Government Cloud Security Overview

李超

OWASP

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

ABOUT ME

- 目前就职于浪潮云服务公司，浪潮云安全技术总监，负责云安全方向。
- 在政府行业的安全领域有深入研究和独特的见解有丰富的网络安全、系统安全、访问控制、云安全设计经验。

目录

- 政务云安全方向
- 政务云安全问题

从云计算定义看安全

美国国家标准与技术委员会(NIST)关于云计算可视化模型的定义

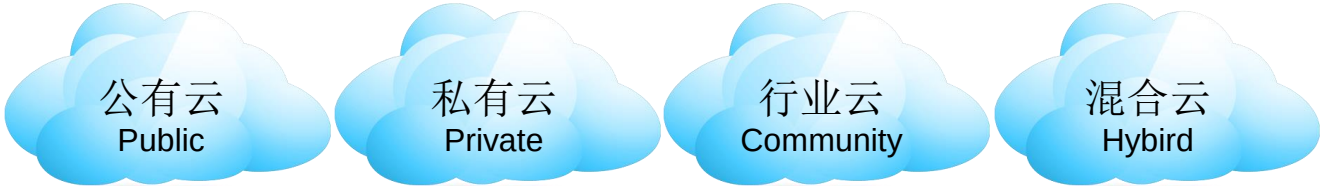
核心本质特征
Essential Characteristics

- 可量化的服务 Measured Service
- 快速而弹性的部署 Rapid Elasticity
- 按需提供的自服务 On-Demand Self Service
- 通过网络广泛访问 Broad Network Access
- 资源的池化整合 Resource Pooling

业务交付模式
Service Model

- 软件即服务 Software as a Service (SaaS)
- 平台即服务 Platform as a Service (PaaS)
- 基础架构即服务 Infrastructure as a Service (IaaS)

架构部署模式
Deployment Model



云安全内涵

云安全（Cloud Security）：

1. 云自身的安全保护，也称之为云计算安全，包括云计算应用系统安全、云计算应用服务安全、云计算用户信息安全。
2. 使用云的形式提供和交付安全，即云计算技术在安全领域的具体应用，即通过采用云计算技术来提升安全系统的服务性能，如基于云计算的防病毒技术、挂马检测技术 。

