# 第5章 Hypervisor安全

## 5.1 Hypervisor安全概述

Hypervisor又称虚拟机监视器(Virtual Machine Monitor,VMM),是虚拟化的重要组成部分。Hypervisor是运行在基础物理服务器和操作系统之间的中间软件层,支持多个操作系统和应用共享一套基础物理硬件。Hypervisor可以看作虚拟环境中的元(meta)操作系统,能够协调对服务器上的所有物理设备和虚拟机的访问,并且可以非中断地支持多工作负载迁移。Hypervisor提供虚拟机之间的隔离技术,从而使得这些虚拟机可以彼此独立运行,而且可以运行不同的操作系统。Hypervisor还提供多租户的功能,从而简化了虚拟机的创建和管理。

常用的硬件虚拟化架构如图5-1所示。在此架构中,Hypervisor的作用是提供平台虚拟化。其中,平台虚拟化是通过某种方式隐藏底层物理硬件的过程,从而让多个操作系统可以透明地使用和共享它。

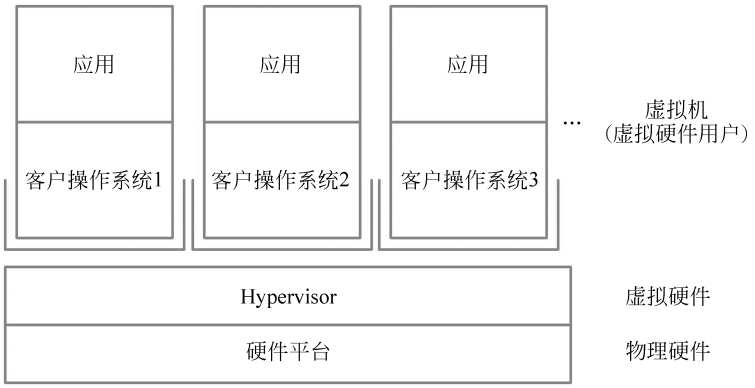


图5-1 常用硬件虚拟化架构

Hypervisor的构成如图5-2所示。可以看出,Hypervisor需要一些用于启动客户操作系统的设施,包括需要驱动的内核映射、配置(例如IP地址和所需的内存容量)、磁盘以及网络设备,还需要一组用于管理客户操作系统的工具。其中,磁盘和网络设备通常映射到计算机器的物理磁盘和网络设备。

Hypervisor需要一组用于管理客户操作系统的工具,从而使客户操作系统可以和宿主操作系统同时运行。实现这个功能需要一些特定的要素,如图5-3所示。这些要素包括:将用户应用程序和内核函数连接起来的系统调用,通常一个可用的虚拟化调用层能

