McAfee Virtual Network Security Platform

适用于云网络的全面威胁检测方案

McAfee® Virtual Network Security Platform 是一种功能完备的网络威胁和入侵防护系统 (IPS) 解决方案，能够满足私有云、公共云的独特需求。该解决方案准性高，操作简单，能够发现并拦截云架构中的复杂威胁，从而使组织能够恢复合规性，并对云安全充满信心。此解决方案采用无特征码检测、串联模拟和基于特征码的漏洞修补等高级技术，并支持 Amazon Web Services (AWS) 和网络虚拟化。凭借简化的工作流、多种集成技术和简化的产品许可，企业能够轻松地在最复杂的云架构中管理和监控云安全。

采用高级安全技术全面确保公共云安全

公共云使用便捷，不仅能节省成本，还能将基础设施开支转为运营开支模型。但是，公共云使用也带来了全新级别的风险，其中，公共访问软件存在的漏洞能够让攻击者入侵云并泄露敏感信息，或无意中将客户数据泄露给使用相同服务的其他租户。McAfee Virtual Network Security Platform 支持当前领先的公共云服务 AWS，能够对通过 Internet 网关的数据以及东西向通信实施全面威胁监控。利用此解决方案，通过入侵防护系统 (IPS) 平台 (提供准确的东西向通信检测)，能够恢复公共云架构的全面威胁监控和安全合规性。

确保虚拟环境的安全

企业正在迅速采用虚拟化 IT 基础设施 (如私有云和公共云)，其中，物理服务器能够同时托管多台虚拟机 (VM) 甚至整个虚拟工作负载。这会实现虚拟机内部通信，并即时迁移、复制和备份这些工作负载，从而大大增加私有云、公共云和 SDDC 中的东西向通信量。更麻烦的是，网络虚拟化的灵活性导致这些增加的通信量变化莫测、难以捉摸。为了解决这个问题，虚拟化安全解决方案必须具备灵活性和可扩展性，更重要的是，它们必须与用于协调持续时间短的虚拟机和工作负载的软件定义网络 (SDN) 平台无缝协作。

主要优势

无可比拟的高级威胁防护

- 无特征码的高级恶意软件分析。
- 防范跨站点脚本和 SQL 注入。
- 高级僵尸网络回拨和恶意软件检测。
- 基于行为的分析和分布式拒绝服务 (DDoS) 攻击防范。
- 与 McAfee Advanced Threat Defense 集成。
- IPS 和入侵检测系统 (IDS) 部署。
- 常开 VMware ESX-McAfee Virtual Network Security Platform 解决方案。

云就绪架构

- 使用一个许可就能跨公共云和私有云的所有组合共享吞吐量。
- 极富创新性的 AWS 检测法能够真正实现在公共云中保护东西向通信的安全。

提升私有云的敏捷性

McAfee Virtual Network Security Platform 能够与常用私有云平台（包括 VMware NSX 和基于 OpenStack 的 SDN 环境）无缝集成，从而满足确保虚拟化环境安全的需求。事实上，McAfee Virtual Network Security Platform 是通过认证的，唯一能够与 VMware NSX 协作的专用虚拟化 IPS 解决方案。此解决方案能够在虚拟化环境中自动对虚拟机执行微分段，并对东西向通信量进行深入检测，即使快速产生、迁移和废弃工作负载时也能实现。

无可比拟的威胁防御功能

McAfee Virtual Network Security Platform 基于新一代检测架构，专门对虚拟网络流量进行深入分析。它综合运用各种高级检测技术，包括完整协议分析、威胁信誉和行为分析，以及高级恶意软件分析来检测并防御网络上的已知攻击和零日攻击。

任何一项恶意软件检测技术均无法抵御所有攻击，这也正是 McAfee Virtual Network Security Platform 综合运用多个特征码和无特征码检测引擎，以共同防止有害恶意软件破坏云的原因。它提供了多种检测技术，如串联模拟浏览器、JavaScript 和 Adobe 文件，僵尸网络和恶意软件回拨检测，基于行为的 DDoS 检测和防御高级威胁攻击技术（如跨站点脚本和 SQL 注入）。通过与 McAfee Advanced Threat Defense（能够对提交的文件执行深入的行为分析）集成，McAfee Virtual Network Security Platform 还能够识别和拦截最隐匿的恶意文件。McAfee Advanced Threat Defense 将深度静态代码分析、动态分析（恶意软件沙盒）和机器学习相结合，以提高零日威胁检测能力，包括使用规避技术的威胁和勒索软件。

