文章编号：1007-1423(2014)04-0075-06 DOI：10.3969/j.issn.1007-1423.2014.04.018

虚拟化安全服务器研究与设计

丘惠军

(深圳供电局有限公司，深圳 518048)

摘要：
随着服务器虚拟化技术的推广与发展，深圳供电局开始引入虚拟化应用来提高硬件资源使用率，虚拟化技术在给深圳供电局带来便利的同时也暴露一些安全问题，例如出现针对虚拟化操作系统的新型攻击，在虚拟环境下无法有效实现访问控制、流量检测及安全审计等隐患。通过对虚拟化环境基础架构及虚拟化环境信息安全整体防护的探讨，提出一套适用于深圳供电局的虚拟化安全服务器解决方案。

关键词：
信息安全；服务器虚拟化；虚拟化安全；虚拟化统一威胁管理系统

0 引言

随着全球信息化进程和网络技术发展的不断加快，深圳供电局对于 IT 系统和信息的依赖性越来越强，企业应用的扩充以及数据的增加使得 IT 设施以及管理相应地膨胀，深圳供电局一直在寻找提高 IT 服务水平、降低 IT 成本、提升灵活性并快速应对计算需求变化的方法。

深圳供电局应用的重心集中在服务器和存储设备中，应用的扩充需要越来越多的服务器和存储设备，导致深圳供电局在管理硬件基础设施的压力和成本不断增大；另外，因为应用的多样性，服务器和存储难以有效地整合，服务器运行状态都远低于其实际的处理能力，存储的容量难以充分利用。

因此，深圳供电局开始引入服务器虚拟化来构建安全、可靠、稳定的 IT 基础架构，以保证可以有效执行灾难恢复和业务连续性计划，保证数据安全，同时减少物理服务器数量，降低管理维护成本。

但虚拟化技术同时也带来虚拟化环境下数据和系统的保密性和安全性问题，这也成为了保障深圳供电局信息安全的新挑战。

1 虚拟化安全问题分析

服务器虚拟化技术给深圳供电局带来了极大的便利，从安全的角度看，也带来了许多好处，例如：数据的集中存储，通过加强对数据的集中管控，理论上比在分布大量各种终端上的数据更安全(DLP)；虚拟化的同质化使得安全审计、安全评估、测试更加简单；更容易实现系统容错、高可用性和冗余及灾备；更容易实现网络犯罪取证，只需要拷贝虚拟机。

但同时也存在安全风险和威胁，主要有如下几个方面：

●针对虚拟化操作系统的攻击，例如虚拟机逃逸：是指在已控制一个虚拟机(以下简称“VM”)的前提下，通过利用各种安全漏洞攻击 Hypervisor。典型案例：蓝色药丸、CloudBurst ，安装 Hypervisor 级后门，进行拒绝服务攻击，数据窃取以及控制其他 VM 。

●同一物理主机上 VM 之间流量的不可见性，导致其通信流量不经过传统的防火墙等控制手段，无论是 VM 之间的攻击数据，还是攻击之后传输数据的隐蔽信道，传统的基于网络的检测技术都将完全失效。而解决这一问题的主要手段是部署各种虚拟化安全引擎。

●虚拟环境下的安全审计更加困难，主要还是由于统一物理机上虚拟机流量的不可见，导致审计系统无法完成全部作业。

●缺乏有效手段自动部署虚拟安全措施，目前在

虚拟环境下部署安全措施，例如 UTM、IDS 等，需要配置虚拟机，安装引擎，配置参数，十分复杂且加大了账户管理的难度也增加了安全风险。

对于虚拟化环境来说，安全措施和手段的要求没有发生变化，关键是解决虚拟化环境下的安全措施（或者是安全产品）的部署和监管。

2 设计目标

提供一套针对虚拟化环境的安全服务器一体化解决方案（以下简称“安全服务器”），实现虚拟化环境的基础架构及虚拟化环境的信息安全整体防护。安全服务器支持将物理服务器虚拟化，并提供各虚拟化主机的统一管理及资源整合功能，同时整合各类安全防护措施（FW、IPS、AV、VPN 等）的自动部署和配置，统一监控虚拟化环境下的安全整体状态、虚拟机和安全设备状态，支持虚拟化主机可视化集中展示，虚拟化环境下的安全风险监控和分析等。

