The 8th China Cloud Computing Conference
第八届中国云计算大会
技术融合 应用创新

构建安全的云计算平台

新致云　　田奎

目录

PART 1

概述

随着用户对云接受程度的增加和云计算商业模式的成熟，越来越多的个人和企业都开始使用云。移动、大数据、物联网、社交等应用类的发展带动云发展的同时也给云带来了安全方面的巨大挑战。云计算相对于传统的计算，使用模式发生了革命性的变化，安全也随之发生很大变化：威胁更多，攻击面更大，目标价值更高，影响面更广。因此对于安全防范也面临新的挑战，本议题主要深入分享包括物理安全、数据安全、计算安全、网络安全、威胁分析、防护探讨等一系列问题。

PART 2

云平台基础架构安全

- 云平台整体架构安全
- 云平台虚拟化安全

云平台整体架构安全

云平台整体架构安全既包括云平台物理架构的安全，也包含云平台虚拟架构的安全。

云平台物理架构安全包含机房的安全，云平台物理网络架构的安全，在物理网络架构安全设计中要包含防范各种各样的威胁，如病毒，木马，DDos 攻击，Web 攻击等。

云平台虚拟架构的安全中，传统的安全设备可能使不上力，比如同一宿主机上的虚机之间的安全访问，这就要借用虚拟防火墙。在云平台虚拟架构的安全设计中，我们将网络安全设备资源池化，形成一个资源池，在需要安全的地方调用合适的安全资源。且这种安全设备资源池化后，具有弹性扩展功能，更能适应云平台的弹性伸缩的架构。

