病毒爆发过滤器

本章包含以下部分：

病毒爆发过滤器概述

病毒爆发过滤器既能保护您的网络免受大规模病毒爆发，又能在出现小规模非病毒攻击时防御它们，例如网络钓鱼、诈骗和恶意软件传播。大多数防恶意软件安全软件在收集数据及发布软件更新之前无法检测新爆发，而思科与之不同，我们可在爆发传播时收集相关数据并实时向您的邮件网关发送更新信息，从而阻止这些邮件到达用户。

思科使用全局流量模式开发规则，由此确定传入邮件安全还是爆发的一部分。可能属于爆发的邮件将被隔离，直到根据思科更新的爆发信息或 Sophos 和 McAfee 发布的新防病毒定义，确定它们安全为止。

小规模、非病毒攻击的邮件采用外观合法的设计、收件人的信息和指向网络钓鱼及恶意软件网站的自定义 URL，这些自定义 URL 仅短期有效，且网络安全服务无法识别。病毒爆发过滤器可分析邮件内容，并搜索 URL 链接以检测此类非病毒攻击。病毒爆发过滤器可以重写 URL，通过网络安全代理将流量重定向到可能有害的网站，由此警告用户其尝试访问的网站可能是恶意的，或者完全阻止该网站。

病毒爆发过滤器工作原理

相关主题

- 延迟、重定向和修改邮件, on page 2
- 威胁类别, on page 2

延迟、重定向和修改邮件

病毒爆发过滤器功能使用三种方法保护您的用户免受爆发：

- **延迟**。病毒爆发过滤器隔离可能属于病毒爆发或非病毒攻击的邮件。隔离后，邮件网关将会收到更新的爆发信息并重新扫描邮件以确认它是否属于攻击。

Note 如果爆发过滤器将具有垃圾邮件特征的邮件识别为具有爆发特征，则该邮件不会被发送到病毒爆发隔离区。

- **重定向**。病毒爆发过滤器重写非病毒攻击邮件中的 URL，以便在收件人尝试访问任何链接的网站时，通过思科网络安全代理重定向他们。如果网站仍在运行，代理将显示启动画面，警告用户该网站可能包含恶意软件；如果网站已经下线，将显示错误消息。有关重定向URL的详细信息，请参阅重定向 URL, on page 4。
- **修改**。除了重写非病毒威胁邮件中的URL之外，病毒爆发过滤器还可以修改邮件主题和在邮件正文上方添加免责声明，以警告用户注意邮件内容。有关详细信息，请参阅修改邮件, on page 5。

威胁类别

爆发过滤器功能可防御两类基于邮件的爆发：病毒爆发，即邮件附件中包含前所未见的病毒；以及非病毒威胁，其中包括网络钓鱼尝试、诈骗和恶意软件传播，通过链接传播到外部网站。

默认情况下，病毒爆发过滤器在爆发期间会扫描传入和外发邮件中的潜在病毒。如果在邮件网关上已启用反垃圾邮件扫描，则除了病毒爆发之外，还可对非病毒威胁启用扫描。

Note 要让病毒爆发过滤器扫描非病毒威胁，邮件网关需要一个功能密钥以用于反垃圾邮件或智能多次扫描。

相关主题

- 病毒爆发, on page 3

• 网络钓鱼、恶意软件传播和其他非病毒威胁, on page 3

病毒爆发

在对抗病毒爆发时，病毒爆发过滤器功能可为您提供领先优势。如果邮件附件包含前所未见的病毒，或现有病毒的变体通过专用网络和互联网快速传播，则会发生爆发。由于这些新病毒或变体进入互联网，所以从病毒发布到防病毒供应商发布更新的病毒定义，这段时间窗口最为关键。预先通知 - 即使只有几个小时，对于遏制恶意软件或病毒的传播也至关重要。在该漏洞时段，新发现的病毒可能全局传播，导致邮件基础设施中断服务。

网络钓鱼、恶意软件传播和其他非病毒威胁

包含非病毒威胁的邮件，其设计看起来与合法来源的邮件很像，而且通常是发送给少量收件人。为了看起来可靠，这些邮件可能具有以下一个或多个特征：

- 收件人的联系信息。
- 旨在模仿合法来源（例如社交网络和在线零售商）邮件的 HTML 内容。
- URL 指向使用新 IP 地址且仅短期上线的网站，也就是说，邮件和网络安全服务没有关于该网站的充足信息来确定其是否属于恶意网站。
- URL 指向 URL 缩短服务。

所有这些特性，使得这些邮件更加难以被作为垃圾邮件检测到。病毒爆发过滤器功能提供对这些非病毒威胁的多层防御，以防用户下载恶意软件或向可疑新网站提供个人信息。

如果 CASE 发现邮件中存在 URL，则将该邮件与现有爆发规则比较，以确定该邮件是否属于小规模非病毒爆发，然后分配威胁级别。根据威胁级别，邮件网关将延迟传送给收件人，直到收集到更多威胁数据；如果收件人尝试访问网站，设备将重写邮件中的 URL，以便将收件人重定向到思科网络安全代理。代理将显示启动页面，警告用户该网站可能包含恶意软件。

思科安全智能运营中心

思科安全智能运营中心 (SIO) 是一种安全生态系统，它将全球威胁信息、基于信誉的服务和复杂分析连接到邮件网关，从而提供更强大的保护，并缩短响应时间。

SIO 由三个组件组成：

- SenderBase、世界上最大的威胁监控网络和漏洞数据库。
- 威胁操作中心 (TOC)。一支安全分析师和自动化系统全球团队，提取由 SenderBase 收集的切实可行的情报。
- 动态更新。发生爆发时，自动将实时更新传送到邮件网关。

SIO 会比较全球 SenderBase 网络提供的实时数据与常规流量模式，以识别被证实为爆发征兆的异常。TOC 将审查数据并发布潜在爆发的威胁级别可能的爆发。邮件网关下载更新的威胁级别和爆发规则，并使用它们来扫描传入和外发邮件，以及爆发隔离区中已有的邮件。

有关当前病毒爆发的信息，请参阅以下 SenderBase 网站：

http://www.senderbase.org/

SIO 网站提供当前的非病毒威胁列表，包括垃圾邮件、网络钓鱼和恶意软件传播尝试：

http://tools.cisco.com/security/center/home.x

上下文自适应扫描引擎

病毒爆发过滤器由思科独特的情景自适应扫描引擎 (CASE) 提供支持。CASE 根据对邮件威胁的实时分析，定期利用自动调整的 100,000 多个自适应邮件属性。

对于病毒爆发，CASE 可分析邮件内容、上下文和结构，以便准确确定可能的自适应规则触发器。CASE 可以结合自适应规则与 SIO 发布的实时爆发规则，共同评估每封邮件并分配唯一的威胁级别。

