

基于虚拟化的办公系统因特网安全访问

周 峰

(上海大学 计算机学院, 上海 200072)

摘 要:随着中国金融业国际化程度提高,金融企业内部信息安全成为重中之重。而作为公司与外界沟通的桥梁,办公访问 Internet 服务成为了一个不可关闭的风险敞口。通过对主流虚拟化技术的研究,研发一种基于虚拟交换机的 Internet 安全访问控制方法,用以兼顾 Internet 访问的必要性与内部信息的安全性。文中详细剖析如何使用虚拟交换机技术实现特殊带外管理,隔离 Internet 和内部网络,通过总结方案实施过程中的实际经验提出自动监控解决方案,完善了安全隐患和虚拟机状态的汇报措施,动态地控制风险。针对金融行业信息中心级 Internet 安全访问架构给出了关键部分解决方案,通过部署实施实现了逻辑上完全隔离了 Internet 访问。

关键词:VMware;虚拟机;Internet;安全访问

中图分类号:TP393.08

文献标识码:A

文章编号:1673-629X(2010)10-0184-05

High - Security Internet Accessing in OA Based on Virtualization Technology

ZHOU Feng

(School of Computer, Shanghai University, Shanghai 200072, China)

Abstract: As China's financial sector to improve the degree of internationalization, the financial enterprise information security has become a priority. As a bridge to communicate with the outside world, office services, access to Internet has become a non-closed exposure. In this paper, mainstream virtualization technology research, development of Internet-based virtual switch security access control methods, which take into account the need for Internet access and internal information security. The article detailed analysis of how to use the Virtual Switch technology to achieve a special band management, isolation Internet and internal networks, while the program implementation process by summarizing the practical experience of automated monitoring solutions to improve the security risks and the virtual machine state reporting measures, and dynamically control risk. In this paper, the financial industry information center-level framework for secure access to Internet is given a key part of the solution, achieved through the deployment of the implementation of complete separation of the logic of the Internet access.

Key words: VMware; VM; Internet; accessing control methods

1 概 述

随着中国金融业迈入国际化竞争的行列,对于企业内部信息安全问题的关注程度正逐步提高。为提高国内金融信息系统安全性,部分金融机构采用办公网络与 Internet 实行隔离的安全策略。虽然隔离办公网 Internet 访问有利于防止信息泄露、阻止外部主动攻击,但是同时给员工日常访问 Internet 资源带来了不便。文中以虚拟交换技术为基础,搭建一套用于 OA 的安全 Internet 访问机制,同时针对虚拟化网络环境

可能产生的风险给出关键部分解决方案。

办公终端平时以浏览 Web 站点以及接收 Email 为主,一般机构内部通过网络防火墙屏蔽、访问代理等技术手段已经可以杜绝使用 P2P,对外应用端口映射等用户行为可能带来的网络安全隐患。现有问题主要集中在用户访问 Web 站点、接收 Email 可能带来的信息安全问题。为解决以上问题,系统必须满足以下目标:(1)Internet 与 OA 应当无信息交换;(2)外部网络不能够通过任何方式渗透到内部网络。

现有 OA 访问 Internet 常用的安全隔离技术有两种产品,它们分别是网络隔离卡、Citrix 应用代理。

2 基于虚拟化技术网络安全访问控制原理

根据目标分析,上述两种产品难以满足金融机构

收稿日期:2010-01-05;修回日期:2010-04-08

作者简介:周 峰(1984-),男,上海人,硕士研究生,研究方向为信息安全、虚拟化应用;导师:雷咏梅,副教授,研究方向为高性能计算。

端 Management Console。^[10]

这样做的效果类似在公司内建立了一个与办公系统分网的网吧,但是可以彻底隔绝用户直接将下载的文件移入办公系统,所有的 Guest OS 与 OA 的通信都是封闭的,由于虚拟交换机不能够级联,宿主机不接受直接从远程客户端取得用户在 Internet 上下载的文件,如果用户的确需要这些文件,可以通过与 Guest OS 同处一个 VLAN 中的中转服务器上通过安全部门授权拷贝获得^[7]。

3.2 虚拟宿主机与 Internet 出口网络环境架构

要讨论整个网络出口架构,需要至少以下设备:一台普通具有接入层交换机,一台可以进行三层交换的汇聚层交换机,一个应用代理防火墙(硬件防火墙性能更好些,条件不能够满足的话可以用 Microsoft 的 ISA 作为软件防火墙替代)。满足以上条件后,可以开始搭建出口网络环境(见图 2)^[8]。

