# 哪种操作系统和管理器适合您？

您的硬件平台可以运行两种操作系统之一。对于每种操作系统，您都可以选择管理器。本章介绍操作系统和管理器选项。



## 操作系统

您可以在硬件平台上使用 Cisco Secure Firewall ASA 或 Cisco Secure Firewall Threat Defense（之前的 Firepower Threat Defense） 操作系统。

- ASA - ASA 是传统的高级状态防火墙和 VPN 集中器。

  如果您不需要威胁防御的高级功能，或者您需要威胁防御尚未提供的纯ASA功能，则可能需要使用 ASA。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。

- 威胁防御—威胁防御是下一代防火墙，它将高级状态防火墙、VPN 集中器和新一代 IPS 结合在一起。也就是说，威胁防御 拥有最佳的ASA功能，并将其与最佳的新一代防火墙和IPS功能结合起来。

  我们建议使用 威胁防御 而非 ASA，因为它包含 ASA 的大多数主要功能，以及额外的新一代防火墙和 IPS 功能。

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

**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） | 管理中心是一个功能强大的、基于 Web 的多设备管理器，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。如果您需要多设备管理器，并且您需要 威胁防御上的所有功能，则应使用 管理中心 。管理中心 还提供强大的流量和事件的分析与监控功能。<br><br>管理中心 可以从外部（或其他数据）接口而不是标准管理接口来管理 威胁防御。此功能用于远程分支机构部署。<br><br>**注释** 管理中心与其他管理器不兼容，因为管理中心拥有威胁防御配置，不允许绕过管理中心直接配置威胁防御。<br><br>要开始使用管理网络上的管理中心，请参阅使用管理中心部署威胁防御。<br><br>要开始使用远程网络上的 管理中心，请参阅使用远程管理中心部署威胁防御。 |
| Secure Firewall 设备管理器（之前的 Firepower 设备管理器） | 设备管理器是一个基于 Web 的、简化的设备上管理器。由于它是简化的，因此使用 设备管理器 时不支持某些 威胁防御 功能。如果您只管理少量设备，而不需要多设备管理器，应使用 设备管理器。<br><br>**注释** 设备管理器 和 CDO 在 FDM 模式下都能发现防火墙上的配置，因此您可以使用 设备管理器 和 CDO 来管理相同的防火墙。管理中心与其他管理器不兼容。<br><br>要开始使用 设备管理器，请参阅使用设备管理器部署威胁防御。 |
| 思科防御协调器 (CDO) | CDO 提供两种管理模式：<br><br>• （7.2 及更高版本）云交付的管理中心模式，拥有本地管理中心的所有配置功能。对于分析功能，您可以使用云中的 Cisco Secure Cloud Analytics 或本地管理中心。<br><br>• （仅限现有 CDO 用户）可带来简化用户体验的设备管理器模式。此模式仅适用于已在设备管理器模式下使用 CDO 管理 威胁防御 的用户。本指南不介绍该模式。<br><br>由于 CDO 是基于云的，因此在自己的服务器上运行 CDO 不会产生任何开销。CDO 还管理其他安全设备（例如 ASA），因此您可以对所有安全设备使用单一的管理器。<br><br>要开始 CDO 调配，请参阅使用 CDO 部署威胁防御。 |

| 理器 | 说明 |
| --- | --- |
| 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。此 API 可与 设备管理器 和 CDO 同时使用，因为二者都可以发现防火墙上的配置。如果您使用 管理中心 管理 威胁防御，则无法使用此 API。<br>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。<br>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 |
| --- | --- |
| 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。如果您喜欢使用 GUI 胜于 CLI，并且只需管理少量 ASA，应使用 ASDM。ASDM 可以发现防火墙上的配置，因此您还可以将 CLI、CDO 或 CSM 与 ASDM 配合使用。<br>要开始使用 ASDM，请参阅使用 ASDM 部署 ASA。 |
| CLI | 如果您喜欢 CLI 胜过 GUI，应使用 ASA CLI。<br>本指南不涵盖 CLI。有关详细信息，请参阅 ASA 配置指南。 |
| CDO | CDO 是一个简化的、基于云的多设备管理器。由于它是简化的，因此使用 CDO 时不支持某些 ASA 功能。如果您需要一个多设备管理器来提供简化的管理体验，应使用 CDO。由于 CDO 是基于云的，因此在自己的服务器上运行 CDO 不会产生任何开销。CDO 还管理其他安全设备（例如 威胁防御），因此您可以对所有安全设备使用单一的管理器。CDO 可以发现防火墙上的配置，因此您也可以使用 CLI 或 ASDM。<br>本指南中不涵盖 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功能强大的多设备管理器。如果您需要管理大量的 ASA，应使用 CSM。CSM 可以发现防火墙上的配置，因此您也可以使用 CLI 或 ASDM。CSM 不支持管理 威胁防御。<br>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 REST API | 使用 ASA REST API 可自动化 ASA 配置。但是，API 不包括所有 ASA 功能，也不再增强。<br><br>本指南不涵盖 ASA REST API。有关详细信息，请参阅思科 ASA REST API 快速入门指南。 |

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。