SACC 2014中国系统架构师大会
SYSTEM ARCHITECT CONFERENCE CHINA 2014
发现架构之美

云计算中的网络功能虚拟化及安全应用解决方案

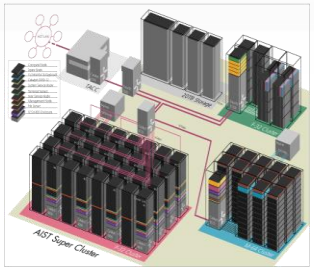
上海有云信息技术有限公司
江均勇
E-mail: jiangjunyong@cloudguarding.com
微信:15261619

目 录

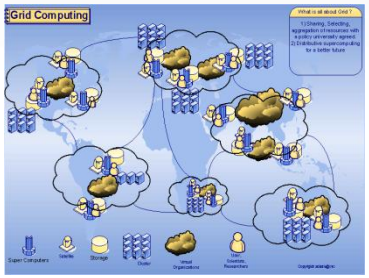
- 云计算的背景与架构模型
- NFV的发展趋势探索
- 传统数据中心的网络与业务应用
- 云计算虚拟网络功能与应用业务
- SDN技术与云计算的融合
- 实例剖析：WEB应用安全从传统到云计算的演进方案

云计算背景与架构模型

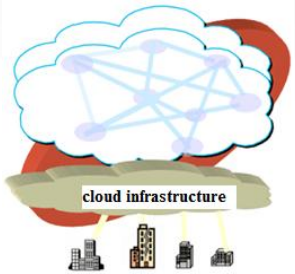
并行计算



集群计算

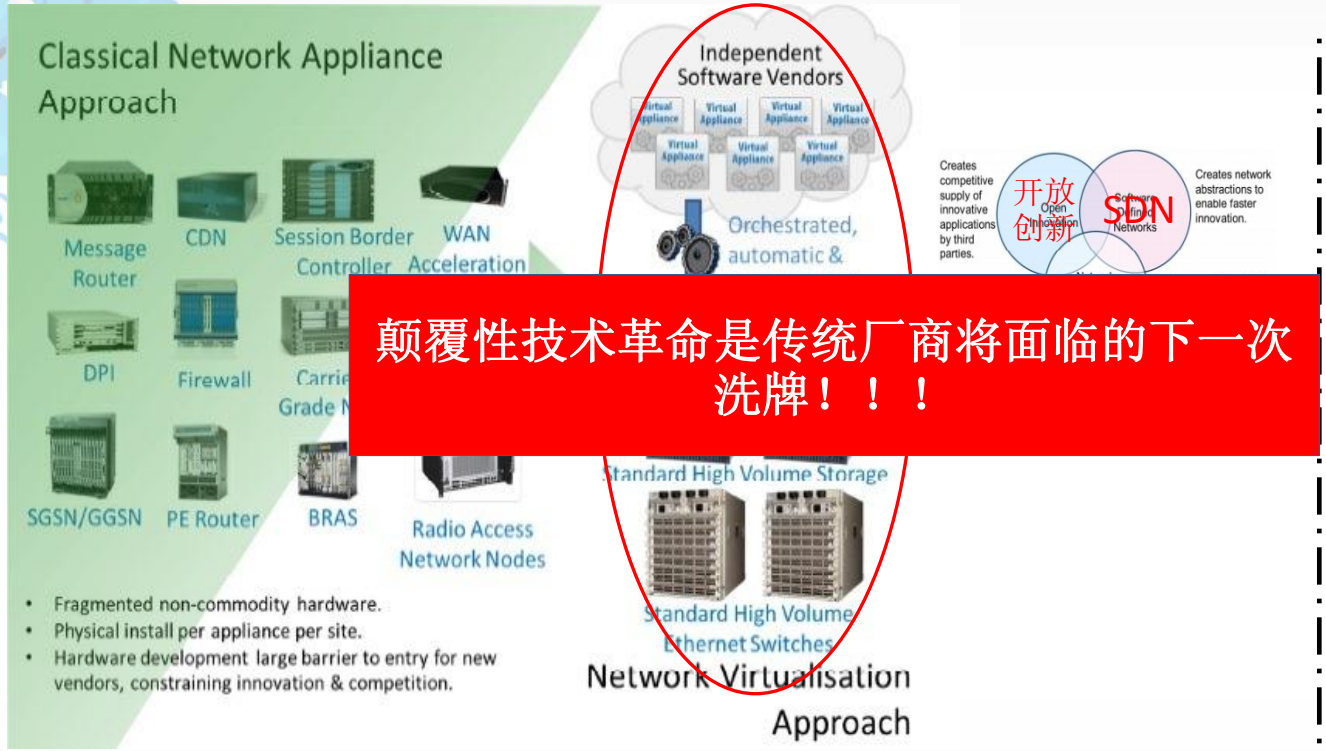


网格计算

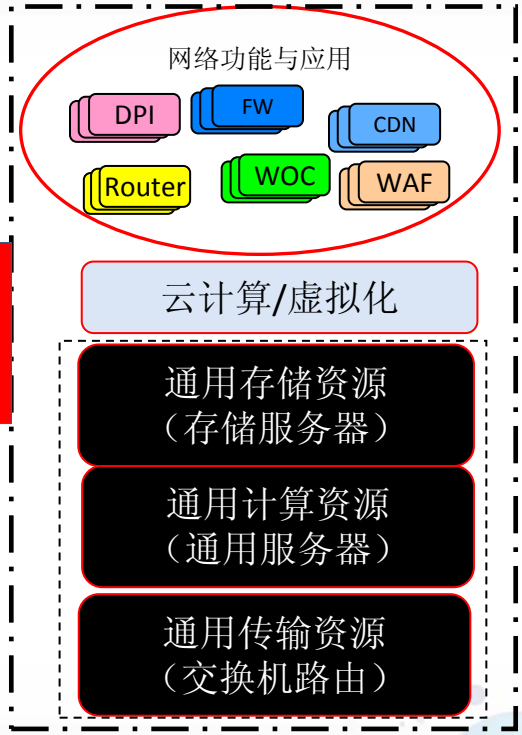


云计算

NFV发展趋势探索

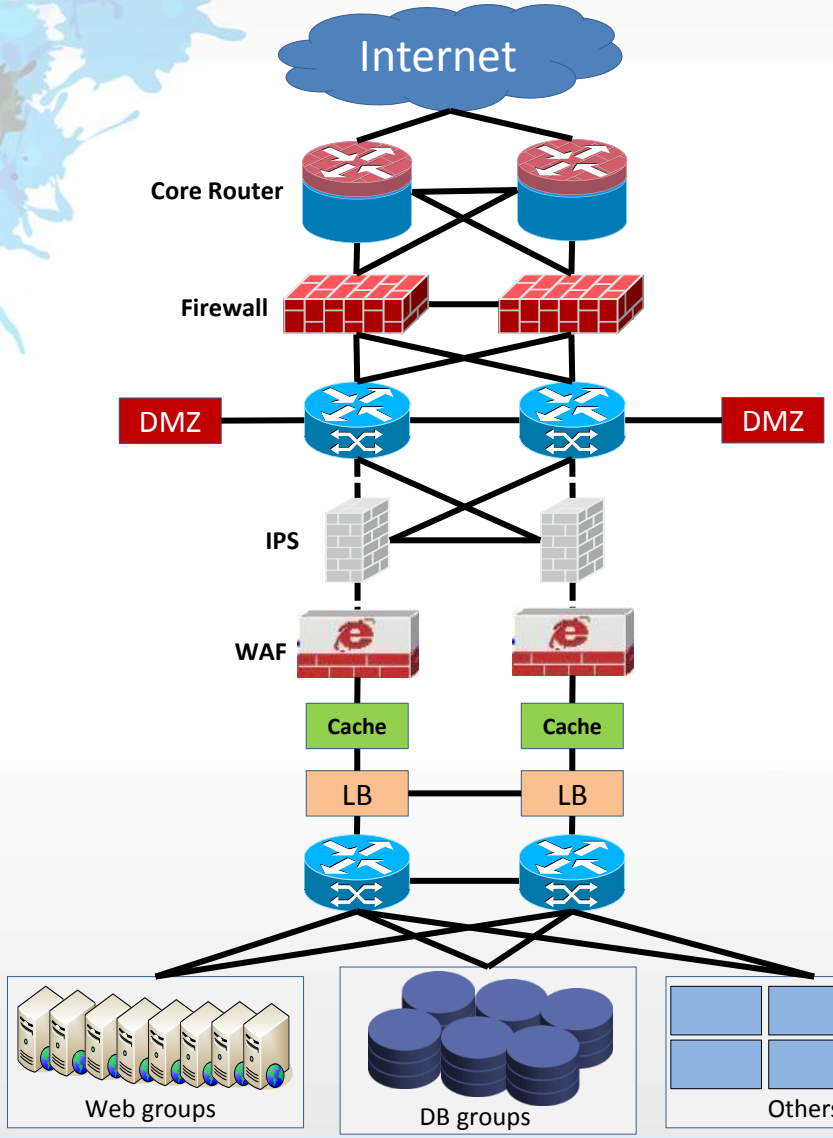