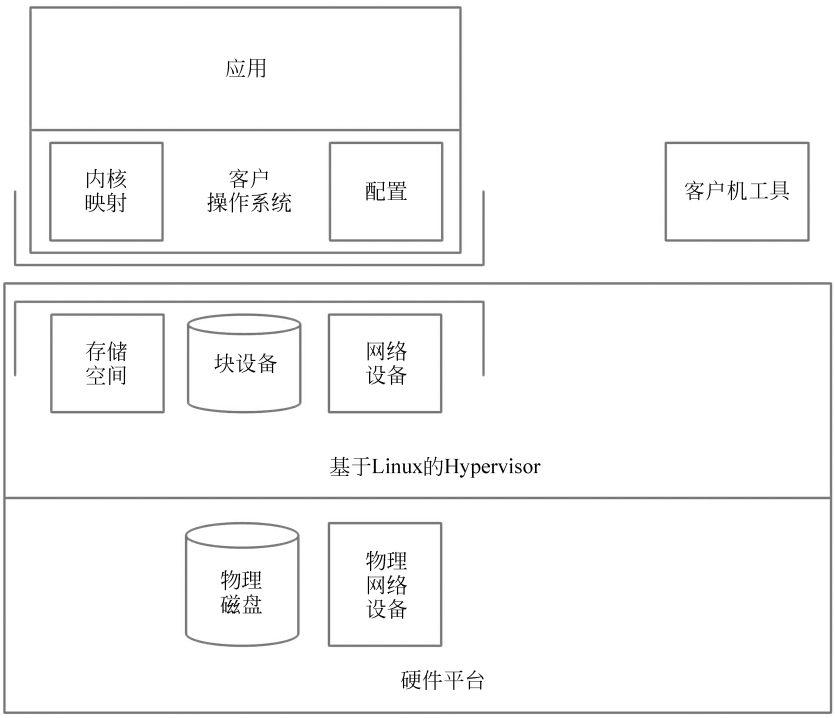


图 5-2　Hypervisor 的构成

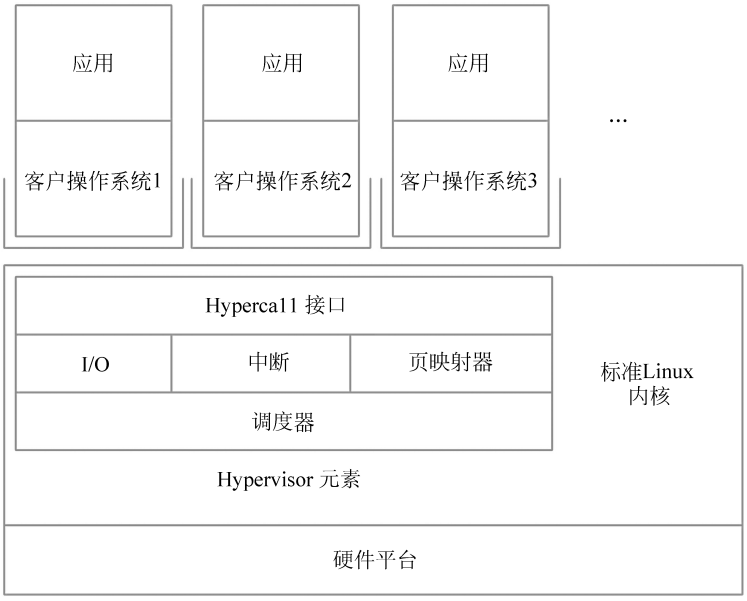


图 5-3　Hypervisor 的要素

够允许客户操作系统向宿主操作系统发出请求，例如 Hypercall，即 Hypervisor 对操作系统进行的系统调用；可以在内核中虚拟化 I/O，或通过客户操作系统的代码支持它。Hypercall 的添加是与内核相关的，所以必须修改内核代码；故障必须由 Hypervisor 来处理，或将虚拟设备故障发送给客户操作系统；Hypervisor 必须处理在客户操作系统内部发生的异常。页映射器是 Hypervisor 的核心要素之一，它将硬件指向特定操作系统（客户或 Hypervisor）的页；通过一个高级别的调度器在 Hypervisor 和客户操作系统之间进行传输控制。

根据运行位置的不同，可以将 Hypervisor 分成两类：第一类是裸机型，直接运行在物理硬件上，例如基于内核的虚拟机（Kernel-based Virtual Machine，KVM）；第二类是主机托管型，运行在具有虚拟化功能的操作系统上，例如 QEMU 和 WINE。

Hypervisor 不仅协调硬件资源的访问，而且在各个虚拟机之间施加防护。当服务器启动并执行 Hypervisor 时，它会加载所有虚拟机客户端的操作系统，同时会分配给每一台虚拟机适量的内存、CPU、网络和磁盘资源。Hypervisor 的安全性至关重要，因此大部分针对虚拟化的安全研究都是以 Hypervisor 可信为前提的。但是，Hypervisor 并非完全可信，由于其本身的代码量巨大，功能结构复杂，因此存在着许多已知和未知的安全漏洞。

目前已发现 CNware、FusionSphere、CAS 等主流的虚拟化软件都有十多种安全漏洞。另外，针对 Hypervisor 的恶意攻击也层出不穷，例如虚拟机跳跃、虚拟机移植攻击、虚拟机逃逸等。Hypervisor 上承载着大量的虚拟机，一旦被攻陷，则会使得所有受 Hypervisor 管辖的虚拟机都可能遭受非授权访问，严重危害 Hypervisor 本身以及各租户的安全。因此，保障 Hypervisor 的安全是增强虚拟化平台安全性的重要内容。

