(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103258160 A
(43)申请公布日 2013.08.21

(21)申请号 201310208995.6

(22)申请日 2013.05.30

(71)申请人 浪潮集团有限公司
地址 250101 山东省济南市高新区舜雅路 1036 号

(72)发明人 宋桂香 高丽琴

(51)Int.Cl.
G06F 21/53(2013.01)

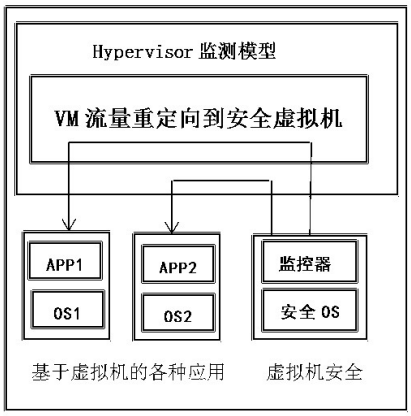
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种虚拟化环境下的云安全监测方法

(57)摘要

本发明公开了一种虚拟化环境下的云安全监测方法，属于计算机信息安全技术领域，直接在云的服务器端的内部部署虚拟机安全软件，通过对虚拟机开放的API接口的利用，将所有虚拟机之间的流量交换在进入到虚拟机之前，先引入到虚拟机安全软件进行检查。本发明的一种虚拟化环境下的云安全监测方法和现有技术相比，进一步防止快速增长且具有动态性的网络威胁，提高云计算虚拟化环境下的整体安全性能。



CN 103258160 A

1. 一种虚拟化环境下的云安全监测方法，其特征在于直接在云的服务器端的内部部署虚拟机安全软件，通过对虚拟机开放的 API 接口的利用，将所有虚拟机之间的流量交换在进入到虚拟机之前，先引入到虚拟机安全软件进行检查。

2. 根据权利要求 1 所述的一种虚拟化环境下的云安全监测方法，其特征在于虚拟机安全软件为 VMware 开发的虚拟机安全软件。

3. 根据权利要求 1 所述的一种虚拟化环境下的云安全监测方法，其特征在于所述的流量指虚拟机之间的横向流量。

4. 根据权利要求 1 或 3 所述的一种虚拟化环境下的云安全监测方法，其特征在于虚拟机之间的横向流量安全 :同一个服务器的不同虚拟机之间的流量将直接在服务器端内部实现交换，服务器端的内部部署虚拟机安全软件，通过对虚拟机开放的 API 接口的利用，将所有虚拟机之间的流量交换在进入到虚拟机之前，先引入到虚拟机安全软件进行检查。

一种虚拟化环境下的云安全监测方法

[0001]

技术领域

[0002] 本发明涉及一种计算机信息安全技术领域，具体地说是一种虚拟化环境下的云安全监测方法。

背景技术

[0003] 传统的企业流量模型相对比较简单，各种应用基准流量及突发流量有规律可循，即使对较大型的数据中心，仍然可以根据 web 应用服务器的重要程度进行有针对性的防护，对安全设备的处理能力没有太高的要求。

[0004] 传统的安全威胁检测模式中，客户端安全软件或硬件安全网关充当了威胁检测的主体，所有的流量都将在客户端或网关上完成全部的威胁检测。这种模式的优点是全部检测基于本地处理延时较小，但是由于客户端相互独立，系统之间的隔离阻止了威胁检测结果的共享。这也意味着在企业 A 已经检测到的新型威胁在企业 B 依然可能造成破坏，没有形成整体的安全防护。

[0005] 虚拟化是目前云计算最为重要的技术支撑，需要整个虚拟化环境中的存储、计算及网络安全等资源的支持。在这个方面，基于服务器的虚拟化技术走在了前面，已开始广泛的部署应用。基于该虚拟化环境，系统的安全威胁和防护要求也产生了新的变化。

[0006] 传统风险依旧，防护对象扩大。一方面，一些安全风险并没有因为虚拟化的产生而规避。尽管单个物理服务器可以划分成多个虚拟机，但是针对每个虚拟机，其业务承载和服务提供和原有的单台服务器基本相同，因此传统模型下的服务器所面临的问题，虚拟机也同样会遇到，诸如对业务系统的访问安全、不同业务系统之间的安全隔离、服务器或虚拟机的操作系统和应用程序的漏洞攻击、业务系统的病毒防护等；另一方面，服务器虚拟化的出现，扩大了需要防护的对象范围，如 IPS 入侵防御系统就需要考虑以 Hypervisor 和 vCenter 为代表的特殊虚拟化软件，由于其本身所处的特殊位置和在整个系统中的重要性，任何安全漏洞被利用，都将可能导致整个虚拟化环境的全部服务器的配置混乱或业务中断。