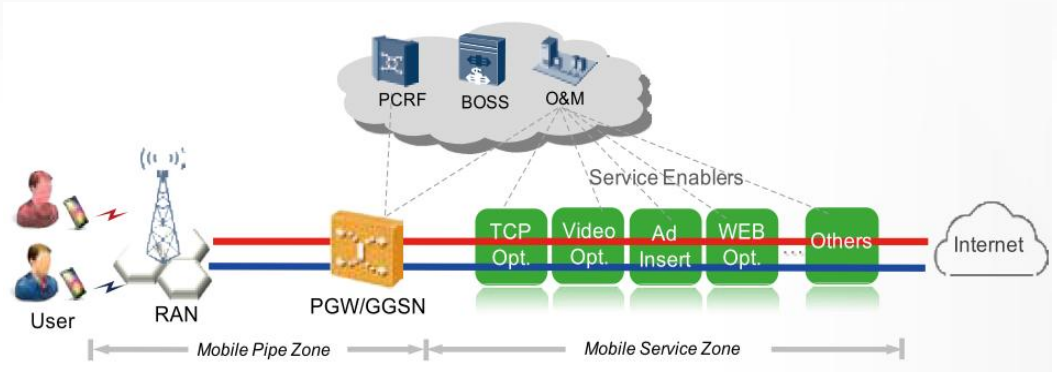
颠覆性技术革命是传统厂商将面临的下一次洗牌！！！



运营商对行业和技术的垄断引导了通信技术与数据中心技术的发展方向，NFV技术集合了云计算与虚拟化、SDN技术以及开放创新思路，是对传统设备厂商“封闭式”系统的挑战，运营商倡导降低Capax和Opex为核心思想，以通用计算、存储和网络资源的基础设施，采用虚拟化技术，实现网络业务功能“软件化”的灵活部署以及方案的可复制性，推动NFV的迅猛发展和应用。

传统数据中心的网络与业务应用





- 传统数据中心的网络架构主要包含核心层、汇聚层和接入层
- 网络业务应用和网络安全通常以物理设备的形态接入三层架构之间，包括网络防火墙、IPS、DMZ、WAF、Cache、LB等安全与增值业务设备
- 为解决可靠性问题，不同网络设备和增值业务、网络安全设备通常以负荷分担或主备的方式部署
- 不同的网络设备、安全设备和增值业务设备，往往由不同的运维人员管理，共同维护整个数据中心的网络业务运营支撑
- 业务系统的运维由业务运维管理人员负责
- 数据中心业务的增扩容复杂：需要制定明确的组网解决方案、购买设备、规划机架等进行部署实施
- 网络安全体系架构通常包含：网络防火墙→DMZ→IPS(IDS)→WAF(针对WEB)等完善架构，通常DB还包含DB审计和防护

