防病毒

本章包含以下部分：

防病毒扫描概述

思科设备包括来自第三方公司 Sophos 和 McAfee 的集成病毒扫描引擎。您可以获取思科设备的许可密钥，以便使用其中一种或这两种病毒扫描引擎来扫描邮件中的病毒，然后将设备配置为使用任一种防病毒扫描引擎扫描病毒。

McAfee 和 Sophos 引擎包含执行以下操作所需的程序逻辑：在特定位置扫描文件、处理和模式匹配病毒定义与在您的文件中找到的数据、在模拟环境下解密和运行病毒代码、应用启发式技术以识别新病毒，以及从合法文件中删除受感染代码。

您可以将设备配置为扫描邮件病毒（根据匹配的传入或外发邮件策略），如果发现病毒，则对该邮件执行不同的操作（包括“修复”病毒邮件、修改主题信头、添加额外的 X-Header、将邮件发送到备用地址或邮件主机、存档邮件或删除邮件）。

如果启用，则在设备的“工作队列”中进行反垃圾邮件扫描后，立即执行病毒扫描。（请参阅邮件管道和安全服务。）

默认情况下，默认传入和外发邮件策略启用病毒扫描。

相关主题

- 试用版密钥， 第 2 页
- 使用多个防病毒扫描引擎扫描邮件， 第 2 页

试用版密钥

思科设备为每个可用的防病毒扫描引擎附送30天的试用版密钥。通过以下方式可启用试用版密钥：访问“系统设置向导”(System Setup Wizard) 或“安全服务”(Security Services) > “Sophos/McAfee 防病毒”(Sophos/McAfee Anti-Virus) 页面中的许可协议，或者运行 `antivirusconfig` 或 `systemsetup` 命令（在 CLI 中）。一旦接受许可协议，默认情况下将为默认传入和外发邮件策略启用防病毒扫描引擎。有关在30天试用期过后如何启用该功能的信息，请与思科销售代表联系。可以通过**系统管理 > 功能密钥**页面或发出 `featurekey` 命令来查看评估的剩余时间。（有关详细信息，请参阅 功能密钥。）

使用多个防病毒扫描引擎扫描邮件

AsyncOS 支持使用多个防病毒扫描引擎扫描邮件 - 多层防病毒扫描。您可以将思科设备配置为：基于每个邮件策略使用一个或两个许可的防病毒扫描引擎。例如，可以为高管创建一个邮件策略，并将该策略配置为同时使用 Sophos 和 McAfee 引擎扫描邮件。

使用多个扫描引擎扫描邮件可结合 Sophos 和 McAfee 防病毒扫描引擎的优势，提供“深度防御”。每个引擎都具有领先的防病毒捕获率，但由于每种引擎依赖不同的技术基础（在McAfee防病毒过滤，第 4 页和Sophos 防病毒过滤，第 2 页中已讨论）来检测病毒，所以多次扫描方法更为有效。使用多个扫描引擎可能造成系统吞吐量下降，有关详细信息，请与您的思科支持代表联系。

无法配置病毒扫描的顺序。启用多层防病毒扫描时，McAfee 引擎首先扫描病毒，其次 Sophos 引擎再扫描病毒。如果 McAfee 引擎确定某封邮件无病毒，Sophos 引擎再扫描邮件，可添加第二层保护。如果 McAfee 引擎确定某封邮件包含病毒，思科设备将跳过 Sophos 扫描，并根据您配置的设置对病毒邮件执行操作。

Sophos 防病毒过滤

思科设备包括来自 Sophos, Plc. 的集成病毒扫描技术。Sophos 防病毒技术可以跨平台提供防病毒保护、检测和杀毒。

Sophos 防病毒技术提供病毒检测引擎，可扫描文件中的病毒、特洛伊木马和蠕虫。这些程序统称为恶意软件，即“带有恶意的软件”。各种恶意软件之间的相似之处在于，不仅允许防病毒扫描程序检测和删除病毒，还允许检测和删除所有类型的恶意软件。

相关主题

- 病毒检测引擎，第 3 页
- 病毒扫描，第 3 页
- 检测方法，第 3 页
- 病毒描述，第 4 页
- Sophos 警报 ，第 4 页
- 发现病毒时，第 4 页

病毒检测引擎

Sophos 病毒检测引擎的核心是 Sophos 防病毒技术。它使用类似于 Microsoft COM（组件对象模型）的专有架构，其中包括许多带有已明确定义接口的对象。该引擎使用的模块化文件系统基于独立、完备的动态库，每个库处理不同的“存储类”，例如文件类型。这种方法允许在通用数据源中应用病毒扫描操作，不考虑类型。

