

虚拟化安全技术调研分析

介绍了云计算虚拟化技术存在的安全风险，分析了应对时所采取的安全防护方法，对国内外典型的虚拟化安全产品功能特性进行了对比和分析，为企业开展软件定义数据中心安全产品选型提供一定的借鉴和参考。

陈乐然 王刚 陈威 徐小天/国网冀北电力有限公司电力科学研究院

0 引言

目前大部分的企业级数据中心采用虚拟化的部署模式，无论是全虚拟化、半虚拟化以及操作系统虚拟化都能提供动态的资源分配，有效降低硬件购置和运维管理成本，大幅提升企业IT环境的可靠性和运行稳定性。

伴随着云计算虚拟化技术的普及，针对云的网络攻击也是愈演愈烈。2014年2月，提供防御分布式拒绝服务攻击（Distributed Denial of Service Attack, DDoS）攻击服务的云计算公司Cloudflare遭遇了史上攻击流量最大的DDoS攻击，峰值流量超过400 Gbit/s。同年9月，iCloud遭到针对用户名、密码和安全问题的定向攻击，导致好莱坞百名女星存放在云中的私密照片泄露，引发了人们对iCloud安全性的担忧^[1]。同年11月，Xen开元管理程序中的一个安全漏洞导致包括AWS、Rackspace和SoftLayer等多个公有云服务商被迫紧急重启，中断了大量客户的业务运

营。2015年初，黑客组织Lizard Squad利用DNS劫持，DDoS等手段对微软、Facebook和谷歌的大规模网络攻击，致使上述公司部分网站页面无法正常登录。3月，由于苹果公司内部DNS错误，包括App Store、iTunes Store、Mac App Store以及iBooks Store在内的一系列苹果在线商店服务遭遇大面积服务中断，事故恢复时间长达11 h，全球5亿iCloud用户中的40%受到影响。

1 虚拟化安全风险

虚拟化系统的安全风险包括传统安全风险和由于虚拟化引入的新型风险。传统风险包括物理安全、操作系统安全漏洞、应用层漏洞、各类口令爆破、拒绝服务攻击和数据泄露等。虚拟化技术引入的新型安全风险包括以下几类。

1.1 虚拟网络流量的不可视导致虚拟机间攻击难以发现

在虚拟网络中，有一部分网络流量并不流经物理网络，例如在虚拟交换机中同属一个虚拟局域网（Virtual Local Area Network, VLAN）下的两台虚拟机（Virtual Machine, VM）在通信时，流量将直接在虚拟层面转发。传统的流量分析设备往往部署在网络边界，对类似的虚拟网络攻击无能为力。攻击者可以利用这种特性，避开安全管理员的监控，从一台VM向VLAN内的其他VM发起攻击。这种攻击方式被称为VM Hopping，是各类虚拟化安全产品重点解决的问题之一。

1.2 资源的高度集中难以应对拒绝服务攻击

云环境资源的高度集中和动态分配



陈乐然/工程师

关键词/Keywords

虚拟化·
安全风险·
防护方法·
安全产品·

带来弹性的同时，也引入了严重的DDoS攻击安全隐患。由于虚拟化技术允许在一台宿主机上运行多个业务应用系统，当该宿主机遭到DDoS攻击时，其上承载的所有业务应用都将受到影响。目前DDoS已成为针对云环境的首选攻击手段，2015年许多知名公有云都出现了因为超大流量拒绝服务攻击导致的服务中断，对业务高度依赖云环境的企业造成了巨大的经济损失。

1.3 云平台组件安全风险

云平台组件的安全风险主要对象是管理控制平台和宿主机。管理控制平台管理员具有虚拟化环境的全部操作权限，包括对主机和虚拟机的开关机及配置修改，对共享存储和虚拟机数据的增删改，对虚拟资源的任意调配等等。然而管理员的身份认证仅采用账号+密码的方式，强度明显不足，容易被“社工”、字典爆破等方式破译。一旦管理控制平台被攻克，将带来严重的安全隐患。

宿主机的安全风险包括两方面：一是来自主机外部的攻击，方式与物理环境类似，例如信息收集、系统漏洞扫描、Web攻击、远程溢出和社会工程学攻击等等；二是来自宿主机内部的攻击，由其他VM发出，利用虚拟化软件漏洞获取主机底层操作系统权限，这种攻击方式被称为虚拟机逃逸（VM Escape）。

