使用 Cisco Defense Orchestrator 管理 FDM 管理 设备

- 使用 Cisco Defense Orchestrator 管理 FDM 管理 设备 ， 第 i 页

使用 Cisco Defense Orchestrator 管理 FDM 管理 设备

重要事项 Firepower 设备管理器 (FDM) 支持和功能仅应要求提供。如果您的租户上尚未启用 防火墙设备管理器 支持，则无法管理或部署到 FDM 管理 设备。向支持团队发送请求以启用此平台。通过 TAC 打开提交支持请求

思科防御协调器 CDO 提供对 Firepower 设备管理器 设备的简化管理接口和云访问。FDM 管理 管理员会注意到 FDM 接口和 CDO 接口之间的许多相似之处。我们建立 CDO 的理念是让经理之间尽可能保持一致。

使用 CDO 管理物理或虚拟 FDM 管理 设备的以下方面：

- 载入 FDM 托管的设备
- 设备管理
- 设备升级
- ASA 到 威胁防御 迁移
- 接口管理
- 路由
- 高可用性
- 安全策略
- 提升策略和配置一致性
- 站点间 VPN

使用 Cisco Defense Orchestrator 管理 FDM 管理 设备

- 远程接入 VPN
- 监控网络
- 思科安全分析和日志记录

软件和硬件支持

CDO 支持版本 6.4 及更高版本，可安装在许多不同的设备或虚拟机上。有关详细信息，请参阅 FDM 管理 支持详情。

管理智能许可证

您可以在载入期间或将设备载入到 CDO 后，使用思科智能许可证来许可 FDM 管理 设备。智能许可内置于我们的工作流程中，可从 CDO 接口轻松访问。有关详细信息，请参阅 应用或更新智能许可证。

注释 如果要载入的设备运行的是软件版本 6.4 或 6.5，并且已获得智能许可，则该设备可能已向思科智能软件管理器注册。**您必须先从智能软件管理器取消注册该设备，然后再使用注册密钥将其载入 CDO**。取消注册时，与设备关联的许可证和所有可选许可证将在您的虚拟帐户中释放。

如果要载入的设备运行的是软件版本 6.6 及更高版本，并且已向思科云注册，**则必须先从思科云服务取消注册设备，然后再使用注册密钥将其载入 CDO**。

CDO 用户接口

CDO GUI 和 CLI 接口

CDO 是一种基于 Web 的管理产品，为您提供图形用户界面 (GUI) 和命令行接口 (CLI)，以便一次管理一个或多个设备。

使用 CLI 接口，您可以直接从 CDO 向 FDM 管理 设备发送命令。使用 CLI 宏保存和运行常用命令。有关详细信息，请参阅命令行接口文档和CDO 命令行接口。

API 支持

CDO 提供可使用设备的 REST API 在 FDM 管理 设备上执行高级操作的 API 工具接口。此外，此接口还提供以下功能：

- 记录已执行的 API 命令的历史记录。
- 提供可重复使用的系统定义的 API 宏。
- 允许使用标准 API 宏、已执行的命令或其他用户定义的宏创建用户定义的 API 宏。

有关 API 工具的详细信息，请参阅使用 API 工具。

使用 Cisco Defense Orchestrator 管理 FDM 管理 设备

载入 FDM 管理 设备

在载入 FDM 托管的设备之前，请查看一般设备要求和载入必备条件。

最佳实践是使用注册令牌来载入 FDM 管理 设备。有关详细信息，请参阅使用注册密钥载入运行软件版本 6.6+ 的 FDM 托管设备。

您还可以使用以下其他方法将 FDM 管理 设备载入 CDO：

- 使用用户名、密码和 IP 地址载入 FDM 管理 设备
- 使用设备的序列号载入已配置的 FDM 托管设备
- 使用低接触调配载入 FDM 管理 设备的工作流程和必备条件

