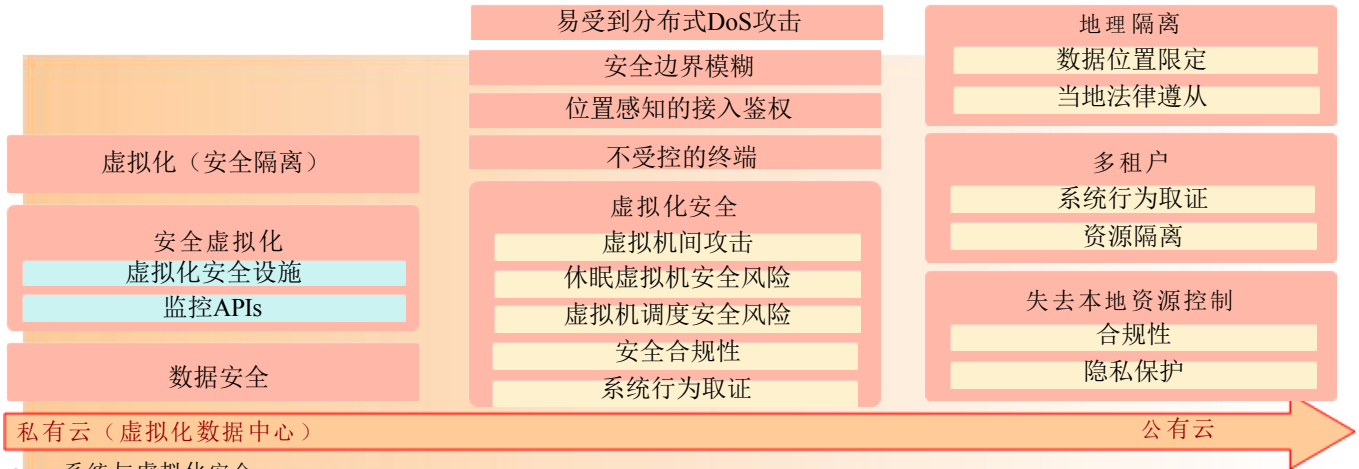
云计算安全技术

目录

云计算带来新的安全威胁



- 系统与虚拟化安全
  - 存虚拟化平台运行在操作系统与物理设备之间，其设计和实现中存在漏洞风险
- 应用与数据安全
  - 不同安全需求的租户可能运行在同一台物理机上，传统安全措施难以处理
- 网络与边界安全
  - 网络边界的模糊化，传统的边界防护手段在虚拟网络中无法直接使用
- 身份与安全管理
- 应用系统和资源所有权的分离，导致云平台管理员可能访问用户数据

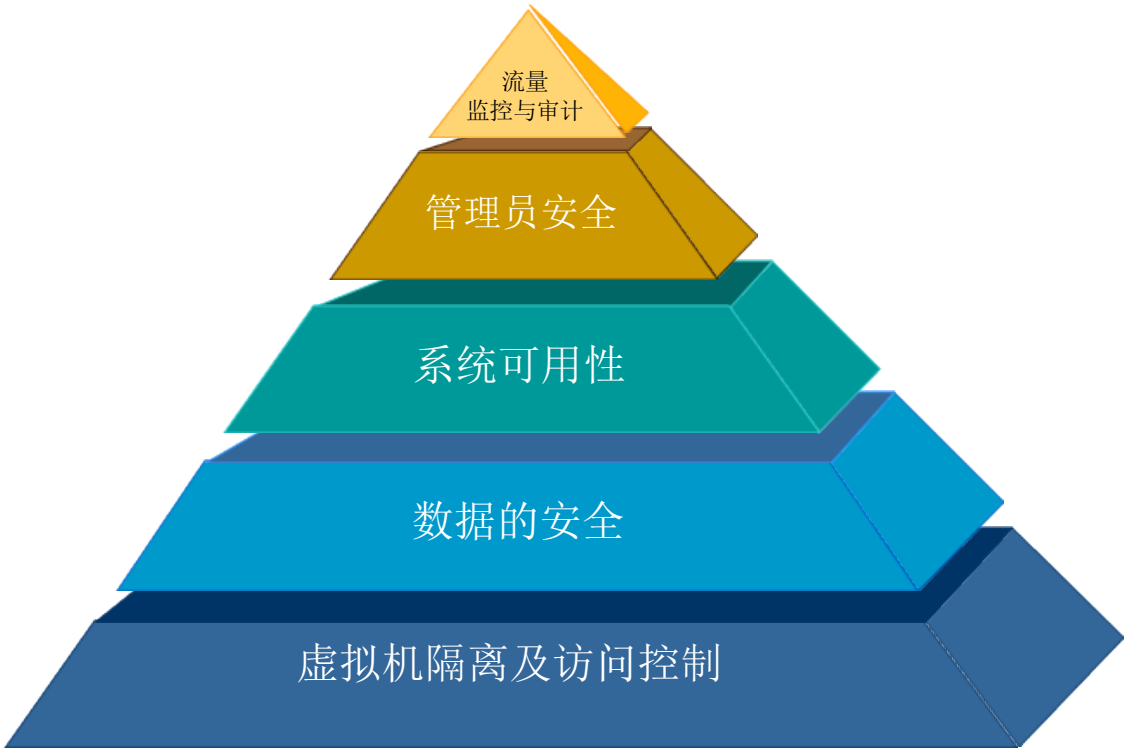
云计算安全威胁分析(1)

