网络恶意软件防护和文件策略

以下主题概述文件控制、文件策略、文件规则、高级恶意软件保护(AMP)、云连接和动态分析连接。

- 关于网络恶意软件防护和文件策略， 第 1 页
- 文件策略的要求和前提条件， 第 2 页
- 文件和恶意软件策略许可证要求， 第 3 页
- 文件策略和恶意软件检测的最佳实践 ， 第 3 页
- 如何配置恶意软件防护， 第 6 页
- 恶意软件防护的云连接， 第 11 页
- 文件策略和文件规则， 第 20 页
- 追溯处置情况更改， 第 34 页
- 文件和恶意软件检测性能和存储选项， 第 35 页
- 调整文件和恶意软件检测性能和存储 ， 第 36 页
- （可选）Cisco Secure Endpoint 的恶意软件防护， 第 37 页
- 网络恶意软件保护和文件策略的历史记录， 第 41 页

关于网络恶意软件防护和文件策略

要检测和阻止恶意软件，请使用文件策略。您还可以使用文件策略按文件类型来检测和控制流量。

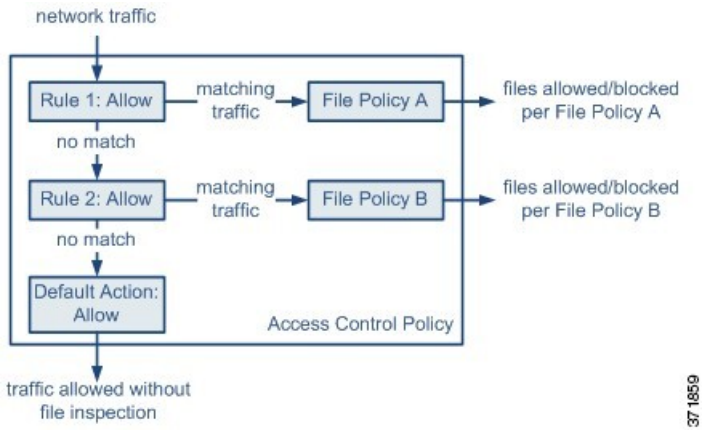
面向 Firepower 的高级恶意软件防护 (AMP) 可以检测、捕获、跟踪、分析、记录并选择性地阻止网络流量中恶意软件的传输。在 Cisco Secure Firewall Management Center Web 界面中，此功能称为恶意软件防护，以前称为面向 *Firepower* 的 *AMP*。思科高级恶意软件保护利用内联部署的托管设备和来自思科云的威胁数据来识别恶意软件。

您可以将文件策略与处理网络流量的访问控制规则作为整体访问控制配置的一部分关联起来。

当系统检测到网络上的恶意软件时，它会生成文件和恶意软件事件。要分析文件和恶意软件事件数据，请参阅《Cisco Secure Firewall Management Center 管理指南》 中的文件/恶意软件事件和网络文件轨迹一章。

文件策略

文件策略是作为整体访问控制配置的一部分供系统用于执行恶意软件保护和文件控制的一组配置。这种关联保证系统在传递流量中与访问控制规则的条件匹配的文件之前，首先检查该文件。在内联部署中，可考虑下图所示的简单访问控制策略。



策略有两个访问控制规则，两者都使用“允许”(Allow)操作并与文件策略关联。策略的默认操作也是允许流量，但不执行文件策略检查。在这种情况下，流量的处理方式如下：

- 与 `Rule 1` 匹配的流量根据 `File Policy A` 进行检查。
- 与 `Rule 1` 不匹配的流量根据 `Rule 2` 进行评估。与 `Rule 2` 匹配的流量根据 `File Policy B` 进行检查。
- 允许与任一规则都不匹配的流量；不能将文件策略与默认操作关联。

通过将不同文件策略与不同访问控制规则相关联，可以精细控制如何识别并阻止网络上传输的文件。

文件策略的要求和前提条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 访问管理员

文件和恶意软件策略许可证要求

要执行此操作	所需许可证	文件规则操作
阻止或允许特定类型的所有文件（例如，阻止all.exe文件）	IPS （对于 设备） 保护 （适用于传统设备）	允许、阻止、阻止并重置
根据文件包含或可能包含恶意软件的判断，选择性地允许或阻止文件	IPS （对于 设备） 保护 （适用于传统设备） 恶意软件防御	恶意软件云查找、阻止恶意软件
存储文件	IPS （对于 设备） 保护 （适用于传统设备） 恶意软件防御	选择了 **存储文件** 的任何文件规则操作

有关 恶意软件防御 许可证的详细信息，请参阅：

- 《Cisco Secure Firewall Management Center 管理指南》中的恶意软件防御许可证

文件策略和恶意软件检测的最佳实践

除下述项目外，请按照 如何配置恶意软件防护，第 6 页 和参考主题中的步骤操作。

文件规则最佳实践

在配置文件规则时，请注意以下准则和限制：

- 配置为在被动部署中阻止文件的规则不会阻止匹配的文件。由于连接继续传输文件，因此如果配置规则以记录连接的开始，则您可能会看到为此连接记录的多个事件。
- 一个策略可以包含多个规则。在创建规则时，请确保没有规则被先前的规则“隐藏”。
- 动态分析支持的文件类型是其他分析类型支持的文件类型的子集。要查看每种分析支持的文件类型，请导航至文件规则配置页面，选择**阻止恶意软件 (Block Malware)** 操作，然后选中所需的复选框。

  要确保系统检查所有的文件类型，请为动态分析和其他类型的分析创建单独的规则（在同一策略内）。

- 如果文件规则配置有**恶意软件云查找**或**阻止恶意软件**操作，并且 防火墙管理中心无法与 AMP 云建立连接，则系统无法执行任何已配置的规则操作选项，直到恢复连接为止。
- 思科建议启用**重置连接 (Reset Connection)**（适用于**阻止文件 [Block Files]** 和**阻止恶意软件 [Block Malware]** 操作）以防止受阻应用会话保持打开，直到 TCP 连接重置为止。如果不重置连接，则客户端会话会保持打开，直到 TCP 连接重置为止。
- 如果监控大量流量，请**勿**存储所有捕获文件，或者将所有捕获文件提交进行动态分析。否则可能对系统性能产生不利影响。
- 不能对系统检测到的所有文件类型都执行恶意软件分析。从 **Application Protocol**、**Direction of Transfer** 和 **Action** 下拉列表中选择值之后，系统会对文件类型的列表进行约束。

文件检测最佳实践

请考虑文件检测的以下注意事项和限制：

- 如果未启用自适应分析，则访问控制规则无法执行文件控制（包括 AMP）。
- 如果文件与带有应用协议条件的规则相匹配，在系统成功确定该文件的应用协议之后，会生成文件事件。无法识别的文件不生成文件事件。
- FTP 通过不同信道传输命令和数据。在被动或内联分流模式部署中，来自 FTP 数据会话及其控制会话的流量可能不会均衡分摊到同一个内部资源。
- 如果 POP3、POP、SMTP 或 IMAP 会话中文件的所有文件名的总字节数超过 1024，则会话中的文件事件可能无法反映文件名缓冲区填充后检测到的文件的正确文件名。
- 当通过 SMTP 传输基于文本的文件时，某些邮件客户端会将换行符转换为 CRLF 换行符标准。由于基于 MAC 的主机使用回车 (CR) 字符，并且基于 Unix/Linux 的主机使用换行 (LF) 字符，因此，邮件客户端进行的换行可能修改文件的大小。注意某些邮件客户端在处理无法识别的文件类型时默认进行换行。
- 要检测 ISO 文件，请将“限制执行文件类型检测时检查的字节数”选项设置为大于 36870 的值，如文件和恶意软件检测性能和存储选项，第 35 页中所述。
- 无法检测到某些 .rar 存档中的 .Exe 文件，可能包括 rar5。
- 如果文件处置为中性，则为未知处置。

文件阻止最佳实践

请考虑文件阻止的以下注意事项和限制：

- 无论使用何种传输协议，如果未检测到文件的文件结尾标记，**Block Malware** 规则或自定义检测列表不会阻止该文件。系统会等待接收整个文件后再阻止文件（如文件结尾标记所指示），并在检测到该标记后阻止文件。
- 如果 FTP 文件传输的文件结尾标记单独从最后一个数据段进行传输，则会阻止该标记，并且 FTP 客户端会指示文件传输失败，但是文件实际上将完整传输到磁盘。

- 具有**阻止文件 (Block Files)** 和**阻止恶意软件 (Block Malware)** 操作的文件规则会阻止通过 HTTP 自动恢复文件下载，方法是在进行初始文件传输尝试后检测到相同的文件、URL、服务器和客户端应用达到 24 小时的情况下阻止新会话。
- 在极少数情况下，如果来自 HTTP 上传会话的流量顺序错误，则系统无法正确重组流量，并因此不会阻止该会话或生成文件事件。
- 如果通过 NetBios-ssn 传输使用**阻止文件 (Block Files)** 规则阻止的文件（例如 SMB 文件传输），则目标主机上可能会显示文件。但是，该文件不可用，原因是在下载启动后阻止了该文件，导致文件传输未完成。
- 如果您创建文件规则来检测或阻止通过 NetBIOS-ssn 传输的文件（例如 SMB 文件传输），系统不会检测正在进行的文件传输。但是，系统会检测部署调用文件策略的访问控制策略后传输的新文件。
- SMB 的多通道功能可以创建 IP 地址相同但端口不同的多个并行会话。对于多通道上的给定事务，文件下载会在未由系统作为单个文件检测的这些会话之间多路复用。
- 系统不会检测单个 TCP 或 SMB 会话中同步传输的文件。
- 在集群环境中，如果现有 SMB 会话因集群角色更改或设备故障而移至新设备，则任何正在传输的文件可能无法得到检测。
- Microsoft Windows 系统之间的一些 SMB 文件传输使用非常高的 TCP 窗口大小来进行快速文件传输。要检测或阻止此类文件传输，建议您增大**网络分析策略 (Network Analysis Policy)** > **TCP 数据流配置 (TCP Stream Configuration)** > **故障排除选项 (Troubleshooting Options)** 下的**最大排队字节数 (Maximum Queued Bytes)** 和**最大排队分段数 (Maximum Queued Segments)** 的值。
- 如果配置了 Firepower 威胁防御高可用性，并且在原始主用设备识别文件时发生故障切换，则文件类型不同步。即使文件策略阻止该文件类型，新的主用设备也会下载该文件。

