第五届安天网络安全冬训营

网络空间威胁对抗技术与实战研讨会

暨 关键信息基础设施保护实践论坛

“云”网络空间的威胁对抗和实战

北京上元信安技术有限公司

郑曙光

红旗漫卷

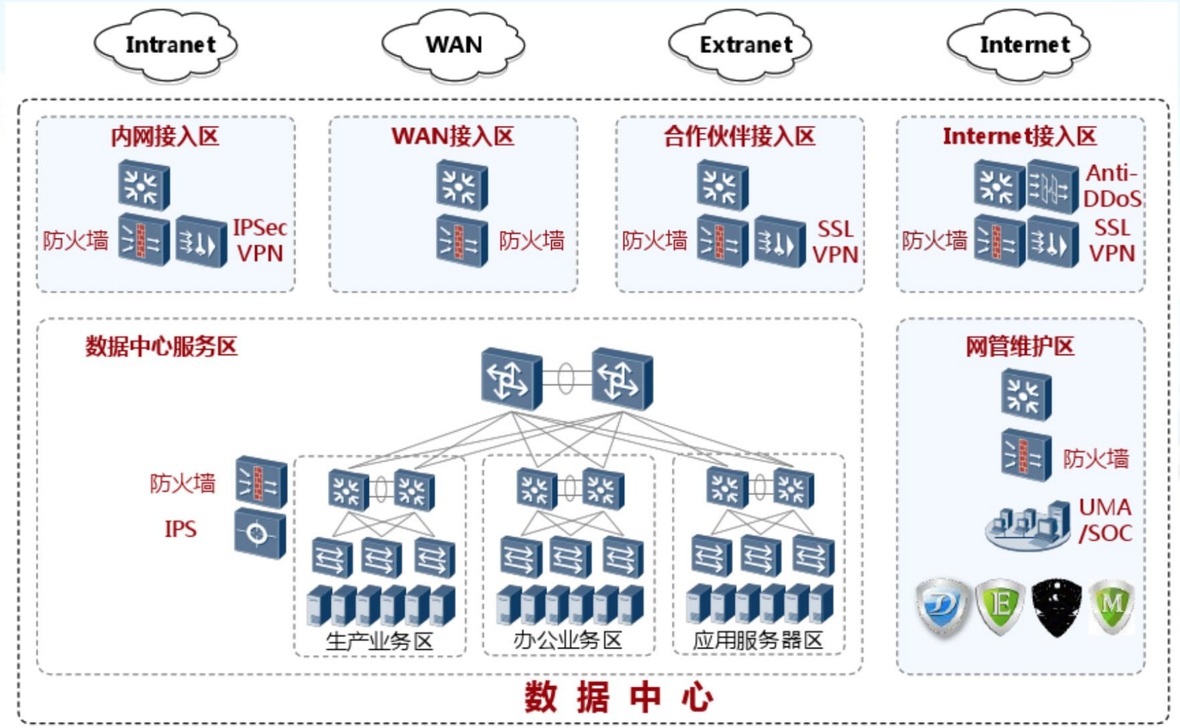
敌情想定是前提，网络安全实战化

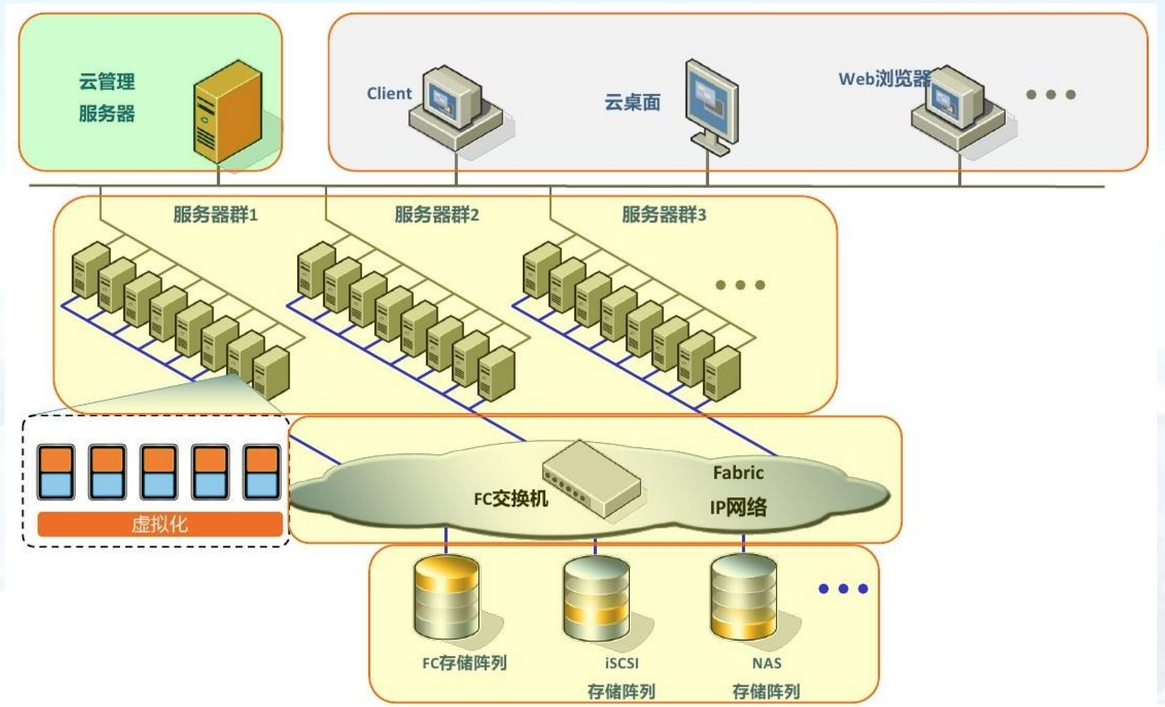
提纲

- 云化数据中心（私有云）内安全防护的困境