3 总体设计

安全服务器由安全服务器管理平台、虚拟化软件平台、虚拟化统一威胁管理系统（以下简称 vUTM）及物理服务器硬件组成。

●安全服务器管理平台，提供对虚拟化主机及虚拟化统一威胁管理系统的集中管理和集中监控功能。

●虚拟化软件平台由虚拟化基础架构平台软件 vServer 和虚拟化基础架构管理软件 vCenter 组成，前者把物理服务器虚拟化，后者则把各虚拟化的主机整合成为一个统一的资源池，并对外提供服务。

●vUTM 增强了虚拟环境内部虚拟机流量的可视性和可控性，提供 FW、IPS、AV、VPN 等功能，可以随时随地提供虚拟环境内部的全方位网络安全防护。

●物理服务器硬件：通用服务器硬件。

安全服务器管理软件需要和虚拟化软件平台交互，以实现虚拟化业务环境的全生命周期的管理。

安全服务器的体系架构图如图 1 所示。

4 功能设计

4.1 虚拟化环境管理

虚拟环境管理提供了一个总体性的视图来展示隐蔽在虚拟平台中的各类虚拟节点，并对虚拟节点的逻辑关系、运行状态进行展现。

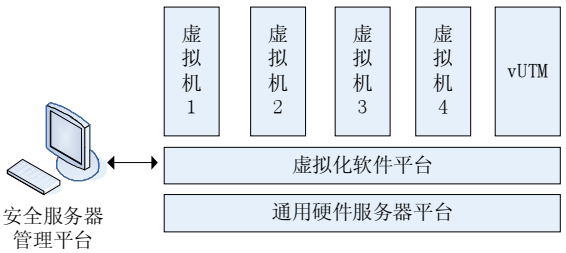

图 1 安全服务器体系架构

通过与虚拟化软件平台的通信，安全服务器可以自动发现虚拟化软件平台上部署的各类虚拟节点，例如虚拟路由器、虚拟交换设备、分布式交换设备、虚拟接口组、虚拟机、虚拟安全设备并形成图形化逻辑拓扑图。安全服务器能发现虚拟设备类型，自动读取虚拟设备的属性信息，自动发现后的拓扑图可以编辑、调整，在形成拓扑图同时，可以根据管理层次形成树形管理目录。所有虚拟设备在拓扑图上能清楚展示，直接逻辑关系清晰，正确，如图 2 所示。

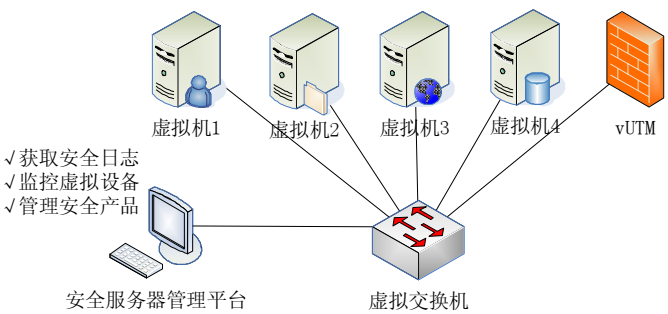

图2 虚拟逻辑拓扑图

在拓扑图上可直接展示各虚拟设备节点的运行状态，节点的告警信息，用不同的颜色标识设备的运行情况，可修改拓扑图的背景，并提供对节点管理的工具，例如远程的连接登录接口 SSH、Telnet 和 ping 等，可直接查看节点的详细信息，例如节点的名称、设备类型、IP、设备描述等。

总体虚拟节点拓扑视图为系统其他功能的操作提供基础的执行入口，可直接选中虚拟节点建立监控任务，还可以在拓扑视图中直接进行虚拟安全设备的部

署,修改本平台部署设备的配置信息。

在虚拟化环境管理功能中，还提供虚拟设备的分类管理、列表展示、设备的查询搜索功能。提供流量信息展示、故障显示。

4.2 虚拟化功能

(1)虚拟化基础功能

安全服务器虚拟化软件平台提供虚拟化基础功能,它以服务器虚拟化的方式,优化和管理业界标准 IT 环境。服务器虚拟化通过软件的方式，在一台服务器上,模拟运行多个标准硬件配置的物理服务器,并依此基础技术,将传统数据中心改变为可扩展的、动态的、绿色的数据中心。

安全服务器虚拟化软件平台包含两个关键组件:虚拟化基础架构平台软件 vServer 和虚拟化基础架构管理软件 vCenter,前者把物理服务器虚拟化,后者则把各虚拟化的服务器整合成为一个统一的资源池,并对外提供服务。

(2)虚拟机动态迁移

安全服务器虚拟化软件平台提供虚拟机动态迁移功能，可以方便地在不同物理服务器之间不中断业务地迁移虚拟机,极大地方便了物理服务器的故障维修,避免维修过程中的长时间业务中断。同时,可以方便地进行业务整合及业务部署调整。

