使用邮件安全监控

本章包含以下部分：

邮件安全监控概述

邮件安全监控功能可收集邮件传送过程中各个步骤的数据。数据库根据 IP 地址识别和记录各个邮件发件人，同时与 IP 信誉服务进行交互以获取实时身份信息。您可以即时报告任何发件人的本地邮件流历史记录，并显示一个配置文件，其中包括互联网上的发件人全局记录。通过邮件安全监控器功能，安全团队可以“封闭循环”监控向用户发送邮件的人员、用户发送和接收的邮件数量以及安全策略的有效性。

本章介绍如何执行以下操作：

- 访问邮件安全监控功能，以监控入站和出站邮件流量。
- 通过查询发件人的 IP 信誉得分，制定邮件流量策略决策（更新允许列表、阻止列表和灰名单）。您可以查询网络所有者、域，甚至各个 IP 地址。
- 报告邮件流量、系统状态以及从您的网络收到和发出的邮件。

对于传入邮件的任何给定邮件发件人，邮件安全监控数据库都会捕获关键参数，例如：

- 邮件数量
- 连接历史记录
- 已接受与拒绝的连接数
- 接受率和截流限制
- 发件人信誉过滤器匹配数量
- 针对可疑垃圾邮件和确定为垃圾邮件的反垃圾邮件数
- 防病毒扫描检测到的具有病毒特征的邮件数

有关反垃圾邮件扫描的详细信息，请参阅管理垃圾邮件和灰色邮件；有关防病毒扫描的详细信息，请参阅防病毒。

邮件安全监控器功能还会捕获有关特定邮件触发哪个内容过滤器的信息，包括向其发送或从其发送邮件的内部用户（邮件收件人）。

邮件安全监控功能只能通过 GUI 使用，通过它可查看您的邮件流量和邮件网关状态（包括隔离区、工作队列和爆发）。邮件网关可识别不属于正常流量配置文件的发件人。界面中将突出显示确实表现异常的发件人，您可以通过将该发件人分配到某个发件人组或优化该发件人的访问配置文件来采取纠正措施；或者，可以利用 AsyncOS 的安全服务继续作出反应和响应。出站邮件具有类似的监控功能，允许您查看邮件队列的顶部域及接收主机的状态（请参阅“传送状态详细信息”(Delivery Status Details) 页面, on page 17）。

Note 有关重启邮件网关时工作队列中存在的邮件信息，邮件安全监控功能不予报告。

相关主题

- 邮件安全监控和集中管理, on page 2

邮件安全监控和集中管理

要查看聚合的报告数据，请部署思科安全邮件和 Web 管理器。

无法聚合集群设备的邮件安全监控报告。所有报告都限于计算机级别。这意味着无法在组或集群级别运行它们，只能在单个计算机上运行。

对于“存档的报告”(Archived Reports) 页面，也是如此 - 每台计算机实际上都有自己的存档。因此，“生成报告”功能在选定的计算机中运行。

“计划的报告”(Scheduled Reports) 页面并非限于计算机级别；因此，可以在多台计算机之间共享设置。在计算机级别运行的单个计划报告就像是交互式报告，所以，如果您在集群级别配置计划的报告，集群中的每台计算机都将发送自己的报告。

“预览此报告”(Preview This Report) 按钮始终针对登录主机运行。

“邮件安全监控器”(Email Security Monitor) 页面

邮件安全监控功能包括“监控”(Monitor) 菜单中可用的所有页面，但“隔离区”(Quarantine) 页面除外。

在 GUI 中，使用这些页面可以监控连接到设备侦听程序的域。您可以监控、排序、分析和分类邮件网关的“邮件流量”，并区分大量合法邮件的发件人与潜在“垃圾邮件发送者”（大量未经请求的商业邮件的发件人）或病毒发送者。此外，这些页面还可以帮助排除系统入站连接故障（包括域的 IP 名义得分和最近发件人组匹配等重要信息）。

这些页面可帮助您对与邮件网关相关以及与存在于网关范围之外的服务相关的邮件分类，例如 IP 信誉服务、反垃圾邮件扫描服务、防病毒扫描安全服务、内容过滤器和病毒爆发过滤器。

对于任何邮件安全监控页面，通过点击页面右上角的“可打印 PDF”(Printable PDF) 链接，可以生成打印机友好格式的 .PDF 版本。有关生成非英语版本的 PDF 的信息，请参阅有关报告的注意事项, on page 76。

通过**导出 (Export)** 链接可以将图表及其他数据导出为 CSV（逗号分隔值）格式。

导出的 CSV 数据将以 GMT 显示所有邮件跟踪和报告数据（不考虑邮件网关中的设置）。GMT 时间转换是为了允许独立于邮件网关使用数据，或从分布于多个时区的设备中引用数据的情况。

Note 如果导出本地化 CSV 数据，则标题在某些浏览器中可能不会正常呈现。出现该情况是因为某些浏览器可能没有为本地化文本使用正确的字符集。要解决该问题，可以将文件保存到磁盘，然后使用“文件”(File) > “打开”(Open) 打开该文件。当打开该文件时，选择字符集以显示本地化文本。

有关自动导出报告数据的详细信息，请参阅检索 CSV 数据, on page 33。

邮件安全监控页面列表

- “系统容量”(System Capacity) 页面, on page 27
- “系统状态”(System Status) 页面, on page 30
- “大量邮件”(High Volume Mail) 页面, on page 32
- “邮件过滤器”(Message Filters) 页面, on page 32
- “地理分布”(Geo Distribution) 页面 , on page 16
- “安全打印”(Safe Print) 页面 , on page 32

搜索和邮件安全监控

许多邮件安全监控页面都包含搜索表单。您可以搜索不同类型的项目：

- IP 地址（IPv4 和 IPv6）
- domain
- 网络所有者
- 内部用户
- 目标域
- 内部发件人域
- 内部发件人 IP 地址
- 传出域传送状态

对于域、网络所有者和内部用户搜索，需要选择是完全匹配搜索文本还是仅查找以所输入文字开头的项目（例如，以“ex”开头将匹配“example.com”）。

对于 IPv4 地址搜索，始终会将输入的文本解释为最多四个 IP 八位组（采用点分十进制格式）的开头。例如，输入“17”将会在 17.0.0.0 至 17.255.255.255 的范围内搜索，因此 17.0.0.1 匹配搜索结果，而 172.0.0.1 不匹配。对于完全匹配搜索，需要输入所有四个八位组。IP 地址搜索还支持 CIDR 格式 (17.16.0.0/12)。

对于 IPv6 地址搜索，AsyncOS 支持以下格式：

- 2001:db8:2004:4202::0-2001:db8:2004:4202::ff
- 2001:db8:2004:4202::
- 2001:db8:2004:4202::23
- 2001:db8:2004:4202::/64

所有搜索都必须在页面中当前选择的时间范围内。

查看报告中所含邮件的详细信息

只有报告和跟踪都在本地执行（并非在思科安全邮件和 Web 管理器中集中执行）时，此功能才有效。

Procedure

步骤 1 点击报告页面上表中的任何蓝色编号。

（并非所有的表格都有这些链接。）

“邮件跟踪”(Message Tracking) 中将显示该数字下包含的邮件。

步骤 2 向下滚动以查看列表。

What to do next

相关主题

- 处理邮件跟踪搜索结果

“我的控制面板”(My Dashboard) 页面

您可以创建自定义邮件安全报告页和，方法是组合现有报告页中的图表（图形）和表格。

要想	相应操作
将模块添加到自定义报告页面。	1. 转到**监控 (Monitor) > 我的控制面板 (My Dashboard)**，通过点击模块右上角的 [**X**] 删除不需要的任何示例模块。 2. 执行以下操作之一： • 点击模块块中的 **[+]** 按钮（位于“监控”(Monitor) 菜单的报告页），将其添加到您的自定义报告中。 • 转到**监控 (Monitor) > 我的控制面板 (My Dashboard)**，点击其中一个部分的 **[+]** 按钮，然后选择要添加的报告模块。您可能需要检查每个部分的 **+ 报告模块**，以找到查找的报告。 3. 添加的模块使用默认设置。如果添加已自定义的模块（例如，通过添加、删除或重新排序列，），可在添加这些模块后对其自定义。原始模块的时间范围无法保留。 4. 如果添加包含单独图例的图表（例如，“概述”(Overview) 页面中的图形），请单独添加图例。如果需要，请将其拖放至所描述数据旁边的位置。 说明： • 某些报告页面的部分模块，只能通过上述某种方法使用。如果使用一种方法无法添加模块，请尝试另一种方法。 • 每个模块只能添加一次；如果您已向报告中添加特定模块，则用于添加该模块的选项将不可用。

要想	相应操作
查看自定义报告页面	1. 选择**监控 (Monitor) > 我的控制面板 (My Dashboard)** 2. 对于“时间范围”(Time Range) 部分中的报告：针对所有报告页面所选的时间范围会应用到“我的控制面板”页面中的所有模块。选择要查看的时间范围。 新添加的模块显示在相关部分顶部。
在自定义报告页面上重新排列模块	将模块拖放到所需的位置。
从您的自定义报告中删除模块	点击模块右上角的 [X]。

“概述”(Overview) 页面

“概述”(Overview) 页面会概括介绍邮件网关的邮件活动，包括隔离区和爆发过滤器状态的概述（在页面的“系统概述”[System Overview] 部分）。“概述”(Overview) 页面还包含传入和传出邮件的图形以及详细邮件计数。可以使用此页面来监控进出网关的所有邮件的流量。

“概述”(Overview) 页面重点介绍了邮件网关与 IP 信誉服务相集成以处理传入邮件（例如，由信誉过滤拦截的邮件）的方式。在**概述 (Overview)** 页面中，可以执行以下操作：

- 查看出入网关的所有邮件的邮件趋势图。
- 查看随着时间的推移显示以下信息的图表：尝试发送的邮件数、被 IP 信誉过滤 (SBRS) 拦截的邮件数、包含无效收件人的邮件数、标记为垃圾邮件的邮件数、标记为具有病毒特征的邮件数和正常邮件数。
- 查看系统状态和本地隔离区的摘要。
- 根据威胁操作中心 (TOC) 提供的信息，查看当前的病毒和非病毒爆发信息。

“概述”(Overview) 页面分为两部分：“系统概述”(System Overview) 与“传入和传出邮件”(Incoming and Outgoing Mail) 图表及概要。

相关主题

- 系统概况, on page 6
- 传入和传出摘要与图形, on page 8
- 邮件分类, on page 8
- 邮件分类方法, on page 9

系统概况

“概述”(Overview) 页面的“系统概述”(System Overview) 部分相当于系统控制面板，提供有关邮件网关的详细信息，包括系统和工作队列状态、隔离区状态及爆发活动。

相关主题

- 状态, on page 7
- 系统隔离区, on page 7
- 防病毒爆发(VOF), on page 7

状态

此部分提供邮件网关和入站邮件处理的当前状态概述。

系统状态：以下状态之一：

- 在线
- 资源节约
- 传送挂起
- 接收挂起
- 工作队列暂停
- 离线

有关详细信息，请参阅 使用 CLI 进行管理和监控。

传入邮件 (Incoming Messages)：每小时传入邮件的平均速。

工作队列 (Work Queue)：在工作队列中等待处理的邮件数。

点击“系统状态详细信息”(System Status Details) 链接可导航到“系统状态”(System Status) 页面。

系统隔离区

本部分显示有关按邮件网关上的磁盘使用情况排名前三的隔离区的信息，包括隔离区的名称、隔离区的满溢程度（磁盘空间）和隔离区中当前的邮件数。

点击“本地隔离区”(Local Quarantines) 链接可导航到“本地隔离区”(Local Quarantines) 页面。

防病毒爆发(VOF)

此部分显示威胁操作中心 (TOC) 报告的爆发状态。此外还显示病毒爆发隔离区的状态，包括其满溢程度（磁盘空间）和隔离区中的邮件数。仅当已在邮件网关上启用爆发过滤器功能时，才会显示病毒爆发隔离区。

Note 为使威胁级别指示器正常工作，您需要将防火墙上的端口 80 对“**downloads.ironport.com**”开放。或者，如果指定了本地更新服务器，威胁级别指示器将尝试使用该地址。如果针对通过“服务更新”(Service Updates) 页面下载配置了代理，威胁级别指示器也可正常更新。有关详细信息，请参阅服务更新。

点击“爆发详细信息”(Outbreak Details) 链接，可查看外部“威胁操作中心”(Threat Operations Center) 网站。请注意，为使此链接正常工作，您的邮件网关必须能够访问互联网。请注意，“单独的窗口”(Separate Window) 图标表示点击后将以单独窗口打开链接。您可能需要配置浏览器的弹出窗口阻止程序设置才能允许显示这些窗口。

传入和传出摘要与图形

传入和传出摘要部分提供对系统上所有邮件活动的实时活动的访问，并且包含传入和传出邮件图形与邮件摘要。通过“时间范围”(Time Range) 菜单，可以选择报告的时间范围。您选择的时间范围在所有邮件安全监控器页面的各处使用。下面介绍了邮件的各种类型或类别（请参阅邮件分类, on page 8）。

邮件趋势图显示了邮件流量的视觉表达，而摘要表提供了相同信息的数字细分表达。摘要表包括每种类型邮件的比例和实际数量，包括尝试发送的邮件总数、威胁邮件数和正常邮件数。

传出邮件图表和摘要显示了出站邮件的类似信息。

相关主题

- 邮件安全监控中的邮件计数注意事项, on page 8

邮件安全监控中的邮件计数注意事项

邮件安全监控用于计算传入邮件数量的方法取决于每封邮件的收件人数。例如，从 example.com 发送给三个收件人的传入邮件将计算为三封来自该发件人的邮件。

由发件人信誉过滤拦截的邮件实际不会进入工作队列，因此，邮件网关无权访问传入邮件的收件人列表。在这种情况下，使用倍数来估算收件人数量。此倍数由思科基于对大量现有客户数据样本的研究得出。

邮件分类

“概述”(Overview) 和“传入邮件”(Incoming Mail) 页面报告的邮件分类如下：

- **由 IP 信誉过滤拦截**：由 HAT 策略拦截的所有连接数乘以一个固定倍数（请参阅邮件安全监控中的邮件计数注意事项, on page 8），再加上由收件人限制拦截的所有收件人数。
- **由域信誉过滤拦截**：根据发件人域的信誉来判定阻止的邮件总数。
- **无效收件人**：会话 LDAP 拒绝以及所有 RAT 拒绝所拒绝的所有收件人。
- **检测到的垃圾邮件**：反垃圾邮件扫描引擎检测到的具有垃圾邮件或可疑垃圾邮件特征，以及既有垃圾邮件特征又有病毒特征的总邮件数。
- **检测到的病毒邮件**：被检测为具有病毒特征，但不是垃圾邮件的邮件总数和百分比。

Note 如果您已配置防病毒设置以传送不可扫描或已加密的邮件，这些邮件将被计为正常邮件，而不是病毒。否则，邮件将被计入具有病毒特征的邮件。

- **由高级恶意软件防护检测**：文件信誉过滤发现邮件附件为恶意文件。该值不包括判定更新或由文件分析发现为恶意的文件。
- **包含恶意 URL 的邮件 (Messages with Malicious URLs)**：通过 URL 过滤发现邮件中的一个或多个 URL 是恶意的。
- **由内容过滤器拦截**：由内容过滤器拦截的邮件总数。
- **由 DMARC 拦截 (Stopped by DMARC)**：在 DMARC 验证后被拦截的邮件总数。

Note 邮件网关根据“失败-拒绝”、“失败-隔离”和“失败-无操作”结果显示“Stopped by DMARC” 消息的总数。

- **S/MIME 验证/解密失败 (S/MIME Verification/Decryption Failed)**：S/MIME 验证、解密或两者均失败的邮件总数。
- **S/MIME 验证/解密成功 (S/MIME Verification/Decryption Successful)**：成功通过 S/MIME 验证、解密或解密和验证的邮件总数。
- **正常邮件**：已被接受且被视为无病毒和垃圾邮件的邮件-考虑到每个收件人的扫描操作（例如，正在按照单独的邮件策略处理的拆分邮件）时接受的对正常邮件最准确的表达。但是，由于标记为垃圾邮件或病毒特征并且仍然提交了的邮件不进行计数，因此所传送邮件的实际数量可能不同于正常邮件的计数。
- 灰色邮件
  - **营销邮件**：专业营销组织（例如 Amazon.com）发送的广告邮件总数。
  - **社交网络邮件**：社交网络、交友网站、论坛等发送的通知邮件总数。示例包括 LinkedIn 和 CNET 论坛。
  - **批量邮件**：无法识别的营销组织（例如技术媒体公司 TechTarget）发送的广告邮件总数。

  点击与上述任何灰色邮件类别对应的数字，可通过“邮件跟踪”(Message Tracking) 查看属于该类别的邮件列表。

Note 如果邮件与邮件过滤器匹配并且未被过滤器丢弃或退回，则被视为正常。邮件过滤器丢弃或退回的邮件不计入总数。

邮件分类方法

当邮件通过邮件管道时，可应用于多个类别。例如，可将邮件标记为具有垃圾邮件、病毒或恶意软件特征；也可以匹配内容过滤器。各种判定遵循以下优先规则：爆发过滤器隔离（在此情况下，在从隔离区发行邮件并再次通过工作队列进行处理之前，不会对邮件进行计数），接下来是具有垃圾邮件特征、具有病毒特征、具有恶意软件特征，以及匹配内容过滤器。

例如，如果某个邮件被标记为具有垃圾邮件特征，并且您的反垃圾邮件设置被设置为丢弃具有垃圾邮件特征的邮件，则该邮件将被丢弃，垃圾邮件计数器会增加。此外，如果反垃圾邮件设置被设置为允许具有垃圾邮件特征的邮件继续在邮件管道中通行，并且后续内容过滤器将会丢弃、退回或隔离该邮件，则垃圾邮件计数器仍会增加。仅当该邮件不具有垃圾邮件、病毒或恶意软件特征时，内容过滤器才会增加。

“传入邮件”(Incoming Mails) 页面

传入邮件 (Incoming Mail) 页面提供一种报告机制，即报告连接到您的邮件网关设备的所有远程主机的邮件安全监控功能收集的实时信息。这可以让您收集有关向您发送邮件的 IP 地址、域和组织（网

络所有者）的详细信息。也可以基于 IP 地址、域以及向您发送邮件的组织执行发件人配置文件搜索。

“传入邮件”(Incoming Mail) 页面包含三个视图：“域”(Domain)、“IP 地址”(IP Address) 和“网络所有者”(Network Owner)，并提供在选定视图环境中连接到系统的远程主机的快照。

其中显示向邮件网关中配置的所有公共侦听程序发送邮件的顶部域（或 IP 地址或网络所有者，具体取决于视图）表格（传入邮件详细信息）。可以监控流入网关的所有邮件的流量。您可以点击任何域/IP/网络所有者，深入访问“发件人配置文件”(Sender Profile)（这是特定于您所点击的域/IP/网络所有者的“传入邮件”(Incoming Mails) [Incoming Mail] 页面）页面中有关此发件人的详细信息。

不是所有可用列默认都会显示。点击表格下方的“列”(Columns) 链接，可显示不同组的信息。例如，您可以显示默认情况下隐藏的“由高级恶意软件防护检测”列。

“传入邮件”(Incoming Mail) 页面扩展以包含一组页面（“传入邮件”[Incoming Mail]、“发件人配置文件”[Sender Profiles] 和“发件人组报告”[Sender Group Report]）。从**传入邮件 (Incoming Mail)** 页面可以执行如下操作：

- 对已向您发送邮件的 IP 地址、域或组织（网络所有者）执行搜索。
- 查看“发件人组”(Sender Groups) 报告，以了解通过特定发件人组执行的连接数及邮件流量策略操作。有关详细信息，请参阅发件人组报告, on page 14。
- 查看有关向您发送邮件的发件人的详细统计数据，包括按安全服务（发件人信誉过滤、反垃圾邮件、防病毒、灰色邮件等）细分的尝试发送的邮件数量。
- 按已向您发送大量垃圾邮件或病毒邮件（如反垃圾邮件或防病毒安全服务所确定）的发件人排序。
- 使用 IP 信誉服务可深入查看和检查特定 IP 地址、域和组织之间的关系，以获取有关发件人的详细信息。
- 深入探讨特定发件人，以便从 IP 信誉服务中获取有关发件人的详细信息，包括发件人的 IP 信誉得分，以及该域最近匹配的发件人组。将发件人添加到发件人组。
- 深入探讨曾发送大量垃圾邮件或病毒邮件（由反垃圾邮件或防病毒安全服务决定）的特定发件人的信息。
- 收集到关于域的信息后，即可点击域、IP 地址或网络所有者配置文件页面中的“添加到发件人组”(Add to Sender Group)，将该 IP 地址、域或组织添加到现有发件人组。请参阅配置网关以接收邮件。

相关主题

- 传入邮件, on page 10
- 传入邮件详细信息列表, on page 11
- 填充了数据的报告页面：发件人配置文件页面, on page 13
- 发件人组报告, on page 14

传入邮件

“传入邮件”(Incoming Mail) 页面提供访问系统中配置的所有公共侦听程序的实时活动的权限，其中包括两部分：汇总接收的顶部发件人域的邮件趋势图（按威胁邮件总数、正常邮件总数和灰色邮件总数）和“传入邮件详细信息”(Incoming Mail Details) 列表。

有关“传入邮件详细信息”(Incoming Mail Details) 列表中包含的数据的说明，请参阅传入邮件详细信息列表, on page 11。

相关主题

邮件趋势图中的时间范围说明, on page 11

邮件趋势图中的时间范围说明

邮件安全监控功能不断记录进入网关的邮件流量的相关数据。这些数据每60秒更新一次，但所示的显示时间有所延迟，落后当前系统时间 120 秒。可以指定所示结果中包括的时间范围。由于数据实时监控，因此信息会在数据库中定期更新和汇总。

从下表的时间范围选项中进行选择。

Table 1: 邮件安全监控功能可用的时间范围

在 GUI 中选择的以下时间范围	...定义为：
小时	最近 60 分钟 + 最多 5 分钟
天	过去 24 小时 + 过去 60 分钟
周	前 7 天 + 当日经过的小时数
30 天	最近 30 天 + 当日的耗用小时数
90 天	最近 90 天 + 当日的耗用小时数
昨天	00:00 到 23:59（午夜到下午 11:59）
上一日历月	当月第一天的 00:00 到当月最后一天的 23:59
自定义范围	您指定的开始日期和小时及结束日期和小时包含的范围

