 | 专业DDoS防护 | 专业IPS防护 | IPv6安全



- 基于应用的信誉防护体系和会话检测技术，提供业界首个“零误判”方案
- 支持所有攻击类型IPv4/IPv6共栈防御，防御种类业界第一

云的智慧：深度安全

精细化管控 | 专业DDoS防护 | 专业IPS防护 | IPv6安全

Identify → **Parse** → **Scan**

基于应用的识别

可识别超过240种协议

可识别多种伪装的数据

高效的内容解析

基于规范的解析，无需盲扫

深入的检测能力，缓存关键信息，忽略无关内容。

基于漏洞的扫描

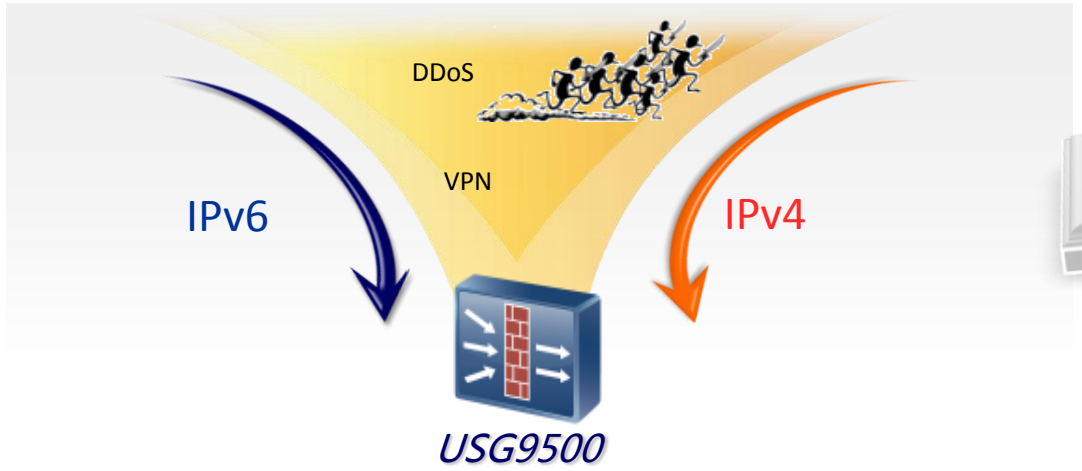
基于漏洞的签名，最小的签名关联，极低的误报

