虚拟化安全手册

虚拟化安全手册

虚拟化是一个广义的术语，是指计算元件在虚拟的基础上而不是真实的基础上运行，是一个为了简化管理，优化资源的解决方案，这种方案在 IT 领域就叫做虚拟化技术。虚拟化技术能集中并共享资源，降低成本、优化利用率，正因为有这些优势，未来企业在 IT 基础架构建设中，将侧重于建设领先的虚拟化 IT 环境。同时在云计算的发展过程中，虚拟化也将扮演重要支撑角色。但是，虚拟化环境面临着不同于过去物理环境的安全问题，企业要想建立一个可靠的虚拟化环境，必须重视虚拟化安全问题。

本技术手册将从三个方面，为你详细介绍虚拟化安全挑战，并提供解决策略和方法。

虚拟化环境面临的安全问题

虚拟化技术改变了服务器和数据中心的定义。与物理上独立的、通过网络联接的服务（可以认为这些服务器是安全的，且可以监测的）相比，虚拟环境是一个“装在盒子中”的隔离的、自成体系的数据中心，以往通过网络进行的进程间的通信现在只发生在一个 IT 部件中，毫无疑问，安全问题的影响是非常重要的。那么究竟都有哪些问题呢？

- ❖虚拟化安全未知问题
- ❖虚拟化挑战传统安全概念

如何看待虚拟化安全问题

许多公司都已经配置了虚拟化架构来降低成本，提高效率，但是虚拟化方面的安全专家表示，这些公司应该再次评估他们的安全措施，从而解决这一技术所造成的缺陷。企业应该从哪些方面来评估虚拟化安全，厂商们又做了哪些努力呢？

- 减少虚拟化安全风险需要物理的视角
- 虚拟化不再是网络安全黑洞
- 安全厂商致力于解决虚拟化安全的性能问题

实现虚拟化安全的技术策略

认识了虚拟化环境面临的安全问题，具备了看待虚拟化安全问题的视角，本部分我们就具体介绍解决虚拟化安全问题的策略和方法。包括如何在虚拟化环境中实施 IDS/IPS，vShield Endpoint 和 Edge 功能，在哪里安置防火墙连接等等。

- 如何应对层出不穷的虚拟化安全问题？
- 虚拟化技术的安全：IDS/IPS 实施策略
- 虚拟化安全：vShield Endpoint 和 Edge 功能
- VMware JRE 中的漏洞是否会妨碍虚拟化的实施
- 虚拟化安全问题：在哪里安置防火墙连接？
- 实现虚拟化安全的新方法

虚拟化安全未知问题

虚拟化技术正在数据中心这一领域风靡，有其必然原因。典型的服务器其利用率不足40%，虚拟化技术有助于更高效的利用技术资源，并可大幅度降低费用。从EMC公司的VMware业务和其他一些虚拟化平台业务的扩展来看，这一技术很显然正处于快速发展阶段。

通常情况下，安全性问题只是满足需求之后才考虑的问题，这存在很大的问题。虚拟化技术改变了服务器和数据中心的定义。与物理上独立的、通过网络联接的服务（可以认为这些服务器是安全的，且可以监测的）相比，虚拟环境是一个“装在盒子中”的隔离的、自成体系的数据中心，以往通过网络进行的进程间的通信现在只发生在一个IT部件中，毫无疑问，安全问题的影响是非常重要的。

实际上，虚拟化技术会在多大程度上影响工业界在过去15年为系统和应用构筑的安全措施还不清楚。为了把握这些情况，了解虚拟化世界中安全功能的特别之处很重要。

更明确的说，还不可能准确地描述出虚拟化技术所面临的最重要的安全性挑战是什么，但是可以从以下几个关键点进行考虑。

网络防御变得不再具有实际意义。大多数网络安全防御技术都基于监测数据流，将数据包或其行为与已知的恶意数据包进行比较，然后采取行动。如果不能监测数据流，则需要在虚拟服务器内实现一种基于网络的防御方法。换句话说，监测进程间的通信，这些进程间的通信发生在虚拟机中或是发生在不同物理设备上的虚拟设施之间。

在虚拟化的世界中，网络的定义有很大的不同，且需要不同的防御措施。不管这一问题结果如何，Blue Lane Technologies公司和Reflex Security公司这两家厂商已着手研究这一问题。

管理程序对于防御攻击来讲太重要了。每个人都在议论操作系统是多么的不安全。的确，所有的操作系统都是不安全的，一组可能有潜在安全问题的操作系统运行在一个有潜在安全问题的管理程序之上，会使这一安全问题变得更为复杂。

对于不熟悉虚拟化技术的人来讲，管理程序可以理解为计算机硬件与运行在其上的操作系统之间的一个软件抽象层。它是一个软件，和其他我们知道的大部分软件一样，它非常易受攻

击。问题是：易受攻击的程度如何？它的栈很高；如果处于底层的管理程序受到威胁，很可能也会威胁到运行在它上面的所有虚拟机。

如果管理程序确实易受攻击，那就如同浮沙之上筑高楼。普通人，不必是结构工程师，也能说出这将导致什么样的后果。

配置管理的困难。当每个物理服务器上安装了 5 个、10 个或 100 个虚拟设备时，就会给现有的配置管理设施增加许多的压力。例如，管理 5000 个运行不同操作系统的虚拟镜像几乎是不可能的。当今的配置管理提供的功能在规模（和有效性）方面必须增加一个量级才能适用于虚拟环境。

保持业务连续是一个挑战。许多机构使用独立的服务器，并在必要情况下切换到备份系统中。关键任务中的应用，由于工作中断代价非常高，这种做法是合适的。但如果这些关键的应用部署在虚拟空间中，则应改进为保持业务的连续性所做的规划，将虚拟环境这一因素考虑在内。

正如“what's old is now again”（过去场面再次出现）所述，这是一个已经解决了的问题。大型主机操作系统在过去遇到过这个问题。但是，仅仅是人们过去遇到过这个问题并可以找到一个参考，并不意味着这一问题在新的环境中已经接近解决。

软件的商业模式必须改变。很多种软件，特别是管理软件，以被管理的设备数目为标准收取费用，但在虚拟世界中，被管理的设备又如何定义呢？是不是建立每一个虚拟镜像都要付费？当删除一个镜像时是不是也要留下记录？我不知如何回答这些问题，但我可以说的是现有的定价模式是不够的。

我们将会看到，由于虚拟技术的推广会出现新的软件定价模式。

也许会有解决这些问题的初步方案。我知道有很多的聪明人士提出一些想法，并将新的产品推向市场以解决这些问题。

但是，在列举出所有的关键问题之前，与公司中管理数据中心的员工合作提出具体环境中的虚拟设备的安全规划是非常重要的。通向虚拟化的道路非常有趣--这种感觉有点像刚刚走下过山车之后的眩晕感。

（作者：Mike Rothman　译者：陈志辉　来源：TechTarget 中国）

虚拟化挑战传统安全概念

毫无疑问你会听到有人怀疑传统的安全控制在虚拟环境中的作用。尽管不确定是否有相关的新技术，还是有很多改善安全的方法，可以使攻击者窃取敏感数据变得更困难。

虚拟化向 IT 行业提供对传统安全概念和更有价值的保护业务架构的有力挑战的机会。这些安全方面的好处可以从 IT 行业对于应用环境配置、漏洞管理的更简单的程序以及把原始的应用图像向企业的所有端点的快速传送等的更强大的控制上实现。

虚拟环境还将面临攻击，但是这些攻击将不只简单地存在于应用环境中，还将在渗透入企业环境中存在更大的困难。在本质上，业务应用的攻击界面充分地降低到了虚拟机——操作系统、可执行应用和配置轮廓——所管理的。

挑战传统的安全方法的第一步是认识到所有的计算机系统都总是处于被恶意攻击的风险之中。没有任何适当的安全技术可以保证技术架构的完全安全。虚拟系统对化妆成授权软件来窃取数据或者修改配置中端业务的攻击比非虚拟系统并不具有更大的免疫力。虚拟化厂商在保护管理程序、执行 VM 的完整性检查的证明以及检测新型攻击方面的友好表示是使这个架构尽可能安全方面正在付出的很重要的努力。IT 行业的机会是利用虚拟化改变商业上的交付应用的方式，以及改变保护商业的方式。