如果已启用集中报告，则显示的时间范围选项将会不同。有关详细信息，请参阅在思科安全邮件和 Web 管理器（M 系列）上集中管理服务中有关“集中报告模式”的信息

传入邮件详细信息列表

根据所选的视图，“传入邮件”(Incoming Mail) 页面底部的“已接收的外部域”(External Domains Received) 列表中将列出已连接到邮件网关公共侦听程序的顶部发件人。点击列标题可对数据进行排序。有关各种类别的说明，请参阅邮件分类, on page 8。

系统通过执行双重 *DNS* 查找，获取和验证远程主机 IP 地址（即域）的有效性。有关双向 DNS 查找和发件人验证的详细信息，请参阅配置网关以接收邮件。

“发件人详细信息”(Sender Detail) 列表有两个视图：“摘要”(Summary) 和“全部”(All)。

默认“发件人详细信息”(Sender Detail) 视图显示每个发件人尝试发送的邮件总数，并包括按类别的细分（与“概述”(Overview) 页面上“传入邮件摘要”(Incoming Mail Summary) 图表中的类别相同）。

“由 IP 信誉过滤拦截”(Stopped by IP Reputation Filtering) 的值根据多个因素进行计算：

- 此发件人的“受限制”邮件数量。
- 被拒绝或被 TCP 拒绝的连接数量（可能是部分计数）。
- 每个连接的邮件数量的保守倍数。

当邮件网关的负载繁重时，不会为逐个发件人维护已拒绝的连接准确计数。而是针对每个时间间隔内最重要的发件人来记录被拒绝的连接计数。在这种情况下，显示的值可以解释为“地板”，换句话说，大于等于该值才会拦截许多邮件。

Note “概述”(Overview) 页面上的“由 IP 信誉过滤拦截”(Stopped by IP Reputation Filtering) 总计始终基于所有已拒绝的连接的完整计数。由于负载，只有每个发件人的连接计数曾受限制。

可以显示的附其他列如下：

拒绝的连接：HAT 策略阻止的所有连接。当邮件网关的负载繁重时，不会为逐个发件人维护已拒绝的连接准确计数。而是针对每个时间间隔内最重要的发件人来记录被拒绝的连接计数。

接受的连接：接受的所有连接

由域信誉过滤拦截 (Stopped by Domain Reputation Filtering)：由发件人域的信誉判定阻止的所有邮件。

由收件人限制拦截：这是由信誉过滤拦截的组件。表示由于超出下列任何 HAT 限制而拦截的收件人邮件的数量：每小时的最大收件人数、每封邮件的最大收件人数或每个连接的最大邮件数。此值加上与被拒绝或被 TCP 拒绝的收件人邮件估算值就得到了“由信誉过滤拦截”(Stopped by Reputation Filtering) 的值。

由高级恶意软件防护检测：文件信誉过滤发现附件为恶意的邮件数。该值不包括判定更新或由文件分析发现为恶意的文件。

威胁总数 (Total Threat)：威胁邮件（由发件人信誉拦截、作为无效收件人拦截、垃圾邮件以及病毒）的总数。

点击表格底部的“列”(Column) 链接，可显示或隐藏列。

点击列标题链接可排序列表。列标题旁边的小三角形表示数据当前排序所依照的列。

相关主题

- “没有域信息”, on page 12
- 查询详细信息, on page 13

“没有域信息”

已连接至邮件网关并且无法通过双重DNS查找进行验证的域将自动分组到名为“没有域信息”的特殊域。可以控制通过发件人验证来管理此类未验证主机的方式。请参阅配置网关以接收邮件。

可以通过“显示的项目”(Items Displayed) 菜单选择要在列表中显示的发件人数。

查询详细信息

对于“邮件安全监控”(Email Security Monitor) 表中列出的发件人，点击发件人（或“没有域名信息”[No Domain Information] 链接），深入了解有关特定发件人的详细信息。结果显示在“发件人配置文件”(Sender Profile) 页面，其中包括来自 IP 信誉服务的实时信息。从“发件人配置文件”(Sender Profile) 页面中，可以深入了解有关特定 IP 地址或网络所有者的详细信息（请参阅填充了数据的报告页面：发件人配置文件页面, on page 13）。

还可以通过点击“传入邮件”(Incoming Mails) 页面底部的“发件人组”(Sender Groups) 报告链接，查看另一种报告 - 发件人组报告。有关发件人组报告的的详细信息，请参阅发件人组报告, on page 14。

填充了数据的报告页面：发件人配置文件页面

如果点击了“传入邮件”(Incoming Mails) 页面“传入邮件详细信息”(Incoming Mail Details) 表格中的某个发件人，将列出生成的“发件人配置文件”*(Sender Profile)* 页面及特定 IP 地址、域或组织（网络所有者）的数据。“发件人配置文件”(Sender Profile) 页面显示发件人的详细信息。您可以通过点击“传入邮件”(Incoming Mails) 页面或其他“发件人配置文件”(Sender Profile) 页面上的指定项目，来访问任何网络所有者、域或 IP 地址的“发件人配置文件”(Sender Profile) 页面。网络所有者是包含域的实体；域是包含 IP 地址的实体。有关此关系的详细信息及其与 IP 信誉服务的关系，请参阅配置网关以接收邮件。

为 IP 地址、网络所有者和域显示的“发件人配置文件”(Sender Profile) 页面稍有不同。不管是哪个页面，页面都包含来自此发件人的传入邮件的图表和摘要表。图形下方是一个表，其中列出与发件人关联的域或 IP 地址（各个 IP 地址的“发件人配置文件”(Sender Profile) 页面不包含详细列表），以及包含发件人的当前 SenderBase、发件人组和网络信息的信息部分。

- 网络所有者配置文件页面包含网络所有者以及与该网络所有者关联的域和 IP 地址的信息。
- 域配置文件页面包含与该域关联的域和 IP 地址。
- IP 地址配置文件页面只包含有关该 IP 地址的信息。

每个发件人配置文件页面底部的“当前信息”(Current Information) 表格中都包含以下数据：

- 来自 IP 信誉服务的**全局**信息，包括：
  - IP 地址、域名和/或网络所有者
  - 网络所有者类别（仅限网络所有者）
  - CIDR 范围（仅限 IP 地址）
  - IP 地址、域和/或网络所有者的日流量和月流量
  - 自上次从此发件人收到第一封邮件以来的天数
  - 上一个发件人组以及是否进行了 DNS 验证（仅 IP 地址发件人配置文件页面）

日流量用于衡量某个域在最近 24 小时内发送了多少邮件。SenderBase 流量类似于用来衡量地震的里氏震级，使用以 10 为底数的对数标尺计算邮件数量。该标尺的最大理论值设置为 10，等同于 100% 的实际邮件数量（大约 100 亿封邮件/天）。使用该对数标尺时，流量每增加 1 个单位，实际数量就会增加 10 倍。

月流量的计算方法与日流量相同，只是百分比基于最近 30 天发送的邮件数量来计算。

- 平均流量（仅限 IP 地址）

- 生命周期流量/30 天流量（仅限 IP 地址配置文件页面）
- 担保发件人状态（仅 IP 地址配置文件页面）
- IP 信誉得分（仅限 IP 地址配置文件页面）
- 自第一封邮件以来的天数（仅网络所有者和域配置文件页面）
- 与此网络所有者关联的域的数量（仅限网络所有者和域配置文件页面）
- 此网络所有者中的 IP 地址的数量（仅限网络所有者和域配置文件页面）
- 用于发送邮件的 IP 地址的数量（仅限网络所有者页面）

点击“SenderBase 的更多信息”(More from SenderBase) 链接可看到一个页面，其中包含由 IP 信誉服务提供的所有信息。

- **邮件流量统计数据**信息，包含在您指定的时间范围内收集的有关该发件人的邮件安全监控信息。
- 有关此网络所有者控制的域和 IP 地址的**详细信息**，将显示在网络所有者配置文件页面。有关域中的 IP 地址的详细信息，将显示在域页面。

从域配置文件页面中，可深入了解特定 IP 地址，也可深入查看组织配置文件页面。此外，点击“IP 地址”(IP Addresses) 表底部的“列”(Columns) 链接，还可显示验证的 DNS 状态、IP 信誉得分以及该表格中每个发件人地址的上一个发件人组。还可以隐藏该表中的任何列。

在某个网络所有者配置文件页面中，点击“域”(Domains) 表底部的“列”(Columns) 链接，可以显示已拒绝的连接、已接受的连接，由收件人限制拦截和由高级恶意软件防护检测等信息。您还可以隐藏该表中的任何列。

如果您是系统管理员，在其中每个页面，都可以选择将网络所有者、域或 IP 地址添加到发件人组，方法是点击实体的复选框（如果需要），然后点击“添加到发件人组”(Add to Sender Group)。

此外，也可以点击发件人“当前信息”(Current Information) 表中“发件人组信息”(Sender Group Information) 下方的**添加到发件人组 (Add to Sender Group)** 链接，再点击“添加到发件人组”(Add to Sender Group)，将该发件人添加到发件人组。有关将发件人添加到发件人组的详细信息，请参阅配置网关以接收邮件。当然，您不必进行任何更改 - 可以让安全服务来处理传入邮件。

相关主题

- 发件人配置文件搜索, on page 14

发件人配置文件搜索

在“快速搜索”(Quick Search) 框中键入 IP 地址、域或组织名称，可搜索特定发件人。

系统将显示“发件人配置文件”(Sender Profile) 页面，其中包含发件人的信息。请参阅填充了数据的报告页面：发件人配置文件页面, on page 13。

发件人组报告

“发件人组”(Sender Groups) 报告按发件人组和邮件流量策略操作提供连接摘要，从而便于查看 SMTP 连接和邮件流量策略趋势。“按发件人组的邮件流量 (Mail Flow by Sender Group)”列表显示每个发件人组的连接的百分比和数量。“按邮件流量策略操作的连接”(Connections by Mail Flow

Policy Action) 图表显示每个邮件流量策略操作的连接百分比。此页面概述了主机访问表 (HAT) 策略的有效性。有关 HAT 的详细信息，请参阅配置网关以接收邮件。

“发件人域信誉”(Sender Domain Reputation) 页面

您可以使用“发件人域信誉”(Sender Domain Reputation) 报告页面：

- 以图形格式根据从 SDR 服务接收的判定查看传入邮件。
- 以表格格式根据从 SDR 服务接收的威胁类别和判定查看传入邮件摘要。
- 以图形格式根据从 SDR 服务接收的威胁类别查看传入邮件。

注释 只有那些 SDR 判为 "不受信任" 或 "有问题" 的信息才被归入 SDR 威胁类别，如 "垃圾邮件"、"恶意 "等。

- 根据从 SDR 服务中表格的形式接收的威胁类别的传入邮件摘要。

在“SDR 处理的传入邮件摘要”(Summary of Incoming Messages handled by SDR) 部分，您可以点击与特定判定对应的邮件数量，在“邮件跟踪”(Message Tracking) 中查看相关邮件。

传出目标

“传出邮件目标”(Outgoing Destinations) 页面提供有关您的公司发送邮件所至的域的信息。该页面包含两个部分。页面上半部分包含一些图表，这些图表描述按传出威胁邮件排名靠前的目标，以及按页面上半部分的传出正常邮件排名靠前的目标。页面下半部分显示一个图表，包含按收件人总数（默认设置）排序的所有列。

您可以选择报告的时间范围，例如小时、周或自定义范围。与所有报告相同，通过**导出 (Export)** 链接可以将图表数据或详细信息列表导出为 CSV 格式。

“外发目标”(Outgoing Destinations) 页面可用于回答以下类型的问题：

- 邮件网关将邮件发送到哪些域？
- 向每个域发送多少邮件？
- 该邮件中有多少是正常的、具有垃圾邮件特征、具有病毒特征、具有恶意软件特征或由内容过滤器拦截？
- 传送了多少邮件以及被目标服务器硬性退回了多少邮件？

传出邮件发件人

“传出邮件发件人”(Outgoing Senders) 页面提供有关正从网络内的 IP 地址和域发送的邮件数量和类型的信息。当查看此页面时，您可以按域或 IP 地址查看结果。如果您要查看每个域正在发送的邮件的数量，则可能要按域查看结果；如果要查看哪些 IP 地址发送的病毒邮件最多或者正在触发内容过滤器，则可能要按 IP 地址查看结果。

该页面包含两部分。页面左侧是一个描绘按威胁邮件总数排名靠前的发件人的图形。威胁邮件总数包括具有垃圾邮件特征、病毒特征的邮件，恶意软件邮件或触发了内容过滤器的邮件数量。页面右侧包含一个图表，其中显示按页面上半部分的正常邮件排名靠前的发件人。页面下半部分显示一个图表，其中显示按邮件总数（默认设置）排序的所有列。

Note 此页面未显示有关邮件发送的信息。使用“传送状态”(Delivery Status) 页面可跟踪传送信息，例如从特定域退回了多少邮件。

您可以选择报告的时间范围，例如小时、周或自定义范围。与所有报告相同，通过**导出 (Export)** 链接可以将图表数据或详细信息列表导出为 CSV 格式。

“传出发件人”(Outgoing Senders) 页面可用于回答以下类型的问题：

- 哪些 IP 地址正在发送最具病毒特征、垃圾邮件特征的邮件或恶意软件邮件？
- 哪些 IP 地址最频繁触发内容过滤器？
- 哪些域发送最多邮件？

“地理分布”(Geo Distribution) 页面

可以使用“地理分布”报告页面查看：

- 以图形格式显示的基于来源国家/地区的传入邮件连接排行榜。
- 以表格格式显示的基于源国家/地区的传入邮件连接总数。

您可以点击特定地理位置的传入邮件连接数来查看邮件跟踪中的相关消息。

“邮件总数”列仅显示在 SMTP 连接级别接受的邮件。

注释 报告生成期间：

- 如果将一个或多个传入邮件连接检测为私有 IP 地址，则这些传入邮件连接将在报告中归类为“私有 IP 地址”。
- 如果将一个或多个传入邮件连接检测为非有效 IP 信誉得分，则这些传入邮件连接将在报告中归类为“无国家/地区信息”。

“传送状态”(Delivery Status) 页面

如果您怀疑向特定收件人域进行传送有问题，或者如果要收集有关虚拟网关地址的信息，则“监控”(Monitor) >“传送状态”(Delivery Status) 页面会提供有关与特定收件人域相关的邮件操作的监控信息。

传送状态 (Delivery Status) 页面显示的信息与 CLI 中的 tophosts 命令所示的信息相同。（有关详细信息，请参阅使用 CLI 进行管理和监控中的“确定邮件队列的构成”）

此页面显示系统在过去三个小时内传送的邮件的前 20、50 或 100 个收件人域列表。可以通过点击每项统计数据列标题中的链接，按最新主机状态、有效收件人（默认）、连接超时、发送的收件人、软退回事件以及硬退回收件人进行排序。

- 要搜索特定域，请在“域名：”(Domain Name:) 字段键入域的名称，并点击**搜索 (Search)**。
- 要深入查看所显示的域，请点击域名链接。

结果将显示在“传送状态详细信息”(Delivery Status Details) 页面中。

Note 收件人域有任何活动，都会导致该域被“激活”，从而出现在概述页面。例如，如果邮件由于传送问题留在出站队列，则该收件人域将继续列在传出邮件概述中。

相关主题

- 重试传送, on page 17
- “传送状态详细信息”(Delivery Status Details) 页面, on page 17

重试传送

点击**重试所有传送 (Retry All Delivery)**，可立即重试计划稍后传送的邮件。“重试所有传送”(Retry All Delivery) 允许您重新安排立即传送队列中的邮件。标记为“已关闭”的所有域以及任何已计划或软退回的邮件会加入队列等候立即传送。

要重试传送到特定目标域，请点击域名链接。在“传送状态详细信息”(Delivery Status Details) 页面，点击**重试传送 (Retry Delivery)**。

您也可以在 CLI 中使用 delivernow 命令来重新安排立即传送邮件。有关详细信息，请参阅安排邮件立即传送。

“传送状态详细信息”(Delivery Status Details) 页面

使用**传送状态详细信息 (Delivery Status Details)** 页面可以查找有关特定收件人域的统计数据。此页面显示的信息与 CLI 内的 **hoststatus** 命令所示的信息相同：邮件状态、计数器和计量器。（有关详细信息，请参阅使用 CLI 进行管理和监控）要搜索特定域，请在“域名:”字段中键入域的名称，然后点击**搜索 (Search)**。如果使用的是 **altsrchost** 功能，则会显示虚拟网关地址信息。

“内部用户”(Internal Users) 页面

“内部用户”(Internal Users) 页面按邮件地址提供有关内部用户发送和接收的邮件的信息（一个用户可能列出了多个邮件地址 - 报告中不合并邮件地址）。

该页面包含两部分：

- 描述按正常传入和传出邮件排名靠前用户和收到灰色邮件的靠前用户的图表。
- 用户邮件流量详细信息

您可以选择报告时间范围（小时、天、周或月）。与所有报告相同，通过**导出 (Export)** 链接可以将图表数据或详细信息列表导出为 CSV 格式。您还可以通过点击表下方的“列”(Columns) 链接显示隐藏表列或隐藏默认列。

“用户邮件流量详细信息”(User Mail Flow Details) 列表将每个邮件邮件地址收到和发送的邮件细分为“正常”(Clean)、“检测到垃圾邮件”(Spam Detected)（仅限传入）、“检测到病毒”(Virus Detected) 和“内容过滤器匹配”(Content Filter Matches)。您可以通过点击列标题对列表排序。

使用内部用户报告，可以回答以下类型的问题：

- 谁发送的外部邮件最多？
- 谁接收的正常邮件最多？
- 谁接收的灰色邮件最多？
- 谁接收的垃圾邮件最多？
- 谁触发了哪些内容过滤器？
- 谁的邮件被内容过滤器拦截？

入站内部用户是您根据“收件人：”(Rcpt To:) 地址为其收到邮件的用户。出站内部用户基于“发件人: (Mail From:)”地址，在跟踪内部网络中的发件人所发送邮件的类型时非常有用。

请注意，某些出站邮件（如退回）包含空发件人。它们计入出站和“未知”之下。

点击某个内部用户，可查看该用户的“内部用户详细信息”(Internal User detail) 页面。

点击表下方的“列”链接可显示默认隐藏的列，例如“由高级恶意软件防护检测到的传入邮件”列或“由高级恶意软件防护检测到的传出邮件”列。

相关主题

- “内部用户详细信息”(Internal User Details), on page 18
- 搜索特定的内部用户, on page 18

“内部用户详细信息”(Internal User Details)

“内部用户详细信息”(Internal User detail) 页面显示有关指定用户的详细信息，包括显示每个类别（检测到垃圾邮件、检测到病毒、由高级恶意软件防护检测到、由内容过滤器拦截、检测到灰色邮件和正常）邮件数量的传入和传出邮件明细。或者，对于传入邮件，您可以点击表下方的“列”(Columns) 链接来显示“由高级恶意软件防护检测到的传入邮件”(Incoming Detected by Advanced Malware Protection) 列。此值反映包含的附件被文件信誉过滤确定为恶意的邮件数。它不包括判定更新或由文件分析发现为恶意的文件。此外，还显示传入和传出邮件内容过滤器和 DLP 策略匹配。

点击内容过滤器名称，可在相应的内容过滤器信息页面中查看该过滤器的详细信息（请参阅“内容过滤器”(Content Filters) 页面, on page 20）。使用此方法可查看发送或接收了与特定内容过滤器匹配的邮件的用户列表。

搜索特定的内部用户

您可以通过“内部用户”(Internal Users) 页面和“内部用户详细信息”(Internal Users detail) 页面底部的搜索表单，搜索特定的内部用户（邮件地址）。选择是完全匹配搜索文本还是查找以输入的文本开头的项目（例如，以“ex”开头将匹配“example.com”）。

“DLP 事件”(DLP Incidents) 页面

“DLP 事件”(DLP Incidents) 页面显示传出邮件中发生的防数据丢失 (DLP) 策略违规事件的相关信息。邮件网关使用在“传出邮件策略”(Outgoing Mail Policies) 表中启用的 DLP 邮件策略来检测用户发送的敏感数据。违反 DLP 策略的每个外发邮件均报告为一个事件。

使用 DLP 事件报告，可以回答以下类型的问题：

- 用户发送什么类型的敏感数据？
- 这些 DLP 事件具有什么样的严重性？
- 传送的这些邮件有多少数量？
- 丢弃的这些邮件有多少数量？
- 是谁在发送这些邮件？

“DLP 事件”(DLP Incidents) 页面包括两个主要部分：

- DLP 事件趋势图，按严重性（低、中、高、关键）和策略匹配排名靠前的 DLP 事件；
- DLP 事件详细信息列表。

您可以选择报告的时间范围，例如小时、周或自定义范围。与所有报告相同，通过**导出 (Export)** 链接可以将图表数据或详细信息列表导出为 CSV 格式；或通过点击**可打印 (PDF) (Printable [PDF])** 链接导出为 PDF 格式。有关生成英语以外的其他语言的 PDF 的信息，请参阅有关报告的注意事项, on page 76。

点击 DLP 策略的名称，可查看有关策略检测到的 DLP 事件的详细信息。使用此方法可以获取发送的邮件包含策略检测到的敏感数据的用户列表。

相关主题

- DLP 事件详细信息, on page 19
- “DLP 策略详细信息”(DLP Policy Detail) 页面, on page 19

DLP 事件详细信息

当前为邮件网关的传出邮件策略启用的DLP策略会在“DLP 事件”(DLP Incident) 页面底部的“DLP 事件详细信息”(DLP Incident Details) 表格中列出。点击某个 DLP 策略的名称，可查看更多详细信息。

“DLP 事件详细信息”表显示了每个策略的DLP事件总数，并按严重性级别细分。严重性级别还包括已退回的邮件数，以及在清除、已发送的加密或删除的邮件中传递的邮件数。点击列标题可对数据进行排序。

“DLP 策略详细信息”(DLP Policy Detail) 页面

如果点击了“DLP 事件详细信息”(DLP Incident Details) 表中某个 DLP 策略的名称，则随之打开的“DLP 策略详细信息”(DLP Policy Detail) 页面将会显示该策略的 DLP 事件数据。该页面根据严重性显示有关 DLP 事件的图表。

该页面还包括一个位于页面底部的“按发件人的事件”(Incidents by Sender) 列表，其中列出了发送的邮件违反 DLP 策略的各个内部用户。该列表还按用户显示此策略的 DLP 事件总数（按严重级别

细分）以及其中是否有任何邮件以明码形式传送、以加密形式传送或已经丢弃。您可以使用“按发件人的事件 (Incidents by Sender)”列表了解可能将组织的敏感数据发送给网络之外人员的用户。

点击发件人名称，将打开“内部用户”(Internal Users) 页面。有关详细信息，请参阅“内部用户”(Internal Users) 页面, on page 17。