要检测非病毒威胁，CASE 可扫描邮件中的 URL，如果发现一个或多个 URL，可使用 SIO 的爆发规则评估邮件的威胁级别。

根据邮件的威胁级别，CASE 将给出隔离邮件的时间建议，以防爆发。此外，CASE 还可决定重新扫描间隔，这样即可根据来自 SIO 的更新爆发规则重新评估邮件。威胁级别越高，越经常重新扫描隔离的邮件。

从隔离区放行邮件后，CASE 也会对它们重新扫描。如果 CASE 在重新扫描后确定某封邮件是垃圾邮件或包含病毒，可以重新将其隔离。

有关 CASE 的详细信息，请参阅 思科反垃圾邮件：概述。

延迟邮件

从发生爆发或邮件攻击到软件供应商发布更新的规则，这段期间是您的网络和用户最容易受到攻击的时段。在此段时间内，现代病毒可以全局传播，恶意网站可以传送恶意软件或收集用户的敏感信息。病毒爆发过滤器通过在限定时段内隔离可疑邮件，可保护您的用户和网络，并为思科和其他供应商提供时间调查新的爆发。

发生病毒爆发时，带附件的可疑邮件将被隔离，直到更新的爆发规则和新的防病毒签名证明邮件附件正常或属于病毒。

小规模、非病毒威胁包含的指向恶意网站的URL可能是短期上线，以便规避网络安全服务检测；或者通过URL缩短服务在中间放置可靠的网站，由此规避网络安全。通过隔离包含符合威胁级别阈值的 URL 的邮件，CASE 不仅有机会基于来自 SIO 的更新爆发规则重新评估邮件内容，而且这些邮件可以在隔离区保留足够长的时间，直到链接的网站下线或被网络安全解决方案阻止。

有关病毒爆发过滤器如何隔离可疑邮件的详细信息，请参阅动态隔离, on page 9。

重定向 URL

当 CASE 在病毒爆发过滤器阶段扫描邮件时，除了其他可疑内容以外，它还会搜索邮件正文中的 URL。CASE 使用发布的爆发规则来评估邮件是否属于威胁，然后为该邮件评定适当的威胁级别。根据威胁级别，病毒爆发过滤器将通过以下方式来保护收件人：重写所有URL（指向绕行域的URL除外），将收件人重定向到思科网络安全代理，并延迟邮件传送，以便TOC详细了解出现在更大爆发中的网站。有关绕行受信任的域的 URL 的详细信息，请参阅 URL 重写和绕行域, on page 18。

在邮件网关放行并传送邮件后，系统将通过思科网络安全代理重定向收件人访问网站的任何尝试。这是由思科托管的外部代理，如果网站仍在运行，它将显示启动画面，警告用户该网站可能具有危险。如果该网站已下线，启动画面将显示错误消息。

如果收件人决定单击邮件的URL，思科网络安全代理将在用户的Web浏览器中显示启动画面，警告该用户注意邮件的内容。下图显示启动画面警告的示例。收件人可以单击**忽略此警告 (Ignore this warning)** 继续访问网站，也可以单击**退出 (Exit)** 离开并安全关闭浏览器窗口。

Figure 1: 思科安全启动画面警告 ***(proxy_splash_screen)***

要访问思科网络安全代理，只能通过重写邮件中 URL。通过在 Web 浏览器中键入 URL，无法访问该代理。

Note 您可以自定义此启动画面的外观，并显示您所在组织的品牌，例如公司徽标、联系信息等。请参阅自定义最终用户访问恶意站点时看到的通知。

Tip 要将可疑垃圾邮件中的所有URL重定向到思科网络安全代理服务，请参阅使用自定义信头将疑似垃圾邮件中的 URL 重定向到思科网络安全代理：配置示例。

修改邮件

病毒爆发过滤器功能可以修改非病毒威胁邮件的邮件正文，不仅是重写 URL，还可提示用户该邮件是可疑威胁。病毒爆发过滤器功能可以修改主题信头，也可以在邮件正文上方添加关于邮件内容的免责声明。有关详细信息，请参阅邮件修改, on page 17。

通过“邮件策略”(Mail Policies) >“文本资源”(Text Resources) 页面的免责声明模板，可创建威胁免责声明。有关详细信息，请参阅文本资源管理概述。

规则的类型：自适应和病毒爆发

病毒爆发过滤器使用两类规则来检测潜在爆发：自适应和爆发。病毒爆发过滤器功能使用这两个规则集提供效果最高、标准最集中的威胁检测，以确保过滤器可聚焦于特定爆发。病毒爆发过滤器规则和操作对于管理员可见，而不是隐藏在幕后，由此可即时访问隔离的邮件及其被隔离的原因。

相关主题

- 适应规则, on page 6
- 爆发规则, on page 6

爆发规则

爆发规则由威胁操作中心 (TOC) 生成，威胁操作中心是思科安全情报运营中心的一部分，注重邮件整体，而不是附件文件类型。爆发规则使用 SenderBase 数据（实时和历史流量数据）及邮件参数的任意组合（例如附件文件类型、文件名称关键字或防病毒引擎更新）实时识别和防御爆发。系统会为爆发规则指定一个唯一 ID，用来在 GUI 的各个位置引用规则（例如爆发隔离区）。

然后，比较来自全球 SenderBase 网络的实时数据与此基准，以识别证实为爆发征兆的异常。TOC 可审查数据并发布威胁指标或威胁级别。威胁级别是一个介于 0（无威胁）和 5（非常危险）之间的数值（非常危险），衡量邮件是威胁的可能性（因为思科客户尚未针对其广泛部署任何其他网关防御）（有关详细信息，请参阅威胁级别, on page 7）。威胁级别由 TOC 作为爆发规则发布。

爆发规则中可以合并的一些示例特征包括：

- 文件类型、文件类型和大小、文件类型和文件名关键字等
- 文件名关键字和文件大小
- 文件名关键字
- 邮件 URL
- 文件名和 Sophos IDE

适应规则

自适应规则是 CASE 内的一组规则，可精确比较邮件属性与已知病毒爆发邮件的属性。这些规则是在学习大量病毒资料库内的已知威胁邮件和已知正常邮件后创建的。自适应规则通常随着资料库评估而更新。它们与现有的爆发规则相互补充，确保始终检测爆发邮件。虽然爆发规则在可能出现爆发时才生效，但自适应规则（一旦启用）“始终有效”，在本地捕获爆发邮件，然后在全局基础上形成完整的异常。此外，自适应规则可持续响应邮件流量和结构中的细微变化，面向客户提供更新的保护。