云平台整体架构安全

统一网络架构

物理网络平台安全

防Ddos安全设计

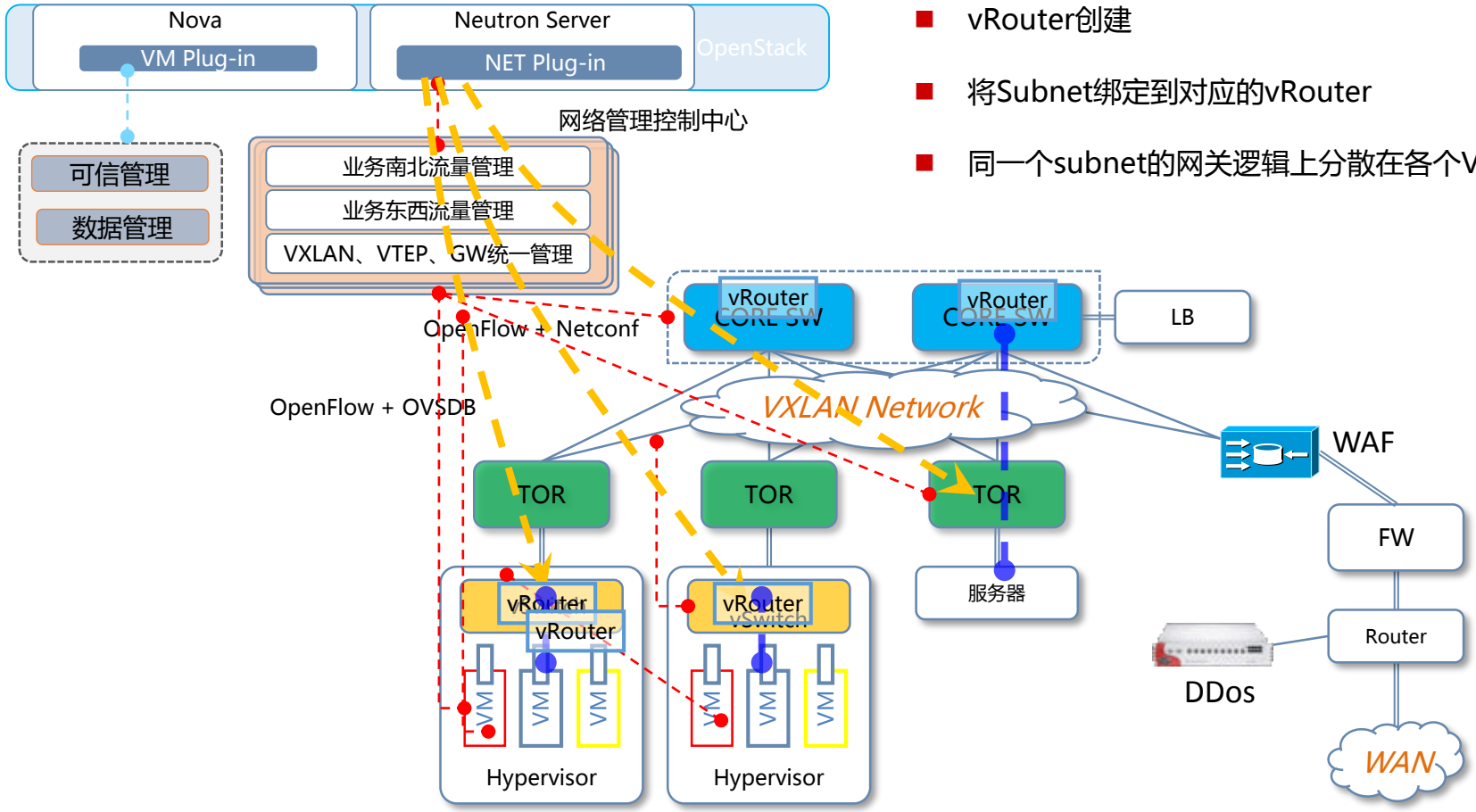
虚拟网络平台安全

呼唤

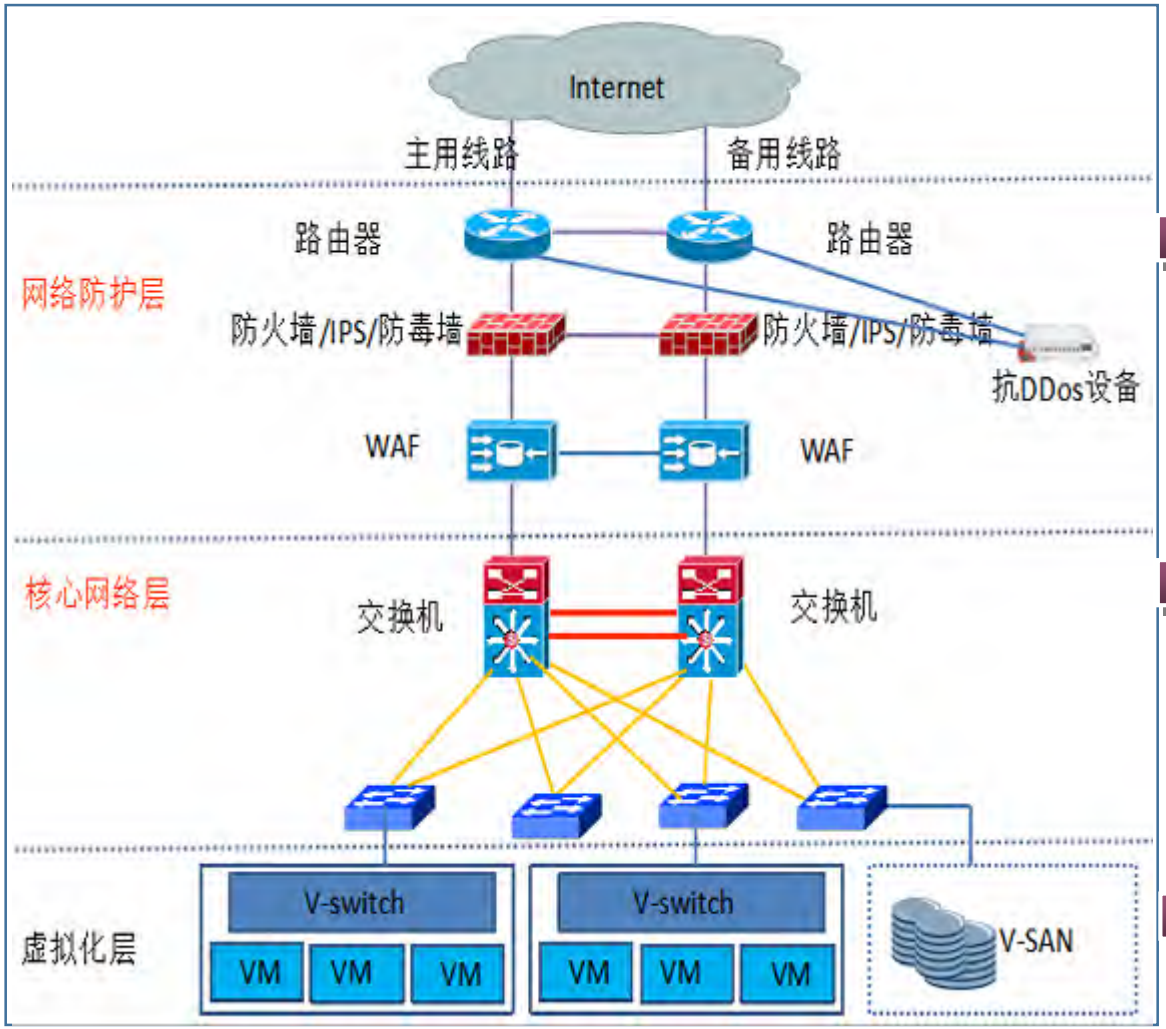
云平台整体架构安全

云平台整体架构安全-统一的网络构架

- 创建网络：VXLAN
- vRouter创建
- 将Subnet绑定到对应的vRouter
- 同一个subnet的网关逻辑上分散在各个VTEP上



云平台整体架构安全-物理网络平台安全



网络防护层通过抗DDOS设备对进入数据中心的流量进行清洗，下一代防火墙和WAF能对3层到7层数据进行。

核心交换机间通过虚拟化成一台设备，保证网络的高可用性。