“内容过滤器”(Content Filters) 页面

“内容过滤器”(Content Filters) 页面通过两种形式显示排名靠前的传入和传出邮件内容过滤器匹配项（匹配邮件数量最多的内容过滤器）：条形图和列表。使用“内容过滤器”(Content Filters) 页面，可以按内容过滤器或按用户查看企业策略，并回答以下类型的问题：

- 传入或传出邮件触发哪些内容过滤器的次数最多？
- 发送或接收的邮件触发了特定内容过滤器的排名靠前的用户有哪些？

点击列表中内容过滤器的名称，可在“内容过滤器详细信息”(Content Filter detail) 页面查看有关该过滤器的详细信息。

相关主题

- 内容过滤器详细信息, on page 20

内容过滤器详细信息

“内容过滤器详细信息”(Content Filter Detail) 页面显示随时间推移的过滤器匹配，以及按内部用户的匹配。

在“按内部用户划分的匹配项”(Matches by Internal User) 部分中，您可以点击用户的名称来查看该内部用户的（邮件地址）“内部用户”(Internal User) 详细信息页面（请参阅“内部用户详细信息”(Internal User Details), on page 18）。

“DMARC 验证”(DMARC Verification) 页面

“DMARC 验证”(DMARC Verification) 页面显示 DMARC 验证失败的排名靠前的域，以及 AsyncOS 针对 DMARC 验证失败的邮件执行的操作详细信息。可以使用此报告优化 DMARC 设置并回答以下类型的问题：

- 哪些域发送的不符合 DMARC 要求的邮件数最多？
- 对于每个域，AsyncOS 针对 DMARC 验证失败的邮件执行了什么操作？

“DMARC 验证”(DMARC Verification) 页面包含：

- 显示按 DMARC 验证失败排名靠前的域的条形图。
- 有关每个域以下信息的表格：
  - 被拒绝、隔离或接受而不采取任何操作的邮件数。点击数字，可查看选定类别下的邮件列表。
  - 通过 DMARC 验证的邮件数。
  - DMARC 验证尝试总数。

您可以选择报告的时间范围，例如小时、周或自定义范围。与所有报告相同，通过**导出 (Export)** 链接可以将图表数据或详细信息列表导出为 CSV 格式；或通过点击**可打印 (PDF) (Printable [PDF])** 链接导出为 PDF 格式。

“宏检测”(Macro Detection) 页面

可以使用“宏检测”(Macro Detection) 报告页面查看：

- 以图形和表格格式显示的按文件类型排名靠前的启用宏的传入附件。
- 以图形和表格格式显示的按文件类型排名靠前的启用宏的传出附件。

您可以点击启用宏的附件数量，以在邮件跟踪中查看相关邮件。

注释 报告生成期间：

- 如果在存档文件中检测到一个或多个宏，则存档文件的文件类型将按一递增。不计算存档文件中启用宏的附件数量。
- 如果在嵌入文件中检测到一个或多个宏，则父文件类型将递增一。不计算嵌入文件中启用宏的附件数量。

“外部威胁源”(External Threat Feeds) 页面

您可以使用“外部威胁源”(External Threat Feeds) 报告页面查看：

- 以图形格式查看用于检测邮件威胁的排名靠前的 ETF 来源
- 以表格格式查看用于检测邮件威胁的 ETF 来源的摘要。
- 以图形格式查看与检测到的邮件威胁相匹配的排名靠前的 IOC。
- 以图形格式查看用于过滤恶意传入邮件连接的排名靠前的 ETF 来源。
- 以表格格式查看用于过滤恶意传入邮件连接的 ETF 来源的摘要。

在“外部威胁源来源摘要”(Summary of External Threat Feed Sources) 部分：

- 您可以点击特定 ETF 来源的邮件数量，在邮件跟踪中查看相关邮件。
- 您可以点击特定威胁源来源，根据 IOC 查看 ETF 来源的分布情况。

在“感染指标 (IOC) 匹配摘要”部分：

- 您可以点击特定 ETF 来源的 IOC 数量，在邮件跟踪中查看相关邮件。
- 您可以点击特定 IOC，根据 ETF 来源查看 IOC 的分布情况。

“爆发过滤器”(Outbreak Filters) 页面

“病毒爆发过滤器”(Outbreak Filters) 页面显示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。您可以使用此页面可以监控对针对性的病毒、诈骗和网络钓鱼攻击的防御。

“按类型划分的威胁”(Threats By Type) 部分显示邮件网关接收的不同类型的威胁邮件。

“威胁摘要”(Threat Summary) 部分显示按恶意软件、网络钓鱼、诈骗和病毒统计的威胁邮件细分。点击数字可使用“邮件跟踪”(Message Tracking) 查看该数字中包括的所有邮件的列表。

“过去一年爆发摘要 (Past Year Outbreak Summary)”会列出过去一年的全局及局部爆发，以便将局部网络趋势与全局趋势进行比较。全局爆发列表是所有爆发情况（包括病毒和非病毒）的超集，而局部爆发仅限于影响邮件网关的病毒爆发。局部爆发数据不包括非病毒威胁。全局病毒爆发数据表示威胁操作中心检测到的所有病毒爆发，该数据超过病毒爆发隔离区的当前配置的阈值。本地病毒爆发数据表示在此设备上检测到的所有病毒爆发，该数据超过病毒爆发隔离区的当前配置的阈值。“本地防护总时间”(Total Local Protection Time) 始终基于威胁操作中心检测到各病毒爆发的时间与主要供应商发布防病毒签名的时间之间的时间差。请注意，并非每个全局爆发都会影响邮件网关。值“--”表示保护时间不存在，或防病毒供应商未提供特征码时间（某些供应商可能不报告特征码时间）。这并不表示保护时间为零，而是表示计算保护时间所需的信息不可用。

“隔离的邮件”(Quarantined Messages) 部分汇总爆发过滤器隔离情况，是测量爆发过滤器捕获的潜在威胁邮件数的有用计量器。隔离的邮件在放行时计数。通常，邮件在防病毒和反垃圾邮件规则可用之前会被隔离。放行时，它们会被防病毒和反垃圾邮件软件进行扫描并确定是阳性还是正常邮件。由于爆发跟踪的动态性质，当邮件处于隔离区中时，用于隔离邮件的规则（甚至关联的爆发）可能会更改。在放行时（而不是在进入隔离区中时）对邮件进行计数可避免混淆计数增加和减少的情况。

“威胁详细信息”(Threat Details) 列表显示有关特定病毒爆发的信息，包括威胁类别（病毒、诈骗或网络钓鱼）、威胁名称、该威胁的说明和识别的邮件数。对于病毒爆发，“过去一年病毒爆发 (Past Year Virus Outbreaks)”包括爆发名称和 ID、首次全局出现病毒爆发的时间和日期、爆发过滤器提供的保护时间以及隔离的邮件数。通过左侧的菜单，可以选择全局或局部爆发以及显示的邮件数。您可以通过点击列标题对列表排序。点击数值可使用“邮件跟踪”(Message Tracking) 查看该数值中包含的所有邮件的列表。

首次全局出现时间由威胁操作中心根据 SenderBase（全球最大的邮件和网络流量监控网络）中的数据确定。保护时间始终基于威胁操作中心检测到各个威胁的时间与主要供应商发布防病毒特征码的时间之间的差异。

值为“--”表示防护时间不存在，或者防病毒供应商未提供签名时间（某些供应商可能不会报告签名时间）。这并不表示防护时间为零。相反，这表示计算保护时间所需的信息不可用。

“传入邮件中的命中邮件”(Hit Messages from Incoming Messages) 部分显示病毒附件、其他威胁（非病毒）和正常传入邮件的百分比和数量。

“按威胁级别的命中邮件”(Hit Messages by Threat Level) 部分基于威胁级别（级别 1-5）显示传入威胁邮件的百分比和数量。

“爆发隔离区中的邮件”(Messages resided in Outbreak Quarantine) 部分基于持续时间显示位于爆发隔离区的威胁邮件数。

“重写的排名靠前的 URL”(Top URL's Rewritten) 部分列出基于出现次数重写的前 10 个 URL。使用“显示的项目”(Items Displayed) 下拉菜单可查看更多重写的 URL。点击数字可在“邮件跟踪”(Message Tracking) 页面查看包含所选重写 URL 的所有邮件列表。

使用“病毒爆发过滤器”(Outbreak Filters) 页面可回答如下问题：

- 有多少邮件被隔离？它们是哪些类型的威胁？
- 为病毒爆发提供病毒爆发过滤器功能的交付期是多久？
- 我的本地病毒爆发如何与全局病毒爆发进行比较？

“病毒类型”(Virus Types) 页面

“病毒类型”(Virus Types) 页面提供发送到网络以及从网络发出的病毒的概述。“病毒类型”(Virus Types) 页面显示已由邮件网关中运行的病毒扫描引擎检测到的病毒。要针对特定病毒采取具体操作，可能需要使用此报告。例如，如果发现收到已知嵌入 PDF 文件中的大量病毒，则您可能要创建过滤器操作来隔离具有 PDF 附件的邮件。

如果运行多个病毒扫描引擎，则“病毒类型”(Virus Types) 页面包括来自所有启用的病毒扫描引擎的结果。显示在该页面上的病毒的名称由病毒扫描引擎确定。如果多个扫描引擎检测到某个病毒，则同一病毒可能具有多个对应的条目。

“病毒类型”(Virus Types) 页面提供从网络发出或发送到网络的病毒的概述。“检测到的排名靠前的传入邮件病毒”(Top Incoming Virus Detected) 部分按降序显示已发送到您的网络的病毒图表视图。“检测到的排名靠前的传出邮件病毒”(Top Outcoming Virus Detected) 部分按降序显示从您的网络发出的病毒图表视图。

Note 要查看哪些主机向您的网络发送了感染病毒的邮件，请转到“传入邮件”(Incoming Mail) 页面，指定相同的报告期间，然后按病毒阳性进行排序。同样，要查看哪些 IP 地址在您的网络中发送了具有病毒特征的邮件，请查看“传出发件人”(Outgoing Senders) 页面并按具有病毒特征的邮件排序。

“病毒类型详细信息”(VirusTypes Details) 列表显示有关特定病毒的信息，包括受感染的传入和传出邮件及受感染的邮件总数。受感染的传入邮件详细信息列表显示病毒名称和感染此病毒的传入邮件数。同样，传出邮件部分显示病毒名称和感染此病毒的传出邮件数。您可以按“传入邮件数”(Incoming Messages)、“传出邮件数”(Outgoing Messages) 和“受感染邮件总数”(Total Infected Messages) 对病毒类型详细信息进行排序。

“URL 过滤”(URL Filtering) 页面

- 仅当启用 URL 过滤时，才会填充 URL 过滤报告模块。
- 提供传入和传出邮件的“URL 过滤”(URL Filtering) 报告。
- 只有由 URL 过滤引擎扫描的邮件（作为反垃圾邮件/爆发过滤器扫描的一部分或通过邮件/内容过滤器）才会包含在这些模块中。但是，并非所有结果都有必要专门可归属于URL过滤功能。
- “排名靠前的 URL 类别”(Top URL Categories) 模块包含已扫描的邮件中找到的所有类别，无论其是与内容过滤器还是邮件过滤器匹配都如此。

- 每封邮件都只能与一个 URL 信誉级别关联。对于包含多个 URL 的邮件，统计信息反映邮件中任何 URL 的最低信誉。
- 在“安全服务”(Security Services) >“URL 过滤”(URL Filtering) 中配置的全局允许列表内的 URL 未包含在报告中。

  报告中包含个别过滤器中使用的允许列表内的 URL。

- 恶意 URL 是爆发过滤器确定为信誉不佳的 URL。不确定 URL 是爆发过滤器确定需要点击时间保护的 URL。因此，不确定 URL 已被重写，从而重定向到思科网络安全代理。
- 基于 URL 类别的过滤器的结果会反映在内容和邮件过滤器报告中。
- 思科网络安全代理的点击时间 URL 评估结果不会反映在报告中。

“网络交互跟踪”(Web Interaction Tracking) 页面

- 只有启用了网络交互跟踪功能，才能填充网络交互跟踪报告。
- 网络交互跟踪报告模块不会实时更新，而是每 30 分钟刷新一次。此外，点击重写的 URL 后，网络交互跟踪报告最长可能需要两小时，才会报告此事件。
- 网络交互跟踪报告不会实时更新。点击云重定向的重写URL后，网络交互跟踪报告最长可能需要两小时，才会报告此事件。
- 网络交互跟踪报告适用于传入和传出邮件。
- 这些模块中仅包含最终用户（通过策略或爆发过滤器）点击的云重定向重写 URL。
- “网络交互跟踪”(Web Interaction Tracking) 页面包括以下报告：

最终用户点击的排名靠前的重写恶意 URL。点击 URL 可查看包含以下信息的详细报告：

- 点击了重写恶意 URL 的最终用户列表。
- 点击该 URL 的日期和时间。
- URL 是否已由策略或爆发过滤器重写。
- 点击重写的URL时采取的操作（允许、阻止或未知）。请注意，如果URL被爆发过滤器重写，且未提供最终判定，则状态显示为“未知”(unknown)。

点击重写的恶意 URL 的排名靠前的最终用户

网络交互跟踪详细信息 (Web Interaction Tracking Details)。包括以下信息：

- 所有云重定向重写 URL（恶意和非恶意）的列表。点击某个 URL 可查看详细报告。
- 点击云重定向重写的 URL 时采取的操作（允许、阻止或未知）。

要显示数据，请执行以下操作：

- 选择**传入邮件策略 (Incoming Mail Policies) > 爆发过滤器(Outbreak Filters)** 配置爆发过滤器，并启用邮件修改和 URL 重写。
- 为内容过滤器配置“**重定向到思科安全代理**”操作。

请注意，如果最终用户点击某个URL时，其判定（正常或恶意）未知，则状态将显示为未知。这可能是因为，需要进一步审查该 URL，或用户点击时网络服务器停止服务或无法访问。

- 最终用户点击重写的 URL 的次数。点击数字可查看包含可点击的 URL 的所有邮件列表。

- 在使用网络交互跟踪报告时，请记住以下限制：
  - 如果已将内容或邮件过滤器配置为重写恶意 URL 后传送邮件并通知其他用户（例如管理员），则原始收件人的网络交互跟踪数据将增加，即使获得通知的用户点击的是重写的 URL 也不例外。
  - 如果使用 Web 界面将包含重写 URL 的被隔离邮件副本发送给用户（例如管理员），则原始收件人的网络交互跟踪数据将增加，即使接收邮件副本的用户点击的是重写的URL 也不例外。
  - 在任何时候，如果您计划修改邮件网关时间，请确保系统时间与协调世界时 (UTC) 同步。

伪造邮件匹配项报告

请参阅监控伪造邮件检测结果。

文件信誉和文件分析报告

有关以下报告的信息，请参阅文件信誉和文件分析报告与跟踪：

- 高级恶意软件防护
- 文件分析
- AMP 判定更新

邮箱自动修复报告

您可以使用邮箱自动补救报告页面（**监控 (Monitor) > 邮箱自动补救 (Mailbox Auto Remediation)**）查看邮箱补救结果的详细信息。使用此报告可以查看详细信息，如：

- 对邮件执行的修复操作
- 与 SHA-256 散列关联的文件名
- 为其邮箱执行补救操作成功或不成功的收件人定义的配置文件名称列表
- 补救失败原因
- 没有映射到域的配置文件

点击 SHA-256 散列以在邮件跟踪中查看相关邮件。

有关详细信息，请参阅 补救邮箱中的邮件

“TLS 连接”(TLS Connections) 页面

“TLS 连接”(TLS Connections) 页面显示所收发邮件的 TLS 连接的整体使用情况。该报告还显示使用 TLS 连接发送邮件的每个域的详细信息。

“TLS 连接”(TLS Connections) 页面可用于确定以下信息：

- 总体而言，传入和传出连接的哪个部分使用 TLS？
- 我与哪些合作伙伴成功建立了 TLS 连接？

- 我与哪些合作伙伴建立的 TLS 连接没有成功？
- 在 DANE 支持下，我与哪些合作伙伴成功建立了 TLS 连接？
- 在 DANE 支持下，我未能与哪些合作伙伴成功建立 TLS 连接？
- 哪些合作伙伴的 TLS 证书存在问题？
- 某个合作伙伴使用 TLS 的邮件占总邮件的百分比是多少？
- DANE 支持的传出连接成功的百分比是多少？
- DANE 支持的传出连接不成功的百分比是多少？

“TLS 连接”(TLS Connections) 页面分为传入连接部分和传出连接部分。每个部分都包括图表、摘要和详细信息表格。

图表显示您指定的时间范围内，传入或传出 TLS 加密和未加密连接的视图。该图显示邮件总数、加密和未加密邮件的数量成功和失败的 TLS 加密邮件的数量以及成功和失败的 DANE 连接的数量。需要 TLS 的连接图表和仅首选 TLS 的连接图表有所不同。

此表显示发送或接收加密邮件的域的详细信息。对于每个域，可以查看成功和失败的需要及首选的 TLS 连接数量、尝试的 TLS 连接总数（无论成功还是失败）未加密连接总数以及 DANE 连接总数（根据是成功还是失败）。您还可以查看所有尝试 TLS 连接的百分比和成功发送的加密邮件总数，不考虑 TLS 是首选还是需要。您可以通过点击此表底部的“列”(Columns) 链接来显示或隐藏列。

“入站 SMTP 身份验证”(Inbound SMTP Authentication) 页面

“入站 SMTP 身份验证”(Inbound SMTP authentication) 页面显示了使用客户端证书和“SMTP AUTH”命令对邮件网关与用户的邮件客户端之间的 SMTP 会话进行身份验证。如果邮件网关接受证书或 SMTP AUTH 命令，则会建立到邮件客户端的 TLS 连接，供客户端用来发送邮件。因为邮件网关无法逐个用户跟踪这些尝试，因此报告会根据域名和域 IP 地址显示有关 SMTP 身份验证的详细信息。

使用此报告可确定以下信息：

- 总体而言，多少入站连接使用 SMTP 身份验证？
- 多少连接使用经过认证的客户端？
- 多少连接使用 SMTP AUTH？
- 当尝试使用 SMTP 身份验证时，哪些域无法连接？
- 当 SMTP 身份验证失败时，多少连接成功使用回退？

“入站 SMTP 身份验证”(Inbound SMTP Authentication) 页面包含一个表示已接收的连接的图形、一个表示已尝试 SMTP 身份验证连接的邮件收件人的图形，以及一个包含有关对连接进行身份验证的尝试的详细信息的表。

“已接收的连接”(Received Connections) 图形显示在指定时间范围内来自尝试使用 SMTP 身份验证对其连接进行身份验证的邮件客户端的传入连接。该图表显示邮件网关接收的连接总数、未尝试使用 SMTP 身份验证进行验证的次数，使用客户端证书验证连接的成功和失败次数，以及使用 SMTP AUTH 命令进行验证的成功和失败次数。

“已接收的收件人”(Received Recipients) 图形显示了收件人的数量，这些收件人的邮件客户端尝试对其与邮件网关的连接进行身份验证以使用 SMTP 身份验证来发送邮件。该图形还显示其连接已进行身份验证的收件人数和其连接未进行身份验证的收件人数。

“SMTP 身份验证详细信息”(SMTP Authentication details) 表显示了域的详细信息，这些域的用户尝试对其与邮件网关的连接进行身份验证以发送邮件。对于每个域，可以查看尝试使用客户端证书进行连接的成功或失败次数、尝试使用 SMTP AUTH 命令进行连接的成功或失败次数，以及在客户端证书连接尝试失败后回退到 SMTP AUTH 的次数。可以使用页面顶部的链接按域名或域 IP 地址显示此信息。

“速率限制”(Rate Limits) 页面

通过按信封发件人进行速率限制，您可以根据发件人地址从单个发件人限制每个时间间隔的邮件收件人数。“速率限制”(Rate Limits) 报告显示最严重超过此限制的发件人。

使用此报告可帮助确定以下内容：

- 可能用于批量发送垃圾邮件的有漏洞用户账户。
- 组织中的失控应用程序，这些应用程序使用邮件发送通知、风险通告、自动声明等内容。
- 组织中具有大量邮件活动的来源，用于内部计费或资源管理目的。
- 可能未被视为垃圾邮件的大量入站邮件流量的来源。

请注意，包含内部发件人（例如内部用户或传出邮件发件人）的统计信息的其他报告仅测量已发送的邮件数；它们不会向大量收件人表明少数邮件的发件人的身份。

“按事件划分的排名靠前的危害”图表显示最频繁尝试向超过配置限制的收件人发送邮件的信封发件人。每次尝试都是一个事件。此图表汇总所有侦听程序的事件计数。

“按已拒绝收件人划分的排名靠前的危害”图表显示向高于配置限制的最大数量的收件人发送邮件的信封发件人。此图表汇总所有侦听程序的收件人计数。

要按信封发件人配置速率限制或修改现有速率限制，请参阅使用邮件流策略定义传入邮件规则。

“系统容量”(System Capacity) 页面

“系统容量”(System Capacity) 页面提供有关系统负载的详细说明，包括工作队列中的邮件、花费在工作队列中的平均时间、传入和传出邮件（总量、大小和数量）、总体CPU使用率、按功能的CPU使用率和内存页面交换信息。

“系统容量”(System Capacity) 页面可用于确定以下信息：

- 识别邮件网关超过推荐容量，进而需要优化配置或添加邮件网关的情况。
- 确定系统行为方面指向即将发生的容量问题的历史趋势。
- 确定系统中协助故障排除耗用资源最多的部分。

务必要监控邮件网关，以确保您的容量适合邮件总量。随着时间的推移，邮件量会不可避免地增加，适当的监控可确保主动添加容量或进行配置更改。监控系统容量的最有效方式是跟踪总量、工作队列中的邮件以及资源节约模式下的事件。

- **邮件量**：了解环境中的“正常”邮件量和“一般”峰值非常重要。随着时间的推移跟踪此数据以测量邮件量增长。您可以使用“传入邮件”(Incoming Mail) 和“传出邮件”(Outgoing Mail) 页面长期跟踪数量。有关详细信息，请参阅系统容量 - 传入邮件, on page 29和系统容量 - 传出邮件, on page 29。
- **工作队列**：工作队列旨在充当“缓冲器” - 吸收和过滤垃圾邮件攻击并处理非垃圾邮件的不正常增加情况。但是，工作队列也是系统具有压力的最佳指示器，长时间并频繁地备份工作队列可能表明存在容量问题。使用“工作队列”(Workqueue) 页面可跟踪邮件在工作队列中花费的平均时间，以及工作队列中的活动。有关详细信息，请参阅系统容量 - 工作队列, on page 28。
- **资源节约模式**：当邮件网关变得过载时，会进入“资源节约模式”(RCM)，并发送“关键”系统警报。这旨在保护设备，使其可以处理任何邮件积压情况。邮件网关不应频繁进入RCM，并且应仅在邮件量出现超大或异常增长期间进入。频繁的 RCM 警报可能表明系统正在超负荷。请参阅系统容量 - 系统负载, on page 29。