专业的数据加载和搜索技术，支持该引擎实现快速扫描。其中包含：

- 用于检测多态病毒的完整代码仿真程序
- 用于扫描存档文件内部的在线解压程序
- 用于检测和查杀宏病毒的 OLE2 引擎

思科设备通过 SAV 接口与病毒引擎集成。

病毒扫描

宽泛来讲，引擎的扫描功能由强强联合的两个重要组件来管理：知道查找位置的分类器和知道查找内容的病毒数据库。引擎按类型对文件分类，而不依赖扩展名。

病毒引擎查找系统收到的邮件正文和附件中的病毒；附件的文件类型有助于确定其扫描。例如，如果邮件的附件是可执行文件，引擎将检查信头，从中得知可执行文件代码的开始位置及其外观。如果该文件是 Word 文档，引擎将在宏数据流中查找。如果是 MIME 文件（用于邮件传输的格式），引擎将在存储附件的位置查找。

检测方法

检测病毒的方式取决于病毒类型。在扫描过程中，引擎将分析每个文件，识别类型，然后应用相关的技术。所有方法的基本原理都是查找特定类型的指令或指令的特定顺序。

相关主题

- 模式匹配，第 3 页
- 启发式方法，第 3 页
- 仿真，第 4 页

模式匹配

在模式匹配技术中，引擎知道特定的代码序列，并查找将代码识别为病毒的完全匹配。更常见的是，引擎查找与已知病毒代码序列类似的代码序列，但不一定完全相同。在创建扫描过程中比较文件的说明时，Sophos 病毒研究人员努力确保以尽可能通用的方式识别代码，以便（使用启发式技术，如下所述）引擎不仅可发现原始病毒，还能发现其后续衍生物。

启发式方法

病毒引擎可结合基本模式匹配技术与启发式技术（使用通用规则而不是特定规则），由此检测相同系列的多种病毒，即使 Sophos 研究人员可能仅分析了该系列的一种病毒亦不例外。利用此项技术，

只需创建一个描述，即可捕获一种病毒的多个变体。Sophos 可使用其他方法改动其启发式技术，将误报的可能性降到最低。

仿真

仿真是病毒引擎应用于多态病毒的一种技术。多态病毒是加密病毒，可自我修改以便隐藏自己。病毒代码没有明显固定的样式，并且该病毒每次传播时都以不同的方式对自己加密。运行时，可以自行解密。DOS 和 Windows 可执行文件中使用病毒检测引擎中的仿真程序，而多态宏病毒可通过以 Sophos 的病毒描述语言编写的检测代码发现。

此解密输出即真正的病毒代码，在仿真程序中运行它们后，Sophos 病毒检测引擎即可检测到这种输出。

发送到引擎进行扫描的可执行文件在仿真程序中运行，仿真程序可在病毒体写入内存时跟踪其解密。通常，病毒入口点位于文件前端，是要运行的首批内容。大多数情况下，只需解密少量病毒体，即可识别病毒。大多数安全可执行文件在执行几个指令后就会停止模拟，从而降低开销。

由于仿真程序在限定区域内运行，所以如果代码被证实为病毒，不会感染设备。

病毒描述

Sophos 每个月会与其他可信防病毒公司交换病毒。此外，客户每个月会直接向 Sophos 发送数千个可疑文件，其中大约 30% 被证实是病毒。每个样本都会在高度安全的病毒实验室进行严格分析，以确定其是否为病毒。对于每个新发现的病毒或病毒组，Sophos 将创建描述。

Sophos 警报

思科建议启用 Sophos 防病毒扫描的客户在 Sophos 站点 (http://www.sophos.com/virusinfo/notifications/) 上订用 Sophos 警报。从 Sophos 直接订用接收警报，可确保您了解最新的病毒爆发及其可用的解决方案。

发现病毒时

检测到病毒时，Sophos 防病毒可以修复（查杀）文件。Sophos 防病毒通常可以修复发现病毒的任何文件，在此之后即可毫无风险地使用该文件。具体采取的操作取决于病毒。

提到查杀病毒可能有所限制，因为并不总是能将文件恢复为原始状态。有些病毒会覆盖部分无法恢复的可执行程序。在这种情况下，需要定义如何处理附件可能无法修复的邮件。使用邮件安全功能可基于每个收件人配置这些设置：**邮件策略 > 传入或外发邮件策略**页 (GUI) 或 `policyconfig -> antivirus` 命令 (CLI)。有关配置这些设置的详细信息，请参阅配置面向用户的病毒扫描操作，第 7 页。

