适用于 VMware 的 Cisco NGIPSv

产品概述

行业领先的威胁防御、实时情景感知、全堆叠可视性以及智能安全自动化，利用适用于 VMware 的 Cisco® NGIPSv（Cisco FirePOWER™ 下一代入侵防御系统 [NGIPS] 解决方案的虚拟化产品），您将获得由所有这些功能带来的可靠安全保护。这款高效的入侵防御系统不仅具有可靠的性能，而且总拥有成本也相对较低。它支持通过可选的订用许可证扩展威胁防御能力，添加高级恶意软件防护 (AMP)、应用可视性和可控性，以及 URL 过滤功能。根据世界领先的信息安全研究和咨询公司 NSS Labs 进行的研究所得出的评估结果，Cisco FirePOWER 设备在威胁检测效力、检查的吞吐量和价值方面均为业界树立了标杆。

虚拟化解决方案的优势

服务器虚拟化可带来显著的业务优势，例如降低成本、实现快速部署，以及提高系统可用性。然而，实施虚拟化会造成潜在的安全风险：

- 由于无法检测到拓扑或配置的更改，因此会产生“盲点”。
- 过去由不同团队单独管理的功能（例如网络或安全）如今整合到一起，可能导致配置错误。
- 在没有充分协调或监管的情况下，虚拟机 (VM) 快速激增（即我们常说的虚拟机无序蔓延问题）。

适用于 VMware 的 Cisco NGIPSv 使您能够在虚拟环境中部署思科领先的 NGIPS 解决方案，从而解决虚拟化带来的风险。该虚拟化 NGIPS 能够检查虚拟机之间的流量，并使其更易于在资源可能有限的远程站点部署和管理 NGIPS 解决方案，从而增强对物理和虚拟资产的保护。

在实现虚拟化的同时弥补可视性上的不足

受虚拟网络的动态性质影响，虚拟网络拓扑和个人虚拟化主机配置经常需要更改。遗憾的是，大多数系统管理解决方案均无视这些更改。无论是有意还是无意，如果不正确地执行这些更改，则会导致您的重要处理环境在您不知道的情况下产生安全漏洞。

例如，在同一物理主机上部署两个不同的虚拟网络。一个是生产环境，另一个是包含生产环境源代码的开发环境，如果由于配置错误或意外违反策略，这两个虚拟网络连接到一起，则会造成重大安全风险（但外界很难察觉）。

适用于 VMware 的 Cisco NGIPSv 可针对这些更改发出警报，以便您可以在更改演变为故障之前解决配置错误和策略违反问题。它还能发现并阻止虚拟化网络与各个虚拟机之间的所有恶意流量，从而实现威胁防御。适用于 VMware 的 Cisco NGIPSv 可提供对虚拟化环境的可视性，以便您对处理环境中的这个重要部分进行更好的控制和保护。

更轻松、更广泛地部署保护

物理设备使用的专用硬件虽然对高性能部署（例如数据中心）极具价值，但是却有其他相关成本，而且可能无法满足每个使用案例的要求。物理设备必须被运送到最终位置，某些国际目的地的海关针对硬件具有苛刻的要求，这会造成巨额成本或延迟。物理设备还必须配备机架空间和电源。最后，某些环境有严格的硬件要求（由认证要求或恶劣的运行条件造成）。

由于虚拟设备是基于软件的，因此适用于 VMware 的 Cisco NGIPSv 能够以更低的运营成本满足物理设备无法满足的 NGIPS 部署使用案例要求。它可以：

- 部署在现有硬件中，并且立即开始监控流量。
- 监控不存在 IT 安全资源的位置。
- 监控无法部署物理设备的网段（例如，零售场所，远程办公室）。
- 由于安全分析师可以通过同一 Cisco FireSIGHT™ 管理中心管理物理和虚拟 NGIPS 设备，因此可以保持职责分离。

将支付卡行业 (PCI) 合规性扩大至虚拟环境

PCI 安全标准委员会的虚拟化特别兴趣小组补充的信息“保护虚拟付款系统”，为如何在虚拟环境中实现并保持 PCI 合规性提供了明确指导。新的指导意义深远，并为虚拟化的持卡人数据环境 (CDE) 确定具体安全建议。建议包括：