文件策略最佳实践

在配置文件策略时，请注意以下常规准则和限制：

- 可以将单个文件策略与其操作为**允许 (Allow)**、**交互式阻止 (Interactive Block)** 或**交互式阻止并重置 (Interactive Block with reset)** 的访问控制规则关联。
- 您**不能**使用文件策略检查由访问控制默认操作处理的流量。
- 对于新策略，Web 界面会指出该策略未在使用。如果编辑的是使用中的文件策略，则 Web 界面会告知您使用该文件策略的访问控制策略的数量。在任一情况下，可以点击文本以跳至“访问控制策略”(Access Control Policies) 页面。
- 要使文件阻止起作用，应用于访问控制策略的NAP策略必须在保护模式（也称为内联模式）下运行。
- 根据您的配置，您可以在系统首次检测到某个文件时对其进行检查并等待云查找结果，也可以在首次检测到文件时不等待云查找结果即对文件放行。

- 默认情况下，已加密负载的文件检查会被禁用。当已加密连接与已配置文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。

注意　默认情况下，为文件/恶意软件策略启用具有以下生成器 ID (GID) 的文件检查预处理器：GID: 146 和 GID: 147。

- 如果在使用恶意软件操作或存储文件选项的文件策略中启用访问控制策略，则会降低设备的计算能力和系统性能。

如何配置恶意软件防护

本主题总结设置系统以保护网络免受恶意软件侵害时必须执行的步骤。

过程

步骤 1 规划和准备恶意软件防护，第 7 页

步骤 2 配置文件策略，第 8 页

步骤 3 将文件策略添加到访问控制配置，第 8 页

步骤 4 配置网络发现策略，将文件和恶意软件事件与网络上的主机相关联。

（不要简单地打开网络发现；您必须将其配置为发现网络上的主机，以构建组织的网络映射。）

请参阅网络发现策略以及子主题。

步骤 5 将策略部署到托管设备。

请参阅部署配置更改。

步骤 6 测试您的系统，确保它按预期处理恶意文件。

步骤 7 设置恶意软件防护的维护和监控，第 10 页

下一步做什么

- （可选）要进一步增强对网络中恶意软件的检测，请部署和集成思科Cisco Secure Endpoint。请参阅（可选）Cisco Secure Endpoint 的恶意软件防护，第 37 页以及子主题。
- 了解如何调查文件和恶意软件事件。

  请参阅 《Cisco Secure Firewall Management Center 管理指南》中文件/恶意软件事件和网络文件轨迹 。

规划和准备恶意软件防护

此程序是配置系统以提供恶意软件防护的完整过程中的第一组步骤。

过程

步骤 1 购买和安装许可证。

请参阅 文件和恶意软件策略许可证要求，第 3 页 和 《Cisco Secure Firewall Management Center 管理指南》中的 许可证。

步骤 2 了解文件策略和恶意软件防护如何融入您的访问控制计划。

请参阅章节访问控制概述。

步骤 3 了解文件分析和恶意软件防护工具。

请参阅文件规则操作，第 26 页以及子主题。

也可以考虑 高级和存档文件检查选项，第 21 页。

步骤 4 确定您将使用公共云还是私有（本地）云进行恶意软件防护（文件分析和动态分析）。

请参阅恶意软件防护的云连接，第 11 页以及子主题。

步骤 5 如果您将使用私有（本地）云进行恶意软件防护：购买、部署和测试这些产品。

有关信息，请联系思科客户代表或授权经销商。

步骤 6 配置防火墙以允许与您选择的云进行通信。

请参阅 《Cisco Secure Firewall Management Center 管理指南》中的 安全、互联网接入和通信端口 。

步骤 7 配置 Firepower 和恶意软件防护云（公共或私有云）之间的连接。

- 有关 AMP 云，请参阅更改 AMP 选项，第 16 页。
- 如果您部署了本地 Secure Secure Malware Analytics 设备，请参阅连接到内部动态分析设备，第 17 页。（访问公共 Secure Secure Malware Analytics 云不需要配置。）

下一步做什么

继续执行恶意软件防护工作流程的下一步：

请参阅如何配置恶意软件防护，第 6 页。

配置文件策略

开始之前

完成恶意软件防护工作流程中到目前为止的任务：

请参阅如何配置恶意软件防护，第 6 页。

过程

步骤 1 查看文件策略和文件规则限制。

请参阅文件策略和恶意软件检测的最佳实践，第 3 页以及子主题。

步骤 2 创建文件策略。

请参阅创建或编辑策略，第 20 页。

步骤 3 在文件策略中创建规则。

请参阅文件规则，第 25 页以及子主题。

步骤 4 配置高级选项。

请参阅高级和存档文件检查选项，第 21 页。

下一步做什么

继续执行恶意软件防护工作流程的下一步：

请参阅如何配置恶意软件防护，第 6 页。

将文件策略添加到访问控制配置

访问控制策略可能有多个与文件策略相关联的访问控制规则。您可以为任何 Allow 或 Interactive Block 访问控制规则配置文件检测，这样，您就可在网络中不同类型的流量到达其最终目的地之前，将不同的文件和恶意软件检测配置文件与其匹配。

开始之前

完成恶意软件防护工作流程中到目前为止的任务：

请参阅如何配置恶意软件防护，第 6 页。

过程

步骤 1 查看访问控制政策中的文件策略准则。（这些准则与您之前查看的文件规则和文件策略准则不同。）

查看 文件和入侵检查顺序。

步骤 2 将文件策略与访问控制策略关联。

请参阅配置访问控制规则以执行恶意软件保护，第 9 页

步骤 3 将访问控制策略分配给被托管的设备。

请参阅将设备分配给访问控制策略。

下一步做什么

继续执行恶意软件防护工作流程的下一步：

请参阅如何配置恶意软件防护，第 6 页。

配置访问控制规则以执行恶意软件保护

注意 在**检测文件**或**阻止文件**规则中启用启用或禁用**存储文件**，或添加包含**恶意软件云查找**或**阻止恶意软件**文件规则操作与分析选项（**Spero 分析或 MSEXE**、**动态分析**或**本地恶意软件分析**）或存储文件选项（**恶意软件**、**未知**、**清理**或**自定义**）的第一个文件规则，或者删除最后一个这样的文件规则，在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。

注释 当访问控制规则中包含文件策略时，会自动启用内联规范化。有关详细信息，请参阅 https://www.cisco.com/go/snort3-inspectors。

开始之前

- 如 配置自适应配置文件 中所述，为了让访问控制规则执行文件控制（包括 AMP），**必须**启用（默认状态）
- 您必须是管理员，访问管理员或网络管理员用户才能执行此任务。

过程

步骤 1 在访问控制规则编辑器中（从**策略 (Policies)** > **访问控制 (Access Control)**），从**操作 (Action)** 选择**允许 (Allow)**, **交互式阻止 (Interactive Block)** 或**交互式阻止并重置 (Interactive Block with reset)**。

步骤 2 （仅限旧版 UI。）点击**检测 (Inspection)**。

步骤 3 选择**文件策略 (File Policy)** 以检查与访问控制规则相匹配的流量，或选择**无 (None)** 禁用对匹配流量的文件检查。

步骤 4 （可选）通过点击**日志记录 (Logging)** 并取消选中**日志文件 (Log Files)** 为匹配连接禁用文件或恶意软件文件的日志记录。

注释
思科建议您保持启用文件和恶意软件日志记录。

步骤 5 保存规则。

步骤 6 点击**保存**保存策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

相关主题

创建或编辑策略， 第 20 页
Snort 重新启动场景

设置恶意软件防护的维护和监控

持续维护对于保护您的网络至关重要。

开始之前

配置您的系统以保护您的网络免受恶意软件的侵害。

请参阅如何配置恶意软件防护， 第 6 页和引用的程序。

过程

步骤 1 确保您的系统始终具有最新、最有效的保护。

请参阅维护您的系统：符合动态分析条件的文件类型， 第 19 页。

步骤 2 为恶意软件相关事件和运行状况监控配置警报。

有关配置 恶意软件防护 警报的信息以及有关以下模块的信息，请参阅《Cisco Secure Firewall Management Center 管理指南》：

- 本地恶意软件分析
- 安全智能
- 设备中威胁数据更新
- 入侵和文件事件率
- 面向 Firepower 的 AMP 状态
- Cisco Secure Endpoint状态

下一步做什么

查看恶意软件防护工作流程中的“后续操作”：

请参阅如何配置恶意软件防护，第 6 页。

恶意软件防护的云连接

为了保护网络免受恶意软件，需要连接到公共云或私有云。

AMP 云

高级恶意软件防护 (AMP) 云是一种 Cisco 托管服务器，它使用大数据分析和持续分析提供系统用于检测和阻止网络中的恶意软件的情报。

AMP 云为由托管设备在网络流量中检测到的潜在恶意软件提供处置情况，并为本地恶意软件分析和文件预分类提供数据更新。

如果您的组织已部署Cisco Secure Endpoint 并且已配置 Firepower 以导入其数据，则系统会从 AMP 云导入这些数据，包括扫描记录、恶意软件检测、隔离和危害表现 (IOC)。

Cisco 提供以下选项，用于从 思科云获取有关已知恶意软件威胁的数据：

- **AMP 公共云**

  您的 Cisco Secure Firewall Management Center 直接与公共 思科云通信。有三个公共 AMP 云，分别位于美国、欧洲和亚洲。

- **AMP 私有云**

  AMP 私有云虚拟设备用作压缩的内部 AMP 云，以及用于连接到公共 AMP 云的匿名代理。有关详细信息，请参阅思科 AMP 私有云，第 14 页。

  如果与Cisco Secure Endpoint 集成，则 AMPv 会有一些限制。请参阅Cisco Secure Endpoint 和 AMP 私有云，第 39 页。

动态分析云

- **Secure Secure Malware Analytics 云**

  公共云处理您提交进行动态分析的符合条件的文件，并提供威胁评分和动态分析报告。Firepower 支持 200 个样本/天进行 Secure Secure Malware Analytics 分析。

- **本地 Secure Secure Malware Analytics 设备**

  如果您的组织的安全策略不允许系统发送网络外部的文件，则您可以配置本地设备。此设备不会联系公共 Secure Secure Malware Analytics 云。

  有关详细信息，请参阅动态分析本地设备 (Cisco Secure Secure Malware Analytics)，第 17 页。

配置与 AMP 和 Secure Secure Malware Analytics 云的连接

- AMP 云连接配置，第 12 页
- 动态分析连接，第 16 页

AMP 云连接配置

以下主题介绍不同场景的 AMP 云连接配置：

- 选择 AMP 云，第 13 页
- 连接到 AMP 私有云，第 14 页
- 集成 Firepower 和 Cisco Secure Endpoint，第 39 页