设备管理

使用 CDO 为 FDM 管理 设备升级软件、配置高可用性并配置设备设置和网络资源。

- **系统设置**。获得 FDM 管理 设备的许可并将其载入后，即可完全从 CDO 管理 FDM 管理 设备设置。您将能够配置管理访问协议、日志记录设置、DHCP 和 DNS 服务器交互、设备的主机名、设备使用的时间服务器以及 URL 过滤首选项。
- **安全数据库更新**。让您的设备保持最新状态并符合当前的安全数据库更新要求，以便在必要时检查和更新您的设备。
- **高可用性**。使用 FDM 管理 高可用性页面管理 HA 配置和操作。

设备升级

使用以下方法之一对 FDM 管理 设备执行即时升级或安排升级：

- 升级单个 FDM 管理 设备。
- 升级多个 FDM 管理 设备。
- 升级 FDM 管理 HA 对。

ASA 到 威胁防御 迁移

CDO 可帮助您将自适应安全设备 (ASA) 迁移到 FDM 管理 设备。CDO 提供了一个向导来帮助您将 ASA 的运行配置的这些元素迁移到 防火墙设备管理器 模板：

以下元素支持此迁移：

- 访问控制规则 (ACL)
- 接口
- 网络地址转换 (NAT) 规则
- 网络对象和网络组对象
- 路由

使用 Cisco Defense Orchestrator 管理 FDM 管理 设备

- 服务对象和服务组对象
- 站点间 VPN

有关详细信息，请参阅将 ASA 配置迁移到 FDM 模板。

接口管理

您可以使用 CDO 配置和编辑 FDM 管理 设备上的数据接口或管理/诊断接口。

路由

所谓路由是指通过网络将信息从源发送到目标的活动。路由涉及两个基本活动：确定最佳路由路径和通过网络传输数据包。使用 CDO 配置路由的以下方面：

- **配置静态路由和默认路由**。使用 CDO，您可以为 FDM 管理 设备定义默认路由和其他静态路由。
- **网桥组支持**。网桥组是将一个或多个接口分组的虚拟接口。对接口分组的主要原因是创建一组交换接口。使用 CDO，您可以在设备上配置和编辑网桥组。
- **NAT（网络地址转换）**。NAT 规则有助于将流量从内部（专用）网络路由到互联网。NAT 规则还可以对网络外部的环境隐藏内部 IP 地址，从而发挥安全作用。您可以使用 CDO 创建和编辑设备的 NAT 规则。有关详细信息，请参阅网络地址转换。

安全策略

安全策略检查网络流量，最终目标是允许网络流量到达或阻止网络流量到达其预定目的地。使用 CDO 管理设备的所有组件：

- **复制并粘贴规则**。通过将规则从策略复制并粘贴到另一个策略，可以轻松地跨策略共享规则。有关详细信息，请参阅复制 FDM 访问控制规则。
- **SSL 解密策略**。某些协议（如 HTTPS）使用安全套接字层 (SSL) 或其后续版本传输层安全性 (TLS) 来加密流量以进行安全传输。由于系统无法检查加密连接，因此，如果要应用可考虑借助更高层流量特性进行访问决策的访问规则，则必须应用 SSL 解密策略将其解密。有关详细信息，请参阅 FDM 管理 SSL 解密策略。
- **身份策略**。使用身份策略从连接中收集用户身份信息。然后，可以在控制面板中基于用户身份查看使用情况，并根据用户或用户组配置访问控制。
- **安全情报策略**。通过安全情报策略能够根据源/目标 IP 地址或目标 URL 提前丢弃非必要流量。在使用访问控制策略评估列入受阻列表的流量前，系统会将其丢弃，从而减少系统资源的使用量。
- **访问控制策略**。访问控制策略通过根据访问控制规则评估网络流量来控制对网络资源的访问。Firepower 设备管理器 会按照访问控制规则在访问控制策略中的显示顺序，将其与网络流量进行比较。当访问控制规则中的所有流量条件都匹配时，Firepower 设备管理器 将执行规则定义的操作。您可以使用 CDO 来配置访问控制策略的所有方面。