做到Hypervisor、虚机安全；用户数据的安全隔离；存储资源重分配之前信息删除。

云平台整体架构安全-DDOS

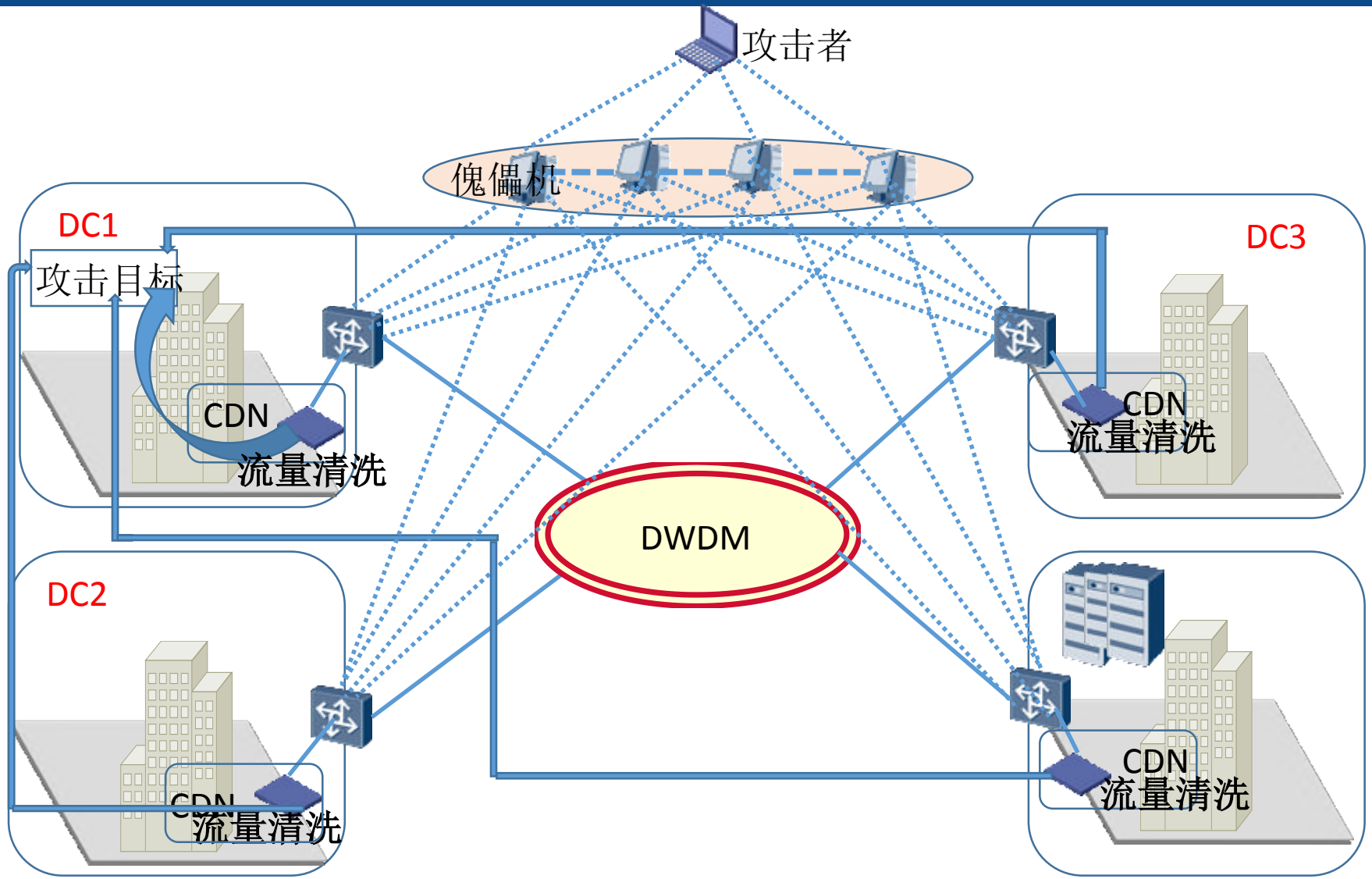
DDos攻击介绍：

指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力。

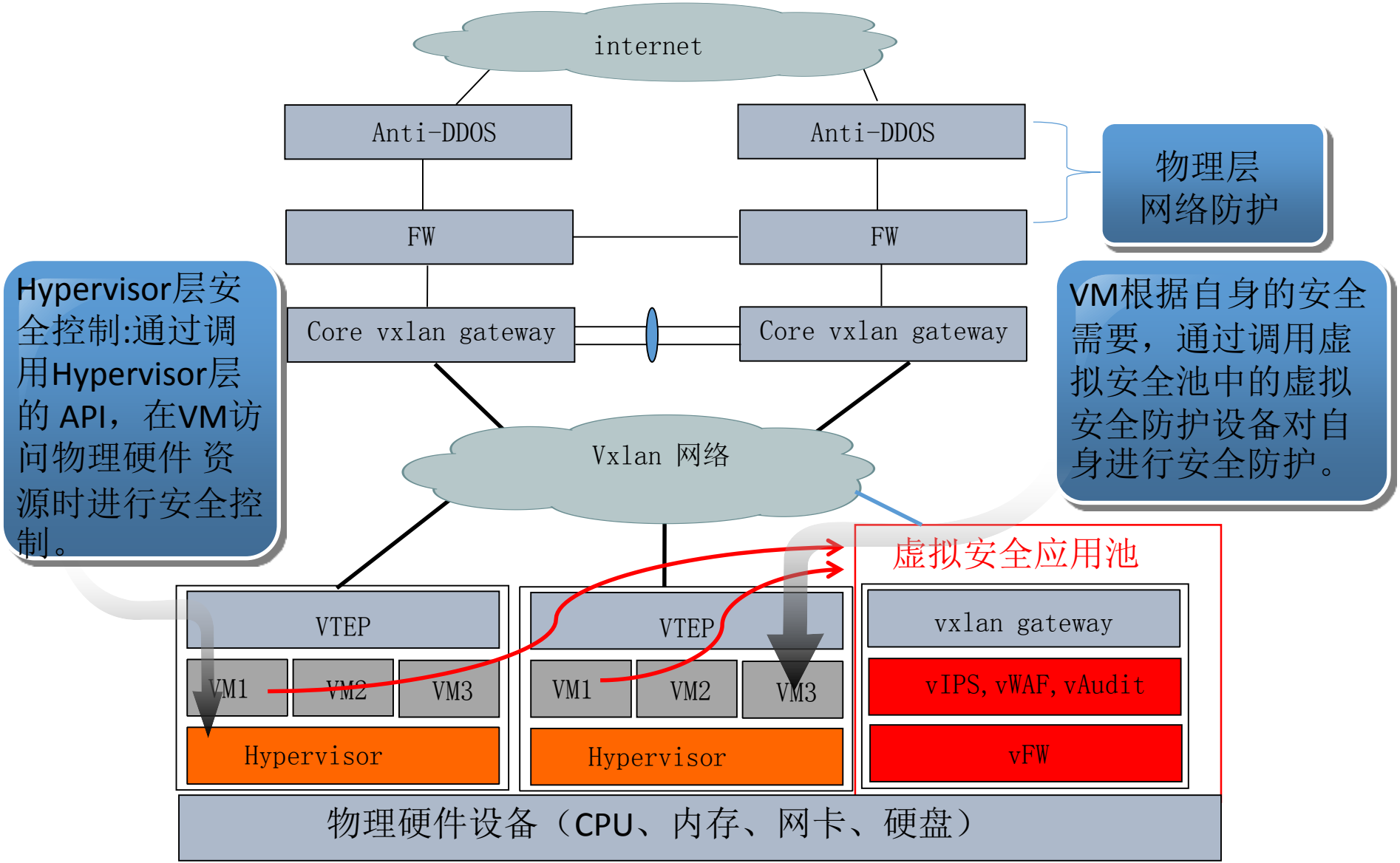
防DDos攻击方法：

攻击者控制多台傀儡机从世界各地向攻击目标发动攻击，其实攻击的是我们在各个数据中心部署的CDN网络,CDN中的流量检测设备检测到后，送给清洗设备，清洗后的流量就送给攻击目标，这样就减轻了攻击目标的压力。