1.4 多租户存储导致数据安全风险

在云环境中，数据被集中保存在共享的存储区域网（Storage Area Networking, SAN）、网络文件系统（Network File System, NFS）和iSCSI等存储设备中，存在数据窃取、篡改和非法访问等安全风险。数据安全风险有两方面成因：一是数据隔离不严格和缺乏严格、有效的身份认证机制；二是数据的明文保存，对敏感数据未进行必要的加密处理。同时由于虚拟化环境在行为审计方面的不足，发生数据泄露时难以进行实时的监测和事后的溯源。

2 虚拟化安全防护方案

针对上述新型安全风险，所采取的常见安全防护方法包括加强虚拟机间的流量监控，建立信任链条实现可信计算，建立严格的访问控制策略

以及数据加密。

2.1 虚拟机间的流量监控

在虚拟网络中，不同VLAN和不同主机VM间的数据通信需要通过上行链路进入物理网络，可以采用传统的安全防护手段，在出口和边界处部署安全设备。对于同一宿主机内相同VLAN虚拟机间的流量监控则需要部署特殊的定制化工具，为了达到这一目的，一些云计算软件供应商积极发布了针对其产品底层的API，加速了安全厂商对适用于云环境的防护软件的研发。

2.2 建立信任链条，实现可信计算

虚拟化安全风险很大程度上来源于虚拟化软件无法识别来自外部的篡改和替换，因此需要建立从VM到宿主机的信任链条。采用可信平台模块（Trusted Platform Module, TPM）可提供密钥生成、加密、解密和签名等功能，有效提升系统安全性。

2.3 严格的访问控制和权限隔离

访问控制和权限隔离包含两个方面：一是云平台基础设施，可采用防火墙或单点登录设备（堡垒机），也可采用双因子登录方式加强用户身份认证；二是对数据的访问，可在虚拟环境内部划分安全域，结合细粒度的访问控制列表，实现基于用户、角色和特权的权限管控，同时还需加强对虚拟磁盘文件和镜像文件的保护。

2.4 数据加密技术

数据在云端存储时应采用加密技术保存敏感和核心业务数据，防止攻击者和云供应商对数据的非法访问和滥用。传输时，应采用加密协议保障数据的安全性和完整性。

3 典型安全产品功能对比

在国外，虚拟化安全产品的研发起步较早，许多安全厂商与云计算解决方案的供应商开展了长期的紧密合作。以VMware为例，早在2009年的vSphere 4.0时代，VMware就发布了VMsafe API，它是一组面向第三方安全厂商的Hypervisor层应用程序编程接口，提供了虚拟化软件层的数据传输可见性。安全厂商基于此API研发适用于云环境的安全产品，实现数据在进入虚拟系统之前的安全检测，可有效防止恶意代码在虚拟机中的传播与

执行^[2]。

3.1 VMware VShield

VMwareVShield是VMware官方发布的安全套件，对应VSpheere的 5.0版本。VShield可全面提升软件定义数据中心应用程序和数据的安全性，提高可见性和控制力，加快整个企业内的云计算遵从性举措。在VSpheere5.5.1及后续的版本中，VShield被重新命名为VCloud Networking and Security，并以VCloud Suite中的一个功能组件的形式出现。

VShield的安全防护方案如图1所示。

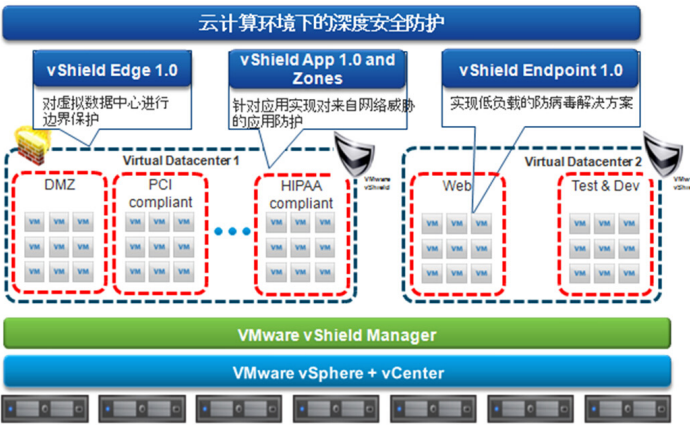


图1 VShield安全防护方案

VShield的核心组件包括VShield Edge、VShield App、VShield Zones、VShield Endpoint和VShield Manager。