病毒爆发

基本上，病毒爆发过滤器规则就是威胁级别（例如威胁级别 4），与一组邮件和附件的特征相关联，例如文件大小、文件类型、文件名、邮件内容等。例如，假设思科 SIO 发现携带 .exe 附件的可疑邮件数量越来越多，附件大小为 143 KB，且文件名中包括特定关键字（例如“hello”）。于是，系统发布了爆发规则，提高与此条件匹配的邮件的威胁级别。默认情况下，您的邮件网关每隔 5 分钟就检查一次新发布的爆发和自适应规则，并进行下载（请参阅更新爆发过滤器规则, on page 15）。自适应规则更新的频率比爆发规则小。在邮件网关上，设置隔离可疑邮件的阈值。如果某封邮件的威胁级别等于或超过隔离阈值，则将该邮件发送到爆发隔离区。此外，还可以设置修改非病毒威胁邮件的阈值，重写可疑邮件中发现的任何 URL 或在邮件正文顶部添加通知。

威胁级别

下表 为其中每个级别提供一系列基本指导原则或定义。

Level	风险	含义
0	无	没有任何邮件威胁风险。
1	低	邮件是威胁的风险较低。
2	低/中	邮件是威胁的风险为低到中等。这是“可疑”威胁。
3	中	邮件属于确认的爆发，或其内容构成威胁的风险为中等到巨大。
4	高	邮件已确认属于大规模爆发，或其内容非常危险。
5	极高	邮件内容已确认属于极大规模、大规模和极其危险的爆发。

有关威胁级别和爆发规则的详细信息，请参阅病毒爆发过滤器规则, on page 14。

相关主题

- 设置隔离区威胁级别阈值的指导原则, on page 7
- 容器：“特定”和“始终”规则, on page 7

设置隔离区威胁级别阈值的指导原则

通过隔离区威胁级别阈值，管理员可以加大或减小隔离可疑邮件的积极性。设置越低（1或2）表示积极性越高，将隔离更多邮件；相反，得分越高（4或5），积极性越低，且只能隔离极大可能是恶意的邮件。

同一阈值既适用于病毒爆发，也适用于非病毒威胁，但可以为病毒攻击和其他威胁指定不同的隔离区保留时间。有关详细信息，请参阅动态隔离, on page 9。

思科建议使用默认值 3。

容器：“特定”和“始终”规则

容器文件是包含其他文件的压缩 (.zip) 存档文件。TOC 可以发布处理存档文件中特定文件的规则。

例如，如果 TOC 确定某个病毒爆发包含带 .exe 文件的 .zip 文件，则会发布特定爆发规则，由此设置 .zip 文件内 .exe 文件的威胁级别 (.zip[exe])，但不会为 .zip 文件内包含的任何其他文件类型（例如 .txt 文件）设置威胁级别。第二规则 (.zip[*]) 涵盖该容器文件类型中的所有其他文件类型。容器总是使用“始终”(Always) 规则来计算邮件的威胁级别，而不考虑容器内的文件类型。如果已知所有这类容器类型都具有危险，SIO 则会发布一项始终规则。

Table 1: 回退规则和威胁级别得分

爆发规则	爆发等级	说明
.zip(exe)	4	此规则集为 .zip 文件中的 .exe 文件设置威胁级别 4。

爆发规则	爆发等级	说明
.zip(doc)	0	此规则集为 .zip 文件中的 .doc 文件设置威胁级别 0。
zip(*)	2	此规则集为所有 .zip 文件设置威胁级别2，不考虑其中包含的文件类型。

病毒爆发过滤器功能的工作原理

邮件网关在处理邮件时，邮件将通过一系列步骤，即“邮件管道”（有关邮件管道的详细信息，请参阅了解邮件通道）。如果为该邮件策略启用了反垃圾邮件和防病毒扫描引擎，则在邮件通过邮件管道继续处理时，将运行这些引擎。换句话说，病毒爆发过滤器功能不会扫描已知垃圾邮件或包含已识别病毒的邮件，因为系统已根据您的反垃圾邮件和防病毒设置，将这些邮件从邮件流中删除 - 删除、隔离等。因此，抵达病毒爆发过滤器功能的邮件已被标记为无垃圾邮件和病毒。请注意，根据更新的垃圾邮件规则和病毒定义，从隔离区放行及由 CASE 重新扫描被病毒爆发过滤器隔离的邮件时，可能会再次将其标记为垃圾邮件或包含病毒。

Note 因过滤器或引擎被禁用而跳过反垃圾邮件和防病毒扫描的邮件，仍要接受病毒爆发过滤器扫描。

相关主题

- 邮件得分, on page 8
- 动态隔离, on page 9

邮件得分

如果新的病毒攻击或非病毒威胁放行而肆虐，任何防病毒或反垃圾邮件软件都还无法识别该威胁，这正是病毒爆发过滤器功能发挥重大价值的所在。CASE 将使用发布的爆发和自适应规则扫描传入邮件，并对其评分（请参阅规则的类型：自适应和病毒爆发, on page 5）。邮件得分与其威胁级别相对应。CASE 根据邮件匹配的规则（如有）分配相应的威胁级别。如果没有关联的威胁级别（邮件与任何规则都不匹配），则为邮件分配威胁级别 0。

一旦完成该计算，邮件网关将检查该邮件的威胁级别是否符合或超过隔离或邮件修改阈值，并隔离邮件或重写其 URL。如果威胁级别低于阈值，将继续传送该邮件以便在管道中进一步进行处理。

此外，CASE会对照最新规则重新评估当前隔离的邮件，以确定邮件的最新威胁级别。这样可确保，只在隔离区内保留威胁级别与爆发邮件一致的邮件，而不再构成威胁的邮件经过自动重新评估后将离开隔离区。

如果一封爆发邮件有多个得分 - 一个得分来自自适应规则（或为多个自适应规则适用时的最高得分），另一个得分来自爆发规则（或为多个爆发规则适用时的最高得分），则使用智能算法来确定最终威胁级别。

可以使用病毒爆发过滤器功能，而不在邮件网关上启用防病毒扫描。两种安全服务的宗旨是相辅相成，但也可以独立工作。也就是说，如果没有在邮件网关上启用防病毒扫描，您则需要监控防病毒