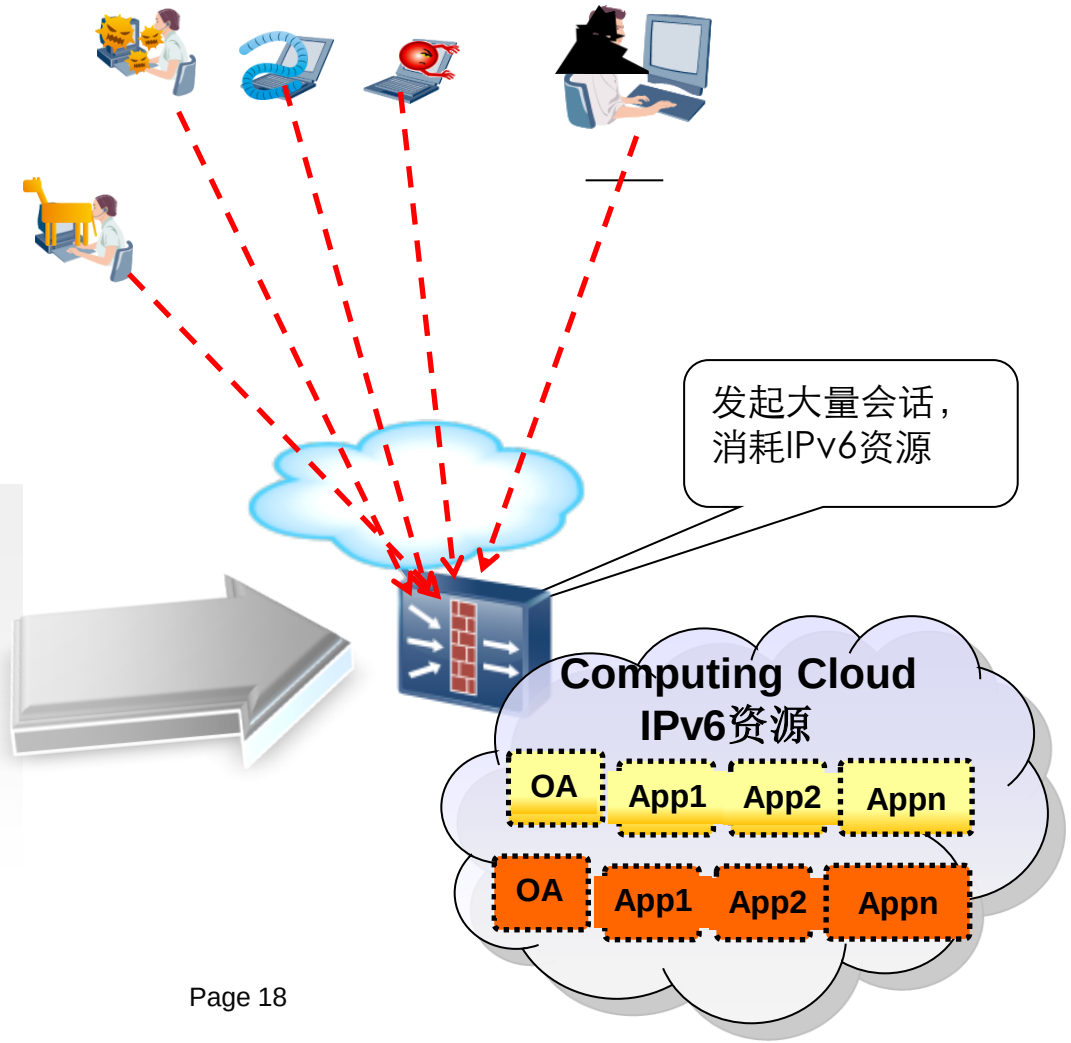
- 专业IPS引擎，基于漏洞的签名技术,可抵御僵木蠕虫攻击及变种，**检出率大于90%**
- **微软MAPP合作伙伴**，可实时更新最新漏洞信息
- 专板专用，独立IPS插卡，**单业务插卡性能高达20Gbps**
- 线性扩展，**即插即用**，双CPU设计，**可靠性高**

云的智慧：深度安全

精细化管控 | 专业DDoS防护 | 专业IPS防护 | IPv6安全

- IPv6 ACL
- IPv6协议检查
  - ✓扩展头检查
  - ✓ASPF
- IPv6 IPsec
- IPv6 DDoS
- 过渡技术安全
  - ✓隧道：双层包过滤、协议检查
  - ✓翻译：防范地址池恶意消耗