下面是 IT 企业利用虚拟化提供更安全的商业环境的例子：

- 一家主要的金融企业正在参与到保护可以被远程电脑获取的客户数据。采用的解决方案是使数据中心的敏感应用虚拟化。因为在这这种虚拟的解决方案中，机密数据从来不离开安全的数据中心，公司就不用太担心数据泄露。企业没有采用严格的端点安全软件，而是使用了虚拟化来避免客户数据被远程收集的问题。
- 一个地区的能源公共事业需要保证控制系统的持续的正常运行时间。这种公共事业利用虚拟架构有规律的在数据中心轮换控制系统，每天更新关键的虚拟机（VM）。这种简单方法在安全方面的好处之一是对 VM 的成功攻击的时间不会超过 VM 更新的周期——当 VM 终止的时候攻击也会终止。其他的好处是公共事业可以有效地进行灾难恢复，来减轻对控制系统攻击的影响。

- 国家服务机构已经使用虚拟化更好地进行远程应用的漏洞管理。机构已经认识到通过在向远程站点发送之前在采用软件更新、补丁、配置管理和对数据中心中的虚拟机的安全扫描收到的管理精力上的节约。IT 提高了应用环境的控制，并可以迅速把新版发送的整个企业。

存在挑战的方面是 IT 必须考虑虚拟架构如何在提高应用能力的同时帮助避免常见的安全问题。虽然安全和虚拟厂商继续生产对攻击弹力更大的产品，但是 IT 也可以使用虚拟化大幅改变攻击表面，使商业受益。

(作者：Eric Ogren 译者：Tina Guo 来源：TechTarget 中国)

减少虚拟化安全风险需要物理的视角

许多公司都已经配置了虚拟化架构来降低成本，提高效率，但是虚拟化方面的安全专家表示，这些公司应该再次评估他们的安全措施，从而解决这一技术所造成的缺陷。

像过去一样，当采用物理架构和系统来满足商业需求时，在许多早期虚拟化配置中安全需求一般被放在次要位置，Dave Shackleford 说道（Shackleford 是 Voodoo Security 公司的创始人兼首席顾问，该公司的总部位于亚特兰大）。但好的消息是，用于防御物理系统免受攻击的策略可以用于解决虚拟化安全风险，Shackleford 表示。

“你仍然需要监测网络流量，同时还需要解决一些配置和补丁管理方面的问题。”Shackleford 说，“从网络的角度来看，真正的改变仅仅是你现在可以通过同一个通道传输更多的流量。”

虚拟化打破了物理系统的界限，将网络转化成了各种配置和内存中的快照文件。该技术使用一个管理程序，使得硬件可以支持多个系统在一个物理平台上同时运行。Shackleford 称虚拟化平台具有“令人难以置信的适应性”。推出这些平台的公司有 VMware、Citrix Systems 和 Microsoft 等厂商，并不断的对其漏洞进行修补。

这些对虚拟系统的威胁，比如：利用管理程序和其他组件发起的攻击，目前已得到了相关的概念验证，Shackleford 说道。研究人员已经记录了侵入一个虚拟服务器并拥有一个虚拟机的复杂方法，不过至今利用虚拟机来攻击的风险还是很低的。事实上，最新的 Verizon 数据泄漏调查报告显示：所有这些被调查的泄漏案件中——超过了 923 个独立案件——没有一个是涉及利用管理程序来允许攻击者越过虚拟机的。

除了被记录的所有复杂的攻击外，Shackleford 相信攻击者更有可能选择破坏用于支持虚拟机的管理基础设施。他说，许多公司都不能将管理基础设施从虚拟网络的其余部分中完全分隔出来。这个漏洞可以是网络犯罪分子用来获得敏感数据的攻击向量。

“你必须确保管理基础设施不仅仅集中在你的生产流量的其余部分，”他说，“这需要额外的工作，但在大多数情况下，人们不愿再这上面花时间。”

Shackleford 是一位经认证的 SANS 研究所讲师，他正在改进由该组织举办的虚拟化培训，该培训的目的是围绕具体的最佳策略拓展其范围。他说，各组织应该评估他们的物理安全设备和系统，看其是否能够在虚拟基础架构上工作。一些传统的方法，比如：隔离包含敏感数据的系统，确保管理团队职责分离，保护管理层不受内部和外部的攻击等等，都应该被采用。另外，安全厂商正在针对虚拟化环境优化它们的产品。

Andy Ellis 是 Akamai Technologies 公司的信息安全高级主管和首席安全架构师，他说他的公司在虚拟服务器上运行基于 Java 的计算环境。Akamai 的客户端在这个环境下运行面向用户的网络应用程序，比如：一个网站组件可以用来寻找一个零售地点或者寻找让网站访问者可以按需求定制产品的配置工具。Ellis 说，这个环境建立起来后，Akamai 可以在需要的时候向基于 Java 的网络应用程序传送计算能力。

为了提供安全性，Ellis 的团队将应用程序以及每个单独的虚拟机限定在了运算系统的核心层。这两个限定层隔离了进程，并提供了对环境的严密监测，他解释到。

“这里有许多针对应用程序的监测以确保它在期望的参数内运行。” Ellis 说。

虚拟机逃逸和虚拟机失窃

Edward L. Haletky 是 AstroArch 咨询公司总裁和首席顾问，他赞同保护虚拟系统应从传统方法开始。将虚拟网络分隔成不同的部分并通过入侵防御和入侵预防系统来运行敏感虚拟机流量。他说，应用程序和底层运算系统应该被修补和更新。

虚拟机自身也是一个威胁面，Haletky 说道。传统的反恶意软件能够扫描内存，但是它通常是基于特征的并可以被攻击者绕过。攻击者可以利用零日漏洞或者新的恶意软件变种来绕过反恶意软件技术，他补充道。

“从本质上讲，这是一个与总是名列前茅的黑客的军备竞赛” Haletky 说。

研究人员继续研究虚拟机逃逸，这种逃逸指一个精明的攻击者能够突破虚拟机，获得管理程序并控制在主机上运行的其他虚拟机。“目前所有公开的逃逸对用于服务器虚拟化的主要管理程序都是无效的，比如 vSphere，XenServer 和 Hyper-V，” Haletky 说道。另一种技术叫做虚拟机失窃，通过这种技术，攻击者可以窃取一个虚拟机文件，然后查看服务器的内容。

“这里有许多不同的攻击途径，” Haletky 说，“管理程序可以以某种方式自我保护，但是企业需要对它进行加强，并且应该像他们会在物理环境中做的那样，添加安全层。”

不过，Haletky 认为攻击者很可能选择快速的效果。“当攻击者可以突破管理网络并得到所有东西时，为什么还费心的去窃取虚拟机并做困难的事情呢？”他说，“由于虚拟机和管理环境很容易被突破，所以当前的管理网络规则要将它从其余所有部分分隔出来。”

现有的工具可以帮助企业获得对虚拟网络和文件子系统的可视性，但是没有一个单一的工具可以做所有的事情，Haletky 说。虚拟环境的审核也是一个需要改进的领域。传统的日志分析工具不能得到完整的情况。“你需要将谁做了什么事情，在哪里，是何时以及如何做的相联系起来，但在虚拟环境中这一点仍然是很难做到的。”他说道。

（作者：Robert Westervelt 译者：Sean 来源：TechTarget 中国）

虚拟化不再是网络安全黑洞

由于虚拟基础架构缺少可见性，许多企业的安全敏感应用程序都避免使用虚拟化技术。而有些公司则尝试使用 VLAN 和防火墙对虚拟机进行物理隔离，以保证虚拟环境的安全，但是这种方式会降低基础架构灵活性，影响虚拟化的动态特性。

现在许多供应商正通过开发新产品和特性来解决虚拟化安全问题。Juniper 收购了虚拟化安全专业公司 Altor Networks。思科推出了它的虚拟安全网关软件。惠普网络则发布了 TippingPoint vController，扩展它的 TippingPoint 入侵防御系统（IPS）的虚拟化安全功能。这个软件是安装在 VMware ESX 宿主上的，它会强制要求宿主服务器将所有需要检测的虚拟机流量转发到一台 TippingPoint IPS 设备上。