## 5.2 Hypervisor 安全保障

维护 Hypervisor 安全是每个数据中心的首要任务。因为一台单主机服务器可能要处理几十个虚拟化的工作负载。单主机上的安全漏洞可能导致断电。不幸的是，目前还没有一个独立的、综合的安全解决方案可以确保数据中心的安全。因此，要保证 Hypervisor 的高安全性，需要从多方面考虑。针对 Hypervisor 的安全保障主要分为两个方面，包括 Hypervisor 自身安全性的提高以及 Hypervisor 防护能力的提高。接下来将对这两个方面进行详细介绍。

### 5.2.1 Hypervisor 安全性

为提高 Hypervisor 的安全性和可信性，在 Hypervisor 自身的安全保障方面，应该建立轻量级 Hypervisor，并采用可信计算技术中的完整性度量和完整性验证对 Hypervisor 进行完整性保护。当然，这两个方面在技术实现上都存在着一定的难度，在大规模的虚拟化部署和防护中不太适用。下面对这两方面进行介绍。

**1. 建立轻量级 Hypervisor**

随着 Hypervisor 功能的增加，其本身的代码量越来越大，结构越来越复杂，体积也越

来越大，这些都降低了 Hypervisor 的可信性。而作为虚拟化体系中上层虚拟机应用程序重要组成部分的可信计算基(Trusted Computing Base，TCB)，如果 Hypervisor 的可信性无法得到保证，那么应用程序运行环境的安全性将无法得到保证。为了解决这个问题，近年来虚拟化研究领域的专家学者致力于轻量级 Hypervisor 的构建，并取得了许多研究成果。构建轻量级的 Hypervisor，主要是通过减小可信计算基来实现，这种方法借鉴了微内核的思想，在最小程度上控制了 Hypervisor 的攻击面。TCB 指的是构成通用安全计算机系统所有安全保护装置的组合体。TCB 也叫作安全子系统，它包含了操作系统的安全内核、处理敏感信息的程序、实施安全策略的软件和硬件、具有特权的程序和命令、负责系统管理的人员等，其自身具有高度的可靠性，可以为整个系统提供安全保障，是上层应用程序安全运行的基础性保证。但是，随着 TCB 代码量越来越大，功能和结构越来越复杂，其存在安全漏洞的可能性也就越来越大，这样它自身的可靠性就无法得到保障，因此要尽量减小 TCB。由此可见，设计轻量级 Hypervisor 时，应尽量降低实现的复杂度，使其尽可能简单，保证其只实现底层硬件抽象接口的功能，这样才能更容易保证 Hypervisor 自身的安全性和可信性。

要构建轻量级 Hypervisor，可以采用轻量的虚拟化架构，为具有较高安全需求的虚拟机应用提供更好的隔离性，也可以通过简化功能来解决 Hypervisor 代码量巨大的问题，另外，还应该提升虚拟机中 I/O 操作的安全性。目前，构建轻量级 Hypervisor 的方法主要是：构建专用 Hypervisor，或者将 Hypervisor 的管理功能和安全功能分开，以减小 Hypervisor 的大小。但是，如何在功能分离开后仍保持 Hypervisor 的特性和功能，仍然是专家学者正在进一步研究的一个难点。

**2. 保护 Hypervisor 的完整性**

Hypervisor 的完整性保护包括完整性度量和完整性验证这两个部分。其中，完整性度量从计算机系统的一个名为可信度量根的硬件安全芯片开始，到硬件平台，再到操作系统，最后到应用，在程序执行之前，由前一个程序来度量该级程序的完整性，并将度量的结果通过可信平台模块(Trusted Platform Module，TPM)提供的扩展操作记录到 TPM 的平台配置寄存器中，最终构建一条可信启动的信任链。完整性验证是对完整性度量报告进行数字签名后发送给远程验证方，再由远程验证方来判断该 Hypervisor 是否安全可行。