- 上元私有云安全的解决方案 — 护云
- 私有云内安全防护的实战分享

1 数据中心云化带来的安全困境

数据中心上云前后的IT架构对比

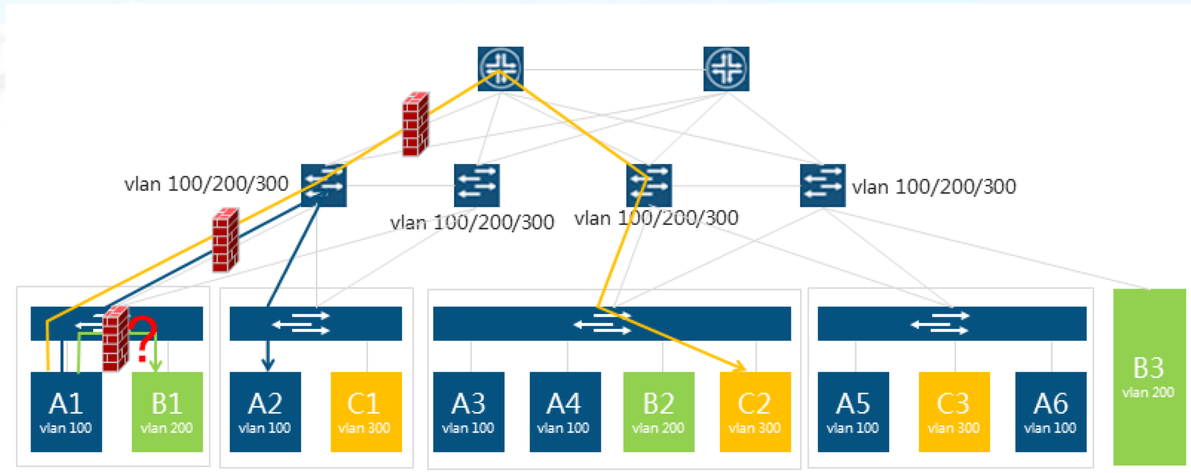




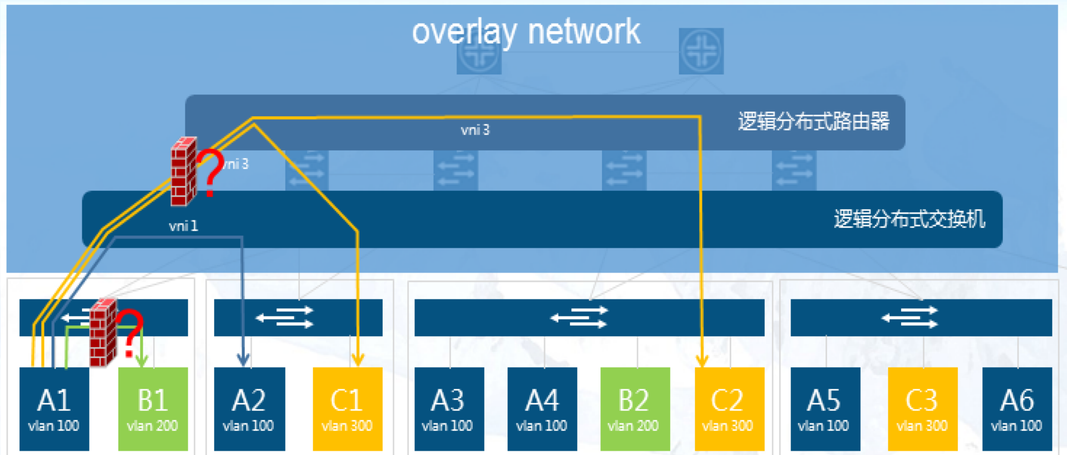
- 各个区域可以通过物理隔离
- 用VLAN划分安全域
- 安全域之间有清晰的物理边界，所以可以部署硬件安全设备如防火墙做安全域间的访问控制与深度安全检测

