vShield Zones 简介

vShield Zones 1.0

CN-000188-00

vmware®

您可以在 VMware 网站上找到最新的技术文档，网址为：

http://www.vmware.com/cn/support/

VMware 网站还提供最新的产品更新。

如果对本文档有任何意见或建议，请将反馈信息提交至以下地址：

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

目录

关于本文档

本手册（《vShield Zones 简介》）提供有关 VMware® vShield Zones 的特性和功能的信息。

目标读者

本手册是为需要熟悉 vShield Zones 的组件和功能的人设计的。本手册的目标读者为熟悉虚拟机技术和数据中心操作且具丰富经验的 Windows 或 Linux 系统管理员。

文档反馈

VMware 欢迎您提出宝贵建议，以便改进我们的文档。如有任何意见或建议，请将反馈发送到 docfeedback@vmware.com。

vShield Zones 文档

vShield Zones 文档集包括下列文档：

- 《vShield Zones 管理指南》
- 《vShield Zones 快速入门指南》
- 《vShield Zones 简介》

技术支持和教育资源

下面各节介绍为您提供的技术支持资源。要访问本文档的当前版本和其他文档，请访问 http://www.vmware.com/cn/support/pubs。

在线支持和电话支持

要通过在线支持提交技术支持请求、查看产品和合同信息以及注册您的产品，请访问 http://www.vmware.com/cn/support。

客户只要拥有相应的支持合同，就可以通过电话支持，尽快获得对优先级高的问题的答复。请访问 http://www.vmware.com/cn/support/phone_support。

支持服务项目

要了解 VMware 支持服务如何帮助您满足业务需求，请访问 http://www.vmware.com/cn/support/services。

VMware 专业服务

VMware 教育服务课程提供了大量实践操作环境、案例研究示例，以及用作作业参考工具的课程材料。这些课程可以通过现场指导、教室授课的方式学习，也可以通过在线直播的方式学习。关于现场试点项目及实施的最佳实践， VMware 咨询服务可提供多种服务，协助您评估、计划、构建和管理虚拟环境。要了解有关教育课程、认证计划和咨询服务的信息，请访问 http://www.vmware.com/cn/services。

vShield Zones 简介

vShield Zones 是专为 VMware vCenter™ Server 集成而构建的可感知应用程序的防火墙。vShield Zones 是保护虚拟化数据中心免遭攻击和误用的关键安全组件，可帮助您实现合规性所要求的目标。

本章包含下列主题：

vShield Zones 组件

vShield Zones 中包含对分析流量和保护虚拟机必不可少的组件和服务。可通过基于 Web 的用户界面和命令行界面 (CLI) 配置 vShield Zones。

vShield Zones 组件被打包为开放虚拟化格式 (OVF) 的文件。要运行 vShield Zones，需要使用一个 vShield Manager OVF 文件和一个 vShield OVF 文件。

vShield Manager

vShield Manager 是 vShield Zones 的集中式网络管理组件，可作为虚拟机安装在 vCenter Server 环境中的任何 ESX 主机上。vShield Manager 可在与 vShield 实例不同的 ESX 主机上运行。

您可以使用 Web 浏览器访问 vShield Manager 用户界面。通过该用户界面，管理员可安装、配置和维护整个 vShield Zones 部署。vShield Manager 用户界面利用 VMware Infrastructure SDK 显示 vSphere Client 清单面板的副本。该界面包括 [Hosts & Clusters] 和 [Networks] 视图。

您可以使用支持的下列 Web 浏览器之一连接到 vShield Manager 用户界面：

- Internet Explorer 5.x 及更高版本
- Mozilla Firefox 1.x 及更高版本
- Safari 1.x 或 2.x

vShield

vShield 是 vShield Zones 的活动安全组件。每个 vShield 实例提供可感知应用程序的流量分析和基于状态检测的防火墙保护，其方法是检查网络流量并基于一组规则确定访问方式。vShield 基于信任区域控制流量，将流量分为不受保护区域和受保护区域。受 vShield 保护的虚拟机位于受保护区域中。传至受保护的虚拟机的所有流量从不受保护区域进入。

使用 vSphere Client，您可以将 vShield OVF 文件作为模板或虚拟机安装。将软件包安装到 vSphere Client 后，使用 vShield Manager 完成安装。如果将 vShield 软件包作为模板安装，则您可以从 vShield Manager 中引用该模板将多个 vShield 实例作为虚拟机安装到 vCenter Server 环境。可在承载物理 NIC 的任何 vSwitch 上安装 vShield 实例。由于一台 ESX 主机可包含多个物理 NIC，因此您可以在单台 ESX 主机上安装多个 vShield 实例。

