通过FDM配置和测试AMP文件策略

目录

简介

本文档介绍如何通过Firepower设备管理器(FDM)配置和测试高级恶意软件防护(AMP)文件策略。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower设备管理器(FDM)
- Firepower Threat Defense (FTD)

使用的组件

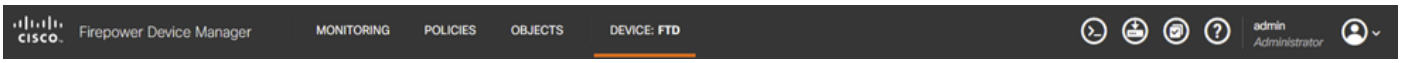
- 通过FDM管理的思科虚拟FTD版本7.0
- 评估许可证(评估许可证用于演示目的。思科建议获取和使用有效的许可证)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

说明

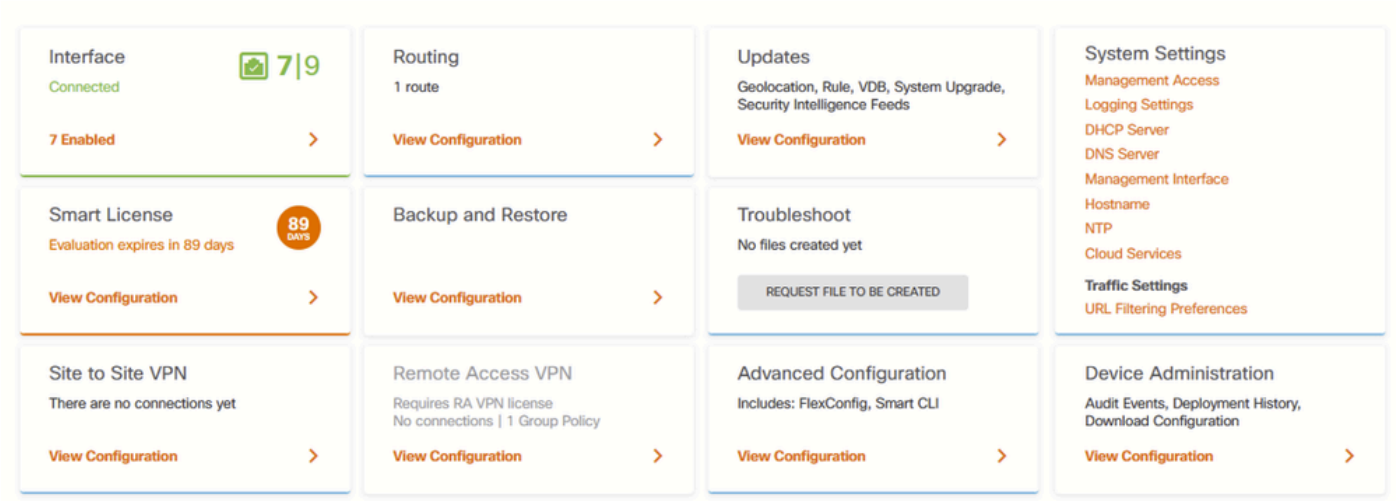
许可

1. 要启用恶意软件许可证，请导航到FDM GUI上的设备页。



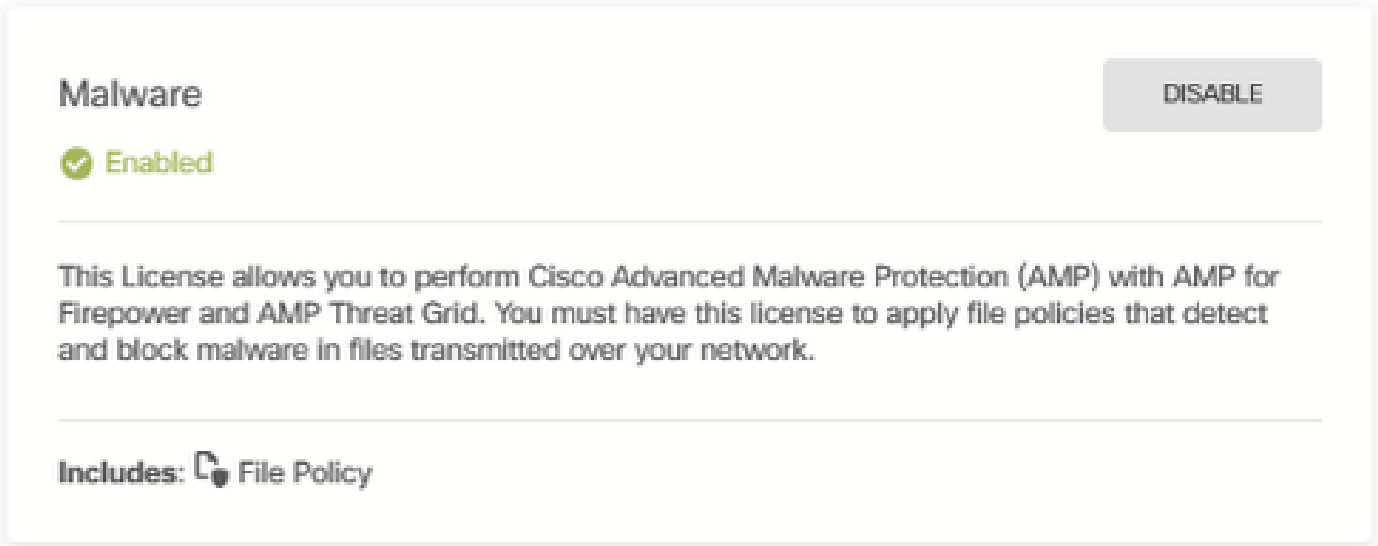
FDM设备选项卡

2. 找到标记为智能许可证的框，然后单击查看配置。



“FDM设备”页

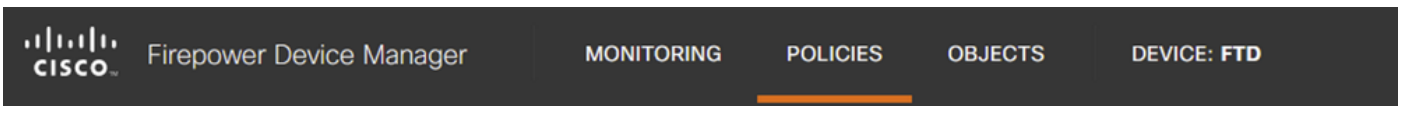
3. 启用标记为Malware的许可证。



恶意软件许可证