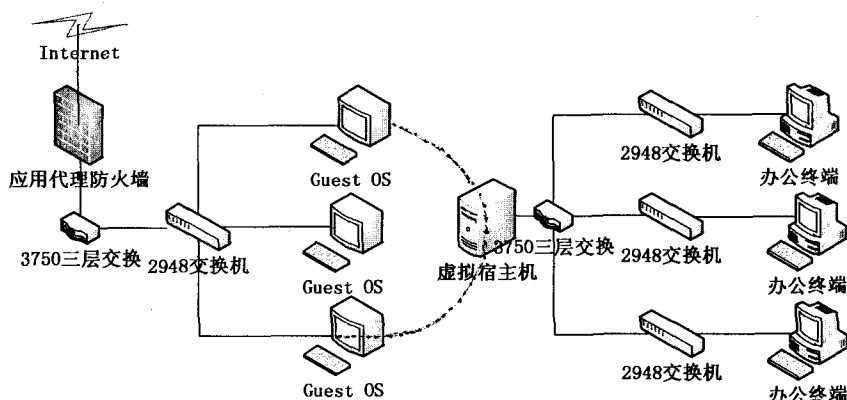


图 2 整体架构

Guest OS 通过虚拟交换机连接到宿主机通向 Internet 的网卡上,该网卡联入的接入层交换机 2948 接入到汇聚交换机 3750 上。因 2948 不具备访问控制能力,故统一在 3750 上对接口做访问接入控制。3750 和 2948 上的每个端口默认是 administratively down/disabled 状态,从而保证不能随意接入 Internet 访问区域^[9]。

在 3750 汇聚交换机和 2948 连接的接口上加入访问控制列表,利用 ACL 限制所有 Guest OS 只能访问代理服务器 Proxy-HD。

针对不同的网络拓扑架构可以采用不同的应用代理方式,如果公司内部本身在应用代理防火墙外还有一层防火墙可采用单 IP 接入方式,如果应用代理防火墙是通向 Internet 最后一道屏障则需要配置两个 IP,一个为 ISP 提供的外部地址。同时防火墙的向外访问策略应当是逐条定义,最后一定要加一条 Deny ALL 的策略。

3.3 宿主机上虚拟机散乱监控的关键技术

通过虚拟化部署技术,构架新的 Guest OS 速度非常快(一般采用虚拟机克隆或者释放系统镜像的方法),但这一优势却潜藏了安全隐患。当批量部署虚拟机时,管理员忽视部分虚拟机正确的虚拟交换机配置,错误地配置在错误的网段上往往可能引发一系列安全问题^[10]。如何解决虚拟机散乱的问题实质就是一个虚拟信息中心的管理员如何面对虚拟机进行动态增减的问题。解决方案一般集中在利用虚拟机供应商提供的 CLI SDK 接口,做一些二次开发。针对 VMware ESXi,则利用 VMware vSphere Command line interface 上的 SDK 做一些小型的 perl 脚本来满足需求^[11]。

以 VMware 为例,利用 ESXi 原有 Server-Side 对象下的一些属性,可以编制一个收集当前 Guest OS 的状态信息,算法核心代码如下:

定义收集的变量

```
.....
my %field_values = (
    'vmname' => 'vmname',
    'hostName' => 'hostName',
    'ipAddress' => 'ipAddress',
);
# 收集 Guest OS 配置
.....
foreach (@valid_properties) {
    if ($ _ eq 'vmname') {
        if (defined($ vm_ view -> config) &&
            defined($ vm_ view -> config ->
                name)) {
            print_log($ vm_ view -> config -> name, "Name", "Name");
        }
        else {
            print_log("Not Known", "Name", "Name");
        }
    }
    elsif ($ _ eq 'hostName') {
        if (defined($ vm_ view -> summary -> guest -> hostName)) {
            print_log($ vm_ view -> summary -> guest -> hostName,
                "hostName", "Host name");
        }
        else {
            print_log("Not Known", "hostName", "Host name");
        }
    }
    elsif ($ _ eq 'ipAddress') {
        if (defined($ vm_ view -> summary -> guest -> ipAddress)) {
            print_log($ vm_ view -> summary -> guest -> ipAddress, "i-
                pAddress", "IP Address");
        }
    }
}
```

```

}
else {
print_log("Not Known", "ipAddress", "IP Address");
}
}
else {
Util::trace(0, "$ - Not Supported\n");
}
}

```

通过这段核心脚本,取得 vCenter 上所有虚拟机的当前状态,包括网卡以及对应 IP。通过定时触发这段脚本,管理员可以及时得到虚拟机状态信息,通过在后台管理口收集对应的状态数据,进行及时汇总、告警,即可实时处理出现的虚拟机散乱问题。

4 系统运行情况分析

4.1 基于虚拟化技术的 Internet 访问安全层次分析

基于虚拟化技术的 Internet 安全访问从本质上将是网络带外管理的一种特殊实例,通过特殊的管理口结点来控制带外虚拟机以达到 Internet 与 OA 之间没有七层网络连接的要求。在上文中,针对虚拟机散乱这个管理问题,作者根据问题的特性给出了实时监控方案,使得整个方案在实际运作过程中更为安全并且可控。