		管理员	用户	黑客
端	TC	非法操作：如利用TCM与TC间正常的升级通道，植入木马控制TC	恶意用户：仿冒其他用户登录，破解密码	伪造TCM管理员
		伪造非法TCM：控制TC	非法TC：非法TC具有获取VM数据能力	TCM漏洞攻击
		权限滥用：对TC USB端口管理不合理		TC被非法破坏：植入木马，非法获取VM数据
	SC	权限滥用	数据泄露到本地，如截屏	SC漏洞攻击
管	网络		截获其他用户密码	常见网络攻击
			PC等设备绕过安全网关	

云计算安全威胁分析(2)

		管理员	用户	黑客
云	虚拟机	非法重置用户密码	用户非法登录：弱口令或口令保管不善	拒绝服务攻击，导致VM不可用
		误挂卷	用户虚拟机被篡改	
		利用虚拟机备份文件非法恢复用户数据	攻击相邻虚拟机，如ARP攻击	
		虚拟机自然损坏	非授权访问相邻虚拟机	
			攻击虚拟化平台	
			利用虚拟化资源从事非法活动，如攻击外网	
			虚拟机迁移过程中安全策略失效	
	虚拟化层	管理员非法登录：利用弱口令或口令保管不善	还原出前一用户硬盘数据	利用租用的虚拟机攻击虚拟化平台
		权限滥用：如果缺三权分立	还原出前一用户内存数据	利用租用的虚拟机攻击虚拟化管理平台，如利用OS/web漏洞
		关键操作无法回溯		虚拟机迁移中截获用户数据
		破坏镜像文件，植入木马		
		管理员权限扩大化：如节点间采用互信，则获取单节点权限即可控制整朵云		
		非法获取敏感信息，如数据库口令		
		非法监视用户虚拟机流量		
		非法获取用户密码		