供应商的更新，并手动放行或重新评估爆发隔离区的部分邮件。使用病毒爆发过滤器而未启用防病毒扫描时，请牢记以下事项：

- 应该禁用自适应规则
- 将根据爆发规则来隔离邮件
- 如果威胁级别降低或时间过期，邮件将被放行

下游防病毒供应商（桌面/组件）可能会捕获放行的邮件。

Note 要通过病毒爆发过滤器功能扫描非病毒威胁，需要在邮件网关上全局启用反垃圾邮件扫描。

动态隔离

病毒爆发过滤器功能的爆发隔离区是用来临时存储邮件的区域，直到邮件被确认为威胁或可安全传送给用户为止。（有关详细信息，请参阅病毒爆发生命周期和规则发布, on page 10。）可通过多种方式放行爆发隔离区中隔离的邮件。下载新规则后，系统将根据 CASE 计算的推荐重新扫描间隔，重新扫描爆发隔离区中的邮件。如果某封邮件修订的威胁级低于隔离区保留阈值，则会自动放行该邮件（不考虑爆发隔离区的设置），由此尽可能地减少其在隔离区中耗费的时间。如果在重新评估邮件时有新规则发布，则会重新启动重新扫描。

请注意，当新的防病毒签名可用时，不会从病毒爆发隔离区自动放行作为病毒攻击隔离的邮件。新规则可能会引用新的防病毒签名，也可能不会引用；但邮件不会由于防病毒引擎更新而被放行，除非爆发规则将该邮件的威胁级别改为低于威胁级别阈值的得分。

此外，在 CASE 建议的保留期限过后，也会从爆发隔离区放行邮件。CASE 根据邮件的威胁级别计算保留期限。您可以为病毒爆发和非病毒威胁定义独立的最长保留时间。如果 CASE 建议的保留时间超过该威胁类型的最长保留时间，邮件网关将在最长保留时间过后放行邮件。病毒邮件的默认最长隔离期限为 1 天。非病毒威胁的默认隔离期限为 4 小时。您可以手动从隔离区放行邮件。

另外，如果隔离区已满且有更多邮件插入（这种情况称为“溢出”），邮件网关也会放行邮件。只有爆发隔离区的容量达到100%，并有新邮件添加到隔离区时，才会发生溢出。此时，将按以下优先顺序放行邮件：

- 自适应规则隔离的邮件（计划尽快放行的邮件优先）
- 爆发规则隔离的邮件（计划尽快放行的邮件优先）

一旦爆发隔离区的容量低于100%，则停止溢出放行。有关如何处理隔离区溢出的详细信息，请参阅邮件在隔离区中的保留时间和自动处理的隔离邮件的默认操作。

如果为邮件策略启用了防病毒和反垃圾邮件引擎，则这些引擎将对从爆发隔离区放行的邮件重新扫描。如果邮件现在被标记为已知病毒或垃圾邮件，则会按照邮件策略设置进行处理（包括可能再次被病毒隔离区或垃圾邮件隔离区隔离）。有关详细信息，请参阅病毒爆发过滤器功能和病毒爆发隔离区, on page 19。

因此，需要注意的是，在邮件的生命期限内，它实际上可能被隔离两次 - 一次是由于病毒爆发过滤器功能，一次是从爆发隔离区释放时。如果两次扫描（在病毒爆发过滤器之前和从爆发隔离区放行

时）的判定相符，则不会再次隔离邮件。另请注意，病毒爆发过滤器功能不会对邮件采取任何最终操作。病毒爆发过滤器功能将隔离邮件（以便进一步处理），或将邮件移至管道中的下一个步骤。

相关主题

- 病毒爆发生命周期和规则发布, on page 10

病毒爆发生命周期和规则发布

在病毒爆发生命周期的早期阶段，系统使用更广泛的规则来隔离邮件。随着越来越多的信息变得可用，发布的规则越来越突出重点，从而缩小了对隔离内容的定义。发布新规则后，不再被视为潜在病毒邮件的邮件将从隔离区中放行（发布新规则时，会重新扫描爆发隔离区中的邮件）。

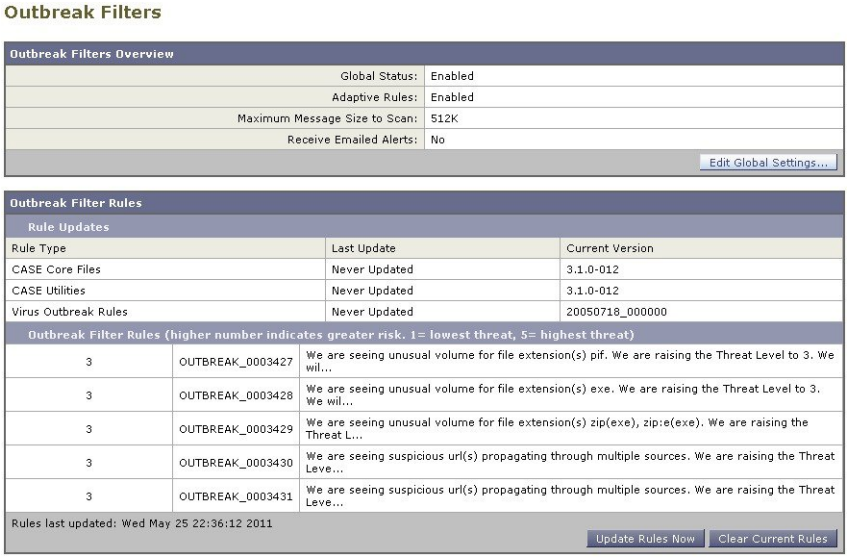
Table 2: 病毒爆发生命周期的规则示例

时间	规则类型	规则说明	操作
T=0	自适应规则（基于过去的爆发）	根据 100,000 多个邮件属性合并的规则集，分析邮件内容、情景和结构	如果邮件与自适应规则匹配，则自动隔离邮件。
T=5 分钟	爆发规则	隔离包含 .zip (exe) 文件的邮件	隔离属于包含 .exe 的 .zip 的所有附件
T=10 分钟	爆发规则	隔离包含的 .zip (exe) 文件超过 50 KB 的邮件	如果任何邮件包含的 .zip (exe) 文件小于 50 KB，将从隔离区放行
T=20 分钟	爆发规则	隔离 .zip (exe) 文件介于 50 到 55 KB 之间且文件名中包含“Price”的邮件	不符合此条件的任何邮件将从隔离区放行。
T=12 小时	爆发规则	对照新签名扫描	对照最新的防病毒签名扫描所有剩余的邮件

管理病毒爆发过滤器

登录到图形用户界面 (GUI)，选择菜单中的“安全服务”(Security Services)，然后单击“病毒爆发过滤器”(Outbreak Filters)。

Figure 2: 病毒爆发过滤器主页



“病毒爆发过滤器”(Outbreak Filters) 页面显示两部分：病毒爆发过滤器概况和当前病毒爆发过滤器规则的列表（如有）。

在上图中，已启用病毒爆发过滤器、自适应扫描，并且最大邮件大小设置为 512k。要更改这些设置，请单击**编辑全局设置 (Edit Global Settings)** 有关编辑全局设置的详细信息，请参阅配置病毒爆发过滤器全局设置, on page 11。