相关主题

- 系统容量 - 工作队列, on page 28
- 系统容量 - 传入邮件, on page 29
- 系统容量 - 传出邮件, on page 29
- 系统容量 - 系统负载, on page 29
- 内存页面交换说明, on page 30
- 系统容量 - 全部, on page 30

系统容量 - 工作队列

“工作队列”(Workqueue) 页面显示邮件在工作队列中花费的平均时间，在垃圾邮件隔离区中或在策略、病毒或病毒爆发隔离区中花费的任何时间除外。您可以查看时间段，从一小时到一个月。此平均值可以帮助确定延迟邮件传送的短期事件和确定系统上工作负载的长期趋势。

Note 如果邮件从隔离区释放到工作队列中，“工作队列中的平均时间”指标将忽略此时间。这可防止重复计数，以及由于在隔离区中花费的时间延长而造成统计信息失真。

此报告也显示指定时间段内的工作队列中的邮件量，并且显示相同时间段内工作队列中的最大邮件数量。工作队列中的最大邮件数图表还显示工作队列阈值级别。

工作队列图形中的偶尔峰值是正常的，并在预期之内。如果工作队列中的邮件数长时间保持高于配置的阈值，可能表示存在容量问题。这种情况下，请考虑调整阈值级别或审核系统配置。

有关更改工作队列阈值级别的说明，请参阅为系统运行状况参数配置阈值。

Tip 当查看工作队列页面时，您可能要测量工作队列备份的频率，并标注超过 10000 封邮件的工作队列备份。

系统容量 - 传入邮件

传入邮件页面显示传入连接、传入邮件总数、平均邮件大小和传入邮件总大小。您可以将结果限制到指定的时间范围。了解环境中的正常邮件量和峰值趋势至关重要。可以使用传入邮件页面，帮助随着时间的推移跟踪邮件量增长并规划系统容量。您可能还希望比较传入邮件数据与发件人配置文件数据，以查看从特定域发送到网络的邮件量的趋势。

Note 传入连接数增加不一定会影响系统负载。

系统容量 - 传出邮件

传出邮件页面显示传出连接、传出邮件总数、平均邮件大小和传出邮件总大小。您可以将结果限制到指定的时间范围。了解环境中的正常邮件量和峰值趋势至关重要。可以使用传出邮件页面，帮助随着时间的推移跟踪邮件量增长并规划系统容量。您可能还要将“传出邮件”(Outgoing Mail) 数据与“外发目标”(Outgoing Destinations) 数据进行比较，以查看从特定域或 IP 地址发送的邮件量的趋势。

系统容量 - 系统负载

系统负载报告显示如下信息：

- CPU 总体使用情况
- 内存页面交换
- 资源节约活动

CPU 总体使用情况

邮件网关经过优化，可使用空闲 CPU 资源来提高邮件吞吐量。高 CPU 使用率并不一定表示存在系统容量问题。如果高 CPU 使用率与持续的大容量内存页面交换一同出现，则可能表示存在容量问题。

Note 此图还显示 CPU 的阈值级别。如果要更改阈值级别，请在 Web 界面中依次使用**系统管理 (System Administration)** > **系统运行状况 (System Health)** 页面或在 CLI 中使用 **`healthconfig`** 命令。请参阅为系统运行状况参数配置阈值。

该页面还包含一个图，用于显示不同功能（包括邮件处理、垃圾邮件和病毒引擎、报告和隔离）使用的 CPU 量。按功能划分的 CPU 图形可以很好地指示产品的哪些方面在系统上使用最多资源。如果需要优化邮件网关，则此图有助于确定哪些功能可能需要调整或禁用。

内存页面交换

内存页面交换图显示系统必须切换到磁盘的频率。此图还显示内存页面交换的阈值级别。如果要更改阈值级别，请在 Web 界面中依次使用**系统管理 (System Administration)** > **系统运行状况 (System Health)** 页面或在 CLI 中使用 **`healthconfig`** 命令。请参阅为系统运行状况参数配置阈值。

资源节约活动

资源节约活动图显示邮件网关进入资源节约模式 (RCM) 的次数。例如，如果图中显示 n 次，则意味着邮件网关进入了 RCM n 次，并已退出至少 n-1 次。

邮件网关不应频繁进入RCM，并且应仅在邮件量出现超大或异常增长期间进入。如果“资源节约活动”(Resource Conservation Activity) 图显示您的邮件网关频繁进入RCS，则可能表明系统变得过载。

内存页面交换说明

该系统旨在定期交换内存，因此进行一些内存交换是适当的，并不表示邮件网关存在问题。除非系统一致地大容量交换内存，否则内存交换正常，并且是预期行为（尤其在 C170 和 C190 设备上）。为提高性能，您可能需要将邮件网关添加到网络或调整配置以确保实现最大吞吐量。

系统容量 - 全部

“全部”(All) 页面将以前的所有系统容量报告整合在一个页面上，以便查看不同报告之间的关系。例如，您可能会发现在进行过量内存交换时，邮件队列很高。这可能是表示存在容量问题。您可能希望将此页面另存为 PDF 文件，以保留系统性能快照供以后参考（或与支持人员共享）。有关生成英语以外的其他语言的 PDF 的信息，请参阅有关报告的注意事项, on page 76。

“系统状态”(System Status) 页面

系统状态页面详细展示了系统的所有实时邮件和 DNS 活动。显示的信息与使用 CLI 中的 status detail 和 **dnsstatus** 命令得到的信息一样。有关详细信息，请参阅“监控详细邮件状态”了解状态详细命令，并请参阅“查看 DNS 状态”了解使用 CLI 进行管理和监控中的 **dnsstatus** 命令。

“系统状态”(System Status) 页面包括四个部分：“系统状态”(System Status)、“计量器”(Gauges)、“速率”(Rates) 和“计数器”(Counters)。

相关主题

- 系统状态, on page 30
- 规格, on page 31
- 比率, on page 31
- 计数器, on page 31

系统状态

系统状态部分显示邮件系统状态和版本信息。

相关主题

- 邮件系统状态, on page 30
- 版本信息, on page 31

邮件系统状态

“邮件系统状态”(Mail System Status) 部分包括：

- 系统状态（有关系统状态的详细信息，请参阅状态, on page 7）
- 上次状态报告时间。
- 邮件网关的正常运行时间。
- 系统中最早的邮件，包括尚未排队等待传送的邮件。

版本信息

“版本信息”(Version Information) 部分包括：

- 邮件网关型号名称。
- 安装的 AsyncOS 操作系统的版本和构建日期。
- AsyncOS 操作系统的安装日期。
- 您连接的系统的序列号。

如果要联系思科客户支持，此信息非常有用。（请参阅使用技术支持。）

规格

“计量器”(Gauges) 部分显示队列和资源利用率。

- 邮件处理队列
- 队列中正在处理的收件人
- 队列空间
- CPU Utilization

邮件网关设备是指 AsyncOS 进程所占用的 CPU 百分比。CASE 指多个项目，包括反垃圾邮件扫描引擎和病毒爆发过滤器进程。

- 常规资源利用率
- 日志磁盘利用率

比率

“速率”(Rates) 部分显示收件人的速率处理。

- 邮件处理速率
- 完成速率

计数器

建议避免在云邮件安全设备上重置计数器。

可以重置系统统计数据的累积邮件监控计数器，并查看上次重置计数器的时间。重置操作会影响系统计数器以及每个域的计数器。重置不会影响与重试计划相关的传送队列中的邮件计数器。

Note 只有管理员组或操作员组的用户账户有权重置计数器。在访客组创建的用户账户无法重置计数器。有关详细信息，请参阅处理用户帐户。

点击“重置计数器”(Reset Counters) 可重置计数器。此按钮提供与 CLI 中的 **resetcounters** 命令相同的功能。有关详细信息，请参阅重置邮件监控计数器。

- 邮件处理事件数量
- 完成事件数量
- 域密钥事件数量
- DNS 状态

“大量邮件”(High Volume Mail) 页面

Note “大量邮件”(High Volume Mail) 页面仅显示使用“信头重复”规则的邮件过滤器的数据。

“大量邮件”(High Volume) 页面包含以下条形图形式的报告：

- **排名靠前的主题**。使用此图表可以了解 AsyncOS 接收的邮件的热门主题。
- **排名靠前的信封发件人**。使用此图表可以了解 AsyncOS 接收的邮件排名靠前的信封发件人。
- **按匹配数排名靠前的邮件过滤器**。使用此图表可以了解排名靠前的邮件过滤器（使用“信头重复”规则）匹配项。

“大量邮件”(High Volume Mail) 页面还提供排名靠前的邮件过滤器和各个邮件过滤器的匹配项数表格。点击数值可使用“邮件跟踪”(Message Tracking) 查看该数值中包含的所有邮件的列表。

您可以选择报告的时间范围，例如小时、周或自定义范围。与所有报告相同，通过**导出 (Export)** 链接可以将图表数据或详细信息列表导出为 CSV 格式；或通过点击**可打印 (PDF) (Printable [PDF])** 链接导出为 PDF 格式。

“邮件过滤器”(Message Filters) 页面

“邮件过滤器”(Message Filters) 页面通过两种形式显示排名靠前的邮件过滤器匹配项（匹配邮件数量最多的邮件过滤器）：条形图和表格形式。

使用条形图，可查找传入和传出邮件触发最多的邮件过滤器。表格形式显示排名靠前的邮件过滤器和各个邮件过滤器的匹配项数。点击数值可使用“邮件跟踪”(Message Tracking) 查看该数值中包含的所有邮件的列表。

您可以选择报告的时间范围，例如小时、周或自定义范围。与所有报告相同，通过**导出 (Export)** 链接可以将图表数据或详细信息列表导出为 CSV 格式；或通过点击**可打印 (PDF) (Printable [PDF])** 链接导出为 PDF 格式。

“安全打印”(Safe Print) 页面

您可以使用“安全打印”(Safe Print) 报告页面查看：

- 以图形格式显示的基于文件类型的安全打印附件的数量。
- 基于表格格式的文件类型的安全打印附件摘要。

在“安全打印文件类型的摘要”(Summary of Safe Print File Types) 部分中，点击要在邮件跟踪中查看邮件详细信息的安全打印附件总数。

检索 CSV 数据

可以 CSV 格式检索邮件安全监控中用来生成图表的数据。CSV 数据可通过两种方式访问：

- **通过邮件传送的 CSV 报告**。可以生成通过邮件传送或存档的 CSV 报告。当您要为“报告”(Reports) 页面上显示的每个表分隔报告时，或者当您要将 CSV 数据发送给无权访问内部网络的用户时，这种传送方式非常有用。

  逗号分隔值 (CSV) 报告类型是 ASCII 文本文件，其中包含计划报告的表格数据。每个 CSV 文件最多可以包含 100 行。如果报告包含多种类型的表格，则会为每种表格创建一个单独的 CSV 文件。单个报告的多个 CSV 文件将压缩成单个 .zip 文件以作为存档文件存储选项，或全部附加到不同的邮件进行传送。

- **通过 HTTP 检索的 CSV 文件**。可以通过 HTTP 检索邮件安全监控功能中用来生成图表的数据。如果您计划通过其他工具对数据执行进一步分析，此传送方法十分有用。您可以自动检索这些数据（例如通过可下载原始数据的自动脚本），处理数据，然后在其他某些系统中显示结果。

相关主题

- 通过自动化流程检索 CSV 数据, on page 33

通过自动化流程检索 CSV 数据

获取所需的 HTTP 查询的最简单方法是将其中一个邮件安全监控器页面配置为显示所需的数据类型。然后，可以复制**导出 (Export)** 链接。这是下载 URL。在自动执行此类数据检索时，务必要注意的是，下载 URL 中的哪些参数应该固定，哪些应该变化（见以下内容）。

下载 URL 的编码方式允许将其复制到可执行相同查询（使用适当的 HTTP 身份验证）和获得类似数据集的外部脚本。该脚本可以使用基本 HTTP 身份验证或 cookie 身份验证。当通过自动化过程检索 CSV 数据时，请记住以下几点：

- 时间范围选择（过去的小时、天、星期等）与再次使用该 URL 的时间有关。如果复制 URL 来检索“过去一天”的 CSV 数据集，则下次使用该 URL 时，会获得从再次发送该 URL 起覆盖“过去一天”的新数据集。日期范围选择予以保留并显示在 CSV 查询字符串中（例如，date_range=current_day）。
- 过滤和组合数据集的首选项。过滤器将保留并显示在查询字符串中。请注意报告中的过滤器很少见 - 一个示例是爆发报告中的“全局/本地”爆发选择器。
- CVS 下载将返回所选时间范围内表中的所有数据行。
- CSV 下载按时间戳和密钥顺序返回表中的数据行。可以在单独的步骤中执行进一步的排序，例如通过电子表格应用程序。
- 第一行包含与报告中所示的显示名称匹配的列标题。请注意，还会显示时间戳（请参阅时间戳, on page 34）和密钥（请参阅按键, on page 34）。

相关主题

- 示例 URL, on page 34
- 添加基本 HTTP 身份验证凭证, on page 34
- 文件格式, on page 34
- 时间戳, on page 34
- 按键, on page 34
- 流传输, on page 34

示例 URL

http://example.com/monitor/content_filters?format=csv&sort_col_ss_0_0_0=
MAIL_CONTENT_FILTER_INCOMING.RECIPIENTS_MATCHED&section=ss_0_0_0
&date_range=current_day&sort_order_ss_0_0_0=desc&report_def_id=mga_content_filters

添加基本 HTTP 身份验证凭证

要为 URL 指定基本 HTTP 身份验证凭据：

`http://example.com/monitor/`

变成：

`http://username:password@example.com/monitor/`

文件格式

下载的文件为 CSV 格式，文件扩展名为 .csv。文件标题包含默认文件名，即以报告名称开头，然后是报告的部分。

时间戳

导出流数据将显示每个原始时间“间隔”的开始和结束时间戳。提供两个开始时间戳，两个结束时间戳 - 一个为数字格式，另一个是人类可读的字符串格式。时间戳为 GMT 时间，如果您的邮件网关分布于多个时区，则更方便进行日志汇聚。

请注意，有时候数据会与其他来源的数据合并在一起，导出文件不含时间戳，不过这种情况很少见。例如，导出的爆发详细信息会与威胁操作中心 (TOC) 数据合并在一起，由于没有间隔，所以会使时间戳变得不相关。

按键

此外，导出还包括报告表格密钥，即使在报告中的密钥不可见的情况也不例外。在显示密钥的情况下，将使用报告中的显示名称作为列标题。否则，将显示“key0”、“key1”等列标题。

流传输

大多数导出会将其数据传输到客户端，因为数据流可能会非常大。但是，有些导出会返回整个结果集，而不是流数据。当报告数据与非报告数据（例如爆发详细信息）汇聚在一起时，通常会出现这种情况。

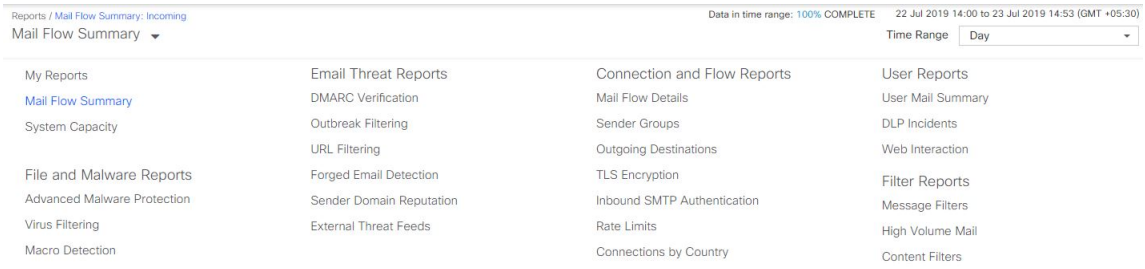
新 Web 界面上的“邮件安全监控”(Email Security Monitor) 页面

要访问新的 Web 界面，请点击**邮件安全网关以获得新的外观。试试！** leagcy Web 界面上的链接。有关详细信息，请参阅访问基于 Web 的图形用户界面 (GUI)。

如下图所示，您可以使用**报告 (Reports)** 下拉列表查看邮件网关的报告：

Note “邮件流摘要报告”(Mail Flow Summary) 页面是登录页面（登录后显示的页面）。

Figure 1: “报告”下拉列表



在 GUI 中，使用这些页面可以监控连接到邮件网关侦听程序的域。您可以监控、排序、分析和分类邮件网关的“邮件流量”，并区分大量合法邮件的发件人与潜在“垃圾邮件发送者”（大量未经请求的商业邮件的发件人）或病毒发送者。此外，这些页面还可以帮助排除系统入站连接故障（包括域的 IP 名义得分和最近发件人组匹配等重要信息）。

这些页面可帮助您对与邮件网关相关以及与存在于网关范围之外的服务相关的邮件分类，例如 IP 信誉服务、反垃圾邮件扫描服务、防病毒扫描安全服务、内容过滤器和病毒爆发过滤器。

通过**导出 (Export)** 链接可以将图表及其他数据导出为 CSV（逗号分隔值）格式。

导出的 CSV 数据将以 GMT 显示所有邮件跟踪和报告数据（不考虑邮件网关中的设置）。GMT 时间转换是为了允许独立于邮件网关使用数据，或从分布于多个时区的邮件网关中引用数据的情况。

Note 如果导出本地化 CSV 数据，则标题在某些浏览器中可能不会正常呈现。出现该情况是因为某些浏览器可能没有为本地化文本使用正确的字符集。要解决该问题，可以将文件保存到磁盘，然后使用“文件”(File) > “打开”(Open) 打开该文件。当打开该文件时，选择字符集以显示本地化文本。

有关自动导出报告数据的详细信息，请参阅检索 CSV 数据, on page 33。

邮件安全监控页面列表

- “我收藏的报告”(My Favorite Reports) 页面, on page 38

搜索与交互式邮件报告页面

许多交互式邮件报告页面均在页面底部包含“**搜索：**”**(Search For:)** 下拉菜单。

从下拉菜单中，您可以搜索多种类型的条件，包括以下条件：

- IP 地址
- 域 (Domain)
- 网络所有者 (Network owner)
- 内部用户 (Internal User)
- 目标域 (Destination domain)
- 内部发件人域 (Internal sender domain)
- 内部发件人 IP 地址 (Internal sender IP address)
- 传入 TLS 域 (Incoming TLS domain)
- 传出 TLS 域 (Outgoing TLS domain)
- SHA-256

对于大多数搜索，请选择是要精确匹配搜索文本还是查找以输入的文本开头的项（例如，以“ex”开头将匹配“example.com”）。

对于 IPv4 搜索，输入的文本始终会解释为点分十进制格式的多达四组 IP 八位二进制数。例如，“17”将在范围 17.0.0.0 至 17.255.255.255 中搜索，因此它将匹配 17.0.0.1，但不匹配 172.0.0.1。对于精确匹配搜索，请输入所有四组二进制八位数。IP 地址搜索还支持无类别域间路由 (CIDR) 格式 (17.16.0.0/12)。

对于 IPv6 搜索，您可以使用以下示例中的格式输入地址：

- 2001:db8:2004:4202::0-2001:db8:2004:4202::ff
- 2001:db8:2004:4202::
- 2001:db8:2004:4202::23
- 2001:db8:2004:4202::/64

查看报告中所含邮件的详细信息

只有报告和跟踪都在本地执行（并非在思科安全邮件和 Web 管理器中集中执行）时，此功能才有效。

Procedure

步骤 1 点击报告页面上表中的任何蓝色编号。

（并非所有的表格都有这些链接。）

“邮件跟踪”(Message Tracking) 中将显示该数字下包含的邮件。

步骤 2 向下滚动以查看列表。

What to do next

相关主题

- 处理邮件跟踪搜索结果

时间范围报告

邮件安全监控功能不断记录进入网关的邮件流量的相关数据。这些数据每60秒更新一次，但所示的显示时间有所延迟，落后当前系统时间 120 秒。可以指定所示结果中包括的时间范围。由于数据实时监控，因此信息会在数据库中定期更新和汇总。

从下表的时间范围选项中进行选择。

Table 2: 邮件安全监控功能可用的时间范围

在 GUI 中选择的以下时间范围	...定义为：
小时	最近 60 分钟 + 最多 5 分钟
天	过去 24 小时 + 过去 60 分钟
周	前 7 天 + 当日经过的小时数
30 天	最近 30 天 + 当日的耗用小时数
90 天	最近 90 天 + 当日的耗用小时数
昨天	00:00 到 23:59（午夜到下午 11:59）
上一日历月	当月第一天的 00:00 到当月最后一天的 23:59
自定义范围	您指定的开始日期和小时及结束日期和小时包含的范围

“我收藏的报告”(My Favorite Reports) 页面

您可以创建自定义报告页面，方法是在“我的报告”(My Reports) 页面上组合所有现有电子邮件安全报告中的图表（图形）和表格。

要想	相应操作
将模块添加到“我收藏的报告”(My Favorite Reports) 页面	请参阅： • 无法添加到“我的报告”(My Reports) 页面的模块，第 39 页 • 在“我收藏的报告”(My Favorite Reports) 页面上添加报告，第 39 页

要想	相应操作
查看“我收藏的报告”(My Favorite Reports) 页面	1. 从“报告”下拉列表中选择**我收藏的报告**。 2. 选择要查看的时间范围。所选时间范围会应用到所有报告，包括“我收藏的报告”(My Favorite Reports) 页面中的所有模块。 新添加的模块显示在自定义报告的顶部。 **注释** 您在新 Web 界面的“我收藏的报告”(My Favorite Reports) 页面上添加的报告模块与旧版 Web 界面上添加的报告模块不同。它还可以根据您分配的用户角色而有所不同。
重新排列“我收藏的报告”(My Favorite Reports) 页面上的模块	在“我收藏的报告”(My Favorite Reports)页面上，将模块拖放到所需位置。
从“我收藏的报告”(My Favorite Reports)页面删除模块	您可以通过以下任意一种方式从“我收藏的报告”(My Favorite Reports) 页面删除报告模块： • 点击所需报告模块右上角的 ★。 • 转到**我收藏的报告**页面，选择**管理收藏夹**以删除所需的报告模块。

无法添加到“我的报告”(My Reports) 页面的模块

- “系统状态”(System Status) 页面上的所有模块。
- “报告数据可用性”(Reporting Data Availability) 页面上的所有模块
- 位于“邮件跟踪数据可用性”(Message Tracking Data Availability) 页面上的所有模块
- 以下按域的模块来自“发件人配置文件”详细信息报告页面：“SenderBase 中的当前信息”、“发件人组信息”和“网络信息”。
- “爆发过滤器”(Outbreak Filters) 报告页面上的“过去一年病毒爆发摘要”(Past Year Virus Outbreak Summary) 图表和“过去一年病毒爆发”(Past Year Virus Outbreaks) 表格

