哪种应用和管理器适合您？

您的硬件平台可以运行两种应用操作系统之一： Cisco Secure Firewall Threat Defense 或 ASA。对于每种应用操作系统，您都可以选择管理器。本章介绍应用操作系统和管理器选项。

应用

您可以在硬件平台上使用以下任一应用：

- 威胁防御— 威胁防御 （此前称为 Firepower Threat Defense） 是下一代防火墙，它将高级状态防火墙、VPN 集中器和新一代 IPS 结合在一起。
- ASA - ASA 是传统的高级状态防火墙和 VPN 集中器。

Cisco 提供 ASA-to-威胁防御 的迁移工具，如果您最初为 ASA，后期要重新映像到 威胁防御，可使用这些工具将 ASA 转换为 威胁防御。

要在 ASA 和威胁防御之间重新映像，请参阅 Cisco Secure Firewall ASA 和 Secure Firewall Threat Defense 重新映像指南。

管理器

威胁防御和 ASA 支持多个管理器。

威胁防御管理器

注释 Secure Firewall 设备管理器 （以前称为 Firepower 设备管理器）在 Cisco Secure Firewall 4200 上不受支持。

表 *1:* 威胁防御管理器

理器	说明
Cisco Secure Firewall Management Center（之前的 Firepower 管理中心）	管理中心 是一个多设备管理器，它在自己的服务器硬件上运行，或者在虚拟机监控程序上作为虚拟设备运行。 对于本地 管理中心，请参阅 使用管理中心部署威胁防御。 对于远程 管理中心，请参阅 使用远程管理中心部署威胁防御。
思科防御协调器 (CDO) 云交付的防火墙管理中心	CDO的 云交付的防火墙管理中心 具有本地管理中心的所有配置功能。对于分析功能，您可以使用云解决方案或本地管理中心。 CDO 还管理其他安全设备，例如 ASA。 请参阅使用CDO部署威胁防御。
Cisco Secure Firewall Threat Defense REST API	威胁防御 REST API 支持自动化直接配置威胁防御。如果您使用 管理中心 或 CDO管理 威胁防御 ，则无法使用此 API。 本指南未涵盖威胁防御 REST API。有关详细信息，请参阅Cisco Secure Firewall Threat Defense REST API 指南。
Cisco Secure Firewall Management Center REST API	管理中心 REST API 允许自动配置 管理中心 策略，随后可将其应用于托管的 威胁防御。该 API 不直接管理 威胁防御。 本指南未涵盖管理中心 REST API。有关详细信息，请参阅Secure Firewall Management Center REST API 快速入门指南。

ASA 管理器

表 *2: ASA* 管理器

理器	说明
CLI	您可以使用 CLI 配置所有 ASA 功能。 本指南不涵盖 CLI。有关详细信息，请参阅 ASA 配置指南。
自适应安全设备管理器 (ASDM)	ASDM 是基于 Java 的设备上管理器，提供完整的 ASA 功能。 请参阅使用 ASDM 部署 ASA。
CDO	CDO 是基于云的多设备管理器。 CDO 还管理其他安全设备，例如 威胁防御。 本指南中不涵盖适用于 ASA 的CDO 。要开始使用 CDO，请参阅 CDO 主页。
Cisco Security Manager (CSM)	CSM 是在自己的服务器硬件上运行的多设备管理器。CSM 不支持管理 威胁防御。 本指南中不涵盖 CSM。有关详细信息，请参阅 CSM 用户指南。

理器	说明
ASA HTTP 接口	使用 HTTP，自动化工具可以通过访问特定格式的 URL 在 ASA 上执行命令。 本指南不涵盖 ASA HTTP 接口。有关详细信息，请参阅 Cisco Secure Firewall ASA HTTP 自动化接口。

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。