以下主题也相关：

- 思科 AMP 私有云，第 14 页
- AMP 云连接的要求和最佳实践，第 12 页
- 管理与 AMP 云的连接（公共或私有），第 15 页

AMP 云连接的要求和最佳实践

AMP 云连接的要求

您必须是管理员用户才能设置 AMP 云。

为保证 防火墙管理中心 可与 AMP 云通信，请参阅《Cisco Secure Firewall Management Center 管理指南》中安全、互联网接入和通信端口。

AMP 和高可用性

尽管高可用性对中的防火墙管理中心共享文件策略和相关配置，但它们不共享 AMP 云连接、捕获的文件、文件事件和恶意软件事件。为确保操作的连续性，并且使两台防火墙管理中心上的恶意软件处置相同，主用和备用防火墙管理中心都必须能够访问云。

这些要求适用于公共和私有 AMP 云。

AMP 云连接和多租户

在多域部署中，在全局级别配置 恶意软件防护 连接。每个 防火墙管理中心只能有一个恶意软件防护 连接。

选择 AMP 云

默认情况下，为您的系统配置并启用与美国 (US) AMP 公共云的连接。（此连接会在 Web 界面中显示为 恶意软件防护，有时会显示为面向 Firepower 的 AMP。）您无法删除或禁用 恶意软件防护 云连接，但您可以使用此程序在不同的地理 AMP 云之间切换，或者配置私有云 (AMPv) 连接。

开始之前

- 如果您将使用 AMP 私有云，请参阅连接到 AMP 私有云，第 14 页而不是本主题。
- 除非 Firepower 与Cisco Secure Endpoint 集成，否则只能配置一个 AMP 云连接。此连接标记为 **面向网络的 AMP** 或 **面向 Firepower 的 AMP**。
- 如果您已部署Cisco Secure Endpoint，并且想要添加一个或多个 AMP 云以将该应用与 Firepower 集成，请参阅集成 Firepower 和 Cisco Secure Endpoint，第 39 页。
- 请参阅AMP 云连接的要求和最佳实践，第 12 页。

过程

步骤 1 选择**集成** > **AMP** > **AMP 管理**。

步骤 2 点击铅笔以编辑现有云连接。

步骤 3 从**云名称 (Cloud Name)** 下拉列表中，选择离 Cisco Secure Firewall Management Center最近的区域云：

APJC 是指亚太地区/日本/中国。

步骤 4 点击**保存**。

下一步做什么

- 如果您的部署为高可用性配置，请参阅AMP 云连接的要求和最佳实践，第 12 页。
- （可选）更改 AMP 选项，第 16 页。

思科 AMP 私有云

防火墙管理中心必须连接到AMP云，才能对在网络流量中检测到的文件进行处置情况查询并接收追溯性恶意软件事件。此云可以是公共云，也可以是私有云。

您的组织可能会担心隐私或安全，以致在受监控网络和 AMP 云之间难以或无法进行频繁或直接连接。在这些情况下，您可以设置一个思科AMP私有云，它是一个思科专有的产品，用作压缩内部版 AMP 云，以及网络与 AMP 云之间的安全中介。将 防火墙管理中心连接到 AMP 私有云会禁用到公共 AMP 云的现有直接连接。

所有到 AMP 云的连接均通过 AMP 私有云进行筛选，AMPv 用作匿名代理，以确保受监控网络的安全和隐私。此项筛选包括，对在网络流量中检测到的文件进行处置情况查询、接收追溯性恶意软件事件等等。AMP 私有云不通过外部连接共享任何终端数据。

注释 AMP 私有云既 **不** 执行动态分析，也不支持匿名检索其他依靠思科综合安全智能 (CSI)（例如，URL 和安全智能过滤）的功能的威胁情报。

有关 AMP 私有云（有时称为“AMPv”）的信息，请参阅 https://www.cisco.com/c/en/us/products/security/fireamp-private-cloud-virtual-appliance/index.html。

连接到 AMP 私有云

开始之前

- 根据该产品的文档中的方向配置思科AMP私有云。在配置过程中，请记下私有云的主机名。配置 防火墙管理中心上的连接需要使用此主机名。
- 确保 防火墙管理中心 可与 AMP 私有云通信，并确认私有云可访问互联网，以便它可与公有 AMP 云通信。请参阅《Cisco Secure Firewall Management Center 管理指南》中安全、互联网接入和通信端口下的主题。
- 除非您的部署与Cisco Secure Endpoint 集成，否则每个 防火墙管理中心 只能有一个 AMP 云连接。此连接标记为 **面向网络的 AMP** 或 **面向 Firepower 的 AMP**。

  如果与 Cisco Secure Endpoint 集成，可以配置多个 Cisco Secure Endpoint 云连接。

过程

步骤 1 选择**集成** > **AMP** > **AMP 管理**。

步骤 2 点击**添加 AMP 云连接**。

步骤 3 从**云名称 (Cloud Name)** 下拉列表中，选择**私有云 (Private Cloud)**。

步骤 4 输入 **Name**。

此信息显示在 AMP 私有云生成或传输的恶意软件事件中。

步骤 5 在**主机 (Host)** 字段中，输入在设置私有云时配置的私有云主机名。

步骤 6 点击**证书上传路径 (Certificate Upload Path)** 旁边的**浏览 (Browse)**，浏览至私有云的有效 TLS 或 SSL 加密证书的位置。有关详细信息，请参阅 AMP 私有云文档。

步骤 7 如果要将此私有云用于 恶意软件防护 和 Cisco Secure Endpoint，请选中**用于面向 Firepower 的 AMP** 复选框。

如果配置其他私有云来处理 恶意软件防护 通信，则可以清除此复选框；如果这是唯一的 AMP 私有云连接，则无法清除。

在多域部署中，此复选框仅显示在全局域中。每个防火墙管理中心只能有一个恶意软件防护连接。

步骤 8 点击**注册 (Register)**，确认要禁用到 AMP 云的现有直接连接，并最终确认要继续至 AMP 私有云管理控制台以完成注册。

步骤 9 登录管理控制台并完成注册过程。有关进一步说明，请参阅 AMP 私有云文档。

下一步做什么

在高可用性部署中，在两个管理中心配置 AMP 云连接。这些配置不会同步。

管理与 AMP 云的连接（公共或私有）

使用防火墙管理中心管理与用于恶意软件防护 或Cisco Secure Endpoint 或两者的公共和私有 AMP 云的连接。

如果不想再从云接收恶意软件相关信息，则可以删除与公共或私有 AMP 云的连接。请注意，使用 Cisco Secure Endpoint 或 AMP 私有云管理控制台取消注册连接不会从系统中删除连接。取消注册的连接会在Cisco Secure Firewall Management Center Web 界面上显示失败状态。

您还可以临时禁用连接。当重新启用云连接时，云恢复向系统发送数据，包括禁用期内的已排队数据。

⚠

注意 对于已禁用的连接，公共或私有 AMP 云可以存储恶意软件事件和危害表现等，直到重新启用连接。在极少数情况下（例如，事件率超高或连接长时间禁用），云可能无法存储在连接处于禁用状态时生成的所有信息。

在多域部署中，系统会显示在当前域中创建的连接，您可以对其进行编辑。系统还会显示在祖先域中创建的连接，您不可以对其进行管理。要管理较低域中的连接，请切换至该域。每个 防火墙管理中心只能具有一个属于全局域的恶意软件防护 连接。

过程

步骤 1 选择**集成** > **AMP** > **AMP 管理**。

步骤 2 管理 AMP 云连接：

- 删除 - 点击 **删除** ( )，然后确认选择。

- 启用或禁用 - 点击滑块，然后确认选择。

下一步做什么

在高可用性部署中，在两个管理中心配置 AMP 云连接。这些配置不会同步。

更改 AMP 选项

过程

步骤 1 选择**集成** > **其他集成** > **云服务**。

步骤 2 选择选项：

表 *1:* 适用于网络的 *AMP* 的选项

选项	说明
启用自动本地恶意软件检测更新 (Enable Automatic Local Malware Detection Updates)	本地恶意软件检测引擎使用思科提供的签名对文件进行静态分析和预分类。如果启用此选项，则 防火墙管理中心每 30 分钟检查一次签名更新。
与思科共享恶意软件事件中的 URI (Share URI from Malware Events with Cisco)	系统可以向 AMP 云发送有关网络流量中检测到的文件的信息。此信息包括与被检测的文件相关联的 URI 信息及其 SHA-256 散列值。虽然共享功能是可选的，不过向思科传输此信息对未来的恶意软件识别和跟踪工作有帮助。

步骤 3 点击**保存**。

动态分析连接

动态分析的要求

您必须是管理员、访问管理员或网络管理员用户并且在全局域中，才能使用动态分析。

通过适当的许可证，系统会自动访问 Secure Secure Malware Analytics 云。

动态分析要求托管设备具有对 Secure Secure Malware Analytics 云或本地 Secure Secure Malware Analytics 设备的端口 443 的直接或代理访问权限。

另请参阅哪些文件符合动态分析的条件？，第 30 页。

如果您将连接到本地 Secure Secure Malware Analytics 设备，另请参阅连接到内部动态分析设备，第 17 页中的前提条件。

查看默认动态分析连接

默认情况下，Cisco Secure Firewall Management Center 可以连接到 Secure Secure Malware Analytics 公共云以提交文件并检索报告。您既不能配置也不能删除此连接。

过程

步骤 1 选择**集成** > **AMP** > **动态分析连接AMP** > **动态分析连接**。

步骤 2 请点击 **编辑** (✎)。

注释

有关**集成 (Integration)** > **AMP** > **动态分析连接 (Dynamic Analysis Connections)** 页面上的 **关联** （  ）的信息，请参阅启用对公共云中动态分析结果的访问权限，第 18 页。

动态分析本地设备 (Cisco Secure Secure Malware Analytics)

如果您的组织担心提交文件到公共 Secure Secure Malware Analytics 云可能会造成隐私或安全问题，您可以部署内部 Secure Secure Malware Analytics 设备。如同公共云一样，内部设备在沙盒环境下运行合格文件，然后向系统传回威胁评分和动态分析报告。但是，内部设备不会与公共云或位于您的网络外部的任何其他系统通信。

有关本地 Secure Secure Malware Analytics 设备的详细信息，请参阅https://www.cisco.com/c/en/us/products/security/threat-grid/index.html。

