配置网络AMP的Firepower有ASDM的模块或文件控制。

目录

简介

本文描述Firepower模块和方法的网络提前的恶意软件保护(AMP) /file访问控制功能用可适应安全设备管理器(ASDM)配置他们。

先决条件

要求

Cisco 建议您了解以下主题：

- 可适应安全工具(ASA)防火墙和ASDM的知识。
- Firepower设备知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本5.4.1的ASA Firepower模块(ASA 5506X/5506H-X/5506W-X， ASA 5508-X， ASA 5516-X)及以后。
- ASA Firepower模块(ASA 5515-X， ASA 5525-X， ASA 5545-X， ASA 5555-X)该运行软件版本6.0.0及以后。
- ASDM 7.5.1及以后。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

恶意的软件/恶意软件在组织网络能输入通过多种方式。为了识别和减轻此恶意的软件和恶意软件的作用， Firepower的AMP功能可以用于为了检测和或者阻塞恶意的软件和恶意软件发射在网络。

使用文件控制功能，您能选择监控(检测)，阻塞或者允许文件加载和下载转移。例如，由用户阻塞可执行文件下载的文件策略可以实现。

使用网络AMP功能，您能选择您希望在常用的协议监控，并且发送SHA 256切细的文件类型，文件的元数据从文件，甚至复制到恶意软件分析的Cisco安全智能Cloud。Cloud文件的回归处理切细如根据文件分析的干净或有恶意。

作为您的整体访问控制配置一部分，文件控制和AMP Firepower的可以配置作为文件策略和使用。文件策略关联与访问控制规则检查网络流量符合规则情况。

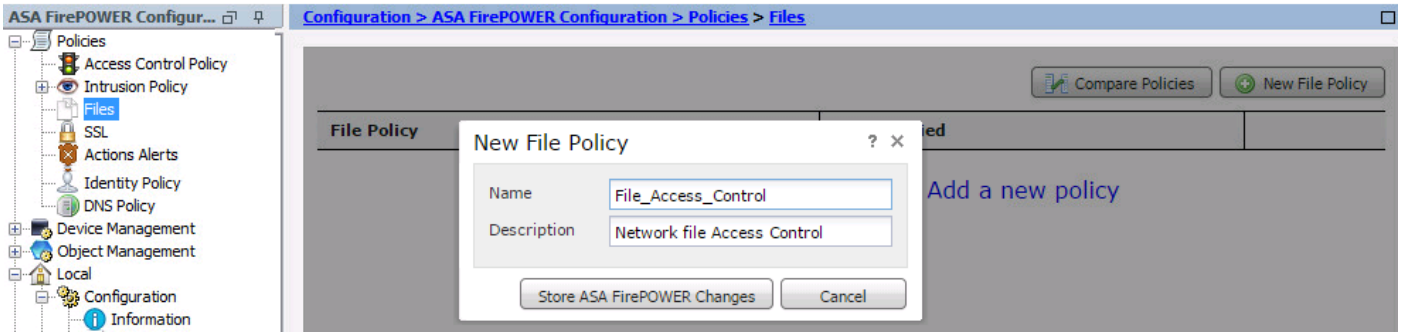
> **Note**:保证Firepower模块有一个保护/控制/恶意软件许可证为了配置此功能。为了验证许可证，请选择**Configuration> ASA Firepower Configuration>许可证。**

配置文件控制/network AMP的文件策略

配置文件访问控制

登陆对ASDM并且选择**Configuration> ASA Firepower Configuration>策略>文件。 新的文件策略**对话框出现。

输入一个名称和可选说明您新的策略的，然后点击**存储ASA Firepower更改**选项。文件策略规则页出版。



单击**增加文件规则**为了增加规则到文件策略。文件规则给您对您要为恶意软件记录，阻塞或者扫描的文件类型的粒状控制。

应用程序协议： 指定应用协议作为其中**任一**(默认)或特定协议(HTTP、SMTP， IMAP， POP3， FTP， SMB)。

转移的方向：指定文件传输的方向。它能是其中任一或根据应用协议的加载/下载。您能检查协议(HTTP， IMAP， POP3， FTP， SMB)文件下载的和协议(HTTP， SMTP， FTP， SMB)文件加载