云计算安全风险关注要点



目录

云计算安全设计原则

内容监管、SOX法案、 SAS 70、 PCI/HIPAA等

数据隔离、数据访问控制、剩余信息保护、
数据盘加密存储、存储位置要求

虚拟机隔离、虚拟防火墙，恶意VM预防

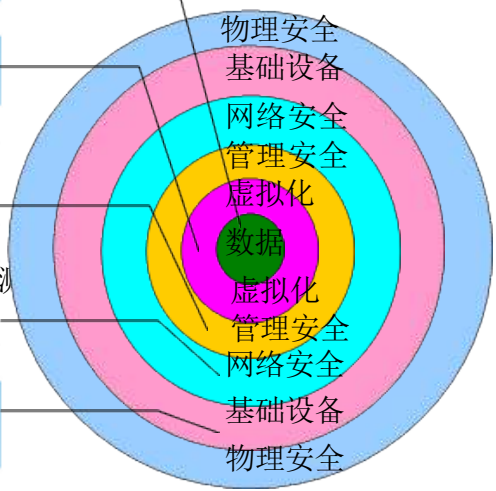
集中用户管理和认证、集中日志审计

防火墙、IDS/IPS、Anti-DDOS、僵尸网络/蠕虫检测
网络平面隔离、传输安全（SSL、VPN）

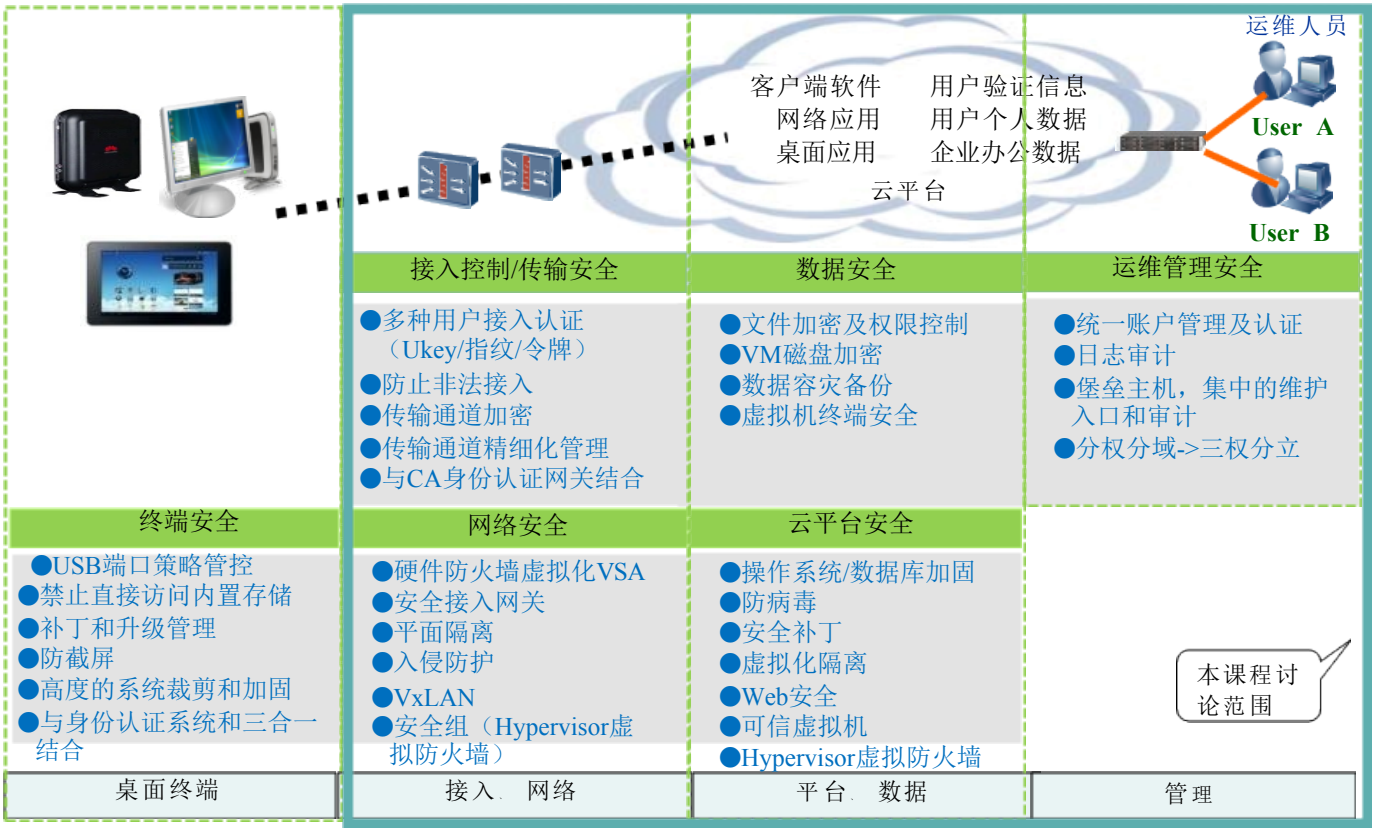
系统完整性保护、OS/DB/Web加固、安全补丁、
病毒防护等