目前，对 Hypervisor 完整性保护的研究有很多，比较典型的成果有：Hypervisor 提供运行时控制流完整性保证，阻止恶意软件在 Hypervisor 运行过程中执行的 Hypersafe 架构，采用独立于 Hypervisor 的软件组秘密对 Hypervisor 进行实时完整性度量的 HyperSentry 架构，基于硬件辅助的用于保证 Hypervisor 完整性的探测篡改框架 HyperCheck，等等。这些方法目前是比较流行的，因为它们不仅部署容易，而且不影响 Hypervisor 的任何能力。

### 5.2.2 Hypervisor 防御方法

为保护 Hypervisor 的安全，既要提高 Hypervisor 自身的安全性，又要增强

Hypervisor 的防御能力。常见的集中防御方法包括合理分配主机资源、扩大 Hypervisor 的安全范围至远程控制台、安装虚拟防火墙以及限制用户特权等，下面对这几种防御方法进行介绍。

### 1. 合理分配主机资源

如果物理主机没有采取相应的措施对主机资源的使用情况进行管理，那么，由于在默认条件下，所有虚拟机对物理主机提供的资源都有同样的使用权利，因此可能会有恶意攻击者利用这一点发起类似于物理服务器的拒绝服务攻击，恶意的虚拟机会占据主机的有限资源，从而导致其他虚拟机因资源匮乏而崩溃，运行在这些虚拟机上的服务也被迫中断。由此可见，Hypervisor 应该采取合理的措施对主机资源进行分配和控制。具体来说，可以采取限制、预约等机制，让重要的虚拟机能够优先访问主机资源。另外，还可以划分主机资源并隔离成不同的资源池，然后将其上的虚拟机分配到不同的资源池中，并规定每台虚拟机只能使用其在资源池中分配到的资源，这样可以有效降低恶意虚拟机占据主机所有资源而引起虚拟机拒绝服务的风险。

### 2. 扩大 Hypervisor 安全范围至远程控制台

虚拟机的远程控制台可以使用远程访问技术来启用、禁用和配置虚拟机，因此，一旦虚拟机的远程控制台配置不当，就会给 Hypervisor 带来很大的安全隐患。例如，虚拟机的远程控制台往往允许多人同时连接，如果一个具有较高权限的用户先登录了远程控制台，随后一个具有较低权限的用户也登录了远程控制台，那么后者就可以获得第一个用户所具备的较高权限，从而导致越权访问。另外，用户可以在本地计算机操作系统和远程虚拟机操作系统之间进行内容的复制和粘贴，这样，所有通过远程控制台连接到虚拟机的用户都可以使用剪贴板上的信息，从而造成信息泄露。

为了规避上述风险，必须将 Hypervisor 的安全范围扩大至远程控制台，规范远程控制台的使用，增强 Hypervisor 的安全性。首先，应当规定在同一时刻只允许一个用户访问虚拟机远程控制台，并且按需分配权限，这样可以防止多用户登录造成具有较低权限的用户越权访问其他用户的敏感信息的情况。其次，应该禁止连接到虚拟机的远程管理控制台的复制和粘贴，以避免信息泄露。

### 3. 安装虚拟防火墙

虚拟机之间的流量在同一个虚拟交换机和端口组上传输的时候，网络的流量不会经过物理网络，只在物理主机内部的虚拟网络中存在，而物理防火墙只为连接到物理网络中的服务器和设备提供服务，因此这些网络流量都在物理防火墙的保护区域之外，物理防火墙无法保证这些流量的安全。为保护 Hypervisor 的安全，需要安装虚拟防火墙，它能在虚拟机的虚拟网卡层获取并查看网络流量，因此能够监控和过滤虚拟机之间的流量。为确保网络流量的安全，可以将虚拟防火墙与物理防火墙配合使用。

### 4. 限制用户特权

为简化访问授权这一环节，许多 Hypervisor 的管理人员往往会直接将管理员的权限分配给用户，这样，一些恶意用户可能会利用管理员权限执行各种危险操作，包括窃取数

据、更改网络配置、重新配置虚拟机、更改用户权限等，从而严重破坏 Hypervisor 的安全。为应对这些安全风险，必须对用户进行细粒度的权限分配。具体来说，应该在最初创建用户角色的时候先不给该角色分配任何权限，在将角色分配给用户时，再根据用户的需求增加相应的权限，这样可以保证用户只获取其申请的权限，从而避免用户因享有管理员特权而给 Hypervisor 带来安全隐患。