McAfee 防病毒过滤

McAfee® 扫描引擎可以：

- 通过匹配病毒签名与文件中数据的模式扫描文件。
- 在模拟环境下解密和运行病毒代码。
- 应用启发式技术以识别新的病毒。
- 从文件中删除受感染的代码。

相关主题

- 病毒签名模式匹配， 第 5 页
- 加密的多态病毒检测， 第 5 页
- 启发式分析， 第 5 页
- 发现病毒时， 第 4 页

病毒签名模式匹配

McAfee 使用防病毒定义 (DAT) 文件及扫描引擎检测特定病毒、病毒类型或其他可能不需要的软件。同时，它们还可以从文件中的已知位置开始搜索病毒签名，进而检测简单的病毒。通常，它们只需搜索文件的一小部分便可确定该文件是否未受到病毒侵害。

加密的多态病毒检测

复杂病毒通常使用两种技巧来规避签名扫描检测：

- **加密**。对病毒内的数据加密，使防病毒扫描程序看不到邮件或病毒的计算机代码。当激活病毒时，它会将自身转变为运行版本，然后执行。
- **多态**。此过程与加密类似，但病毒会自我复制，改变其外观。

为了应对此类病毒，引擎将使用仿真技术。如果引擎怀疑某个文件包含此类病毒，将创建一个人为环境，在此环境下病毒可以毫无危害地运行，直到其自我解码并显示出真正的形式。然后，引擎通常可通过扫描病毒签名识别该病毒。

启发式分析

仅使用病毒签名时，由于签名尚不可知，引擎无法检测新的病毒。因此，引擎可以使用其他技术 - 启发式分析。

携带病毒的计划、文档或邮件通常具有不同的特性。它们可能会尝试对文件进行自发修改、调用邮件客户端，或者通过其他方式进行自我复制。引擎可分析程序代码，以检测这些类型的计算机说明。此外，引擎还可搜索类似无病毒的合法行为（例如在执行操作前提示用户），由此避免引发错误警报。

通过这些技术，引擎可以检测到许多新的病毒。

发现病毒时

检测到病毒时，Sophos 防病毒可以修复（查杀）文件。Sophos 防病毒通常可以修复发现病毒的任何文件，在此之后即可毫无风险地使用该文件。具体采取的操作取决于病毒。

提到查杀病毒可能有所限制，因为并不总是能将文件恢复为原始状态。有些病毒会覆盖部分无法恢复的可执行程序。在这种情况下，需要定义如何处理附件可能无法修复的邮件。使用邮件安全功能可基于每个收件人配置这些设置：**邮件策略 > 传入或外发邮件策略**页 (GUI) 或 `policyconfig -> antivirus` 命令 (CLI)。有关配置这些设置的详细信息，请参阅配置面向用户的病毒扫描操作，第 7 页。

如何配置设备以扫描病毒

如何扫描邮件中的病毒

	相应操作	更多信息
第 1 步	在邮件安全设备上启用防病毒扫描。	启用病毒扫描和配置全局设置，第 6 页
第 2 步	定义您想要扫描其邮件病毒的用户组。	为发件人和收件人组创建邮件策略
第 3 步	（可选）配置您希望病毒隔离区如何处理邮件。	配置策略、病毒和爆发隔离区
第 4 步	确定您希望设备如何处理带病毒的邮件。	配置面向用户的病毒扫描操作，第 7 页
第 5 步	为您定义的用户组配置防病毒扫描规则。	为不同发件人和收件人组配置防病毒策略，第 12 页
第 6 步	（可选）发送邮件以测试配置。	向设备发送邮件以测试防病毒扫描，第 15 页

相关主题

- 启用病毒扫描和配置全局设置，第 6 页
- 配置面向用户的病毒扫描操作，第 7 页
- 为不同发件人和收件人组配置防病毒策略，第 12 页
- 防病毒配置注意事项，第 13 页
- 防病毒操作的流程图，第 14 页