“病毒爆发过滤器规则”(Outbreak Filter Rules) 部分列出各种组件（规则引擎以及规则本身）最新更新的时间、日期和版本，以及当前的病毒爆发过滤器规则及威胁级别列表。

有关爆发规则的详细信息，请参阅病毒爆发过滤器规则, on page 14。

相关主题

- 配置病毒爆发过滤器全局设置, on page 11
- 病毒爆发过滤器规则, on page 14
- 爆发过滤器功能和邮件策略, on page 15
- 病毒爆发过滤器功能和病毒爆发隔离区, on page 19

配置病毒爆发过滤器全局设置

Procedure

步骤 1 依次单击**安全服务 (Security Services)** > **病毒爆发过滤器 (Outbreak Filters)**。

步骤 2 单击**编辑全局设置 (Edit Global Settings)**。

步骤 3 根据您的要求，执行以下操作：

- 全局启用病毒爆发过滤器

- 启用自适应规则扫描
- 设置要扫描的文件的最大大小（请注意要以字节为单位输入大小）
- 启用爆发过滤器警报
- 启用网络交互跟踪请参阅Web 互动跟踪。

步骤 4 提交并确认更改。

What to do next

此功能还可以通过 outbreakconfig CLI 命令来获取（请参阅《适用于思科安全邮件网关的 AsyncOS 的 CLI 参考指南》）。做出更改后，请提交并确认更改。

Note 无法使用 Web 界面启用 URL 的日志记录。有关使用 CLI 启用 URL 日志记录的说明，请参阅启用 URL 日志记录和 URL 邮件跟踪详细信息 , on page 13。

相关主题

- 启用病毒爆发过滤器功能, on page 12
- 启用自适应规则, on page 12
- 启用病毒爆发过滤器的警报, on page 13
- 启用 URL 日志记录和 URL 邮件跟踪详细信息 , on page 13

启用病毒爆发过滤器功能

要全局启用病毒爆发过滤器功能，请选中“爆发过滤器全局设置”(Outbreak Filters Global Settings) 页面“启用爆发过滤器”(Enable Outbreak Filters) 旁边的复选框，然后单击**提交 (Submit)**。您必须首先同意病毒爆发过滤器许可协议。

一旦全局启用，则可以针对每个传入和外发邮件策略（包括默认策略）单独启用或禁用病毒爆发过滤器功能。有关更多信息，请参阅爆发过滤器功能和邮件策略, on page 15。

病毒爆发过滤器功能使用情景自适应扫描引擎 (CASE) 检测病毒威胁，不考虑是否启用反垃圾邮件扫描，但要扫描非病毒威胁，则确实要在邮件网关上全局启用反垃圾邮件或智能多次扫描。

Note 如果您尚未在系统设置期间同意许可（请参阅第 4 步：安全），则必须在“安全服务”(Security Services) >“病毒爆发过滤器”(Outbreak Filters) 页面上单击**启用 (Enable)**，然后阅读并同意许可。

启用自适应规则

自适应扫描支持在病毒爆发过滤器中使用自适应规则。如果与邮件内容相关的病毒签名或垃圾邮件条件不可用，则使用一组因素或特征（文件大小等）来确定邮件属于爆发的可能性。要启用自适应

扫描，请选中“病毒爆发过滤器全局设置”(Outbreak Filters Global Settings) 页面“启用自适应规则”(Enable Adaptive Rules) 旁边的复选框，然后单击**提交 (Submit)**。

启用病毒爆发过滤器的警报

选中标记为“邮件警报”的框，以启用病毒爆发过滤器功能警报。启用病毒爆发过滤器启用邮件警告，只是让警报引擎发送有关病毒爆发过滤器的警报。通过“系统管理”(System Administration) 选项卡的“警报”(Alerts) 页面，指定发送的以及配置的邮件地址。有关配置病毒爆发过滤器警报的详细信息，请参阅警报、SNMP 陷阱和病毒爆发过滤器, on page 22。

启用 URL 日志记录和 URL 邮件跟踪详细信息

默认情况下，将禁止记录与URL相关的日志，并禁止在邮件跟踪详细信息中显示此信息。其中包括以下事件的日志：

- 邮件中与 URL 类别过滤器匹配的任何 URL 的类别
- 邮件中与 URL 信誉过滤器匹配的任何 URL 的信誉得分
- 病毒爆发过滤器将重写邮件中的任何 URL

要启用这些事件的日志记录，请在命令行界面 (CLI) 中使用 outbreakconfig 命令。

相关主题

- 示例：使用 outbreakconfig 命令启用 URL 的日志记录 , on page 13
- 管理爆发过滤器规则, on page 14
- 示例：使用 outbreakconfig 命令启用 URL 的日志记录 , on page 13

示例：使用 outbreakconfig 命令启用 URL 的日志记录

以下示例展示如何使用 outbreakconfig 命令启用 URL 的日志记录

```
mail.example.com> outbreakconfig

Outbreak Filters: Enabled

Choose the operation you want to perform:

- SETUP - Change Outbreak Filters settings.

[]> setup

Outbreak Filters: Enabled

Would you like to use Outbreak Filters? [Y]>

Outbreak Filters enabled.

Outbreak Filter alerts are sent when outbreak rules cross the threshold (go above or back
down below), meaning that new messages of

certain types could be quarantined or will no longer be quarantined, respectively.

Would you like to receive Outbreak Filter alerts? [N]>

What is the largest size message Outbreak Filters should scan?
```

```
[524288]>

Do you want to use adaptive rules to compute the threat level of messages? [Y]>

Logging of URLs is currently disabled.

Do you wish to enable logging of URL's? [N]> Y

Logging of URLs has been enabled.

The Outbreak Filters feature is now globally enabled on the system.  You must use the
'policyconfig' command in the CLI or the Email

Security Manager in the GUI to enable Outbreak Filters for the desired Incoming and Outgoing
 Mail Policies.

Choose the operation you want to perform:

- SETUP - Change Outbreak Filters settings.

[]>
```

病毒爆发过滤器规则

爆发规则由思科安全情报运营中心发布，邮件网关每隔5分钟将检查一次新爆发规则，并进行下载。此更新间隔可以更改。有关详情，请参见配置服务器设置以下载升级和更新。

相关主题

- 管理爆发过滤器规则, on page 14

管理爆发过滤器规则

由于系统自动下载病毒爆发过滤器规则，所以实际上并不需要用户进行任何管理。

但是，如果您的邮件网关一段时间后由于某种原因无法访问思科的更新服务器获取新规则，可能是本地缓存的得分失效，例如某个已知病毒附件类型在防病毒软件中已更新和/或不再构成威胁时。这时，您可能希望不再隔离具有这些特征的邮件。