- 计算、网络、存储都以分布式、横向可扩展的方式集中于云数据中心
- 云数据中心的互联网接入边界依然可以根据物理资源来划分，但其他区域比如内部接入区、合作伙伴接入区等由于虚拟化技术引入导致不能再简单的根据物理边界或VLAN来划分
- 安全域边界的消失从而导致传统的安全防护措施难以实施

数据中心上云遇到的安全困境



- 用VLAN划分安全域，虚拟化系统和物理接入交换机都需要配置VLAN
- 跨节点的安全域之间有清晰的物理边界，所以可以部署硬件安全设备如防火墙做安全域间的访问控制与深度安全检测
- 同节点的安全域之间访问不出物理节点，所以硬件安全设备无法部署



- 用VXLAN构建逻辑网络，通过VNI划分安全域
- 跨节点的安全域之间是VXLAN逻辑网络，传统硬件安全设备或安全软件无法部署
- 同节点的安全域之间访问不出物理节点，所以硬件安全设备无法部署

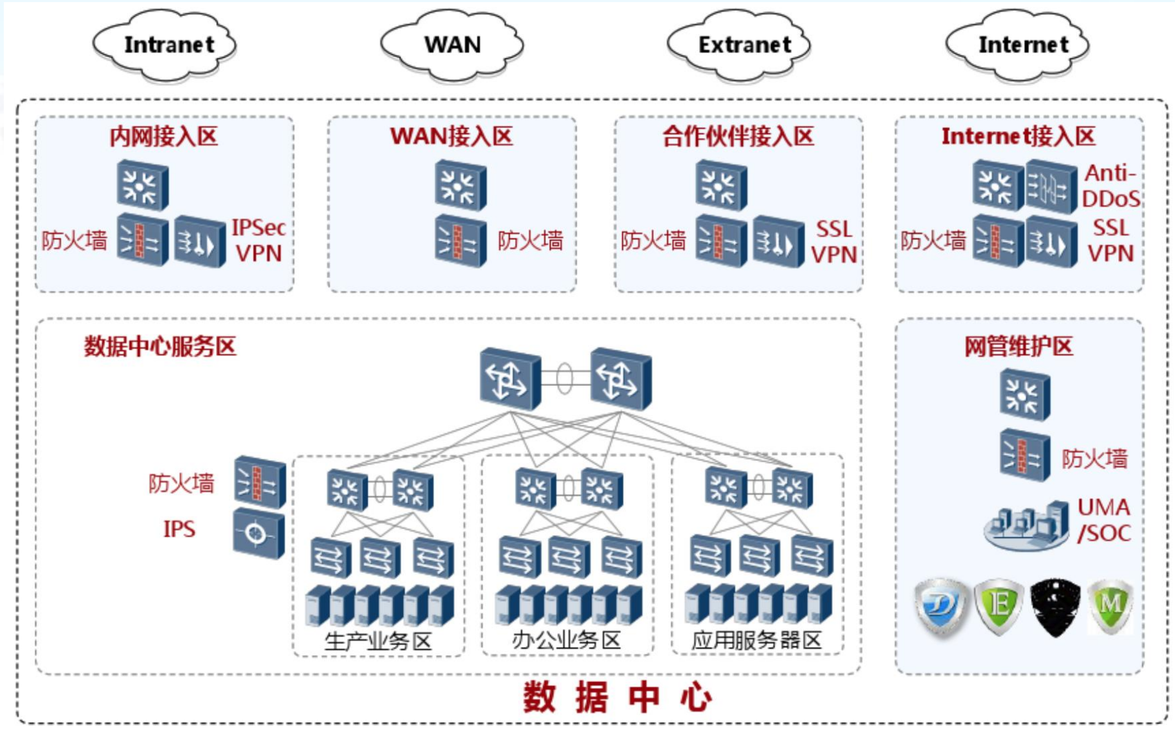
数据中心上云遇到的安全困境

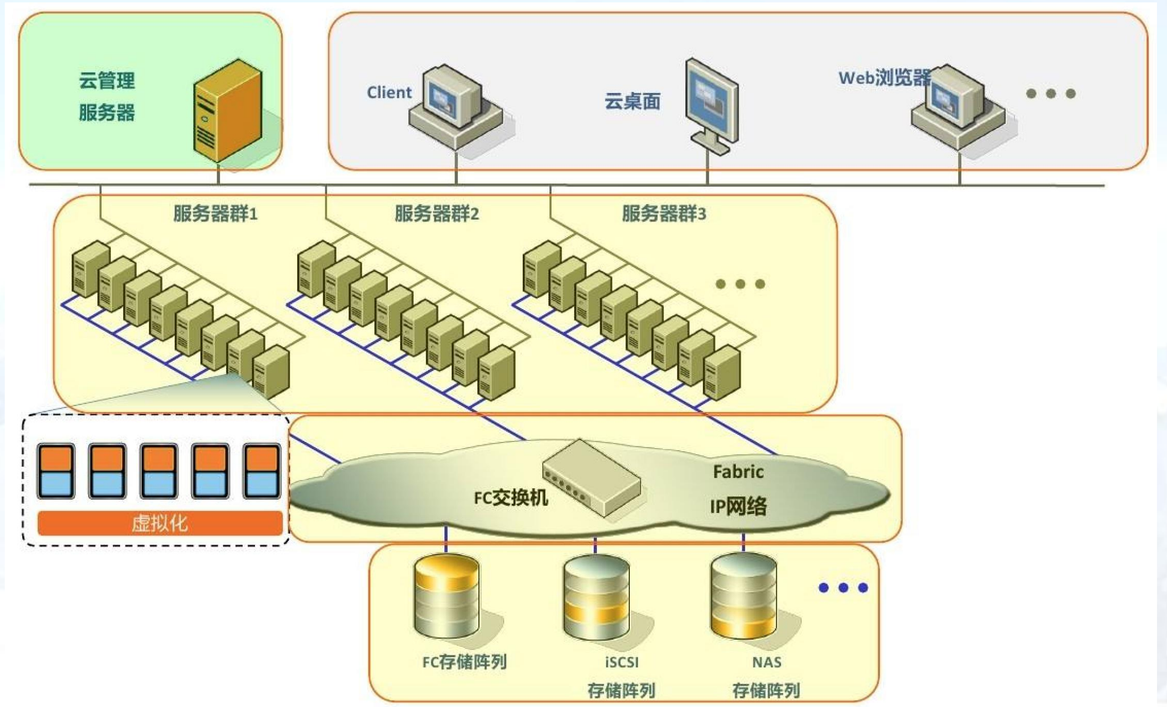
- **传统安全解决方案无法直接应用到私有云场景：**
  - 网络边界消失导致基于网络边界防护的措施无法实施