运营商与传统网络业务的痛点及对NFV诉求

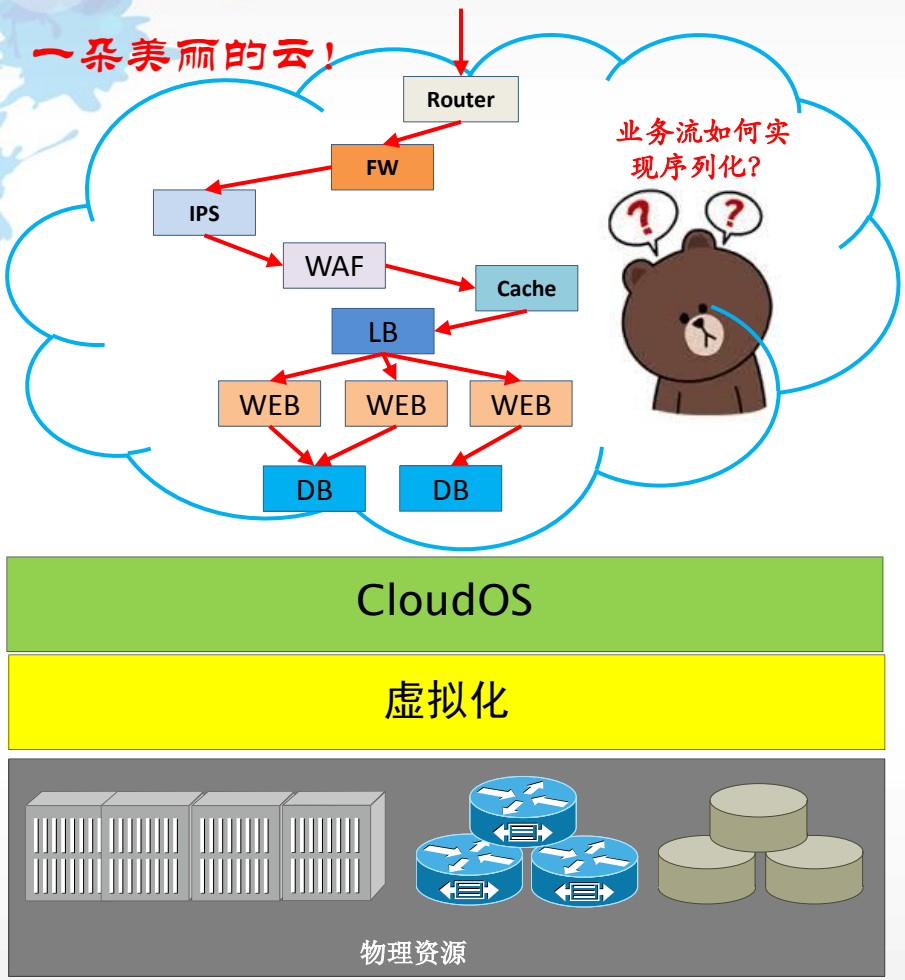
痛点：

- 随着“流量经营”模式的推行，运营商数据中心建设、扩容的购买成本和运维成本越来越大，而利润却并没有线性增加
- 各个厂家专用硬件设备强调硬件能力，价格昂贵，操作管理和维护成本高
- 数据中心建设的可复制性差，业务上线运营方案复杂，周期长