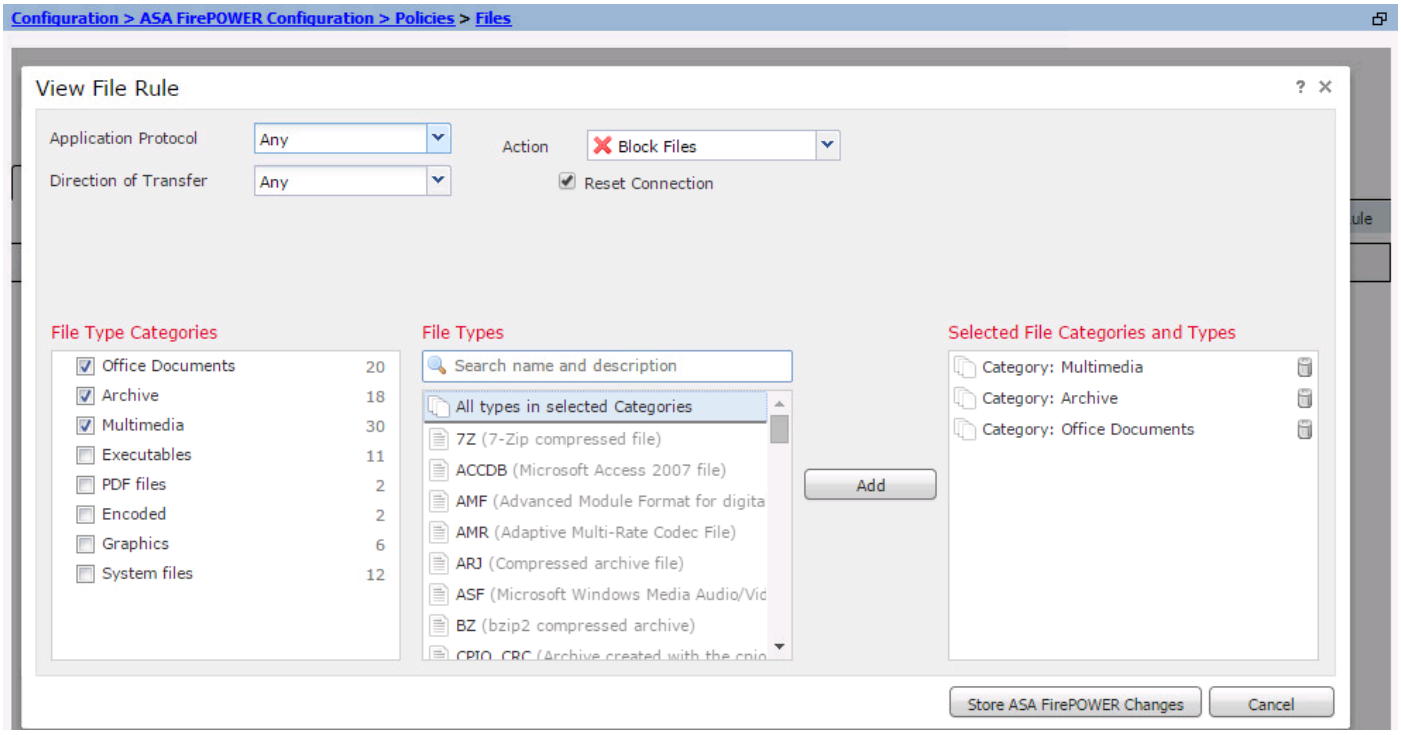
的。请使用**所有**选项为了检测在多个应用程序协议的文件，不管用户是否发送或接收文件。

操作：指定文件访问控制功能的操作。操作是**检测文件**或**块文件。 检测文件**操作生成事件，并且**块文件**操作生成事件并且阻塞文件发送。使用**块文件**操作，您能或者选择**重置连接**终止连接。

