思科 Cisco Secure Firewall Threat Defense Virtual 简介

思科 Cisco Secure Firewall Threat Defense Virtual（threat defense virtual）将 Cisco 的新一代防火墙功能带到虚拟环境，支持采用一致的安全策略来跟踪物理、虚拟和云环境以及云之间的工作负载。

如今，组织依靠混合使用物理和虚拟控制点来满足其网络安全需求。他们需要灵活地在各种环境中部署不同的物理和虚拟防火墙，同时仍要在分支机构、企业数据中心以及它们之间的所有点都保持一致的策略。从数据中心整合到办公室搬迁、兼并和收购，以及应用需求的季节性高峰，思科的虚拟防火墙产品组合都能帮助您简化安全管理，提供统一策略的便利性和随处部署的灵活性。

思科 Cisco Secure Firewall Threat Defense Virtual 将思科成熟的网络防火墙与 Snort IPS、URL 过滤和恶意软件防御相结合。它在物理、私有和公共云环境中采用一致的安全策略，从而简化了威胁防护。深入了解您的网络，快速检测威胁来源和活动。然后，在攻击影响您的运营之前阻止它们。

Cisco Secure Firewall Threat Defense Virtual 是常用的虚拟化解决方案。通过自动风险排名和影响标志来确定威胁的优先级，从而将资源集中用于需要立即采取行动的事件。许可证的可移植性为从企业内部私有云迁移到公共云提供了灵活性，同时还能在所有设备上保持一致的策略和统一的管理。通过思科智能软件许可，可轻松部署、管理和跟踪虚拟防火墙实例。

- 如何管理 Cisco Secure Firewall Threat Defense Virtual 设备，第 1 页

如何管理 Cisco Secure Firewall Threat Defense Virtual 设备

您可以使用以下选项来管理 Cisco Secure Firewall Threat Defense Virtual 设备：

Cisco Secure Firewall Management Center

如果要管理大量设备或要使用 威胁防御 支持的更复杂的功能和配置，请使用 管理中心（而不是集成的 设备管理器）来配置您的设备。

重要事项 您不能同时使用 设备管理器 和 管理中心 来管理 威胁防御 设备。在启用 设备管理器 集成管理功能后，将无法使用 管理中心 来管理 威胁防御 设备，除非您禁用本地管理功能并重新配置管理功能以使用 管理中心。另一方面，当您向 威胁防御 注册 管理中心 设备时，设备管理器 载入管理服务会被禁用。

注意 目前，思科不提供将 设备管理器 配置迁移到 管理中心 的选项，反之亦然。选择为 威胁防御 设备配置的管理类型时，请考虑这一点。

Cisco Secure Firewall 设备管理器

设备管理器 板载集成的管理器。

设备管理器 是基于 Web 的配置界面，包含在某些 威胁防御 设备上。设备管理器可以配置小型网络最常用软件的基本功能。此产品专为包括一台或几台设备的网络而设计，在这种网络中，无需使用高功率多设备管理器来控制包含许多 威胁防御 设备的大型网络。

注释 有关支持 设备管理器 的 威胁防御 设备的列表，请参阅《Cisco Secure Firewall 设备管理器配置指南》。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。