可以单击**立即更新规则 (Update Rules Now)**，从思科更新服务器手动下载更新的爆发规则。

Note **立即更新规则 (Update Rules Now)** 按钮不会“刷新”邮件网关上所有现有的爆发规则，只是替换更新的爆发规则。如果思科的更新服务器上没有可用的更新，单击此按钮时，邮件网关不会下载任何爆发规则。

相关主题

- 更新爆发过滤器规则, on page 15

更新爆发过滤器规则

默认情况下，邮件网关每隔 5 分钟尝试下载一次新病毒爆发过滤器规则。通过“安全服务”(Security Services) >“服务更新”(Service Updates) 页面，可更改此间隔。有关详细信息，请参阅服务更新。

爆发过滤器功能和邮件策略

病毒爆发过滤器功能包含可根据邮件策略进行的设置。在邮件网关上，可针对每个邮件策略启用或禁用病毒爆发过滤器功能。根据邮件策略，可对特定文件扩展名和域免于执行病毒爆发过滤器功能处理。此功能还可以通过 policyconfig CLI 命令来获取（请参阅《适用于思科安全邮件网关的 AsyncOS 的 CLI 参考指南》）。

Note 要通过病毒爆发过滤器功能扫描非病毒威胁，需要在邮件网关上全局启用反垃圾邮件或智能多次扫描。

要修改特定邮件策略的病毒爆发过滤器功能设置，请单击要更改策略“病毒爆发过滤器”(Outbreak Filters) 列中的链接。

要启用和自定义特定邮件策略的病毒爆发过滤器功能，请选择**启用病毒爆发过滤器（自定义设置）(Enable Outbreak Filtering (Customize Settings))**。

可以为邮件策略配置以下病毒爆发过滤器设置：

- 隔离区威胁级别
- 隔离区最长保留时间
- 立即传送非病毒威胁邮件，而不将其添加到隔离区
- 绕行的文件扩展名类型
- 邮件修改阈值
- 使用自定义文本和爆发过滤器变量修改主题信头，例如 $threat_verdict、$threat_category、$threat_type、$threat_description 和 $threat_level。
- 包括以下邮件信头：
  - X-IronPort-Outbreak-Status
  - X-IronPort-Outbreak-Description
- 将邮件发送到备用目标，例如邮件网关或交换服务器。
- URL 重写
- 威胁免责声明

选择**启用爆发过滤（继承默认邮件策略设置）(Enable Outbreak Filtering [Inherit Default mail policy settings])**,可使用为默认邮件策略定义的病毒爆发过滤器设置。如果默认邮件策略已启用病毒爆发过滤器功能，则所有其他邮件策略将使用相同的病毒爆发过滤器设置，除非已进行自定义。

进行更改后，请确认您的更改。

相关主题

- 设置隔离区级别阈值, on page 16
- 隔离区最长保留时间, on page 16
- 绕过文件扩展名类型, on page 16
- 邮件修改, on page 17

设置隔离区级别阈值

从列表中选择适用于爆发威胁的隔离区威胁级别阈值。数字越小,表示隔离的邮件越多；而数字越大，隔离的邮件越少。思科建议使用默认值 3。

有关详细信息，请参阅设置隔离区威胁级别阈值的指导原则, on page 7。

隔离区最长保留时间

指定邮件留在爆发隔离区的最长时间。对于可能包含病毒附件的邮件和可能包含网络钓鱼或恶意软件链接等其他威胁的邮件，可以指定不同的保留时间。对于非病毒威胁，选中**传送邮件而不将其添加到隔离区 (Deliver messages without adding them to quarantine)** 复选框可立即传送邮件，而不将其添加到隔离区。

Note 除非已为策略启用“邮件修改”(Message Modification)，否则无法隔离非病毒威胁。

CASE 建议在向邮件分配威胁级别时设置隔离区保留期限。在 CASE 建议的时间内，邮件网关将保持隔离邮件，除非建议的时间超出隔离区适用于其威胁类型的最长保留时间。

绕过文件扩展名类型

您可以修改策略以绕行特定文件类型。CASE 计算邮件的威胁级别时，不含绕行的文件扩展名；但附件仍由其余邮件安全管道处理。

要绕行某个文件扩展名，请单击“绕行附件扫描”(Bypass Attachment Scanning)，选择或键入文件扩展名，然后单击**添加扩展名 (Add Extension)**。AsyncOS 在“绕行的文件扩展名”(File Extensions to Bypass) 列表中显示扩展名类型。

要从绕行的扩展名列表中删除某个扩展名，请在“绕行的文件扩展名”(File Extensions to Bypass) 列表中单击该文件扩展名旁边的垃圾桶图标。

相关主题

- 绕过文件扩展名：容器文件类型, on page 16

绕过文件扩展名：容器文件类型

绕行文件扩展名时，如果扩展名在绕行的扩展名列表中，将绕行容器文件中的相关文件（例如 .zip 文件中的 .doc 文件）。例如，如果将 .doc 添加到绕行的扩展名列表中，则绕过所有 .doc 文件，即便它们在容器文件内亦不例外。

邮件修改

如果希望邮件网关扫描网络钓鱼尝试或恶意软件网站链接等非病毒威胁，请启用“邮件修改”(Message Modification)。

根据邮件的威胁级别，AsyncOS 可以修改邮件以重写所有 URL，从而通过思科网络安全代理重定向收件人（如果他们尝试打开邮件中的网站）。另外，邮件网关也可以在邮件中添加免责声明，以提示用户邮件内容可疑或是恶意的。

要隔离非病毒威胁邮件，需要启用邮件修改。

相关主题

- 邮件修改威胁等级, on page 17
- 邮件主题, on page 17
- 病毒爆发过滤器邮件信头, on page 17
- 备用目标邮件主机, on page 18
- URL 重写和绕行域, on page 18
- 威胁免责声明, on page 19

邮件修改威胁等级

从列表中选择一个邮件修改威胁级别阈值。此设置决定是否根据 CASE 返回的威胁级别修改邮件。数字越小，表示要修改的邮件越多；而数字越大，表示要修改的邮件越少。思科建议使用默认值3。

邮件主题

对于包含已修改链接的非病毒威胁邮件，可以改动其主题信头文本，以便通知用户为了提供保护已对邮件进行修改。在主题信头前面或后面加上自定义文本、病毒爆发过滤器变量，例如：`$threat_verdict`、`$threat_category`、`$threat_type`、`$threat_description` 和 `$threat_level`，或者两者的组合。要插入变量，请单击**插入变量 (Insert Variables)** 并从变量列表中选择。