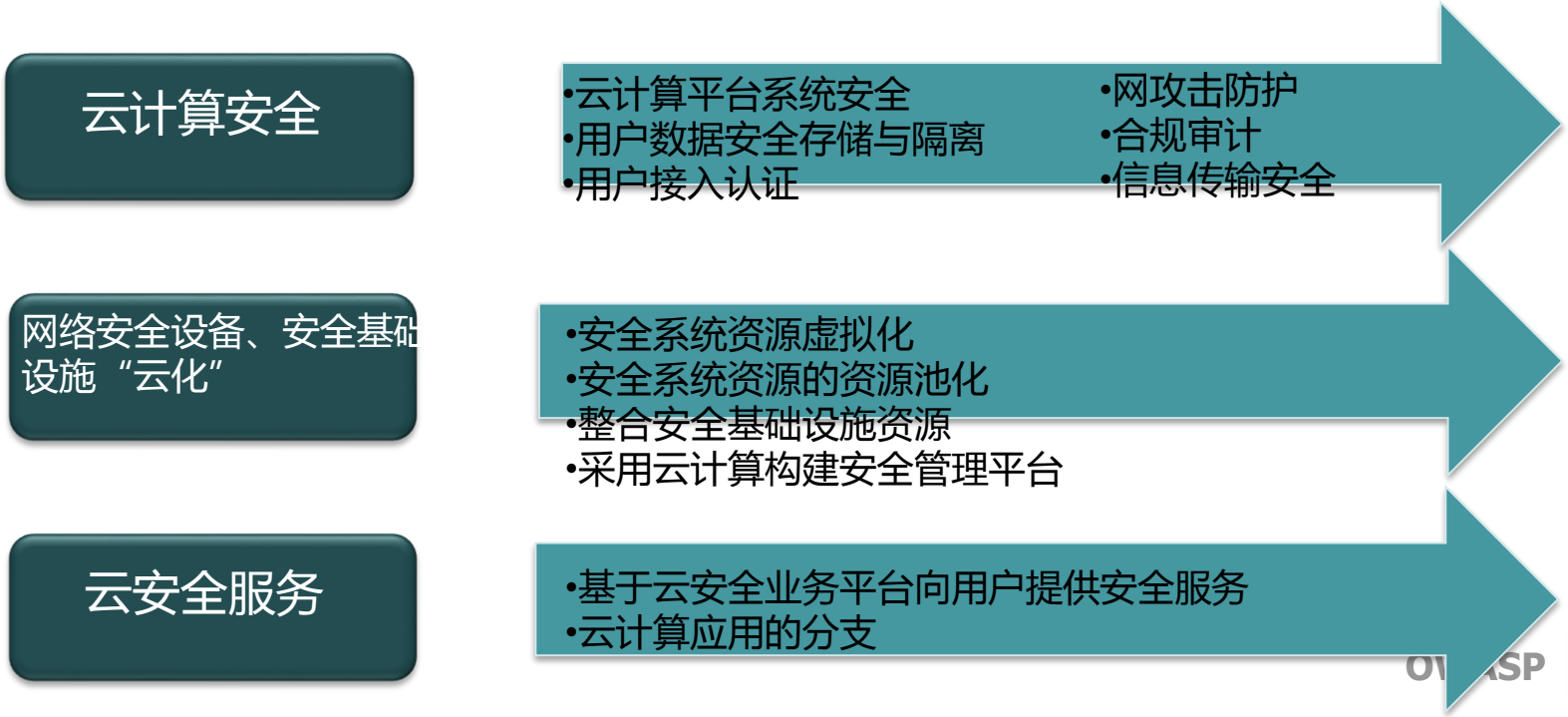
云安全的研究方向：

1. 云计算安全：主要研究研究如何保障云自身及其上的各种应用的安全：包括云计算系统安全、用户数据的安全存储与隔离、用户接入认证、信息传输安全、网络攻击防护、合规审计审计有等
2. 安全基础设备的云化：主要研究如何采用云计算技术新建与整合安全基础设备资源、优化安全防护机制、包括通过云计算技术构建超大规模安全基础设施资源，优化安全防护合机制。
3. 云安全服务：研究提供基于云计算平台为用户提供的安全服务。

云安全内涵

云安全（Cloud Security）：

1. 云自身的安全保护，也称之为云计算安全，包括云计算应用系统安全、云计算应用服务安全、云计算用户信息安全。
2. 使用云的形式提供和交付安全，即云计算技术在安全领域的具体应用，即通过采用云计算技术来提升安全系统的服务性能，如基于云计算的防病毒技术、挂马检测技术 。



云安全特征

- 云计算信息系统与传统信息系统组织架构上的差异性导致其安全防护理念上存在差异，很重要的一个原则是其三地边界的安全隔离和访问控制，强调针对不同安全区域设置有差异化的安全防护策略
- 物理计算资源共享带来的虚拟机的安全问题，在同一物理机如何对虚拟机之间的问题涉及传统的网络结构，如何在虚拟化环境中实现，
- 数据的拥有者与数据之间的物理分离带来的用户隐私与云计算可用性之间的矛盾

政务云安全方向

- 政务云安全定位于保障云云计算自身的安全，而不是作担任安全的服务。
- 政务云要建设一个安全的云计算环境，引入各种安全措施和安全管理制度，创造一个安全的运行环境，提供政府单位可信赖的计算环境。当用户对云计算有一定的了解和认识，并且能够信任云计算中心的方式，才会购买各种安全服务。
- 目前的问题先解决云云计算信息系统的安全问题，再发展云安全服务。