位于达拉斯的住宅抵押货款公司 PrimeLending 采用了 TippingPoint vController 软件，以便确保它成百上千运行在 25 台 VMware ESX 宿主服务器上的虚拟机安全。

John Hernandez 是 PrimeLending 的副总裁和信息安全主管，他说：“vController 很强大，它让我们可以透明且精细地查看虚拟机及宿主之间传输的实际流量。它使我们知道威胁结构是什么，以及我们在部署技术时面临的潜在风险和问题是什么。”

随着 PrimeLending 将更多的关键应用程序部署到虚拟化基础架构中，Hernandez 需要这种专业的虚拟化安全产品。他最近在数据中心部署了一对 TippingPoint S660N IPS 设备，并在 25 个 ESX 宿主上部署了两个 vController 实例。

在安装 TippingPoint 硬件和软件之前，Hernandez 只能对虚拟化基础架构进行有限的监控。

他说：“您无法精细地监控传统虚拟机之间传输的流量。在大多数时候，监控流量都是在外部，即从一台主机到另一台主机，或者从一台主机到网络的另一个节点。实际上，您无法清晰地区分虚拟机之间的事务。”

TippingPoint 虚拟化安全属于分层安全策略

PrimeLending 已经将它的 TippingPoint 技术整合到诸多供应商提供的多层安全技术中。Hernandez 说，公司使用思科防火墙保护网络边界，并使用了 RSA 数据丢失预防技术。它还使用 RSA enVision 安全意外与事物管理（SIEM）处理由防火墙和 IPS 检测到的事件。

分层方法最近帮助公司检测到了一个受攻击的设备。Hernandez 说：“信贷人员把一个文档带回家，然后在家里一台感染了病毒的 PC 上进行处理。完成工作后，信贷人员将文档带回企业，在企业网络中继续处理剩余工作。这个中毒的文档会尝试访问 “东部集团”的一些 IP 地址，以此感染我们的环境。幸好，TippingPoint 发现了这个问题，并阻止了这个外部连接， 同时将该问题通知给我们的团队。从直觉上来看，这并不是虚拟环境能够做到的，而是 TippingPoint 所特有的功能。”

使用虚拟化安全工具处理大量流量

在使用 TippingPoint 虚拟化安全工具时，Hernandez 没有注意到虚拟机之间产生的流量数量。当 vController 开始将这些事务转发到网络及其 IPS 设备上时，他发现，当虚拟基础架构增长时，他最终需要升级到更强大的 TippingPoint 设备。

“我们开始采用中端 TippingPoint 设备，我们将其中一台专门用来处理网络流量，而另一台专门用来传输虚拟机流量。这两台设备都能够正常工作，但是考虑到我们的企业目标是在未来两至三年实现组织规模扩大二至三倍，我们显然需要考虑采用更大型的设备，以获得更多的带宽。”

(作者：Shamus McGillicuddy 译者：曾少宁 来源：TechTarget 中国)

安全厂商致力于解决虚拟化安全的性能问题

随着虚拟化和云计算继续吸引着注重成本的企业用户，安全厂商们正致力于重新设计它们的技术，用以集中解决在虚拟环境中实施安全时出现的问题。

“毫无疑问，为物理环境所设计的安全性被引入到虚拟环境会引起性能问题，” Ogren 集团的创立者和首席分析师 Eric Ogren 说，“一个虚拟设备仅仅拥有安全是不够的。虽然安全是毋庸置疑的，但是 CPU、存储器和网络资源与虚拟机的连接可以迅速使系统的性能下降。”

市场研究公司 Current Analysis 的高级分析员 Paula Musich 表示，一些安全厂商已采取的策略，即在一个物理服务器上的每一个虚拟机内安装安全软件的实例，会导致系统处于停滞状态。

“每天早上当人们登录时，做的第一件事通常是使用防病毒软件，并同时扫描所有机器，”她说，“突然之间你的物理服务器瘫痪了，因为你进行的扫描接管了几乎在它上面所有可用的 CPU 处理周期。”一些厂商已经通过随机化扫描时间来解决这个问题，以使它们不会同时地全部自动发生，Musich 说道。“也许一个更加长远的解决办法是：在你试图保护的每一个虚拟机上并不需要使用实例的方式来执行安全。”她补充道。

打击 AV 风暴

Musich 和其他安全专家赞扬了 Trend Micro 公司，因其在固定的虚拟环境中处理“AV 风暴”问题的创新方法。

位于美国加州 Cupertino 的 Trend Micro 公司的云安全副总裁 Dave Asprey 表示，已经有在 100 个虚拟桌面上安装 AV（反病毒）的情况引起了糟糕的性能问题，以至于公司不得不放弃安全，并“希望使性能重新恢复正常，但这并不是最好的做法。”

Trend 公司的工程师检查了需要采取什么措施来解决在虚拟架构中的新威胁，并确定它们能带来的效率。Asprey 解释了公司的深度安全产品的发展情况：“如果我们注意到了虚拟服

务器上的云中所需要的大多数安全功能，在每个物理服务器上将它们集中到一个单一的虚拟实例里，那么我们将从根本上得到更好的密度和同等的效果，甚至会有更好的安全性。”

“我们使用虚拟机来工作，它拥有应用程序接口，使我们可以检查和管理文件请求，就像它们脱离了在物理主机上运行的每个虚拟机。”他继续说道，“所以只需一个 Trend Micro 公司的实例，而不是 100 个，并且我们得到了更好的性能和密度数字。”

Tolly 集团，一个第三方的 IT 测试实验室，在今年早些时候报道说：Trend Micro 公司的深度安全产品在使用关键系统资源方面的效率，是虚拟环境中的另外两个竞争产品的 11 倍。据 Trend 公司所说，这个效率可以帮助企业增加每个主机上的机器数量，或者虚拟机密度。

虚拟环境的安全性优化

惠普公司的主管说：考虑到在固定的虚拟环境中避免类似于 AV 风暴的问题，公司设计了新的入侵防御系统设备。惠普网络的安全产品管理总监 Greg Adams 说道，入侵防御系统 S6100N 为企业在物理和虚拟环境中应用安全措施提供了一个无缝的方式。它检查虚拟机到虚拟机的流量和虚拟机到物理系统的流量。

惠普公司的 vController 是一个轻量级的代理程序，它与虚拟机的 VMsafe 应用程序接口相结合，拦截虚拟环境内的流量，并把它发送到物理的入侵防御系统，从而用于检查，Adams 说道，这个架构方法允许惠普公司“在虚拟机自身上放置一个资源利用率低的代理程序”。

位于加州桑尼维尔的 PacketMotion 公司也致力于用它最近的用于虚拟环境的安全产品版本来阻止性能问题。公司的 PacketSentry 虚拟探测（VirtualProbe）将公司的网络活动监测技术扩展到虚拟机集群。这项技术用于实时地检测潜在的恶意内部行为或者违反规定，并旨在填补公司首席执行官 Paul Smith 所说的缺乏用于监测虚拟机到虚拟机流量的企业工具这一不足。

“我们作为客户虚拟机被部署，它不会使虚拟主机负荷变重，” Smith 说道。据 PacketMotion 公司，作为一个客户虚拟机，PacketSentry 虚拟探测只占用主机 CPU 的 3%到 5%。

同时，位于卡尔加里的 Wedge Networks 公司最近宣称它的 BeSecure Web 安全网关可以作为云服务提供商的虚拟设备。总裁和首席执行官 Hongwen Zhang 表示，该技术在虚拟环境中提供了近乎无痕迹的深度内容检测。“我们的隐形路由技术没有对虚拟网络配置造成任何影响，

利用这项技术，我们可以在不改变流量流的介质访问控制/虚拟局域网/互联网协议的情况下来进行内嵌策略执行。”他说道。

增长的市场

安全厂商正在提升他们虚拟安全产品的供给，因为企业越来越意识到它们的虚拟环境对安全的需要。据位于加州坎贝尔的 Infonetics Research 公司的最近的一项研究，企业预计在 2012 年将比 2010 年平均多花费 51%的费用在虚拟环境的安全上。该公司调查了 105 个就职于北美公司的 IT 买家，这些买家公司都部署了服务器虚拟化技术。