## 5.3 安全策略

Hypervisor 向下需要对基本硬件设施进行抽象和管理，向上则需要集中管理所有运行在其上的虚拟机，并需要负责管理这些虚拟机的资源分配、资源访问以及运行维护。因此，Hypervisor 作为虚拟化的重要组成部分，提高其安全性，能够为运行于其上的虚拟机提供有效的安全保障，进而增强虚拟化平台的安全防护能力。下面介绍虚拟机安全监控机制和虚拟机间流量安全防护这两种策略。

### 5.3.1 虚拟机安全监控机制

在云计算环境中，要保证虚拟机的运行安全，需要部署有效的监控机制对虚拟机的运行状态进行实时观察，及时发现危害虚拟机运行安全的因素并迅速作出响应。然而，虚拟化平台的应用给云计算带来了不小的安全挑战，云应用不再受企业内部防火墙和入侵检测系统的保护，传统的安全监控机制也已经不再适用，亟须提出针对虚拟机的安全监控机制。

近年来，虚拟化研究领域的专家学者都在致力于虚拟机安全监控架构的研究。所谓虚拟机安全监控架构，指的是安全工具为适应虚拟计算环境而采取的架构模式。目前比较流行的虚拟机安全监控架构主要是虚拟机自省监控框架以及基于虚拟化的安全主动监控框架。

#### 1. 虚拟机自省监控框架

虚拟机自省是从虚拟机外部获取客户虚拟机操作系统内部状态信息的技术。通过将安全工具放在单独的虚拟机中来实现该框架，并利用该安全工具对其他虚拟机进行安全检测，该框架的典型代表是 Livewire。采用虚拟机自省监控框架的安全监控系统有 Wizard 和 Xenacces。Wizard 是一个基于 Xen 的内核监控器，它能发现高级的内核事件以及低级的硬件设备事件之间的关系，具备安全、高效截获应用级和操作系统级行为的能力。Xenacces 是一种处于 Xen 管理域中的虚拟机监控库，它的实现依赖于 Xen 提供的 libxc 和 libblktap 库。Xenacces 为目标虚拟机内存和磁盘的查看提供高级接口，但它必须在操作系统内核完整的情况下才能提供安全监控功能，一旦有恶意攻击者篡改了操作系统内核的关键数据结构，则会致使 Xenacces 的安全监测功能失效。

#### 2. 基于虚拟化的安全主动监控框架

该框架通过安全资源池的虚拟安全能力或者在租户网络内部署虚拟安全能力两种方式提供安全服务，包括系统漏扫、配置基线核查和 Web 漏洞扫描等，只需安全能力与扫描

对象网络可达，即可扫描租户虚拟机的配置和漏洞情况，并根据扫描结果提供相应建议。在实现时，将安全工具部署到一个处在安全域的虚拟机中，并利用该安全工具对运行在目标虚拟机上的操作系统进行安全监测。

目前，虚拟化安全监控主要可以分为内部监控和外部监控两种。内部监控通过在虚拟机中加载内核模块来对虚拟机中的内部事件进行拦截。所谓事件拦截，指的是拦截虚拟机中发生的某个事件，从而触发安全工具对其进行安全检测，而虚拟机中内核模块的安全则需要由 Hypervisor 来保护。内部监控的典型系统是 Lares 和 SIM。外部监控是在虚拟机外部进行安全检测，它指的是在 Hypervisor 中对目标虚拟机中的事件进行拦截，其典型系统是 Livewire。下面分别对这两种监控方式进行介绍。

### 1. 内部监控

内部监控模型如图 5-4 所示。在基于虚拟化的内部监控模型中，安全工具部署在一个被隔离的且处于安全域的虚拟机中，该虚拟机所处的环境在理论上被认为是安全的。被监控的客户操作系统运行在目标虚拟机中，该目标虚拟机中会部署一个用于拦截文件读写、进程创建等事件的重要工具——钩子函数，其典型代表是 lares 和 sim，可以直接截取系统级语义。这些钩子函数在加载到客户操作系统中时，会通知 Hypervisor 它们所占据的内存空间，这样 Hypervisor 中的内存保护模块就可以根据钩子函数所告知的内存页面对其进行保护，从而为存在于不可信的客户操作系统中的钩子函数提供安全保护。除了内存保护模块，Hypervisor 中还有一个跳转模块，它的作用是为目标虚拟机和安全域之间的通信搭建桥梁。钩子函数和跳转模块都必须是简单的、自包含的，不能调用内核的其他函数，这样内存保护模块才能更好地保护它们，防止它们被恶意攻击者篡改。