(3)虚拟机高可用性(HA)

安全服务器虚拟化软件平台提供 HA 功能，当虚拟机集群中的某台物理服务器故障后，其上的虚拟机会自动地在另外一台 HA 服务器上启动，保护业务系统不会因为物理服务器的故障长时间中断。

(4)虚拟机镜像(VMirror)

安全服务器虚拟化软件平台提供虚拟机镜像(VMirror)功能,两台物理服务器之间实时进行虚拟机状态同步，当一台物理服务器或其上的虚拟机发生故障后，另外一台服务器上镜像虚拟机立即接替故障服务器上的虚拟机运行,业务不中断。VMirror 功能提供了虚拟机和物理服务器的高容错性保障。

(5)负载均衡

安全服务器虚拟化软件平台提供负载均衡功能,实现集群服务器之间根据负载情况进行自动的、动态的虚拟机迁移，从而平衡集群之间各物理服务器的负载,充分利用硬件资源保证业务处理性能。

(6)备份及快照

安全服务器虚拟化软件平台提供虚拟机备份及快照功能,管理员可以手工备份虚拟机,也可以配置策略定时备份,同时还可以创建虚拟机快照,保存虚拟机运行状态。备份和快照功能提供了故障恢复机制,当前虚拟机故障后,可以方便地从快照点或备份点还原。

(7)热添加

安全服务器虚拟化软件平台提供热添加功能,可以在虚拟机运行状态下动态添加 CPU、存储及网络设备等，用户可以很方便地根据业务的扩展动态调整虚拟机的资源,在调整资源时不影响正常业务的运行,保证良好的虚拟化系统可扩展性。

4.3 虚拟化安全防护

安全服务器的防护功能由 vUTM 提供，它采用了一体化的软件设计，集防火墙、VPN、入侵防御功能(IPS)、防病毒(AV)、反垃圾邮件、抗拒绝服务攻击(Anti-DoS)、Web 内容过滤、漏洞扫描等多种安全技术于一身,同时全面支持路由、QoS、高可用性(HA)、日志审计等功能，为虚拟化主机边界提供了全面实时的安全防护，帮助深圳供电局抵御日益复杂的虚拟化安全威胁。

vUTM 虚拟化统一威胁管理系统充分利用虚拟化层提供的内省 API 来实现对其他虚拟系统的安全监控及防护,实现原理如图 3 所示。

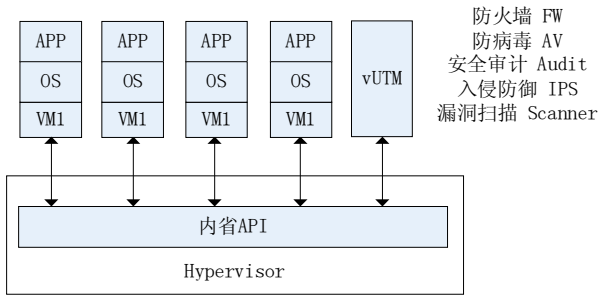

图 3 vUTM 实现原理

虚拟化统一威胁管理系统的策略可由安全服务器管理平台统一进行配置和下发。

vUTM 功能描述:

工作模式:工作于虚拟化平台内部,保护 VM 之间的访问,支持透明模式、路由模式、混合模式;