在“我收藏的报告”(My Favorite Reports) 页面上添加报告

开始之前

- 确保您要添加的模块可以添加。请参阅无法添加到“我的报告”(My Reports) 页面的模块，第 39 页。
- 通过点击模块右上角的 ★ 删除不需要的任何默认模块。

过程

步骤 1 您可以通过以下任意一种方式在“我收藏的报告”(My Favorite Reports) 页面上添加报告模块：

注释 某些模块仅在使用这些方法中的一种时可用。如果无法使用一种方法添加模块，请尝试另一种方法。

- 转到报告下拉列表下的报告页面，然后点击报告模块顶部的 ★。
- 从 "报告"(Reports) 下拉列表中，选择**我的报告 (My Reports)**，然后点击**管理收藏夹 (Manage Favorites)**。

  报告模块按照邮件报告页面上的表格和图表列出。选择所需的报告模块，然后点击**添加 (Add)** 以添加到“我收藏的报告”(My Favorite Reports) 页面。如果您不希望在“我收藏的报告”(My Favorite Reports) 页面上显示任何报告，请选择报告模块，然后点击**删除 (Delete)**。

  每个模块只能添加一次；如果您已向报告中添加特定模块，则用于添加该模块的选项将不可用。

  注释 在“我收藏的报告”(My Favorite Reports) 页面上最多可以添加 10 个报告模块。

步骤 2 如果添加已自定义的模块（例如，通过添加、删除或重新排序列，或者通过在图表中显示非默认数据），则在“我的报告”(My Reports) 页面上自定义模块。

添加的模块使用默认设置。原始模块的时间范围无法保留。

步骤 3 如果添加包含单独图例的图表（例如，“邮件流摘要”(Mail Flow Summary) 页面中的图形），请单独添加图例。如果需要，请将其拖放至所描述数据旁边的位置。

“邮件流摘要”(Mail Flow Summary) 页面

“邮件流摘要”报告页面提供邮件网关上的邮件活动概要。“邮件流摘要”(Mail Flow Summary) 页面包括传入邮件和传出邮件的图形和摘要表。

“邮件流摘要：传入”报告页面显示由邮件网关处理和阻止的邮件总数以及传入邮件摘要的传入邮件图表。

您可以使用此页面上的邮件趋势图来根据所选的时间范围监控邮件网关处理和阻止的所有传入邮件的流。有关详细信息，请参阅时间范围报告，第 38 页。

要在您的数据中搜索特定信息，请参阅 搜索与交互式邮件报告页面 ，第 37 页

以下邮件趋势图提供传入邮件流的视觉表达。

- 威胁检测摘要
- 内容摘要

您可以根据相应类别的所需计数器查看传入邮件的邮件趋势。有关详细信息，请参阅使用计数器过滤趋势图上的数据，第 45 页。

“邮件流摘要：传出”报告页面显示由邮件网关处理和传送的邮件总数以及传出邮件摘要的传出邮件图表。

您可以使用此页面上的邮件趋势图来根据所选的时间范围监控邮件网关处理和传送的所有传出邮件的流。有关详细信息，请参阅时间范围报告，第 38 页。

以下邮件趋势图提供传出邮件的邮件流的视觉表达。

您可以根据所处理邮件的所需计数器查看传出邮件的邮件趋势。有关详细信息，请参阅使用计数器过滤趋势图上的数据，第 45 页。

以下列表解释“邮件流摘要”报告页面上的各部分：

表 *3*:“邮件流摘要”*(Mail Flow Summary)* 页面上的详细信息

部分	说明
邮件流摘要：传入	
邮件数量	“邮件数量”图表提供所处理邮件总数的视觉表达，包括处理为威胁邮件的邮件。
威胁邮件	“威胁邮件”图表提供邮件网关阻止的邮件总数的视觉表达。
威胁检测摘要	“威胁检测摘要邮件”趋势图提供基于以下类别的视觉表达： • **连接和 IP 信誉过滤**：由 IP 信誉过滤和无效收件人归类为威胁的邮件。 • **垃圾邮件检测**：被反垃圾邮件扫描引擎归类为威胁的邮件。 • **邮件欺骗**：由于DMARC验证失败而被归类为威胁的邮件。 • **病毒爆发威胁摘要**：由病毒爆发过滤引擎归类为网络钓鱼、欺诈、病毒或恶意软件的邮件。 • **附件和恶意软件检测**：被防病毒和 AMP 引擎归类为威胁的邮件。 • **所有类别**：归类为威胁的所有邮件。
内容摘要	“内容摘要”邮件趋势图提供基于以下类别的视觉表达： • **灰色邮件**：归类为市场营销、批量或社交网络的邮件。 • **内容过滤器**：由内容过滤器分类的邮件。 • **所有类别**：由灰色邮件引擎和内容过滤器分类的所有邮件。
邮件流摘要：传出	
邮件数量	“邮件数量”图表提供所处理邮件总数的视觉表达，包括处理为正常邮件的邮件。

部分	说明
邮件传输	“邮件传送”图表提供所传送邮件的视觉表达，包括硬退回。
传出邮件	“传出邮件”趋势图提供基于以下类别的视觉表达： • 垃圾邮件 • 病毒邮件 • 由 AMP 检测到 • 由内容过滤器拦截 • DLP 拦截

相关主题

- 邮件网关如何对邮件分类， 第 42 页
- 传入和传出摘要与图形， 第 8 页
- 在“邮件流摘要”(Mail Flow Summary) 页面上对邮件进行分类， 第 43 页
- 使用计数器过滤趋势图上的数据， 第 45 页

邮件网关如何对邮件分类

由于邮件持续通过邮件管道，因此其可以应用于多个类别。例如，邮件可以标记为垃圾邮件或病毒邮件；它还可以与内容过滤器相匹配。各种过滤器和扫描活动的优先顺序会极大地影响邮件处理的结果。

在上面的示例中，各种判定遵循以下优先顺序规则：

- 垃圾邮件
- 病毒邮件
- 匹配内容过滤器

按照这些规则，如果某个邮件被标记为具有垃圾邮件特征，并且您的反垃圾邮件设置被设置为丢弃具有垃圾邮件特征的邮件，则该邮件将被丢弃，垃圾邮件计数器会增加。

此外，如果反垃圾邮件设置被设置为允许具有垃圾邮件特征的邮件继续在邮件管道中通行，并且后续内容过滤器将会丢弃、退回或隔离该邮件，则垃圾邮件计数器仍会增加。仅当该邮件不具有垃圾邮件或病毒特征时，内容过滤器才会增加。

或者，如果邮件被爆发过滤器隔离，则在该邮件从隔离中释放出来并再次进入工作队列之前，不会进行计数。

有关邮件处理优先级的完整信息，请参阅邮件网关在线帮助或用户手册中有关邮件管道的章节。

传入和传出摘要与图形

传入和传出摘要部分提供对系统上所有邮件活动的实时活动的访问，并且包含传入和传出邮件图形与邮件摘要。通过“时间范围”(Time Range) 菜单，可以选择报告的时间范围。您选择的时间范围在所有邮件安全监控器页面的各处使用。下面介绍了邮件的各种类型或类别（请参阅邮件分类, on page 8）。

邮件趋势图显示了邮件流量的视觉表达，而摘要表提供了相同信息的数字细分表达。摘要表包括每种类型邮件的比例和实际数量，包括尝试发送的邮件总数、威胁邮件数和正常邮件数。

传出邮件图表和摘要显示了出站邮件的类似信息。

相关主题

- 邮件安全监控中的邮件计数注意事项, on page 8

邮件安全监控中的邮件计数注意事项

邮件安全监控用于计算传入邮件数量的方法取决于每封邮件的收件人数。例如，从 example.com 发送给三个收件人的传入邮件将计算为三封来自该发件人的邮件。

由发件人信誉过滤拦截的邮件实际不会进入工作队列，因此，邮件网关无权访问传入邮件的收件人列表。在这种情况下，使用倍数来估算收件人数量。此倍数由思科基于对大量现有客户数据样本的研究得出。

在“邮件流摘要”(Mail Flow Summary) 页面上对邮件进行分类

被视为威胁的传入邮件以及在“邮件流摘要”报告页面中传送的传出邮件按照如下方式进行分类：

表 *4:*“邮件流摘要”*(Mail Flow Summary)* 页面上的邮件类别

类别	说明
邮件流摘要：传入	

类别	说明
IP 信誉过滤	由 HAT 策略拦截的所有连接乘以一个固定倍数，再加上由收件人限制拦截的所有收件人。 “由 IP 信誉过滤拦截”(Stopped by IP Reputation Filtering) 值的计算取决于多种因素： • 此发件人的“受限制”邮件数量。 • 被拒绝或被 TCP 拒绝的连接数量（可能是部分计数）。 • 每个连接的邮件数量的保守倍数。 当邮件网关的负载繁重时，不会为逐个发件人维护已拒绝的连接准确计数。而是针对每个时间间隔内最重要的发件人来记录被拒绝的连接计数。在这种情况下，所显示的值可以解释为指示被拦截的最小邮件数的值。 “邮件流摘要”报告页面上的“IP 信誉过滤”总数和百分比始终基于所有被拒绝连接的完整计数。只有每个发件人的连接计数会因负载而受到限制。
发件人域信誉过滤	根据发件人域的信誉来判定阻止的邮件总数。
无效收件人	除所有 RAT 拒绝外，还包括会话 LDAP 拒绝所拒绝的所有邮件收件人的总数和百分比。
反垃圾邮件	反垃圾邮件扫描引擎检测为具有垃圾邮件特征或可疑的传入邮件总数和百分比。此外还包括同时是垃圾邮件和具有病毒特征的邮件。
防病毒	被检测为具有病毒特征但不是垃圾邮件的传入邮件总数和百分比。 以下消息计入 " 检测到病毒 " 类别中： • 病毒扫描结果为“已修复”(Repaired) 或“感染”(Infectious) 的邮件 • 在选中了将已加密的邮件计为包含病毒的选项时，病毒扫描结果为“已加密”(Encrypted) • 在针对不可扫描的邮件执行的操作不是“传送”(Deliver) 时，病毒扫描结果为“不可扫描”(Unscannable) • 在选中了传送到备用邮件主机或备用收件人的选项时，病毒扫描结果为“不可扫描”(Unscannable) 或“已加密”(Encrypted) 的邮件 • 以手动方式或通过超时从“病毒爆发”(Outbreak) 隔离区删除的邮件。

类别	说明
高级恶意软件防护	文件分析服务阻止的传入邮件的总数和百分比。 文件信誉过滤发现邮件附件是恶意软件。该值不包括通过文件分析发现为恶意的判定更新或文件。
内容过滤器	由邮件和内容过滤器拦截的传入邮件的总数和百分比。
DMARC 策略	DMARC 验证策略失败的传入邮件的总数和百分比。
S/MIME 验证/解密失败	未通过 S/MIME 验证和/或解密的传入邮件的总数和百分比。
邮件流摘要：传出	
硬退回	永久无法传送的传出邮件的总数和百分比。
已送达	已传送的传出邮件的总数和百分比。

注释 如果您已配置防病毒设置以传送不可扫描或已加密的邮件，这些邮件将被计为正常邮件，而不是病毒。否则，邮件将被计入具有病毒特征的邮件。

此外，如果邮件与某个邮件过滤器相匹配，且未被该过滤器丢弃或退回，则这些邮件被视为正常邮件。邮件过滤器丢弃或退回的邮件不计入总数。

相关主题

“邮件流详细信息”(Mail Flow Details) 页面 ， 第 58 页

使用计数器过滤趋势图上的数据

您可以基于所需的时间范围和趋势图上可用计数器过滤数据。

在“时间范围”(Time Range) 下拉列表中选择的时间范围用于趋势图，直到选择了其他值。

“邮件流摘要”报告页趋势图上的计数器用于查看特定于不同过滤器的数据。点击可用计数器以过滤数据。

“系统容量”(System Capacity) 页面

“系统容量”(System Capacity) 页面提供有关系统负载的详细说明，包括工作队列中的邮件、花费在工作队列中的平均时间、传入和传出邮件（总量、大小和数量）、总体CPU使用率、按功能的CPU使用率和内存页面交换信息。

“系统容量”(System Capacity) 页面可用于确定以下信息：

- 识别邮件网关超过推荐容量，进而需要优化配置或添加邮件网关的情况。
- 确定系统行为方面指向即将发生的容量问题的历史趋势。
- 确定系统中协助故障排除耗用资源最多的部分。

务必要监控邮件网关，以确保您的容量适合邮件总量。随着时间的推移，邮件量会不可避免地增加，适当的监控可确保主动添加容量或进行配置更改。监控系统容量的最有效方式是跟踪总量、工作队列中的邮件以及资源节约模式下的事件。

- **邮件量**：了解环境中的“正常”邮件量和“一般”峰值非常重要。随着时间的推移跟踪此数据以测量邮件量增长。您可以使用“传入邮件”(Incoming Mail) 和“传出邮件”(Outgoing Mail) 页面长期跟踪数量。有关详细信息，请参阅系统容量 - 传入邮件, on page 29和系统容量 - 传出邮件, on page 29。
- **工作队列**：工作队列旨在充当“缓冲器” - 吸收和过滤垃圾邮件攻击并处理非垃圾邮件的不正常增加情况。但是，工作队列也是系统具有压力的最佳指示器，长时间并频繁地备份工作队列可能表明存在容量问题。使用“工作队列”(Workqueue) 页面可跟踪邮件在工作队列中花费的平均时间，以及工作队列中的活动。有关详细信息，请参阅系统容量 - 工作队列, on page 28。
- **资源节约模式**：当邮件网关变得过载时，会进入“资源节约模式”(RCM)，并发送“关键”系统警报。这旨在保护设备，使其可以处理任何邮件积压情况。邮件网关不应频繁进入RCM，并且应仅在邮件量出现超大或异常增长期间进入。频繁的 RCM 警报可能表明系统正在超负荷。请参阅系统容量 - 系统负载, on page 29。

相关主题

- 系统容量 - 工作队列, on page 28
- 系统容量 - 传入邮件, on page 29
- 系统容量 - 传出邮件, on page 29
- 系统容量 - 系统负载, on page 29
- 内存页面交换说明, on page 30
- 系统容量 - 全部, on page 30

系统容量 - 工作队列

“工作队列”(Workqueue) 页面显示邮件在工作队列中花费的平均时间，在垃圾邮件隔离区中或在策略、病毒或病毒爆发隔离区中花费的任何时间除外。您可以查看时间段，从一小时到一个月。此平均值可以帮助确定延迟邮件传送的短期事件和确定系统上工作负载的长期趋势。

Note 如果邮件从隔离区释放到工作队列中，“工作队列中的平均时间”指标将忽略此时间。这可防止重复计数，以及由于在隔离区中花费的时间延长而造成统计信息失真。

此报告也显示指定时间段内的工作队列中的邮件量，并且显示相同时间段内工作队列中的最大邮件数量。工作队列中的最大邮件数图表还显示工作队列阈值级别。

工作队列图形中的偶尔峰值是正常的，并在预期之内。如果工作队列中的邮件数长时间保持高于配置的阈值，可能表示存在容量问题。这种情况下，请考虑调整阈值级别或审核系统配置。

有关更改工作队列阈值级别的说明，请参阅为系统运行状况参数配置阈值。

Tip 当查看工作队列页面时，您可能要测量工作队列备份的频率，并标注超过 10000 封邮件的工作队列备份。

系统容量 - 传入邮件

传入邮件页面显示传入连接、传入邮件总数、平均邮件大小和传入邮件总大小。您可以将结果限制到指定的时间范围。了解环境中的正常邮件量和峰值趋势至关重要。可以使用传入邮件页面，帮助随着时间的推移跟踪邮件量增长并规划系统容量。您可能还希望比较传入邮件数据与发件人配置文件数据，以查看从特定域发送到网络的邮件量的趋势。

Note 传入连接数增加不一定会影响系统负载。

系统容量 - 传出邮件

传出邮件页面显示传出连接、传出邮件总数、平均邮件大小和传出邮件总大小。您可以将结果限制到指定的时间范围。了解环境中的正常邮件量和峰值趋势至关重要。可以使用传出邮件页面，帮助随着时间的推移跟踪邮件量增长并规划系统容量。您可能还要将“传出邮件”(Outgoing Mail) 数据与“外发目标”(Outgoing Destinations) 数据进行比较，以查看从特定域或 IP 地址发送的邮件量的趋势。

系统容量 - 系统负载

系统负载报告显示如下信息：

- CPU 总体使用情况
- 内存页面交换
- 资源节约活动

CPU 总体使用情况

邮件网关经过优化，可使用空闲 CPU 资源来提高邮件吞吐量。高 CPU 使用率并不一定表示存在系统容量问题。如果高 CPU 使用率与持续的大容量内存页面交换一同出现，则可能表示存在容量问题。

Note 此图还显示 CPU 的阈值级别。如果要更改阈值级别，请在 Web 界面中依次使用**系统管理 (System Administration)** > **系统运行状况 (System Health)** 页面或在 CLI 中使用 **`healthconfig`** 命令。请参阅为系统运行状况参数配置阈值。

该页面还包含一个图，用于显示不同功能（包括邮件处理、垃圾邮件和病毒引擎、报告和隔离）使用的 CPU 量。按功能划分的 CPU 图形可以很好地指示产品的哪些方面在系统上使用最多资源。如果需要优化邮件网关，则此图有助于确定哪些功能可能需要调整或禁用。

内存页面交换

内存页面交换图显示系统必须切换到磁盘的频率。此图还显示内存页面交换的阈值级别。如果要更改阈值级别，请在 Web 界面中依次使用**系统管理 (System Administration)** > **系统运行状况 (System Health)** 页面或在 CLI 中使用 **`healthconfig`** 命令。请参阅为系统运行状况参数配置阈值。

资源节约活动

资源节约活动图显示邮件网关进入资源节约模式 (RCM) 的次数。例如，如果图中显示 n 次，则意味着邮件网关进入了 RCM n 次，并已退出至少 n-1 次。

邮件网关不应频繁进入RCM，并且应仅在邮件量出现超大或异常增长期间进入。如果“资源节约活动”(Resource Conservation Activity) 图显示您的邮件网关频繁进入 RCS，则可能表明系统变得过载。

内存页面交换说明

该系统旨在定期交换内存，因此进行一些内存交换是适当的，并不表示邮件网关存在问题。除非系统一致地大容量交换内存，否则内存交换正常，并且是预期行为（尤其在 C170 和 C190 设备上）。为提高性能，您可能需要将邮件网关添加到网络或调整配置以确保实现最大吞吐量。

系统容量 - 全部

“全部”(All) 页面将以前的所有系统容量报告整合在一个页面上，以便查看不同报告之间的关系。例如，您可能会发现在进行过量内存交换时，邮件队列很高。这可能是表示存在容量问题。您可能希望将此页面另存为 PDF 文件，以保留系统性能快照供以后参考（或与支持人员共享）。有关生成英语以外的其他语言的 PDF 的信息，请参阅有关报告的注意事项, on page 76。

报告数据可用性

使用**报告数据可用性**页面可以查看数据，实时洞察资源利用率和邮件流量故障点。

所有数据资源利用率和邮件流量问题位置都显示在此页面上，包括由思科安全邮件和 Web 管理器管理的整体邮件网关的数据可用性。

在此报告页面中，还可以查看特定邮件网关和时间范围的数据可用性。

“思科高级恶意软件保护”(Advanced Malware Protection)页面

高级恶意软件防护通过如下方式防范邮件附件中的零日威胁和基于文件的针对性威胁：

- 获取已知文件的信誉。
- 分析尚不为信誉服务所知的某些文件行为。
- 在获得新信息时评估新出现的威胁，并在确定为威胁的文件进入您的网络后通知您。

此功能适用于传入和传出邮件。

有关文件信誉过滤和文件分析的详细信息，请参阅《适用于*Cisco Secure Email Gateway*的 *AsyncOS* 的用户指南或联机帮助》。

要查看报告页面，请从“报告”下拉列表的“文件和恶意软件报告”部分中选择**高级恶意软件保护**。

“高级恶意软件保护”报告页面显示以下报告视图：

- 高级恶意软件防护 - 摘要， 第 49 页
- 高级恶意软件保护 - AMP 信誉， 第 49 页
- 高级恶意软件保护 - 文件分析， 第 50 页
- 高级恶意软件防护 - 文件追溯， 第 51 页
- 高级恶意软件保护 - 邮箱自动修复， 第 51 页

“高级恶意软件保护”报告页面显示的指标栏提供连接到思科威胁网格设备的邮件网关实时数据。

注释

- 您必须在CLI上使用 `trailblazerconfig > enable` 命令来填充指标栏上的数据。有关详细信息，请参阅《思科邮件安全设备命令参考指南》。
- 您只能在思科威胁网格设备中查看“天”、“周”和“月”的数据。

相关主题

- 通过 SHA-256 散列标识文件 ， 第 52 页
- 查看其他报告中的文件信誉过滤数据 ， 第 52 页

高级恶意软件防护 - 摘要

“高级恶意软件保护 - 摘要”页显示由文件信誉和文件分析服务标识的基于传入和传出文件的威胁完整摘要。

有关详细信息，请参阅 高级恶意软件保护 - AMP 信誉， 第 49 页 和 高级恶意软件保护 - 文件分析 ， 第 50 页。

高级恶意软件保护 - AMP 信誉

“高级恶意软件保护 - AMP 信誉”(Advanced Malware Protection - AMP Reputation) 页面显示由文件信誉服务标识的基于文件的传入和传出威胁。

有关判定已更改的文件，请参阅 AMP 判定更新报告。这些判定不会反映在“高级恶意软件防护”(Advanced Malware Protection) 报告中。

如果从某个已压缩或已存档的文件中提取的某个文件是恶意文件，则只有这个已压缩或已存档的文件的 SHA 值包括在“高级恶意软件防护”(Advanced Malware Protection) 报告中。

AMP 处理的传入文件部分按不同的类别显示传入恶意软件文件，例如恶意、安全、未知、不可扫描和低风险。

传入恶意文件分类如下：

- 从 AMP 信誉服务器接收的分类为**恶意软件**且已列入阻止列表的文件 SHA 百分比。
- 从面向终端的 AMP 控制台接收的分类为**自定义检测**且已列入阻止列表的文件 SHA 百分比。从面向终端的 AMP 控制台获取的已列入阻止列表的文件 SHA 百分比在报告的“传入恶意软件威胁文件”部分中显示为**简单自定义检测**。
- 根据阈值设置分类为**自定义阈值**且已列入阻止列表的文件的 SHA 百分比。