NFV的诉求：

- 硬件设备通用化
- 网络业务功能的软硬件解耦
- 平台管理的云化、资源池化
- 业务部署快捷化
- 运维自动化
- 开放编程接口

云计算虚拟网络功能与应用业务–向虚拟化的华丽转身

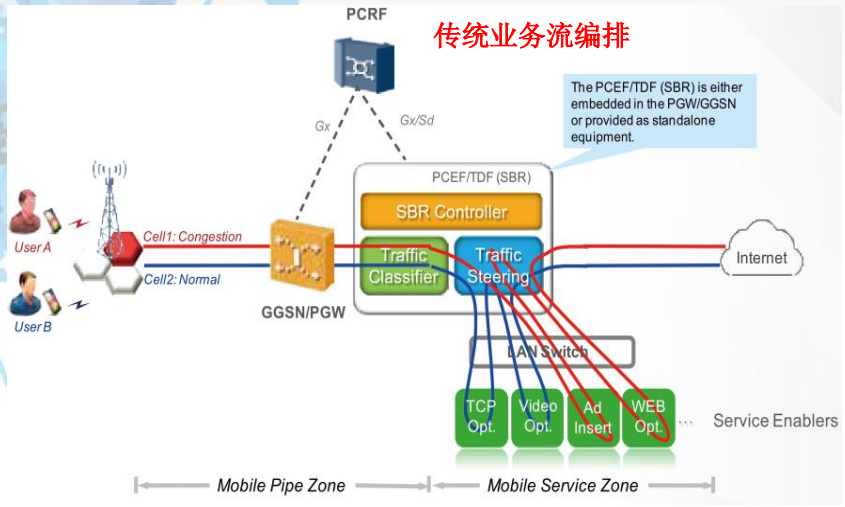


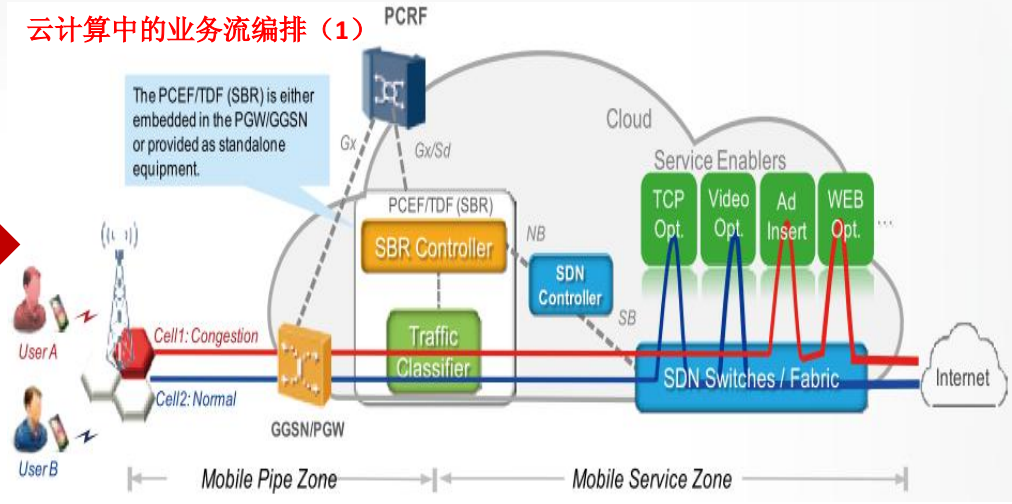
云计算及虚拟网络功能与应用业务引入的新问题：

- 云计算的特点是业务与硬件解耦，部署的位置无关性，各种网络功能、安全、增值业务与业务可能运行于不同的物理服务器，业务流如何实现序列化？
- 通用服务器可靠性较专用网络设备差，业务的可靠性如何保障？
- 虚拟网络功能的性能如何满足业务诉求？
- 虚拟网络功能与应用业务如何在云计算平台中自动化的部署和运维？
- 新业务上线与业务扩容如何实现？
- 其他...

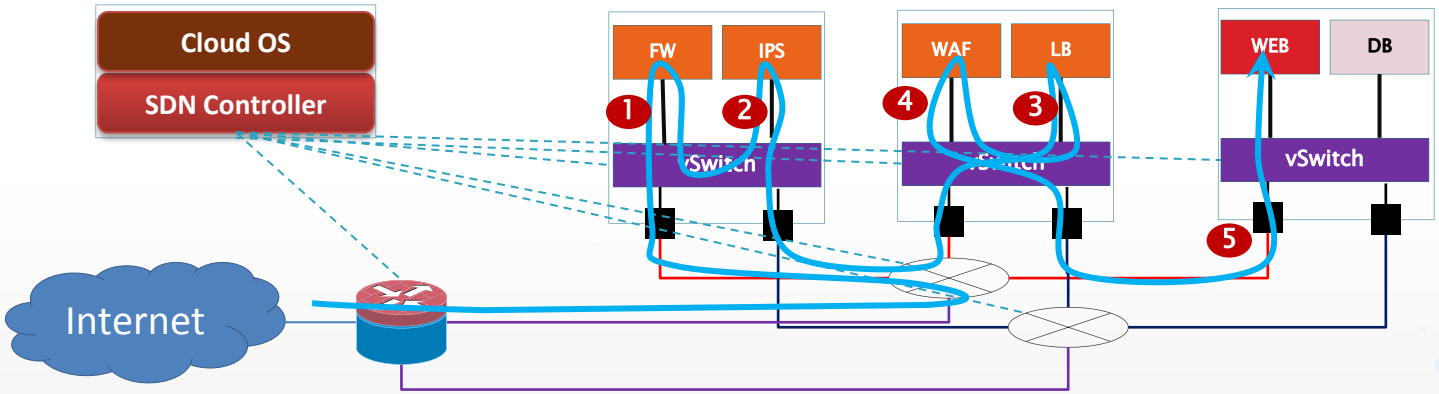
网络功能虚拟化和业务的虚拟化，为数据中心云计算引入了新的技术挑战...