该研究还表明，在虚拟环境中使用新的安全产品的三大驱动力：阻止针对虚拟环境的威胁，阻挡虚拟机之间的威胁和维护安全的服务器配置。

Infonetics 市场研究公司称，虚拟化环境的安全解决方案的市场是很混乱的，包括许多虚拟化厂商， VMware 就是其中的一个领导者。

（作者：Marcia Savage 译者：Sean 来源：TechTarget 中国）

如何应对层出不穷的虚拟化安全问题？

理想情况下，服务器应该足够稳定，能够抗御互联网的所有攻击，网络提供最优的端到端传输。但现实情况是，数据中心网络总是通过嵌入的防火墙实现主要的安全保护来减少暴力攻击造成的拒绝服务，对入站流量极少执行 TCP 端口过滤。

使用防火墙来保护数据中心网络的物理服务器已经很难了，把它用于保护虚拟服务器，或者私有云环境，那么难度会更大。毕竟，虚拟服务器会经常迁移，所以防火墙不需要必须位于服务器物理边界内。有几种策略可以为虚拟环境提供防火墙保护。

虚拟网络安全

传统数据中心架构的网络安全设计众所周知：如果服务器的物理边界属于同一个安全域，那么防火墙通常位于聚合层。当你开始实现服务器虚拟化，使用 VMware 的 vMotion 和分布式资源调度（Distributed Resource Scheduler）部署虚拟机移动和自动负载分发时，物理定界的方式就失去作用。在这种情况下，服务器与剩余的网络之间的流量仍然必须通过防火墙，这样就会造成严重的流量长号，并且会增加数据中心的内部负载。

虚拟网络设备能够让你在网络中任何地方快速部署防火墙、路由器或负载均衡器。但当你开始部署这样的虚拟网络设备时，上述问题会越来越严重。这些虚拟化设备可以在物理服务器之间任意移动，其结果就是造成更加复杂的流量流。VMware 的 vCloud Director 就遇到这样的设计问题。

使用 DVFilter 和虚拟防火墙

几年前，VMware 开发了一个虚拟机管理程序 DVFilter API，它允许第三方软件检查网络和存储并列虚拟机的流量。有一些防火墙和入侵检测系统 （IDS）供应商很快意识到它的潜在市场，开始发布不会出现过度行为的虚拟防火墙。VMware 去年发布了 vShield Zones 和 vShield App，也成为这类供应商的一员。

基于 DVFilter 的网络安全设备的工作方式与典型的防火墙不同。它不强迫流量必须通过基于 IP 路由规则的设备，而是明确地将防火墙插入到虚拟机的网卡（vNIC）和虚拟交换机（vSwitch）之间。这样，不需要在虚拟机、虚拟交换机或物理网络上进行任何配置，防火墙就能够检测所有进出 vNIC 的流量。vShield 通过一个特别的配置层进一步扩充这个概念：你

可以在数据中心、集群和端口组（安全域）等不同级别上配置防火墙规则，在创建每个 vNIC 的策略时防火墙会应用相应的规则。

并列防火墙自动保护虚拟机的概念似乎是完美的，但是由于 DVFilter API 的构架原因，它只能运行在虚拟机管理程序中，所以它也有一些潜在的缺点。

虚拟机防火墙的缺点：

每一个物理服务器都必须运行一个防火墙 VM。防火墙设备只能保护运行在同一台物理服务器上的虚拟机。如果希望保护所有物理位置的虚拟机，那么你必须在每一台物理服务器上部署防火墙 VM。

所有流量都会被检测。你可能将 DVFilter API 只应用到特定的 vNIC 上，只保护其中一些虚拟机，但是 vShield 产品并不支持这个功能。部署这些产品之后，所有通过虚拟机管理程序的流量都会被检测到，这增加了 CPU 使用率，降低了网络性能。

防火墙崩溃会影响到 VM。防火墙 VM 的另一个问题是它会影响 DVFilter API。受到影响的物理服务器上所有虚拟机网络都会中断。然而，物理服务器仍然可以运行，并且连到网络；因此，高可用特性无法将受影响的 VM 迁移到其他物理服务器上。

相同流量流会执行多次检测。DVFilter API 在 vNIC 上检测流量。因此，即使虚拟机之间传输的流量属于同一个安全域，它们也会被检测两次，而传统防火墙则不会出现这种情况。

虚拟交换机在虚拟化安全中的作用

虚拟化安全设备制造商也可以选择 vPath API，它可用于实现自定义虚拟交换机。思科系统最近发布了虚拟安全网关（Virtual Security Gateway ，VSG)产品，该产品可能整合传统（非 DVFilter）虚拟防火墙方法和流量流优化技术。思科宣布 VSG 只进行初始流量检测，并将卸载流量转发到虚拟以太网模块（Virtual Ethernet Modules，VEM：虚拟机管理程序中改良的虚拟交换机），从而防止出现流量长号和性能问题。如果这一切是真的，那么 VSG 可能是工程师部署安全云服务的最理想工具。

（作者：Ivan Pepelnjak　译者：曾少宁　来源：TechTarget 中国）

虚拟化技术的安全：IDS/IPS 实施策略

同时在主机和网络层面进行入侵监测和预防，是当今信息安全基础设施建设的主要内容。然而，随着虚拟化技术的出现，许多安全专家意识到，传统的入侵监测工具可能没法融入或运行在虚拟化的网络或系统中，像它们在传统企业网络系统中所做的那样。

例如，由于主要平台厂商提供的虚拟交换机不支持建立 SPAN 或镜像端口、禁止将数据流拷贝至 IDS 传感器，网络入侵监测可能会变得更加困难。类似地，内联在传统物理网区域中的 IPS 系统可能也没办法轻易地集成到虚拟环境中，尤其是面对虚拟网络内部流量的时候。基于主机的 IDS 系统也许仍能在虚拟机中正常运行，但是会消耗共享的资源，使得安装安全代理软件变得不那么理想。

幸运的是，我们有办法调整 IDS/IPS 系统的实现策略，从而允许监控虚拟系统的网络流量。这就是本文将要讲述的内容。

对初学者来说，VMware 公司的虚拟交换机允许交换机或端口组运行在“混杂模式”，这时虚拟的 IDS 传感器能够感知在同一虚拟段上的网络流量。另外，我们也可以把网络流量送至物理端口，然后用物理的 IDS 传感器监测流量。目前有大量开源的或第三方虚拟交换机工具可供使用，它们能够进行如传统交换机一样的操作。

相较于 Citrix 系统公司的基于内核的虚拟机（KVM）和甲骨文公司的 VirtualBox 平台，Open vSwitch 项目提供了虚拟交换机的完整功能，允许建立 SPAN 端口进行流量镜像和监控。思科系统公司的商业产品 Nexus 1000v 交换机提供了同样的能力，并使用广为人知的思科 IOS 命令行接口。这两种交换机都支持流数据的捕获和分析，还可以用于在系统间和网络间进行行为监控。

除了重新设计系统和使用功能更加全面的虚拟交换机外，安全专家还应研究一些开源或商业的入侵检测和预防产品是否有虚拟化的版本。许多知名的厂商，如 Sourcefire 公司、HP TippingPoint 公司以及 IBM ISS 都将他们已有的 IDS 和 IPS 平台移植为对应的虚拟化设备。所有这些虚拟化设备都能容易的集成到虚拟化网络中，在虚拟机之间提供流量监测，也能在虚拟网络与真实物理网络之间提供流量监测。

如今我们可以在市场上看到由 Reflex 系统有限责任公司、Catbird 网络公司、HyTrust 公司等提供的专业虚拟化产品。这些公司还提供虚拟环境中基于政策的（policy-based）监控和

分析工具。虽然不是真正的基于签名的入侵监测，但是这些产品可以加强传统的 IDS/IPS 系统，允许更精确的流量监控和访问控制，还能分析网络行为，为虚拟网络提供更高的安全性。

有许多免费产品可以考虑使用。你可以从 VMware 的虚拟设备市场（Virtual Appliance Marketplace）获得 Snort 和 Shadow 入侵监测系统。这两个工具可接入 Vmware 虚拟环境中，监控和侦测入侵企图。值得一提的是，这一独特能力是 Vmware 公司相比竞争对手而言的一项优势。