启用病毒扫描和配置全局设置

在运行“系统设置向导”(System Setup Wizard) 时，您可能已启用防病毒扫描引擎。无论如何，请按照以下过程配置设置。

注释 根据您的功能密钥，可以启用 Sophos、McAfee 或两者。

过程

步骤 1 导航到**安全服务 > McAfee** 页面。

或

导航到**安全服务 > Sophos** 页面。

步骤 2 单击**启用 (Enable)**。

注释 单击**启用 (Enable)** 全局对设备启用该功能。但是，稍后必须在邮件策略中启用每个收件人的设置。

步骤 3 阅读许可协议后，滚动到页面底部并单击**接受 (Accept)** 以接受该协议。

步骤 4 单击**编辑全局设置 (Edit Global Settings)**。

步骤 5 选择最大病毒扫描超时值。

配置系统停止执行邮件防病毒扫描的超时值。默认值为 60 秒。

步骤 6 （可选）单击**启用自动更新**以启用引擎自动更新。

设备从更新服务器获取特定引擎所需的更新。

步骤 7 提交并确认更改。

下一步做什么

基于每个收件人配置防病毒设置。请参阅配置面向用户的病毒扫描操作，第 7 页。

配置面向用户的病毒扫描操作

思科设备中集成的病毒扫描引擎可根据您使用邮件安全管理器功能配置的策略（配置选项），处理传入和传出邮件中的病毒。使用邮件安全功能基于每个收件人启用防病毒操作：“邮件策略”(Mail Policies) >“传入或传出邮件策略”(Incoming or Outgoing Mail Policies) 页面 (GUI) 或 `policyconfig > antivirus` 命令 (CLI)。

相关主题

- 邮件扫描设置，第 7 页
- 邮件处理设置，第 8 页
- 配置邮件处理操作的设置，第 9 页

邮件扫描设置

- 仅扫描病毒：

  扫描系统处理的邮件是否存在病毒。不尝试修复受感染的附件。可以选择是丢弃附件并传送包含病毒的邮件的邮件正文，还是无法修复。

- 扫描并修复病毒：

  扫描系统处理的邮件是否存在病毒。如果在附件中发现病毒，系统将尝试“修复”附件。

- 丢弃附件

  您可以选择丢弃受感染的附件。

  当防病毒扫描引擎扫描邮件受感染的附件并丢弃附件后，原附件将替换为名为“已删除附件”的新附件。附件为纯文本类型，并包含以下信息：

```
This attachment contained a virus and was stripped.
 Filename: filename
Content-Type: application/filetype
```

如果用户的邮件由于感染不安全附件而出现任何形式的修改，用户总会收到通知。您也可以配置辅助通知操作（请参阅发送通知，第 11 页）。如果选择丢弃受感染的附件，在通知用户邮件修改时，则不需要通知操作。

- X-IronPort-AV 信头

  在设备上，防病毒扫描引擎处理的所有邮件都会向邮件中添加信头 X-IronPort-AV:。在调试防病毒配置的问题时（特别是被视为“不可扫描”的邮件），此信头可为您提供更多信息。对于是否在扫描订单邮件中包括 X-IronPort-AV 信头，可以切换。建议包含此信头。

邮件处理设置

可配置病毒扫描引擎来处理侦听程序收到的四种不同类别的邮件，并为每类邮件配置单独的操作。图 - 处理病毒扫描邮件的选项总结了启用病毒扫描引擎时系统执行的操作。

对于以下每种邮件类型，可以选择要执行的操作。下面介绍了相关操作说明（请参阅配置邮件处理操作的设置，第 9 页）。例如，可以为感染病毒的邮件配置防病毒设置，这样将丢弃受感染的附件、修改邮件主题，并向邮件收件人发送自定义警报。

已修复邮件处理

如果邮件经过全面扫描且所有病毒均已修复或删除，则认为这些邮件已修复。这些邮件将按原样传送。

已加密邮件处理

如果引擎因邮件中的加密或保护字段而无法完成扫描，则认为这些邮件已加密。标记为已加密的邮件也可以修复。

请注意加密检测邮件过滤器规则（请参阅加密检测规则）和面向“已加密”邮件的病毒扫描操作之间的差异。对于使用 PGP 或 S/MIME 加密的任何邮件，加密的邮件过滤器规则评估为“true”。已加密规则只能检测 PGP 和 S/MIME 加密的数据。无法检测受密码保护的压缩文件或包括加密内容的 Microsoft Word 和 Excel 文档。病毒扫描引擎将受密码保护的任何邮件或附件都视为“已加密”。

注释 如果要从 AsyncOS 3.8 或更早版本升级，并已配置 Sophos 防病毒扫描，则在升级后必须配置“加密邮件的处理”部分。

不可扫描邮件的处理

如果已达到扫描超时值或引擎因内部错误而变得不可用，则认为这些邮件不可扫描。被标记为不可扫描的邮件也可以修复。

感染病毒的邮件的处理

系统可能无法丢弃附件或彻底修复邮件。在这些情况下，可以配置系统如何处理仍可能包含病毒的邮件。

加密邮件、不可扫描的邮件和病毒邮件的配置选项相同。

配置邮件处理操作的设置

要应用的操作

选择针每种类型（已加密、不可扫描或具有病毒特征）的邮件要采取的总体操作：丢弃邮件、将邮件作为新邮件的附件传送、原样传送邮件或将邮件发送到防病毒隔离区（隔离区和防病毒扫描，第 10 页）。