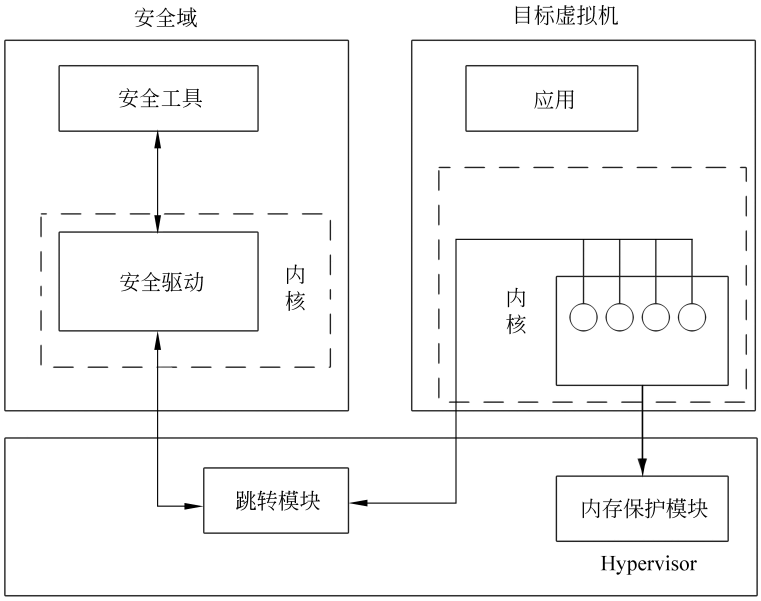


图 5-4　内部监控模型

在进行一次事件拦截响应的过程中，内部监控模型中的钩子函数在探测到目标虚拟

机中发生了某个事件时会主动陷入 Hypervisor 中，并通过其中的跳转模块将目标虚拟机中发生的事件传递给安全域中的安全驱动，再由安全驱动将事件传递给安全工具；之后，安全事件会根据目标虚拟中发生的事件执行某种安全策略，产生响应，并将响应传递给安全驱动，进而对目标虚拟机中的安全事件作出响应。

由上面的内容可以看到，内部监控模型可以在虚拟机中实现事件截获，因此可以直接获取操作系统级语义而不需要进行语义重构，从而减少了性能开销。语义重构指的是由低级的二进制语义重构出高级的操作系统语义。另外，该模型中的安全工具和客户操作系统相互隔离，可以增强安全工具的安全性。但与此同时，该模型需要在客户操作系统中植入内核模块，这会使得目标虚拟机的监控缺乏透明性。另外，该模型中的跳转模块以及内存保护模块都不具有通用性，需要根据目标虚拟机来进行特殊设计，这会限制内部监控框架的进一步研究和使用。

**2. 外部监控**

外部监控模型如图 5-5 所示。与内部监控模型相同的是，外部监控模型中的安全工具和客户操作系统位于两个彼此分离的虚拟机中，而不同点在于外部监控模型在 Hypervisor 中部署了监控点，该监控点不仅为目标虚拟机与安全域中的安全工具建立通信桥梁，还可以用于拦截目标虚拟机中发生的安全事件，并能重构出高级语义，传递给安全工具。其中，语义重构的过程与客户操作系统的版本和类型密切相关，主要是利用某些内存地址或寄存器对内核中的关键数据结构进行解析。安全工具会根据安全策略对目标虚拟机中的事件作出响应，进而通过监控点来控制目标虚拟机。由于监控点部署在处于目标虚拟机底层的 Hypervisor 中，所以它能观测到目标虚拟机的 CPU 信息、内存页面等状态信息，从而协助安全工具对目标虚拟机进行较为全面的检测。