此外，一些基于主机的 IDS 和 IPS 产品也已被推出，它们经过了测试，被证明能够在许多虚拟环境中工作。Check Point 软件技术公司、McAfee 公司以及赛门铁克公司是支持基于主机的 IDS/IPS 系统的代表厂商，这类 IDS/IPS 系统可以在虚拟客户系统中使用。另一个例子是可免费使用的 ISSEC HIDS（现在被趋势科技公司拥有），它被证明能在虚拟机中使用，尽管在虚拟系统中的性能和稳定性还不能够得到保证。大多数情况下，商业的 HIDS 和 HIPS 代理都经过了测试和修改，它们在虚拟系统中占用更少的资源，避免过度消耗宿主机的硬件能力。然而，基于主机的设备仍然要消耗大量的资源，且要求更加集约化的管理。为确保虚拟机资源不会在扫描或检测活动中被过度消耗，额外的调度和控制能力也是必要的。

许多公司面临的关键问题应该是：“我们需要多大程度的监控？”对许多公司而言，已有的基于硬件的设备足以监控进出虚拟网络的流量。如今大多数公司都很少，如果还有的话，在特殊的网络段监控系统间的网络活动。然而，对于那些想要或需要更高级的入侵检测和预防系统的公司来说，好消息是无论是在网络层面还是主机层面，我们都有许多选项可供选择。鉴于虚拟化技术变得越来越流行，虚拟 IDS 和 IPS 技术无疑将更加普遍。

（作者：Dave Shackleford 译者：Sean 来源：TechTarget 中国）

虚拟化安全：vShield Endpoint 和 Edge 功能

在 2010 年，VMware 把 vShield 重新定位为用于 ESX 和 ESXi 的安全保护套件。该 VMware 系列的第一部分涵盖 vShield Manager、Zones and App。主要针对 vShield Edge 和 Endpoint 的功能以及 vShield 的许可费用问题。

vShield Edge

VMware vShield Zones 和 App 保障的是虚拟系统内的安全性，而 vShield Edge 的作用范围在外围网络上。它通过安全和网关服务实现对虚拟机的隔离，提供控制区、外网 VPN 和参数保护等功能实现对多租户云应用环境的支持。

vShield Edge 服务包含如下内容：

- 网络地址转换（NAT）。NAT 服务保护内部的私有网络跟公网隔离。NAT 规则可以设定为只允许拥有私有地址的虚拟机访问。

- 动态主机配置协议（DHCP）。该功能支持 IP 地址池和一对一的静态 IP 地址分配。静态 IP 地址的捆绑可以基于请求终端的 vCenter 管理对象 ID 或接口 ID 进行。

- 站点间 VPN。Edge 支持在 Edge 和远程站点间的 IPsec（Internet Protocol security）VPN 连接。同时也可以支持共享密钥模式，IP 地址单向传播而不是采用在 vShield Edge 和远程 VPN 路由器之间的动态路由方式。在每个远程 VPN 路由器之下，您还可以设置多个子网络通过 IPSec 通道连接到 vShield Edge 保护下的内网。

- Web 负载均衡。vShield Edge 提供了 HTTP 流量的负载均衡功能。负载均衡（包括第七层协议的支持）功能允许 Web 应用可以自动扩展。您可以把外部（或公网）IP 地址映射到一组内部服务器上实现负载均衡。负载均衡器可以接受外部 IP 地址的 HTTP 请求并决定使用哪台内部服务器。

- 端口组隔离。该服务在受 Edge 保护的虚拟机和外部网络之间设置了隔断。端口组隔离和 vLAN 具有相同的效果，但是不需要交换机链路聚合带来的复杂连接和端口映射规则。

vShield Edge 可以支持各种 vSphere 的 vSwitch 模式，标准的、分布式的 vSwitch 包括 Cisco Nexus 1000V 都可以。

vShield Endpoint

代替传统的在每台虚拟机内安装极其消耗资源的反病毒/反恶意软件代理程序的方式，vShield Endpoint 把反病毒（AV）软件功能卸载到一台专用的虚拟安全设备上。vShield Endpoint 驱动在子 OS 内被加载并链接到某台运行于被保护 vSwitch 上的专用安全强化虚拟机，通过位于虚拟化管理层上的 vShield Endpoint 的可加载内核模块（LVM）。

通过这种机制，该专用于安全保障的虚拟机可以透过 Endpoint 驱动对虚拟机进行病毒和恶意软件监控（目前还不能支持虚拟机内存扫描。）同时，防病毒引擎和签名的升级只需在供应商的 AV 设备上进行一次就可以，不再需要对运行于每台虚拟机上的 AV 代理端进行操作。另外，通过 AV 设备可以进行集中策略管理，这样 Endpoint 瘦代理端就可很快决定如何处理客户端 OS 内的恶意文件。

VMware 提供了知识库和 API，方便安全厂商把自己的产品集成到 vShield Endpoint 中。现在趋势科技的 Deep Security 是唯一的可以支持 vShield Endpoint 的产品，它提供了无客户端保护，不会在客户端虚拟机内留下任何痕迹。不过其他的厂商，如 McAfee 和 Symantec 已经宣布不久他们也将推出 Endpoint 兼容产品。

vShield Endpoint 现在仅支持运行于虚拟机上的 32 位和 64 位 Windows 操作系统。

vShield 授权

vShield Manager 和原始的 vShield Zones 产品在 vSphere Advanced、Enterprise 和 Enterprise Plus 版本中都有包含，其中 Zones 是基于每台宿主机进行授权的。

同时，vShield Endpoint、Edge 和 App 需要单独授权，以 25 台虚拟机为一个授权包。每个 vShield 产品都已经包含在 vShield 的下载中，只不过额外的这些产品需要在 vCenter Server 中使用授权码来激活才可用。

vCloud Director 产品中包含了 vShield Edge，vCloud Director 授权码可用于激活 vShield Edge 的相关功能。在 VMware View Premier 版中也含有一个 vShield Endpoint 授权码。在 vShield 系列的下一部分，我们将关注 vShield 的部署以及配置和管理技巧。

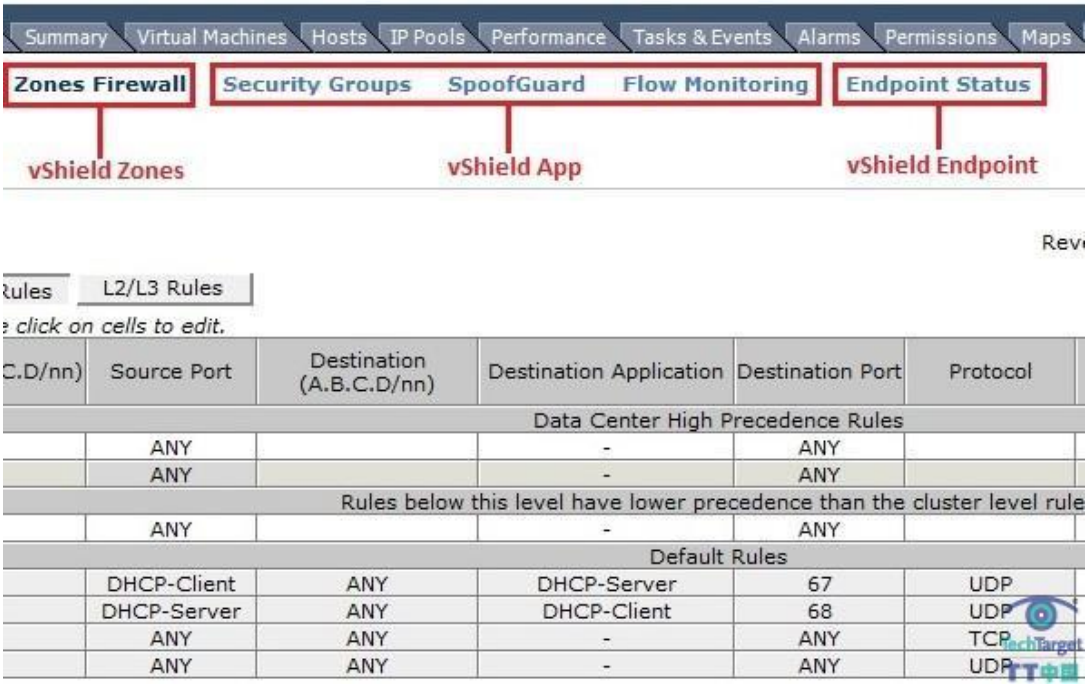


图 1

25 台虚机套餐	基本(12/5) 服务	金牌(24/7)服务
vShield App	$4,538	$4,688
vShield Edge	$4,538	$4,688
vShield Endpoint	$1,513	$1,563