将设备配置为作为新邮件的附件传送受感染的邮件，这样允许收件人选择如何处理原始受感染的附件。

如果选择传送邮件或作为新邮件的附件传送该邮件，还可以进行以下操作：

- 修改邮件主题
- 存档原始邮件
- 发送常规通知 在 GUI 的“高级”部分，可执行以下操作：
- 为邮件添加自定义信头
- 修改邮件收件人
- 将邮件发送到备用目标主机
- 发送自定义警报通知

注释 这些操作相互之间并不排斥，在不同的传入或外发策略中可以不同的方式组合其中某些或全部操作，以满足用户组的不同处理需求。有关使用这些选项定义各种扫描策略的详细信息，请参阅以下部分和防病毒配置注意事项，第 13 页。

已修复邮件只有两个高级选项：添加自定义信头和发送自定义警报通知。所有其他邮件类型都能访问全部高级选项。

隔离区和防病毒扫描

在标记为放入隔离区的同时，邮件继续通过邮件管道的其余部分。当邮件到达管道末尾时，如果此邮件被标记为放入一个或多个隔离区，邮件将加入这些队列。请注意，如果邮件没有到达管道末尾，邮件不会被放入隔离区。

例如，内容过滤器可能导致邮件被丢弃或退回，在这种情况下，不会隔离邮件。

存档原始邮件

您可以将系统判定为包含（或可能包含）病毒的邮件存档到“avarchive”目录。日志文件为 mbox 格式。您必须配置“防病毒存档”日志订用，才能存档包含病毒的邮件或无法全面扫描的邮件。有关详细信息，请参阅日志记录

注释 在 GUI 中，可能需要单击“高级”(Advanced) 链接，才能显示“存档原始邮件”(Archive original message) 设置。

修改邮件主题信头

您可以通过前置或后加某些文本字符串更改已识别邮件的文本，从而帮助用户轻松识别邮件及对识别的邮件排序。

注释 “修改邮件主题”字段中不会忽略空格。在此字段中输入的文本后面（如果是前置）或前面（如果是后加）添加空格，可分隔添加的文本与邮件的原始主题。例如，如果要后加，可在添加文本 `[WARNING: VIRUS REMOVED]` 后加上几个空格。

默认文本为：

适用于修改防病毒主题行的默认主题行文本

裁定	添加到主题的默认文本
已加密	`[WARNING: MESSAGE ENCRYPTED]`
受感染	`[WARNING: VIRUS DETECTED]`
已修复	`[WARNING: VIRUS REMOVED]`

裁定	添加到主题的默认文本
不可扫描	[WARNING: A/V UNSCANNABLE]

如果任何邮件包含多个状态，将会生成一封多部分通知邮件，用来通知用户设备对邮件所执行的操作（例如，通知用户已修复邮件中的病毒，但邮件的另一部分已加密）。

发送通知

当系统判定邮件包含病毒时，可以向发件人、收件人和/或其他用户发送默认通知。在指定要通知的其他用户时，请用逗号分隔多个地址（在 CLI 和 GUI 中）。默认通知邮件如下所示：

防病毒通知的默认通知

判定	**Notification**
已修复	在邮件中检测到以下病毒：<病毒名称> 执行操作：已丢弃感染的附件（或已修复感染的附件）。
已加密	由于加密，防病毒引擎无法全面扫描以下邮件。
不可扫描	防病毒引擎无法全面扫描以下邮件。
感染病毒	在邮件中检测到以下不可修复的病毒：<病毒名称>。