连接到内部动态分析设备

如果在网络上安装内部 Secure Secure Malware Analytics 设备，则可以配置动态分析连接以提交文件并从该设备中检索报告。当配置内部设备动态分析连接时，可将 Cisco Secure Firewall Management Center注册到内部设备。

开始之前

- 设置本地 Secure Secure Malware Analytics 应用。

  可从 https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/tsd-products-support-series-home.html获得应用的说明文档：

  请参阅 *Cisco Firepower* 兼容性指南。

- 如果您的 Secure Secure Malware Analytics 设备使用自签名公钥证书，请从 Secure Secure Malware Analytics 设备下载证书；有关您的 Secure Secure Malware Analytics 设备信息，请参阅设备管理员指南。

  如果使用证书颁发机构 (CA) 签名的证书，则证书必须满足以下要求：

  - 必须在 Secure Secure Malware Analytics 设备上安装服务器密钥和签名证书。按照 Secure Secure Malware Analytics 设备《管理员指南》中的上传说明进行操作。

- 如果存在多级 CA 签名链，则所有必需的中间证书和根证书必须包含在 防火墙管理中心将上传到的单个文件中。
- 所有证书都必须采用 PEM 编码。
- 文件的换行符必须是 UNIX，而不是 DOS。

- 如果要使用代理连接到内部设备，请配置代理；请参阅 《Cisco Secure Firewall Management Center 管理指南》中的 修改防火墙管理中心 管理接口 。
- 托管设备必须在端口 443 上直接或代理访问 Secure Secure Malware Analytics 设备。

过程

步骤 1 选择**集成** > **AMP** > **动态分析连接AMP** > **动态分析连接**。

步骤 2 点击**添加新连接 (Add New Connection)**。

步骤 3 输入 **Name**。

步骤 4 输入**主机**。

步骤 5 在**证书上传 (Certificate Upload)**旁，点击**浏览 (Browse)** 以上传本地设备的证书。

如果 Secure Secure Malware Analytics 设备将提供自签名证书，请上传您从该设备下载的证书。

如果 Secure Secure Malware Analytics 设备将提供 CA 签名证书，请上传包含证书签名链的文件。

步骤 6 如果要使用已配置的代理建立连接，选中 **在可用时使用代理**复选框。

步骤 7 点击 **Register**。

步骤 8 点击**是**以显示本地 Secure Secure Malware Analytics 设备登录页面。

步骤 9 将用户名和密码输入到本地 Secure Secure Malware Analytics 设备。

步骤 10 点击 **Sign in**（**登录**）。

步骤 11 您有以下选择：

- 如果先前将 Cisco Secure Firewall Management Center注册到内部设备，请点击**返回**。
- 如果未注册 Cisco Secure Firewall Management Center，请点击**激活**。

启用对公共云中动态分析结果的访问权限

Secure Secure Malware Analytics 提供的有关已分析文件的报告比 防火墙管理中心提供的要详细。如果您的组织有 Secure Secure Malware Analytics 云账户，则您可以直接访问 Secure Secure Malware Analytics 门户，查看有关从托管设备发出的进行分析的文件的其他详细信息。但是，出于隐私方面的考虑，只有提交文件的组织才能查看文件分析详细信息。因此，在查看此信息之前，您必须将 防火墙管理中心 与其托管设备提交的文件相关联。

开始之前

您必须有一个 Secure Secure Malware Analytics 云账户，并准备好您的账户凭证。

过程

步骤 1 选择**集成** > **AMP** > **动态分析连接AMP** > **动态分析连接**。

步骤 2 在 Secure Secure Malware Analytics 云对应的表行中点击 **关联** （  ） 。

将打开一个 Secure Secure Malware Analytics 门户窗口。

步骤 3 登录到 Secure Secure Malware Analytics 云。

步骤 4 点击**提交查询**。

注释
请勿更改**设备 (Devices)** 字段中的默认值。

如果在执行此流程时遇到困难，请与思科 TAC 的 Secure Secure Malware Analytics 代表联系。

此更改最多可能需要 24 小时才能生效。

下一步做什么

激活关联后，请参阅 《Cisco Secure Firewall Management Center 管理指南》 中 查看思科云中的动态分析结果 。

维护您的系统：符合动态分析条件的文件类型

符合动态分析条件的文件类型列表由漏洞数据库 (VDB) 确定，该列表定期更新（但每天不超过一次）。如果您是管理员用户，则可以更新符合动态分析条件的文件类型。

每个版本中自动提交支持的文件类型可能不同。当前支持自动提交的文件包括：

- PE 可执行文件（仅 32 位）
- EXE
- DLL
- PDF
- MSOLE2（Microsoft 对象链接和嵌入复合文件）
- DOCX、PPTX、XLSX

注释 GZ 和 ZIP 文件类型不支持自动提交。

为确保您的系统拥有最新列表：

过程

步骤 1 执行以下操作之一：

- （推荐）请参阅 《Cisco Secure Firewall Management Center 管理指南》中所述的 漏洞数据库更新自动化
- 定期检查新的 VDB 更新，并根据需要 手动更新 *VDB*（如 《Cisco Secure Firewall Management Center 管理指南》 中所述）。

  如果您选择此选项，建议您安排定期提醒来执行此操作。

步骤 2 如果您的文件策略指定单个文件类型，而不是指定**支持动态分析**文件类型类别，请更新您的文件策略以使用新支持的文件类型。

步骤 3 如果符合条件文件类型列表发生更改，请部署到托管设备。

文件策略和文件规则

创建或编辑策略

开始之前

如果要配置恶意软件防护策略，请参阅 配置文件策略，第 8 页中的所有必要程序。

过程

步骤 1 选择**策略** > **访问控制标题** > **恶意软件和文件** 。

步骤 2 创建新策略或编辑现有策略。

如果要编辑现有策略： 如果显示**视图** ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

提示
要复制现有文件策略，请点击 **复制** ( )，然后在出现的对话框中为新策略键入唯一名称。然后就可以修改副本。

步骤 3 如创建文件规则，第 33 页中所述，向文件策略添加一个或多个规则。

步骤 4 或者，也可以选择“高级”，并如 高级和存档文件检查选项，第 21 页中所述配置高级选项。

步骤 5 保存文件策略。

下一步做什么

- 如果要配置恶意软件防护策略，请参阅 配置文件策略， 第 8 页中的其他所需程序。
- 其他:
  - 如将文件策略添加到访问控制配置， 第 8 页中所述，将该文件策略添加到访问控制规则。
  - 部署配置更改；请参阅 部署配置更改。

高级和存档文件检查选项

文件策略编辑器中的“高级”设置具有以下常规选项：

- **首次文件分析**-选择此选项可在 AMP 云处置处于待定状态时分析首次看到的文件。该文件必须与配置为执行恶意软件云查找和Spero、本地恶意软件或动态分析的规则相匹配。如果取消选择此选项，则会将首次检测到的文件标记为具有“未知”处置情况。
- **启用自定义检测列表** - 阻止自定义检测列表上的文件。
- **启用干净列表**-如果启用，此策略将允许干净列表上的文件。
- **如果 AMP 云处置情况为未知，则根据威胁评分覆盖处置情况**-选择一个选项：
  - 如果您选择 **禁用**， 系统将不会覆盖 AMP 云提供的处置情况。
  - 如果设置了阈值威胁评分，则AMP云判定为“未知”的文件如果其动态分析评分等于或低于阈值，则会被视为恶意软件。
  - 如果选择更低的阈值，请增加被视为恶意软件的文件数。根据文件策略中选择的操作，这可能导致受阻文件数增加。
  - 有关威胁评分范围的数字，请参阅 《Cisco Secure Firewall Management Center 管理指南》中的 威胁评分和动态分析摘要报告 。

文件策略编辑器中的“高级”设置具有以下存档文件检查选项：

- **检测存档** - 对于大小可达**可存储的最大文件大小**高级访问控制设置的存档文件，启用内容检测。
- **阻止加密存档**-阻止受密码保护的存档。
- **阻止不可检测的存档** - 阻止系统并非因加密原因而无法检测其内容的存档文件。此类文件通常包括损坏的文件，或超过指定的最大存档深度的文件。
- **最大存档深度** - 阻止超过指定深度的嵌套存档文件。此计数中未计入顶级存档文件；深度从 1（第一级嵌套文件）开始。

存档文件

存档文件是包含其他文件的文件，例如 `.zip` 或 `.rar` 文件。

如果存档中的任何单个文件与包含阻止操作的文件规则相匹配，系统将阻止整个存档而非该单个文件。

有关存档文件检查选项的详细信息，请参阅高级和存档文件检查选项，第 21 页。

可进行检查的存档文件

- **文件类型**

  可检查存档文件类型的完整列表会显示在 FMC Web 接口中的文件规则配置页面上。要查看该页面，请参阅创建文件规则，第 33 页。

  包含的可检查的文件显示在同一页面上。

- **文件大小**

  您可以检查的存档文件大小可达**可存储的最大文件大小**文件策略高级访问控制设置。

- **嵌套存档**

  存档文件可以包含其他存档文件，而其他存档文件反过来又可以包含所述存档文件。文件嵌套的级别是其存档文件深度。请注意，深度计数中未计入顶级存档文件；深度从 1（第一级嵌套文件）开始。

  系统可以检查最外层存档文件（级别 0）以下的最多三级嵌套文件。您可以将文件策略配置为阻止超过该深度（或指定的较低最大文件深度）的存档文件。

  如果您选择不阻止超过最大存档文件深度 3 的文件，当受监控流量中出现包含某些可提取内容和某些嵌套深度为 3 或更大值的内容的存档文件时，系统仅检查其能够检查的文件并报告相关数据。

  所有适用于未压缩的文件的功能（例如，动态分析和文件存储）也适用于存档文件中的嵌套文件。

- **加密文件**

  您可以将系统配置为阻止内容已加密或无法检查的存档。

- **不会检查的存档**

  如果包含存档文件的流量在安全智能阻止列表或不阻止列表中，或者，如果顶级存档文件的 SHA - 256 值在自定义检测列表中，则系统将不检查该存档文件的内容。

  如果嵌套文件被阻止，则整个存档也将被阻止；但是，如果嵌套文件被允许，则存档不会自动通过（取决于任何其他嵌套文件和特性）。

  无法检测到某些 .rar 存档中的 .Exe 文件，可能包括 rar5。

存档文件处置情况

存档文件处置情况基于分配给存档内文件的处置情况。对于包含已确定的恶意软件文件的**所有**存档，将赋予其 `Malware` 性质。对于不含已确定恶意软件文件的存档，如果其包含任何未知文件，则其性质为 `Unknown`；如果其仅包含安全文件，则其性质为 `Clean`。