文件类型类别： 选择您希望到块文件或生成警报的文件类型类别。

文件类型：选择文件类型。文件类型选项给一更加粒状的选择的选项特定文件类型。

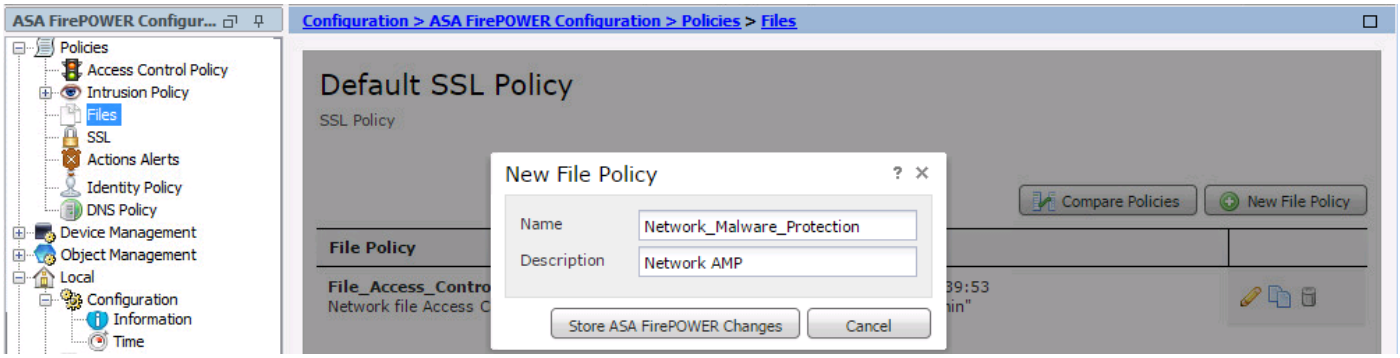
选择**存储ASA Firepower更改**选项保存配置。



Configure network恶意软件保护(网络AMP)

登陆对ASDM并且导航到**Configuration> ASA Firepower Configuration>策略>文件。** 文件策略页出版。现在请单击新的文件策略对话框出现。

输入一个**名称**和可选说明您新的策略的，然后点击**存储ASA Firepower更改**选项。文件策略规则页出版。



单击**添加文件规则**选项添加规则对文件策略。文件规则给您对您要为恶意软件记录，阻塞或者扫描的文件类型的粒状控制。

应用程序协议： 指定其中任一(默认)或特定协议(HTTP、SMTP， IMAP， POP3， FTP， SMB)

转移的方向：指定文件传输的方向。它能是其中任一或根据应用协议的加载下载。您能检查协议(HTTP， IMAP， POP3， FTP， SMB)文件下载的和协议(HTTP， SMTP， FTP， SMB)文件加载的。请使用**所有**选项检测在多个应用程序协议的文件，不管发送或接收文件的用户。