为邮件添加自定义信头

可以定义额外的自定义信头，从而添加到防病毒扫描引擎扫描的所有邮件。单击**是 (Yes)**，并定义信头名称和文本。

此外，还可以创建使用 `skip-viruscheck` 操作的过滤器，以便某些邮件绕开病毒扫描。请参阅绕过防病毒系统操作。

修改邮件收件人

您可以修改邮件收件人，使邮件传送到不同的地址。单击**是 (Yes)**，并输入新的收件人地址。

发送邮件到备用目标主机

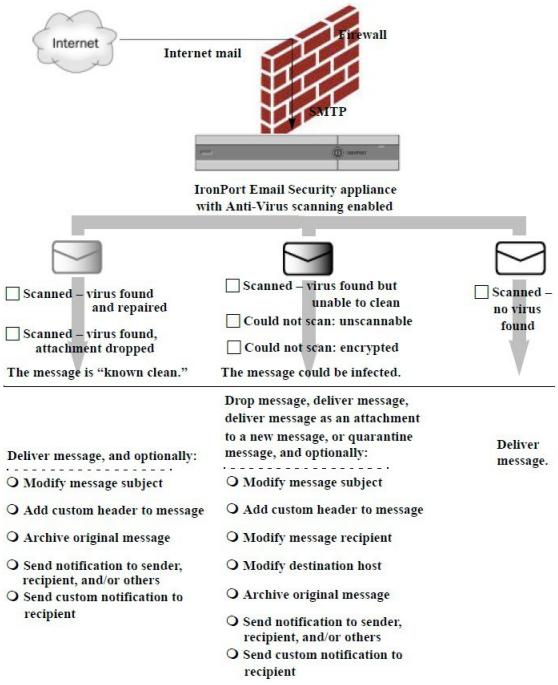
对于已加密、不可扫描或感染病毒的邮件，可以选择将通知发送到其他收件人或目标主机。单击**是 (Yes)**，并输入备用地址或主机。

例如，可以将可疑邮件路由到管理员邮箱或专门的邮件服务器，以便进行后续检查。如果该邮件包含多个收件人，则只会向备用收件人发送一个副本。

发送自定义警报通知

您可以向发件人、收件人和/或其他用户（邮件地址）发送自定义通知。为此，首先必须创建自定义通知，然后再配置设置。有关详细信息，请参阅了解文本资源。

图 *1:* 处理扫描病毒邮件的操作



注释 默认情况下，WHITELIST 发件人组引用的公共侦听程序所用的 $TRUSTED 邮件流策略中启用防病毒扫描。请参阅使用邮件流策略定义邮件发件人的访问规则。

为不同发件人和收件人组配置防病毒策略

为邮件策略编辑每个用户的防病毒设置的过程，与为传入或外发邮件编辑的过程基本相同。

各个策略（非默认策略）有一个使用“使用默认”(Use Default) 设置的额外字段。选择此设置可继承默认邮件策略的设置。

使用传入或外发邮件策略可基于每个收件人启用防病毒操作。可以在 GUI 中配置邮件策略，也可以在 CLI 中使用 policyconfig > antivirus 命令配置。在全局启用防病毒设置后，需要单独为创建的每个邮件策略配置这些操作。可以为不同的邮件策略配置不同的操作。

过程

步骤 1 导航到“邮件策略”(Mail Policies) >“传入邮件策略”(Incoming Mail Policies) 或“邮件策略”(Mail Policies) >“外发邮件策略”(Outgoing Mail Policies) 页面。

步骤 2 对于要配置的策略，单击防病毒安全服务的链接。

注释 单击默认策略行中的链接，以编辑默认策略的设置。

步骤 3 单击**是 (Yes)** 或**使用默认 (Use Default)**，对该策略启用防病毒扫描。

页面中的第一个设置定义是否对该策略启用此服务。可以单击**禁用 (Disable)** 完全禁用该服务。

对于默认策略之外的邮件策略，选择“是”(Yes) 可启用已修复、已加密、不可扫描和感染病毒的邮件中的字段。

步骤 4 选择防病毒扫描引擎。可以选择 McAfee 或 Sophos 引擎。

步骤 5 配置“邮件扫描”(Message Scanning) 设置。

有关详细信息，请参阅邮件扫描设置，第 7 页。

步骤 6 配置已修复、已加密、不可扫描和感染病毒的邮件的设置。

请参阅邮件处理设置，第 8 页 和 配置邮件处理操作的设置，第 9 页。

步骤 7 单击**提交**。

步骤 8 确认更改。

防病毒配置注意事项

丢弃附件标记会对防病毒扫描的工作方式产生很大的影响。当系统配置为“发现病毒且病毒无法修复时，丢弃受感染的附件”(Drop infected attachments if a virus is found and it could not be repaired) 时，将从邮件中清除任何病毒或不可扫描的 MIME 部分。然后，防病毒扫描的输出几乎都是正常邮件。GUI 面板中所示的为不可扫描邮件定义的操作几乎不会执行。

在“仅扫描病毒”环境中，这些操作将通过丢弃邮件不安全的部分来“清理”邮件。只有 RFC822 信头本身遭受攻击或遇到一些其他问题，才会执行不可扫描的操作。但是，如果为“仅扫描病毒”配置了防病毒扫描，但未选择“发现病毒且病毒无法修复时，丢弃受感染的附件”，则很可能执行不可扫描操作。