门禁、机房监控系统 、云监控

其他：法律法规的遵循



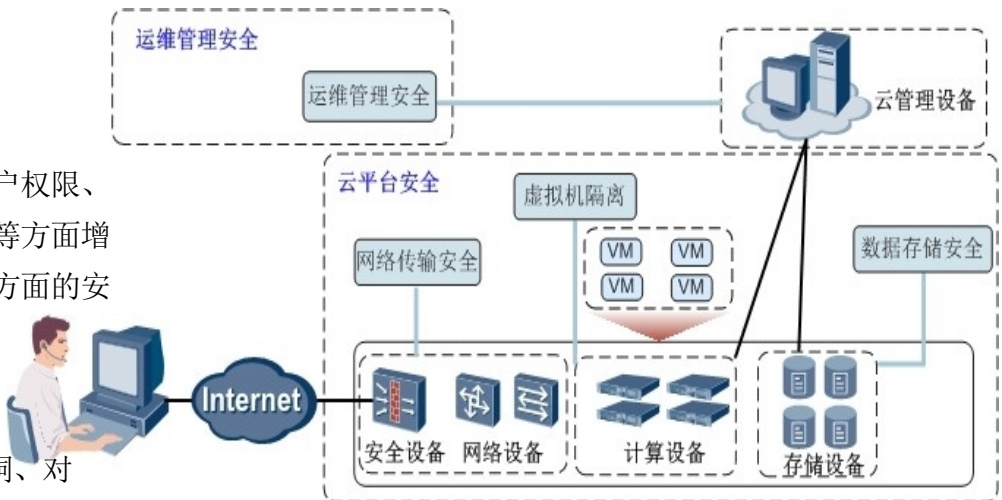
华为“端管云”立体信息安全防护策略



目录

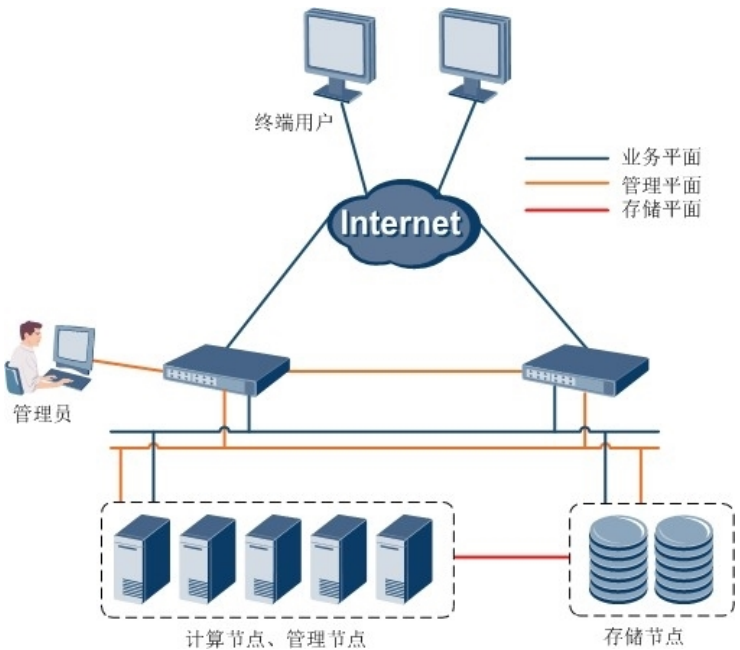
FusionSphere总体安全框架

- 云平台安全：
  - 网络传输安全
  - 虚拟机隔离
  - 数据存储安全
- 运维管理安全：
  - 从帐号密码、用户权限、日志、传输安全等方面增强日常运维管理方面的安全措施
- 物理主机的安全：
  - 修复Web应用漏洞、对操作系统和数据库进行加固、安装安全补丁和防病毒软件等手段