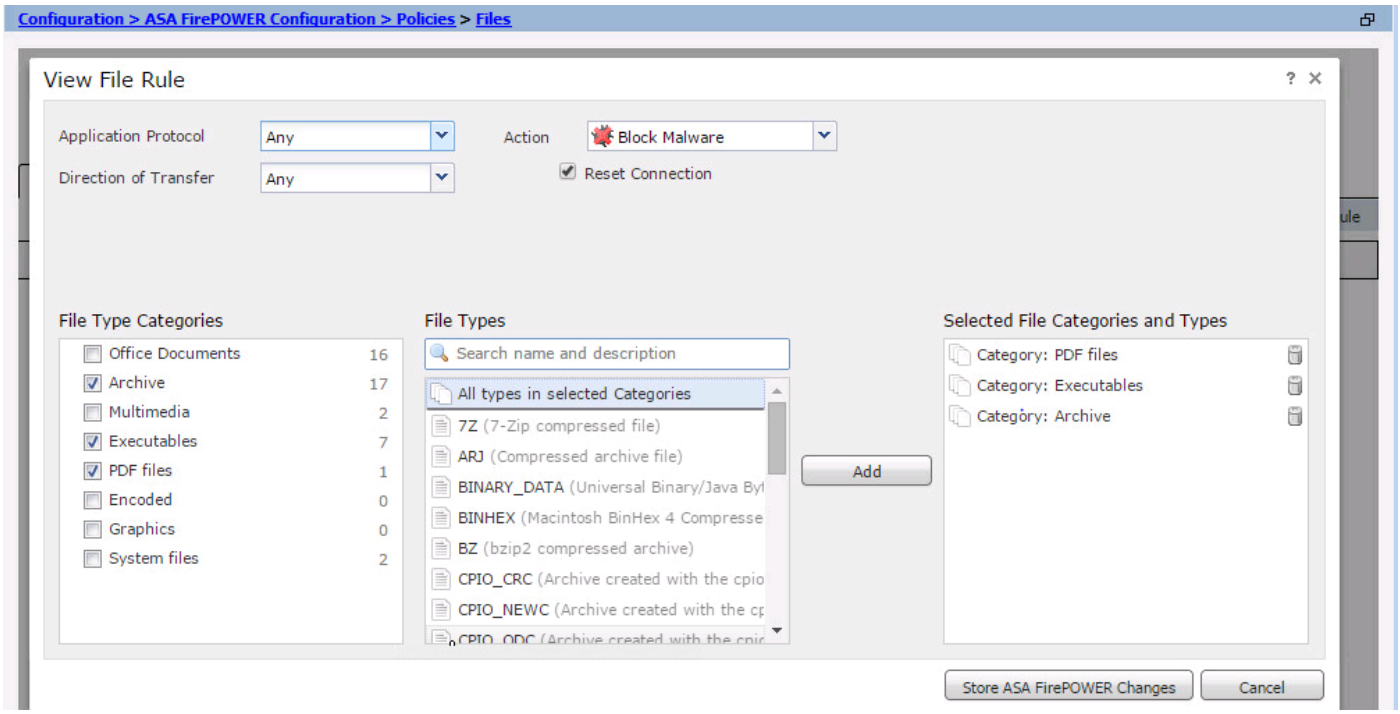
操作：对于网络恶意软件保护功能，操作是**恶意软件Cloud查找**或**阻塞恶意软件。** 操作**恶意软件Cloud查找**生成仅事件，而操作**块恶意软件**生成事件以及阻塞恶意软件文件发送。

> Note:**恶意软件Cloud查找**andBlock**恶意软件**规则允许Firepower计算SHA-256哈希和发送它为了网云查找进程能确定穿程网络的文件是否包含恶意软件。