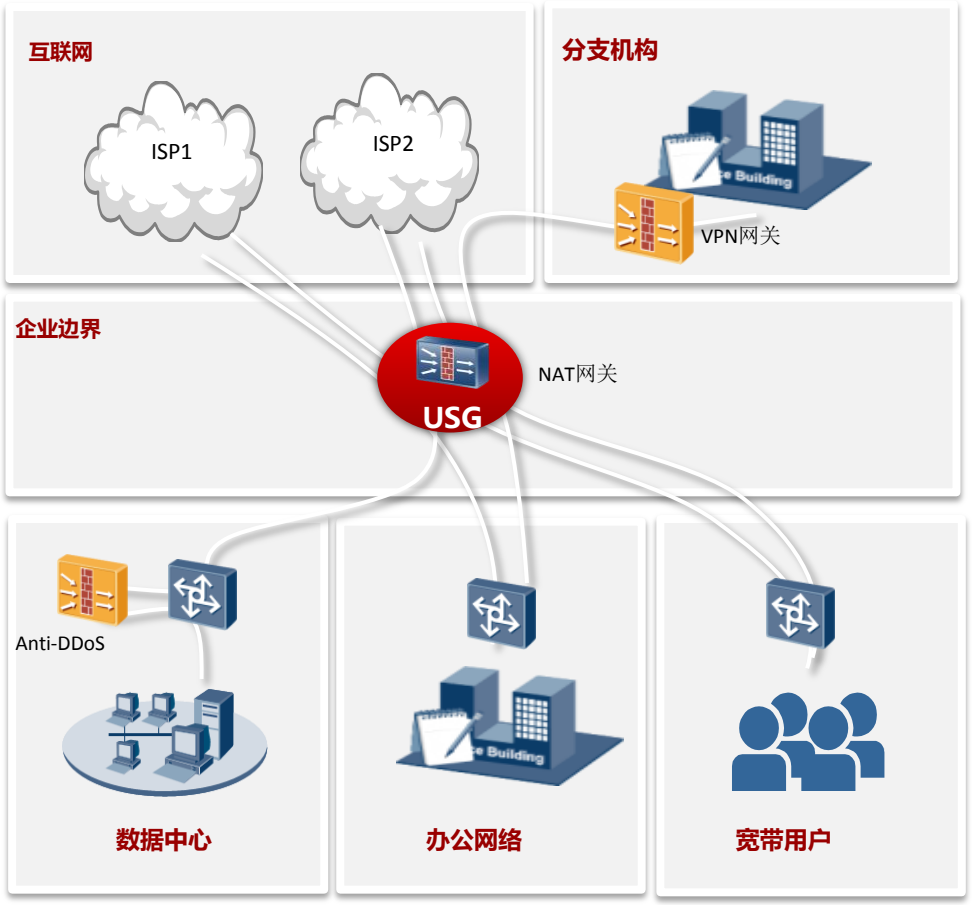




内容

- 云计算时代的安全问题
- 华为高性能综合业务安全网关
- 应用场景分析
- 案例分享

典型场景一：广电和二级运营商网络



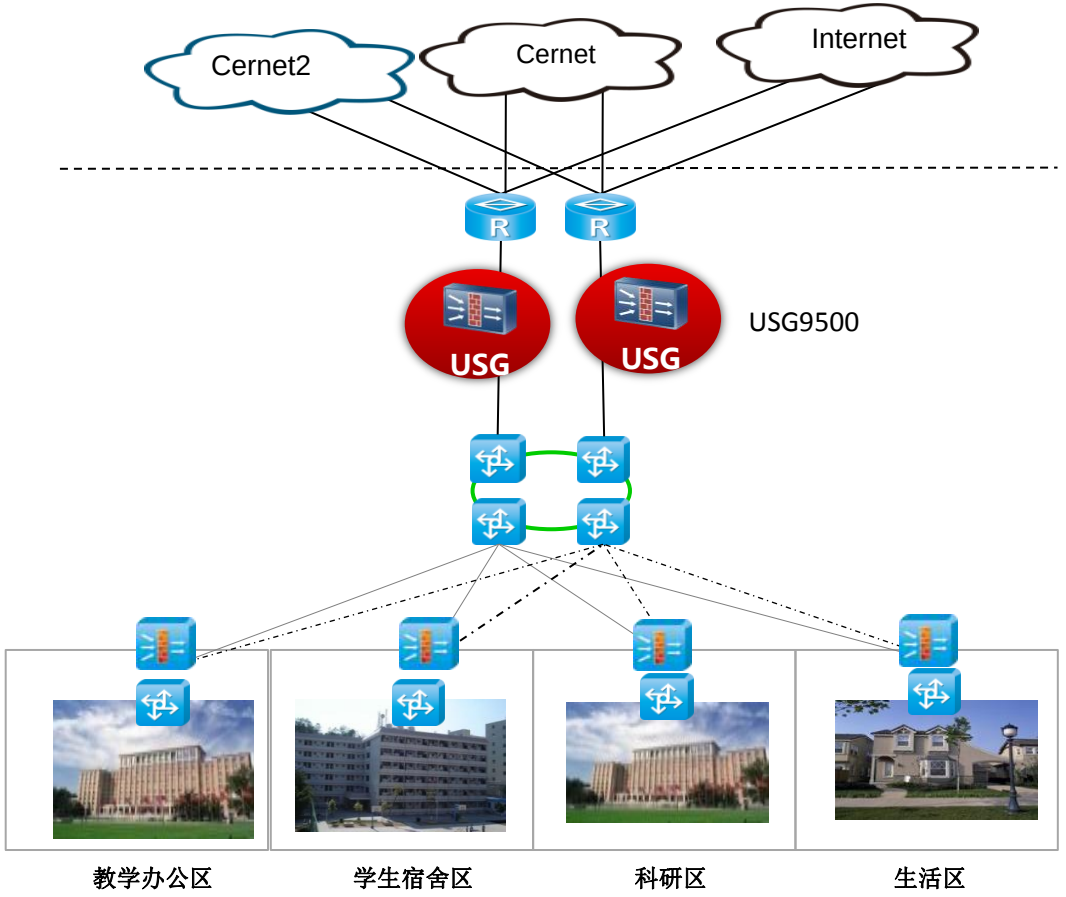
存在的问题

- 多出口链路，租用ISP价格不同，低价值业务占用大量高价值带宽；
- 非法流量造成运营商封杀公网IP；
- 对外服务器需要针对不同ISP需要部署多台设备

解决方案

- 智能选路，基于应用和路由权重的业务分类，降低无谓带宽消耗；
- 公网IP防封杀探测，自动切换备份链路；
- 多对一NAT服务器发布，节省内部资源，提升带宽利用率，降低带宽租赁费用