  - 单个虚机或容器的性能不高导致基于主机防护的措施无法实施或得不偿失
  - 虚拟化层的安全漏洞补丁需无干扰升级
  - 私有云动态环境需要安全策略能够自适应
  - 随时、按需提供安全服务

- **私有云独特安全风险急需有效解决方案：**
  - 虚拟化安全：虚拟化层的引入，扩大了被攻击面，一旦虚拟化层被击穿，波及整个云内的业务稳定
  - 东西向流量不可见：云内70%流量都是东西向流量
  - 租户隔离达到物理级：资源隔离、网络隔离、数据隔离
  - 云数据防泄漏、隐私保护
  - 攻击溯源困难：多样的网络访问来源和方式，攻击方法不可预知
  - 云操作：如何区分误操作与恶意操作
  - 运维复杂度显著提升：如何实现自动化运维、可视化运维

2 上元私有云安全解决方案-护云

消除数据中心上云的安全障碍





- 上元通过网络层切入，将云计算和网络安全有效整合，使得传统信息安全防护措施能够无缝的应用到云基础设施，同时能够充分利用已有的安全防护系统和设备，减少企业在安全方面的重复投入
- 上元借助在云计算和网络安全领域的积累，提供不低于传统数据中心的安全防护能力，并能够有效应对云的新型安全威胁，使数据中心安心上云