云平台整体架构安全-DDOS攻击



云平台整体架构安全-虚拟网络平台安全



云平台虚拟化安全

同台物理机器上运行多台虚拟机，共用cpu资源，实现对CPU指令集的扩展和虚拟机运行模式的控制。

内存安全

同台物理机器上运行多台虚拟机，多台虚拟机共享使用物理主机的内存空间。

存储安全

虚拟机镜像无论在静止还是运行状态都有被窃取或篡改脆弱漏洞。对应的解决方案是在任何时候对虚拟机镜像进行加密和逻辑镜像隔离。

网络安全

虚拟化对网络安全带来巨大的威胁，虚拟机间可能通过内存而不是网络进行通讯，因此这些通讯流量对标准的网络安全控制来说是不可见的。

云平台基础架安全-虚拟化安全

- CPU虚拟化安全性保证
- 内存虚拟化安全性保证
- 存储虚拟化安全性保证
- 网络虚拟化安全性保证

呼唤

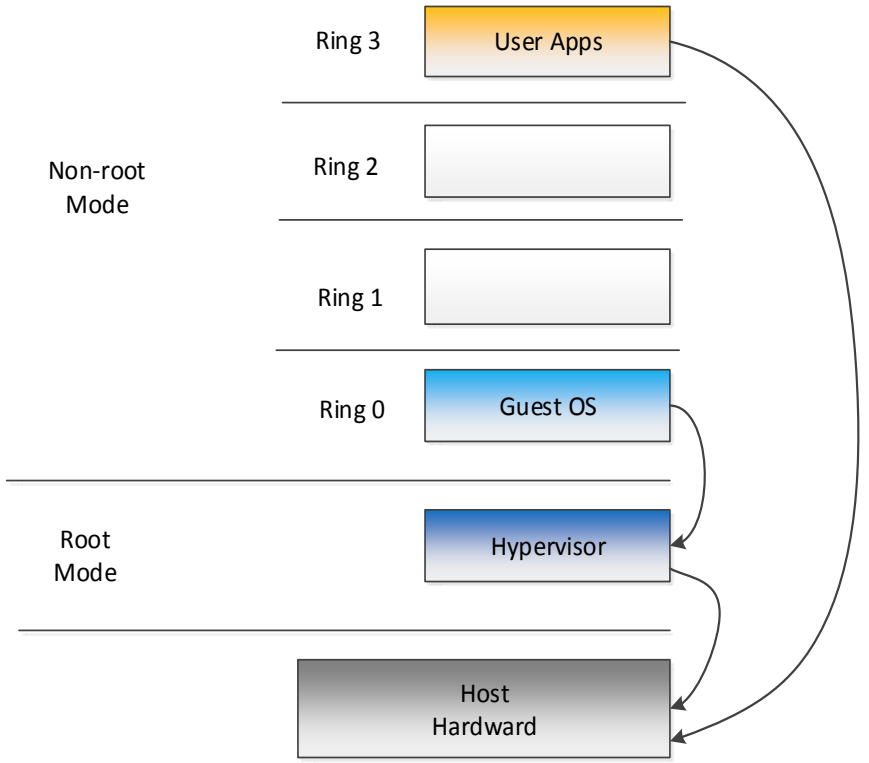
虚拟化安全

虚拟化安全--CPU虚拟化安全性保证

cpu虚拟化安全：

1.传统的软件辅助虚拟化使用优先级压缩和二进制代码翻译相结合的方式来实现完全虚拟化，但这种方式存在虚拟化漏洞。

2.基于intel VT-x硬件虚拟化的技术，对cpu的指令进行扩展，对指令的优先级增加了一个维度，即root模式和非root模式，Hypervisor运行在root模式下，客户虚拟机运行在非root模式，当执行敏感指令时被Hypervisor截获，能有效避免虚拟化漏洞。