(作者：Eric Siebert　译者：李哲贤　来源：TechTarget 中国)

VMware JRE中的漏洞是否会妨碍虚拟化的实施

问：VMware公司最近发现了一些有关Java运行环境（JRE）的安全漏洞。难道这些漏洞暗示着还会出现更多的漏洞？这些漏洞会成为人们不实施虚拟化的一个理由吗？

答：VMware公司已报告了一些有关Java运行环境问题的漏洞，其中几个漏洞可被黑客用来攻击系统。在最近几个月里，其他主要的虚拟化厂商也已经发布了一些补丁。虽然虚拟化不是一项新技术，但直到最近它才得到广泛的采用。由于它在越来越多的配置中使用，各种安全漏洞现在也陆续被发现，这并不奇怪。此外，每当一项技术开始流行起来，它就会引起黑客们的兴趣，黑客会开始积极寻找那些可以被利用的漏洞。

一个被破坏的管理程序使得攻击者可以访问一个虚拟服务器上数以千计的台式机，这是一件非常可怕的事情。目前还出现了一些令人吃惊的攻击展示，教人如何逃出一个虚拟机操作系统，侵入本地机，从而“对本地机的操作系统大肆攻击”。Joanna Rutkowska的Blue Pill虚拟rootkit是“无法察觉的”，因为它安装在管理程序上，但这些虚拟机逃逸技术仍停留在实验室阶段，目前还没有看到严重虚拟机安全攻击的报道。在这一点上，这些攻击都是理论上的，如果风险评估认可了实施虚拟化的决定，那么即使未来可能会面临一些安全威胁，也不能阻止公司去实施虚拟化。

我可以肯定的是，我们将看到更多的虚拟化漏洞被发现，这就要求我们采用一种有着标准安全强化机制的技术。如果你决定继续实施虚拟化，请确保您的IT团队接受了足够的培训，以便能应对物理和虚拟环境的不同。仅仅使用现有的、保护物理服务器的安全政策和措施去保护虚拟服务器是不够的。例如，当IP地址的改变比虚拟机的创建、弃用或迁移更为频繁时，安全设备和政策需要消除对IP地址的依赖性。

在虚拟化的主机内还将有一些网络可见性的损失。传统的网络安全工具不一定能观测到一个单主机中多个虚拟机彼此之间的通信流量，这使得对不良信息流量的监测更加困难。改变管理程序也需要进行一次全面回顾，从而防止“虚拟机散乱现象”（VM sprawl），如果真的发生这种现象，虚拟化实例会突然弹出但没有人能够对它们进行持续跟踪。我强烈推荐你们去实施分割（以避免多个虚拟机产生混乱，这些虚拟机运行在一个主机的多个不同安全态势和要求的区域上），并把高级权限的虚拟机隔离在它们自己的网段上。同时，你还需要监测对虚拟化资源的访问和所有的管理活动，这样在遇到任何重大的事件时就能够发出警报信息。

毫无疑问，虚拟化有许多好处，它可降低因购买软件所有权而产生的总成本，但是你必须跟踪虚拟化威胁的最新发展，并了解为了保护虚拟化技术而进行的研究和创新。 VMware 公司的技术资源中心是一个学习虚拟化知识的好地方，因为它有很多关于如何保护虚拟基础设施的指导。

（作者：Michael Cobb 译者：Sean 来源：TechTarget 中国）

虚拟化安全问题：在哪里安置防火墙连接？

问：是否有可能在防火墙连接前实施一个病毒阻止程序？特别是，这将有助于增加虚拟服务器的安全性？

答：执行远离服务器的基于签名的阻止活动或嵌入式补丁（inline patching）是有可能的。使用网络第七层（layer-7）保护技术，比如 Web 应用防火墙或在线入侵防御系统（IPS）将有助于缓解或解决病毒和其他恶意软件带来的威胁，在它们到达服务器前。

不过，考虑到未过滤的互联网流量所产生的大量噪音，我不会将这样一种产品安置在防火墙连接前。理想的情况是，这些产品应该安置在防火前和交换器的基础设施托管服务器之间，作为一个网络第二层（layer-2）的桥。

由于这种阻止活动是在远离服务器的情况下执行的——在虚拟化环境以外——所以它对于保护同一物理硬件上的多个虚拟服务器是非常有效的。

（作者：Anand Sastry　译者：Ping　来源：TechTarget 中国）

实现虚拟化安全的新方法

传统的安全方法在虚拟化的世界里依然是可以使用的。用户不仅需要对服务器和相关的应用做保护，而且需要监控哪些人可以对哪些资源进行访问，对进入数据中心的访问者做鉴定和管理。赋予在数据中心内工作的用户以适当的通关权限，并在他们完成认证后给予相对应的访问权限。

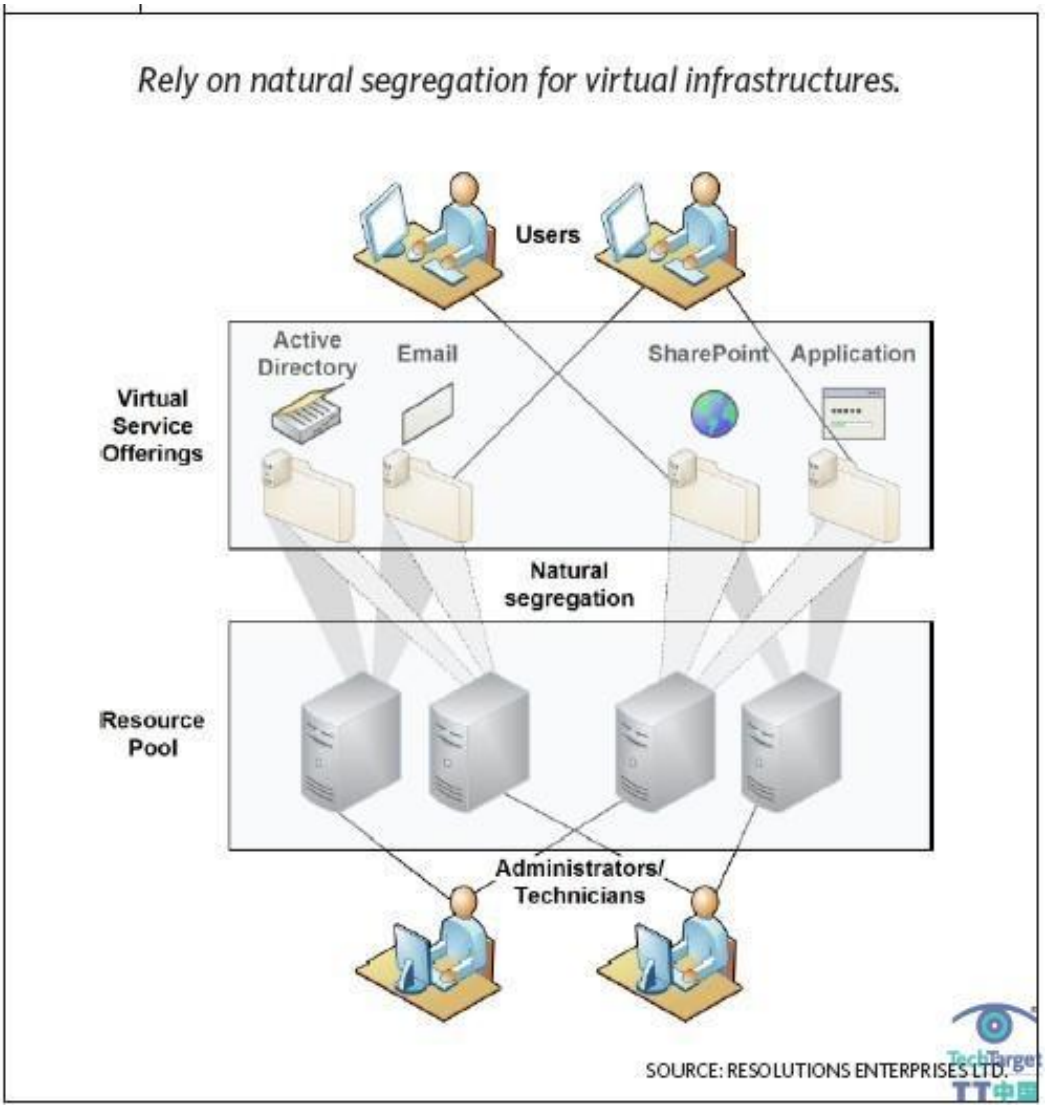
另外，您还需要确保那些数据中心内可以做数据更改操作的人员都是拥有授权才这么做的，也就是说现有的安全方面的经验在虚拟环境里是可以获得延续的。如果您把现有的终端用户服务进程都迁移到了虚拟机和 VSO 上，那么传统的安全方法也应该位于同一级别上。