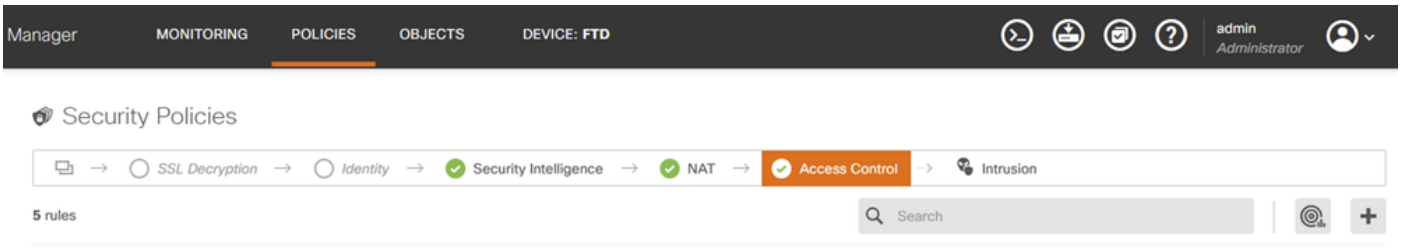
配置

1. 导航到FDM上的“策略”页。



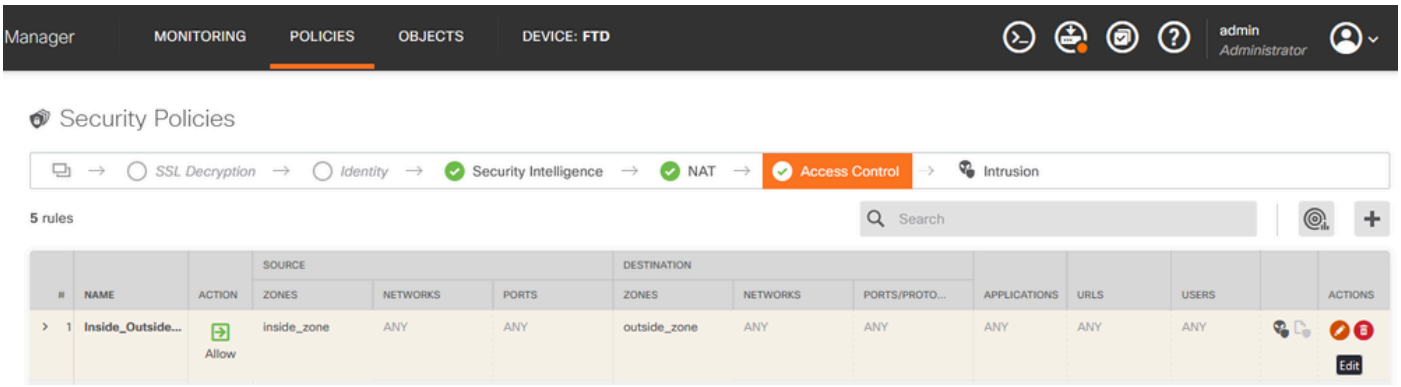
“FDM策略”选项卡

2. 在安全策略下，导航到访问控制部分。



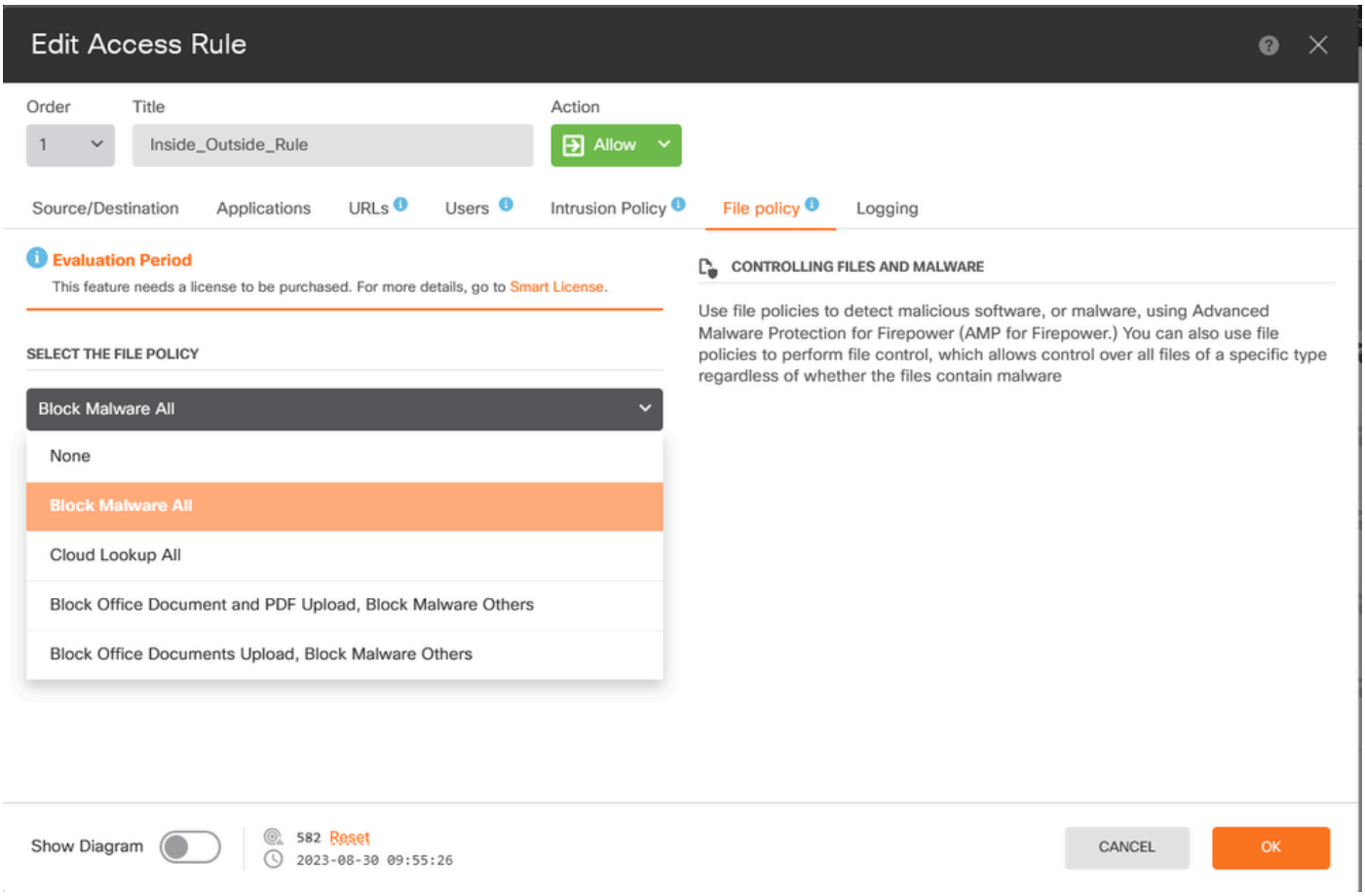
"FDM访问控制"选项卡

3. 查找或创建访问规则以配置文件策略。点击访问规则编辑器。有关如何创建访问规则的说明，请参阅此链接。



FDM访问控制规则

4. 单击访问规则上的文件策略部分，然后从下拉菜单中选择首选的文件策略选项。点击确定，保存规则更改。