您可以点击报告的“更多详细信息”部分中的链接，以查看在面向终端的AMP控制台中已列入阻止列表的文件 SHA 的文件轨迹详细信息。

您可以在报告的“AMP 处理的传入文件”部分查看**低风险**判定详细信息。

您可以使用“高级恶意软件保护: 传入”报告页面的“AMP 信誉”视图查看以下内容：

- 由高级恶意软件保护引擎的文件信誉服务标识的传入文件的摘要，以图形格式表示。
- 基于所选时间范围的所有传入恶意软件威胁文件的趋势图。
- 传入恶意软件威胁文件排行榜。
- 基于文件类型的传入威胁文件排行榜。
- 列出了传入恶意软件威胁文件排行榜的“传入恶意软件威胁文件”交互式表。

  深入分析以查看详细的分析结果，包括每个文件的威胁特征。

  如果您的访问权限允许您查看填充此报告之邮件的邮件跟踪数据，请点击表中的蓝色数字链接。

您可以使用“高级恶意软件保护: 传出”报告页面的“AMP 信誉”视图查看以下内容：

- 由高级恶意软件保护引擎的文件信誉服务标识的传出文件的摘要，以图形格式表示。
- 基于所选时间范围的所有传出恶意软件威胁文件的趋势图。
- 传出恶意软件威胁文件排行榜。
- 基于文件类型的传出威胁文件排行榜。
- 列出了由文件信誉服务标识的传出恶意软件威胁文件的排行榜的“传出恶意软件威胁文件”交互式表。

  深入分析以查看详细的分析结果，包括每个文件的威胁特征。

  如果您的访问权限允许您查看填充此报告之邮件的邮件跟踪数据，请点击表中的蓝色数字链接。

高级恶意软件保护 - 文件分析

高级恶意软件保护 -“文件分析”(File Analysis) 页面显示了发送以供分析的每个文件的时间和判定（或临时判定）。邮件网关每 30 分钟检查一次分析结果。

要查看超过 1000 个文件分析结果，请将数据导出为 .csv 文件。

对于采用现场思科 AMP Threat Grid 设备的部署：在 AMP Threat Grid 设备上列入允许列表的文件显示为“正常”(clean)。有关允许列表的信息，请参阅 AMP Threat Grid 文档或联机帮助。

深入分析以查看详细的分析结果，包括每个文件的威胁特征。

您还可以搜索有关SHA的其他信息，或点击文件分析详细信息页面底部的链接以在分析了文件的服务器上查看其他详细信息。有关详细信息，请参阅通过 SHA-256 散列标识文件 ，第 52 页。

如果您的访问权限允许您查看填充此报告的邮件的邮件跟踪数据，请点击表中的**详细信息 (Details)**链接。

如果从某个已压缩或已存档的文件中提取的某个文件送交分析，则只有这个已提取文件的SHA值包括在“文件分析”(File Analysis) 中。

您可以使用“思科高级恶意软件保护报告”(Advanced Malware Protection) 页面中的“文件分析”(File Analysis) 视图进行查看：

- 由高级恶意软件保护引擎的分析服务上传以进行文件分析的传入和传出文件的数量。
- 已完成文件分析请求的传入和传出文件的列表。
- 具有待处理文件分析请求的传入和传出文件的列表。

高级恶意软件防护 - 文件追溯

“高级恶意软件防护 - 文件追溯”(Advanced Malware Protection - File Retrospection) 页面列出了由此邮件网关处理的文件，对于这些文件，自收到邮件以来判定已经发生变化。有关此场景的详细信息，请参阅邮件网关的相应文档。

由于“高级恶意软件防护”重点关注有针对性的威胁和零日威胁，因此威胁判定可以随着汇聚数据提供更多信息而发生变化。

要查看超过 1000 个裁定更新，请将数据导出为 .csv 文件。

如果单个 SHA-256 的判定多次发生变化，此报告仅显示最新的判定，而不显示判定历史记录。

要查看特定 SHA - 256 在最大可用时间范围内的所有受影响的邮件（无论为报告选择的时间范围如何），请点击 SHA-256 链接。

您可以使用“高级恶意软件保护”报告页的“文件追溯”视图来查看：

- 带有追溯性判决更改的传入和传出文件的列表。

高级恶意软件保护 - 邮箱自动修复

“高级恶意软件保护 - 邮箱自动修复”报告页显示传入文件的邮箱修复结果的详细信息。

您可以使用“高级恶意软件保护 - 邮箱自动修复”页查看追溯性安全详细信息，例如：

- 对其邮箱执行的补救操作成功或不成功的收件人的列表
- 对邮件执行的修复操作
- 与 SHA-256 散列关联的文件名
- 为其邮箱执行补救操作成功或不成功的收件人定义的配置文件名称列表
- 补救失败原因

- 没有映射到域的配置文件

在以下情况下，将更新未成功修复的收件人字段：

- 邮箱无效：收件人不是有效的 Microsoft Exchange Online 用户或 Microsoft Exchange On-Premise 用户，或者收件人不属于 Microsoft Exchange Online 域帐户或在您邮件网关上配置的 Microsoft Exchange On-Premise 域帐户。
- 包含附件的邮件在邮箱中不再可用，例如，最终用户删除了邮件。
- 身份验证错误：邮件网关上提供的用于连接到 Microsoft Exchange On-Premise 邮箱的用户账号不正确。
- 连接错误：当邮件网关尝试执行补救操作时，邮件网关与 Microsoft Exchange Online 服务或 Microsoft Exchange On-Premise 服务之间存在连接问题。
- 权限错误：
  - 如果是 Microsoft Exchange On-Premise 帐户，则邮件网关上提供的用于连接到 Microsoft Exchange On-Premise 邮箱的用户账号不会分配 impersonator 角色。
  - 如果是 Microsoft Exchange Online 帐户，则 Office 365 应用没有访问收件人邮箱所需的权限。
- 没有映射到域的配置文件：没有映射到收件人域的配置文件。
- 邮箱不可访问或无效：
  - 用于访问邮箱的帐户配置文件的配置文件类型不正确。
  - 收件人不是有效的 Microsoft Exchange Online 用户或 Microsoft Exchange On-Premise 用户。
  - 收件人不属于 Microsoft Exchange Online 域帐户或邮件网关上配置的 Microsoft Exchange On-Premise 域帐户。

点击 SHA-256 散列可查看邮件跟踪中的相关邮件。

通过 SHA-256 散列标识文件

由于文件名很容易更改，因此设备会使用安全散列算法 (SHA-256) 为每个文件生成标识符。如果设备处理具有不同名称的同一文件，所有实例被识别为相同的 SHA-256。如果多个设备处理相同的文件，则该文件的所有实例都具有相同的 SHA-256 标识符。

在大多数报告中，文件按其 SHA-256 值列出（以缩写格式）。

查看其他报告中的文件信誉过滤数据

用于文件信誉和分析的数据会在其他相关的报告中提供。在适用的报告中，“由高级恶意软件防护检测到”(Detected by Advanced Malware Protection) 列在默认情况下可能处于隐藏状态。要显示其他列，请点击表格右上角的“自定义列”图标。

“病毒过滤”(Virus Filtering) 页面

“病毒过滤”(Virus Filtering) 页面提供发送到网络以及从网络发出的病毒的概述。“病毒筛选”(Virus Filtering) 页面显示已由邮件网关中运行的病毒扫描引擎检测到的病毒。要针对特定病毒采取具体操

作，可能需要使用此报告。例如，如果发现收到已知嵌入 PDF 文件中的大量病毒，则您可能要创建过滤器操作来隔离具有 PDF 附件的邮件。

如果运行多个病毒扫描引擎，则“病毒过滤”(Virus Filtering) 页面包括来自所有启用的病毒扫描引擎的结果。显示在该页面上的病毒的名称由病毒扫描引擎确定。如果多个扫描引擎检测到某个病毒，则同一病毒可能具有多个对应的条目。

“病毒过滤”(Virus Filtering) 页面提供从网络发出或发送到网络的病毒的概述。“检测到的排名靠前的传入邮件病毒”(Top Incoming Virus Detected) 部分按降序显示已发送到您的网络的病毒图表视图。“检测到的排名靠前的传出邮件病毒”(Top Outcoming Virus Detected) 部分按降序显示从您的网络发出的病毒图表视图。

Note 要查看哪些主机向您的网络发送了感染病毒的邮件，请转到“传入邮件”(Incoming Mail) 页面，指定相同的报告期间，然后按病毒阳性进行排序。同样，要查看哪些 IP 地址在您的网络中发送了具有病毒特征的邮件，请查看“传出发件人”(Outgoing Senders) 页面并按具有病毒特征的邮件排序。

“病毒类型详细信息”(VirusTypes Details) 列表显示有关特定病毒的信息，包括受感染的传入和传出邮件及受感染的邮件总数。受感染的传入邮件详细信息列表显示病毒名称和感染此病毒的传入邮件数。同样，传出邮件部分显示病毒名称和感染此病毒的传出邮件数。您可以按“传入邮件数”(Incoming Messages)、“传出邮件数”(Outgoing Messages) 和“受感染邮件总数”(Total Infected Messages) 对病毒类型详细信息进行排序。

“宏检测”(Macro Detection) 页面

可以使用“宏检测”(Macro Detection) 报告页面查看：

- 以图形和表格格式显示的按文件类型排名靠前的启用宏的传入附件摘要。
- 以图形和表格格式显示的按文件类型排名靠前的启用宏的传出附件摘要。

您可以点击启用宏的附件数量，以在邮件跟踪中查看相关邮件。

要在邮件网关上查看“宏检测”报告页面，请从“报告”(Reports) 下拉列表中选择**宏检测 (Macro Detection)**。

注释 报告生成期间：

- 如果在存档文件中检测到一个或多个宏，则存档文件的文件类型将按一递增。不计算存档文件中启用宏的附件数量。
- 如果在嵌入文件中检测到一个或多个宏，则父文件类型将递增一。不计算嵌入文件中启用宏的附件数量。

“DMARC 验证”(DMARC Verification) 页面

“DMARC 验证”(DMARC Verification) 页面显示 DMARC 验证失败的排名靠前的域，以及 AsyncOS 针对 DMARC 验证失败的邮件执行的操作详细信息。可以使用此报告优化 DMARC 设置并回答以下类型的问题：

- 哪些域发送的不符合 DMARC 要求的邮件数最多？
- 对于每个域，AsyncOS 针对 DMARC 验证失败的邮件执行了什么操作？

“DMARC 验证”(DMARC Verification) 页面包含：

- 显示按 DMARC 验证失败排名靠前的域的图形表示形式。
- 有关每个域以下信息的表格：
  - 被拒绝、隔离或接受而不采取任何操作的邮件数。点击数字，可查看选定类别下的邮件列表。
  - 通过 DMARC 验证的邮件数。
  - DMARC 验证尝试总数。

您可以选择报告的时间范围，例如小时、周或自定义范围。与所有报告相同，通过**导出 (Export)** 链接可以将图表数据或详细信息列表导出为 CSV 格式。

“URL 过滤”(URL Filtering) 页面

- 仅当启用 URL 过滤时，才会填充 URL 过滤报告模块。
- 提供传入和传出邮件的“URL 过滤”(URL Filtering) 报告。
- 只有由 URL 过滤引擎扫描的邮件（作为反垃圾邮件/爆发过滤器扫描的一部分或通过邮件/内容过滤器）才会包含在这些模块中。但是，并非所有结果都有必要专门可归属于URL过滤功能。
- “排名靠前的 URL 类别”(Top URL Categories) 模块包含已扫描的邮件中找到的所有类别，无论其是与内容过滤器还是邮件过滤器匹配都如此。
- 每封邮件都只能与一个 URL 信誉级别关联。对于包含多个 URL 的邮件，统计信息反映邮件中任何 URL 的最低信誉。
- 在“安全服务”(Security Services) >“URL 过滤”(URL Filtering) 中配置的全局允许列表内的 URL 未包含在报告中。

  报告中包含个别过滤器中使用的允许列表内的 URL。
- 恶意 URL 是爆发过滤器确定为信誉不佳的 URL。不确定 URL 是爆发过滤器确定需要点击时间保护的 URL。因此，不确定 URL 已被重写，从而重定向到思科网络安全代理。
- 基于 URL 类别的过滤器的结果会反映在内容和邮件过滤器报告中。
- 思科网络安全代理的点击时间 URL 评估结果不会反映在报告中。

“URL 追溯”(URL Retrospection) 页面

“URL 追溯报告”(URL Retrospection Report) 页面显示由 URL 追溯服务处理的 URL。此页面随即列出以下详细信息：

- URL - 思科安全邮件云网关发送到 URL 追溯服务分析的 URL。
- 接收判定 - 思科安全邮件云网关从 URL 追溯服务收到判定的日期和时间。
- 受影响邮件的补救状态 - 对恶意 URL 采取的操作以及针对每种补救状态的邮件数。可能的补救状态包括：正在进行、成功、失败和已跳过。

“病毒爆发过滤”(Outbreak Filtering) 页面

“病毒爆发过滤”报告页面显示有关最近的病毒爆发的信息，并显示由于“爆发过滤器”而隔离的邮件的相关信息。使用此页面可以监控对针对性病毒、诈骗和网络钓鱼攻击的防御。

使用“病毒爆发过滤”报告页面可回答以下类型的问题：

- 多少封邮件被隔离？依据的是哪项“爆发过滤器”(Outbreak Filters) 规则？
- 邮件在病毒爆发隔离区中停留多长时间？
- 哪些可能是恶意的 URL 是最常见的？

要查看“病毒爆发过滤”(Outbreak Filtering) 报告页面，请从“报告”下拉列表中选择**病毒爆发过滤 (Outbreak Filtering)**。

下表解释了“病毒爆发过滤”报告页面上的各部分：

表 5:“病毒爆发过滤”(Outbreak Filtering) 页面上的详细信息

部分	说明
时间范围 (Time Range) （下拉列表）	包含用于选择时间范围选项的下拉列表。
按类型划分的威胁	“按类型划分的威胁”(Threats By Type) 部分显示邮件网关接收的不同类型的威胁邮件。
威胁概要	“威胁概要”部分按恶意软件、网络钓鱼、垃圾邮件和病毒显示威胁邮件的细分。 要查看填充此报告的邮件的邮件跟踪详细信息，请点击表中的蓝色数字链接。

部分	说明
威胁详情	威胁详情交互表会显示有关特定病毒爆发的详细信息信息，包括威胁类别（病毒、诈骗或网络钓鱼）、威胁名称、威胁说明和识别的邮件数。 要查看填充此报告的邮件的邮件跟踪详细信息，请点击表中的蓝色数字链接。
传入邮件中的被拦截邮件	“传入邮件中被拦截的邮件"部分显示在所选时间段内由爆发过滤器处理的传入邮件数的图表和摘要。 非病毒性威胁包括网络钓鱼邮件、诈骗和使用指向外部网站的链接进行的恶意软件分发。
按威胁级别划分的被拦截邮件	“按威胁级别划分的被拦截邮件”部分显示爆发过滤器捕获的威胁的严重性级别图表和摘要。 级别 5 威胁表示在范围或影响方面非常严重，而级别 1 威胁表示威胁风险较低。有关威胁级别的说明，请参阅邮件网关的在线帮助或用户指南。
病毒爆发隔离区中驻留的邮件	“病毒爆发隔离区中驻留的邮件”显示邮件在病毒爆发隔离区中所驻留的时间长度。 此持续时间取决于系统需要多长时间收集关于潜在威胁的足够数据以对其安全性做出判定。带有病毒性威胁的邮件通常比带有非病毒性威胁的邮件在隔离区中花费更多时间，因为它们必须等待防病毒程序更新。还会反映您为每个邮件策略指定的最大保留时间。
频繁重写的 URL	“频繁重写的URL”部分显示重写最频繁的URL，重写的目的是将邮件收件人重定向到思科网络安全代理，以便在收件人点击邮件中潜在恶意链接时对网站进行点击时间评估。 此列表可能包括非恶意的URL，因为如果邮件中的任何URL被视为恶意，则邮件的所有 URL 均会被重写。 要查看填充此报告的邮件的邮件跟踪详细信息，请点击表中的蓝色数字链接。

注释 为了正确填充“病毒爆发过滤器”报告页面上的各个表，邮件网关必须能够与思科更新服务器进行通信。

“伪造邮件检测”(Forged Email Detection) 页面

“伪造邮件检测”(Forged Email Detection) 页面包括以下报告：

- **排名靠前的伪造邮件检测**。显示内容字典中与传入邮件中的伪造“发件人：”信头匹配的前十个用户。
- **伪造邮件检测：详细信息**显示内容词典中与传入邮件中的伪造“发件人：”信头匹配所有用户的列表，对于给定用户，还会显示匹配的邮件的数量。

要在安全管理设备上查看“伪造邮件检测”报告页面，请从“报告”下拉列表中选择**伪造邮件检测**。

只有在使用“伪造邮件检测”内容过滤器或 `forged-email-detection` 邮件过滤器时，才会填充“伪造邮件检测”报告。

从“伪造邮件检测”报告页面中，您还可以将原始数据导出到CSV文件。点击报告页面顶部的**导出 (Export)** 链接。选择要导出的所需报告模块，然后点击**下载 (Download)**。

“发件人域信誉”(Sender Domain Reputation) 页面

您可以使用“发件人域信誉”(Sender Domain Reputation) 报告页面：

- 以图形格式根据从 SDR 服务接收的判定查看传入邮件。
- 以图形格式根据从 SDR 服务接收的威胁类别查看传入邮件。

注释 只有那些 SDR 判为 "不受信任" 或 "有问题" 的信息才被归入 SDR 威胁类别，如 "垃圾邮件"、"恶意 "等。

- 根据从 SDR 服务中表格的形式接收的威胁类别的传入邮件摘要。

要在安全管理设备上查看“发件人域信誉”报告页面，请从“产品”下拉列表中选择**发件人域信誉**。

“外部威胁源”(External Threat Feeds) 页面

您可以使用“外部威胁源”(External Threat Feeds) 报告页面查看：

- 以图形格式查看用于检测邮件威胁的排名靠前的 ETF 来源
- 以表格格式查看用于检测邮件威胁的 ETF 来源的摘要。
- 以图形格式查看与检测到的邮件威胁相匹配的排名靠前的 IOC。
- 以图形格式查看用于过滤恶意传入邮件连接的排名靠前的 ETF 来源。
- 以表格格式查看用于过滤恶意传入邮件连接的 ETF 来源的摘要。

在“外部威胁源来源摘要”(Summary of External Threat Feed Sources) 部分：

- 您可以点击特定 ETF 来源的邮件数量，在邮件跟踪中查看相关邮件。
- 您可以点击特定威胁源来源，根据 IOC 查看 ETF 来源的分布情况。

在“感染指标 (IOC) 匹配摘要”部分：

- 您可以点击特定 ETF 来源的 IOC 数量，在邮件跟踪中查看相关邮件。
- 您可以点击特定 IOC，根据 ETF 来源查看 IOC 的分布情况。

要查看“外部威胁源”(External Threat Feeds) 报告页面，请从“报告”(Reports) 下拉列表中选择**外部威胁源 (External Threat Feeds)**。

“邮件流详细信息”(Mail Flow Details) 页面

“邮件流详细信息”报告页面为连接到托管思科安全邮件和 Web 管理器的所有远程主机提供实时信息的交互式报告。您可以收集有关发送邮件到您的系统的 IP 地址、域和网络所有者（组织）的信息。您还可以收集有关传出发件人的 IP 地址和域的信息。

要查看“邮件流详细信息”报告页面，请从“报告”下拉列表中选择**邮件流详细信息**。

“邮件流详细信息”报告页面包含以下选项卡：

- 传入邮件
- 传出邮件发件人

要在您的数据中搜索特定信息，请参阅搜索与交互式邮件报告页面 ， 第 37 页。

您可以从“传入邮件”选项卡中执行以下操作：

- 按威胁邮件总数查看发件人排行榜（采用图形格式）。
- 按安全邮件数查看发件人排行榜（采用图形格式）。
- 按恶意邮件数查看发件人排行榜（采用图形格式）。
- 请参阅已将邮件发送至思科安全邮件和 Web 管理器的 IP 地址、域或网络所有者（组织）。
- 查看关于已将邮件发送到您的邮件网关的发件人的详细统计信息。统计信息包括连接数（接受或拒绝）、按安全服务（发件人信誉过滤、反垃圾邮件、防病毒等）细分的所尝试邮件数量、威胁邮件总数、恶意邮件和安全邮件总数。
- 有关特定 IP 地址、域或网络所有者（组织）的详细信息，请参阅“传入邮件”交互式表。有关详细信息，请参阅“传入邮件”(Incoming Mails) 表 ， 第 61 页。

  如果您的访问权限允许您查看填充此报告的邮件的邮件跟踪数据，请点击表中的数字链接。

您可以从“传出发件人”选项卡中执行以下操作：

- 按威胁邮件总数查看发件人排行榜（采用图形格式）。
- 按安全邮件数查看发件人排行榜（采用图形格式）。
- 查看您的组织中传出威胁邮件（垃圾邮件、病毒等）的发件人排行榜（按 IP 地址或域）。
- 查看关于已从您的邮件网关发送邮件的发件人的详细统计信息。统计信息包括按安全服务（发件人信誉过滤、反垃圾邮件、防病毒等）细分的威胁邮件总数。

- 有关特定 IP 地址或域的详细信息，请参阅“发件人详细信息”交互式表。有关详细信息，请参阅“发件人详细信息”(Sender Details) 表，第 64 页。

  如果您的访问权限允许您查看填充此报告的邮件的邮件跟踪数据，请点击表中的数字链接。

相关主题

- “传入邮件”(Incoming Mails) 表，第 61 页
- “没有域信息”，第 60 页
- 时间范围报告，第 38 页
- “邮件流详细信息”(Mail Flow Details) 页面中的视图，第 59 页

“邮件流详细信息”(Mail Flow Details) 页面中的视图

“邮件流详细信息: 传入”报告页面有三种不同的视图：

- IP 地址
- 域
- 网络所有者

这些视图在选定视图的情景中提供连接到系统的远程主机的快照。

此外，在“邮件流详细信息”(Mail Flow Details) 页面的“传入邮件”(Incoming Mails) 表中，您可以点击“发件人的 IP 地址”(Sender’s IP Address)、“域名”(Domain name) 或“网络所有者信息”(Network Owner Information) 以检索特定的发件人配置文件信息。有关发件人配置文件信息的详细信息，请参阅“发件人配置文件”(Sender Profile) 页面，第 63 页。