基于虚拟化技术的 Internet 安全层次主要有以下三层(见图 3)。当发生一次外部入侵,首先入侵者需要通过应用代理防火墙,参考应用代理防火墙的特点:内网用户对外网的访问变成防火墙对外网的访问,然后再由防火墙转发给内网用户。所有通信都必须经应用层代理软件转发,访问者任何时候都不能与服务器建立直接的 TCP 连接,应用层的协议会话过程必须符合代理的安全策略要求。基于这种特点,外部攻击主要手段集中在 Web 浏览中及 Email 接收中的恶意代码攻击。

假设外部入侵者前期恶意代码攻击得逞,使得控制 Guest OS 的用户成功执行恶意代码,入侵者必须通过第二道安全控制与检测层。通过在活动目录体系架构中,定制组策略,帮助 Guest OS 统一关闭可能存在风险,强制设立浏览器安全策略,同时通过类似 SCCM 等工具及时修补系统补丁、分发防病毒库。在这种体系下,已知的系统安全与软件漏洞都能够被成功屏蔽^[12]。如果较为严重的入侵情况(未知系统与软件漏洞、大规模蠕虫爆发),纵然 Guest OS 全部给攻破,由于虚拟交换机的特性,通向 Internet 物理网卡的虚拟

交换机和连接内部办公系统的交换机完全隔离,对于重要的信息中心而言,损失的只是与内部办公系统无关、可快速重建的 Guest OS,并不会影响正常的内网办公。

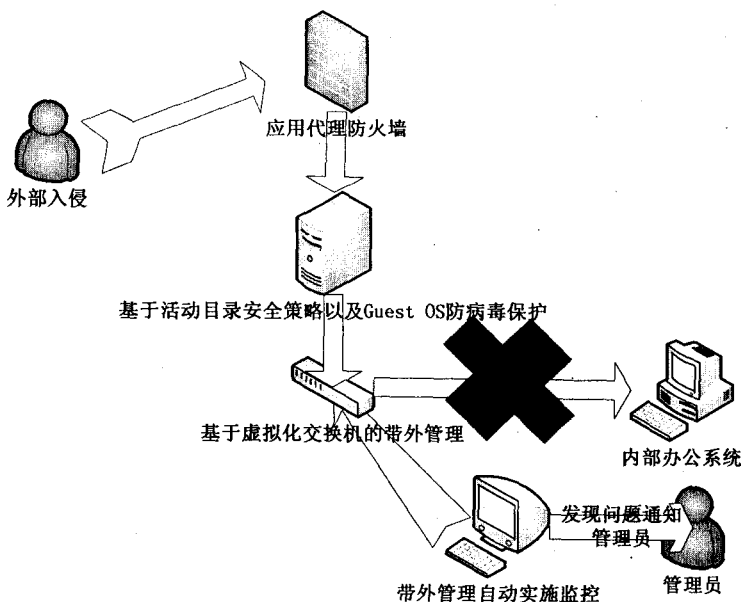


图 3 安全层次

4.2 运用虚拟化技术后整体性能表现

(1) 宿主机磁盘性能。

基于虚拟化技术的 Internet 安全访问达到了安全的要求,但是在性能上是有所牺牲的。性能问题的本质是因为访问 Internet 的终端集中在宿主服务器上,随着客户端访问数量的增多,服务器性能问题首先体现在磁盘 IO 上。

通过测试发现,当一组 LUN 上的虚拟机单元超过 8 台时,磁盘 IO 性能会大幅下降,可以观测到磁盘 IO 量不大但是并发数非常多,用户访问 Guest OS 时很明显能够感受到操作图形不流畅。如果考虑到搭建该环境的成本问题使用服务器本地存储介质,可以考虑不建 Raid,同时取消写缓存,因为 Raid 卡上 Cache 并不多,把 Guest OS 平分在每个 Volume 上。通过在 Guest OS 上同步调用 IE 访问相同网站,建与不建 Raid,网页打开延时时间差异在 11%。

考虑到用户体验和服务可持续性,可以考虑购买 iSCSI 的共享存储作为后台存储,提高 IO 性能。可以将存储上的 LUN 划为 24G 大小,每个 LUN 至多放置 8 个磁盘大小 3G 大小的 Windows XP,同时将 IE 或者其他浏览器的缓存开小(5M 以下),减少磁盘频繁读写的次数。

(2) 宿主机 CPU 和内存性能。

按照使用本地 Raid 的优化方案经过测试,一台 IBM X3650 服务器(1 块 CPU Xeon 2.0G * 4 核,内存

8G,本地磁盘 73 * 4 块),可以运行 30 个 Guest OS,用户使用感受上无明显延迟感。表 1 是根据 vCenter 统计数据取 15 个工作日的使用情况得出的性能数据。