当从引用的模板安装时， vShield 安装过程执行下列步骤：

1 创建 vSwitch 主机的副本。

此 vSwitch 副本不包含 NIC。vSwitch 副本的名称由 vSwitch 主机的名称加 _VS 构成：vSwitch1_VS。

2 创建一个受保护区域端口组 VSprot_*vShield-name*，将此端口组附加到 vSwitch 主机。

3 在 vShield 实例的管理界面的 vSwitch 主机上创建一个管理端口组 VSmgmt_*vShield-name*。

4 创建一个不受保护区域端口组 VSunprot_*vShield-name*，将此端口组附加到 vSwitch 副本。

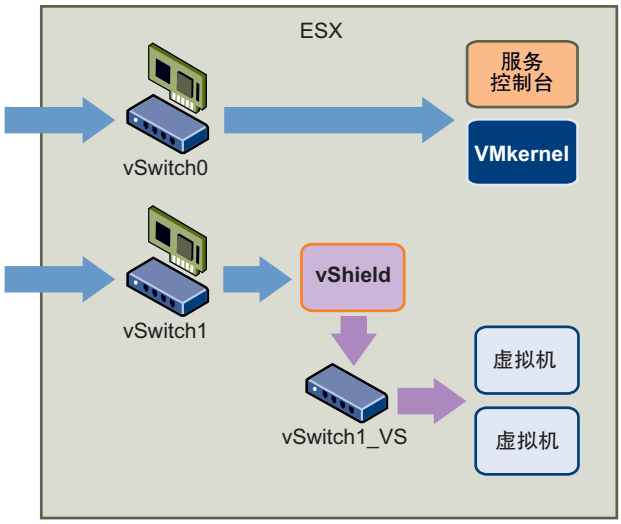
5 连接并启动 vShield 实例。

6 将 vShield 上的虚拟接口分别附加到不受保护和受保护的端口组。

7 将虚拟机从 vSwitch 主机移动到 vSwitch 副本。

如果 vShield Manager 虚拟机驻留在同一 vSwitch 中，则不移动该虚拟机。在 vShield Manager 安装期间，您创建了一个名为 **`vsmgmt`** 的端口组，用于存放 vShield Manager。vShield 安装可识别此端口组名称并忽略此端口组中的任何虚拟机。

图 1. 在 vSwitch 上安装 vShield



安装的每个 vShield 实例将监视 vSwitch 主机上的所有入站和出站流量，其中包括 vSwitch 主机和 vSwitch 副本上的虚拟机之间的流量。当流量通过 vShield 时，将检查各个会话标头以对数据进行分类。对于每个虚拟机，将分别创建一个配置文件，详细说明其操作系统、应用程序和网络通信中使用的端口。基于此信息，vShield 允许使用临时端口，方法是在保持端口 1024 及更高编号的端口处于锁定状态的同时，允许 FTP 和 RPC 这样的动态协议通过。

根据设计，各个 vShield 实例最多允许同时进行 40,000 个会话。

无法使用 vShield 保护服务控制台或 VMkernel，因为这些组件不是虚拟机。

主要功能

vShield Zones 提供了一套丰富的功能，旨在提供有关出入虚拟机的流量的信息并保护虚拟数据中心中的虚拟机。

防火墙保护

vShield Zones 通过在所有部署的 vShield 实例中实施全局和本地访问控制策略提供防火墙保护。 vShield Zones 允许您根据常规流量方向、应用程序协议和端口、特定的源到目标参数来构建防火墙规则。

在 vShield Manager 用户界面中，**[VM Wall]** 选项卡显示 vShield Zones 的防火墙功能。VM Wall 是集中式、层次结构访问控制列表。您可以在数据中心和群集级别上管理 VM Wall 访问规则，从而对这些容器中的多个 vShield 实例提供一致的一组规则。由于这些容器中的虚拟机成员资格可以动态更改，因此 vShield Zones 将保持现有会话的状态，而不要求重新配置访问规则。

默认规则

默认情况下， VM Wall 实施一组用于允许流量通过所有 vShield 实例的规则。这些规则显示在 VM Wall 表的 **[Default Rules]** 部分。无法删除或添加默认规则。但是，您可以将各个规则的**操作**元素从 **[Allow]** 更改为 **[Deny]**。

第 4 层规则和第 2 层 / 第 3 层规则

[VM Wall] 选项卡提供了以下两组可配置规则：L4（ 第 4 层 ）规则和 L2/L3（ 第 2 层 / 第 3 层 ）规则。这些层指的是开放系统互连 (OSI) 参考模型的层。