注释 网络所有者 (Network owners) 是包含域的实体。域 (Domains) 是包含 IP 地址的实体。

根据所选的视图，“传入邮件详细信息 (Incoming Mail Details)”交互式表格中显示将邮件发送至邮件网关上配置的所有公共侦听器的排名靠前的 IP 地址、域或网络所有者。可以监控传入邮件网关的所有邮件的流量。

在“发件人配置文件”(Sender Profile) 页面上点击 IP 地址、域或网络所有者可访问有关发件人的详细信息。“发件人配置文件”(Sender Profile) 页面是与特定 IP 地址、域或网络所有者相关的“邮件流详细信息”(Mail Flow Details) 页面。

如需获得对“传入邮件”交互式表中包括的数据的解释，请参阅“传入邮件”(Incoming Mails) 表，第 61 页。

在“邮件流详细信息”(Mail Flow Details) 页面中，可以将原始数据导出到 CSV 文件。

注释 您可以生成“邮件流详细信息”报告页面的计划报告。请参阅计划的报告，第 77 页。

“邮件流详细信息: 传出”报告页面有两种不同的视图：

- IP 地址
- 域

这些视图在选定视图的情景中提供连接到系统的远程主机的快照。

根据所选的视图，“发件人详细信息”交互式表显示了从公共侦听程序（从邮件安全设备配置）发送邮件的收件人 IP 地址或域排行榜。您可以监控从邮件网关传出的所有邮件流。

如需获得对“发件人详细信息”交互式表中包括的数据的解释，请参阅“发件人详细信息”(Sender Details) 表，第 64 页。

“没有域信息”

已连接至邮件网关并且无法通过双重DNS查找进行验证的域将自动分组到名为“没有域信息”的特殊域。可以控制通过发件人验证来管理此类未验证主机的方式。请参阅配置网关以接收邮件。

可以通过“显示的项目”(Items Displayed) 菜单选择要在列表中显示的发件人数。

时间范围报告

邮件安全监控功能不断记录进入网关的邮件流量的相关数据。这些数据每60秒更新一次，但所示的显示时间有所延迟，落后当前系统时间 120 秒。可以指定所示结果中包括的时间范围。由于数据实时监控，因此信息会在数据库中定期更新和汇总。

从下表的时间范围选项中进行选择。

Table 6: 邮件安全监控功能可用的时间范围

在 GUI 中选择的以下时间范围	...定义为：
小时	最近 60 分钟 + 最多 5 分钟
天	过去 24 小时 + 过去 60 分钟
周	前 7 天 + 当日经过的小时数
30 天	最近 30 天 + 当日的耗用小时数
90 天	最近 90 天 + 当日的耗用小时数
昨天	00:00 到 23:59（午夜到下午 11:59）
上一日历月	当月第一天的 00:00 到当月最后一天的 23:59
自定义范围	您指定的开始日期和小时及结束日期和小时包含的范围

“传入邮件”(Incoming Mails) 表

“邮件流详细信息: 传入邮件”(Mail Flow Details: Incoming Mails) 页面底部的“传入邮件”(Incoming Mails) 交互式表列出了已连接至邮件网关上的公共侦听程序的排名靠前的发件人。下表根据所选视图显示域、IP 地址或网络所有者。

系统通过执行双重 DNS 查找来获得和验证远程主机 IP 地址的有效性。有关双 *DNS* 查找和发件人验证的更多信息，请参阅邮件网关的用户指南或在线帮助。

对于发件人，即“传入邮件”表的第一列或“按威胁邮件总数排名靠前的发件人”中列出的网络所有者、IP 地址或域，请点击“发件人”或“无域信息”链接查看有关发件人的详细信息。结果显示在发件人配置文件 (Sender Profile) 页面上，其中包括来自 IP 信誉服务的实时信息。从“发件人配置文件”(Sender Profile) 页面中，您可以查看有关特定 IP 地址或网络所有者的详细信息。有关详细信息，请参阅“发件人配置文件”(Sender Profile) 页面 ，第 63 页。

您还可以查看“发件人组”(Sender Groups) 报告，方法是点击“邮件流详细信息”(Mail Flow Details) 页面底部的发件人组报告。有关“发件人组报告”(Sender Groups report) 页面的详细信息，请参阅发件人组报告 ，第 65 页。

要查看填充此报告的邮件的邮件跟踪详细信息，请点击表中的数字超链接。

下表显示了“传入邮件”(Incoming Mails) 表的表列说明：

表 *7:* 用于“传入邮件”*(Incoming Mails)* 表的表列说明

列名	说明
发件人域（域）	发件人的域名。
发件人 IP 地址（IP 地址）	发件人的 IP 地址。
主机名（IP 地址）	发件人的主机名。
已验证的 DNS（IP 地址）	由 DNS 验证的 IP 地址。
IP 信誉得分（IP 地址）	发件人的 IP 信誉得分。
上一个发件人组（IP地址）	上一个发件人组的详细信息。
上一个发件人组（IP地址）	上一个发件人组的详细信息。
网络所有者（网络所有者）	发件人的网络所有者。
拒绝的连接（域和网络所有者）	由 HAT 策略阻止的所有连接。当邮件网关的负载繁重时，不会为逐个发件人维护已拒绝的连接准确计数。而是针对每个时间间隔内最重要的发件人来记录被拒绝的连接计数。
接受的连接（域和网络所有者）	所有已接受的连接。
尝试的总数 (Total Attempted)	已尝试的所有已接受和已阻止的连接。

列名	说明
由收件人限制（域和网络所有者）拦截	这是“由信誉过滤拦截”(Stopped by Reputation Filtering) 的一个组件。表示由于超出下列任何 HAT 限制而拦截的收件人邮件的数量：每小时的最大收件人数、每封邮件的最大收件人数或每个连接的最大邮件数。此值加上与被拒绝或被 TCP 拒绝的收件人邮件估算值就得到了“由信誉过滤拦截”(Stopped by Reputation Filtering) 的值。
由 IP 信誉过滤拦截	“由 IP 信誉过滤拦截”(Stopped by IP Reputation Filtering) 的值根据多个因素进行计算： • 来自此发件人的“受限制”邮件数 • 已拒绝或 TCP 拒绝的连接数（可能是部分计数） • 每个连接的邮件数量的保守倍数。 当邮件网关的负载繁重时，不会为逐个发件人维护已拒绝的连接准确计数。而是针对每个时间间隔内最重要的发件人来记录被拒绝的连接计数。在这种情况下，显示的值可以解释为“下限”，即至少已拦截这么多邮件。 **注释** “邮件流摘要”(Mail Flow Summary) 页面上的“IP 信誉过滤”(IP Reputation Filtering) 总数始终基于所有被拒绝连接的完整计数。只有每个发件人的连接计数会因负载而受到限制。
由域信誉过滤拦截	根据发件人域的信誉来判定阻止的邮件总数。
作为无效收件人拦截 (Stopped as Invalid Recipients)	由会话 LDAP 拒绝和所有 RAT 拒绝予以拒绝的所有邮件收件人。
检测到的垃圾邮件 (Spam Detected)	检测到的任何垃圾邮件。
检测到的病毒 (Virus Detected)	检测到的任何病毒
由高级恶意软件保护检测到	高级恶意软件保护引擎检测到的邮件总数。
内容过滤器拦截 (Stopped by Content Filter)	由内容过滤器拦截的邮件总数。
由 DMARC 拦截 (Stopped by DMARC)	基于域的邮件身份验证、报告和一致性 (DMARC) 验证失败的邮件总数。 **注释** 邮件网关根据“失败-拒绝”、“失败-隔离”和“失败-无操作”结果显示 “Stopped by DMARC” 消息的总数。

列名	说明
威胁邮件总数 (Total Threat)	威胁邮件总数（由信誉拦截、作为无效收件人拦截、垃圾邮件以及病毒）
市场营销部门	被检测为不需要的营销邮件的邮件数。
社交	被检测为营销邮件的邮件数。
统计数据	检测为批量的邮件数。
灰色邮件总数	检测为灰色邮件的邮件数。
正常 (Clean)	所有正常邮件。 未启用灰色邮件功能的邮件网关上处理的邮件被计为正常邮件。

“发件人配置文件”(Sender Profile) 页面

当您在**邮件流详细信息 (Mail Flow Details)** [新 Web 界面] 或**传入邮件 (Incoming Mail)** 页面上的传入邮件详细信息 (Incoming Mail Details) 交互式表中点击收件人时，会出现“发件人配置文件”(Sender Profile) 页面。它显示关于特定 IP 地址、域或网络所有者（组织）的详细信息。通过点击传入邮件 (Incoming Mail)页面或其他“发件人配置文件”(Sender Profile) 页面上的相应链接，您可以访问任何 IP 地址、域或网络所有者的“发件人配置文件”(Sender Profile) 页面。

网络所有者是包含域的实体。域 *(Domains)* 是包含 IP 地址的实体。

为 IP 地址、域和网络所有者显示的“发件人配置文件”(Sender Profile) 页面稍有不同。对于每项，该页面包含来自特定发件人的传入邮件的图形和摘要表。在图形下方，表列出与发件人相关联的域或 IP 地址。（单个 IP 地址的“发件人配置文件”[Sender Profile] 页面不包含更精细的列表。）“发件人配置文件”(Sender Profile) 页面还包括一个信息部分，其中包含当前 SenderBase、发件人组和发件人的网络信息。

- 网络所有者配置文件页面包含网络所有者以及与该网络所有者关联的域和 IP 地址的信息。
- 域配置文件页面包含与该域关联的域和 IP 地址。
- IP 地址配置文件页面只包含有关该 IP 地址的信息。

每个“发件人配置文件”(Sender Profile) 页面底部的“当前信息”(Current Information) 表格中都包含以下数据：

- 来自 IP 信誉服务的全局信息，包括：
  - IP 地址、域名和/或网络所有者
  - 网络所有者类别（仅限网络所有者）
  - CIDR 范围（仅限 IP 地址）
  - IP 地址、域和/或网络所有者的日量级和月量级
  - 自从此发件人收到第一封邮件以来的天数

- 上一个发件人组以及是否进行了 DNS 验证（仅 IP 地址发件人配置文件页面）

日流量用于衡量某个域在最近 24 小时内发送了多少邮件。SenderBase 流量类似于用来衡量地震的里氏震级，使用以 10 为底数的对数标尺计算邮件数量。该标尺的最大理论值设置为 10，等同于 100% 的实际邮件数量。使用该对数标尺时，流量每增加 1 个单位，实际数量就会增加 10 倍。

月流量的计算方法与日流量相同，只是百分比基于最近 30 天发送的邮件数量来计算。

- 平均量级（仅限 IP 地址）
- 生命周期数量/30 天数量（仅限 IP 地址配置文件页面）
- 有担保发件人状态（仅限 IP 地址配置文件页面）
- IP 信誉得分（仅限 IP 地址配置文件页面）
- 自从第一封邮件以来的天数（仅限网络所有者和域配置文件页面）
- 与此网络所有者相关联的域数量（仅限网络所有者和域配置文件页面）
- 此网络所有者中的 IP 地址数量（仅限网络所有者和域配置文件页面）
- 用于发送邮件的 IP 地址数量（仅限网络所有者页面）

点击**来自 SenderBase 的详细信息 (More from SenderBase)** 可查看包含 IP 信誉服务提供的所有信息的页面。

- 有关由此网络所有者控制的域和 IP 地址的详细信息显示在网络所有者配置文件页面上。有关域中的 IP 地址的详细信息，将显示在域页面上。

从域配置文件页面中，您可以点击特定 IP 地址以查看特定信息，或查看组织配置文件页面。

“发件人详细信息”(Sender Details) 表

“邮件流详细信息: 传出邮件”(Mail Flow Details: Outgoing) 页面底部的“发件人详细信息”(Sender Details) 交互式表列出了已连接至邮件网关上的公共侦听器的发件人排行榜。下表根据所选视图显示了域或 IP 地址。

要查看填充此报告的邮件的邮件跟踪详细信息，请点击表中的数字超链接。

下表显示了“发件人详细信息”(Sender Details) 表的表列说明：

表 *8*:“发件人详细信息”*(Sender Details)* 表的表列说明

列名	说明
发件人域（域）	发件人的域名。
发件人 IP 地址（IP 地址）	发件人的 IP 地址。
主机名（IP 地址）	发件人的主机名。

列名	说明
检测到的垃圾邮件 (Spam Detected)	检测到的任何垃圾邮件。
检测到的病毒 (Virus Detected)	检测到的任何病毒。
由高级恶意软件保护检测到	高级恶意软件保护引擎检测到的邮件总数。
内容过滤器拦截 (Stopped by Content Filter)	由内容过滤器拦截的邮件总数。
DLP 拦截	由 DLP 引擎拦截的邮件总数。
威胁邮件总数	威胁邮件（垃圾邮件、病毒）总数
正常 (Clean)	所有正常邮件。 未启用灰色邮件功能的邮件网关上处理的邮件被计为正常邮件。
邮件总数	所有邮件的总数。

发件人组报告

“发件人组”(Sender Groups) 报告按发件人组和邮件流量策略操作提供连接摘要，从而便于查看 SMTP 连接和邮件流量策略趋势。“按发件人组的邮件流量 (Mail Flow by Sender Group)”列表显示每个发件人组的连接的百分比和数量。“按邮件流量策略操作的连接”(Connections by Mail Flow Policy Action) 图表显示每个邮件流量策略操作的连接百分比。此页面概述了主机访问表 (HAT) 策略的有效性。有关 HAT 的详细信息，请参阅配置网关以接收邮件。

传出目标

“传出邮件目标”(Outgoing Destinations) 页面提供有关您的公司发送邮件所至的域的信息。该页面包含两部分。页面上半部分包含一些图表，这些图表描述按传出威胁邮件排名靠前的目标，以及按页面上半部分的传出正常邮件排名靠前的目标。页面下半部分显示一个图表，包含按收件人总数（默认设置）排序的所有列。

您可以选择报告的时间范围，例如天、周或自定义范围。与所有报告相同，通过**导出 (Export)** 链接可以将图表数据或详细信息列表导出为 CSV 格式。

“外发目标”(Outgoing Destinations) 页面可用于回答以下类型的问题：

- 邮件网关将邮件发送到哪些域？
- 向每个域发送多少邮件？
- 该邮件中有多少是正常的、具有垃圾邮件特征、具有病毒特征、具有恶意软件特征或由内容过滤器拦截？
- 传送了多少邮件以及被目标服务器硬性退回了多少邮件？

“TLS 加密”(TLS Encryption) 页面

“TLS 加密”(TLS Encryption) 页面显示所收发邮件的 TLS 加密的整体使用情况。该报告还显示使用 TLS 连接发送邮件的每个域的详细信息。

“TLS 连接”(TLS Encryption) 页面可用于确定以下信息：

- 总体而言，传入和传出连接的哪个部分使用 TLS？
- 我与哪些合作伙伴成功建立了 TLS 连接？
- 我与哪些合作伙伴建立的 TLS 连接没有成功？
- 在 DANE 支持下，我与哪些合作伙伴成功建立了 TLS 连接？
- 在 DANE 支持下，我未能与哪些合作伙伴成功建立 TLS 连接？
- 哪些合作伙伴的 TLS 证书存在问题？
- 某个合作伙伴使用 TLS 的邮件占总邮件的百分比是多少？
- DANE 支持的传出连接成功的百分比是多少？
- DANE 支持的传出连接不成功的百分比是多少？

“TLS 加密”(TLS Encryption) 页面分为传入连接部分和传出连接部分。每个部分都包括图表、摘要和详细信息表格。

图表显示您指定的时间范围内，传入或传出 TLS 加密和未加密连接的视图。该图显示邮件总数、加密和未加密邮件的数量成功和失败的 TLS 加密邮件的数量以及成功和失败的 DANE 连接的数量。需要 TLS 的连接图表和仅首选 TLS 的连接图表有所不同。

此表显示发送或接收加密邮件的域的详细信息。对于每个域，可以查看成功和失败的需要及首选的 TLS 连接数量、尝试的 TLS 连接总数（无论成功还是失败）未加密连接总数以及 DANE 连接总数（根据是成功还是失败）。您还可以查看所有尝试 TLS 连接的百分比和成功发送的加密邮件总数，不考虑 TLS 是首选还是需要。您可以通过在表的右上方自定义列图标来显示或隐藏列。

“入站 SMTP 身份验证”(Inbound SMTP Authentication) 页面

“入站 SMTP 身份验证”(Inbound SMTP authentication) 页面显示了使用客户端证书和“SMTP AUTH”命令对邮件网关与用户的邮件客户端之间的 SMTP 会话进行身份验证。如果邮件网关接受证书或 SMTP AUTH 命令，则会建立到邮件客户端的 TLS 连接，供客户端用来发送邮件。因为邮件网关无法逐个用户跟踪这些尝试，因此报告会根据域名和域 IP 地址显示有关 SMTP 身份验证的详细信息。

使用此报告可确定以下信息：

- 总体而言，多少入站连接使用 SMTP 身份验证？
- 多少连接使用经过认证的客户端？
- 多少连接使用 SMTP AUTH？
- 当尝试使用 SMTP 身份验证时，哪些域无法连接？
- 当 SMTP 身份验证失败时，多少连接成功使用回退？

“入站 SMTP 身份验证”(Inbound SMTP Authentication) 页面包含一个表示已接收的连接的图形、一个表示已尝试 SMTP 身份验证连接的邮件收件人的图形，以及一个包含有关对连接进行身份验证的尝试的详细信息的表。

“已接收的连接”(Received Connections) 图形显示在指定时间范围内来自尝试使用 SMTP 身份验证对其连接进行身份验证的邮件客户端的传入连接。该图表显示邮件网关接收的连接总数、未尝试使用 SMTP 身份验证进行验证的次数，使用客户端证书验证连接的成功和失败次数，以及使用 SMTP AUTH 命令进行验证的成功和失败次数。

“已接收的收件人”(Received Recipients) 图形显示了收件人的数量，这些收件人的邮件客户端尝试对其与邮件网关的连接进行身份验证以使用 SMTP 身份验证来发送邮件。该图形还显示其连接已进行身份验证的收件人数和其连接未进行身份验证的收件人数。

“SMTP 身份验证详细信息”(SMTP Authentication details) 表显示了域的详细信息，这些域的用户尝试对其与邮件网关的连接进行身份验证以发送邮件。对于每个域，可以查看尝试使用客户端证书进行连接的成功或失败次数、尝试使用 SMTP AUTH 命令进行连接的成功或失败次数，以及在客户端证书连接尝试失败后回退到 SMTP AUTH 的次数。您可以使用页面顶部的选项卡按域名或域 IP 地址显示此信息。

“速率限制”(Rate Limits) 页面

通过按信封发件人进行速率限制，您可以根据发件人地址从单个发件人限制每个时间间隔的邮件收件人数。“速率限制”(Rate Limits) 报告显示最严重超过此限制的发件人。

使用此报告可帮助确定以下内容：

- 可能用于批量发送垃圾邮件的有漏洞用户账户。
- 组织中的失控应用程序，这些应用程序使用邮件发送通知、风险通告、自动声明等内容。
- 组织中具有大量邮件活动的来源，用于内部计费或资源管理目的。
- 可能未被视为垃圾邮件的大量入站邮件流量的来源。

请注意，包含内部发件人（例如内部用户或传出邮件发件人）的统计信息的其他报告仅测量已发送的邮件数；它们不会向大量收件人表明少数邮件的发件人的身份。

“按事件划分的排名靠前的危害”图表显示最频繁尝试向超过配置限制的收件人发送邮件的信封发件人。每次尝试都是一个事件。此图表汇总所有侦听程序的事件计数。

“按已拒绝收件人划分的排名靠前的危害”图表显示向高于配置限制的最大数量的收件人发送邮件的信封发件人。此图表汇总所有侦听程序的收件人计数。

要按信封发件人配置速率限制或修改现有速率限制，请参阅使用邮件流策略定义传入邮件规则。

“按国家/地区划分的连接”(Connections by Country) 页面

您可以使用“按国家/地区划分的连接”报告页面查看：

- 以图形格式显示的基于来源国家/地区的传入邮件连接排行榜。
- 以表格格式显示的基于源国家/地区的传入邮件连接总数。

您可以点击特定地理位置的传入邮件连接数来查看邮件跟踪中的相关消息。

“邮件总数”列仅显示在 SMTP 连接级别接受的邮件。

注释 报告生成期间：

- 如果将一个或多个传入邮件连接检测为私有 IP 地址，则这些传入邮件连接将在报告中归类为“私有 IP 地址”。
- 如果将一个或多个传入邮件连接检测为非有效 IP 信誉得分，则这些传入邮件连接将在报告中归类为“无国家/地区信息”。

“用户邮件摘要”(User Mail Summary) 页面

“用户邮件摘要”(User Mail Sumamry) 页面按邮件地址提供有关内部用户发送和接收的邮件的信息（一个用户可能列出了多个邮件地址 - 报告中不合并邮件地址）。

该页面包含两部分：

- 描述按正常传入和传出邮件排名靠前用户和收到灰色邮件的靠前用户的图表。
- 用户邮件流量详细信息

您可以选择报告时间范围（小时、天、周或月）。与所有报告相同，通过**导出 (Export)** 链接可以将图表数据或详细信息列表导出为 CSV 格式。您还可以通过点击表格右上方的“自定义列”(Customize Column) 链接显示隐藏表列或隐藏默认列。

“用户邮件流量详细信息”(User Mail Flow Details) 列表将每个邮件邮件地址收到和发送的邮件细分为“正常”(Clean)、“检测到垃圾邮件”(Spam Detected)（仅限传入）、“检测到病毒”(Virus Detected) 和“内容过滤器匹配”(Content Filter Matches)。您可以通过点击列标题对列表排序。

使用内部用户报告，可以回答以下类型的问题：

- 谁发送的外部邮件最多？
- 谁接收的正常邮件最多？
- 谁接收的灰色邮件最多？
- 谁接收的垃圾邮件最多？
- 谁触发了哪些内容过滤器？
- 谁的邮件被内容过滤器拦截？

入站内部用户是您根据“收件人：”(Rcpt To:) 地址为其收到邮件的用户。出站内部用户基于“发件人: (Mail From:)”地址，在跟踪内部网络中的发件人所发送邮件的类型时非常有用。

请注意，某些出站邮件（如退回）包含空发件人。它们计入出站和“未知”之下。

点击某个内部用户，可查看该用户的“内部用户详细信息”(Internal User detail) 页面。

点击表格右上方的“自定义列”图标以显示默认情况下隐藏的列，例如由智能多扫描列检测到的传入垃圾邮件或智能多扫描列检测到的传出垃圾邮件。

相关主题

- 用户邮件控制详细信息, on page 69
- 搜索特定的内部用户, on page 18

用户邮件控制详细信息

“用户邮件流详细信息”部分显示有关指定用户的详细信息，包括显示每个类别（检测到垃圾邮件、检测到病毒、由高级恶意软件防护检测到、由内容过滤器拦截、检测到灰色邮件和正常）邮件数量的传入和传出邮件明细。或者，对于传入邮件，您可以点击表格右上方的自定义列图标，以显示"智能多扫描"列检测到的传入垃圾邮件。此值反映包含的附件被文件信誉过滤确定为恶意的邮件数。它不包括判定更新或由文件分析发现为恶意的文件。此外，还显示传入和传出邮件内容过滤器和 DLP 策略匹配。

