VM-SERIES
新一代防火墙

VM-Series 虚拟化新一代防火墙

保护在大范围的公有云、虚拟化和 NFV 环境中部署的应用和数据安全。

- 识别并控制应用，基于用户授予访问权，并阻止已知和未知威胁。
- 利用零信任原则对任务关键的应用和数据进行分段，以改善安全态势，实现合规性。
- 跨物理和虚拟防火墙集中管理策略，以确保一致的安全状态。
- 简化工作流自动化，使安全性与您的云中的变化速度保持同步。

全球的组织都在执行数字化转型计划，通过包含多种公有云、本地虚拟数据中心以及某些情况下作为网络功能虚拟化 (NFV) 组件的安全措施，实现更快、更高效的网络架构。

云、虚拟化和 NFV 技术所带来的好处众所周知，而面临的数据丢失及相关联业务中断的风险仍然是极大的挑战。为保护您的虚拟应用、工作负载和数据，您的组织需要使用能够做到以下几点的云安全产品：

- 使用应用标识来启用分段和白名单。
- 基于需求和用户身份控制对资源的访问。
- 避免恶意软件获取访问权，并在工作负载间横向传播。
- 简化管理并实现完全自动化，从而在虚拟工作负载发生变化时将摩擦和安全策略滞后降至最低。

Palo Alto Networks VM-Series 可提供与我们的硬件设备中相同的新一代防火墙和高级威胁防御功能，从而保护网络到云中的应用和数据安全。

VM-Series：保护所有云

组织正在快速采用多重云架构，作为分担风险和利用不同云供应商的核心竞争力的手段。为确保您在公有云、虚拟数据中心和 NFV 部署中的应用和数据的安全，VM-Series 旨在提供高达 16 Gbps 启用 App-ID 的防火墙性能，其中包含五个型号：

- **VM-50/VM-50 Lite –** 设计为以最少的资源消耗支持 CPU 超额订阅，同时提供高达 200 Mbps 启用 App-ID 的防火墙性能，适用于从虚拟分支机构/客户端设备到高密度、多租户环境的客户场景。
- **VM-100 和 VM-300 –** 已经过优化，可分别提供 2 Gbps 和 4 Gbps 启用 App-ID 的性能，适用于混合云、分段和互联网网关用例。
- **VM-500 和 VM-700 –** 能够提供业界领先的 8 Gbps 至 16 Gbps 启用 App-ID 的防火墙性能，并可在完全虚拟化的数据中心和服务提供商环境中部署为 NFV 安全组件。

VM-Series 主要特色和功能

VM-Series 使用新一代的安全防护功能保护您的应用和数据，此功能可提供应用级别的优越可视性、精确控制和威胁防御。您可以利用自动化功能和集中管理将安全性嵌入到应用开发流程中，确保安全产品与云速度保持一致。

- **凭借应用可视性制定更明智的安全决策：**VM-Series 可提供跨所有端口的应用可视性，意味着您可以获得更多关于云环境的信息，进而快速做出明智的策略决定。
- **用于安全性与合规性的分段/白名单应用：**当今的网络威胁通常会入侵到单个工作站或用户，然后在网络中横向传播，使您的任务关键应用和数据（不论处于什么位置）面临风险。您可以利用分段和白名单策略控制跨不同子网的应用通信，以阻截威胁横向移动并实现法规合规性。
- **防止在允许的应用流中发生高级攻击：**与很多应用类似，攻击可以利用任何端口得以实现，从而造成传统的防御机制失效。VM-Series 允许您使用 Palo Alto Networks Threat Prevention、DNS 安全防护和 WildFire® 恶意软件防御服务提供特定于应用的策略，从而阻截漏洞利用、恶意软件和之前未知的威胁感染您的云。
- **利用基于用户的策略控制应用访问：**与大量用户存储库（例如 Microsoft Exchange、Active Directory® 和 LDAP）集成，使应用白名单与用户身份互为补充，作为控制对应用和数据访问的附加策略元素。共同部署 VM-Series 与面向端点的 Palo Alto Networks GlobalProtect™ 网络安全产品时，VM-Series 支持您将企业安全策略扩展到任何位置的移动设备和用户。
- **通过集中管理实现策略一致性：**利用 Panorama™ 网络安全管理，您可以对跨多个云部署的 VM-Series 防火墙以及自己的物理安全设备进行管理，从而确保策略的一致性和内聚性。丰富的集中日志记录和报告功能提供了对虚拟化应用、用户和内容的可视性。
- **用于托管 Kubernetes 环境的容器保护：**VM-Series 能够保护在 Google Kubernetes® 引擎和 Azure® Kubernetes 服务中运行的容器，并提供与保护 GCP® 和 Microsoft Azure 的业务关键工作负载相同的可视性和威胁防御功能。容器可视性使安全运营团队能够做出明智的安全决策，并更快速地响应潜在事件。Threat Prevention、WildFire 和 URL Filtering 策略可用于保护 Kubernetes 集群免遭已知或未知的威胁。Panorama 允许您在添加或移除 Kubernetes 服务时自动更新策略，确保安全性能够满足不断变化的托管 Kubernetes 环境。
- **自动化安全部署和策略更新：**VM-Series 包含多种管理功能，使您能够将安全性集成到应用开发工作流中。
  - 使用引导自动配置具有工作配置，且已完整许可并订阅的 VM-Series 防火墙，然后连接到 Panorama 进行集中管理。
  - 在工作负载发生更改时自动执行策略更新，使用完全记录的 API 和动态地址组来允许 VM-Series 以可动态推动策略更新的标签形式使用外部数据。
  - 使用原生云提供商模版和服务以及第三方工具（例如 Terraform® 和 Ansible®）实现完全自动化的 VM-Series 部署和安全策略更新。
- **原生云的可扩展性和可用性：**在虚拟或云环境中，可以通过传统的双设备方法或原生云方法来满足可扩展性和可用性要求。在公有云环境中，我们建议使用云服务（例如应用网关、负载均衡器和自动化）来解决可扩展性和可用性问题。

部署灵活性

要进一步了解 VM-Series 支持的公有云和虚拟环境，请参阅以下资源：

公有云

- **面向 Microsoft Azure/AzureStack 的 VM-Series**
- **面向 Amazon Web Services 的 VM-Series**
- **面向 Google Cloud Platform/GKE 的 VM-Series**
- **面向 Oracle Cloud 的 VM-Series**
- **面向 Alibaba Cloud 的 VM-Series**

- 面向 VMware vCloud Air 的 VM-Series

混合云

- 面向 AWS 的 VMware Cloud (VMC) 的 VM-Series

虚拟数据中心/私有云

- 面向 vSphere 的 VMware NSX 的 VM-Series
- 面向 VMware ESXi 的 VM-Series
- 面向 Cisco ACI 的 VM-Series
- 面向 Microsoft Hyper-V 的 VM-Series
- 面向 KVM 的 VM-Series
- 面向 Nutanix (KVM) 的 VM-Series
- 面向 OpenStack 的 VM-Series

免费咨询热线：400 9911 194
网址：www.paloaltonetworks.cn
邮箱：contact_salesAPAC@paloaltonetworks.com

vm-series-summary-specsheet-ds-012919