文件类型类别： 选择特定文件类别。

文件类型： 选择更加粒状的文件类型的特定**文件类型**。

选择选项**存储ASA Firepower更改**保存配置。

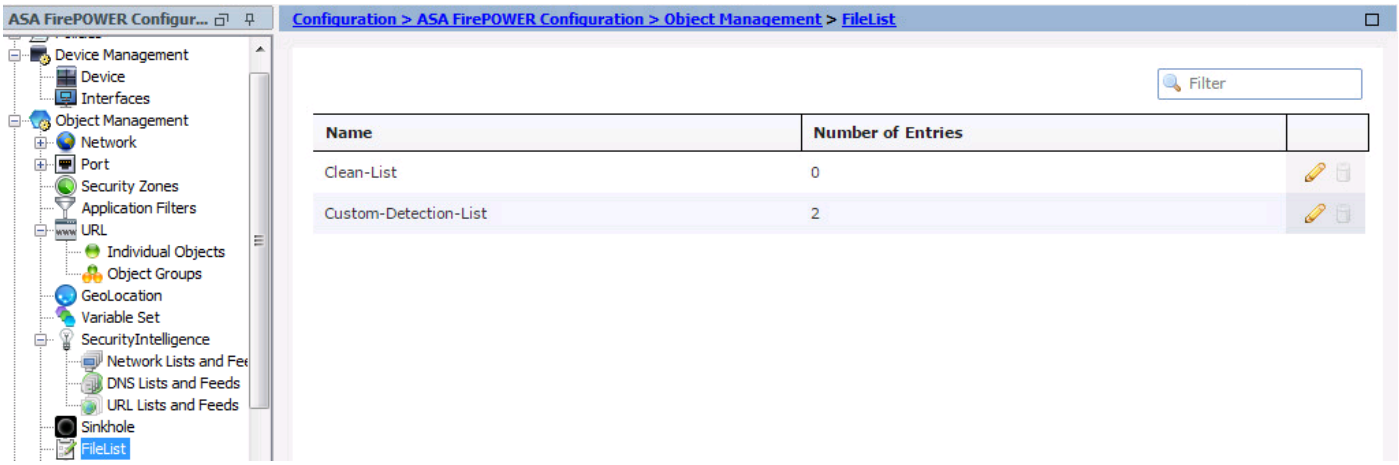


> Note:文件策略把柄文件按以下规则操作顺序：阻塞优先于恶意软件检查，优先于简单检测和记录日志。

如果配置基于网络先进的恶意软件保护(AMP)，并且Cisco Cloud不正确地检测文件的处理，您能添加文件到文件列表使用SHA-256 Hash值改善在将来检测文件处理。根据文件列表种类，您能执行：

- 要对待文件，好象网云分配一个干净的处理，请添加文件到干净的列表。
- 要对待文件，好象网云分配恶意软件处理，请添加文件到定制列表。

配置此，导航到**Configuration> ASA Firepower Configuration>对象Management>文件列表**和编辑列表添加SHA-256。



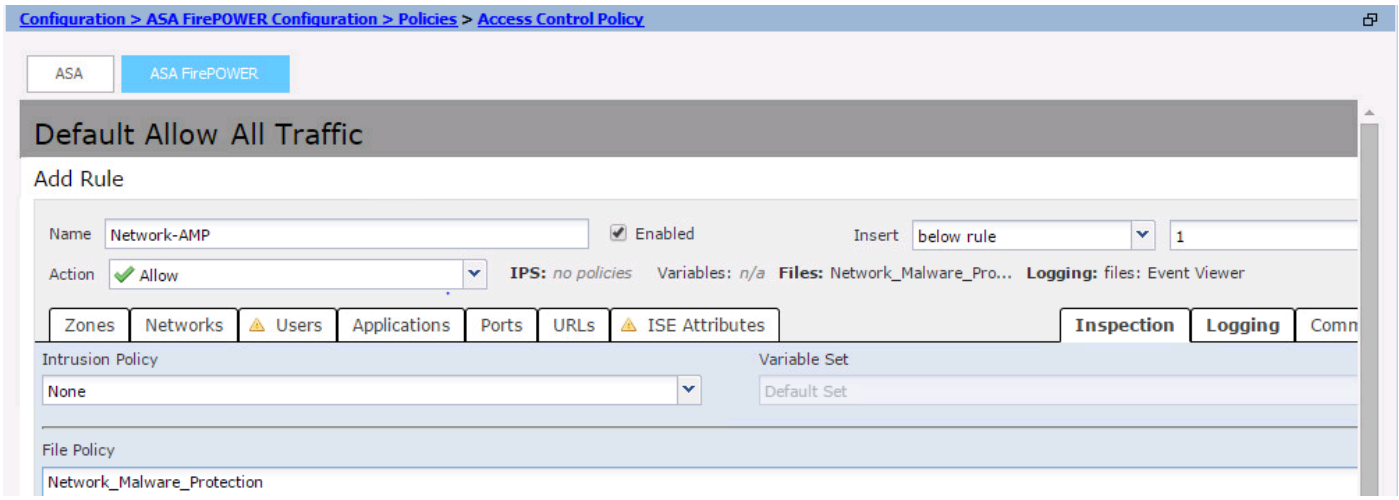
配置文件策略的访问控制策略

如此镜像所显示，导航对Configuration> ASA Firepower Configuration>**策略>访问控制策略**，并且创建新建的**访问规则**或编辑现有**访问规则**。