然而不幸的是，在为 VSO 提供物理资源的资源池级别上，从设计原理看，并不具备和用户进行交互的能力。资源池内的物理机仅仅是装载了虚拟化引擎的宿主机而已。因此，也只有管理员和技术人员可以跟物理机对话。

在这些环境里（资源池和 VSO），通常运行时都带有一个特定的安全文本文件，而该文件是可以被中央目录服务所访问的。我们需要考虑分离不同环境中各自的安全文本文件。毕竟，如果资源池仅仅供管理员和技术人员访问，看起来我们根本没有必要把资源池相关的安全文本文件开放为用户共享模式。

事实上，用户不需要对资源池做任何操作。对于最终用户而言，他们也不需要和网络环境中的路由器或交换机做交互。因此，您需要为资源池和 VSO 创建独立的安全文本文件。例如，如果您运行了 VMware 或 Citrix 的虚拟机管理程序，而您的网络服务运行于 Windows 服务器上，那么资源池的安全文本文件会自动实现和 VSO 安全文本文件的分离（图 1）。这也就是为什么宿主机环境（通常情况下是 Linux）和 VSO 通常运行于不同操作系统的原因。这种方式也自然实现了两个安全文本文件的隔离。

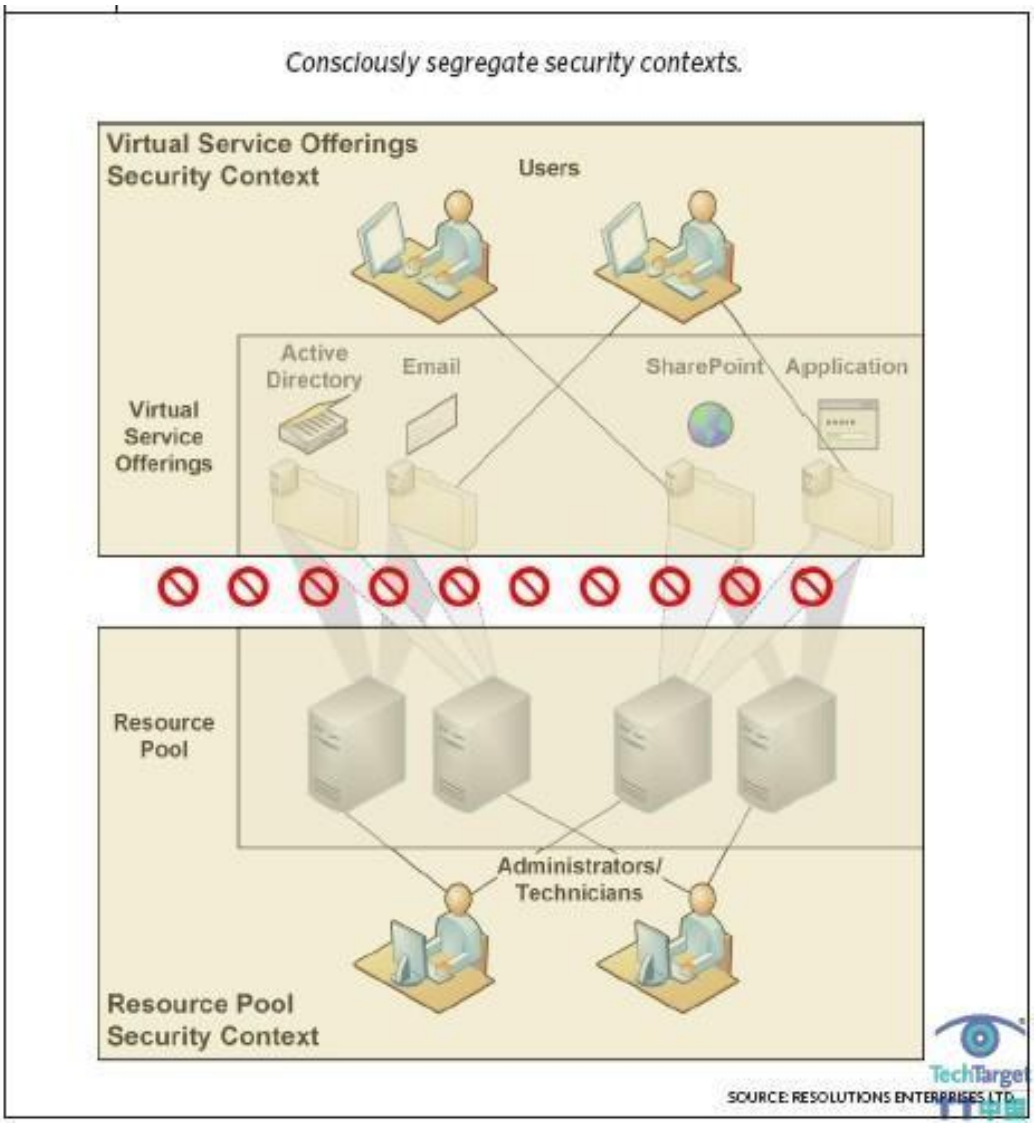
（图一）



然而，如果宿主机和虚拟机所运行的操作系统相同的情况下，您就需要手动分离资源池和VSO的安全文本文件。这种情况一般发生在采用了微软的Hyper-V虚拟化管理程序，之上运行Windows网络环境的时候。同样，当我们运行了Linux网络环境而同时又采用了同一Linux系统下的虚拟化管理程序时也会发生。

以Windows网络环境为例，您需要分别为资源池和VSO创建独立的活动目录树，然后同时断开它们之间的所有连接。在两个独立的架构中创建分离的安全文本也是为了防止发生从一个环境向另一个环境中的渗漏（图二）。

（图二）



实现资源池的安全

为资源池创建独立的安全文本仅仅是实现虚拟架构安全的第一步。您还需要和其它的一些安全措施来配合使用。如下是一些额外的考虑：

- 掌控所有到资源池的访问以确保只有被信任的个体才具备访问权限。每个访问资源池的个体应该具备一个命名账户，而该账户和普通用户用来访问 VSO 的账户命名应该是有所区别的。

- 掌控所有到资源池管理工具的访问。只有被信任的个体拥有访问资源池组件，如物理服务器、虚拟化管理程序、虚拟网络、共享存储，及其它内容相关的管理工具

的权限。向未被认证的用户开放管理工具的访问权限，就等同于向那些恶意操作开放了 IT 系统架构。

- 管理虚拟化引擎或管理程序的访问，以及其上运行的虚拟机。所有的虚拟机都应该是首先通过系统管理员来创建和保护的。如果某些最终用户，如开发人员、测试人员或培训者，需要和网络环境中的虚拟机交互，那么这些虚拟机应该是通过资源池的管理员来创建和管理的。

- 控制虚拟机文件的访问。通过合理的访问权限来实现所有包含了虚拟机的文件夹以及虚拟机所在压缩文件的安全。无论是在线的还是离线的虚拟机文件都必须获得严格的管理和控制。理论上来讲，您需要同时对虚拟机文件的访问做监管。