目录

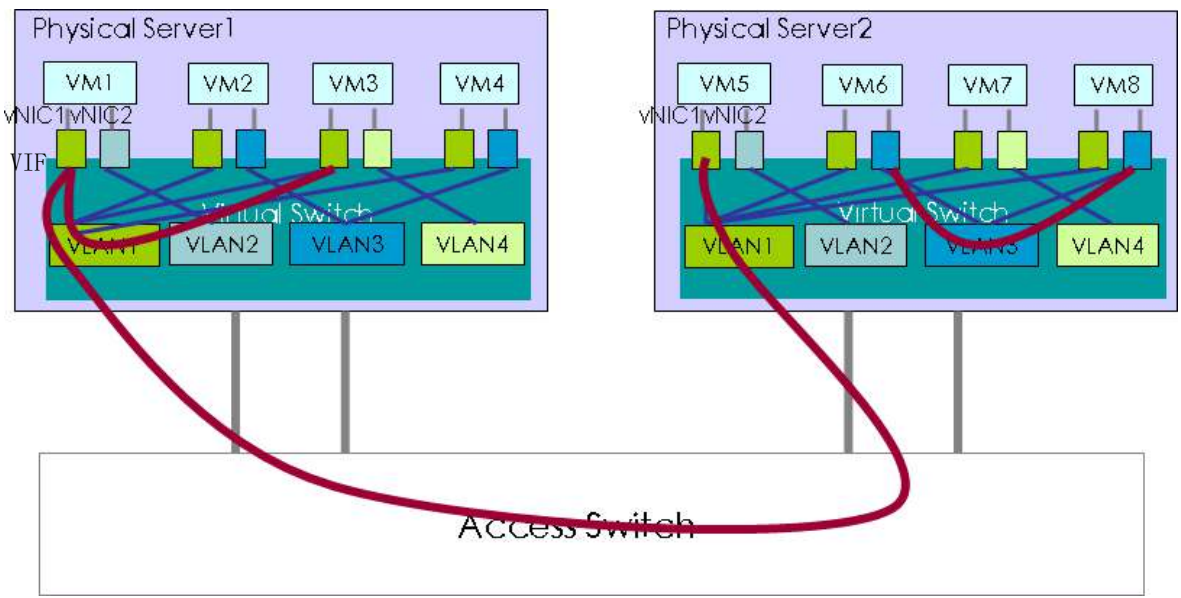
网络平面隔离



- FusionSphere的网络通信平面划分为业务平面、存储平面和管理平面，且三个平面之间隔离
- 存储平面与业务平面、管理平面间物理隔离
- 管理平面与业务平面间是逻辑隔离
- 通过网络平面隔离保证管理平台操作不影响业务运行，最终用户不能破坏基础平台管理
- 业务平面
  - 为用户提供业务通道，为虚拟机虚拟网卡的通信平面，对外提供业务
- 存储平面
  - 为iSCSI存储设备提供通信平面，并为虚拟机提供存储资源，但不直接与虚拟机通信，而通过虚拟化平台转化
- 管理平面
  - 负责整个云计算系统的管理、业务部署、系统加载等流量的通信