下表列出了一些常用的防病毒配置选项

常用的防病毒配置选项

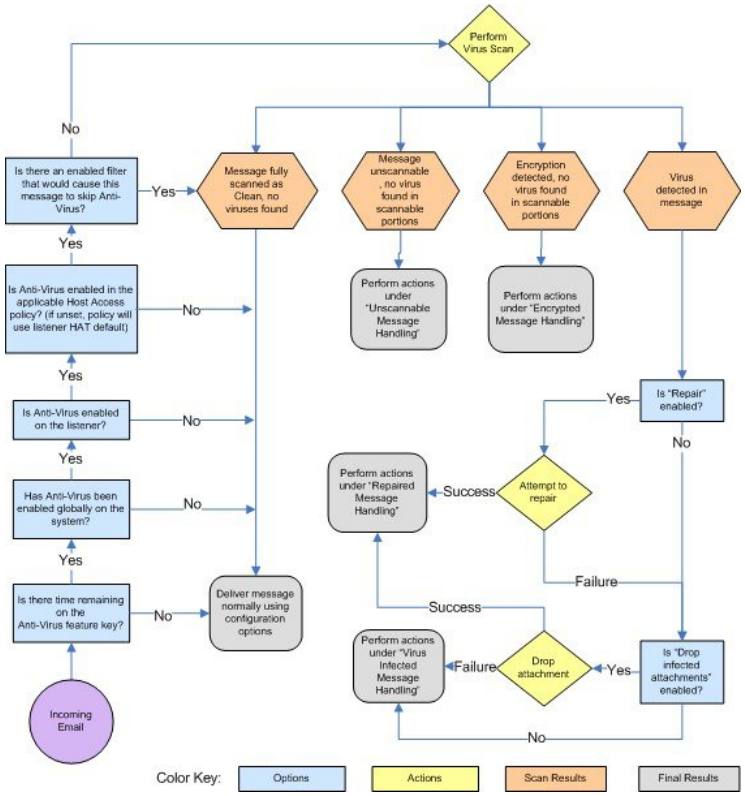
情况	防病毒配置
病毒大范围爆发 从系统中丢弃任何病毒邮件，而不进行任何其他处理。	**丢弃附件**：否 **扫描**：仅扫描 **清除病毒后的邮件**：传送 **不可扫描的邮件**：丢弃邮件 加密邮件：发送给管理员或隔离区以供审核。 病毒邮件：丢弃邮件

情况	防病毒配置
宽松策略 发送尽可能多的文档。	**丢弃附件**：是 **扫描**：扫描并修复 **清除病毒后的邮件**：[清除病毒] 并传送 **不可扫描的邮件**：作为附件转发 加密邮件：标记并转发 病毒邮件：隔离或标记并转发。
较保守型策略	**丢弃附件**：是 **扫描**：扫描并修复 **清除病毒后的邮件**：[清除病毒] 并传送 （对于更谨慎的策略，存档清除病毒后的邮件、。） **不可扫描的邮件**：发送通知、隔离或丢弃并存档。 加密邮件：标记并转发或视为不可扫描 病毒邮件：存档并丢弃
保守待审核 将可能包含病毒的邮件发送到隔离区邮箱，以便管理员能够审核内容。	**丢弃附件**：否 **扫描**：仅扫描 **清除病毒后的邮件**：传送（通常不会执行此操作） **不可扫描的邮件**：作为附件转发、alt-src-host 或 alt-rcpt-to 操作。 加密邮件：视为不可扫描 病毒邮件：转发到隔离区或管理员。

防病毒操作的流程图

下图说明防病毒操作和选项对设备处理的邮件有何影响。

图 *2:* 防病毒操作的流程图



注释 如果已配置多层防病毒扫描，则思科设备将首先使用 McAfee 引擎执行病毒扫描，其次是 Sophos 引擎。它将使用两个引擎扫描邮件，除非 McAfee 引擎检测到病毒。如果 McAfee 引擎检测到病毒，思科设备将执行为邮件策略定义的防病毒操作（修复、隔离等）。

向设备发送邮件以测试防病毒扫描

过程

步骤 1 针对邮件策略启用病毒扫描。

使用**安全服务 > Sophos/McAfee 防病毒**页面或 `antivirusconfig` 命令设置全局设置，然后使用“邮件安全管理器”页面 (GUI) 或 `policyconfig` 的 `antivirus` 子命令配置适用于特定邮件策略的设置。

步骤 2 打开标准的文本编辑器，然后键入下列字符串，让它们单独为一行，不含空格或换行符：

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

注释　以上所示的行在文本编辑器窗口中应显示为一行，所以请确保文本编辑器窗口最大化，并删除任何换行符。此外，请务必在文本消息开头的“X5O...”中键入字母 O，而不是数字 0。