点击内容过滤器名称，可在相应的内容过滤器信息页面中查看该过滤器的详细信息（请参阅“内容过滤器”(Content Filters) 页面, on page 20）。使用此方法可查看发送或接收了与特定内容过滤器匹配的邮件的用户列表。

搜索特定的内部用户

您可以通过“用户邮件摘要”(User Mail Summary) 页面底部的搜索表单，搜索特定的内部用户（邮件地址）。选择是完全匹配搜索文本还是查找以输入的文本开头的项目（例如，以“ex”开头将匹配“example.com”）。

“DLP 事件摘要”(DLP Incident Summary) 页面

“DLP 事件摘要”(DLP Incident Summary) 页面显示传出邮件中发生的防数据丢失 (DLP) 策略违规事件的信息。邮件网关使用在“传出邮件策略”(Outgoing Mail Policies) 表中启用的 DLP 邮件策略来检测用户发送的敏感数据。违反 DLP 策略的每个外发邮件均报告为一个事件。

使用 DLP 事件报告，可以回答以下类型的问题：

- 用户发送什么类型的敏感数据？
- 这些 DLP 事件具有什么样的严重性？
- 传送的这些邮件有多少数量？
- 丢弃的这些邮件有多少数量？
- 是谁在发送这些邮件？

“DLP 事件摘要”(DLP Incident Summary) 页面包括两个主要部分：

- DLP 事件趋势图，按严重性（低、中、高、关键）和策略匹配排名靠前的 DLP 事件；
- DLP 事件详细信息列表。

您可以选择报告的时间范围，例如小时、周或自定义范围。与所有报告相同，通过**导出 (Export)** 链接可以将图表数据或详细信息列表导出为CSV格式。有关生成英语以外的其他语言的PDF的信息，请参阅有关报告的注意事项, on page 76。

点击 DLP 策略的名称可查看有关策略检测到的 DLP 事件的详细信息。使用此方法可以获取发送的邮件包含策略检测到的敏感数据的用户列表。

相关主题

- DLP 事件详细信息, on page 70
- “DLP 策略详细信息”(DLP Policy Detail) 页面, on page 70

DLP 事件详细信息

当前为邮件网关的传出邮件策略启用的DLP策略会在“DLP事件详细信息”表格中列出。点击DLP策略的名称可查看更详细的信息。

“DLP事件详细信息”表显示了每个策略的DLP事件总数，并按严重性级别细分。严重性级别还包括已退回的邮件数，以及在清除、已发送的加密或删除的邮件中传递的邮件数。点击列标题可对数据进行排序。

“DLP 策略详细信息”(DLP Policy Detail) 页面

如果点击了“DLP 事件详细信息”(DLP Incident Details) 表中某个 DLP 策略的名称，则随之打开的“DLP 策略详细信息”(DLP Policy Detail) 页面将会显示该策略的 DLP 事件数据。该页面根据严重性显示有关 DLP 事件的图表。

该页面还包括一个位于页面底部的“按发件人的事件”(Incidents by Sender) 列表，其中列出了发送的邮件违反 DLP 策略的各个内部用户。该列表还按用户显示此策略的 DLP 事件总数（按严重级别细分）以及其中是否有任何邮件以明码形式传送、以加密形式传送或已经丢弃。您可以使用“按发件人的事件 (Incidents by Sender)”列表了解可能将组织的敏感数据发送给网络之外人员的用户。

点击发件人名称，将打开“内部用户”(Internal Users) 页面。有关详细信息，请参阅#unique_1535。

“网络交互”(Web Interaction) 页面

- 只有启用了网络交互跟踪功能，才能填充网络交互跟踪报告。
- 网络交互跟踪报告模块不会实时更新，而是每 30 分钟刷新一次。此外，点击重写的 URL 后，网络交互跟踪报告最长可能需要两小时，才会报告此事件。
- 网络交互跟踪报告不会实时更新。点击云重定向的重写URL后，网络交互跟踪报告最长可能需要两小时，才会报告此事件。
- 网络交互跟踪报告适用于传入和传出邮件。
- 这些模块中仅包含最终用户（通过策略或爆发过滤器）点击的云重定向重写 URL。
- “网络交互跟踪”(Web Interaction Tracking) 页面包括以下报告：

最终用户点击的恶意 URL 排行榜。点击 URL 可查看包含以下信息的详细报告：

- 点击了重写恶意 URL 的最终用户列表。
- 点击该 URL 的日期和时间。
- URL 是否已由策略或爆发过滤器重写。
- 点击重写的URL时采取的操作（允许、阻止或未知）。请注意，如果URL被爆发过滤器重写，且未提供最终判定，则状态显示为“未知”(unknown)。

点击恶意 URL 的最终用户排行榜

本部分显示点击传入和传出邮件中重写恶意 URL 的最终用户排行榜摘要。

网络交互跟踪详细信息 (Web Interaction Tracking Details)。包括以下信息：

- 所有云重定向重写 URL（恶意和非恶意）的列表。点击某个 URL 可查看详细报告。
- 点击云重定向重写的 URL 时采取的操作（允许、阻止或未知）。

要显示数据，请执行以下操作：

- 选择**传入邮件策略 (Incoming Mail Policies) > 爆发过滤器(Outbreak Filters)** 配置爆发过滤器，并启用邮件修改和 URL 重写。
- 为内容过滤器配置“**重定向到思科安全代理**”操作。

请注意，如果最终用户点击某个URL时，其判定（正常或恶意）未知，则状态将显示为未知。这可能是因为，需要进一步审查该 URL，或用户点击时网络服务器停止服务或无法访问。

- 最终用户点击重写的 URL 的次数。点击数字可查看包含可点击的 URL 的所有邮件列表。
- 在使用网络交互跟踪报告时，请记住以下限制：
  - 如果已将内容或邮件过滤器配置为重写恶意 URL 后传送邮件并通知其他用户（例如管理员），则原始收件人的网络交互跟踪数据将增加，即使获得通知的用户点击的是重写的 URL 也不例外。
  - 如果使用 Web 界面将包含重写 URL 的被隔离邮件副本发送给用户（例如管理员），则原始收件人的网络交互跟踪数据将增加，即使接收邮件副本的用户点击的是重写的URL也不例外。
  - 在任何时候，如果您计划修改邮件网关时间，请确保系统时间与协调世界时 (UTC) 同步。

“补救报告”(Remediation Report) 页面

您可以使用“补救”报告来监控“邮箱自动补救”和“邮箱搜索和补救”的补救结果。

使用此报告：

- 要查看尝试进行邮箱自动补救以及邮箱搜索和补救的邮件列表。
- 要了解补救失败原因。例如，连接错误、身份验证错误等。

以下列表解释“速率限制”报告上的各部分：

部分	说明
摘要	“摘要”部分显示以下信息： • 使用邮箱自动补救以及邮箱搜索和补救进行补救的邮件总数。 • 为已配置的补救操作成功补救的邮件数。 • 补救失败的邮件数。
邮箱自动补救	“邮箱自动补救”报告部分显示以下信息： • 邮箱自动修复成功或不成功的收件人列表。 • 对邮件执行的自动修复操作 • 与 SHA-256 散列关联的文件名。点击 SHA-256 散列可查看邮件跟踪页面中的相关邮件。 • 为其邮箱执行自动补救操作成功或不成功的收件人定义的配置文件名称列表 • 自动补救失败的原因。

邮箱搜索和补救	“邮箱搜索和补救”部分显示以下详细信息：
	• 正在进行或已完成的补救批处理列表。
	• 批处理中邮件的补救状态。
	• 批处理名称和批处理ID。点击批处理名称可查看批处理详细信息：
	  • 启动邮箱搜索和补救的日期和时间。
	  • 启动邮箱搜索和补救的来源。
	  • 启动邮箱搜索和补救的主机。
	  • 对邮件执行的补救操作。
	  • 消息的思科 Ironport 邮件 ID。
	  • 一个已读回执图标，用于显示收件人在成功补救邮件之前是否已阅读该邮件。
	  • 特定批处理中的邮件补救状态为“成功”(Success)、“失败”(Failed) 或“进行中”(In Progress)。
	  • 发送邮件的发件人的邮件地址。
	  • 传送邮件并稍后尝试补救的收件人的邮件地址。
	  • 将邮件发送给收件人的日期和时间。

“邮件过滤器”(Message Filters) 页面

“邮件过滤器”(Message Filters) 页面通过两种形式显示排名靠前的邮件过滤器匹配项（匹配邮件数量最多的邮件过滤器）：条形图和表格形式。

使用条形图，可查找传入和传出邮件触发最多的邮件过滤器。表格形式显示排名靠前的邮件过滤器和各个邮件过滤器的匹配项数。点击数值可使用“邮件跟踪”(Message Tracking) 查看该数值中包含的所有邮件的列表。

您可以选择报告的时间范围，例如小时、周或自定义范围。与所有报告相同，通过**导出 (Export)** 链接可以将图表数据或详细信息列表导出为 CSV 格式。

“大量邮件”(High Volume Mail) 页面

Note “大量邮件”(High Volume Mail) 页面仅显示使用“信头重复”规则的邮件过滤器的数据。

“大量邮件”(High Volume) 页面包含以下条形图形式的报告：

- **排名靠前的主题**。使用此图表可以了解 AsyncOS 接收的邮件的热门主题。
- **排名靠前的信封发件人**。使用此图表可以了解 AsyncOS 接收的邮件排名靠前的信封发件人。
- **按匹配数排名靠前的邮件过滤器**。使用此图表可以了解排名靠前的邮件过滤器（使用“信头重复”规则）匹配项。

“大量邮件”(High Volume Mail) 页面还提供排名靠前的邮件过滤器和各个邮件过滤器的匹配项数表格。点击数值可使用“邮件跟踪”查看该数值中包含的所有邮件的列表。

您可以选择报告的时间范围，例如小时、周或自定义范围。与所有报告相同，通过**导出 (Export)** 链接可以将图表数据或详细信息列表导出为 CSV 格式。

“内容过滤器”(Content Filters) 页面

“内容过滤器”(Content Filters) 页面通过两种形式显示排名靠前的传入和传出邮件内容过滤器匹配项（匹配邮件数量最多的内容过滤器）：条形图和列表。使用“内容过滤器”(Content Filters) 页面，可以按内容过滤器或按用户查看企业策略，并回答以下类型的问题：

- 传入或传出邮件触发哪些内容过滤器的次数最多？
- 发送或接收的邮件触发了特定内容过滤器的排名靠前的用户有哪些？

点击列表中内容过滤器的名称，可在“内容过滤器详细信息”(Content Filter detail) 页面查看有关该过滤器的详细信息。

相关主题

- 内容过滤器详细信息, on page 73

内容过滤器详细信息

点击内容过滤器名称链接以查看内容过滤器详细信息。“内容过滤器详细信息”(Content Filter Detail) 页面显示随时间推移的过滤器匹配，以及按内部用户的匹配。

在“按内部用户划分的匹配项”(Matches by Internal User) 部分中，您可以点击用户的名称来查看该内部用户的（邮件地址）“内部用户”(Internal User) 详细信息页面（请参阅#unique_1535）。

“安全打印”(Safe Print) 页面

您可以使用“安全打印”(Safe Print) 报告页面查看：

- 以图形格式显示的基于文件类型的安全打印附件的数量。
- 基于表格格式的文件类型的安全打印附件摘要。

在“安全打印文件类型的摘要”(Summary of Safe Print File Types) 部分中，点击要在邮件跟踪中查看邮件详细信息的安全打印附件总数。

“高级网络钓鱼防护报告”(Advanced Phishing Protection Reports) 页面

报告 (Reports) > 邮件流摘要 (Mail Flow Summary) > 高级网络钓鱼防护 (Advanced Phishing Protection) 报告页面会显示以下内容：

- 已成功转发到思科高级网络钓鱼防护云服务的邮件总数。
- 未转发到思科高级网络钓鱼防护云服务的邮件总数。

注释 如果邮件元数据转发失败，则必须验证“高级网络钓鱼防护”(Advanced Phishing Protection) 功能的配置。有关详细信息，请参阅如何将邮件网关与思科高级网络钓鱼防护云服务相集成

您可以在“高级网络钓鱼防护”(Advanced Phishing Protection) 报告页面上查看以下内容：

- 在控制面板中从组织级别的所有邮件网关发送到思科高级网络钓鱼防护云服务的邮件总数。
- 尝试转发到思科高级网络钓鱼防护云服务的邮件总数，以图形格式显示。

要查看转发到思科高级网络钓鱼防护云服务的邮件元数据的详细信息，请点击链接并登录到思科高级网络钓鱼防护云服务。有关详细信息，请参阅监控思科高级网络钓鱼防护云服务上的邮件元数据。

“邮件策略详细信息报告”(Mail Policy Details Report) 页面

您可以使用“邮件策略详细信息”(Mail Policy Details) 报告页面查看：

- 排名靠前的与配置的邮件策略匹配的传入邮件（图形和表格格式）。
- 排名靠前的与已配置邮件策略匹配的传出邮件（图形和表格格式）。

在“传入策略”(Incoming Policies) 部分中，点击与特定邮件策略匹配的传入邮件总数，以查看“邮件跟踪”(Message Tracking) 中的邮件详细信息。

在“传出策略”(Outgoing Policies) 部分中，点击与特定邮件策略匹配的传入邮件总数，以查看“邮件跟踪”(Message Tracking) 中的邮件详细信息。

报告概述

在 AsyncOS 中报告包括三个基本操作：

- 可以创建计划的报告，每天、每周或每月运行一次。
- 可以立即生成报告（“按需”报告）。
- 可以查看之前运行的报告的存档版本（计划和按需）。

通过“监控”(Monitor) >“计划的报告”(Scheduled Reports) 页面可配置计划的报告和按需报告。通过“监控”(Monitor) >“存档的报告”(Archived Reports) 页面查看存档报告。

您的邮件网关将保留生成的最近报告，所有报告总计最多1000个版本。可以根据需要为报告定义任意数量的收件人，包括零个收件人。如果不指定邮件收件人，则系统仍会将报告存档。但是，如果您需要将报告发送到大量地址，则创建邮件列表比列出各个收件人更容易。

默认情况下，邮件网关会存档每个计划报告的12个最新报告。报告存储在邮件网关的/saved_reports目录中。（有关详细信息，请参阅FTP、SSH 和 SCP 访问。）

相关主题

- 计划或存档报告类型, on page 75
- 设置报告的返回地址, on page 76

计划或存档报告类型

可以选择以下报告类型：

- AMP 信誉
- 高级恶意软件防护文件分析
- 高级恶意软件防护文件追溯
- 按国家分类的连接
- 内容过滤器
- DLP 事件概要
- DMARC 验证报告
- 发送状态
- 内容摘要
- 外部威胁源
- 伪造邮件检测
- 大量邮件
- 入站 SMTP 身份验证
- 宏检测
- 邮件流摘要：传入

- 邮箱自动补救
- 邮件流详细信息（传出发件人：域）
- 邮件流摘要：传出
- 邮件过滤器
- 我的电子邮件报告
- 外发目标
- 速率限制
- 发件人域信誉
- 组
- 系统容量
- TLS 加密
- 用户邮件摘要
- URL 过滤
- 病毒爆发过滤器
- 病毒过滤
- Web 交互

每个报告都包含相应的“邮件安全监控”(Email Security Monitor) 页面的摘要。

相关主题

- 有关报告的注意事项, on page 76

有关报告的注意事项

PDF 格式的内容过滤器报告的内容过滤器数最高限制为 40 个。您可以通过 CSV 格式的报告获取完整列表。

Note 要在 Windows 计算机上生成中文、日语或韩语 PDF，还必须从 Adobe.com 下载合适的字体包并将其安装在本地计算机上。

设置报告的返回地址

要设置报告的返回地址，请参阅为邮件网关生成的邮件配置返回地址。在 CLI 中，请使用 **addressconfig** 命令。

管理报告

可以创建、编辑、删除和查看存档的计划报告。还可以立即运行报告（按需报告）。下面将讨论如何管理和查看这些报告。

Note 在集群模式下，无法查看报告。在计算机模式下，可以查看报告。

“监控”(Monitor)>“计划的报告”(Scheduled Reports) 页面显示邮件网关中已创建的计划报告列表。

相关主题

- 计划的报告, on page 77
- 存档的报告, on page 78

计划的报告

计划的报告可以安排每天、每周或每月运行。可以选择运行报告的时间。无论何时运行报告，它都只包含指定期间的数据，例如过去 3 天或上一个日历月。请注意，安排在凌晨 1 点运行的每日报告包含前一天从午夜到午夜的数据。

邮件网关提供默认的计划报告集 - 您可以使用、修改或删除其中的任何内容。

相关主题

- 将报告计划为自动生成 , on page 77
- 编辑计划的报告 , on page 78
- 删除计划的报告, on page 78

将报告计划为自动生成

Procedure

步骤 1 在“监控”(Monitor)>“计划的报告”(Scheduled Reports) 页面，点击**添加计划的报告 (Add Scheduled Report)**。

步骤 2 选择报告类型。根据所选的报告类型，可能会显示不同的选项。

有关可用的计划报告类型的详细信息，请参阅计划或存档报告类型, on page 75。

步骤 3 输入报告的描述性标题。AsyncOS 不验证报告名称的唯一性。为避免混淆，请勿创建具有相同名称的多个报告。

步骤 4 选择报告数据的时间范围。（此选项对于“病毒爆发过滤器”[Outbreak Filters] 报告不可用。）

步骤 5 选择报告的格式。

- PDF。创建格式化的 PDF 文档以用于传送和/或存档。可以通过点击“预览 PDF 报告”(Preview PDF Report) 来立即以 PDF 文件的形式查看报告。

  有关生成英语以外的其他语言的 PDF 的信息，请参阅有关报告的注意事项, on page 76。

- CSV。创建包含逗号分隔值形式表格数据的 ASCII 文本文件。每个 CSV 文件可包含多达 100 行。如果报告包含多种类型的表格，则会为每种表格创建一个单独的 CSV 文件。

步骤 6 指定报告选项（如果可用）。某些报告没有报告选项。

步骤 7 指定计划和传送选项。如果未指定邮件地址，报告将存档，但不会发送给任何收件人。

Note 如果要将报告发送到外部帐户（例如 Yahoo 或 Gmail 等），可能需要将报告返回地址添加到外部帐户的允许列表，以防止报告邮件被错误地分类为垃圾邮件。

步骤 8 点击**提交 (Submit)**。确认您的更改。

编辑计划的报告

Procedure

步骤 1 点击“服务”(Services) >“集中报告”(Centralized Reporting) 页面上的列表中的报告标题。

步骤 2 进行更改。

步骤 3 提交并确认更改。

删除计划的报告

Procedure

步骤 1 在“服务”(Services) >“集中报告”(Centralized Reporting) 页面，选中您要删除的报告所对应的复选框。

Note 选中“全部”(All) 复选框将删除所有计划的报告。

步骤 2 点击**删除 (Delete)**。

步骤 3 确认删除，然后提交更改。

任何已删除报告的存档版本都不会自动删除。

存档的报告

监控 (Monitor) > 存档报告 (Archived Reports) 页面将列出可用的存档报告。可以通过点击“报告标题”(Report Title) 列中的报告名称查看报告。通过点击**立即生成报告 (Generate Report Now)**，可以立即生成报告

使用“显示”(Show) 菜单可过滤将列出的报告类型。点击列标题可对列表进行排序。

存档的报告将自动删除 - 每个计划的报告最多可保留 30 个实例（最多 1000 个报告），随着新报告的添加，系统将删除时间最长的报告，以保持 1000 这一数字不变。30 个实例的限制适用于各个计划的报告，与报告类型无关。

相关主题

- 生成按需报告, on page 79

生成按需报告

您可以在不计划报告的情况下生产报告。这些按需报告仍然基于指定的时间范围，但是可以立即生成。

Procedure

步骤 1 点击“存档的报告”(Archived Reports) 页面中的**立即生成报告 (Generate Report Now)**。

步骤 2 选择报告类型，并在需要时编辑标题。AsyncOS 不验证报告名称的唯一性。为避免混淆，请勿创建具有相同名称的多个报告。

有关可用的计划报告类型的详细信息，请参阅计划或存档报告类型, on page 75。

步骤 3 选择报告数据的时间范围。（此选项不适用于病毒爆发报告。）

如果创建自定义范围，该范围将显示为链接。要修改范围，请点击该链接。

步骤 4 选择报告的格式。

- PDF。创建格式化的 PDF 文档以用于传送和/或存档。可以通过点击“预览 PDF 报告”(Preview PDF Report) 来立即以 PDF 文件的形式查看报告。

  有关生成英语以外的其他语言的 PDF 的信息，请参阅有关报告的注意事项, on page 76。

- CSV。创建包含逗号分隔值形式表格数据的 ASCII 文本文件。每个 CSV 文件可包含多达 100 行。如果报告包含多种类型的表格，则会为每种表格创建一个单独的 CSV 文件。指定任何报告选项。

步骤 5 选择是否对报告存档（如果是，报告将显示在“存档的报告”(Archived Reports) 页面）。

步骤 6 指定是否通过邮件发送报告以及向哪些邮件地址发送报告。

步骤 7 点击**传送此报告 (Deliver this Report)** 可生成报告，并将其传送给收件人或存档。

步骤 8 确认您的更改。

邮件报告故障排除

- 邮件跟踪链接导致出现意外结果 , on page 79
- 云端的文件分析详细信息不完整, on page 80

邮件跟踪链接导致出现意外结果

问题

从报告深入了解邮件跟踪中的详细信息，会产生意外结果。

解决方案

如果报告和邮件跟踪不同时启用、不能正常工作、不能在本地存储数据（相对于在思科安全邮件和 Web 管理器上集中存储数据），就会出现这种情况。每个功能（报告和邮件跟踪）的数据仅在该功能已启用且在邮件网关上正常工作时存储，不受另一功能（报告或邮件跟踪）是否已启用且正常工作影响。因此，报告可能包括邮件跟踪中不可用的数据，反之亦然。

云端的文件分析详细信息不完整

问题

对于从组织中其他邮件网关上传的文件，无法在公共云中获取完整的文件分析结果。

解决方案

务必将所有要共享文件分析结果数据的邮件网关分组到一起。请参阅（仅公共云文件分析服务）配置设备组。必须在该组中的每台设备上完成此配置。

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。