经过对数据分析可以看出,刚开始上班时服务器较为忙碌,由于刚上班,使用 Internet 收发邮件的员工较多,这一时间段用户使用率较高。另外发现中午由于员工休息时间较长,使用互联网访问 Internet 的频率高,造成服务器负载较重。

表 1 CPU 和内存占用率(I)

测试时间	CPU 占用率	内存占用率
8:30-9:30	84%	87%
9:30-10:30	78%	88%
10:30-11:30	75%	88%
11:30-12:30	91%	89%
12:30-13:30	88%	86%
13:30-14:30	82%	83%
14:30-15:30	76%	85%
15:30-16:30	79%	86%
16:30-17:30	75%	83%

针对这种情况,原补丁更新时间从早上 8:30 开始调整到午夜 12 点,同时制作定时关机脚本,强制在空闲时间段关闭用户虚拟机释放内存和 CPU 资源。通过一系列控制措施,使高峰数据得到缓解(见表 2)。

表 2 CPU 和内存占用率(II)

测试时间	CPU 占用率	内存占用率
8:30-9:30	81%	85%
9:30-10:30	78%	86%
10:30-11:30	75%	86%
11:30-12:30	83%	85%
12:30-13:30	85%	87%
13:30-14:30	82%	85%
14:30-15:30	76%	84%
15:30-16:30	78%	85%
16:30-17:30	75%	82%

5 结束语

通过对虚拟化技术的研究,提出一种基于虚拟交

换机的 Internet 安全访问控制方法。在文中,作者详细剖析技术实现方法以及深层次原理,同时就信息中心级的 Internet 安全访问架构给出了关键部分解决方案。并深刻反思了虚拟化产品的网络安全问题,关于潜在安全问题提出了一个较为可行的解决方案。

当采用虚拟化基础实现网络隔离技术时,如果将本方案反向使用,即可完成基于虚拟化技术的安全 VPN 访问,可通过在外部 DMZ 区的 MP 安全地对内网设备进行操作,达到 VPN 和内部网没有七层协议的作用。

参考文献:

- [1] Heiser G, Elphinstone K, Kuz I, et al. Towards Trustworthy Computing Systems: Taking Microkernels to the Next Level[J]. SIGOPS Operating Systems Review, 2007(7):3-11.
- [2] Ave H. VMware Virtual Networking Concepts[EB/OL]. 2007. <http://www.vmware.com>.
- [3] 熊林. VMware 的技术与应用探析[J]. 开发研究与设计技术, 2007(12):428-429.
- [4] 刘志平. 基于 VMware 虚拟网络的构建[J]. 内蒙古大学学报:自然科学版, 2007(1):94-98.
- [5] Whitaker A, Shaw M, Gribble S D. Denali: lightweight virtual machines for distributed and networked applications [R]. Washington: University of Washington, 2002.
- [6] 杨少春. 采用 VMware 构建虚拟并行计算网[J]. 计算机工程与设计, 2006, 27(14):2546-2547.
- [7] 王一剑, 刘美玲. 虚拟化技术在金融业的应用[J]. 金融电子港, 2008(5):56-57.
- [8] 赵长林. 虚拟化中的网络性能和吞吐量[J]. 第一发现, 2009(3):29-30.
- [9] 李芳社. 虚拟化技术在通信基础设施中的应用[J]. 现代电子技术, 2009(8):149-151.
- [10] 那罡. 虚拟化的风险[J]. 网络传播, 2008(8):80-81.
- [11] 阮越, 秦峰, 周建钦. 基于 Linux Shell 的安全审计机制[J]. 计算机技术与发展, 2007, 17(6):155-158.
- [12] 刘涛, 邓璐娟, 丁孟宝. 计算机反病毒技术及预防新对策[J]. 计算机技术与发展, 2007, 17(5):105-110.

(上接第 183 页)

- [8] Tanenbaum A S. 计算机网络[M]. 第 4 版. 潘爱民, 徐明伟译. 北京:清华大学出版社, 2004:682-684.
- [9] 汪冬. 基于 Kerberos 协议的单点登录系统的研究与实现[J]. 办公自动化, 2007(8):24-26.
- [10] 贾淑红, 刘万军. 基于 Kerberos 协议的单点登录系统的设计[J]. 计算机应用, 2007, 27(6):238-239.
- [11] Kohl J T, Neuman B C. The Kerberos Network Authentica-

tion Service (V5)[R]. [s. l.]: Digital Equipment Corporation, ISI, 1993.

- [12] Steiner J G, Neuman B C, Schiller J I. Kerberos: An Authentication Service for Open Network Systems[C]// Proceedings of the USENIX Winter 1988 Technical Conf. Dallas, Texas: USA: USENIX Association, 1988.