FW典型场景二：高校园区网边界安全



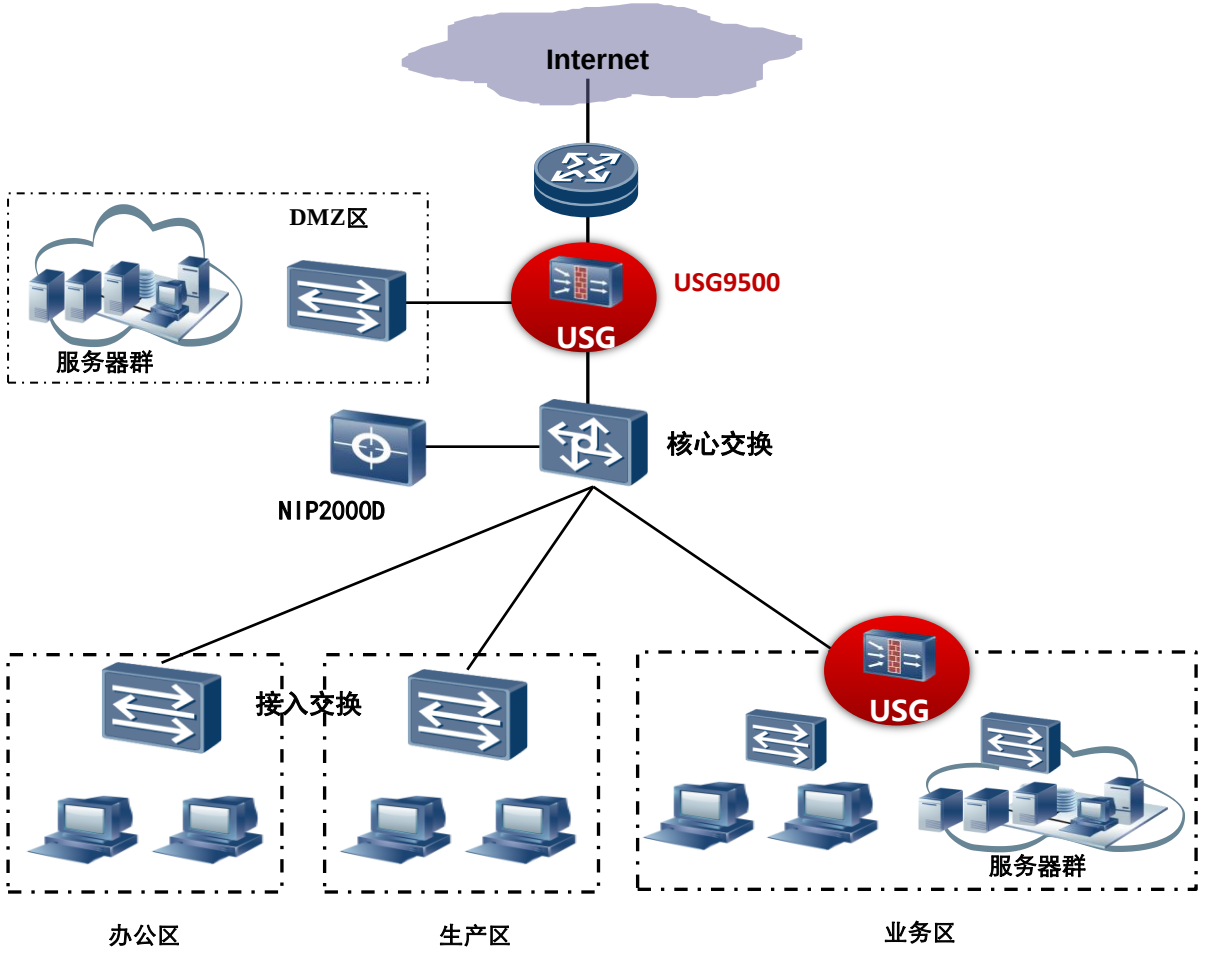
存在的问题

- 高校网络边界安全防护不足（IPv4和IPv6双栈接入），黑客很容易入侵与 发起攻击
- 上网行为监管是加强学校信息安全的重要一环，需要强大的应用识别能力

解决方案

- 高安全性：通过防火墙策略保证校园边界安全性
- 高可靠性：防火墙采用双机备份 ，防止单点故障
- 1200+种应用识别能力
- 全方位IPv6安全特性

典型场景三：企业网络边界防护与访问控制



存在的问题

- 来自互联网的病毒、恶意攻击；
- DMZ区对外提供服务经常遭受非法访问
- 内部业务系统时常遭受来自内外非法攻击、未授权访问；

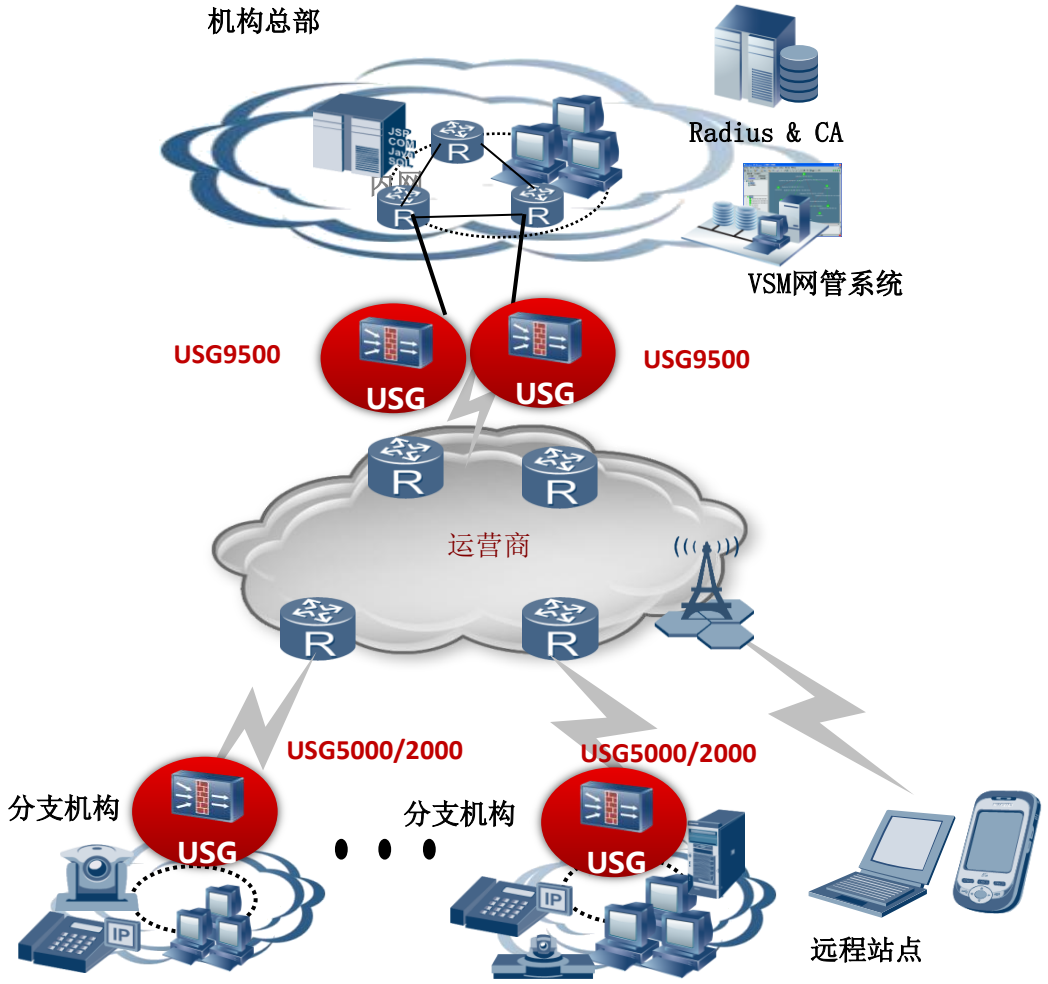
解决方案

- 互联网边界访问控制防护；
- 核心业务区网络边界访问控制防护；

方案价值

- 阻止来自互联网安全威胁对网络破坏；
- 保障DMZ区业务正常运行与服务；
- 保障核心业务正常运行与合法访问；

典型场景四：企业分支机构VPN安全互联



存在的问题

- 分支机构、移动办公安全接入
- 跨互联网数据安全传输

解决方案

- 支持IPSec/L2TP/GRE/SSL/ MPLS等多种VPN技术
- 支持隧道数在线扩展
- 电信级高可靠性

方案价值

- 安全、灵活、可靠VPN接入
- 业务集中管理

内容

- 云计算数据中心的安全问题
- 华为云数据中心安全综合业务网关
- 应用场景分析
- **案例分享**（更多案例请参考《案例集锦》）

浙江宁波广电城域网安全

需求和挑战