从传统的网络功能到虚拟网络功能业务编排的演进



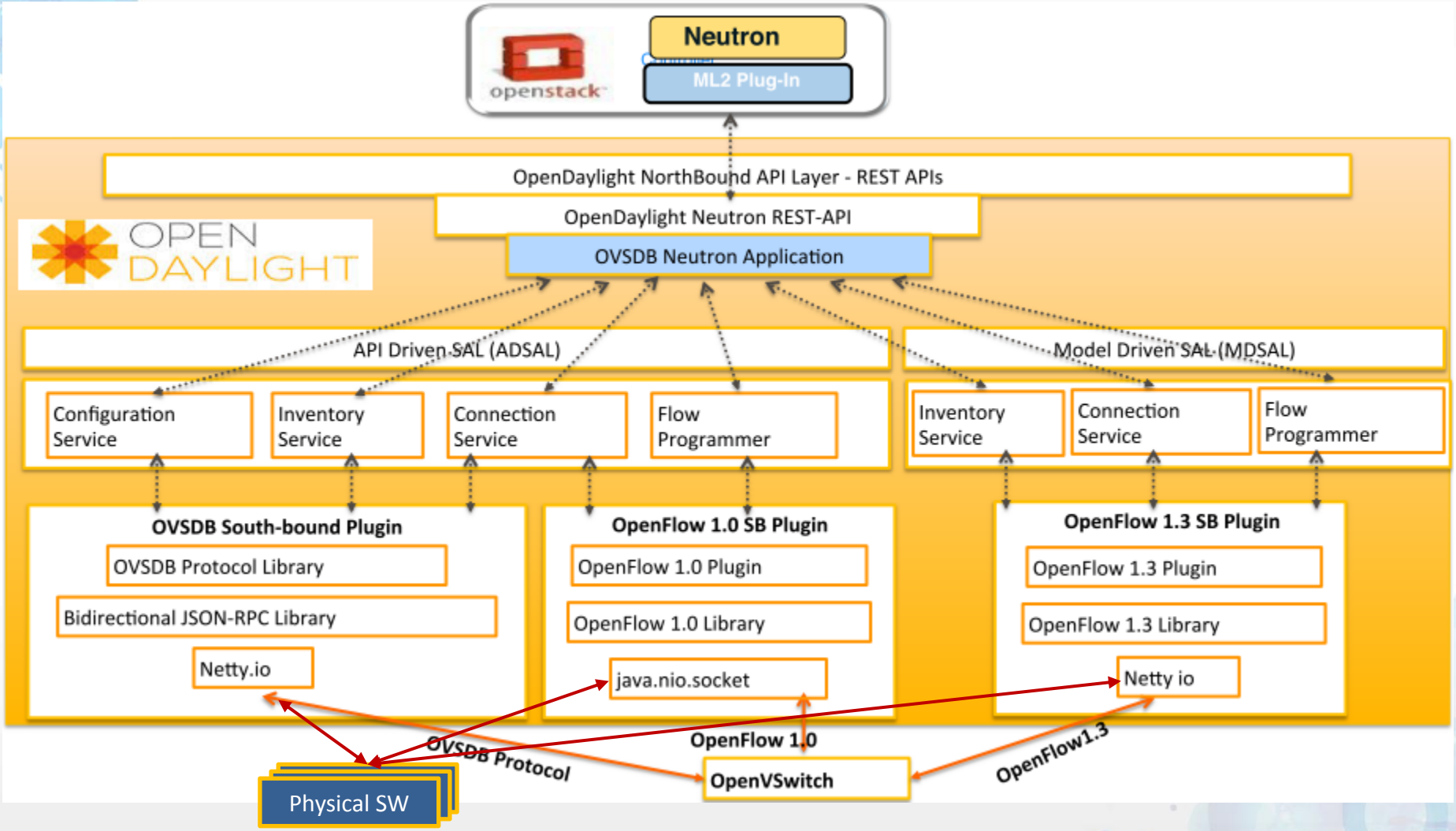


云计算中的业务流编排（2）

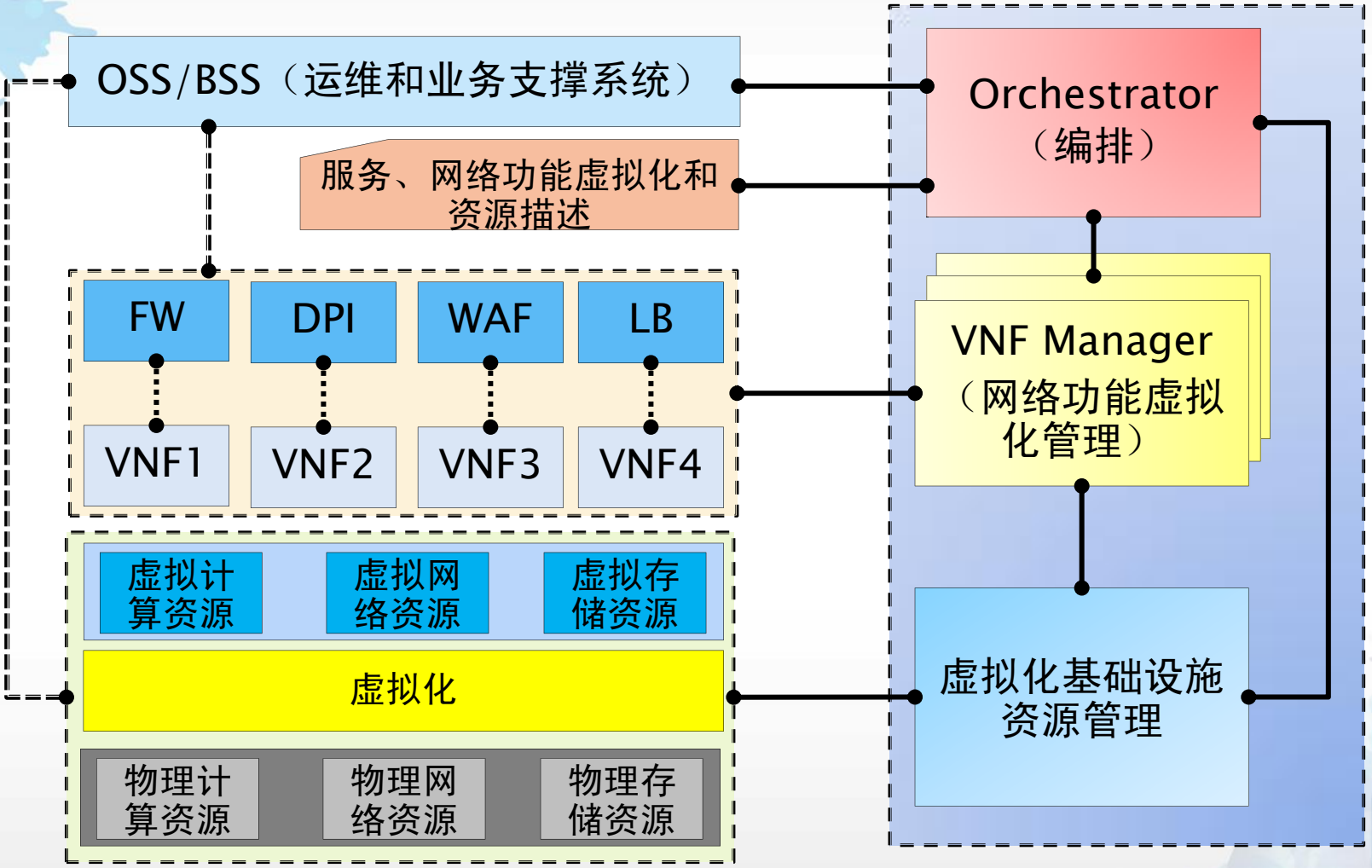


物理/虚拟传输设备的引流编排，成为云计算和虚拟化环境中的业务驱动的迫切需求，SDN与Service Chaining的思想和技术是创新和革命的关键核心…

SDN技术与云计算的融合

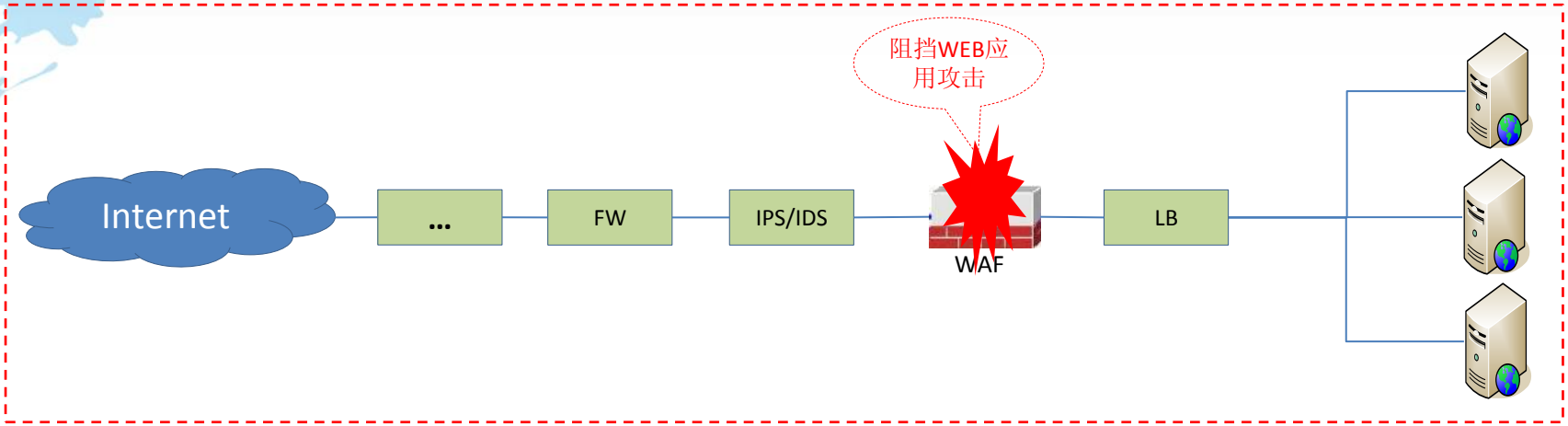


云计算与网络功能虚拟化平台架构—NFV的原动力



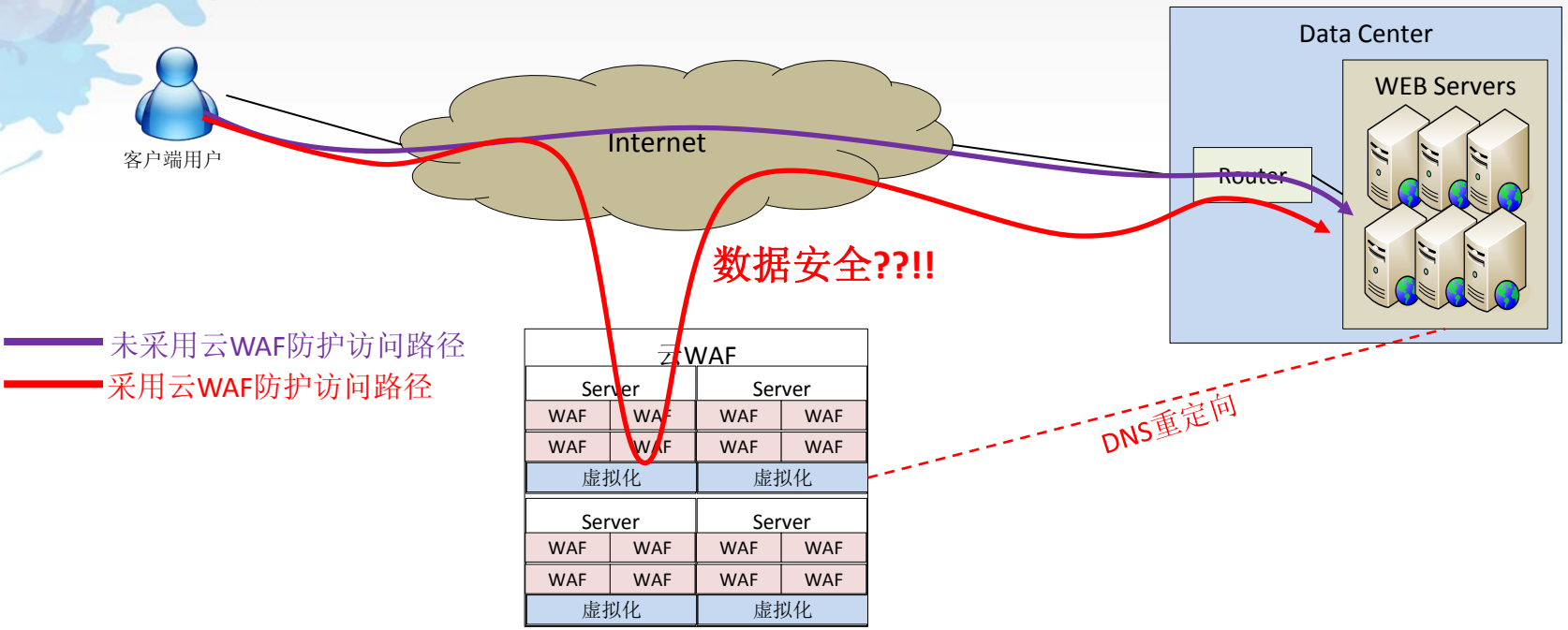
VNF： Virtualized Network Function

实例剖析：WEB应用安全从传统到云计算的演进方案—传统软硬件一体化



- 传统WAF采用软硬件一体化的模式实现，在部署方案中，采用串联或者旁路部署的方式，对被保护的WEB服务器的流量进行安全检测。WAF的功能包括防止黑客进行SQL注入、XSS跨站、畸形报文、文件注入、系统命令注入、网页篡改、信息泄露等攻击，来实现保障WEB服务应用安全。
- 主要缺点：
  - 软硬件一体化，可靠性同时依赖于硬件与软件；
  - 升级与维护复杂，缺少集中的管理平台，硬件一旦出现故障，必须要厂家更换设备或重新购买；
  - 扩容复杂，需要重新制定解决方案；
  - 运维成本高，增加数据中心（或普通机房）内对设备类型的管理和监控。

