McAfee Virtual Network Security Platform

适用于云网络的功能完备的威胁检测和入侵防护解决方案

McAfee® Virtual Network Security Platform (McAfee vNSP) 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。这种解决方案准确性高，操作简单，能够迅速发现并拦截云架构中的复杂威胁，从而让组织可以更有信心地保护工作负载和恢复合规性。这种解决方案采用了无特征码检测、串联模拟和基于特征码的漏洞修补等高级技术。此外，凭借简单的工作流、灵活的集成选项和简化的许可流程，该解决方案能够允许组织轻松地管理和监管其安全状况，以满足其当前和今后的需求。

功能完备的公共云安全

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 vNSP 支持当前一流的公共云服务 Amazon Web Services (AWS)、Microsoft Azure 及 Oracle Cloud Infrastructure (OCI)，能够对通过 Internet 网关的数据或服务器到服务器（东西向通信量）的数据，实施全面的威胁监控和防护。

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），在这种环境下，物理服务器要同时托管多台虚拟机 (VM) 和虚拟化工作负载。由此产生的 VM 之间的通信以及这些工作负载的即时迁移，复制和备份，联合起来大大增加了私有云、公共云以及软件定义数据中心 (SDDC) 内的东西向通信量。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

- 适用于私有云和公共云（AWS、Azure 和 OCI）的全面防护措施
- 真正有效的东西向通信量保护
- 可实现威胁检测及控制的集中式管理控制台
- 可防范已知和未知威胁的高级检测技术
- 高可用性、灾难恢复，以及可提升性能的负载平衡功能
- 可灵活跨越私有云和公共云的云许可证共享机制
- 可与 McAfee 产品组合集成，保障设备到云的安全
- 可从 AWS Marketplace 获取
- 可从 Azure Marketplace 获取

联系我们

提升私有云的敏捷性

McAfee vNSP 可以与常用的私有云平台（包括 VMware NSX 和基于 OpenStack 的 SDN 环境）无缝集成。McAfee vNSP 是唯一通过认证的能够与 VMware NSX 协作的专用虚拟 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。

高级威胁防护

McAfee vNSP 基于新一代检测架构，专门用于对虚拟网络流量进行深入检测和分析。这种解决方案综合运用了各种高级检测技术，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，进而能够检测并防御网络上的已知和未知的零日攻击。

没有任何一项恶意软件检测技术能独自抵御所有攻击，这也正是 McAfee vNSP 综合运用多个特征码和无特征码检测引擎，以防止有害恶意软件破坏云环境的原因。这种解决方案使用了多种检测技术，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，以及针对跨站点脚本和 SQL 注入等高级威胁攻击的防御技术。

通过与 McAfee Advanced Threat Defense（能够对提交的文件进行行为分析）集成，McAfee vNSP 还可以识别和拦截最隐匿的恶意文件。McAfee Advanced Threat Defense 整合了深度静态代码分析、动态分析（恶意软件沙盒）和**机器学习**技术，可提高零日威胁（包括使用了规避技术的威胁和勒索软件）的检测能力。此外，McAfee 还提供了对 Snort 特征码的原生支持，以检测并防御恶意软件。

灵活的云许可证共享功能

为了支持旧应用程序，降低对单个供应商和系统冗余的依赖，以及节为了省成本，企业通常会跨越多个云和多个平台来共享其 IT 资源和基础设施。由于大多数供应商都要求单独购买私有云、公共云许可证以及不同 SDN 平台的许可证，因此，虚拟化环境的许可证安全解决方案不仅复杂，而且费用昂贵。

通过云许可证共享功能，McAfee 允许各个组织跨任意组合的公共云和私有云平台，共享其 McAfee vNSP 许可证和吞吐量，从而简化了许可流程，并降低了成本。通过云许可证共享功能，管理员能够随时随地且及时快速地为东西向通信量提供保护，并对虚拟工作负载进行微分段，而不必执行复杂的许可流程以及耗时的采购流程，灵活性和安全性由此得以提高。

了解更多信息

- 保护 Amazon Web Services 虚拟网络
- 保护 Microsoft Azure 虚拟网络

简化工作流和分析过程

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。如果响应不及时，真正的威胁就有可能会成功规避检测。McAfee vNSP 拥有高级分析技术和切实可行的工作流，能够将多个 IPS 警报与同一个可操作的事件关联起来，从而有助于管理员迅速找出相关的信息。此外，McAfee vNSP 可以与其他 McAfee 安全解决方案集成，从而构建一个真正全面且相互关联的网络威胁检测与消除平台。