虚拟化安全--内存虚拟化安全性保证

虚拟机运行时用到三种内存地址：

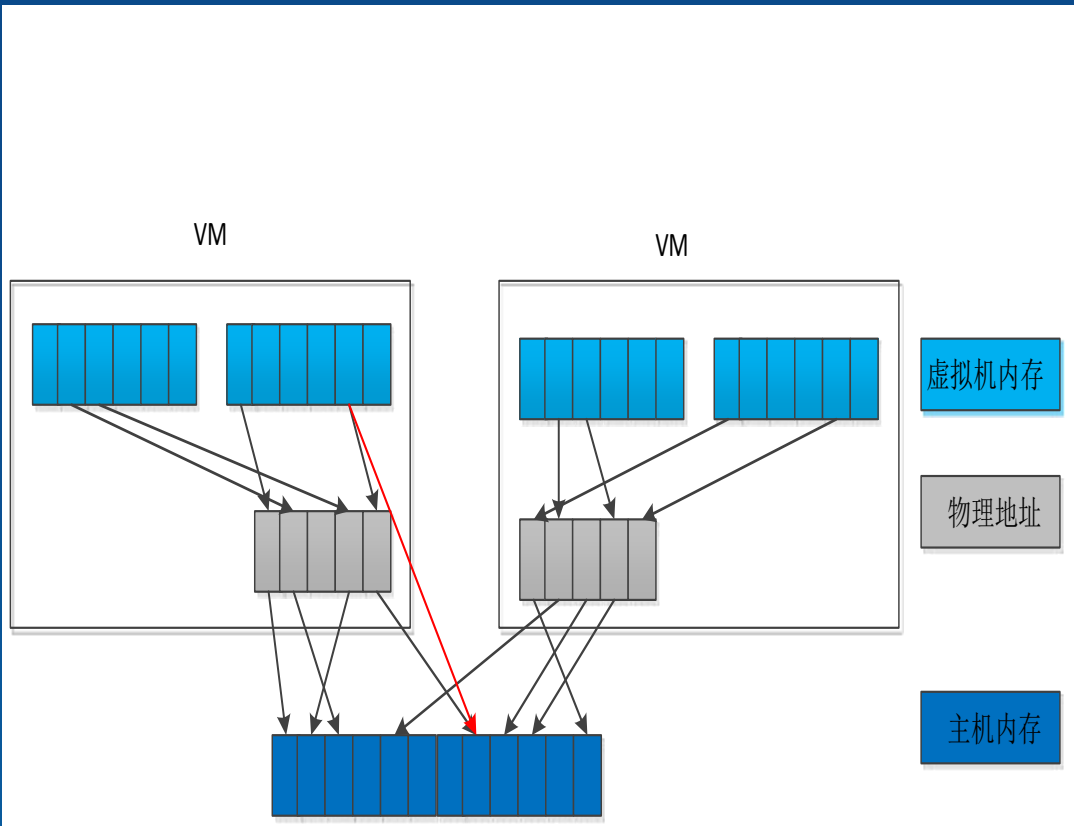
1.虚拟机虚拟地址，虚拟机物理地址，主机物理地址。

2.虚拟机的虚拟地址和虚拟机物理地址是由虚拟机操作系统完成的，

3.虚拟机物理地址和主机物理地址转换是由Hypervisor完成的。

4.基于 intel VT-x的EPT技术，一方面能加快内存访问的效率，

另一方面能够限制vm只访问分配到的内存，从而实现虚拟机之间的内存隔离。



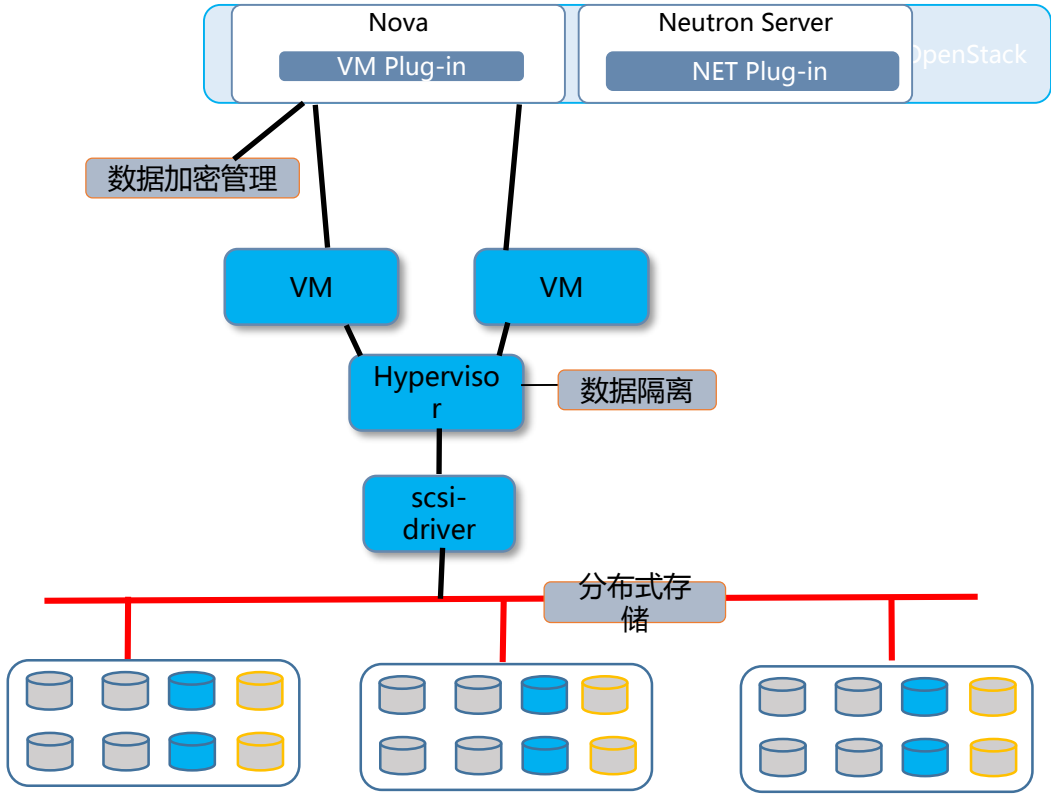
虚拟化安全--存储虚拟化安全性保证

创建虚拟机系统盘和数据盘，维护磁盘到后端存储的映射和磁盘数据加密的基本功能

1.Hypervisor实现对不同虚拟机的逻辑磁盘的管理和安全隔离。

2.分布式存储实现一份数据保存多份，防丢失。

3.分布式存储实现所有数据故障的检测和自动恢复。恢复不需要人工介入，在恢复期间，可以保持正常的数据访问。



虚拟化安全--网络虚拟化安全性保证

虚拟网络安全性保证，不同租户创建不同的vlan网络：

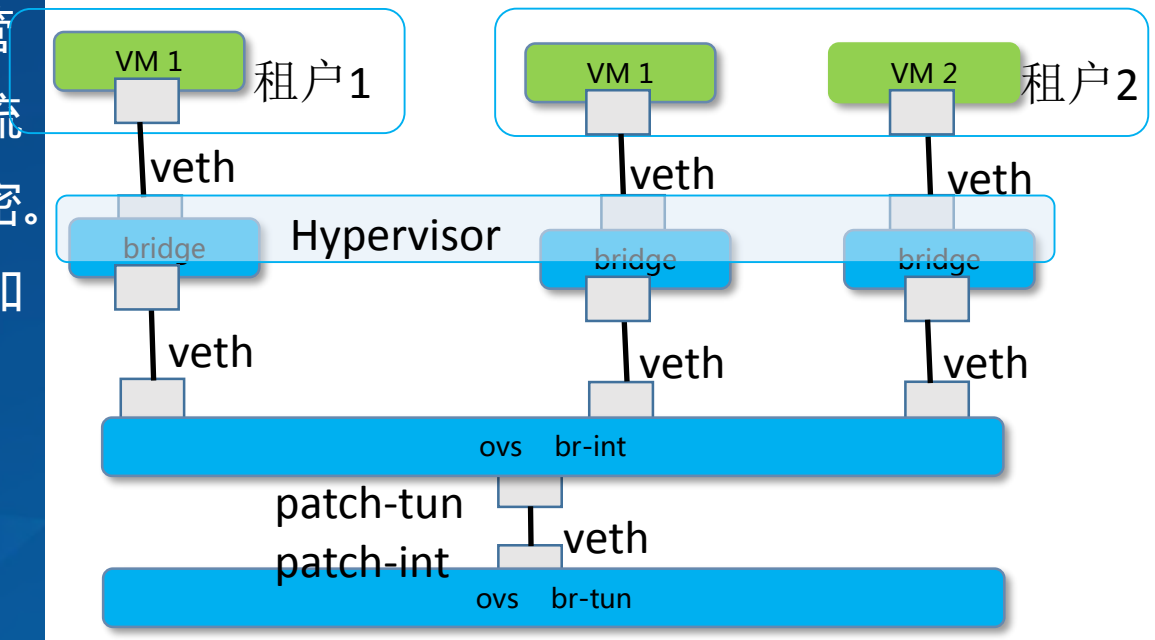
1.实现多虚拟化网络全方位的安全管理功能，所有的虚拟机数据在没有流出网络之前都可以实现网络数据加密。

2.Hypervisor实现高安全网络数据加密功能。

3.bridge实现网络的安全访问控制。

4.br-int实现不同的vlan网络划分和访问隔离。

5.br-tun实现同其它物理机器和外网的通信访问功能。



PART 3

云用户数据安全

云用户数据安全

在云中虚拟化的效率要求多个租户的虚拟机共存于同一物理资源上。虽然传统的数据中心的安全仍然适用于云环境，物理隔离和基于硬件的安全不能保护防止在同一服务器上虚拟机之间的攻击。

管理访问是通过互联网，而不是传统数据中心模式中所坚持的受控制的和限制的直接连接或到现场的连接。这增加了风险和暴露，将需要对系统控制和访问控制限制的变化进行严密监控。