上元云安全-护云介绍

护云vRouter：

- 安装在每台物理机上的一个轻量级agent
- 基于hypervisor层之上；
- 与护云控制器配合，可构建/感知/接入overlay网络；
- VM间的访问控制；
- 引流；

护云控制器：护云的大脑

- 可构建/感知/接入overlay网络；
- 安全服务链的编排，所画即所得；
- 流量可视化；
- 威胁统计和分析；

使用OverLayer技术，支持VXLAN、MPLS over GRE、MPLS over UDP三种隧道封装技术

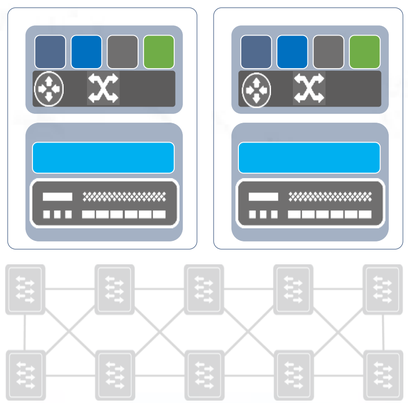
安全组件：

- NGFW、AVG、ACG、WAF、IPS/IDS、LB；
- 可硬可软；

CSG：云交换网关

- 位于云数据中心网络边界
- 支持overlay网络
- 按租户对外提供安全服务

护云提供云内基础设施的安全栈



控制平面

- 与云管理平台对接，按需分配安全资源，简化安全配置；
- 上线新的业务系统，只要在护云的可视化界面上进行简单的操作，即可实现安全防护

VM

- VM层：通过vRouter实现访问控制、封闭端口，收缩攻击面；同一物理机上VM间的访问控制、流量可视；
- Overlay网络：可构建SDN网络，划分逻辑安全域；实现VXLan内或间的安全策略，通过安全服务链实现NGFW功能（FW、IPS/IDS、WAF、AVG、ACG等）

Overlay网络

Hypervisor

- Hypervisor层：通过vRouter实现引流，按需抓取流量或分析；虚机逃逸感知；

物理网络

- 物理网络：通过部署软件化的安全组件，实现传统链路层、网络层的安全防护；通过IPSec构建高安全级别网段，如运维、敏感业务区等
- 物理区域：可构建独立的安全资源池；可利旧，节约成本