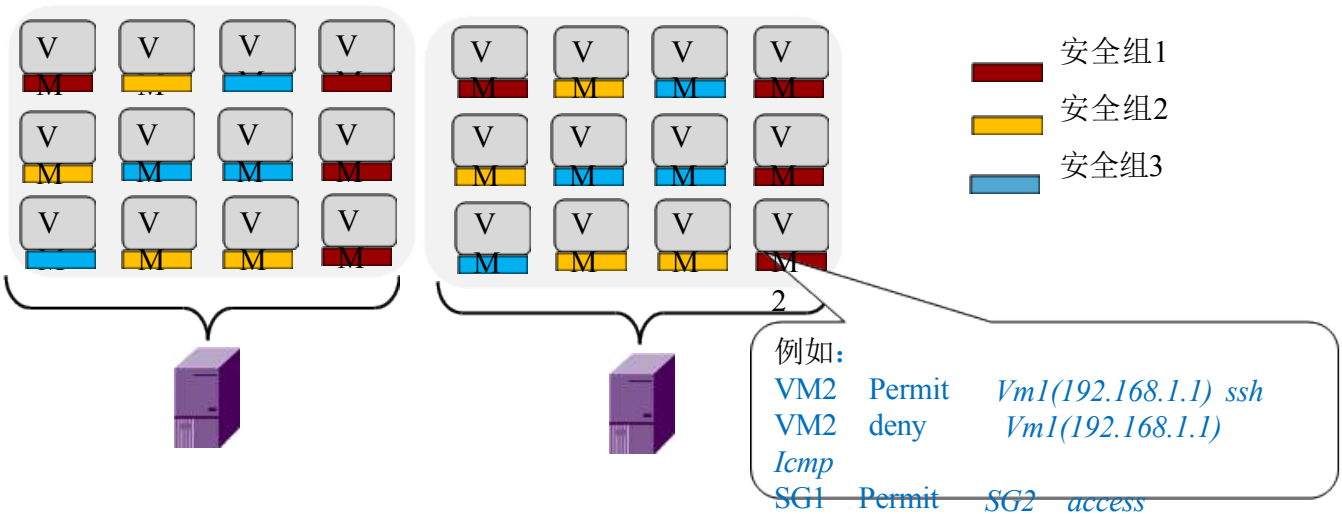
安全组

- 通过虚拟网桥实现虚拟交换功能，虚拟网桥支持VLAN tagging功能，实现VLAN隔离，确保虚拟机之间的安全隔离
- 虚拟网桥的作用是桥接一个物理机上的虚拟机实例



虚拟磁盘文件

- 虚拟机实例可以动态地加入和删除安全组，实现虚拟机间的互通或阻隔。使用防火墙将导致配置的管理复杂性提高和效率降低。
- 安全组可以完成虚拟机的授权、安全组间的授权访问
- 安全组规则可以随虚拟机动态迁移



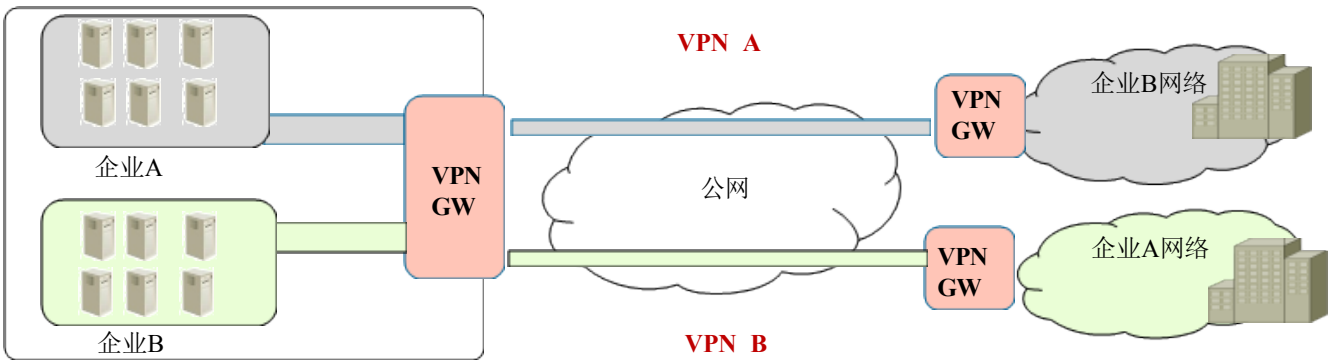
防IP、MAC仿冒 & DHCP隔离

- 通过IP和MAC绑定方式实现：防止虚拟机用户通过修改虚拟网卡的IP、MAC地址发起IP、MAC仿冒攻击，增强用户虚拟机的网络安全
- 具体技术能力包括通过DHCP snooping生成IP-MAC的绑定关系，然后通过IP源侧防护(IP Source Guard)与动态ARP检测（DAI）对非绑定关系的报文进行过滤
- 在虚拟交换层执行虚拟机安全策略，支持对虚拟机的DHCP隔离，禁止用户虚拟机启动DHCP Server服务，防止用户无意识或恶意启动DHCP Server服务，影响正常的虚拟机IP地址分配过程