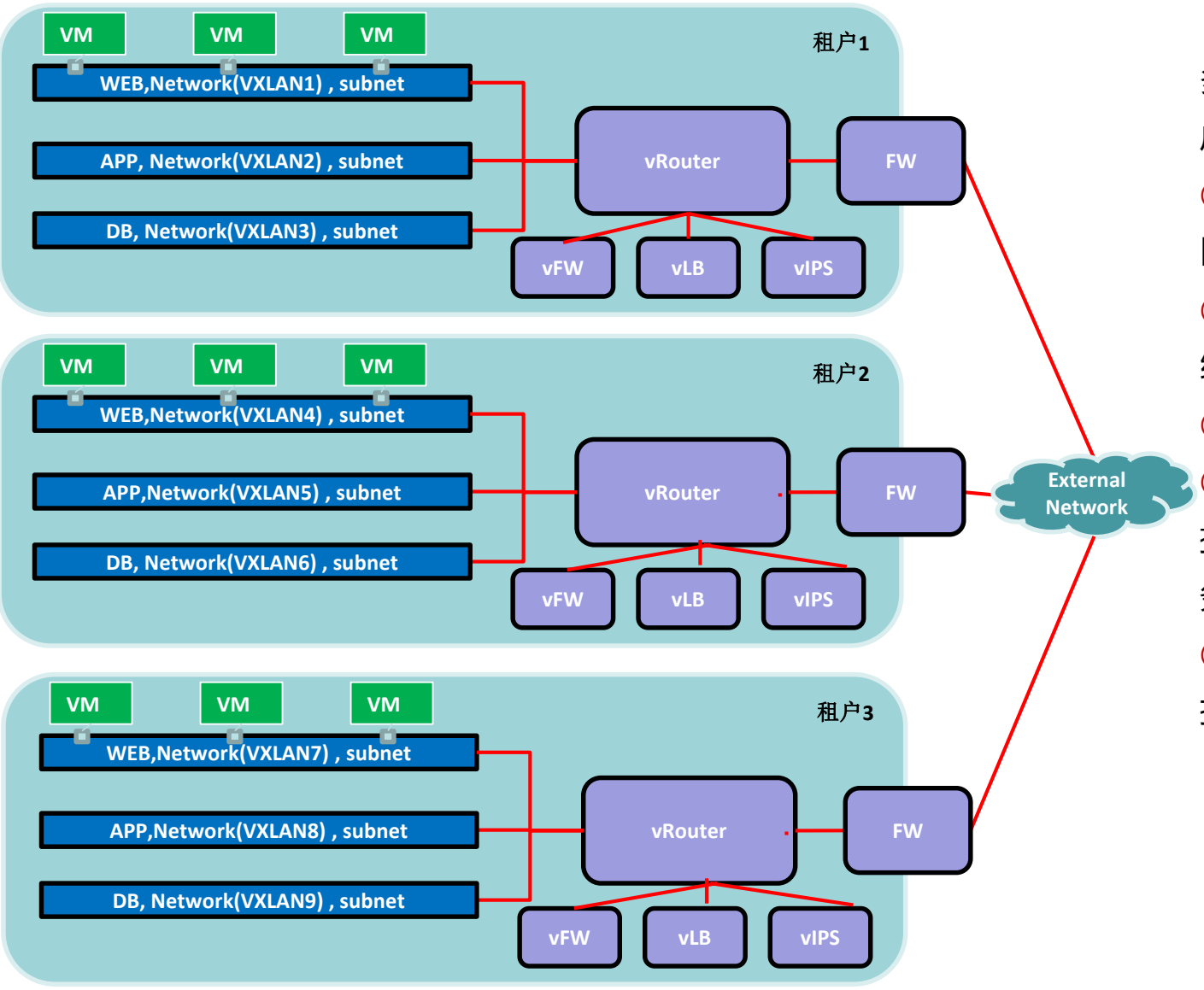
云用户数据安全

- 用户数据安全隔离
- 用户数据存储安全
- 用户数据访问控制安全
- 用户数据传输安全

呼唤

用户数据安全

用户数据安全-创建多租户逻辑隔离的安全网络



多租户基于OpenStack模型对虚拟网络进行逻辑抽象

①vRouter代表逻辑三层网关网络,分散在各个虚拟设备上。

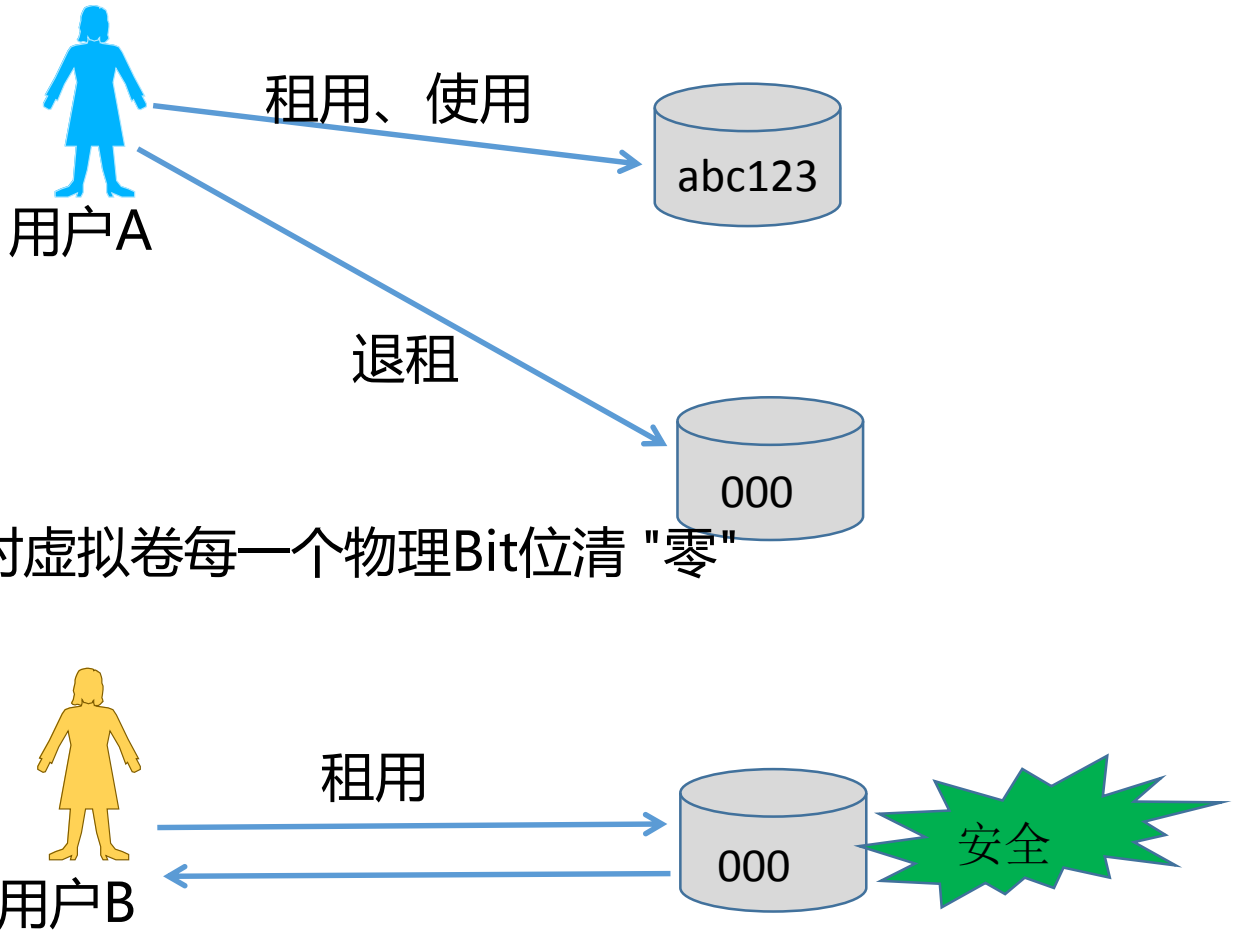
②Network，代表逻辑二层网络，分配到不通的vlan网络。

③Subnet代表某个子网网段

④网络服务功能，为每个租户提供独立的FW、LB及NAT服务

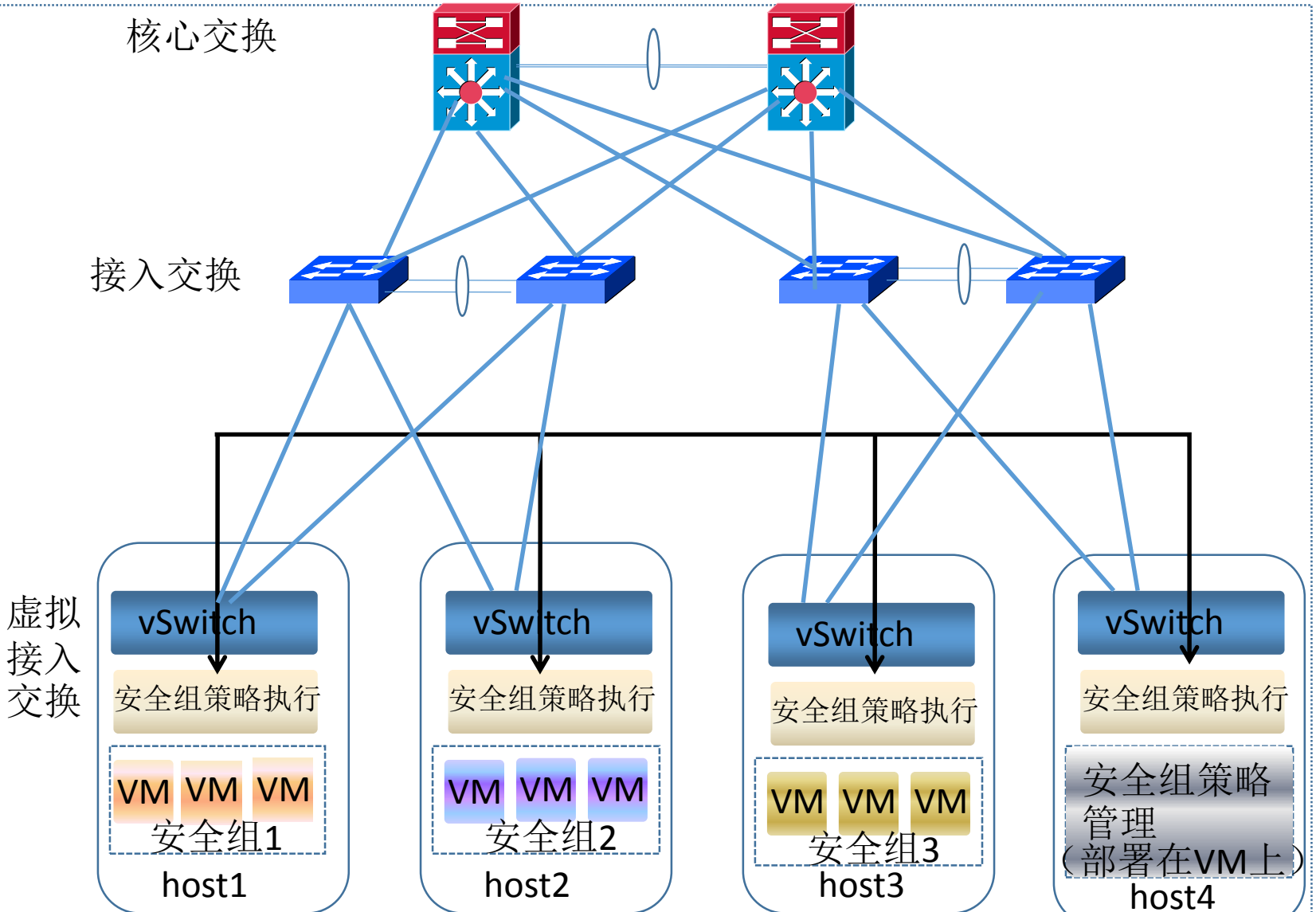
⑤租户之间相互隔离，互不干扰

用户数据安全—用户数据存储安全



对销户虚拟卷采用物理bit清零措施，确保数据不可恢复，杜绝信息泄露风险

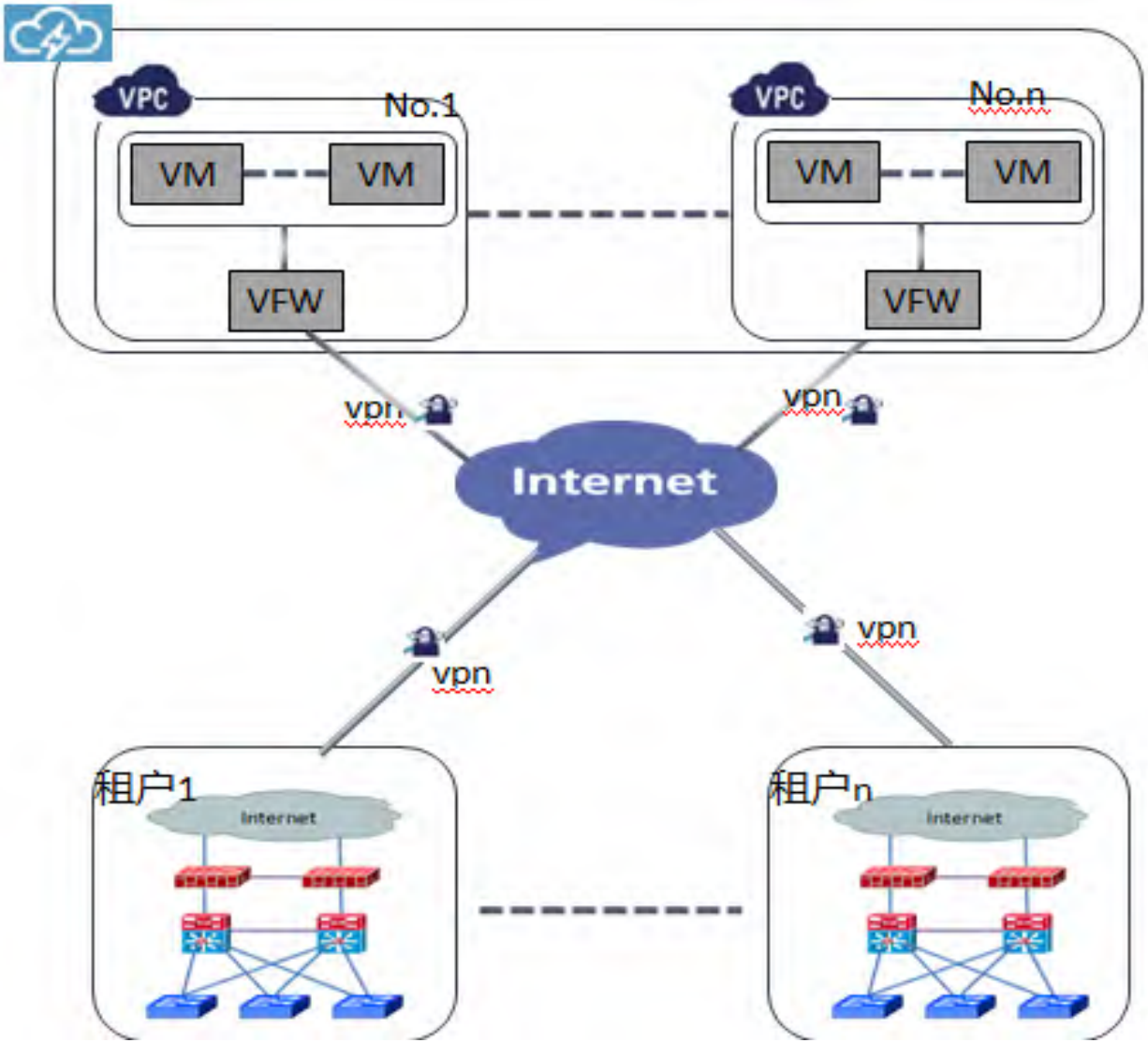