借助云许可证共享简化许可

如今，无论是为了支持旧应用程序，降低对单个供应商、系统冗余的依赖，还是为了节省成本，很多企业都在跨多个云和平台共享 IT 资源和基础设施。由于大多数供应商都需要购买跨私有云和公共云的单独许可证，并用于不同的 SDN 平台，因此，虚拟化环境的许可安全解决方案不仅复杂，而且费用昂贵。

通过云共享，McAfee 不仅能够简化许可，而且能够节省成本。这是一种全新的概念，能够让消费者跨所有公共云和私有云平台组合共享他们的 McAfee Virtual Network Security Platform 的吞吐量和许可证。通过让管理员随时迅速地为东西向通信提供保护以及对虚拟工作负载进行微分段，而不必执行耗时的整个采购流程，云许可证共享还能提高安全性。

- 支持通过 VMware NSX 和基于 OpenStack 的 SDN 环境进行协调，能够自动完成私有云工作负载之间的微分段和通信检测。
- 具有隔离实施功能的 VM 感知信息显示板能够与 VMware 集成。
- 单个集中式管理控制台，用于内部部署和云端物理及虚拟传感器。

智能安全管理

- 单个控制台管理内部部署和云端传感器。
- 智能警报关联和优先排序。
- 强大的恶意软件调查结果信息显示板。
- 预配置的调查工作流程。
- 基于 Web 的可扩展式管理。

可见性和控制性

- 应用程序识别。
- 用户识别。
- 设备识别。
- AWS 中所有 VM 的安全状态。

简化工作流和分析

轻松发现并拦截最复杂的威胁。McAfee Virtual Network Security Platform 具备高级分析功能，而且能与其他安全解决方案集成，从而构建一个真正全面且连接网络的威胁检测和消除平台。

现代威胁能够生成大量警报，很快就会使安全操作员无法对它们进行优先级划分和追踪。如果未及时连接点，真正的威胁就能规避检测。McAfee Virtual Network Security Platform 拥有现成可用的高级分析和切实可行的工作流，能够将多个 IPS 警报与单个可操作性事件关联起来，有助于管理员迅速地透过干扰信息找出相关的可用信息。

通过对实时数据进行实时控制实现集中式管理

一台 McAfee Network Security Manager 设备即可实现基于 Web 的集中管理和无与伦比的易用性。最先进的控制台和加强型图形用户界面让您牢牢掌控实时数据。您可以轻松管理、配置和监控 McAfee Network Security Platform 的所有虚拟或物理设备，以及使用单一控制台管理的跨传统、私有和公共云资源的 McAfee Network Threat Behavior Analysis 设备。基于 Web 的直观管理界面适合进行各种部署——从单一设备直到分布广泛的业务关键群集。McAfee Network Security Manager 还可以在 VMware ESX 服务器上以及 AWS 中作为虚拟实例部署。

高可用性以及灾难恢复

McAfee Network Security Manager 在控制器之间进行仲裁，确定其中一个为激活状态，其余则为待机状态。当激活的控制器变得不可用时，待机控制器将会激活。由此为 AWS 部署提供了控制器高可用性 (HA)，并提供故障转移机制，其中一个控制器始终激活并且可访问。此外，待机 McAfee Network Security Manager 为 AWS 环境提供灾难恢复。

McAfee Virtual Network Security Platform 通过 Manager 灾难恢复 (MDR)、控制器高可用性 (HA) 以及虚拟 IPS 传感器自动扩展功能提供高可用性。这让 McAfee Virtual Network Security Platform 没有中断地无缝工作。MDR 解决方案提供次 Manager，在主 Manager 停机时接管其事务。在控制器 HA 对中，其中一个控制器始终激活并且可访问，从而网络中不会有停机时间。虚拟 IPS 传感器的自动扩展功能在传感器的实例停止时新建虚拟 IPS 传感器。由此一旦网络流量增加，就可执行负载平衡功能。