第 4 层规则管理第 7 层的 TCP 和 UDP 传输，即特定于应用程序的流量。您与 VM Wall 规则的大部分交互都集中在管理第 4 层规则上。

第 2 层 / 第 3 层规则监视 ICMP、ARP 和其他第 2 层和第 3 层协议中的流量。默认情况下，控制第 2 层和第 3 层的 VM Wall 规则允许通过所有流量。仅在数据中心级别下实施第 2 层 / 第 3 层规则。

VM Wall 规则的层次结构

每个 vShield 实例按照从上到下的顺序实施 VM Wall 规则。对于每个流量会话，vShield 首先依据 VM Wall 表中的顶层规则进行检查，然后逐步下移到表中的后续规则。表中第一个与流量参数匹配的规则将被实施。

VM Wall 提供容器级优先和自定义优先顺序两种配置：

- 容器级优先是指认为数据中心级别具有高于群集级别的优先级。配置数据中心级别的规则后，所有群集及其 vShield 实例都将继承此规则。群集级别规则仅适用于群集内的 vShield 实例。
- 自定义优先顺序是指为在数据中心级别创建的规则指定高优先级或低优先级。**数据中心高优先规则**与容器级优先规则的工作方式相同。**数据中心低优先规则**的优先级低于**群集级别规则**，而高于预配置的**默认规则**。这种灵活性使您可以识别应用了优先顺序的多个层。

在 VM Wall 表中，根据以下层次结构实施规则：

1 **数据中心高优先规则**：在数据中心级别创建的优先级最高的一组全局访问规则。

2 **群集级别规则**：优先级低于数据中心高优先规则的一组特定于群集的访问规则。

3 **数据中心低优先规则**：在数据中心级别创建的一组优先级低于群集级别规则的全局访问规则。

4 **默认规则**：优先级最低的一组默认全局访问规则。

作为总的原则，请确保低优先规则与高优先规则不冲突。

规划 VM Wall 规则实施

使用 VM Wall，您可以根据网络策略配置允许和拒绝规则。下列策略表示常用的 VM Wall 配置：

- 保留默认规则以允许所有流量，并根据流量统计信息或手动配置在数据中心级别和群集级别上添加拒绝规则。在此方案中，如果会话不符合任何自定义拒绝规则，则 vShield 允许流量通过。
- 可将默认规则的操作状态从**允许**更改为**拒绝**，并为特定系统和应用程序添加数据中心级别和群集级别的允许规则。在此方案中，如果会话不符合任何自定义允许规则，则 vShield 会在会话到达目标之前丢弃会话。如果您在未创建允许规则的情况下将所有默认规则更改为拒绝所有流量，则 vShield 会丢弃所有入站和出站流量。

流量分析

vShield 检查每个通过的数据包标头来收集有关出入虚拟机的每个会话的信息。会话详细信息包括源、目标、方向和请求的服务。所有部署的 vShield 实例收集的流量数据都汇总在 vShield Manager 用户界面中。

在 vShield Manager 中，**[VM Flow]** 选项卡提供流量分析数据。这些数据中包括会话数以及传输的数据包数和字节数。VM Flow 是一种有用的取证工具，可以检测恶意服务、检查入站和出站会话、创建 VM Wall 访问规则。流量数据还可用于网络故障排除，例如检测服务或客户端的流量高低。

[VM Flow] 选项卡显示数据中心或群集容器内的所有活动 vShield 实例返回的吞吐量统计信息，或单个虚拟机级别的单一 vShield 实例返回的吞吐量统计信息。VM Flow 根据客户端 - 服务器通信中使用的应用程序协议，将统计信息组织在三个图表中显示。图表中的每一种颜色代表一种不同的应用程序协议。使用这种图表方法，您可以跟踪各个应用程序的服务器资源。

默认情况下， VM Flow 显示最近七天内所有检查过的数据流的流量统计信息。

VM Flow 提供每个会话的流量数据综合报告。您可以通过报告数据深入查看特定一对源和目标的统计信息。根据这些数据，您可以创建详细的 VM Wall 允许和拒绝规则。

虚拟机发现

在安装之后，每个 vShield 都会检查所有通过的网络流量，从而构建每个虚拟机上操作系统、应用程序和开放端口的清单。此检查过程称为发现。vShield Manager 在 **[VM Inventory]** 选项卡下显示发现的虚拟机清单。