FDM访问控制规则文件策略选项卡

5. 通过检查文件策略图标是否已启用，确认文件策略已应用于访问规则。

文件

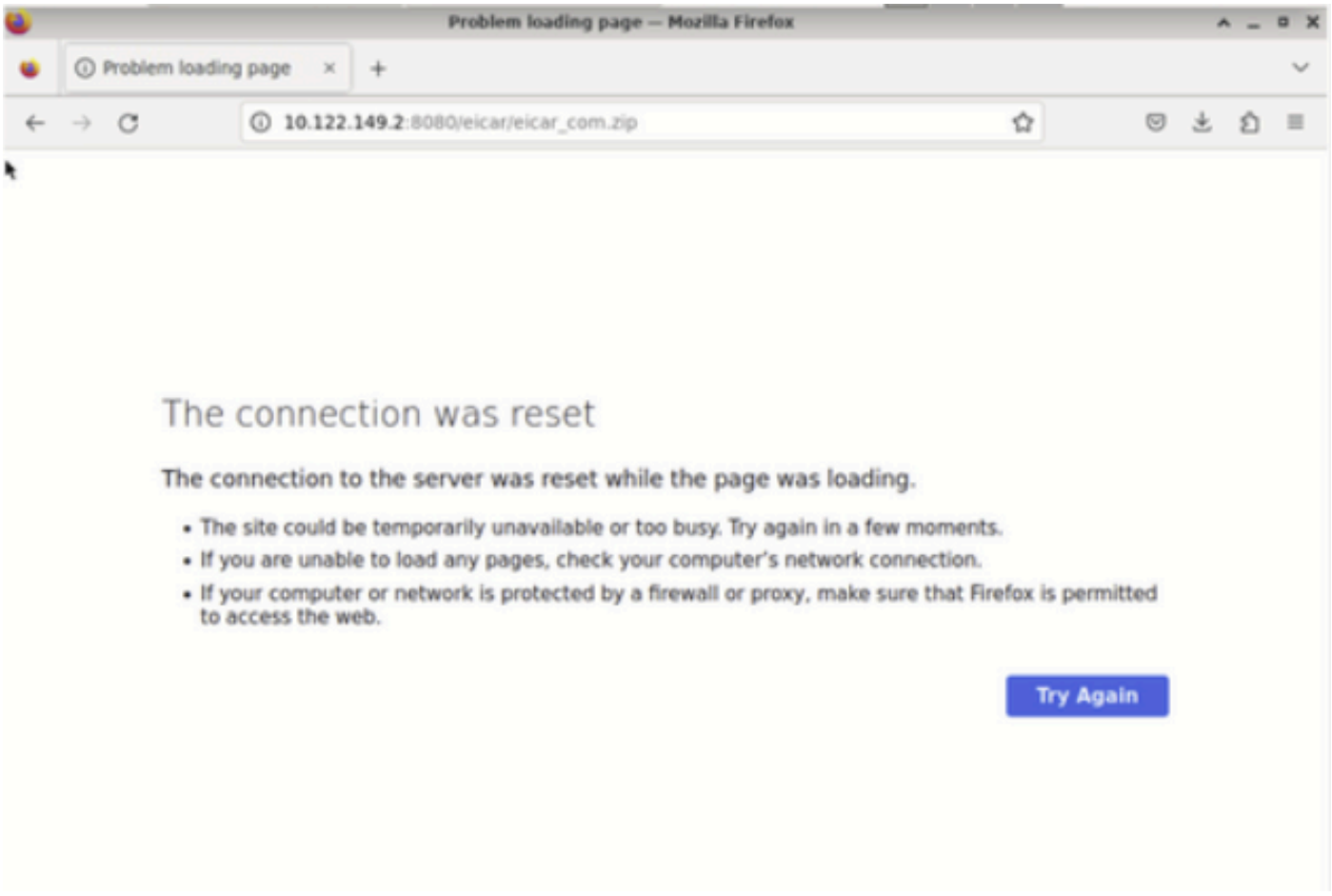
文件策略图标已启用

6.保存并部署对受管设备的更改。

测试

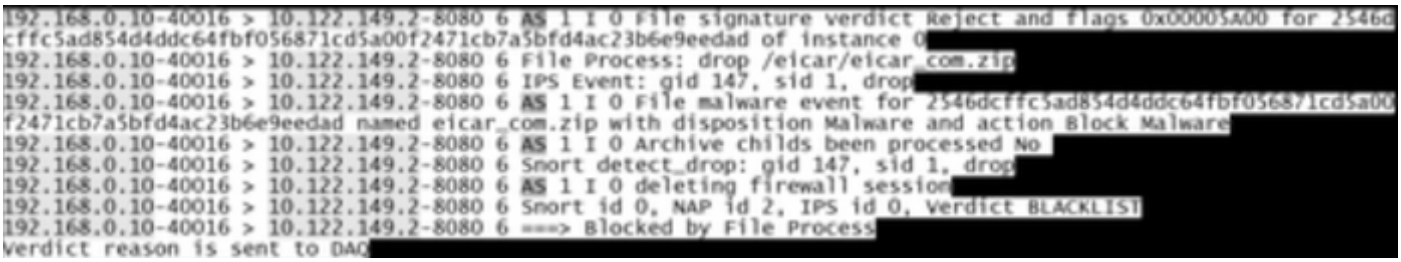
要验证用于恶意软件防护的配置文件策略是否正常工作，请使用以下测试方案尝试从终端主机的Web浏览器下载恶意软件测试文件。

如屏幕截图所示，尝试从Web浏览器下载恶意软件测试文件不会成功。



浏览器下载测试

从FTD CLI中，系统支持跟踪显示文件下载已被文件进程阻止。有关如何通过FTD CLI运行系统支持跟踪的说明，请参阅此链接。



系统支持跟踪测试

这确认文件策略配置已成功阻止恶意软件。

故障排除

如果使用上述配置时未成功阻止恶意软件，请参阅以下故障排除建议：

1. 验证恶意软件许可证未过期。

2. 确认访问控制规则的目标流量是否正确。

3. 确认选定文件策略选项对于目标流量和想要的恶意软件防护是正确的。

如果问题仍无法解决，请联系Cisco TAC获取其他支持。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。