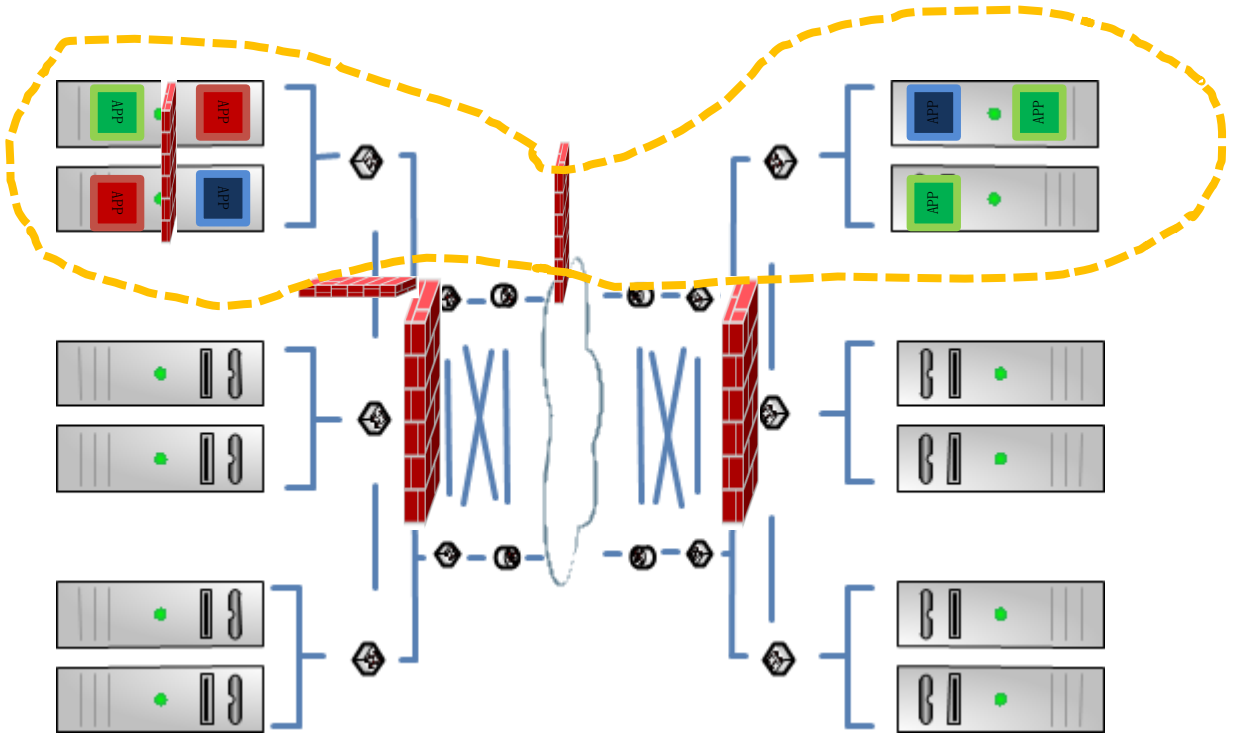
目录

- 政务云安全架构
- 政务云安全问题

虚拟化层安全

云计算环境中业务边界逐渐模糊

- 网络的边界在哪里？
- 被保护的对象在哪里？



虚拟化的网络、
计算、存储

虚拟化后网络接入与虚拟机位置分离带来挑战

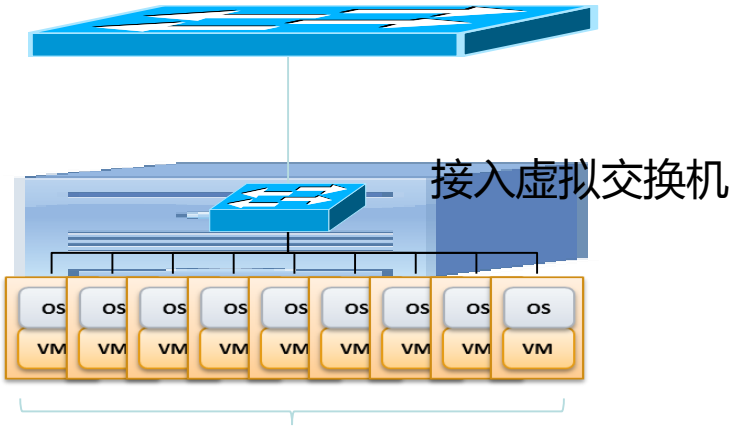
----虚拟化是建立资源池的一个重要手段

虚拟化前

接入交换机