防火墙模块：可基于 IP 地址、协议、物理接口、时间、应用、用户等下达安全策略；

VPN 模块：支持 PPTP、IPSec 和 SSL 等多种 VPN；

入侵防护模块：实时的基于网络的入侵检测和阻断系统；

防病毒模块：能够检测、消除感染现有虚拟化环境的病毒和蠕虫，实时地扫描输入和输出邮件，实现对灰色软件、间谍软件及其变种进行阻断；

Web 内容过滤模块：支持 URL 域名、关键词模式匹配、黑白名单列表等内容过滤；

反垃圾邮件模块：支持黑白名单、反向 DNS 等反垃圾邮件技术，支持实时黑名单 RBL，在线查询垃圾邮件服务器，阻断垃圾邮件源；

漏洞扫描模块：可以对后门、服务探测、文件共享、系统补丁、IE 漏洞等主动式扫描；

认证授权模块：支持 LDAP、Radius 、TACACS/TACACS+、Windows AD、PKI 证书等多种认证方式；

安全管理模块：可通过扩展的安全管理系统，实现安全审计、日志分析、安全报警等功能；

日志模块：可对流量、攻击事件、垃圾邮件、Web 过滤等各方面内容进行日志审计。

4.4 虚拟化安全监控

安全服务器提供虚拟化软件平台和虚拟系统的监控功能，可对虚拟化软件平台和虚拟系统进行性能监控，针对不同的设备类型提供不同的监控指标和图形化的监控面板。

通过建立监控任务，可以配置监控的时间间隔，监控阈值等各项参数，可以对监控的阈值设置上上限、上限、下限和下下限，当监控任务超过阈值将会触发告警。对告警可设置告警动作。能够保存各个监控的数据，用户可以查看最近 24 小时、最近 7 天的实时曲线图形，可以查看自定义时间段的历史数据，可以根据用户设定的时间段生成报表。管理员可以实时查看监控数据，提供实时数据和图形展示。

管理员可以对监控指标进行定制和自定义，根据需要添加自定义的监控指标。对虚拟化平台的监控内容，至少包括虚拟化平台的运行状况、CPU、内存、磁盘利用率，可监控虚拟化平台的资源分配情况。对虚拟设备的监控，包括运行状态、CPU 利用率、内存利用率、磁盘利用率等基本信息。可根据不同虚拟设备的特性设置监控不同的内容。

4.5 告警响应管理

安全服务器提供告警响应管理功能，系统中，虚拟设备运行状态发生变化会触发告警，性能监控超过设定的阈值也会触发告警、这些告警都能产生告警事件，触发一定动作。告警的动作有 Syslog、SNMP Trap、弹出对话框、短信、邮件、即时通信等。告警产生的信息提示能准确反映告警事件的具体内容，告警通知可指定发送的用户，用户可通过管理平台对告警进行确认和处理。系统可以过滤不需要的告警和消除重复告警。系统可对告警进行查询和存储。告警列表和告警查询的结果列表支持导出为文件保存，支持导出为 Excel 文件。

4.6 报表管理

安全服务器提供报表管理功能，可提供虚拟化安全监控报表、虚拟化软件平台运行监控报表。能生成日报、周报、月报、年报，可导出为 PDF、DOC、HTML、XLS 等格式。

4.7 系统功能

(1)资产管理

能够管理构成虚拟化环境的全部物理硬件、网络和软件、虚拟资源，以树形结构和图形化展示当前虚拟环境的资产情况，以及对资产能够手动录入和自动导入，实现虚拟化环境资产的管理，以符合管理和审计要求。

(2)用户管理

安全服务器采用三权分立原则，默认提供用户管理员、系统管理员、审计管理员，其他系统用户由用户管理员创建、授权。用户管理员不能直接对除用户权限管理之外的功能进行操作。默认的系统管理员具有除用户权限管理、系统审计外的操作权限，审计管理员对所用用户的操作行为进行审计。

(3)权限管理

安全服务器内置用户权限，参看用户管理部分。针对系统普通用户的权限设置，分为功能模块、管理设备

权限。针对各功能模块能定义用户是否可见，是否具有读写权限。管理设备权限，用户自己创建部署的虚拟设备归创建用户管理，该用户可以将设备指定给其他用户管理。

(4)系统审计

安全服务器可详细记录每个用户的操作行为。记录管理员用户名、事件发生的日期和时间、功能模块、操作内容等。审计日志与外部事件区分加密存放，除审计管理员外不能查看。系统审计日志禁止修改和删除。根据用户名、时间、标题等查询。

5 预期效果

5.1 总体拥有成本降低

通过安全服务器解决方案，为深圳供电局提供一个一体化的业务及安全部署环境。实现服务器资源整合，控制和减少物理服务器的数量，明显提高每个物理服务器及其 CPU 的资源利用率，并可同步实现服务器虚拟化安全防护，免去部署安全措施产生的时间及人力成本，从而降低总体拥有成本。

5.2 业务连续性保障提升

通过安全服务器解决方案，可以借虚拟化软件平台实现安全措施、硬件、存储、操作系统和数据库的完全统一，并通过 HA 和 vMirror 实现系统状态的实时同步，从而真正实现不间断实时备份，保证业务连续性。

由于系统及安全措施的运行和备份都在虚拟机上实现，安全服务器解决方案可以有效降低业务连续性保障成本，并消除传统安全设备的单点故障问题，以前只能对关键应用进行备份，将关键的安全设备冗余部署，而现在可以对所有应用及安全措施进行完整实时备份，进一步保证业务的连续性。