表 *2:* 按内容划分的存档文件处置情况

存档文件性质	未知文件数	干净文件数	恶意软件文件数
未知	1 个或更多	任意	0
干净 (Clean)	0	1 个或更多	0
恶意软件 (Malware)	任意	任意	1 或更多

存档文件与其他文件一样可以具有自定义检测 (Custom Detection) 或不可用 (Unavailable) 处置情况（如果符合这些处置情况的条件）。

查看存档内容和详细信息

如果将文件策略配置为检查存档文件内容，当存档文件出现在文件事件、恶意软件事件或捕获的文件中时，您可以使用“分析 > 文件”菜单下页面上表格中的上下文菜单，及网络文件轨迹查看器查看有关存档内文件的信息。

存档的所有文件内容均以表形式列出，同时显示其相关信息的摘要：名称、SHA-256 散列值、类型、类别和存档深度。每个文件旁边都会显示一个网络文件轨迹图标，点击该图标即可查看有关该特定文件的详细信息。

使用自定义列表覆盖文件处置情况

如果文件在 AMP 云中的处置情况据您所知不正确，您可向覆盖云中处置情况的文件列表中添加该文件的 SHA-256 值：

- 要好像 AMP 云已为文件分配了干净的处置一样对其进行处理，请将文件添加到干净列表。
- 要好像 AMP 云已为文件分配了恶意软件处置一样对其进行处理，请将文件添加到自定义检测列表。

在后续检测中，设备无需重新评估文件处置情况即可允许或阻止该文件。您可以按文件策略使用干净的列表或自定义检测列表。

注释 要计算文件的 SHA-256 值，您必须将文件策略中的一条规则配置为对匹配的文件执行恶意软件云查找或阻止恶意软件。

有关在 Firepower 中使用文件列表的完整信息，请参阅文件列表。

或者，如果适用，请使用来自Cisco Secure Endpoint 的集中文件列表 ， 第 24 页。

来自*Cisco Secure Endpoint*的集中文件列表

如果您的组织已部署Cisco Secure Endpoint，则在 Firepower 查询 AMP 云获取文件处置情况时，它可以使用在Cisco Secure Endpoint 中创建的阻止名单和允许名单。

要求：

- 您的组织使用的必须是 AMP 公共云。
- 您的组织已部署 Cisco Secure Endpoint。
- 已使用 集成 Firepower 和 Cisco Secure Endpoint，第 39 页 中的过程将系统注册到 Cisco Secure Endpoint。

要创建和部署这些列表，请参阅Cisco Secure Endpoint 的相关文档或在线帮助。

注释 在 Firepower 中创建的文件列表会覆盖在Cisco Secure Endpoint 中创建的文件列表。

管理文件策略

“文件策略”(File Policies) 页面显示现有文件策略的列表及其上次修改日期。您可以使用此页面来管理文件策略。

注释 系统会检查符合动态分析条件的文件类型列表的更新（每天不超过一次）。如果合格文件类型列表更改，这会构成文件策略发生更改；任何使用该文件策略的访问控制策略在部署于任何设备时都会标记为过期。在更新的文件策略可在设备上生效之前，必须先部署策略。请参阅维护您的系统：符合动态分析条件的文件类型，第 19 页。

过程

步骤 1 选择**策略** > **访问控制标题** > **恶意软件和文件** 。

步骤 2 管理文件策略：

- 比较 - 点击**比较策略 (Compare Policies)**；请参阅比较策略。
- 创建 - 要创建文件策略，请点击**新建文件策略 (New File Policy)**，然后如创建或编辑策略，第 20 页中所述继续操作。
- 复制 - 要复制文件策略，请点击 **复制** ()。

  如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。
- 删除 - 如果要删除文件策略，请点击 **删除** ()，然后按照提示点击**是**和**确定**。

  如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

- 部署 - 选择**部署** > **部署**；请参阅部署配置更改。
- 编辑 - 如果要修改现有文件策略，请点击 **编辑** ()。
- 报告 - 点击**报告** ()；请参阅生成当前策略报告。

文件规则

文件策略（例如父项访问控制策略）包含的规则用于确定系统如何处理与每个规则的条件相符的文件。可以配置单独的文件规则，以对不同的文件类型、应用协议或传输方向采取不同操作。

例如，如果某个文件匹配某个规则，则该规则可以：

- 根据简单的文件类型匹配允许或阻止文件
- 根据处置情况阻止文件（无论评估是否表明它是恶意的）
- 将文件存储到设备（有关信息，请参阅捕获的文件和文件存储 ， 第 31 页）
- 提交储存的（捕获的）文件以进行本地恶意软件、Spero 或动态分析

此外，文件策略还可以：

- 根据干净的列表或自定义检测列表中的条目自动将文件视为干净的文件或恶意软件
- 在文件的威胁评分超过可配置阈值时将文件视为恶意软件
- 检查存档文件（例如，`.zip` 或 `.rar`）的内容
- 阻止内容已加密，嵌套超过指定的最大存档深度或因其他原因无法检查的存档文件

文件规则组成部分

表 *3:* 文件规则组成部分

文件规则组成部分	说明
应用协议	系统可以检测和检查通过 FTP、HTTP、SMTP、IMAP、POP3 和 NetBIOS-ssn (SMB) 传输的文件。**Any**（默认值）检测 HTTP、SMTP、IMAP、POP3、FTP 和 NetBIOS-ssn (SMB) 流量中的文件。为了提高性能，可以逐个文件规则将文件检测仅限于其中一种应用协议。
传输方向	对于已下载的文件，可以检查通过 FTP、HTTP、IMAP、POP3 和 NetBIOS-ssn (SMB) 传入的流量；对于已上传的文件，可以检查通过 FTP、HTTP、SMTP 和 NetBIOS-ssn (SMB) 传出的流量。 **提示** 无论用户是发送还是接收，使用 **Any** 都可通过多种应用协议检测文件。

文件规则组成部分	说明
文件类别和类型	系统检测各种类型的文件。这些文件类型分为三类：基本类别，包括多媒体（swf 和 mp3）；可执行文件（exe 和 torrent）；以及 PDF。可以配置用于检测个别文件类型或整个类别的文件类型的规则。 例如，可以阻止所有多媒体文件，或者仅阻止 ShockWave Flash (swf) 文件。或者，可以将系统配置为会在用户下载 BitTorrent (torrent) 文件时向您发出警报。 请注意，可执行文件包括可以运行宏和脚本的文件类型，因为它们可能包含恶意软件。 有关系统可以检查的文件类型的列表，请选择**策略 > 访问控制 > 恶意软件和文件**，创建一个临时的新文件策略，然后点击**添加规则**。选择文件类型类别，系统可以检查的文件类型会显示在**文件类型**列表中。 **注释** 频繁触发的文件规则可能会影响系统性能。例如，检测 HTTP 流量（例如 YouTube，用于传输重要的 Flash 内容）中的多媒体文件可能会产生可能生成数量巨大的事件。
文件规则操作	文件规则操作用于确定系统如何处理与规则条件相符的流量。 根据所选操作，您可以配置系统是存储文件还是对文件执行 Spero、本地恶意软件或动态分析。如果选择“阻止”(Block) 操作，还可以配置系统是否还重置受阻连接。 有关这些操作和选项的说明，请参阅文件规则操作，第 26 页。 文件规则是以规则操作顺序而非数字顺序进行评估。有关详细信息，请参阅文件规则操作：评估顺序，第 32 页。

文件规则操作

借助文件规则，可以精细控制要对其记录、阻止或扫描恶意软件的文件类型。每个文件规则都有用于确定系统如何处理与规则条件匹配的流量的关联操作。文件策略必须包含一个或多个规则才能生效。您可以在文件策略中使用单独的规则，以对不同的文件类型、应用协议或传输方向采取不同操作。

文件规则操作

- 检测文件规则允许将特定文件类型的检测记录到数据库，同时仍允许其传输。
- 阻止文件规则允许阻止特定文件类型。您可以配置选项，以在阻止文件传输时重置连接并将已捕获的文件存储到托管设备。
- 恶意软件云查找 *(Malware Cloud Lookup)* 规则允许您获取并记录通过网络传输的文件的处置情况，同时仍允许文件传输。

- 阻止恶意软件 *(Block Malware)* 规则允许您计算特定文件类型的 SHA-256 散列值，查询 AMP 云以确定通过网络传输的文件是否包含恶意软件，然后阻止表示为威胁的文件。

文件规则操作选项

根据所选择的操作，有不同的选项：

文件规则操作选项	能否阻止文件？	能否阻止恶意软件？	能否检测文件？	能否进行恶意软件云查找？
MSEXE 的 Spero 分析*	否	是，可以提交可执行文件	否	是，可以提交可执行文件
动态分析*	否	是，可以提交具有未知文件处置情况的可执行文件	否	是，可以提交具有未知文件处置情况的可执行文件
容量处理	否	是	否	是
本地恶意软件分析*	否	是	否	是
重置连接	是（推荐）	是（推荐）	否	否
存储文件	是，可以存储所有匹配的文件类型	是，可以存储与选择的文件性质匹配的文件类型	是，可以存储所有匹配的文件类型	是，可以存储与选择的文件性质匹配的文件类型

* 有关这些选项的完整信息，请参阅恶意软件保护选项（在文件规则操作中），第 27 页及其子主题。

注意 启用或禁用**检测文件**或**阻止文件**规则中的**存储文件**，或者添加第一条或删除最后一条将**恶意软件云查找**或**阻止恶意软件**文件规则操作与分析选项（**Spero 分析或 MSEXE**、**动态分析**或**本地恶意软件分析**）或存储文件选项（**恶意软件**、**未知**、**清理**或**自定义**）、在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。结合起来的文件规则

恶意软件保护选项（在文件规则操作中）

系统运用多种文件检测和分析方法来确定文件是否包含恶意软件。

根据您在文件规则中启用的选项，系统将按顺序使用以下工具检查文件：

1. Spero 分析，第 29 页 和 AMP 云查找，第 29 页
2. 本地恶意软件分析，第 30 页
3. 动态分析，第 30 页

有关这些工具的比较，请参阅恶意软件防护选项的比较，第 28 页。

（如果您愿意的话，还可以根据文件类型阻止所有文件。有关详细信息，请参阅按类型阻止所有文件，第 32 页。）

另请参阅（可选）Cisco Secure Endpoint 的恶意软件防护，第 37 页和子主题中有关思科Cisco Secure Endpoint 产品的信息。