护云提供云内安全能力的扩展框架

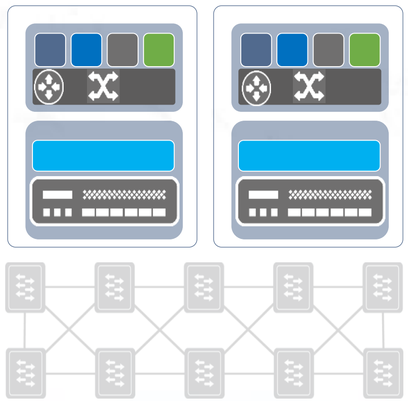
威胁感知/情报

控制平面

- 护云控制器北向接口和威胁感知系统、第三方威胁情报系统对接，对已感知的威胁及时响应，把安全策略下发至安全组件，实现主动防御/协同防御

GuestOS

- 可以和主机防护软件（如安天智甲）联动，实现云内整网安全协同



第三方分析系统

VM

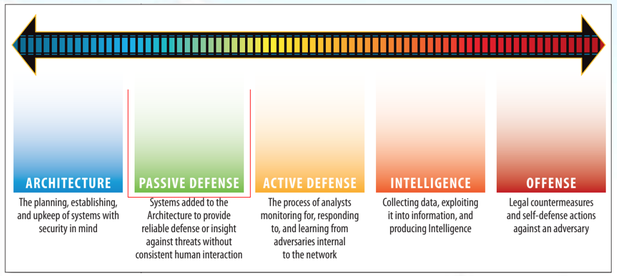
Overlay网络

Hypervisor