5.3 最大限度保障虚拟化业务安全

安全服务器提供的安全保障环境与业务环境完全隔离，避免安全措施遭受攻击的可能。

安全服务器可实现对业务服务器的完全监视，可设置监控策略对包括 CPU、磁盘和网络 I/O，实现全局的审计和性能监控，及时发现业务性能异常现象。

安全服务器可为离线虚拟机提供安全的存储，防止被恶意篡改，甚至可对离线虚拟机进行安全销毁，防止数据泄露。

安全服务器增强了虚拟环境内部虚拟机流量的可视性和可控性，提供 FW、IPS、AV、VPN 等功能，可最大限度保障虚拟化环境业务安全。

5.4 管理和运维效率提升

通过安全服务器解决方案，可以加快新服务器和应用的部署，大大降低服务器重建和应用加载时间，并直接省去了部署安全措施及配置安全策略的时间。

由于虚拟机、虚拟化统一威胁管理系统的创建和调整极为方便，信息中心将有能力对业务部门和应用的需求快速响应，同时提供安全、可靠的服务，不需要像以前那样，需要长时间的采购流程，然后进行尝试。

同样，由于 VM、虚拟化统一威胁管理系统可快速迁移和备份，使得 IT 维护工作变得简单。以前需要数天/周的变更管理准备和 1~3 小时维护窗口的工作，现在可以在零业务中断的情况下进行快速的硬件维护和升级。

表 1

关键任务	传统方法	安全服务器解决方案
调配新服务器	3～10 天硬件购置 1～4 小时调配新服务器	5～10 分钟调配新虚拟机
部署安全设备	10～20 天设备购置 2～5 天设备割接	5～10 分钟调配虚拟化统一威胁管理系统
应用程序迁移或调整	4～6 小时迁移过程 在维护期间服务中断	2～5 分钟使用动态迁移（服务不中断）
硬件维护	服务器需要 1～3 小时维护时段 安全设备需要返厂维修，通常需要数周时间 需要数天/数周变更管理准备	零停机时间使用动态迁移或 热添加技术进行硬件升级、虚拟化统一威胁管理系统升级或替换

6 结语

虚拟化安全服务器解决方案整合了虚拟化软件平台及虚拟化安全措施的优势，经测试可大幅度提高深圳供电局新服务器、应用的部署速度，大大降低服务器重建和应用的加载时间，并且直接省去了部署安全措施及配置安全策略的时间。虚拟化安全服务器解决方案在提供虚拟化技术便利的同时保障了虚拟化业务的信息安全，并具有部署快、易管理的优点，在电力行业内具有良好的推广应用前景。

参考文献:
[1]**云计算关键领域安全指南** V2.1(Security Guidance for Critical Areas of Focus in Cloud Computing V2.1)CSA 2011
[2]**信息安全技术 信息系统安全等级保护体系框架**(GA/T708-2007)[S],2007
[3]**信息安全等级保护管理办法**(**公通字**[2007]43 **号**)[Z] 2007
[4]**信息安全事件管理指南**(GB/z20985-2007)[S],2007

作者简介:
丘惠军(1978-),**男**,**广东惠阳人**,**本科**,**助理工程师**,**从事领域为信息安全技术和管理工作**
收稿日期:2013-12-10　　**修稿日期**:2014-01-10

Research and Design of Server Virtualization Security

QIU Hui-jun

(Shenzhen Power Supply Bureau Limited Company, Shenzhen 518048)

Abstract:
With the promotion and development of server virtualization technology, Shenzhen Power Supply Bureau introduces server virtualization to improve hardware resource utilization. Virtualization technology in Shenzhen Power Supply Bureau brings convenience. But also it exposes some security problems, such as for some new type of attacks in virtualized operating system, we can't effectively implement access control, traffic detection and security audit in the virtual environment, etc. Puts forward a set of virtualization security solutions that are suitable for Shenzhen Power Supply Bureau by probing into the discussion of virtualization environment infrastructure and information security overall virtualization environment protection.
Keywords:
Information Security; Server Virtualization; Virtualization Security, Virtualization Unified Threat Management System

(**上接第** 74 **页**)

Tracking and Monitoring for Data Center Based on HTML

TANG Wen-zhi, HU Ying

(Experimental Center, Network and Modern Educational Technology Center, Guangzhou University, Guangzhou 510006)

Abstract:
HTML5 is a RIA technology, it gives the freedom to render the interface in the browser through Canvas. At the same time, HTML5 is far from pure RIA technology, the WebSocket I/O communication model brings it into a real-time communication (RTC), that's very important for data monitoring and tracking systems. Specifications are listed for design and implement a data health monitoring and tracking solution in a new way.
Keywords:
Canvas; WebSocket; RIA; Asynchronous Communication; Full Duplex