doi: 10.3969/j.issn.1006-1576.2012.08.015

虚拟化数据中心的安全设计

李洪敏[1]，李宇明[2]，葛杨[3]
（1. 中国工程物理研究院总体工程研究所，四川 绵阳 621900；
2. 总装安全检查办公室，北京 100094；3. 军工保密资格认证中心，北京 100094）

摘要：针对虚拟化数据中心的安全需求，提出一种虚拟化数据中心的安全设计方案。分析了虚拟化后数据中心面临的安全问题，从通道隔离、接入控制和网络安全策略可随虚拟机迁移 3 个方面建立了数据中心虚拟化后的三维安全模型，将两层交换机用多条链路进行捆绑连接，实现基于物理端口的负载均衡和冗余备份，并利用交换机和防火墙来实现访问控制。分析结果表明，该设计实现了数据中心虚拟化的安全保护。

关键词：虚拟化；数据中心；安全；访问控制
中图分类号：TP393.08　　**文献标志码：**A

Security Design of Virtualization Data Center

Li Hongmin[1], Li Yuming[2], Ge Yang[3]
(1. *Institute of General Engineering*, *China Academy of Engineering Physics*, *Mianyang* 621900, *China*;
2. *Safety Check Office*, *General Equipment Headquarters of PLA*, *Beijing* 100094, *China*;
3. *Defense Industry Secrecy Examination & Certification Center*, *Beijing* 100094, *China*)

Abstract: Aiming at the security requirements of virtualization data center, the security design of virtualization data center is put forward. The security problems of virtualization data center are analyzed, the three-dimensional security model of virtualization data center is set up from isolation of channel, control of connect and dynamic move of security policy based virtual computer. Use multi-links for binding connect the 2-layers exchange board, realizing the load equilibrium and redundancy backup based on physical port. Use exchange board and fire wall to realize interview control. The analysis results show that the deign realizes security protection of virtualization data center

Key words: virtualization; date center; security; access control

0　引言

数据中心虚拟化是指利用虚拟化技术构建基础设施池，主要包括计算、存储和网络 3 种资源。数据中心虚拟化后不再独立地看待某台设备和链路，而是计算、存储和网络的深度融合，当作按需分配的整体资源来对待[1]。从主机等计算资源角度看，数据中心虚拟化包含多合一、一分多 2 个方向，都提供了计算资源按需调度的手段。存储虚拟化的核心就是实现物理存储设备到单一逻辑资源池的映射，是为了便于应用和服务进行数据管理，对存储子系统或存储服务进行的内部功能抽象、隐藏和隔离的行为。在现代信息技术中，虚拟化技术以其对资源的高效整合、提高硬件资源利用率、节省能源、节约投资等优点而得到广泛应用。但虚拟化技术在为用户带来利益的同时，也对用户的数据安全和基础架构提出了新的要求[2]。如何在安全的范畴使用虚拟化技术，成为迫在眉睫需要解决的问题。因此，笔者对虚拟化数据中心的安全设计进行研究。

1　虚拟化后数据中心面临的安全问题

1) 服务器利用率和端口流量大幅提升，对数据中心网络承载性能提出巨大挑战，对网络可靠性要求更高；

2) 各种应用部署在同一台服务器上，网络流量在同一台服务器上叠加，使得流量模型更加复杂；

3) 虚拟机的部署和迁移，使安全策略的部署更复杂，需要一个动态安全机制对数据中心进行防护；

4) 在应用虚拟存储技术后，面对异构存储设备的特点，存在如何统一监管的问题[3]；虚拟化后不同密级信息混合存储在同一个物理介质上，将造成越权访问等问题。

2　数据中心安全风险分析

2.1　高资源利用率带来的风险集中

通过虚拟化技术，提高了服务器的利用效率和

收稿日期：2012-03-26；修回日期：2012-05-10
作者简介：李洪敏(1968—)，女，辽宁人，硕士，高级工程师，从事计算机应用研究。

灵活性，也导致服务器负载过重，运行性能下降。虚拟化后多个应用集中在 1 台服务器上，当物理服务器出现重大硬件故障是更严重的风险集中问题。虚拟化的本质是应用只与虚拟层交互，而与真正的硬件隔离，这将导致安全管理人员看不到设备背后的安全风险，服务器变得更加不固定和不稳定。

2.2 网络架构改变带来的安全风险

虚拟化技术改变了网络结构，引发新的安全风险。在部署虚拟化技术之前，可在防火墙上建立多个隔离区，对不同的物理服务器采用不同的访问控制规则，可有效保证攻击限制在一个隔离区内，在部署虚拟化技术后，一台虚拟机失效，可能通过网络将安全问题扩散到其他虚拟机。