统一防御架构

复杂攻击没有产品界限，它们会利用所有基础设施的漏洞，尤其是安全产品之间的漏洞。McAfee Virtual Network Security Platform 是唯一跨多个安全产品集成的 IPS，能够利用数据和工作流来填补为了提升投资收益和降低总体拥有成本而造成的漏洞。其他安全产品集成包括：

- **McAfee ePolicy Orchestrator® (McAfee ePO™) 软件：**所有 IPS 事件和警报完全的终端可见性。
- **McAfee Endpoint Intelligence Agent：**综合利用网络和终端来阻止数据泄露。
- **McAfee Enterprise Security Manager：**实现丰富的数据共享和 IPS 警报隔离。

- **McAfee Threat Intelligence Exchange：**跨不同类型的设备共享信息。
- **McAfee Global Threat Intelligence：**全球最大且最活跃的信誉服务。
- **McAfee Network Threat Behavior Analysis：**跨整个网络扩展可视性。
- **McAfee Virtual Advanced Threat Defense**
- **McAfee Cloud Threat Detection**
- **McAfee Management for Optimized Virtual Environments (McAfee MOVE)**
- **第三方安全漏洞扫描程序：**终端的主机和风险分析。

其他功能

高级威胁防护

- McAfee Gateway Anti-Malware 模拟引擎。
- PDF JavaScript 模拟引擎（轻型沙盒）。
- Adobe Flash 行为分析引擎。
- 高级抗逃避防护。

僵尸网络及恶意软件回拨保护

- 域名服务器 (DNS)/域生成算法 (DGA) 快速通量回拨检测。
- DNS Sinkhole。
- 启发式僵尸程序检测。
- 多种攻击关联。
- 命令和控制数据库。

高级入侵防护

- IP 碎片整理和 TCP 流重组。
- McAfee 特征码、用户定义的特征码和开源特征码。
- 主机隔离和速率限制。
- 虚拟环境检测。
- 拒绝服务 (DoS) 和 DDoS 预防。
- 阈值和启发式检测。
- 基于主机的连接限制。
- 基于配置文件的自学习检测。

McAfee Global Threat Intelligence

- 文件信誉。
- IP 信誉。
- 基于地理位置的有限访问权限。
- 基于 IP 地址的访问控制。

产品简介

	传感器类型 1	传感器类型 2	传感器类型 3
平台	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 NSX 6.3 AWS
虚拟 IPS 传感器型号	**IPS-VM100**	**IPS-VM600**	**IPS-VM100-VSS**[1]
虚拟 IPS 部署类型	单机版	单机版	分布式存储库
VMware NSX 支持	否	否	是
AWS 支持	否	否	是
逻辑 CPU 内核数[2]	3	4	3
内存要求[3]	4 GB	6 GB	5 GB
虚拟传感器规格			
最大吞吐量[4]	最高可达 500 Mbps	最高可达 1 Gbps	最高可达 500 Mbps
并行连接数	200,000	600,000	200,000
每秒建立的连接数	6,000	20,000	6,000
支持的 UDP 流数	39,168	254,208	39,168
监控的端口对数	2	3	1[5]
每台传感器的虚拟接口数 (VIDS)	32	100	32
DoS 配置文件数	100	300	100
管理端口	是	是	是
响应端口	是	是	否
部署模式	内部虚拟机检查、物理机到虚拟机检查、物理机到物理机检查、SPAN 端口检查		VMware NSX 内联检查

1.仅供在 VMware NSX 环境中作为插入服务使用。
2.不同版本对虚拟机资源要求可能不同。请参考与该版本对应的文档。
3.同上。
4.在理想测试条件下使用 1518 字节 UDP 数据包测量。
5.进出的虚拟表示。检查密切关注核心层的 VMware NSX。

北京市东城区北三环东路 36 号
北京环球贸易中心 D 座 18 层，100013
电话：8610 8572 2000
www.mcafee.com/cn

McAfee 和 McAfee 徽标、ePolicy Orchestrator，以及 McAfee ePO 是 McAfee, LLC 或其分支机构在美国和/或其他国家/地区的注册商标或商标。其他商标和品牌可能是其各自所有者的财产。Copyright © 2017 McAfee, LLC. 3241_0817
2017 年 8 月