要配置文件策略，操作应该是**准许**。导航对**检查**选项卡，并且选择从下拉菜单的**文件策略**。

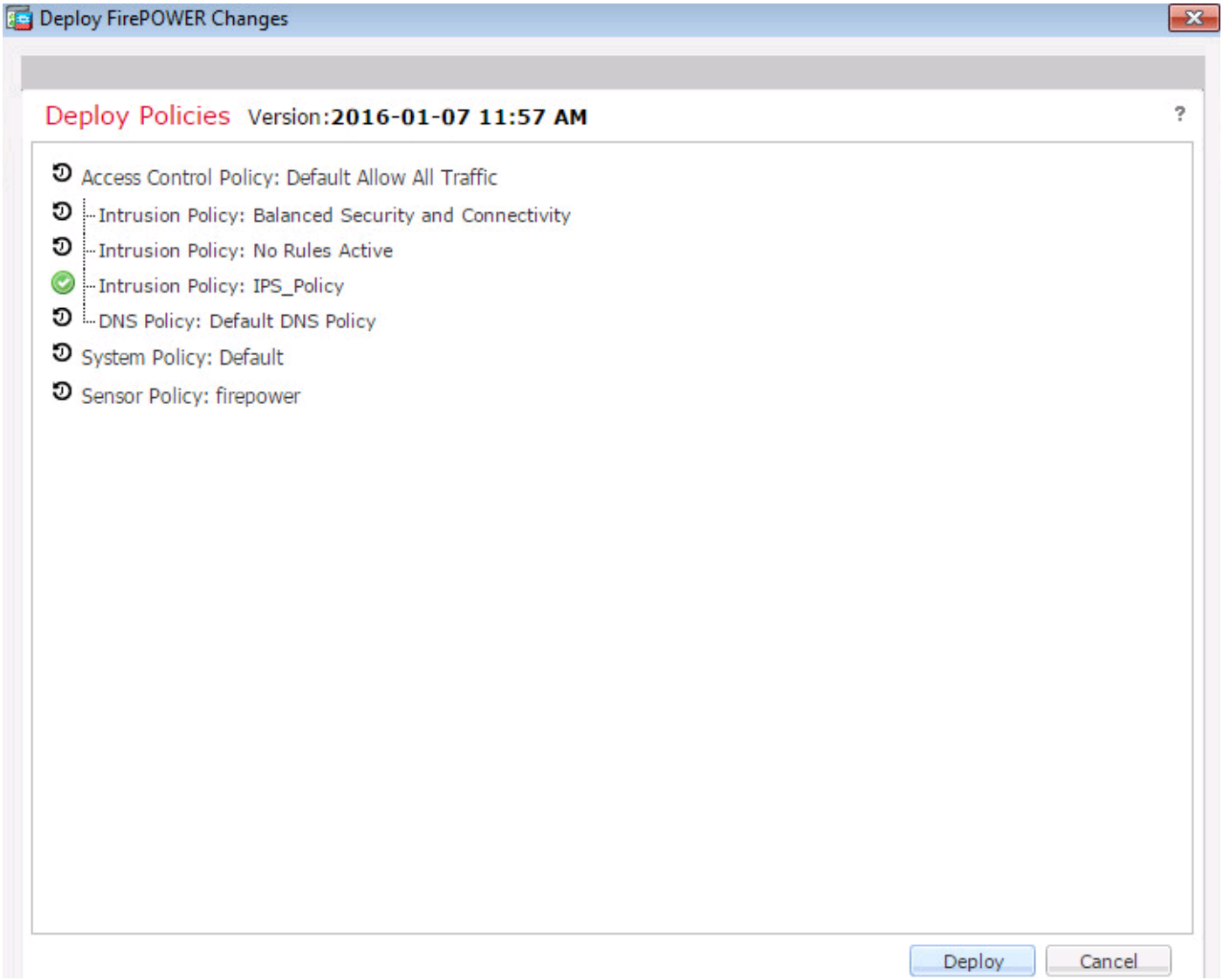
对启用日志，请导航**日志选项**，并且选择适当的日志选项&**日志文件**选项。点击**"Save"/Add按钮**保存配置。