VMware VShield Edge：部署在虚拟网络边界，其功能类似于安全网关，具有动态主机配置协议（Dynamic Host Configuration Protocol, DHCP）、网址转换、防火墙、负载均衡、站点间虚拟专用网络（Virtual Private Network, VPN）和端口组隔离等功能。

VMware VShield App：保护虚拟数据中心应用程序。可创建智能化的安全策略并通过安全组细化实施，实现基于虚拟网络适配器的流量分析和安全管理。

VMware VShield Zones：提供针对网络威胁的基础防护，利用基本流量信息（例如源IP、目的IP 地址和端口），基于自定义的安全与，为应用程序提供防火墙保护和策略管理^[3]。

VShield Endpoint：低负载防病毒软件，提供基于主机的无代理防病毒和恶意软件防护^[3]。

VShield Manager：VShield管理控制平台，用

于管理、部署、报告、记录和集成第三方安全服务。

3.2 趋势Deep Security

趋势是最早与VMware开展合作的安全厂商之一，其Deep Security产品是一款针对虚拟化、云计算和传统数据中心环境的服务器防护系统，同时需要VMsafe API和VMwareVShield Endpoint API的支持。实现了无代理的病毒防护，有效预防针对操作系统和应用程序漏洞的非法入侵，监控系统的完整性及集中的管理日志，有助于提高资源利用率，降低运行和维护的成本。

Deep Security产品由三部分组成：Deep Security管理控制平台（Deep Security Management, DSM）、安全虚拟机（Deep Security Virtual Appliance, DSVA）和Deep Security 客户端（Deep Security Agent, DSA）。DSM负责创建安全策略，查看病毒事件日志，监控服务器防护状态，根据报警并采取预防措施。DSVA以虚拟机形式运行在宿主机上，提供无代理的防病毒、数据包深度防护（Deep Package Inspection, DPI）、防火墙、Web应用程序防护和应用程序控制防护和数据完整性监控等安全功能。DSA部署于物理服务器或被保护的VM上，起到协助执行数据中心安全策略的作用。系统框架如图2所示。

趋势Deep Security的功能非常强大，包含五个功能模块：无代理防病毒、双向防火墙、DPI深度包检测、完整性检测和日志审计。

无代理病毒防护：集成最新的VMware VShield Endpoint API，不用在虚拟机上安装任何代理程序，无需占用任何业务资源，实现对病毒、间谍软件和木马等威胁的查杀，提供实时、手动和计划任务的安全内容过滤，防止虚拟机受到病毒、间谍软件、木马和其他恶意软件的侵害。

DPI深度包检测：深度包检测模块提供了针对已知漏洞和0day漏洞的安全防护功能。对已知漏洞建立漏洞规则库，对未知漏洞采用检测恶意代码中的异常协议数据的方式进行防护。此外，DPI规则还通过一组Web应用程序防护策略，对Web应用程序提供保护。