“邮件主题”(Message Subject) 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，如果要前加，可在添加文本 `[MODIFIED FOR PROTECTION]` 后加上几个空格。

Note “邮件主题”(Message Subject) 字段仅接受 US-ASCII 字符。

病毒爆发过滤器邮件信头

可以向邮件中添加以下附加信头：

信头	格式	示例	选项
X-IronPort-Outbreak-Status	`X-IronPort-Outbreak-Status: $threat_verdict, level $threat_level, $threat_category - $threat_type`	`X-IronPort-Outbreak-Status: Yes, level 4, Phish - Password`	• 对所有邮件启用 (Enable for all messages) • 仅为非病毒爆发启用 (Enable only for non-viral outbreak) • 禁用 (Disable)
X-IronPort-Outbreak-Description	`X-IronPort-Outbreak-Description: $threat_description`	`X-IronPort-Outbreak-Description: It may trick victims into submitting their username and password on a fake website.`	• 启用 • 禁用

Note 如果要根据这些信头过滤邮件，则必须将病毒爆发过滤器处理的邮件发回到邮件网关（通过配置备用目标邮件主机），然后使用与这些信头匹配的内容过滤器扫描它们。

备用目标邮件主机

如果要对病毒爆发过滤器处理的邮件执行基于内容过滤器的扫描，则必须将病毒爆发过滤器配置为：将处理的邮件发回到邮件网关。这是因为，在处理管道中先进行内容过滤器扫描，然后才执行病毒爆发过滤器扫描。

在**备用目标邮件主机 (Alternate Destination Mail Host)** 字段中，输入要发送处理的邮件（以供进一步扫描）的邮件网关的 IP 地址（IPv4 或 IPv6）或 FQDN。

URL 重写和绕行域

如果邮件的威胁级别超过邮件修改阈值，则病毒爆发过滤器功能将重写邮件中的所有 URL，以便在用户单击其中任意URL时将他们重定向到思科网络安全代理的启动页面。（有关详细信息，请参阅重定向 URL, on page 4。）如果邮件的威胁级别超过隔离阈值，设备还会隔离该邮件。如果正在发生小规模、非病毒爆发，隔离邮件会让TOC有时间分析可能是爆发的邮件中链接的任何可疑网站，并确定网站是否是恶意的。CASE 使用 SIO 发布的更新爆发规则重新扫描邮件，以确定它是否属于爆发。在保留期限到期后，邮件网关将从隔离区放行邮件。

AsyncOS 重写邮件中的所有 URL，指向绕行域的 URL 除外。

要重写 URL，可使用以下选项：

- **对未签名的邮件启用 (Enable only for unsigned messages)**。此选项允许 AsyncOS 重写未签名邮件中符合或超出邮件修改阈值的 URL，但不含签名的邮件。思科建议对于 URL 重写使用此设置。

Note 如果在网络中由邮件网关之外的服务器或设备负责验证 DomainKeys/DKIM 签名，则邮件网关可以重写 DomainKeys/DKIM 签名的邮件中的URL，并废弃邮件的签名。

邮件网关会考虑签名的邮件是否使用 S/MIME 进行加密或其是否包含 S/MIME 签名。

- **对所有邮件启用 (Enable for all messages)**。此选项允许 AsyncOS 重写所有邮件中符合或超出邮件修改阈值的 URL，包括签名的邮件。如果 AsyncOS 修改签名的消息，签名将失效。
- **禁用 (Disable)**。此选项将禁用病毒爆发过滤器的 URL 重写。

可以修改策略以排除修改特定域的 URL。要绕过域，请在“绕过域扫描”(Bypass Domain Scanning) 字段中输入 IPv4 地址、IPv6 地址、CIDR 范围、主机名，部分主机名或域。使用逗号分隔多个条目。

绕过域扫描功能与URL过滤使用的全局允许列表类似，但与之无关。有关该允许列表的详细信息，请参阅创建允许的 URL 过滤列表。

威胁免责声明

邮件网关可以在可疑邮件标题上方附加免责声明消息，以警告用户注意其内容。根据邮件类型，此免责声明可以是 HTML 或纯文本形式。

从“威胁免责声明”(Threat Disclaimer) 列表中选择要使用的免责声明文本；或单击“邮件策略”(Mail Policies) > “文本资源”(Text Resources) 链接，使用免责声明模板创建新免责声明。免责声明模板包括用于爆发威胁信息的变量。单击“预览免责声明”(Preview Disclaimer)，可以查看威胁免责声明预览。对于自定义免责声明消息，可以使用变量显示邮件中的威胁级别、威胁类型和威胁说明。有关创建免责声明消息的信息，请参阅文本资源管理概述。

病毒爆发过滤器功能和病毒爆发隔离区

病毒爆发过滤器功能隔离的邮件将发送到爆发隔离区。此隔离区的功能与任何其他隔离区类似（有关使用隔离区的详细信息，请参阅策略、病毒和病毒爆发隔离区），但此隔离区具有“摘要”(summary) 视图，该视图对于根据在隔离区中放置邮件所用的规则，从隔离区删除或放行所有邮件非常有用（对于爆发规则，显示爆发 ID；对于自适应规则，显示通用术语）。有关摘要视图的详细信息，请参阅病毒爆发隔离区和“按规则摘要管理”视图, on page 20。

相关主题

- 监控病毒爆发隔离区, on page 19
- 病毒爆发隔离区和“按规则摘要管理”视图, on page 20

监控病毒爆发隔离区

虽然执行任何监控时正确配置的隔离区需求很少，但最好留意爆发隔离区，特别是在病毒爆发期间或之后，这段时间合法邮件可能被延迟。

如果某个合法邮件被隔离，则根据爆发隔离区的设置，会出现下列情况之一：

- 如果隔离区的“默认操作”(Default Action) 设置为“放行”(Release)，当保留期限到期或隔离区溢出时将放行该邮件。您可以配置爆发隔离区，以便在邮件因溢出而被放行之前，对其执行以下操作：拆离附件、修改主题和添加X-Header。有关这些操作的详细信息，请参阅自动处理的隔离邮件的默认操作。
- 如果隔离区的“默认操作”(Default Action) 设置为“删除”(Delete)，当保留期限到期或隔离区溢出时将删除该邮件。
- 如果隔离区已满，再添加更多邮件，将会发生溢出。在这种情况下，将首先放行距到期日期最近的邮件（不一定是时间最长的邮件），直到为新邮件留出充足的空间。您可以配置爆发隔离区，以便在邮件因溢出而被放行之前，对其执行以下操作：拆离附件、修改主题、添加X-Header。