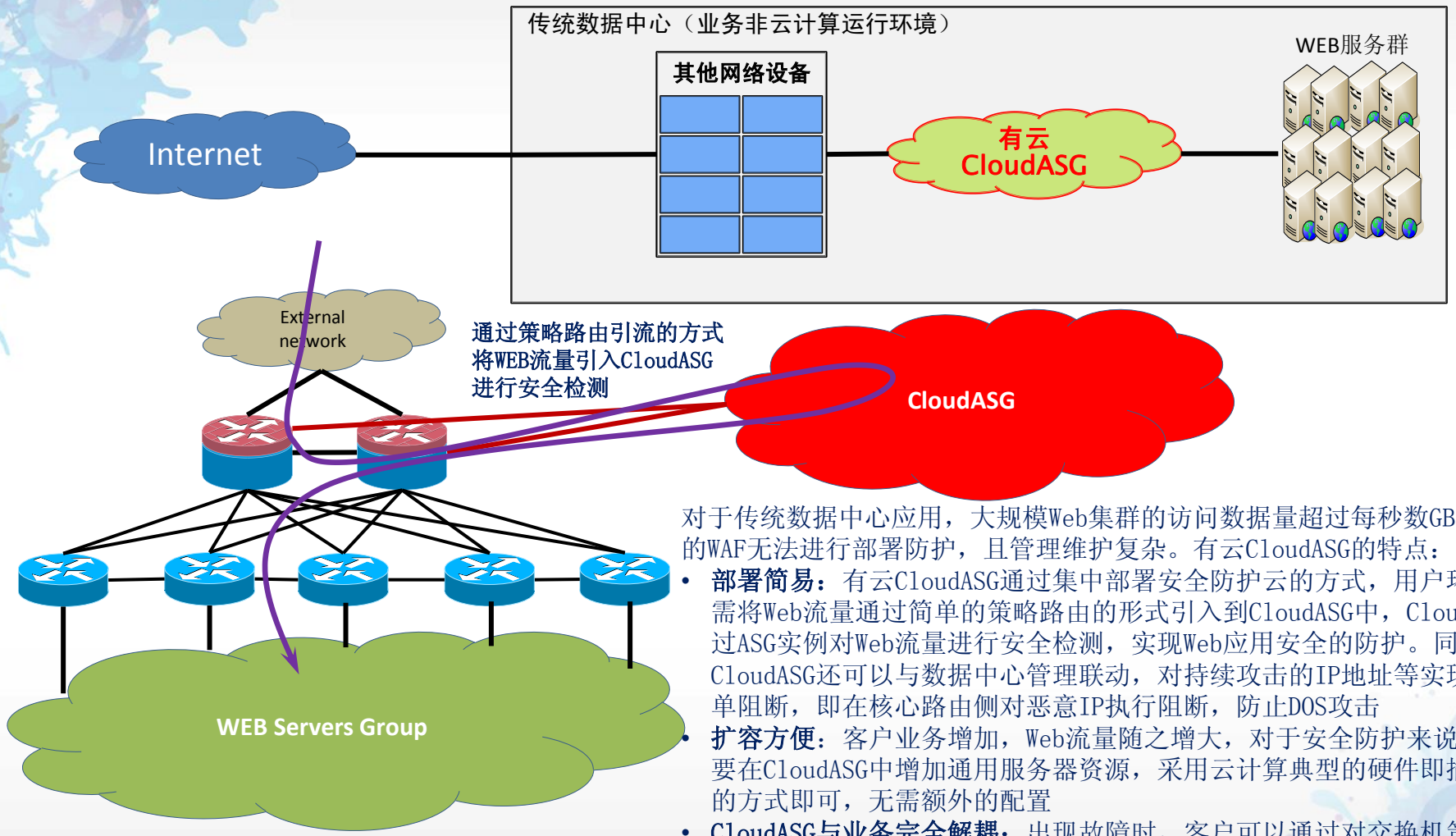
实例剖析：WEB应用安全从传统到云计算的演进方案–云WAF



- **主要原理：访问路径变更，**传统云WAF通过DNS重定向的方式，将需要防护的WEB服务器的DNS定向到“WAF”上，WAF再通过反向代理的方式访问WEB服务器。
- **新的安全问题引入：**1）云WAF不在需要保护的WEB Server用户管理的范畴，所有WEB访问数据经过云WAF是否放心数据安全？2）云WAF到WEB Server的后端访问路径，安全性如何保障？
- **技术实现方案：**云WAF是否为云？传统软硬件一体化设备、软件反向代理等WAF同样可以实现，没有体现出云的特征！