- 网络安全现在必须专门应用于虚拟环境
- 使用入侵检测系统 (IDS) 或 IPS 监控 CDE 中的关键点是强制性要求（PCI 要求 11.4）
- IDS 和 IPS 工具应该能够监控虚拟网络和虚拟机之间的流量

适用于 VMware 的 Cisco NGIPSv 监控包含持卡人数据或个人身份信息 (PII) 的重要虚拟网络并检查虚拟机之间的流量。它提供与其物理对应设备相同的 NGIPS 控制和保护。Cisco NGIPSv 最多使用 8 个 vCPU 提供检查并支持 VMware ESXi 5.x 平台。

PCI 要求 6.3.2 还要求开发、测试和生产环境必须彼此隔离。适用于 VMware 的 Cisco NGIPSv 有助于符合此要求，因为，如果它看到这些网络之间的任何流量，就会产生警报。

适用于 VMware 的 Cisco NGIPSv 的适用性

- PCI 重要服务器、小型分支机构和远程位置（例如，零售商店）
- 采用分布式 IT 安全组织的机构
- 有硬件限制的环境（例如，移动车辆、军用船、室外部署）
- 有冗长的硬件认证要求的组织
- 有空间限制的环境（在数据中心中保持小机架空间）
- 扩展的实时网络、用户和虚拟机发现
- 实验室或培训网络
- 托管安全服务提供商或云计算环境

系统要求

表 1 显示了适用于 VMware 的 Cisco NGIPSv 的最低要求。

表 1. 系统要求

虚拟机监控程序	VMware ESX 5.0、5.1
CPU	4 vCPU
内存	4 GB
磁盘空间	40 GB
网络接口	最少 2 个 vNIC，最多 10 个 vNIC

保修信息

要查找 Cisco.com 上的保修信息，请访问产品保修页。

订购信息

帮助客户了解需要购买的所有组件或部件，以安装和使用相应产品。有关部件号，请参见表 2。同时，为方便客户，本部分还提供访问思科订购工具的直接链接，并列出部件号。

如需下订单，请转至如何购买。您可以在此处下载软件。

表 2. 订购信息

产品名称	部件号
Cisco FirePOWER 虚拟设备和支持捆绑包	FP-VMW-IPS-BUN
Cisco FirePOWER 虚拟 IPS 和应用 1 年期服务订用	FP-VMW-TA-1Y
Cisco FirePOWER 虚拟 IPS 和应用 3 年期服务订用	FP-VMW-TA-3Y
Cisco FirePOWER 虚拟 IPS、应用和 URL 1 年期服务订用	FP-VMW-TAC-1Y
Cisco FirePOWER 虚拟 IPS、应用和 URL 3 年期服务订用	FP-VMW-TAC-3Y
Cisco FirePOWER 虚拟 IPS、应用和 AMP 1 年期服务订用	FP-VMW-TAM-1Y
Cisco FirePOWER 虚拟 IPS、应用和 AMP 3 年期服务订用	FP-VMW-TAM-3Y
Cisco FirePOWER 虚拟 IPS，应用、AMP 和 URL 1 年期服务订用	FP-VMW-TAMC-1Y
Cisco FirePOWER 虚拟 IPS，应用、AMP 和 URL 3 年期服务订用	FP-VMW-TAMC-3Y
适用于 FirePOWER 虚拟应用的 Cisco AMP 1 年期服务订用	FP-VMW-AMP-1Y
适用于 FirePOWER 虚拟应用的 Cisco AMP 3 年期服务订用	FP-VMW-AMP-3Y
Cisco FirePOWER 虚拟设备 URL 过滤 1 年期服务订用	FP-VMW-URL-1Y
Cisco FirePOWER 虚拟设备 URL 过滤 3 年期服务订用	FP-VMW-URL-3Y

更多详情

有关适用于 VMware 的 Cisco NGIPSv 的更多详情，请访问 http://www.cisco.com/c/en/us/products/security/index.html，或者与您当地的客户代表联系。

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 www.cisco.com/go/offices 中。

美国印刷 C78-733165-00 11/14