[0007] 云计算环境下的资源监测是云计算平台资源管理的重要组成部分，为资源分配、任务调度和负载均衡等提供依据。由于云计算环境下资源的透明虚拟化和弹性化，并需要对用户使用资源进行计费，因此原有的资源监测方法不能完全满足云计算环境的要求。

[0008] 发明内容

本发明的技术任务是提供一种进一步防止快速增长且具有动态性的网络威胁，提高云计算虚拟化环境下的整体安全性能的一种虚拟化环境下的云安全监测方法。

[0009] 本发明的技术任务是按以下方式实现的，直接在云的服务器端的内部部署虚拟机安全软件，通过对虚拟机开放的 API 接口的利用，将所有虚拟机之间的流量交换在进入到虚拟机之前，先引入到虚拟机安全软件进行检查。

[0010] 虚拟机安全软件为 VMware 开发的虚拟机安全软件。

[0011] 所述的流量指虚拟机之间的横向流量。

[0012] 虚拟机之间的横向流量安全：同一个服务器的不同虚拟机之间的流量将直接在服务器端内部实现交换，服务器端的内部部署虚拟机安全软件，通过对虚拟机开放的 API 接口的利用，将所有虚拟机之间的流量交换在进入到虚拟机之前，先引入到虚拟机安全软件进行检查。

[0013] 此时可以根据需求将不同的虚拟机划分到不同的安全域，并配置各种安全域间隔离和互访的策略。

[0014] 本发明的一种虚拟化环境下的云安全监测方法，通过虚拟机监测器和 Java 调用 C/C++ 得到资源的状态信息。

[0015] 虚拟机之间的纵向流量包括从客户端到服务器端的正常流量访问请求，以及不同虚拟机之间的三层转发的流量；纵向流量的交换必然经过云的外置的硬件安全防护层进行检查，硬件安全防护层的防护的设备类型是以防火墙和入侵防御系统等产品为主，在部署的方式上要求防火墙或入侵防御设备具备 INLINE 阻断安全攻击的能力，部署的位置可以旁挂在汇聚层或者是串接在核心层和汇聚层之间。

[0016] VMware 是全球桌面到数据中心虚拟化解决方案的领导厂商。在虚拟化和云计算基础架构领域处于全球领先地位，所提供的经客户验证的解决方案可通过降低复杂性以及更灵活、敏捷地交付服务来提高 IT 效率。VMware 虚拟机是 VMware 公司开发的虚拟化平台。

[0017] 本发明的一种虚拟化环境下的云安全监测方法具有以下优点：进一步防止快速增长且具有动态性的网络威胁，提高云计算虚拟化环境下的整体安全性能；因而，具有很好的推广使用价值。

附图说明

[0018] 下面结合附图对本发明进一步说明。

[0019] 附图 1 为一种虚拟化环境下的云安全监测方法的一个实例的结构框图。

[0020] 图中 VM 流量重定向到安全虚拟机，即为虚拟机的流量引入到虚拟机安全软件进行检查的实例。

具体实施方式

[0021] 参照说明书附图和具体实施例对本发明的一种虚拟化环境下的云安全监测方法作以下详细地说明。

[0022] 实施例：

本发明的一种虚拟化环境下的云安全监测方法， 直接在云的服务器端的内部部署虚拟机安全软件，通过对虚拟机开放的 API 接口的利用，将所有虚拟机之间的流量交换在进入到虚拟机（简称 VM）之前，先引入到虚拟机安全软件进行检查。

[0023] 虚拟机安全软件为 VMware 开发的虚拟机安全软件。

[0024] 所述的流量指虚拟机之间的横向流量。

[0025] 虚拟机之间的横向流量安全：同一个服务器的不同虚拟机之间的流量将直接在服务器端内部实现交换，服务器端的内部部署虚拟机安全软件，通过对虚拟机开放的 API 接口的利用，将所有虚拟机之间的流量交换在进入到虚拟机之前，先引入到虚拟机安全软件进行检查。