由于只要发布新规则就会重新扫描隔离的邮件，所以爆发隔离区中的邮件很可能在到期时间之前就被放行。

但是，如果“默认操作”(Default Action) 设置为“删除”(Delete)，监控爆发隔离区仍然非常重要。思科建议大多数用户不要将默认操作设置为“删除”(Delete)。有关从爆发隔离区放行邮件或更改爆发隔离区默认操作的详细信息，请参阅自动处理的隔离邮件的默认操作。

相反，如果您的爆发隔离区中包含邮件，假如在等待新规则更新时希望延长它们在隔离区中的保留期限，可以延迟这些邮件的到期时间。切记，延长邮件的保留时间可能导致隔离区变大。

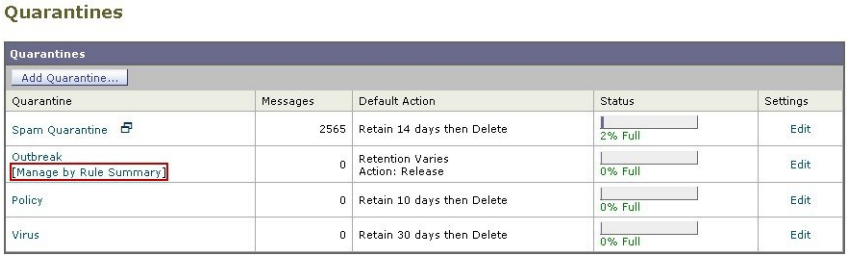
Note 如果已全局禁用防病毒扫描（并非通过邮件策略），而爆发隔离区中包含邮件，则在该邮件离开隔离区时不会对其执行防病毒扫描，即使在该邮件离开隔离区之前重新启用防病毒扫描亦不例外。

Note 可以使用病毒爆发过滤器功能，而不在邮件网关上启用防病毒扫描。但是，如果设备上未启用反垃圾邮件扫描，病毒爆发过滤器则不可扫描非病毒威胁。

病毒爆发隔离区和“按规则摘要管理”视图

在GUI中，单击“监控”(Monitor)菜单中列出的隔离区名称，可查看爆发隔离区的内容。爆发隔离区也有一个额外视图，即爆发隔离区的“按规则管理摘要”(Manage by Rule Summary)链接。

Figure 3: 爆发隔离区的“按规则管理摘要”***(Manage by Rule Summary)*** 视图



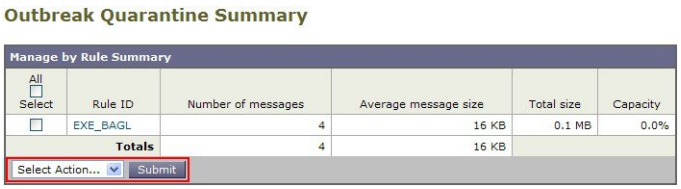
相关主题

- 使用摘要视图可根据规则 ID 对爆发隔离区中的邮件执行邮件操作。, on page 21

使用摘要视图可根据规则 ID 对爆发隔离区中的邮件执行邮件操作。

单击“按规则管理摘要”(Manage by Rule Summary) 链接，可按规则 ID 分组查看爆发隔离区的内容列表：

Figure 4: 爆发隔离区的“按规则管理摘要”***(Manage by Rule Summary)*** 视图



在此视图中，可以选择放行、删除或延迟与特定爆发或自适应规则相关的所有邮件的退出，而不必逐个选择邮件。此外，也可以在列表中搜索或对其排序。

通过 quarantineconfig -> outbreakmanage CLI 命令也可以使用此功能。有关详细信息，请参阅《适用于思科安全邮件网关的 AsyncOS CLI 参考指南》。

监控病毒爆发过滤器

该邮件网关包括多种监控病毒爆发过滤器功能的性能和活动的工具。

相关主题

- 病毒爆发过滤器报告, on page 21
- 爆发过滤器概述和规则列表, on page 21
- 病毒爆发隔离区, on page 22
- 警报、SNMP 陷阱和病毒爆发过滤器, on page 22

病毒爆发过滤器报告

通过病毒爆发过滤器报告，可查看邮件网关中病毒爆发过滤器的当前状态和配置，以及有关最近爆发和由于病毒爆发过滤器而被隔离的邮件的信息。在“监控”(Monitor)>“病毒爆发过滤器”(Outbreak Filters) 页面上可查看此信息。有关详细信息，请参阅“邮件安全监控”一章。

爆发过滤器概述和规则列表

概述和规则列表提供有关病毒爆发过滤器功能当前状态的有用信息。通过“安全服务”(Security Services) >“病毒爆发过滤器”(Outbreak Filters) 页面可查看此信息。

病毒爆发隔离区

使用爆发隔离区可监控被病毒爆发过滤器威胁级别阈值标记的邮件数量。另外，还可查看按规则隔离的邮件列表。有关信息，请参阅病毒爆发隔离区和“按规则摘要管理”视图, on page 20和 策略、病毒和病毒爆发隔离区

警报、SNMP 陷阱和病毒爆发过滤器

病毒爆发过滤器功能支持两种不同类型的通知：普通 AsyncOS 警报和 SNMP 陷阱。

当规则更新失败时，将生成 SNMP 陷阱。有关 AsyncOS 中 SNMP 陷阱的详细信息，请参阅“通过 CLI 管理和监控”一章。

AsyncOS 有两种类型的病毒爆发过滤器功能警报：大小和规则

每当爆发隔离区的大小超过最大大小的 5%、50%、75% 和 95% 时，将生成 AsyncOS 警报。针对 95% 阈值生成的警报的严重性为“严重”(CRITICAL)，而其余警报阈值的严重性为“警告”(WARNING)。随着隔离区范围加大而超过阈值时，将生成警报。随着隔离区范围减小而越过阈值时，不会生成警报。有关警报的详细信息，请参阅警报。

当发布规则、更改阈值时，或更新规则或 CASE 引擎出现问题时，AsyncOS 也会生成警报。

病毒爆发过滤器功能故障排除

本节提供适用于病毒爆发过滤器功能的一些基本故障排除提示。

相关主题

- 向思科报告分类错误的邮件 , on page 22
- 多个附件和绕过的文件类型, on page 22
- 邮件和内容过滤器及邮件管道, on page 22

向思科报告分类错误的邮件

使用爆发隔离区“管理隔离区”(Manage Quarantine) 页面上的复选框，通知思科分类错误。

多个附件和绕过的文件类型

只有邮件的唯一附件是绕过的文件类型时，才会排除绕过的文件类型；如果有多个附件，只有其他附件当前没有设定规则时，才会排除绕过的文件类型。否则，将对邮件进行扫描。

邮件和内容过滤器及邮件管道

首先对邮件应用邮件和内容过滤器，然后才执行病毒爆发过滤器扫描。这些过滤器可能导致邮件跳过或绕过病毒爆发过滤器扫描。