十台物理服务器意味着
至少有十条上联链路和
十个交换接口

虚拟化后

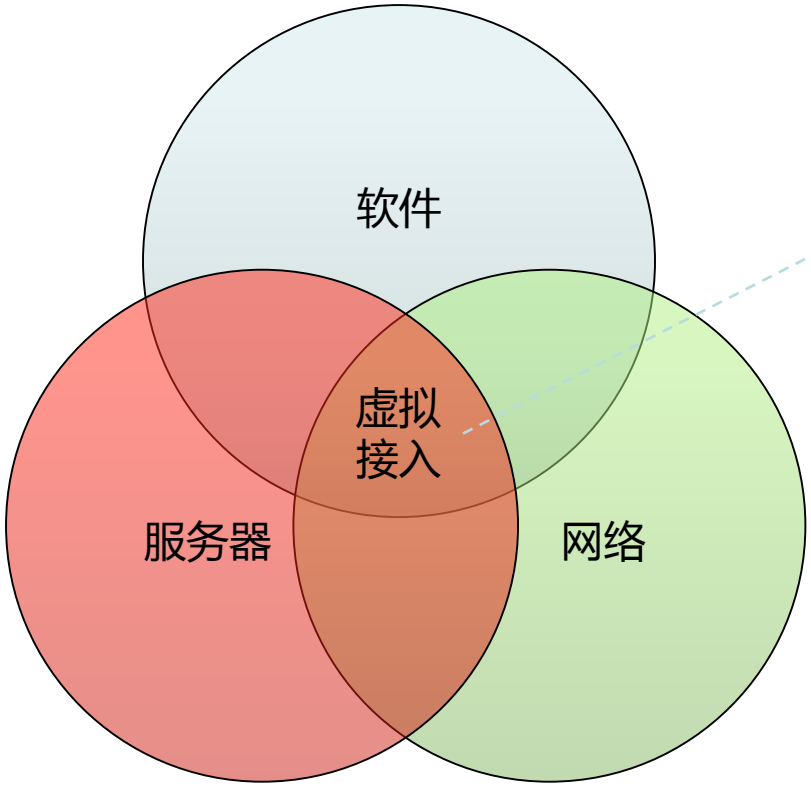


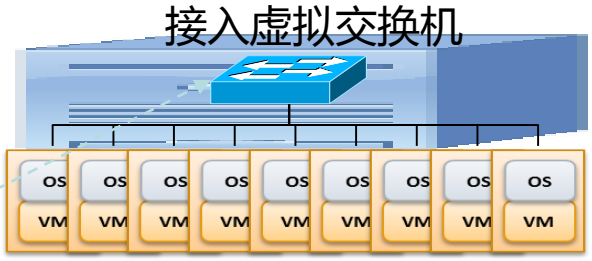
十个虚拟机重用着一条链
路和一个交换接口

如果一个虚拟机中毒，则
会影响其他九个虚拟机的
运行，且原有的基于端口
的安全策略会失效

虚拟接入成了三不管的领域

----虚拟化是建立资源池的一个重要手段