恶意软件防护选项的比较

下表详细介绍每种类型的文件分析的优缺点，以及每种恶意软件防护方法确定文件处置的方式。

分析类型	优点	限制	恶意软件识别
斯佩罗分析	可执行文件的结构分析，将 Spero 签名提交到AMP 云进行分析	没有本地恶意软件分析或动态分析彻底，仅用于可执行文件	仅在明确识别恶意软件时处置情况才会从“未知”(Unknown) 更改为“恶意软件”(Malware)。
本地恶意软件分析	比动态分析消耗的资源少，返回结果更快，尤其当检测到的恶意软件较常见时	分析结果没有动态分析的结果彻底	仅在明确识别恶意软件时处置情况才会从“未知”(Unknown) 更改为“恶意软件”(Malware)。
动态分析	使用 Secure Secure Malware Analytics对未知文件的彻底分析	符合条件的文件将上传到公共云或本地设备。完成分析需要一些时间	威胁评分确定文件的恶意程度。处置情况根据文件策略中配置的威胁评分阈值。
Spero 分析结合本地恶意软件分析	比配置本地恶意软件分析和动态分析消耗的资源少，仍使用 AMP 云资源识别恶意软件	没有动态分析彻底，Spero 分析仅用于可执行文件	仅在明确识别恶意软件时处置情况才会从“未知”(Unknown) 更改为“恶意软件”(Malware)。
Spero 分析结合动态分析	在提交文件和 Spero 签名时使用完整的 AMP 云功能	获取结果的速度没有使用本地恶意软件分析获取结果的速度快	威胁评分根据预分类为可能的恶意软件的文件的动态分析结果更改。处置情况根据文件策略中配置的威胁评分阈值更改，并在 Spero 分析识别恶意软件时从“未知”(Unknown) 更改为“恶意软件”(Malware)。

分析类型	优点	限制	恶意软件识别
本地恶意软件分析结合动态分析	使用两种类型的文件分析使分析结果更彻底	比单独使用任一种分析消耗的资源多	威胁评分根据预分类为可能的恶意软件的文件的动态分析结果更改。处置情况在本地恶意软件分析识别恶意软件时从“未知”(Unknown) 更改为“恶意软件”(Malware)，或根据文件策略中配置的威胁评分阈值更改。
Spero 分析、本地恶意软件分析结合动态分析	分析结果最彻底	运行所有三种类型的文件分析消耗的资源最多	威胁评分根据预分类为可能的恶意软件的文件的动态分析结果更改。处置情况在 Spero 分析或本地恶意软件分析识别恶意软件时从“未知”(Unknown) 更改为“恶意软件”(Malware)，或根据文件策略中配置的威胁评分阈值更改。
（阻止传输指定文件类型的所有文件）	不需要 恶意软件防御许可证 （从技术上讲此选项不是恶意软件防护选项。）	合法文件也将被阻止	（不执行任何分析。）

注释 预分类本身并不确定文件的处置情况；它只是确定文件是否符合动态分析条件的一个因素。

Spero 分析

Spero 分析检查结构特征，例如可执行文件中的元数据和报头信息。根据此信息生成 Spero 签名后，若文件是合法可执行文件，则设备会将其提交到 AMP 云中的 Spero 启发式引擎。基于 Spero 签名，Spero 引擎确定文件是否为恶意软件。您还可以配置以下规则：提交文件以进行 Spero 分析，而不将其提交到 AMP 云。

请注意，您无法手动提交文件以进行 Spero 分析。

AMP 云查找

对于符合条件使用高级恶意软件防护进行评估的文件，防火墙管理中心执行恶意软件云查找，根据其 SHA-256 散列值在 AMP 云中查询文件的处置情况。

为了提高性能，系统会缓存由云返回的处置情况，并为已知文件使用缓存的处置情况而不是查询 AMP 云。有关此缓存的详细信息，请参阅缓存处置情况持久性 ，第 30 页。

本地恶意软件分析

本地恶意软件分析允许托管设备使用由Talos 智能小组 提供的检测规则集，在本地检查可执行文件、PDF、办公文档以及其他类型的文件是否存在最常见的恶意软件类型。由于本地恶意软件分析不需要查询 AMP 云，也不运行该文件，因此节约了时间和系统资源。

如果系统通过本地恶意软件分析识别恶意软件，则它会将现有文件处置情况从“未知”(Unknown) 更改为“恶意软件”(Malware)。然后，系统会生成一个新恶意软件事件。如果系统未识别恶意软件，则它不会将文件处置情况从“未知”(Unknown) 更改为“干净”(Clean)。系统运行本地恶意软件分析后，会缓存 SHA-256 散列值、时间戳以及处置情况等文件信息，以便在特定时间段内再次检测时，系统可以在不进行其他分析的情况下识别恶意软件。有关缓存的详细信息，请参阅缓存处置情况持久性，第 30 页。

本地恶意软件分析不需要与 Secure Secure Malware Analytics 云建立通信。但是，您必须配置与云的通信，以提交文件以进行动态分析，并将更新下载到本地恶意软件分析规则集。

缓存处置情况持久性

从 AMP 云查询返回的处置情况、关联的威胁评分以及本地恶意软件分析分配的处置情况都具有生存时间 (TTL) 值。保持某种处置情况而无更新达到 TTL 值中指定的持续时间后，系统会清除缓存的信息。安全状态及相关的威胁评分具有以下 TTL 值：

- “干净”(Clean) - 4 小时
- “未知”(Unknown) - 1 小时
- “恶意软件”(Malware) - 1 小时

如果对缓存进行查询发现已超时的缓存处置情况，系统会向 本地恶意软件分析数据库和 AMP 云重新查询新的处置情况。

动态分析

您可以将文件策略配置为使用思科的文件分析和威胁情报平台 Secure Secure Malware Analytics （以前称为 Threat Grid）自动提交文件以进行动态分析。

设备将符合条件的文件提交到 Secure Secure Malware Analytics （公共云或本地设备，以您指定的为准），无论设备是否存储文件。

Secure Secure Malware Analytics 在沙盒环境中运行该文件，分析文件的行为以确定该文件是否为恶意文件，然后返回威胁评分，指明文件包含恶意软件的可能性。您可以通过威胁评分查看动态分析摘要报告，该报告包含分配该威胁评分的原因。您还可以查看 Secure Secure Malware Analytics 以查看您的组织提交的文件的详细报告，以及您的组织未提交的文件的有限数据的清理报告。

有关思科 Secure Secure Malware Analytics的详细信息，请参阅 https://www.cisco.com/c/en/us/products/security/threat-grid/index.html

要配置系统以执行动态分析，请参阅动态分析连接，第 16 页下面的主题。

哪些文件符合动态分析的条件？

文件是否符合动态分析的条件取决于：

- 文件类型
- 文件大小
- 文件规则的操作

此外：

- 系统只会提交与您配置的文件规则匹配的文件。
- 在发送文件进行分析时，该文件的恶意软件云查找性质必须为“未知”(Unknown) 或“不可用”(Unavailable)。
- 系统必须将文件预分类为潜在的恶意软件。

动态分析和容量处理

在设备无法与云通信或已达到最大提交次数而系统暂时无法将文件提交到云时，容量处理允许您暂时地存储符合动态分析条件的文件。当阻碍条件消除后，系统会提交存储的文件。

一些设备可以将文件存储在设备硬盘驱动器或恶意软件存储包中。另请参阅恶意软件存储包，第32页。

捕获的文件和文件存储

通过文件存储功能，您可以捕获在流量中检测到的选定文件，并自动将文件副本暂时存储至设备硬盘驱动器（如果已安装）或恶意软件存储包内。

在设备捕获文件后，您可以：

- 将捕获文件存储至设备硬盘驱动器中供后期分析使用。
- 将存储的文件下载至本地计算机，以便进一步实施人工分析或存档。
- 手动提交符合条件的捕获文件，以进行 AMP 云查找或动态分析。

请注意，文件存储在设备中之后，如果未来检测到该文件且设备仍存有该文件，则不会再捕获该文件。

注释 在网络上第一次检测到某个文件时，您可以生成代表文件检测情况的文件事件。但如果您的文件规则执行恶意软件云查找，则系统需要额外的时间来查询AMP云并返回处置情况。由于这种延迟，在网络上第二次出现此文件之前，系统无法存储此文件，并且系统可以立即确定此文件的处置情况。

无论系统捕获还是存储文件，您都可以：

- 从“分析“>”文件“>”捕获的文件”审查捕获文件的信息，包括文件是否存储或提交用于动态分析、文件性质和威胁评分，以便迅速查看网络中检测到的恶意软件潜在威胁。
- 查看文件轨迹，确定其如何穿过网络以及哪些主机有副本。
- 向清空列表或自定义检测列表添加文件，以便在未来检测过程中始终将该文件作为清空或恶意软件性质。

您可以在文件策略中配置文件规则，以便捕获并存储特定类型或者具有特定文件性质的文件（如有）。如果将该文件策略与访问控制策略相关联，并将其部署到设备上，则系统将捕获并存储流量中的匹配文件。还可以限制要存储的最小和最大文件大小。

存储的文件不包含在系统备份中。

您可以在“分析”>“文件”>“捕获的文件”下查看捕获的文件信息，并下载副本进行离线分析。

恶意软件存储包

根据您的文件策略配置，设备可能会将大量文件数据存储到硬盘驱动器。您可以在设备中安装一个恶意软件存储包，系统则会将文件存储到该恶意软件存储包，从而使主硬盘驱动器中有更多空间来存储事件和配置文件。系统会定期删除较早的文件。如果设备的主硬盘驱动器没有足够的可用空间，也未安装恶意软件存储包，则无法存储文件。

注意 请勿尝试在设备中安装非思科提供的硬盘驱动器。安装不受支持的硬盘驱动器可能会损坏设备。恶意软件存储包套件**仅**可从思科购买。如果需要恶意软件存储包方面的帮助，请与技术支持部门联系。

如果未安装恶意软件存储包，则在配置设备以存储文件时，该设备会将主硬盘驱动器空间的设定部分分配用于存储捕获文件。如果将容量处理配置为暂时存储文件以进行动态分析，则系统会使用相同的硬盘驱动器分配来存储这些文件，直至可以将这些文件重新提交到云。

在设备中安装恶意软件存储包并配置文件存储或容量处理时，该设备会分配整个恶意软件存储包来用于存储这些文件。设备无法在恶意软件存储包中存储任何其他信息。

在分配的用于存储捕获文件的空间容量填满时，系统将删除最早存储的文件，直到分配的空间达到系统定义的阈值。根据存储的文件数量，在系统删除文件后，您可能会看到磁盘已用空间明显下降。