- 通过在宿主机上尽可能实现最小化安装来减少主机可能被攻击的接口。请确保虚拟化管理程序的安装尽可能的可靠。

- 部署适合的安全工具。为了支持合理的安全策略，您的系统架构应该包含各种必要的工具，如系统管理工具、管理清单、监管和监视工具等等，包括一些常用的安全设备。

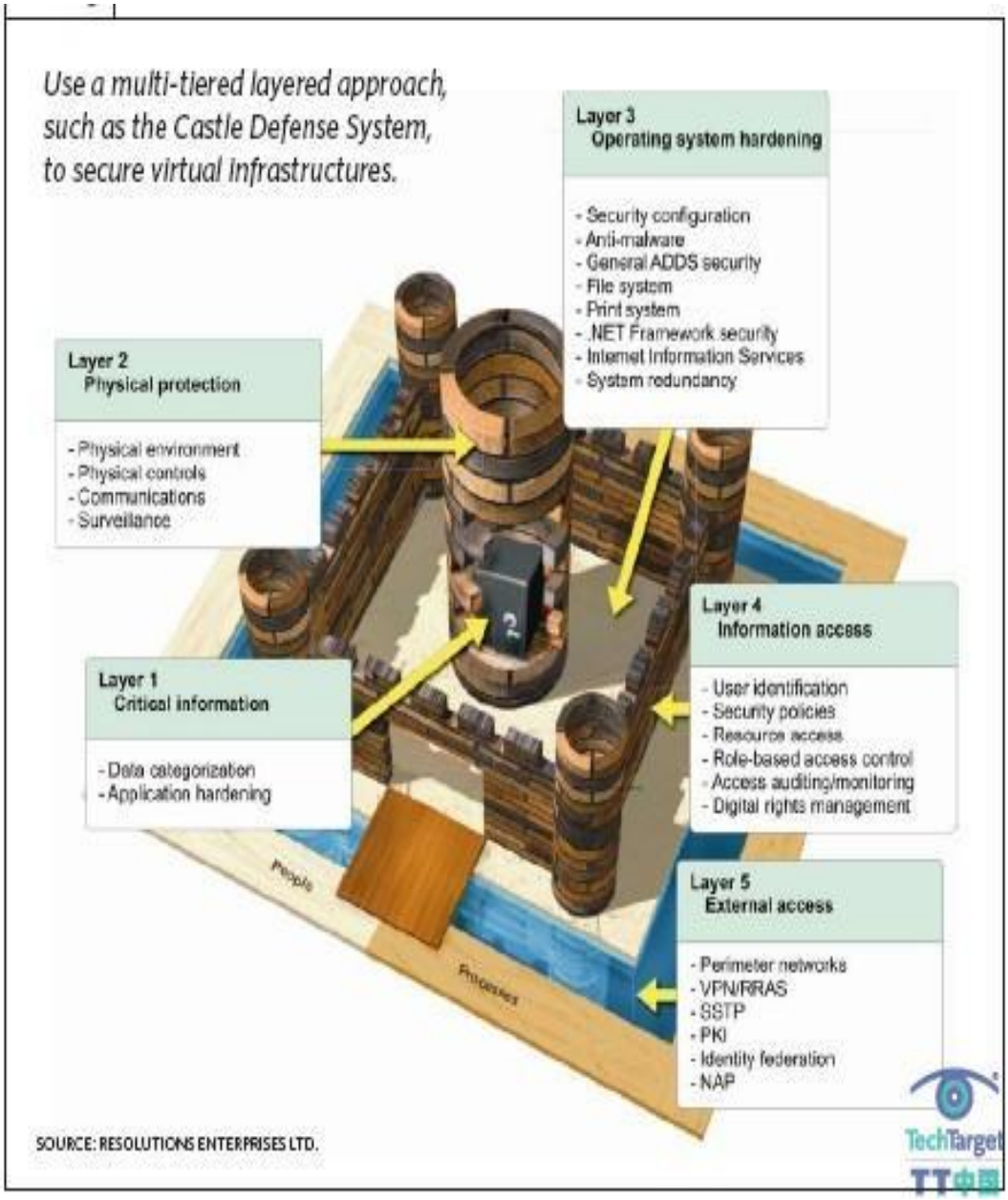
- 分离网络流量。在一个正确设置的资源池系统中，应该包含有几个不同的私有网络用于：管理数据流量、在线迁移流量以及存储系统流量。所有的这些网络都应该和系统架构中的公网流量相分离。

深层防护策略

除了安全文本文件的隔离外，您还应该考虑对虚拟化环境采用深层防护策略。这个像城堡一样的 CDS 防护模型是由 Resolution Enterprise Ltd.,公司提出来，该公司位于英属哥伦比亚省维多利亚地区，是一家独立的数据中心业务咨询公司，致力于推动深层防护方式。很多企业的传统服务提供网络都采用了深层防护策略，通过执行相应的策略实现对资源池的保护（图三）。

用户可以对资源池或者 VSO 采用 CDS 防护模式。如下的表 1 也显示了在您通过部署 CDS 模式对资源池进行保护时，分别在五个不同的层次上需要去考虑的问题。在这个表里，也同时列出了在对最终用户网络和终端网络（如资源池网络）分别部署 CDS 模型时采取的组件之间的差异。

（图三）


Use a multi-tiered layered approach, such as the Castle Defense System, to secure virtual infrastructures.
Layer 3
Operating system hardening
- Security configuration
- Anti-malware
- General ADDS security
- File system
- Print system
- .NET Framework security
- Internet Information Services
- System redundancy
Layer 2
Physical protection
- Physical environment
- Physical controls
- Communications
- Surveillance
Layer 4
Information access
- User identification
- Security policies
- Resource access
- Role-based access control
- Access auditing/monitoring
- Digital rights management
Layer 1
Critical information
- Data categorization
- Application hardening
Layer 5
External access
- Perimeter networks
- VPN/RRAS
- SSTP
- PKI
- Identity federation
- NAP
People
Processes
SOURCE: RESOLUTIONS ENTERPRISES LTD.
TechTarget
TT中国

在城堡防护模型中每一层需要考虑的内容		
城堡防护层	资源池	虚拟服务提供
第一层： 关键信息	■ 数据保护（虚拟机） ■ 应用程序增强（管理程序）	■ 数据目录 ■ 应用程序增强
第二层： 物理防护	■ 数据中心物理环境 ■ 物理链路管理 ■ 和管理员的交互问题 ■ 监管	■ 数据中心物理环境 ■ 物理链路管理 ■ 和所有用户的交互 ■ 监管
第三层： 操作系统增强	■ 安全配置 ■ 反病毒/防止恶意攻击 ■ 终端目录服务 ■ 文件和打印系统 ■ Web 接口 ■ 系统冗余	■ 安全配置 ■ 防止恶意攻击 ■ 生产目录服务 ■ 文件和打印系统 ■ Web 接口 ■ 系统冗余
第四层： 信息的访问管理	■ 管理员用户定义 ■ 安全策略 ■ 资源访问管理 ■ 基于角色的访问控制 ■ 访问审查/监控	■ 管理员和最终用户定义 ■ 安全策略 ■ 资源访问管理 ■ 基于角色的访问控制 ■ 访问审查/监控 ■ 数字化权力管理
第五层： 外围访问管理	■ 周边网络 ■ VPN 和 RRA ■ 为管理通讯启用 SSL/PKI	■ 周边网络 ■ VPN 和 RRA ■ SSL/PKI ■ 联合定义 ■ 网络访问防护

表 1

预防过度管理

改善资源池安全性的另外一个方法就是限制资源池管理的数量。拥有两个具备系统环境完全访问权的管理员已经足够了。然后，根据数据中心规模大小的不同，您可以基于每个角色所需完成的任务内容分配不同的权限和角色定义。资源池管理员应该可以管理 VSO 网络。如果您有足够的人手，那么最好把不同的管理角色分开。如果做不到的话，至少要确保管理在每个不同的环境中使用不同权限的管理角色登录。请理解，如果管理员在某个环境中扮演了指定的角色，那么他在不同的环境中完成同一动作时所扮演的角色是不同的。

最后，任何时候都要注意对虚拟机的保护。例如，虚拟机在暂停休息的状态下和活动的虚拟机相比其风险更高。因为当虚拟机处于保存状态时，会在内存中生成一个文件，而该文件保留了虚拟机所有相关内容。通过分析这个文件可以找到相应的用户名和密码相关信息。同样，

如果有人窃取了虚拟机文件并带出了办公室，也会带来很大的风险。一旦他们在私有环境中搭建了该虚拟机，那么就很容易闯入我们的环境中。

(译者：李哲贤　来源：TechTarget 中国)