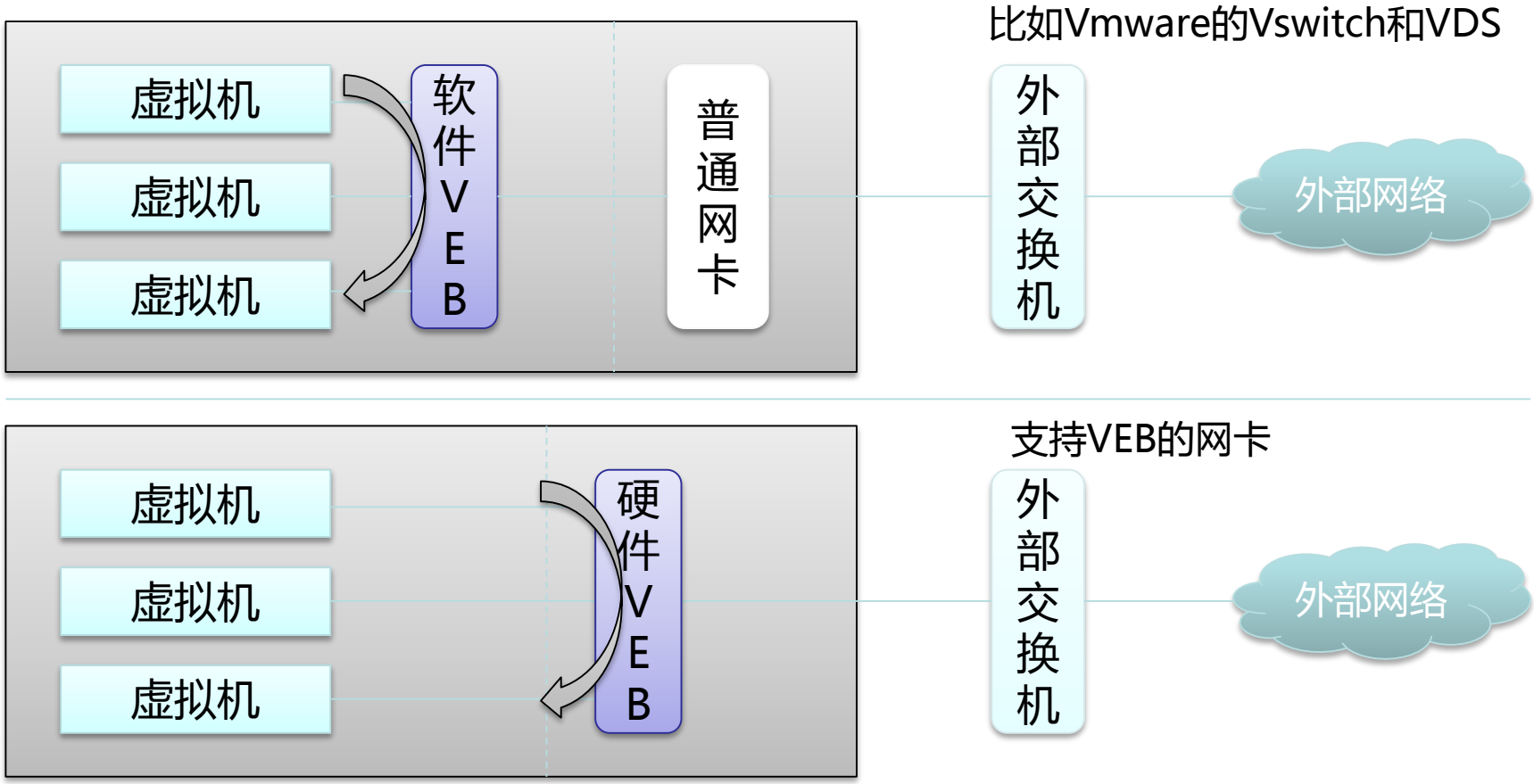
接入层“下沉”到服务器内部，结果谁也不管

虚拟机同交换机之间隔了一层服务器的网卡，网管人员的权限仅仅到交换机的接入端口

网管人员需要登录到Hypervisor上才能管理到虚拟接入层

虚拟接入的重要技术VEB

----Virtual Ethernet Bridge虚拟桥接网络，连接虚拟机到接入交换机



只能完成简单的二层网路转发，不支持Qos机制，二层安全策略，流量镜像等