双向状态防火墙：通过细粒度的数据过滤，执行基于网络环境的安全策略。缩小物理、云和

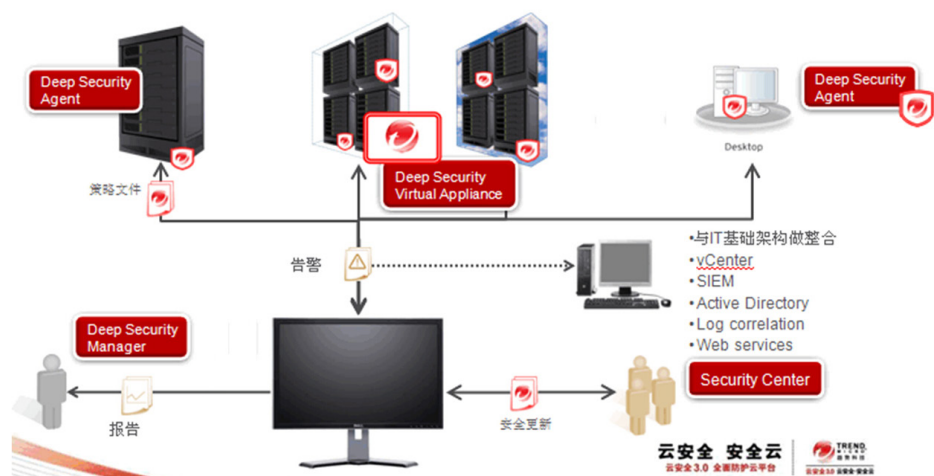


图2 DeepSecurity系统框架

虚拟服务器的受攻击范围，限制对特定IP 或 MAC 地址的数据通信。

完整性监控：扫描和检测计算机系统文件、目录、注册表项、注册表键值已安装软件和运行服务中发生的变更，将更改记录在管理中心中，根据预设策略触发报警。

日志审计：收集和分析操作系统和应用程序安全日志，智能分析需关注安全事件，形成审计报告。

国内方面，虚拟化安全产品的研发起步较晚，但由于国产化的政策激励，发展却较为迅

速。近年来许多顶尖的安全厂商都推出了针对云环境的安全防护产品。

3.3 360 “天擎” 虚拟化安全管理系统

360 “天擎” 虚拟化安全管理系统是一个使用轻代理的私有云防病毒产品，以360私有云和杀毒网络版产品为基础，实现了对虚拟化终端的安全防护，提高虚拟化环境下安全软件的运行效率，有效降低安全软件对虚拟化平台的资源占用。

产品组件方面包括控制中心、查杀服务器和轻代理客户端三部分，如图3所示。

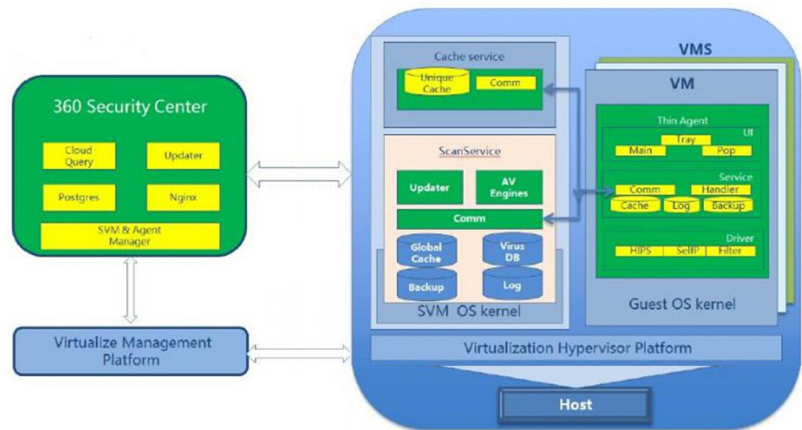


图3 360 “天擎” 虚拟化安全管理系统架构

3.4 瑞星虚拟化系统安全软件

早在2013年10月，瑞星公司推出了瑞星虚拟化系统安全软件，系国内首家自主研发的企业级虚拟化平台安全防护解决方案。该产品基于VMware VShield Endpoint技术，采用无代理模式，具有系统

资源消耗低，实时防护未启动虚拟机，安全策略随虚拟机迁移灵活配置并避免安全风暴发生等特性。瑞星虚拟化系统安全软件采用分布式体系结构，由五个相互关联的子系统组成：管理中心、安全虚拟设备、日志中心、升级中心和查杀协作。各个子系