如果您正在计算机上阅读本手册，可以直接从 PDF 文件或 HTML 文件中将该行复制粘贴到文本编辑器。如果复制此行，请务必删除多余的回车或空格。

步骤 3 使用名称 **EICAR.COM** 保存该文件。

文件大小为 68 或 70 个字节。

注释　此文件不是病毒 - 它不会传播或感染其他文件或者损害您的计算机。但是，在完成扫描程序测试后应删除该文件，以免警报影响其他用户。

步骤 4 将文件 EICAR.COM 附加到电子邮件中，并将其发送到与您在步骤 1 配置的邮件策略匹配的监听程序。

确保在该监听程序上接受您在测试邮件中指定的收件人。（有关详细信息，请参阅添加为其接受邮件的域和用户。）

请注意，如果在思科之外的网关（例如 Microsoft Exchange 服务器）上安装了针对外发邮件的病毒扫描软件，可能难以通过邮件发送文件。

注释　测试文件始终扫描为不可修复。

步骤 5 评估您在监听程序上为病毒扫描配置的操作，并确保它们已启用并按预期运行。

通过执行以下操作之一，可非常轻松地完成这些设置：

1. 将病毒扫描设置配置为“扫描并修复”(Scan and Repair) 模式或“仅扫描”(Scan only) 模式，不丢弃附件。
   - 发送邮件，使用 Eicar 测试文件作为附件。确认执行的操作是否与您对“感染病毒的邮件的处理”(Virus Infected Message Handling) 的配置（感染病毒的邮件的处理，第 9 页中的设置）匹配。
2. 将病毒扫描设置配置为“扫描并修复”(Scan and Repair) 模式或“仅扫描”(Scan only) 模式，丢弃附件。
   - 发送邮件，使用 Eicar 测试文件作为附件。
   - 确认执行的操作是否与您对“已修复邮件的处理”(Repaired Message Handling) 的配置（已修复邮件处理，第 8 页中的设置）匹配。

有关获取测试防病毒扫描用的病毒文件的详细信息，请参阅：
http://www.eicar.org/anti_virus_test_file.htm

此页面提供 4 个文件以供下载。请注意，如果您已安装客户端病毒扫描软件，下载和提取这些文件可能比较困难。

更新病毒定义

相关主题

- 关于通过 HTTP 检索防病毒更新 ， 第 17 页
- 配置更新服务器设置 ， 第 17 页
- 监控和手动检查防病毒更新， 第 17 页
- 验证设备上的防病毒文件是否已更新， 第 18 页

关于通过 HTTP 检索防病毒更新

Sophos 和 McAfee 经常根据新确定的病毒更新其病毒定义。必须将这些更新传递到您的设备。

默认情况下，思科设备配置为每 5 分钟检查一次更新。对于 Sophos 和 McAfee 防病毒引擎，服务器通过动态网站进行更新。

只要将更新有效下载到设备中，系统在更新时就不会超时。如果更新下载由于时间太长而暂停，则下载超时。

系统等待更新完成的最长时间（超过该时间将超时）是一个动态值，定义为比防病毒更新间隔少 1 分钟（在“安全服务”[Security Services] > “服务更新”[Service Updates] 中定义）。对于下载可能超过 10 分钟才能完成的大型更新时连接较慢的设备，此配置值比较有利。

配置更新服务器设置

通过“安全服务”(Security Services) > “服务更新”(Service Updates) 页面，可配置病毒更新设置。例如，您可以配置系统接收防病毒更新的方式和检查更新的频率。有关这些其他设置的详细信息，请参阅服务更新。

监控和手动检查防病毒更新

您可以使用“**安全服务**”>“**Sophos**”或“**McAfee**”页面或`antivirusstatus` CLI 命令验证设备是否已安装最新防病毒引擎和身份文件，并确认最后执行更新的时间。

也可以手动执行更新请参阅手动更新防病毒引擎 ， 第 17 页

手动更新防病毒引擎

过程

步骤 1 导航到“安全服务”(Security Services) > “Sophos 或 McAfee 防病毒”(Sophos or McAfee Anti-Virus) 页面。

步骤 2 单击“当前 McAfee/Sophos 防病毒文件”(Current McAfee/Sophos Anti-Virus Files) 表中的**立即更新 (Update Now)**。

设备将检查并下载最新更新。

下一步做什么

此外，也可以在命令行界面中使用 antivirusstatus 和 antivirusupdate 命令配置此操作

验证设备上的防病毒文件是否已更新

您可以查看更新程序日志，验证是否已成功下载、提取或更新防病毒文件。使用 tail 命令可显示更新程序日志订用的最后条目，确保已获取病毒更新。