必须整合虚拟化软件、物理服务器网卡和上联交换机来支持更多的网络功能

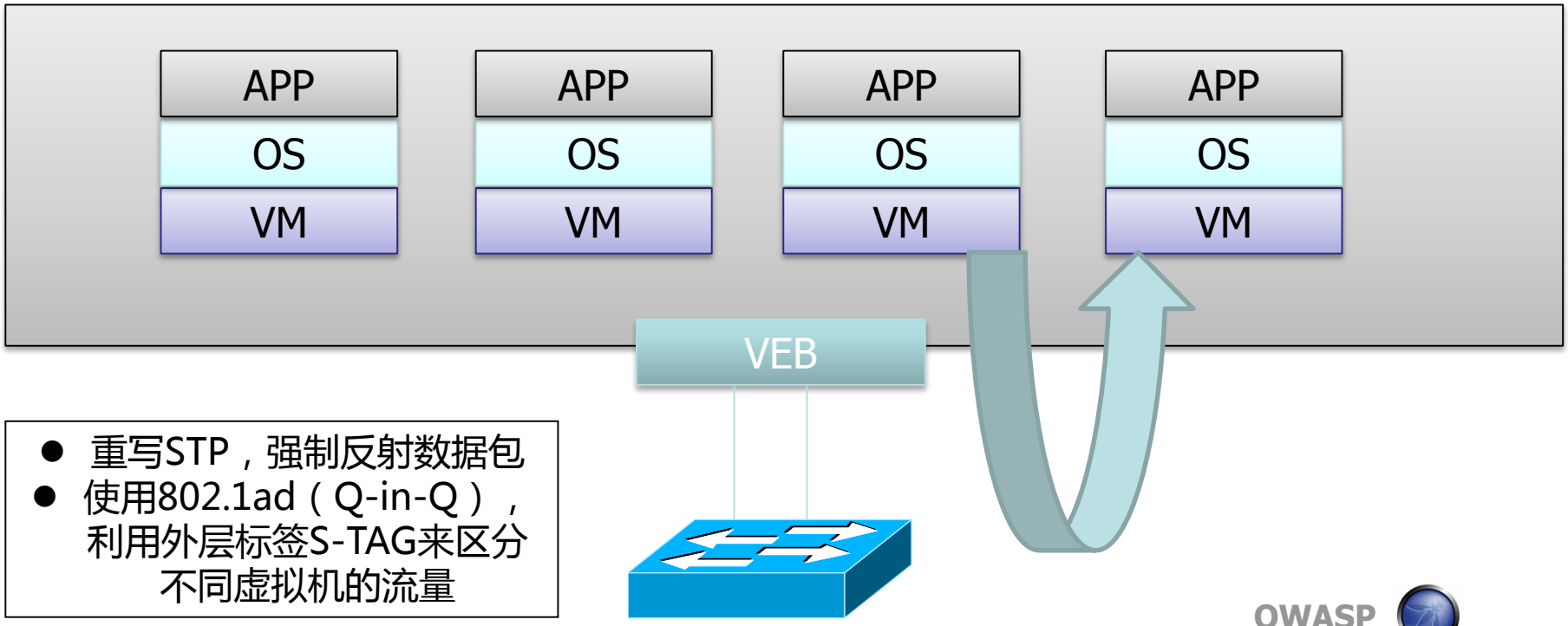
OWASP

识别特定虚拟机的流量VEPA

----修改生成树协议、重用Q-in-Q
----需要交换机、虚拟化软件和服务器网卡全线支持-HP、Juniper

发卡弯

转发步骤：从虚拟机送出的流量，通过服务器网卡送往上联交换机，上联交换机发现目标地址在同一台服务器内（通过MAC地址判断），上联交换机将流量返回到服务器，完成寻址转发