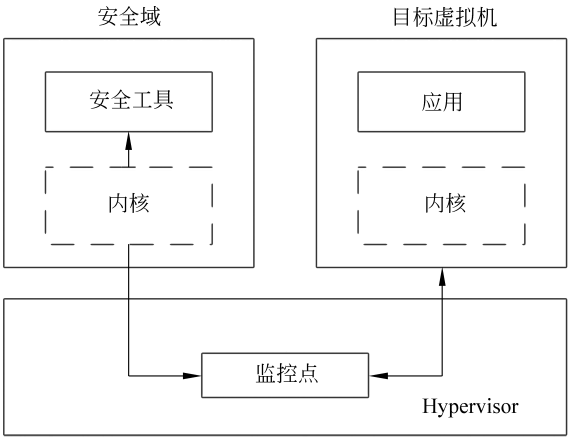


图 5-5　外部监控模型

由上面的内容可以看到，内部监控和外部监控这两种监控方式都能很好地实现对虚拟机的安全监控。但是，虚拟机监控仍然存在着一些不足的地方需要继续改进。

首先需要改进的问题是缺乏通用性，目前的监控系统都是针对特定类型的客户操作系统来实现特定的安全功能，而在云计算环境下，单个物理节点上往往有多台虚拟机，虚

拟机中的客户操作系统又种类繁多，因此监控工具很难有效地对云计算环境下各种不同类型的虚拟机进行监控。要满足监控的通用性需求，构建通用的安全监控机制十分必要。

其次，虚拟机监控与传统的安全工具还存在着融合的问题。在虚拟化环境下，利用 Hypervisor 可以更好地监控虚拟机内部的运行状态，因此，现有的工作多集中在通过 Hypervisor 来保护目标虚拟机中的钩子函数或者从目标虚拟机外部查看内部状态，然而传统的安全工具无法直接使用 Hypervisor 获取的包含二进制语义的信息。为解决虚拟监控工具和传统安全工具的融合问题，一方面应该利用语义恢复来实现从二进制级语义到系统级语义的转变，并且为安全工具提供标准的调用接口。另一方面应该考虑如何在语义的全面性和语义恢复给安全工具带来的额外性能开销之间进行综合权衡，从而让安全工具发挥最大的实用价值。

### 5.3.2　虚拟机间流量安全防护

在虚拟化环境下，同一个服务器上不同虚拟机之间的流量交换是通过服务器内部的虚拟交换网络进行的，虽然这些虚拟机可能处于同一个物理无线局域网（Wireless Local Area Network，WLAN）下，但流量却不需要经过外部交换机。在这种情况下，虚拟机之间的流量交换是不可视的，虚拟化平台的管理人员无法了解和控制虚拟机之间的流量交换。这会带来各种安全隐患，例如，这些虚拟机之间的二层流量在规则允许的范围内是否是合法访问，不同虚拟机间交换的流量中是否存在诸如针对应用层安全漏洞的网络攻击行为，等等。由此可见，对虚拟机间流量进行安全防护是非常重要的。

通常来说，根据流量的转发路径可以将用户的流量分为纵向流量和横向流量两类，因此可以从纵向和横向两个维度采取相应的措施来对虚拟机间的流量进行安全防护。

#### 1. 纵向流量的安全防护

纵向流量包括从客户端到服务器的访问请求流量以及不同虚拟机间三层转发的流量，这些流量的交换都需要经过外置的硬件安全防护层。纵向流量的安全防护与传统数据中心流量的安全防护类似，因此针对纵向流量的安全防护可以借鉴传统的安全防护部署方式，将具备内置阻断安全攻击能力的防火墙和入侵检测系统旁挂在汇聚层，或串接在核心层和汇聚层之间，利用其对虚拟化环境下的纵向流量进行检测。

#### 2. 横向流量的安全防护

横向流量指的是同一台服务器上不同虚拟机之间交换的流量。在虚拟化环境下，同一台服务器上不同虚拟机间的流量直接在服务器内部进行交换，而不需要经过外部物理交换机，且其交换过程是不可视的，因此外层网络的安全管理人员无法通过传统的安全防护与检测技术对虚拟机中的横向流量进行监控和安全防护，横向流量安全成为虚拟化环境下的一个新问题。