如果在安装恶意软件存储包时，设备已经存储文件，则下次重新启动设备时，存储在主硬盘驱动器上的任何捕获文件或容量处理文件都会移至恶意软件存储包。设备未来存储的文件都将存储至恶意软件存储包。

有关在 Firepower 设备上使用 MSP 的详细信息，请参阅您的设备的 Firepower 硬件安装指南 。

按类型阻止所有文件

如果您的组织不仅要阻止恶意软件文件的传输，还要阻止某个特定类型的所有文件的传输（无论文件是否包含恶意软件），您可以做到这一点。

系统可以检测恶意软件的所有文件类型以及许多其他文件类型都支持文件控制。这些文件类型分为三类：基本类别，例如多媒体（swf 和 mp3）；可执行文件（exe 和 torrent）；以及 PDF。

从技术上来说，根据类型阻止所有文件不是恶意软件防护功能；它不需要恶意软件防御许可证，也不会查询 AMP 云。

文件规则操作：评估顺序

文件策略有可能包含针对不同情况的不同操作的多个规则。如果多个规则同时适用于某个特定情况，则将适用本主题中所述的评估顺序。一般来说，简单阻止优先于恶意软件检查和阻止，后者优先于简单检测和日志记录。

文件规则操作的优先顺序为：

- 阻止文件 *(Block Files)*
- 阻止恶意软件
- 恶意软件云查找
- 检测文件

如果已配置，则TID还会影响操作优先级。有关详细信息，请参阅威胁智能导向器-防火墙管理中心操作优先级。

创建文件规则

注意 启用或禁用**检测文件**或**阻止文件**规则中的**存储文件**，或者添加第一条或删除最后一条将**恶意软件云查找**或**阻止恶意软件**文件规则操作与分析选项（**Spero 分析或 MSEXE**、**动态分析**或**本地恶意软件分析**）或存储文件选项（**恶意软件**、**未知**、**清理**或**自定义**）、在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。结合起来的文件规则

开始之前

如果要配置恶意软件防护规则，请参阅配置文件策略， 第 8 页。

过程

步骤 1 依次选择 **策略 > 访问控制 > 恶意软件和文件**。

步骤 2 点击编辑图标以编辑现有文件策略。

步骤 3 在文件策略编辑器中，点击 **添加规则**。

步骤 4 选择**应用协议 (Application Protocol)** 和**传输方向 (Direction of Transfer)**，如文件规则组成部分， 第 25 页中所述。

步骤 5 选择一个或多个**文件类型**。

显示的文件类型取决于所选的应用协议、传输方向和操作。

可以通过以下方式过滤文件类型列表：

- 在**文件类型类别 (File Type Categories)** 中选择一个或多个文件类型类别，然后点击**所选类别中的所有类型 (All types in selected Categories)**。
- 按名称或说明搜索文件类型。例如，在**搜索名称和说明 (Search name and description)** 字段中键入 **`Windows`** 将会显示 Microsoft Windows 专用文件的列表。

提示
将指针悬停在文件类型上方可查看其描述。

步骤 6 按照文件规则操作，第 26 页中的描述选择文件规则**操作**，并考虑文件规则操作：评估顺序，第 32 页。

可用的操作取决于您所安装的许可证。请参阅文件和恶意软件策略许可证要求，第 3 页。

步骤 7 根据您选择的操作，配置选项：

- 在阻止文件后重置连接
- 存储与规则匹配的文件
- 启用 Spero 分析*
- 启用本地恶意软件分析*
- 启用动态分析*和容量处理

* 有关这些选项的信息，请参阅文件规则操作，第 26 页和恶意软件保护选项（在文件规则操作中），第 27 页及其子主题。

步骤 8 点击**添加 (Add)**。

步骤 9 点击**保存**保存策略。

下一步做什么

- 如果要配置恶意软件防护策略，请返回配置文件策略，第 8 页。
- 部署配置更改；请参阅 部署配置更改。

用于恶意软件防护的访问控制规则日志记录

当系统根据文件策略中的设置检测到受禁文件（包括恶意软件）时，会自动将事件记录到Cisco Secure Firewall Management Center数据库中。如果您不想记录文件或恶意软件事件，则可按每条访问控制规则禁用此日志记录功能。

无论调用访问控制规则的日志记录配置如何，系统均会将关联连接的末端记录到 Cisco Secure Firewall Management Center数据库。

追溯处置情况更改

文件处置情况可以更改。例如，当发现新信息时，AMP 云可以确定先前被视为安全的文件现在被识别为恶意软件，或者正好相反，以前被识别为恶意软件的文件实际上是安全的。如果上周查询过的文件的处置情况发生变化，AMP 云会通知系统，使其在下次检测到该文件进行传输时可以自动采取措施。已更改的处置情况称为追溯性处置情况。

文件和恶意软件检测性能和存储选项

提高文件大小会影响系统的性能。

表 *4:* 高级访问控制文件和恶意软件防护检测选项

字段	说明	准则和限制
限制进行文件类型检测时检查的字节数 (Limit the number of bytes inspected when doing file type detection)	指定执行文件类型检测时检查的字节数。	0 - 4294967295 (4GB) 0 可消除限制。 默认值是 TCP 数据包的最大分片大小（1460 个字节）。在大多数情况下，系统可以使用第一个数据包确定常见的文件类型。 要检测 ISO 文件，请输入大于 36870 的值。
Allow file if cloud lookup for Block Malware takes longer than (seconds)	指定进行恶意软件云查找时，没有缓存的处置情况，系统将会保持匹配**阻止恶意软件 (Block Malware)** 规则的文件的最后一个字节的时长。如果该时间过去，系统没有获得处置，文件将会通过。不可用的处置不会被缓存。	0 - 30 秒 如未联系支持部门，请勿将此选项设置为 0。 由于连接故障，思科建议使用默认值以避免阻止流量。
Do not calculate SHA-256 hash values for files larger than (in bytes)	禁止系统存储大于特定大小的文件，对文件进行恶意软件云查找或阻止文件（如果已添加到自定义检测列表）。	0 - 4294967295 (4GB) 0 可消除限制。 该值必须大于或等于**可存储的最大文件大小（字节）**和**用于动态分析测试的最大文件大小（字节）**。

高级文件检查和存储的最小文件大小（字节）	这些设置指定：
	• 系统可以使用以下检测器检测的文件大小：
	  • 斯佩罗分析
	  • 沙盒和预分类
	  • 本地恶意软件分析/ClamAV
	  • 存档检测
	• 系统可以使用文件规则存储的文件大小。
		0 - 10485760 (10MB)
		0 可禁用文件存储。
		必须小于或等于**可存储的最大文件大小（字节）**和**对于文件大小大于以下值的文件，不计算 SHA-256 散列值（以字节为单位）**。

高级文件检查和存储的最大文件大小（字节）		0 - 10485760 (10MB) 0 可禁用文件存储。 必须大于或等于**可存储的最小文件大小（字节）**，并小于或等于**对于文件大小大于以下值的文件，不计算 SHA-256 散列值（以字节为单位）**。

字段	说明	准则和限制
用于动态分析测试的最小文件大小（字节）**(Minimum file size for dynamic analysis testing [bytes])**	指定系统可以提交到 AMP 云以供动态分析的最小文件大小。	0 - 10485760 (10MB) 必须小于或等于**用于动态分析测试的最大文件大小（字节）**和**对于文件大小大于以下值的文件，不计算 SHA-256 散列值（以字节为单位）**。 动态分析的文件大小必须位于文件分析的最小值和最大值设置所定义的限制内。 系统会检查 AMP 云以更新可以提交的最小文件大小（一天不超过一次）。如果新的最小值大于当前值，当前值会更新为新的最小值，而且策略会标记为过期。
用于动态分析测试的最大文件大小（字节）**(Maximum file size for dynamic analysis testing (bytes))**	指定系统可以提交到 AMP 云以供动态分析的最大文件大小。	0 - 10485760 (10MB) 必须大于或等于**用于动态分析测试的最小文件大小（字节）**，并小于或等于**对于文件大小大于以下值的文件，不计算 SHA-256 散列值（以字节为单位）**。 动态分析的文件大小必须位于文件分析的最小值和最大值设置所定义的限制内。 系统会检查 AMP 云以更新可以提交的最大文件大小（一天不超过一次）。如果新的最大值小于当前值，当前值会更新为新的最大值，而且策略会标记为过期。

调整文件和恶意软件检测性能和存储

您必须是管理员，访问管理员或网络管理员用户才能执行此任务。

过程

步骤 1 在访问控制策略编辑器中，点击**高级设置 (Advanced Settings)**。

步骤 2 点击**文件和恶意软件设置 (Files and Malware Settings)** 旁边的 **编辑** (✎) 。

如果显示**视图** (👁)，则表明设置继承自祖先策略，或者您没有修改设置的权限。 如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 3 设置文件和恶意软件检测性能和存储选项，第 35 页中所述的任何选项。

步骤 4 点击**确定**。

步骤 5 点击**保存**保存策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

（可选）Cisco Secure Endpoint 的恶意软件防护

思科的Cisco Secure Endpoint 是一款独立的恶意软件防护产品，它可以补充系统提供的恶意软件防护并与您的 Firepower 部署进行集成。

Cisco Secure Endpoint 是思科的企业级高级恶意软件防护解决方案，它在个人用户的终端（计算机和移动设备）上作为轻量级连接器运行，用于发现、了解和阻止高级恶意软件爆发、高级持续威胁和针对性攻击。

Cisco Secure Endpoint 的优势包括：

- 为整个组织配置自定义恶意软件检测策略和配置文件，以及对所有用户的文件执行快速扫描和全面扫描
- 执行恶意软件分析，包括查看热图、详细文件信息、网络文件轨迹和威胁根本原因
- 配置爆发控制的多个方面，包括自动隔离、用于阻止运行非隔离可执行文件的应用阻止，以及排除列表
- 创建自定义保护，根据组策略阻止某些应用的执行，并创建自定义允许的应用列表
- 使用Cisco Secure Endpoint 管理控制台帮助您减轻恶意软件的影响。管理控制台提供稳健灵活的 Web 界面，您可以通过该界面控制Cisco Secure Endpoint 部署的所有方面并管理爆发的所有阶段。

有关Cisco Secure Endpoint的详细信息，请参阅：

- https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html。
- Cisco Secure Endpoint 管理控制台中的在线帮助。
- 可从以下位置获取 Cisco Secure Endpoint 文档：http://docs.amp.cisco.com。