统协同工作，共同完成对整个虚拟化平台的病毒防护工作。系统架构如图4所示。

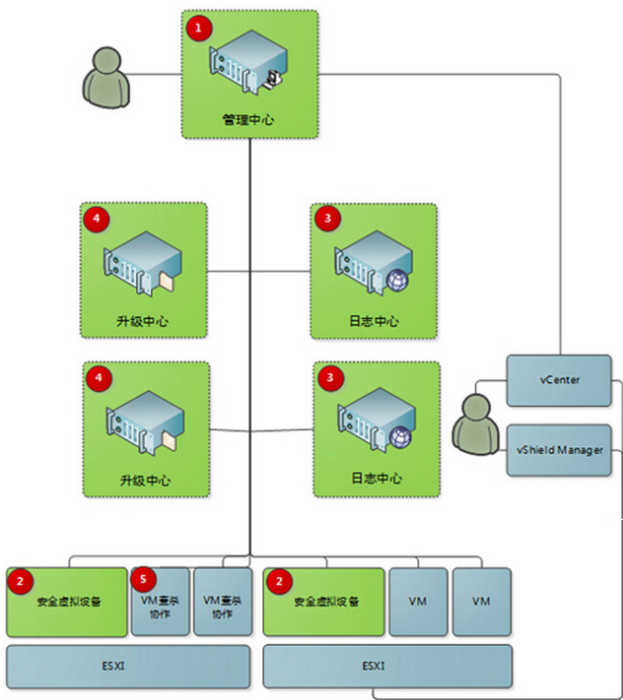


图4 瑞星虚拟化安全软件系统结构

对比360、瑞星和趋势产品的核心组件，都是控制中心、查杀虚拟机和轻量化查杀协作组件，不同之处仅体现在各家安全公司病毒数据库的差异，除此之外趋势Deep Security还增加了一个DPI深度包检测的功能模块，实现了虚拟机间的网络流量监控，可以说是该产品的一大亮点。

3.5 安恒信息技术有限公司云运维审计与风险控制系统、云Web应用防火墙

伴随着国内安全产业的蓬勃发展，从事安全服务的企业纷纷崭露头角。杭州安恒信息技术有限公司是众多行业新秀中的佼佼者，从最初的数据库安全审计系统、Web应用防火墙到现今的十几条成熟产品线，安恒信息逐步形成了以完全自主知识产权为基础，优秀专家队伍为依托的强大研发团队。在云计算的发展趋势下，成功实现了安全产品从物理设备向云环境的转型。2015年9月，安恒信息与阿里云正式签署战略合作协议，双方正式达成战略合作伙伴关系，致力于向云计算用户特别是政企用户提供专业的一站式安全产品及服务。下面将对安恒信息的成功云产品“云端Web应用防火墙”（云WAF）和“云端运维审计与风

险控制系统”（云堡垒机）进行简要介绍。

(1) 云WAF

安恒云WAF是安恒自主开发、拥有独立知识产权的新一代Web安全防护产品。相比于其他以代理技术为基础的Web应用防火墙，新一代WAF并不完全依赖根据攻击特征制定的安全特征匹配，而是以用户网站为核心，自动依据网站学习建模，生成基于用户网站的专有安全规则，因此防护更有针对性，误判极低，且性能得到更大的提升。可实现对网络层、Web服务层、Web应用程序层和应用内容属性四个层面的全方位安全分析与防御。

安恒云WAF可实现十余项功能，包括对常见的三十余类Web通用攻击的安全防护、协议规范性检查、抗Web扫描器扫描、敏感信息防泄漏、CC攻击防护、防盗链、虚拟补丁、白名单技术、基于攻击源识别的智能防护、Web服务自发现、应用程序错误跟踪、静态网页防篡改和站点访问审计等等。

通过添加资产的IP和端口信息并将Web服务器的地址映射到云WAF上，由云WAF对流量清洗后再转发给后端的真实服务器。如图5所示。

Web应用的安全一直是企业安全部门所重点关注的风险点之一，众多的安全漏洞和较大的攻击面使Web应用成为许多渗透行为的起始点和突破点。而虚拟网络的封闭性无疑给安全人员对VM间恶意网络流量的监测造成了一定的困难。云WAF采用虚拟化的部署方式，可有效过滤VM间网络流量，阻断针对Web应用的网络攻击。

(2) 云堡垒机

云堡垒机是安恒信息在总结多年安全运维管理理论和实际运维经验的基础上，结合各类法令法规（如等级保护、ISO27001等）对运维管理的要求，自主研发完成的运维安全管理系统。该产品特点是支持自动建模授权、应用虚拟化应用中心、统一账户管理与单点登录功能，且符合4A（认证Authentication、账号Account、授权Authorization和审计Audit）统一安全管理方案。