- 利用护云引流功能，把流量按需引至第三方安全设备、分析系统或探针，如安天的探海、蜜网、欺骗系统等，可以做进一步的威胁对抗

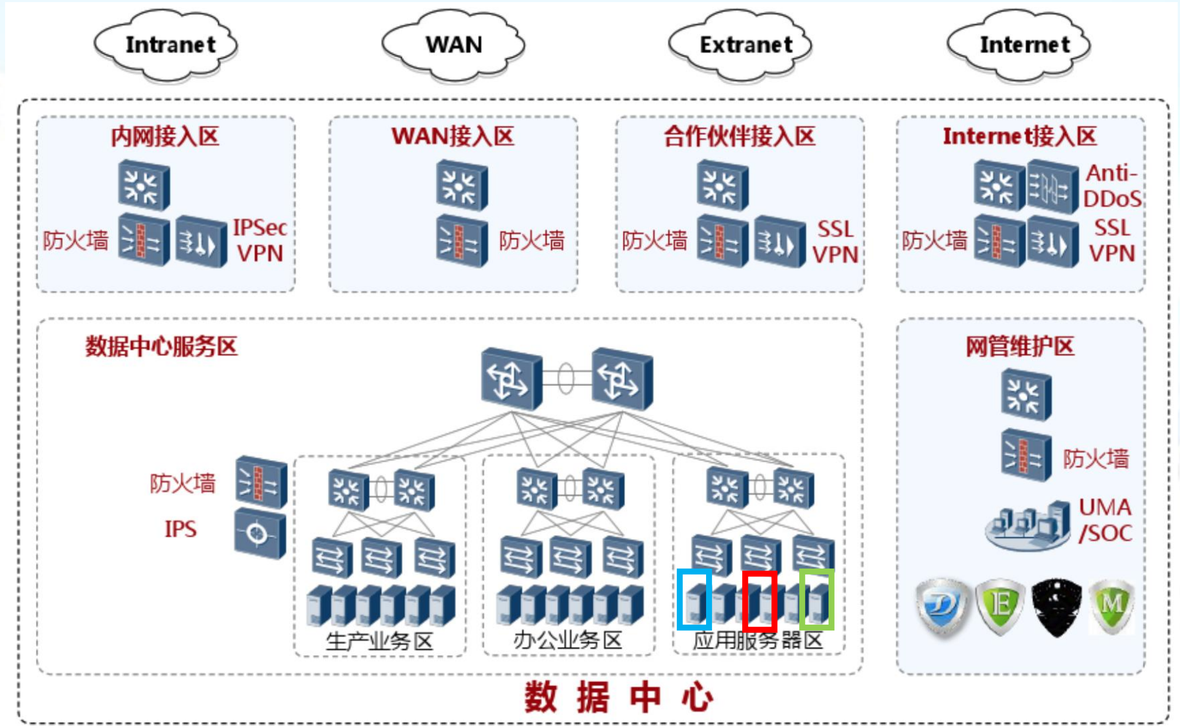
物理网络

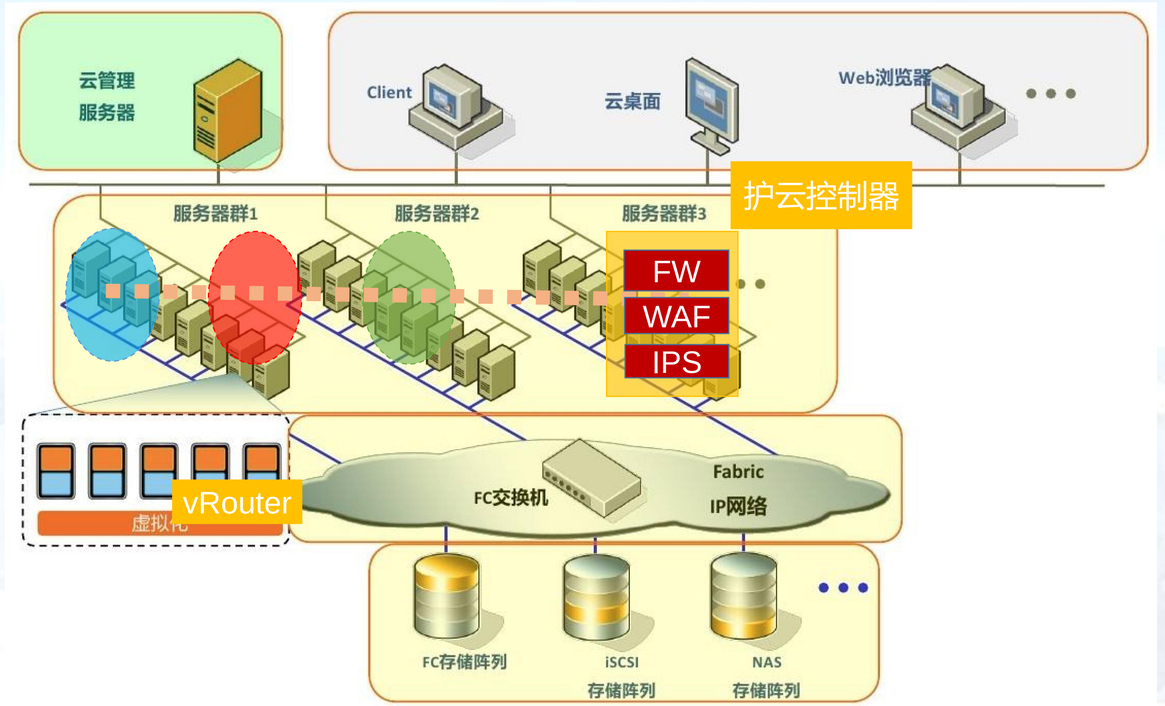
从被动防御向积极防御的叠加演进



3 私有云内安全防护的实战

传统数据中心上云时，安全措施的平滑迁移





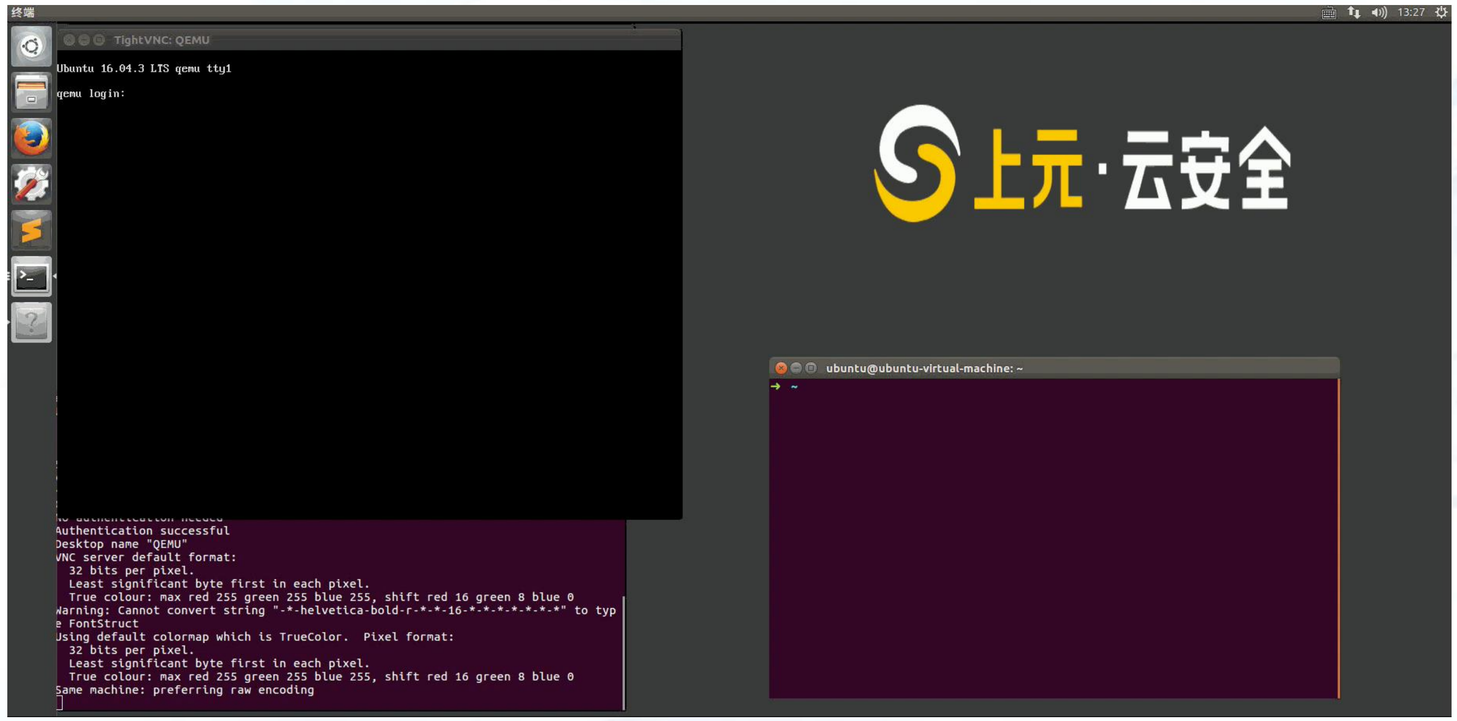
- 在三个物理独立的服务器上安装应用系统
- 根据需要进行物理/二层/三层的隔离
- 根据安全等级要求，部署相应的物理安全设备