2.3 虚拟机脱离物理安全监管的风险

1 台物理机上可以创建多个虚拟机，且可以随时创建，也可被下载到桌面系统上，常驻内存，可以脱离物理安全监管的范畴。很多安全标准是依赖于物理环境发挥作用的，外部的防火墙和异常行为监测等都需要物理服务器的网络流量，有时虚拟化会绕过安全措施。存在异构存储平台的无法统一安全监控和无法有效资源隔离的风险。

2.4 虚拟环境的安全风险

1) 黑客攻击。

控制了管理层的黑客会控制物理服务器上的所有虚拟机，而管理程序上运行的任何操作系统都很难侦测到流氓软件等的威胁。

2) 虚拟机溢出。

虚拟机溢出的漏洞会导致黑客威胁到特定的虚拟机，将黑客攻击从虚拟服务器升级到控制底层的管理程序。

3) 虚拟机跳跃。

虚拟机跳跃会允许攻击从一个虚拟机跳转到同一个物理硬件上运行的其它虚拟服务器。

4) 补丁安全风险。

物理服务器上安装多个虚拟机后，每个虚拟服务器都需要定期进行补丁更新、维护，大量的打补丁工作会导致不能及时补漏而产生安全威胁。安全研究人员在虚拟化软件发现了严重的安全漏洞，即可通过虚拟机在主机上执行恶意代码。黑客还可以利用虚拟化技术隐藏病毒和恶意软件的踪迹。

3 数据中心的安全设计

3.1 数据中心的安全需求

传统的数据中心关注业务流量的访问控制，数据中心虚拟化后增加了主机动态迁移和业务混存的安全风险，因此在安全模型中需要将主机动态迁移到其它物理服务器，并将业务的有效隔离作为第三维的关注点。虚拟化数据中心的安全需求包含 3 个方面：一是通道隔离，即不同的应用、业务和用户进行安全隔离，确保用户群组获得正确的资源和网络流量，保证高可用；二是接入控制，即网络安全策略应支撑集群中成员的动态加入、离开或迁移；三是网络安全策略可随虚拟机迁移。数据中心虚拟化后三维安全模型如 1 所示。

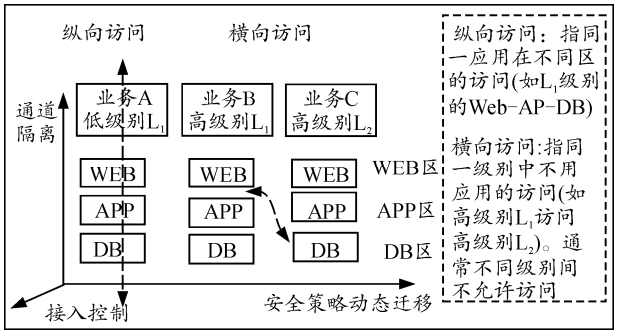

图 1 数据中心虚拟化后安全模型

3.2 虚拟化数据中心的安全设计

1) 数据中心网络架构高可用设计。

在新一代数据中心虚拟化网络架构中，通过 IRF(intelligent resilient framework)技术将多台网络设备虚拟化成 1 台设备统一管理和使用，整体无环设计并提高可用性。在 IRF 架构下，基本原则就是服务器双网卡接在不同交换机上，汇聚交换机堆叠后，将两层交换机用多条链路进行捆绑连接，实现基于物理端口的负载均衡和冗余备份，如图 2。

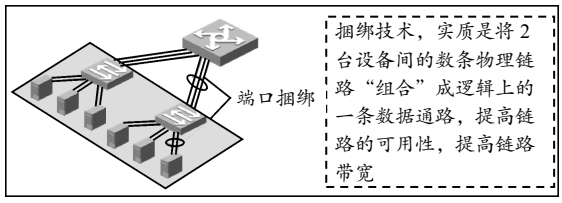

图 2 端口捆绑技术

数据中心架构规划设计时，还需要按照模块化、层次化原则进行[4]。从可靠性角度看，三层架构和二层架构均可以实现数据中心网络的高可用，而二层扁平化网络架构更适合大规模服务器虚拟化集群

和虚拟机的迁移。模块化设计是指针对不同功能或相同功能不同性能、不同规模的应用进行功能分析的基础上，划分出一系列功能模块。在内部网中根据应用系统的重要性、流量特征和用户特征的不同，可大致划分几个区域，以数据中心核心区为中心，其它功能区与核心区相连，成为数据中心网络的边缘区域，如图 3 所示。

2) 网络安全的部署设计。

虚拟化数据中心关注的重点是实现整体资源的灵活调配，因此在考虑访问控制时，要优先考虑对计算资源灵活性调配的程度。网络安全的控制点尽量上移，服务器网关尽量不设在防火墙，避免灵活性的降低。根据应用的重要程度不同，利用交换机和防火墙来实现访问的工作模式如图 4 所示。