云堡垒机采用旁路或串行部署的方式，可支持多种运维协议和运维方式，提供灵活的授权和访问控制，以及对运维过程的完整运维审计功

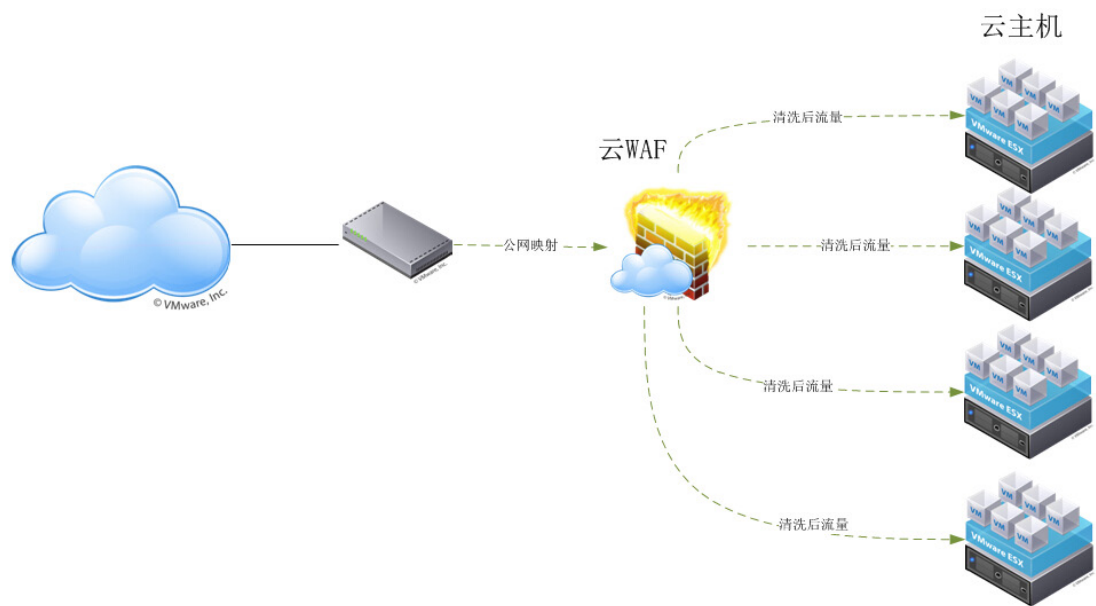


图5 SCB10-800/10变压器声压级随铁心夹紧力变化规律

能。有效解决账号管理的混乱、脆弱密码和不安全认证、用户授权不清晰及访问控制不严格、操作过程无审计等问题。

运维协议：支持SSH、SFTP、FTP、Telnet和RDP等协议，支持对KVM、Xmanager、pcanywhere、VNC、Vmware和数据库等运维工具进行操作审计。

运维方式：支持单点登录，最小限度改变运维习惯，支持putty、secureCRT、Xshell、windows自带命令行和远程桌面等。

安全监测：对资产的安全性、连接性进行自动监测和发现。

灵活授权：支持自动学习建模授权模式，可根据用户日常运维习惯建立起授权模型，自动添加资产IP和用户信息。

访问控制：支持基于IP/IP段、用户/用户组、资产/资产组、协议、时间和危险级别等组合策略进行访问控制，对于匹配规则的行为予以阻断或放行。

运维审计：支持运维全过程安全审计，可进行实时监控和历史运维过程真实回放。

4 结束语

云环境的多租户商业模式带给运维审计的压力是不言而喻的，大多数企业级数据中心都存在账号管理混乱，权限划分不清和访问控制不严格的问题。堡垒机作为运维审计和单点登录利器，可实现对运维用户的集中管理，加强运维权限管控，实现运维自动化，做到运维全过程的透明和可溯源，促进企业IT环境的整体安全性提升。

参考文献

[1] 王笑帝,张云勇,刘楠,等.云计算虚拟化安全技术研究[J].电信科学, 2015, 6:1-5.
[2] 陈乐然,王刚,陈威,等. VMware虚拟化环境安全风险与防护方案研究[J].华北电力技术,2014,9:61-65.
[3] VMware vCloud Director云计算解决方案[J/OL].百度文摘, [2012-09-24].http://wenku.baidu.com.

作者简介

陈乐然（1987-），男，硕士研究生，工程师，从事信息安全领域。

（收稿日期：2015-11-20） **EA**
（编辑：朱历）