目前许多业内专家学者都在加紧研究横向流量的安全防护措施，其中包括在虚拟计算平台上的 Hypervisor 层集成 vSwitch 虚拟交换机，通过该交换机能够实现一些基本的访问控制规则，但是由于不能集成高级的安全防护和检测工具，因而无法实现对虚拟机之间横向流量的安全检测。目前针对横向流量的安全检测技术主要是基于虚拟机的安全防

护技术和利用边缘虚拟桥接(Edge Virtual Bridging,EVB)等技术实现的流量重定向安全防护技术,下面对它们进行介绍。

1) 基于虚拟机的安全防护技术

为解决外部防火墙和入侵检测系统无法对虚拟机之间交换的流量进行安全检测的问题,基于虚拟机的安全防护技术可以直接在服务内部部署虚拟机安全软件,并在所有虚拟机之间的流量交换未进入虚拟机中的交换机前,利用 Hypervisor 开放的 API 将这些流量引入虚拟机安全软件中进行安全检测。虚拟机安全软件会根据需求将不同的虚拟机划分到不同的安全域中,并对各种安全域间的隔离和访问策略进行配置。为检测虚拟机间相互交换的流量中是否存在类似于应用层安全漏洞的网络攻击,该技术还可以通过在软件中集成了入侵防御系统(Intrusion Prevention System,IPS)的深度报文检测技术对流量进行检测。

应用基于虚拟机的安全防护技术的典型例子是在前面提到的外部安全监控框架 Livewire,它是一个基于虚拟机的入侵检测系统。该框架将入侵检测系统部署在一个与被检测虚拟机相互隔离的安全虚拟机中,然后利用虚拟机的自省机制,通过 Hypervisor 来观察目标虚拟机的内部状态,观察的内容还包括该虚拟机与其他虚拟机之间的横向流量。当检测到系统中发生的事件时就将其拦截。Hypervisor 会通过直接访问被检测系统的内存来获取该系统的当前状态,然后利用入侵检测系统的操作系统接口库来恢复出操作系统级的语义,接着再通过入侵检测模块对发生的事件进行安全检测。

基于虚拟机的安全防护技术的一个优势是部署简单,只要在服务器上专门开辟出资源来运行一个隔离的虚拟机,并在该虚拟机中运行虚拟机软件就可以了。但从另一个角度来说,由于每个服务器都需要专门分配一定的资源为虚拟机提供运行环境,因此一旦服务器的流量增大,开启的 IPS 深度检测的功能增多,则其对系统资源的占用将增大,这可能会影响服务器的性能,服务器的投资也可能会随之增加。另外,该模型需要安全软件生产商在 Hypervisor 层进行代码开发,因此低质量的开发可能会给 Hypervisor 带来潜在的安全漏洞,从而给整个系统的正常运转带来安全风险。

2) 流量重定向安全防护技术

流量重定向安全防护技术利用边缘虚拟桥接和虚拟以太网端口汇聚器(Virtual Ethernet Port Aggregator,VEPA)等技术将虚拟机的内部流量引入外部交换机中,并在外部交换机转发这些流量前,通过镜像或重定向等技术将流量引入安全设备中进行安全检测,还有各种安全策略或访问策略的配置。边缘虚拟桥接技术是 IEEE 针对数据中心虚拟化制定的一组技术标准,它包含了虚拟化服务器与网络间数据互通的格式与转发要求以及针对虚拟机和虚拟 I/O 通道对接网络的一组控制管理协议。该技术主要有两个作用,一个是解决计算资源调度与网络自动化感知之间无法连接的问题,另一个是解决服务器虚拟化后计算资源与网络资源之间产生的管理边界模糊问题。虚拟以太网端口汇聚器技术的功能是将服务器上的虚拟机生成的所有流量转移到外部的网络交换机上。

流量重定向安全防护技术的一个特点是将硬件设备外置,它可以在不影响服务器的业务部署且不占用服务器资源的情况下利用数目较少的高端安全设备来实现万兆级甚至是十万兆级的安全检测,而这些外置的安全设备可以由管理员利用其丰富的传统信息系