总结：传统的云WAF采用了互联网的软件服务模式，提供了“SecAAS”（安全作为服务）需求的特性，而并未根除WEB应用安全的最终需求，云的宣传只是一种噱头。

实例剖析：WEB应用安全从传统到云计算的演进方案—有云CloudASG

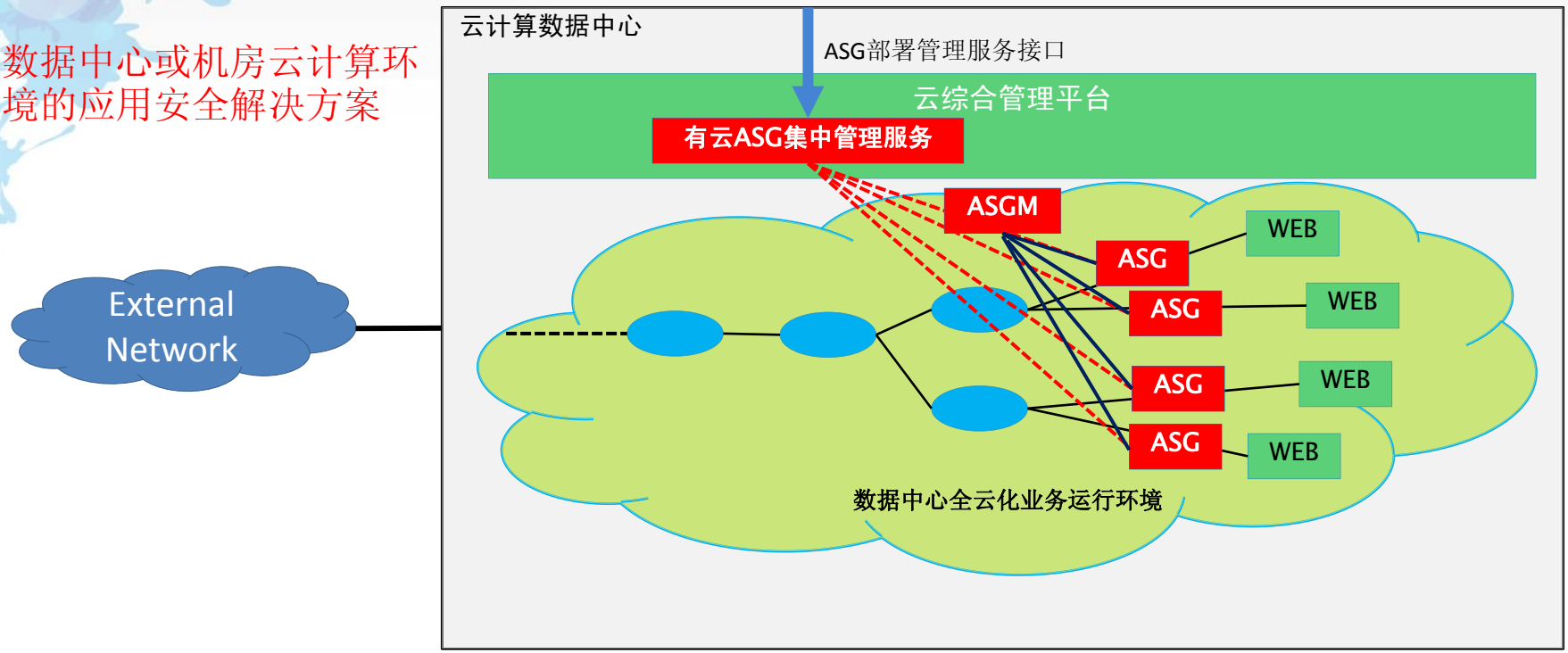


对于传统数据中心应用，大规模Web集群的访问数据量超过每秒数GB，传统的WAF无法进行部署防护，且管理维护复杂。有云CloudASG的特点：

- **部署简易：**有云CloudASG通过集中部署安全防护云的方式，用户环境只需将Web流量通过简单的策略路由的形式引入到CloudASG中，CloudASG通过ASG实例对Web流量进行安全检测，实现Web应用安全的防护。同时，CloudASG还可以与数据中心管理联动，对持续攻击的IP地址等实现黑名单阻断，即在核心路由侧对恶意IP执行阻断，防止DOS攻击
- **扩容方便：**客户业务增加，Web流量随之增大，对于安全防护来说，仅需要在CloudASG中增加通用服务器资源，采用云计算典型的硬件即插即用的方式即可，无需额外的配置
- **CloudASG与业务完全解耦：**出现故障时，客户可以通过对交换机策略路由的配置，直接跳过CloudASG，恢复与部署简便
- **集中管理与开放接口：**大规模应用安全防护，CloudASG提供集中地管理平台ASGM，可以方便安全防护的配置，同时ASGM开放接口，用户可通过开放接口查询安全攻击日志数据和报表等

实例剖析：WEB应用安全从传统到云计算的演进方案—有云CloudASG

数据中心或机房云计算环境的应用安全解决方案



在数据中心云计算环境中，有云CloudASG通过插件式管理方式，利用云平台的自动化部署特性，将Web应用防护实例动态的关联部署到待防护的Web服务器前端，在虚拟化环境中采用SDN引流的方式实现对Web服务的安全防护。

有云CloudASG特点

- 硬件平台采用通用硬件服务器，CloudASG通过云平台自动化镜像的方式进行部署，完全实现软硬件解耦，产品的可靠性采用了互联网的典型架构优势，不再依赖于传统高可靠性的专用硬件平台
- 云传统硬件WAF和云WAF相比，有云CloudASG作为客户环境应用安全解决方案的一部分，不需要改变客户现有服务的配置，数据流量的安全性局限于客户环境管理。
- 部署模式简单：在传统型数据中心，有云CloudASG部署为一个专用的“云WAF”平台环境；在云计算数据中心中，有云CloudASG通过标准的云管理平台，运用有云ASG管理服务进行自动化安全应用部署，动态解决客户环境WEB应用安全问题
- 可靠性：可靠性充分利用云平台的自动化监控、迁移、弹性伸缩等优势解决
- 增扩容：增扩容简单，无须重新制定解决方案，仅需要按照云计算的模式，进行硬件资源的增量配置即可实现
- 性能优势：有云CloudASG的性能仅与硬件资源能力相关，原则上可以无限扩展。
- 运维管理简单：有云CloudASG提供统一的ASGM集中管理平台，实现对各实例ASG的分布式集中管理，防护策略相关配置简易。有云CloudASG支持直连防护、流量监控等多种防护和检测模式

总结：有云Cloud ASG提供了灵活的部署框架模型，极大的降低了运维管理成本，较传统软硬件一体机及传统云WAF方案，安全性、可靠性、可维护性和可操作性具备绝对的优势，对传统数据中心演进以及云计算数据中心增扩容能够平滑过渡和支持。

Q&A

THANKS

SequeMedia 盛拓传媒 | IT168 www.it168.com | ChinaUnix | ITPUB