- 宁波是浙江省第二大城市，三大经济中心之一。宁波数字电视市内骨干汇聚IP网络建于2005年，随着业务的不断发展，尤其是高清交互**点播业务**和**宽带业务**的大规模推广，原有的骨干汇聚IP网络急需扩容，以支撑后续业务的发展。

解决方案

- 在点播业务和宽带业务网络出口，各部署2台分布式USG9500高端防火墙，当前配置40G处理性能，并可通过板卡持续扩展。网络出口提供**NAT转换，多链路的智能选路、基于应用的流控**等功能。
- 为了满足公安部82号令监管要求，配置了**日志服务器与防火墙配合，提供NAT日志、URL地址溯源**等功能。
- 华为高端防火墙的部署，有利支撑了当前及未来宁波广电点播业务和带宽业务的发展，提升了上网体验，并且也满足了上级单位对上网经营单位的**监管要求。**

国家超算中心深圳中心

需求和挑战

- **亚洲最大超算中心**，主机系统运算速度每秒1271万亿次，**排名世界第二**。如何将超高计算能力输出至客户，真正服务于深圳、华南，乃至全国，是信息网络系统建设的首要诉求。
- 在网络安全层面，提出了**“无忧、无感知”**的网络安全顶级要求。

解决方案

- 部署USG9500系列防火墙、SIG 9200系列流量分析管控设备联手阻挡了来自互联网的**网络威胁冲击**。利用99.9999%稳定性、**超百G处理性能**、**七层过滤DDoS防护**为超算中心提供了安全大门，通过设备的超高转发性能、多层过滤防护及高稳定性在提供坚实外部防护的同时，不影响超高计算性能输出到外部客户，在网络安全层面，满足了客户“无忧、无感知”的要求。

国家超级计算深圳中心
National Supercomputing Center in Shenzhen
深圳云计算中心
Shenzhen Cloud Computing Center

Thank you

www.huawei.com