使用 Cisco Defense Orchestrator 管理 FDM 管理 设备

- TLS 1.3 安全身份发现。此功能在版本 6.7 中引入，允许您对使用 TLS 1.3 加密的流量执行 URL 过滤和应用控制。有关详细信息，请参阅 Firepower 威胁防御中的 TLS 服务器身份发现。
- **入侵策略**。思科通过 Firepower 系统提供多种入侵策略。这些策略由思科 Talos 安全情报和研究小组设计，他们设定了入侵和预处理器规则的状态和高级设置。入侵策略是访问控制规则的方面。有关详细信息，请参阅 FDM 访问控制规则中的入侵策略设置。

注释 Snort 3 适用于运行版本 6.7 及更高版本的 FDM 管理 设备。请注意，您可以随意在 Snort 2 和 Snort 3 之间切换，但存在配置不兼容的风险。有关 Snort 3、支持的设备和软件以及任何限制的详细信息，请参阅升级到 Snort 3.0。

- **威胁事件**。威胁事件是在匹配思科 Talos 的入侵策略后已丢弃或已生成警报的流量的报告。在大多数情况下，无需调整 IPS 规则。如有必要，您可以选择通过更改 CDO 中的匹配规则操作来覆盖事件的处理方式。CDO 支持 6.4 和 6.6.1 的所有版本上的 IPS 规则调整。CDO 不支持任何版本 6.5、除 6.6.1 以外的任何 6.6 版本或任何 6.7 版本上的 IPS 规则调整。
- **NAT（网络地址转换）**。NAT 规则有助于将流量从内部（专用）网络路由到互联网。NAT 规则还可以对网络外部的环境隐藏内部 IP 地址，从而发挥安全作用。您可以使用 CDO 来创建和编辑 Firepower 威胁防御的 NAT 规则。

提升策略和配置一致性

对象管理

对象是可在一个或多个安全策略中使用的信息容器。对象使保持策略一致性变得容易，因为您可以修改对象，而该更改会影响使用该对象的所有其他策略。如果没有对象，则需要单独修改需要进行相同更改的所有策略。

使用 CDO 创建和管理以下对象类型：

- Active Directory 领域
- AnyConnect 客户端配置文件
- 应用过滤器
- 证书
- DNS 组
- 地理位置
- 身份源
- IKEv1 策略
- IKEv1 IPSec 提议

使用 Cisco Defense Orchestrator 管理 FDM 管理 设备

- IKEv2 策略
- IKEv2 IPSec 提议
- 网络
- RA VPN 组策略
- 安全区
- 服务
- 安全组标签
- 系统日志服务器
- URL

解决对象问题

CDO 将多台设备上使用的对象称为“共享对象”，并在“对象”页面中使用此标记 进行标识。有时，共享对象会产生一些“问题”，并且不再在多个策略或设备之间完美共享。通过CDO，您可以轻松 解决重复对象问题、解决未使用的对象问题和 解决不一致的对象问题，从而管理您的设备和对象存储库。

模板

Firepower 设备管理器 模板是已载入的 FDM 管理 设备配置的完整副本。然后，您可以修改该模板并使用它来配置您管理的其他 FDM 管理 设备。Firepower 设备管理器 模板可促进设备之间的策略一致性。有关详细信息，请参阅 FDM 模板。

高可用性

通过 CDO，可以轻松配置和管理高可用性对 FDM 托管设备。您可以载入现有的 HA 对，也可以在 CDO 中创建 HA 对。HA 配置使得在设备可能不可用的情况下（例如在升级期间或设备意外故障期间）维护网络安全成为可能；在故障切换模式下，备用设备已配置为主用设备，这意味着即使其中一台 HA 设备不可用，另一台设备也会继续处理流量。