- 安装护云控制器和vRouter
- 分配计算、存储资源，并划分三个逻辑区域
- 分配安全资源池
- 根据逻辑区域间的安全防护要求，在护云控制器进行安全服务编排

私有云纵深防御实践之一：WannaCry病毒的敌情假想

VS

私有云纵深防御实践之二：虚机逃逸



qemu+kvm的逃逸

CVE编号：CVE-2015-5165，CVE-2015-7504

修补时间：2015-08-03修补CVE-2015-5165，2015-12-07修补CVE-2015-7504

影响范围：qemu 2.4及2.4以前版本

原理：

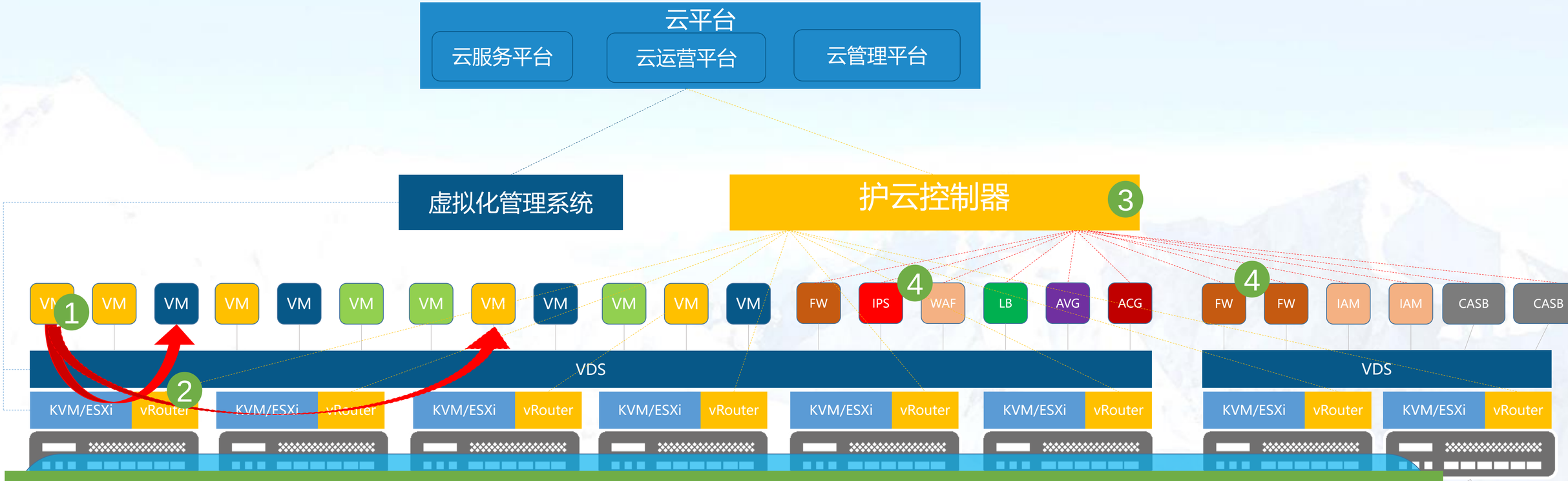
CVE-2015-5165 内存泄漏漏洞，QEMU进行RTL8139网卡设备仿真模拟时，RTL8139网卡在cplus模式下存在内存泄漏漏洞，这允许攻击者可以读取内存信息。

CVE-2015-7504 堆溢出漏洞，QEMU进行PCNET网卡设备仿真模拟时，PCNET网卡在pcnet_receive函数中存在堆溢出漏洞，这允许攻击者可以覆盖一个irq关键结构体，达到执行代码的效果。

私有云纵深防御实践之二：虚机逃逸

- 通过虚机逃逸漏洞，破坏/控制宿主机，或窃取同一宿主机上其他虚拟机的数据
- 通过虚机迁移渗透到更多的宿主机

私有云纵深防御实践之二：虚机逃逸



- 部署主机防护软件，防范恶意行为和病毒入侵
- vRouter在Host OS层级监控来自虚机的操作行为和权限，一旦发现异常或越权，立即向控制器发送告警
- 进行东西向的隔离、访问控制、深度安全检查，防止非法操作
- 给安全域边界或云边界的安全设备提供虚机逃逸漏洞的虚拟补丁

第五届安天网络安全冬训营

网络空间威胁对抗技术与实战研讨会

暨 关键信息基础设施保护实践论坛

Thank You

wtc.antiy.cn

红旗漫卷

敌情想定是前提，网络安全实战化