选择选项**存储ASA Firepower更改**保存AC策略变更。



实施访问控制策略

导航对ASDM**部署**选项，并且选择**部署**从下拉菜单的**Firepower崔凡吉莱**选项。点击Deploy选项部署更改。

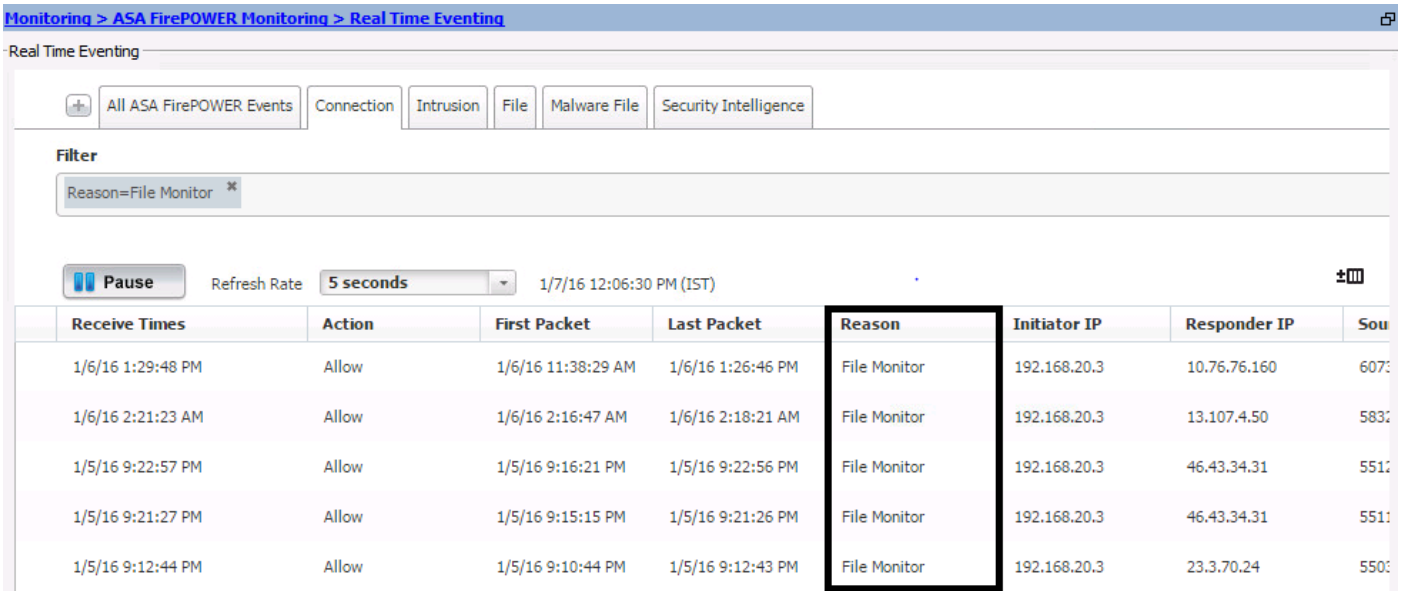


导航对**Monitoring> ASA Firepower Monitoring>任务状态。** 保证任务必须完成应用配置更改。

Note:在版本5.4.x，适用于访问策略传感器，您需要clickApply **ASA Firepower更改。**

文件策略事件的箴言报连接

为了看到Firepower模块生成的事件与文件策略涉及，导航对**Monitoring> ASA Firepower Monitoring>实时Eventing。**



验证

当前没有可用于此配置的验证过程。

故障排除

保证文件策略正确地conifigured与协议方向动作文件类型。 保证那在访问规则包括的正确文件策略。

保证访问控制策略部署成功地完成。

监控连接事件&文件事件(**Monitoring> ASA Firepower Monitoring>实时Eventing**)验证，如果通信流点击正确规则。

相关信息

- 技术支持和文档 - Cisco Systems