[0026] 此时可以根据需求将不同的虚拟机划分到不同的安全域，并配置各种安全域间隔离和互访的策略。

[0027] 本发明的一种虚拟化环境下的云安全监测方法，通过虚拟机监测器和 Java 调用 C/C++ 得到资源的状态信息。

[0028] 虚拟机之间的纵向流量包括从客户端到服务器端的正常流量访问请求，以及不同虚拟机之间的三层转发的流量；纵向流量的交换必然经过云的外置的硬件安全防护层进行检查，硬件安全防护层的防护的设备类型是以防火墙和入侵防御系统等产品为主，在部署的方式上要求防火墙或入侵防御设备具备 INLINE 阻断安全攻击的能力，部署的位置可以旁挂在汇聚层或者是串接在核心层和汇聚层之间。

[0029] 本发明的一种虚拟化环境下的云安全监测方法，除说明书所述的技术特征外，均为本专业技术人员的已知技术。

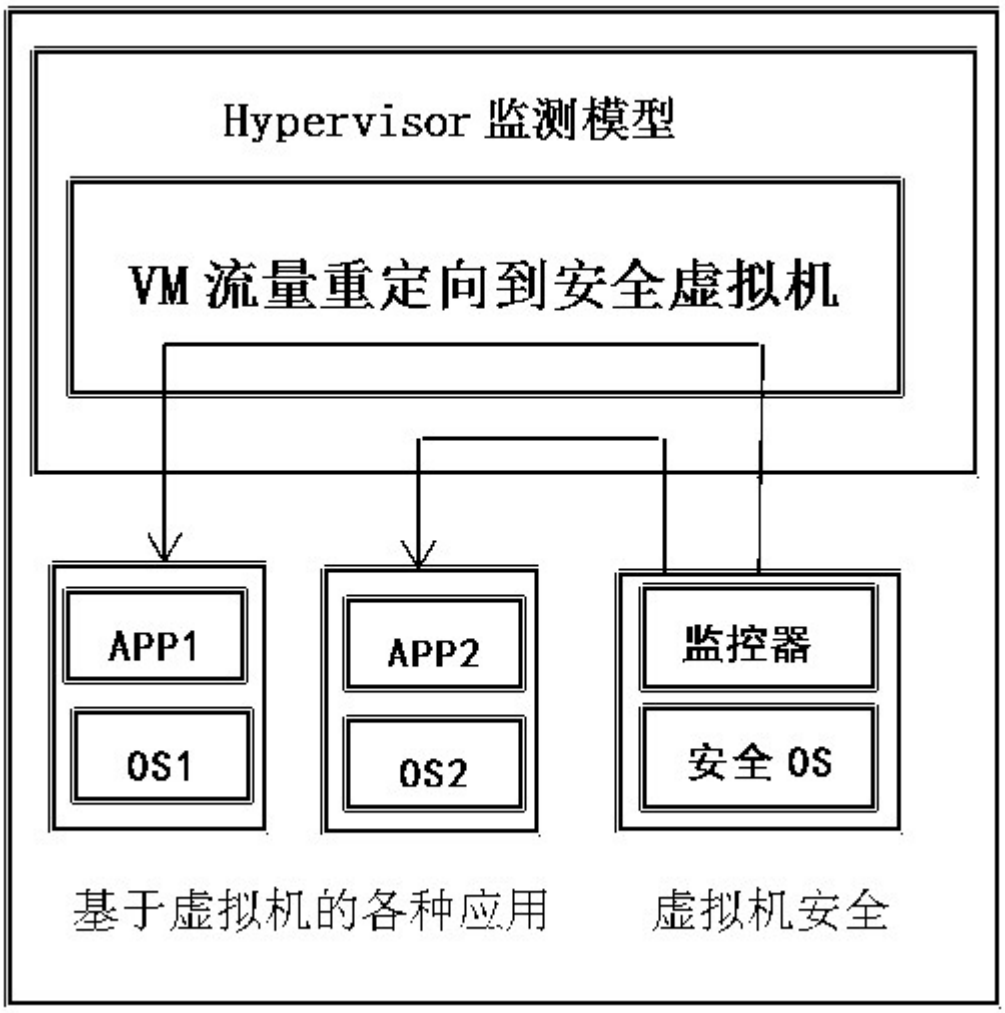

Hypervisor 监测模型
VM 流量重定向到安全虚拟机
APP1
OS1
APP2
OS2
监控器
安全 OS
基于虚拟机的各种应用
虚拟机安全

图 1