可实时检测和控制威胁的集中式管理平台

一台单独的 McAfee Network Security Manager 设备，就可以实现基于 Web 的实时检测和控制的集中式管理。最先进的控制台允许您通过一个界面来牢牢掌控实时数据。通过这个界面，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，以及传统、私有和公共云环境中的所有 McAfee Network Threat Behavior Analysis 设备。此外，这个直观的界面也同样能够帮助您轻松管理分布广泛的业务关键群集。

McAfee Network Security Manager 还可以在 VMware ESX 服务器以及 AWS 或 Azure 环境中作为虚拟实例部署。McAfee vNSP 支持 AWS Identity and Access Management (IAM)，因此，管理员能够根据分配给特定用户和组的权限，轻松、安全地管理 AWS 服务和资源的访问权限。

高可用性，灾难恢复和负载平衡功能

McAfee vNSP 可通过多种方法，自动实现不间断控制、防护和性能提升。McAfee Network Security Manager 能够主动监控环境，因此具有很高的可用性。如果一台正在运行的控制器突然无法使用，McAfee Network Security Manager 可自动故障转移到备用的控制器，进而实现不间断的数据监测和安全防护。此外，在 AWS、Azure 和 OCI 环境中部署备用的 McAfee Network Security Manager，还有助于灾难恢复。

McAfee vNSP 也能够为 IPS 传感器提供备用。如果某台传感器突然无法使用，自动调节功能便可自动创建一个新的虚拟 IPS 传感器，实现无缝隙、不间断的安全防护。此外，如果网络流量增多，可以通过自动平衡传感器间的负载来确保性能优化，而且还可以自动部署更多传感器，以满足所需的吞吐量。

集成式安全防护

复杂攻击不存在产品界限，它们可以迅速利用所有基础设施的漏洞，尤其是安全产品之间的漏洞。McAfee vNSP 是唯一一个实现了多个安全产品无缝集成的 IPS，能够有效利用各解决方案中的数据和工作流，进而实现卓越的安全防护效果并提高投资回报率。有关 McAfee 安全解决方案集成的示例包括：

- **McAfee ePolicy Orchestrator® (McAfee ePO™) 软件：**面向所有 IPS 事件和警报的全面的终端监控
- **McAfee Endpoint Intelligence Agent：**综合利用网络和终端来阻止数据泄露
- **McAfee Enterprise Security Manager：**可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：**在整个网络范围内扩展监控
- **McAfee Virtual Advanced Threat Defense：**可提供深入检测，以检测各种规避式威胁
- **McAfee Cloud Threat Detection：**这项服务可集成到现有 McAfee 安全解决方案中，以检测高级恶意软件
- **McAfee Management for Optimized Virtual Environments (McAfee MOVE)：**适用于虚拟环境的防病毒解决方案
- **第三方漏洞扫描程序：**可托管终端并进行风险分析

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
- 高级规避保护

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 排除
- 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) 和分布式拒绝服务 (DDoS) 防护
- 支持 Structured Threat Information eXpression (STIX) 的白名单/黑名单增强功能
- 阈值和启发式检测
- 基于主机的连接限制
- Snort 特征码的原生支持
- 基于配置文件的自学式检测

McAfee Global Threat Intelligence

- 文件信誉
- IP 信誉
- 基于地理位置的受限式访问
- 基于 IP 地址的访问控制

	传感器类型 1	传感器类型 2
平台	VMware ESX 5.5/6.0/6.5	AWS Azure OCI 支持 VMware vSphere 6.5 和 NSX 6.3
虚拟 IPS 传感器型号	IPS-VM600	IPS-VM600-VSS
虚拟 IPS 部署类型	单机版	分布式存储库
VMware NSX 支持	否	是
AWS 支持	否	是
Azure 支持	否	是
OCI 支持	否	是
逻辑 CPU 的数量	4	AWS 4、Azure 5
所需内存	7 GB	7 GB
存储	8 GB	8 GB
虚拟传感器规格		
最大吞吐量	最高可达 1 Gbps	最高可达 1 Gbps
监控的端口对数	3	1（监控端口，而非端口对）
每台传感器的虚拟接口数 (VIDS)	100	100
DoS 配置文件数	300	300
管理端口	是	是
响应端口	否	否
部署模式	内部虚拟机检测、物理机到虚拟机检测、物理机到物理机检测、SPAN/串联端口检测	

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