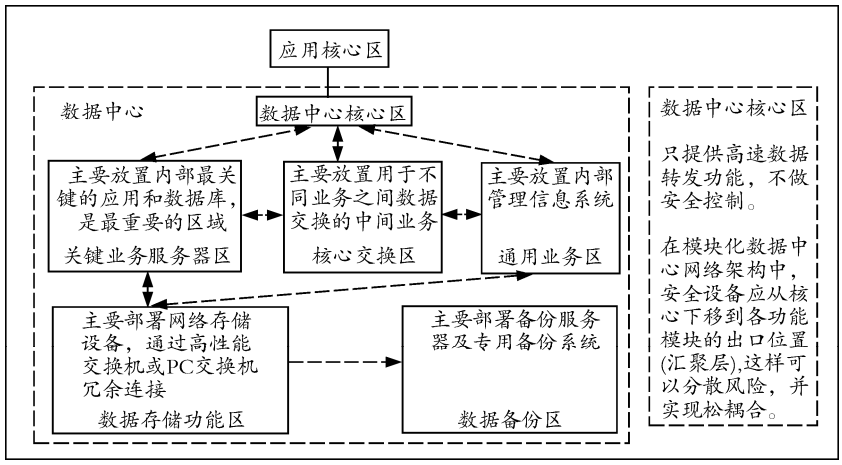

图 3　数据中心的模块化设计

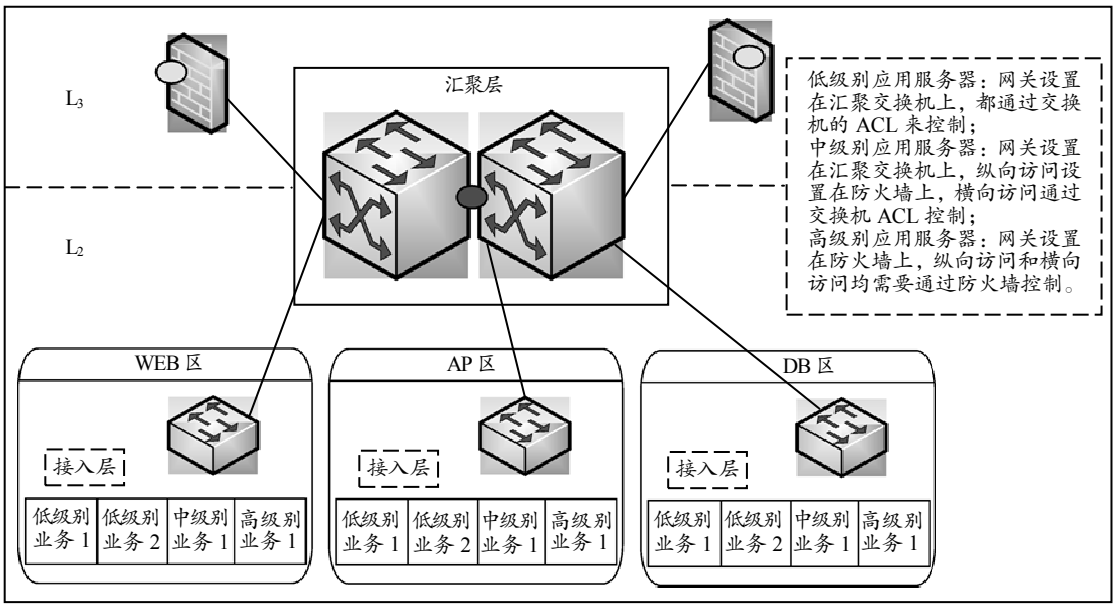

图 4　不同涉密等级网关安全控制模型

服务器网关设置在汇聚交换机上的工作模式：汇聚交换机作为 Web/AP/DB 服务器的网关，Web/AP/DB 服务器二层分区之间互访经过汇聚交换机 ACL 做访问控制，防火墙做边界安全控制。同一业务在同一 VRF（虚拟路由表）内，而 Web/AP/DB 分布在同一 VRF 的不同二层分区内，Web/AP/DB 通过交换机三层转发访问；不同业务之间的访问，跨 VRF 通过防火墙控制。

服务器网关设置在防火墙上的工作模式：服务器网关设置在防火墙上，通过静态路由下一跳指向汇聚交换机的三层接口，三组服务器网关地址各不相同，各组服务器内的虚拟机只能在本 VLAN 内迁移，如 Web/AP/DB 3 种服务器部署在不同 VLAN，L_2 分区之间互访需经过防火墙实现访问控制，属于强隔离措施。

（下转第 54 页）