恶意软件防护比较：Firepower 与Cisco Secure Endpoint

表 *5:* 按检测产品进行比较的高级恶意软件防护差异

特性	Firepower 恶意软件防护（恶意软件防护）	Cisco Secure Endpoint
文件类型检测和阻止方法（文件控制）	在网络流量中，使用访问控制和文件策略	不支持
恶意软件检测和阻止方法	在网络流量中，使用访问控制和文件策略	在单个终端（最终用户计算机和移动设备）上，使用与 AMP 云进行通信的连接器

特性	Firepower 恶意软件防护（恶意软件防护）	Cisco Secure Endpoint
检查的网络流量	流量传递通过托管设备	无；终端上安装的连接器直接检查文件
恶意软件情报数据源	AMP 云（公共或私有）	AMP 云（公共或私有）
恶意软件检测稳健性	有限的文件类型	所有文件类型
恶意软件分析方案	防火墙管理中心为基础的分析，以及在 AMP 云中的分析	防火墙管理中心为基础的分析，以及Cisco Secure Endpoint 管理控制台上的其他选项
恶意软件缓解	网络流量中的恶意软件阻止， 防火墙管理中心 发起的补救	基于 Cisco Secure Endpoint 的隔离和爆发控制方案，防火墙管理中心发起的纠错
生成的事件	文件事件、捕获文件、恶意软件事件及追溯性恶意软件事件	恶意软件事件
恶意软件事件中的信息	基本的恶意软件事件信息，以及连接数据（IP 地址、端口和应用协议）	深入的恶意软件事件信息；无连接数据
网络文件轨迹	基于防火墙管理中心	防火墙管理中心 和 Cisco Secure Endpoint 管理控制台均具有网络文件轨迹。两者均很有用。
所需许可证或订用	执行文件控制和所需的许可证 恶意软件防护	Cisco Secure Endpoint 订用。将 Cisco Secure Endpoint 数据导入 防火墙管理中心 无需许可证。

关于将 Firepower 与Cisco Secure Endpoint 进行集成

如果您的组织已部署Cisco Secure Endpoint，您可以选择将该产品与 Firepower 部署进行集成。

与Cisco Secure Endpoint 进行集成不需要专用 Firepower 许可证。

集成 Firepower 和Cisco Secure Endpoint 的优势

将Cisco Secure Endpoint 部署与系统集成具有以下优势：

- Cisco Secure Endpoint 中配置的集中屏蔽应用和允许应用可确定从 Firepower 发送到 AMP 云用于处置的文件 SHA 的判定。

  请参阅来自Cisco Secure Endpoint 的集中文件列表， 第 24 页。

- 系统可以将Cisco Secure Endpoint 检测到的恶意软件事件导入到 Cisco Secure Firewall Management Center，这样您便可以管理这些事件以及系统生成的恶意软件事件。这些事件的导入数据包括扫描、恶意软件检测、隔离、阻止的执行和云召回，以及防火墙管理中心为其监控的主机显示的危害表现 (IOC)。

  有关详细信息，请参阅《Cisco Secure Firewall Management Center 管理指南》中的使用*Cisco Secure Endpoint* 进行恶意软件事件分析 。

- 您可以在Cisco Secure Endpoint 控制台中查看文件轨迹和其他详细信息。

  有关详细信息，请参阅《Cisco Secure Firewall Management Center 管理指南》中的使用*Cisco Secure Endpoint* 控制台中的事件数据 。

重要事项 如果您使用思科 AMP 私有云虚拟设备 (AMPv)，请参阅 Cisco Secure Endpoint 和 AMP 私有云 ，第 39 页中的限制。

Cisco Secure Endpoint 和 AMP 私有云

如果您配置思科 AMP 私有云以收集您的网络的 Cisco Secure Endpoint数据，则所有Cisco Secure Endpoint 连接器都会将数据都发送到私有云，然后私有云会将这些数据转发到 Cisco Secure Firewall Management Center。私有云不通过外部连接共享任何终端数据。

如果您的组织已部署 AMP 私有云，则所有到 AMP 云的连接均通过私有云进行筛选，AMPv 用作匿名代理，以确保受监控网络的安全和隐私。这包括导入Cisco Secure Endpoint 数据。私有云不通过外部连接共享任何终端数据。

如果您使用 AMP 私有云，以下集成功能将不可用：

- 使用Cisco Secure Endpoint 中配置的“阻止的应用”和“允许的应用”列表。（这些列表用于阻止或允许文件。）
- Firepower 生成的恶意软件事件在Cisco Secure Endpoint 中的可视性。

您可以配置多个私有云来支持所需的容量。

集成 Firepower 和 Cisco Secure Endpoint

如果您的组织已部署思科的 Cisco Secure Endpoint 产品，您可以将该应用与 Firepower 进行集成以实现集成 Firepower 和Cisco Secure Endpoint 的优势，第 38 页中所述的优势。

在与 Cisco Secure Endpoint集成时，即使已配置了 恶意软件防护 （面向 Firepower 的 AMP）连接，也必须配置 Cisco Secure Endpoint 连接。您可以配置多个 Cisco Secure Endpoint 云连接。

注释 未成功注册的 Cisco Secure Endpoint 连接不会影响 恶意软件防护。

开始之前

- 您必须是管理员用户才能执行此任务。
- 如果您的部署使用思科 AMP 私有云虚拟设备，请参阅 Cisco Secure Endpoint 和 AMP 私有云，第 39 页中的限制。
- Cisco Secure Endpoint必须在您的网络中正确设置并正常工作。
- 防火墙管理中心 必须具有互联网访问权限。

- 确保您的 防火墙管理中心 和 Cisco Secure Endpoint 可以互相通信。请参阅《Cisco Secure Firewall Management Center 管理指南》中安全、互联网接入和通信端口下的主题。
- 如果在重新映像或从备份恢复 防火墙管理中心 之后连接到 AMP 云，请使用 Cisco Secure Endpoint 管理控制台移除之前的连接。
- 在此程序期间，您需要使用 Cisco Secure Endpoint 凭证来登录 Cisco Secure Endpoint 控制台。

过程

步骤 1 选择**集成** > **AMP** > **AMP 管理**。

步骤 2 点击**添加 AMP 云连接**。

步骤 3 从**云名称**下拉菜单中，选择要使用的云。

- AMP 云最接近 防火墙管理中心的地理位置。

  APJC 是指亚太地区/日本/中国。

- 对于 AMP 私有云 (AMPv)，选择 **私有云** ，然后如 思科 AMP 私有云 ，第 14 页中所述继续操作。

步骤 4 如果要将此云用于 恶意软件防护 和 Cisco Secure Endpoint，请选中**用于面向 Firepower 的 AMP** 复选框。

如果配置其他云来处理 恶意软件防护（面向 Firepower 的 AMP）通信，则可以清除此复选框；如果这是唯一的 AMP 云连接，则无法清除。

步骤 5 点击 **Register**。

旋转状态 （ ） 图标指示连接处于待处理状态，例如，在 防火墙管理中心 上配置连接后，但在使用 Cisco Secure Endpoint 控制台对其进行授权之前。**已拒绝**（ ） 图标表示云已拒绝连接，或者连接因其他原因而失败。

步骤 6 确认是否要继续访问 Cisco Secure Endpoint 管理控制台，然后登录管理控制台中。

步骤 7 使用管理控制台，授权 AMP 云以将 Cisco Secure Endpoint 数据发送到 防火墙管理中心。

步骤 8 如果要限制 防火墙管理中心 接收的数据，请选择您的组织中要为其接收信息的特定组。

默认情况下，AMP 云发送所有组的数据。要管理组，请在 Cisco Secure Endpoint 管理控制台上选择**管理** > **组** 。有关详细信息，请参阅设备管理器联机帮助。

步骤 9 点击**允许 (Allow)** 以启用连接并开始传输数据。

点击**拒绝**会将您返回到 防火墙管理中心，其中连接标记为已拒绝。如果离开 Cisco Secure Endpoint 管理控制台上的“应用”页面，并且既未拒绝也未允许连接，则连接在 防火墙管理中心 的 Web 界面上标记为待处理。运行状况监控器在其中任一情况下**不**提示您连接失败。如果稍后要连接到AMP 云，请删除失败或待处理的连接，然后重新创建连接。

未完成 Cisco Secure Endpoint 连接注册不会禁用 恶意软件防护 连接。

步骤 10 要验证连接是否已正确配置，请执行以下操作：

a) 在 **集成** > **AMP** > **AMP 管理** 页面上，点击**思科 AMP 解决方案类型**列中包含Cisco Secure Endpoint 的“云名称”。

b) 在显示的Cisco Secure Endpoint 控制台窗口中，选择**账户** > **应用**。

c) 验证您的 防火墙管理中心在列表中。

d) 在Cisco Secure Endpoint 控制台窗口中，选择**管理** > **计算机**。

e) 验证您的 防火墙管理中心在列表中。

下一步做什么

- 在Cisco Secure Endpoint 控制台窗口中，根据需要配置设置。例如，定义您的管理中心的组成员，并分配策略。有关信息，请参阅Cisco Secure Endpoint 在线帮助或其他文档。
- 在高可用性部署中，在两个管理中心配置 AMP 云连接。这些配置不会同步。
- 如果防火墙管理中心在初始成功连接后无法连接到Cisco Secure Endpoint 门户，或者如果使用 AMP 门户取消注册了连接，则默认运行状况策略会向您发出警告。

  验证是否在**系统** > **运行状况** > **策略**下启用了**Cisco Secure Endpoint 状态**监控器。

网络恶意软件保护和文件策略的历史记录

功能	防火墙管理中心最低版本	最低版本	详细信息
与 AMP 云的通信	7.0	任意	不再支持使用旧版端口 32137 与 AMP 公共云或私有云进行通信。 新增/修改的屏幕：在**系统** > **集成** > **云服务**页面上，**对网络的 AMP 使用旧版端口 32137**选项不再可用。
章节重组	虽然是在第 6.4 版时间段内做出的更改，但是这些更改将会出现在重新发布的所有版本中	任意	重组了本章节的内容以减少混淆。 《Cisco Secure Firewall Management Center 管理指南》 中的某些内容已移至文件/恶意软件事件和网络文件轨迹一章或从中移出。

功能	防火墙管理中心最低版本	最低版本	详细信息
将 URL 过滤信息移动到了新的“URL过滤”章节	6.3	任意	将有关为 URL 过滤配置云通信的信息移动至新的“URL 过滤”章节。在本章节中对思科 CSI 主题的结构进行了相关更改。

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。