- 重写STP，强制反射数据包
- 使用802.1ad（Q-in-Q），利用外层标签S-TAG来区分不同虚拟机的流量

识别特定虚拟机的流量VN-TAG

----为虚拟机打上特定的网络标签（使用VIF)
----需要交换机、虚拟化软件和服务器网卡全线支持-Cisco、Vmware

MAC地址	802.1Q标记位	TL	Payload	校验位

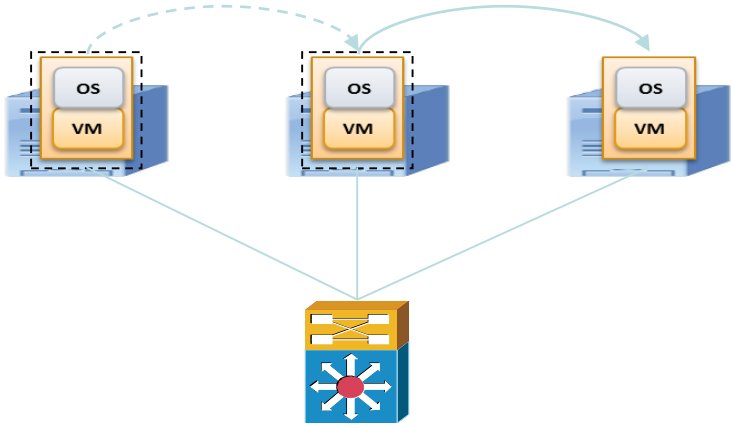
原有以太网帧结构

MAC地址	VN-TAG	802.1Q标记位	TL	Payload	校验位

VN-TAG帧结构

Dvif_id	Svif_id

当数据从虚拟机流出后，就被加上一个VN-TAG标签，从而区分出不同的虚拟机流量，形成对应的虚拟通道



只要VN-TAG和VIF不变，虚拟机即使迁移后，在接入交换机看来他们的虚拟接入关系不变，原来针对VIF的策略也就保持不变

网络安全设备虚拟化

- 安全设备资源池化
  - 安全设备，实现多类型虚拟设备组成的服务链、硬件虚拟化和Hypervisor集成的虚拟化等。在提供了底层支撑平台后，各产品线只需将自己的引擎部署在这些平台上，就可以快速交付可扩展的设备资源池；产品线需开放设备的应用接口，简化各种定制的模块，提高稳定性。
- 安全设备的交付形态变化：虚拟设备镜像

虚拟化安全

- 虚拟机蔓延
  - 僵尸虚拟机
  - 幽灵虚拟机
  - 虚胖虚拟机
- 虚拟机化安全攻击
  - 虚拟机跳跃
  - 虚拟机逃逸

虚拟化安全问题

- 宿主机安全机制
- Hypervisor安全机制
- 虚拟机隔离机制
- 虚拟机安全监控
- 虚拟机的安全防护与检测

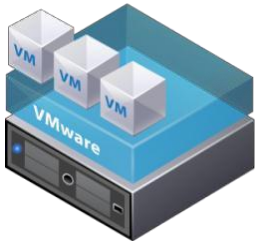
数据层安全

云计算带来数据的变化

- 控制权的丢失
- 对云服务提供商的信任有限
- 数据没有加密

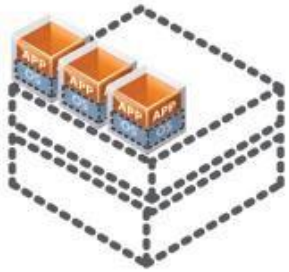
服务器

虚拟化 &
私有云

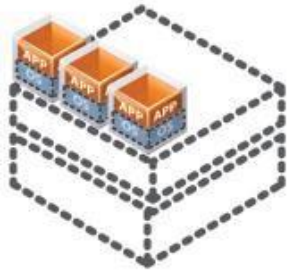


公有云
IaaS

公有云
PaaS



公有云
SaaS



最终用户

服务提供商

数据安全问题

- 密文检索：用户将数据加密后存储是常见手段，但用户需要对数据检索时，解密密钥的云服务商无法直接对密文相应处理。
- 密钥管理：密码算法可以公开评估，但密钥的管理、实施包含了复杂、细致的工作，既有技术问题，又有管理问题。
- 数据完整性：在本地没有数据副本的情况下高效验证外包云数据的完整性。

云安全标准及评估

云安全标准

- 国外云平台标准研究
  - NIST:美国国家标准与技术研究院
  - CSA:云安全联盟
  - ENISA:欧洲网络与信息安全局
- 国内标准
  - 中国信息安全标准化委员会:国家安全云计算服务安全标准指南

标准、制度的疑问

- 虚拟层安全：云平台具有资源动态分配、主机网络虚拟化，急需“虚拟化主机、网络防护”标准；
- 代码、接口标准：应用的开发缺乏统一标准应用程序从IDC到云或从云到IDC非常复杂。
- 数据安全存储：海量数量存储在云端且存在数据可移植性的问题。

云安全的测评挑战

- 云安全的测试
  - 虚拟化后管理员角色、管理方式的变化
  - 云服务用户系统的安全管理能力
  - 物理安全测评的挑战。
  - 网络安全测评：缺乏网络虚拟化的评测内容
  - 主机安全测评：缺乏对虚拟化主机防护测试内容
  - 应用安全测评：缺乏代码、接口安全。
  - 数据安全测评：数据加密、解密，数据移植、数据挖掘保护。

谢谢！