用户数据安全—用户数据安全控制



通过安全组提供VM粒度的隔离机制，每个VM一组ACL，VM迁移时安全策略自动刷新。

分布式控制策略，报文无需迂回到集中的策略控制点，避免形成性能瓶颈。

用户数据安全—用户数据传输安全



用户在访问VPC的过程中，会和数据中心中的VFW建立vpn。经过internet的数据都将被加密。

PART 4

云平台运营管理安全

云平台运营管理安全

用户管理:

•对用户帐号进行集中维护管理，为集中访问 控制、集中授权、集中审计提供可靠的原始数据。

认证授权:

•建立统一、集中的认证和授权系统，以提高 访问的安全性。

安全审计:

•建立安全审计系统，进行统一、完整的审计 分析，通过对操作、维护等各类日志的安全审计，提高 对违规溯源的事后审查能力。

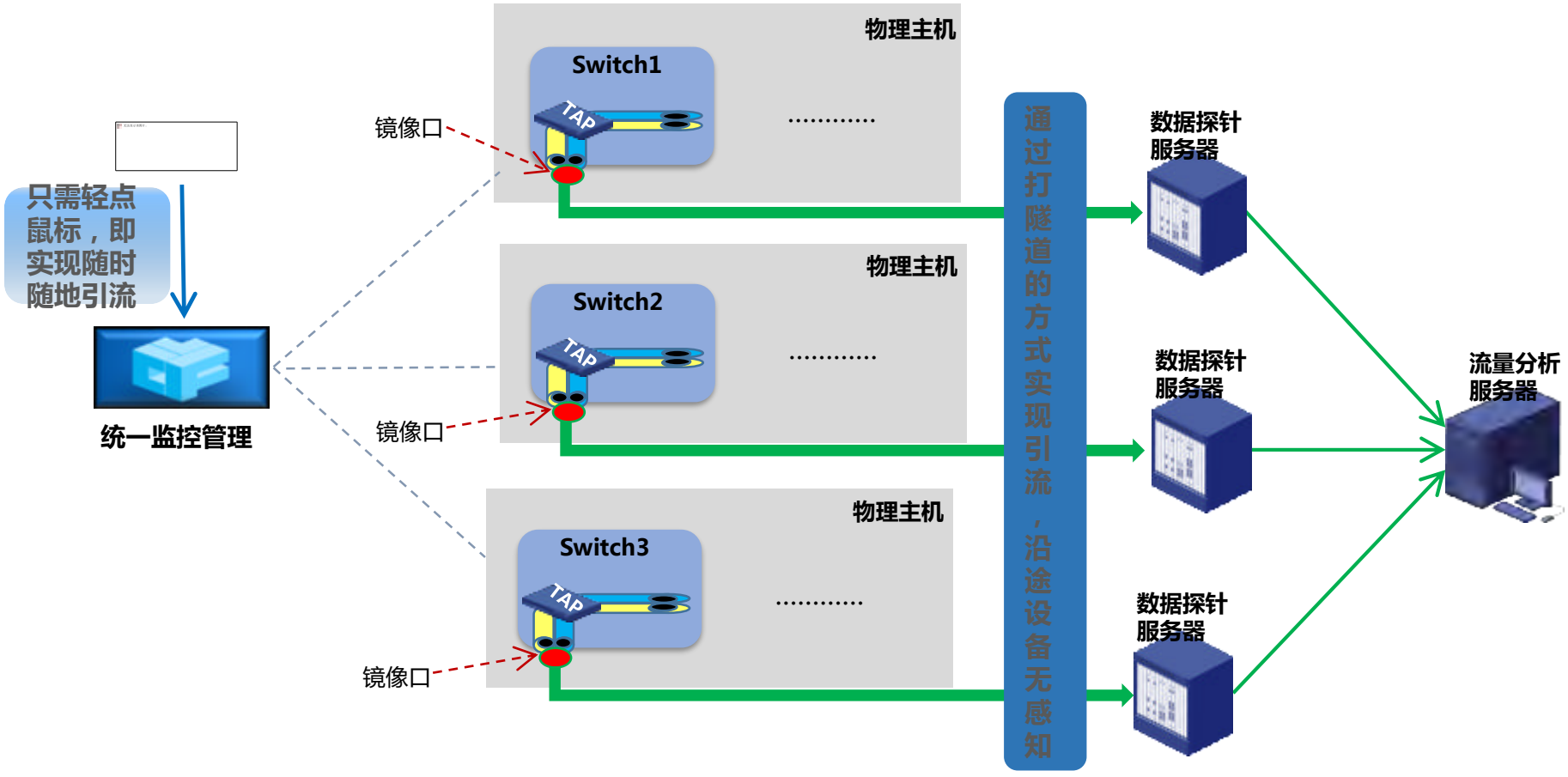
管理流程:

•制定安全运营策略及安全维护规章要求。

应急响应:

•制定数据中心安全事件应急响应机制及流程， 包括安全事件的等级划分、处理流程、事件上报等规范要求。

统一安全监控管理


只需轻点鼠标，即实现随时随地引流
统一监控管理
物理主机
Switch1
TAP
镜像口
物理主机
Switch2
TAP
镜像口
物理主机
Switch3
TAP
镜像口
通过打隧道的方式实现引流，沿途设备无感知
数据探针服务器
数据探针服务器
数据探针服务器
流量分析服务器

云平台安全实践

外网的syn攻击

某天新致云监控平台通过监控发现外网的机器发出惊人的syn半连接，因为我们前期通过防火墙部署过syn过滤数，流量在进入到我们真正的服务器前都被我们的流量清洗设备过滤了，然后将干净的流量送到了真正的被攻击服务器。其实黑客攻击的是我们在各个数据中心部署的CDN网络,CDN中的流量检测设备检测到后，送给清洗设备，清洗后的流量就送给攻击目标，这样就减轻了攻击目标的压力。事后，我们统计下来 ，这次我们的清洗设备挡住了将近百G的攻击。

The 8th China Cloud Computing Conference

Thank you