您可以在 CDO 中升级 FDM 管理 高可用性对。有关详细信息，请参阅升级 FDM 管理 高可用性对。

配置虚拟专用网络

站点间 VPN

虚拟专用网络 (VPN) 由多个远程对等体组成，这些对等体通过不安全的网络相互传输私有数据，从而实现网络到网络的连接。CDO 使用隧道将数据包封装在正常 IP 数据包中，以便通过基于 IP 的网络转发，使用加密来确保隐私，并使用身份验证来确保数据完整性。有关详细信息，请参阅站点间 VPN。

有关虚拟专用网络的其他信息，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》。

使用 Cisco Defense Orchestrator 管理 FDM 管理 设备

远程接入 VPN

远程访问 (RA) VPN 允许个人使用受支持的笔记本电脑、台式机和移动设备与您的网络建立安全连接。CDO 提供直观的用户界面，供您在 FDM 管理 设备上设置 RA VPN。AnyConnect 是终端设备上通过 RA VPN 连接 FDM 管理 设备的唯一受支持客户端。

CDO 支持 FDM 管理 设备上的 RA VPN 功能的以下方面：

- 传输层安全 (TLS) 或数据报传输层安全 (DTLS)，用于实现隐私、认证和数据完整性
- 基于 SSL 客户端的远程访问
- IPv4 和 IPv6 寻址
- 跨多台 FDM 管理 设备共享 RA VPN 配置

有关详细信息，请参阅 RA VPN。有关虚拟专用网络的其他信息，请参阅 适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南。

监控网络

CDO 提供总结安全策略的影响的报告，以及查看这些安全策略触发的显着事件的方法。CDO 还会记录您对设备所做的更改，并为您提供一种标记这些更改的方法，以便您可以将您在CDO中所做的工作与帮助请求或其他操作请求相关联。

“执行摘要”报告

执行摘要报告显示操作统计信息的集合，例如加密流量、拦截的威胁、检测到的 Web 类别等。当网络流量触发 FDM 管理 设备上的访问规则或策略时，会生成报告中的数据。我们建议启用恶意软件和 许可证，并为访问规则启用文件日志记录，以允许设备生成反映在报告中的事件。

阅读FDM管理执行摘要报告，了解有关报告内容以及如何使用它来改进网络基础设施的详细信息。要创建和管理报告，请参阅管理报告。

思科安全分析和日志记录

思科安全分析和日志记录允许您从所有 FDM 管理 设备捕获连接、入侵、文件、恶意软件和安全情报事件，并在 CDO 中的一个位置进行查看。

事件存储在思科云中，可从CDO中的“事件日志记录”页面查看，您可以在其中过滤和查看事件，以便清楚地了解在网络中触发的安全规则。**日志记录和故障排除** 软件包为您提供这些功能。

使用 **防火墙分析和监控** 软件包，系统可以将安全云分析动态实体建模应用于 FDM 管理 设备事件，并使用行为建模分析生成安全云分析观察结果和警报。如果您获取**全部网络分析和监控** 软件包，则系统会对 FDM 管理 设备事件和网络流量应用动态实体建模，并生成观察结果和警报。您可以使用思科单点登录从CDO交叉启动为您调配的安全云分析门户。有关详细信息，请参阅思科安全分析和日志记录。

变更日志

变更日志 会持续捕获在 CDO 中进行的配置更改。此单一视图包括所有受支持设备和服务的更改。以下是更改日志的一些功能：

使用 Cisco Defense Orchestrator 管理 FDM 管理 设备

- 并排比较对设备配置所做的更改
- 所有更改日志条目的纯英文标签。
- 记录设备的自行激活和删除。
- 检测在 CDO 之外发生的策略更改冲突。
- 回答事件调查或故障排除期间的人员、内容和时间。
- 可以将完整更改日志或仅一部分下载为 CSV 文件。

更改请求管理

变更请求管理允许您将在第三方故障单系统中打开的变更请求及其业务理由与变更日志中的事件相关联。使用更改请求管理在CDO中创建更改请求，使用唯一名称进行标识，输入更改说明，并将更改请求与更改日志事件相关联。您可以稍后在更改日志中搜索更改请求名称。

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。