广播报文抑制

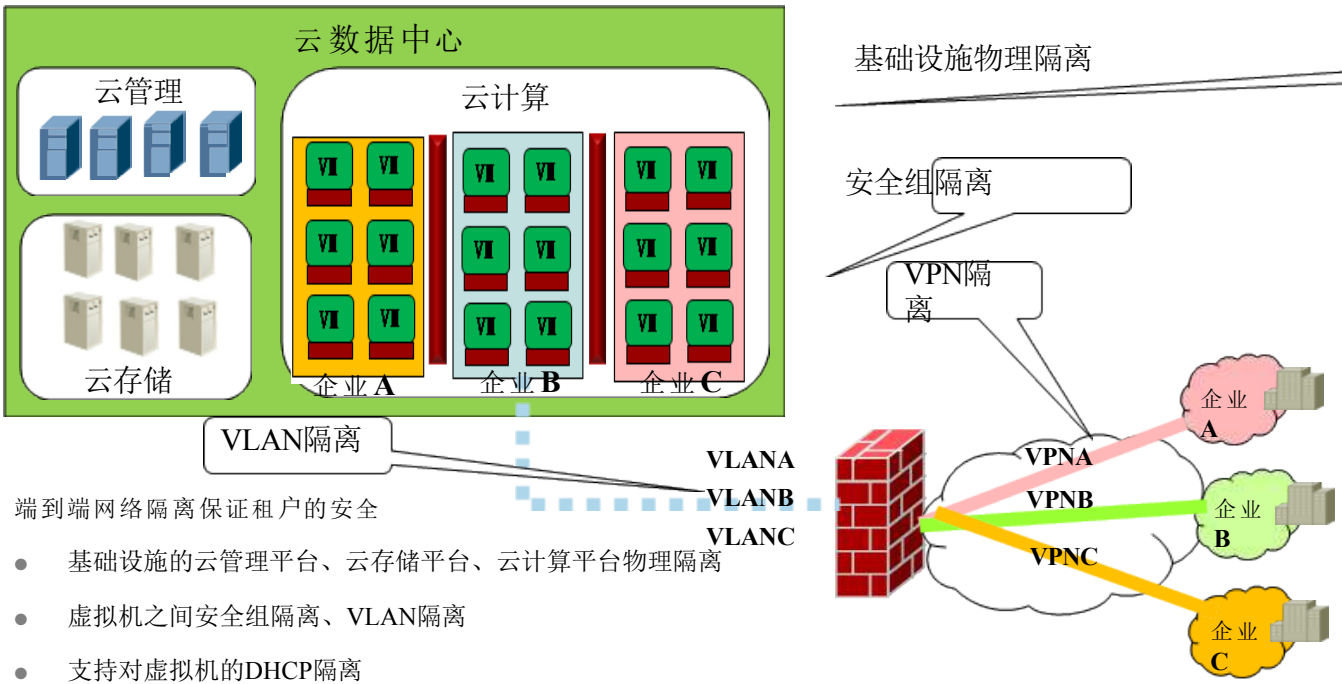
- 在服务器整合、桌面云等企业应用场景，如果发生网络攻击或病毒发作等引起的广播报文攻击，可能造成网络通信异常，此时可以开启虚拟交换机的广播报文抑制功能
- 虚拟交换机提供虚拟机虚端口发送方向ARP广播报文和IP广播报文的抑制开关，以及抑制阈值设置功能。可以通过开启虚拟机网卡所在端口组的广播包抑制开关设置阈值，减少过量广播报文对二层网络带宽的消耗
- 管理员可以通过系统Portal，基于虚拟交换机端口组对象，配置广播报文抑制开关、ARP广播报文抑制阈值、IP广播报文抑制阈值

VPC－虚拟私有云



- VPC（虚拟私有云）现数据中心基础上的局域网功能，一个VPC相当于一个局域网。VPC通过VPN（Virtual Private Network）等方式也可以连接到外部网络，实现局域网与外网的互通。
- VPC作为企业数据中心的延伸，减少企业的对于数据中心的投资降低企业的CPEX和OPEX
- VPC保证不同企业在网络和云中完全隔离
- VPC客户按需分配，动态增加、删除、扩展数据中心
- VPC企业自助配置IP，VPN资源

网络安全总结



端到端网络隔离保证租户的安全

- 基础设施的云管理平台、云存储平台、云计算平台物理隔离
- 虚拟机之间安全组隔离、VLAN隔离
- 支持对虚拟机的DHCP隔离
- 不同企业租户之间VPC隔离
- 不同企业租户之间VPN隔离
- 基础设施与公网之间通过防火墙隔离

目录