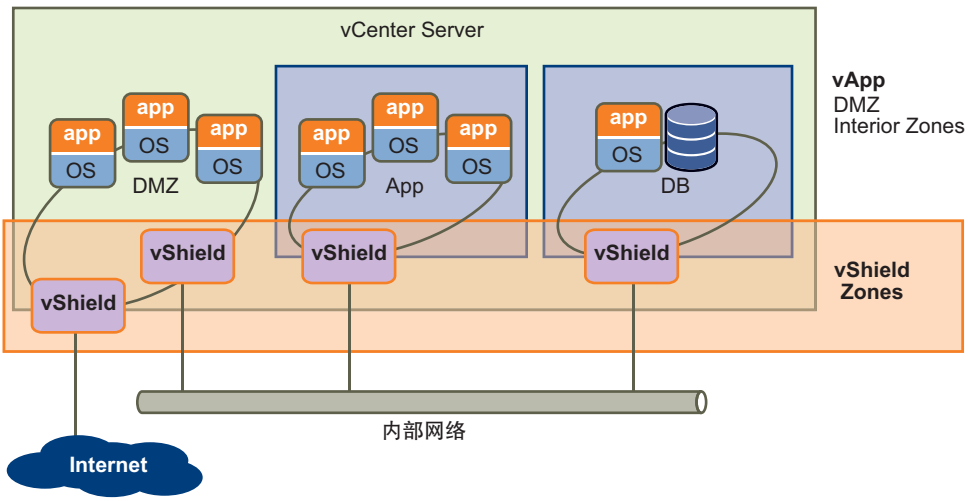
如果 vShield 发现了向不受保护的虚拟机传送的流量，该虚拟机会在 vShield Manager 用户界面的 [inventory] 面板中突出显示为红色。这使您能够快速标识易受到攻击的服务器，并使用新的或现有 vShield 保护它们。被发现过程标识为不受保护的每台虚拟机在 vShield Manager 用户界面的清单面板中显示为红色。这使您能够标识和保护所有虚拟机。

vShield 发现操作还可用于扫描虚拟机，标识可能存在安全风险的开放应用程序。

部署方案

使用 vShield Zones，您可以为各种虚拟机部署构建安全区域。您可以根据特定应用程序、 VLAN 分段或自定义合规性因素隔离虚拟机。确定区域分配策略后，您可以部署 vShield Zones 实施这些区域的访问规则。

图 2. 使用 vShield Zones 保护虚拟网络中的特定区域



保护 DMZ

DMZ 是指混合信任区域。客户端从 Internet 进入以获得 Web 和电子邮件服务，而 DMZ 内的服务可能要求访问内部网络中的服务。要求内部服务的 DMZ 服务的一个常见示例是 Microsoft Exchange。Microsoft Outlook Web Access (OWA) 通常驻留在 DMZ 群集中，而 Microsoft Exchange 后端位于内部群集中。在内部群集上，您可以创建 VM Wall 规则以仅允许来自 DMZ 的 Exchange 相关请求，标识特定的源到目标参数。从 DMZ 群集中，您可以创建规则以使得对于 DMZ 的外部访问仅限于使用 HTTP、 FTP 或 SMTP 协议的特定目标。

隔离 VLAN

如果您利用 VLAN 标记对流量进行分段，则可以使用 VM Wall 创建智能访问策略。使用 VM Wall（而不是物理防火墙），您可以合并或混合共享 ESX 群集中的信任区域。这样，您会从诸如 DRS 和 HA 等功能获得最佳利用率和整合效果，而不是拥有单独的分段群集。将整个 ESX 部署作为单个池来管理比单独管理多个池更为简单。

例如，可根据逻辑、组织或网络边界使用 VLAN 对虚拟机区域分段。利用 Virtual Infrastructure SDK，vShield Manager 清单面板会在 [Networks] 视图下显示 VLAN 网络的视图。您可以为每个 VLAN 网络构建访问规则来隔离虚拟机并丢弃传到这些计算机的未标记流量。

对 VMware View™ 用户进行分段

VMware View 用户也可从 VM Wall 访问策略受益。您可以基于某个方向的（例如，由外到内）流量、动态应用程序（例如 RDP）或其他类似要求创建访问规则，以在不同的 View 端口组之间提供访问控制。例如，您可以创建端口组以根据员工状态（例如，长期工或合同工）隔离用户。然后，您可以使用 VM Wall 规则确定从这些端口组到内部网络的访问方式，以及尝试从虚拟机到达 Internet 时的访问方式。

更多内容

表 1 提供了 vShield Zones 文档参考以及其中包含的任务。

关于所有 VMware 产品的文档位于 Web 上，网址为 http://www.vmware.com/cn/support/pubs。

表 1. 文档

任务	文档
安装 vShield Zones。	《vShield Zones 快速入门指南》
配置、监视和维护 vShield Zones。 在 vNetwork 分布式交换机环境中安装 vShield Zones。	《vShield Zones 管理指南》