在思科安全邮件和 Web 管理器（M 系列）上集中管理服务

本章包含以下部分：

思科安全邮件和 Web 管理器服务概述

思科安全邮件和 Web 管理器（M 系列设备）是外部或“机下”位置，为邮件网关上的某些服务提供单一界面。

思科安全邮件和 Web 管理器包括以下功能：

- 外部垃圾邮件隔离区。为最终用户暂存垃圾邮件和可疑垃圾邮件，并允许用户和管理员在做出最终决定前审核标记为垃圾邮件的邮件。
- 集中策略、病毒和爆发隔离区。在防火墙后提供单一位置，用来存储和管理防病毒扫描、病毒爆发过滤器和策略隔离的邮件。
- 集中报告。运行关于来自多个邮件网关的汇聚数据的报告。
- 集中跟踪。跟踪经过多个邮件网关的邮件。

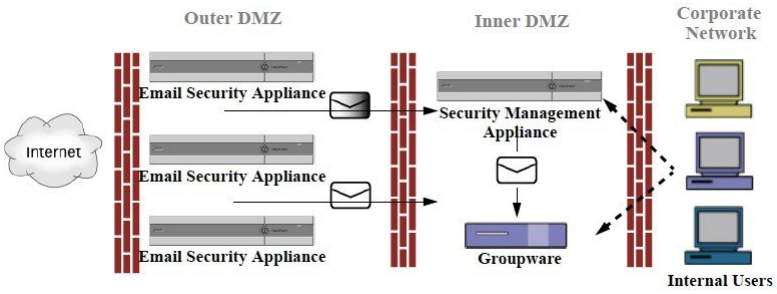
有关配置和使用思科安全邮件和 Web 管理器的完整信息，请参阅《思科安全邮件和 Web 管理器用户指南》。

网络规划

思科安全邮件和 Web 管理器可以让您将最终用户界面（例如，邮件应用）与驻留在您的各种 DMZ 上的更加安全的网关系统分隔开来。使用两层防火墙可灵活地进行网络规划，这样最终用户就不用直接连接到外部 DMZ 了。

下图显示纳入思科安全邮件和 Web 管理器和多个 DMZ 的典型网络配置。

Figure 1: 利用思科安全邮件和 ***Web*** 管理器的典型网络配置



大型企业数据中心可以分享一个思科安全邮件和 Web 管理器，将其用作一个或多个邮件网关的外部垃圾邮件隔离区。与此同时，远程办公室可以在邮件网关上维护本地垃圾邮件隔离区，以供本地使用。

使用外部垃圾邮件隔离区

邮件流和外部垃圾邮件隔离区

如果您的网络配置方式与网络规划, on page 2 中所述的方式相同，则外部 DMZ 中的设备会收到来自互联网的传入邮件。正常邮件会直接发送到内部 DMZ 中的邮件传输代理 (MTA)（组件），最终发送给企业网络内的最终用户。

垃圾邮件和可疑垃圾邮件（取决于邮件流策略设置）发送到思科安全邮件和 Web 管理器上的垃圾邮件隔离区。然后，最终用户访问该隔离区，选择删除垃圾邮件并放行其认为应传送给他们的邮件。垃圾邮件隔离区中剩余的邮件经过一段时间（可配置）后将自动删除。

从思科安全邮件和 Web 管理器的外部隔离区放行的邮件将返回到原始邮件网关以便传送。在传送前，这些邮件通常不通过以下进程：HAT 和其他策略或扫描设置、RAT、域例外、别名、传入过滤器、伪装、退回验证和工作队列。

邮件网关配置为向思科安全邮件和 Web 管理器发送邮件，将自动期望接收从思科安全邮件和 Web 管理器放行的邮件，并且在重新接收这些邮件时不重新处理。为此，不得更改思科安全邮件和 Web 管理器的 IP 地址。如果思科安全邮件和 Web 管理器的 IP 地址发生改变，接收邮件网关将像处理任何其他传入邮件一样处理该邮件。应在思科安全邮件和 Web 管理器上始终使用相同的 IP 地址进行接收和传送。

思科安全邮件和 Web 管理器接受来自在垃圾邮件隔离区设置中指定的 IP 地址的邮件以进行隔离。要在思科安全邮件和 Web 管理器上配置垃圾邮件隔离区，请参阅《思科内容安全管理设备用户指南》。

思科安全邮件和 Web 管理器放行的邮件传送到在垃圾邮件隔离区设置中定义的主要主机和辅助主机（内容安全设备或其他组件主机）（请参阅《思科安全邮件和 Web 管理器用户指南》）。因此，无论向思科安全邮件和 Web 管理器传送邮件的邮件网关的数量如何，所有放行的邮件、通知和警报都将发送到一台主机（组件或内容安全设备）。请注意，不要让负责传送来自思科安全邮件和 Web 管理器的邮件的主要主机负担过重。

从本地垃圾邮件隔离区迁移到外部隔离区

如果您当前正在邮件网关上使用本地垃圾邮件隔离区，但是想要迁移到思科安全邮件和 Web 管理器上托管的外部垃圾邮件隔离区（同时保留对本地隔离区中邮件的访问权限），则您应在过渡期间阻止新邮件进入本地隔离区。

请考虑下列可能的策略：

- 配置反垃圾邮件设置 - 在邮件策略中配置反垃圾邮件设置，将思科安全邮件和 Web 管理器指定为备用主机。此操作会将新垃圾邮件发送到外部隔离区，但仍允许访问本地隔离区。
- 设置更短的过期时间 - 将本地隔离区中的“保留天数 (之后自动删除)”(Schedule Delete After) 设置配置为更短的期限。
- 删除所有剩余的邮件 - 要删除本地隔离区中的所有剩余邮件，请禁用隔离区，然后点击本地隔离区页面中的“全部删除”(Delete All) 链接（请参阅删除垃圾邮件隔离区中的邮件）。只有还含有邮件的本地垃圾邮件隔离区被禁用，此链接才可用。

现在，您可以启用外部隔离区并禁用本地隔离区。

Note 如果本地隔离区和外部隔离区均启用，则使用本地隔离区。

启用外部垃圾邮件隔离区和外部安全列表/阻止列表

您只能在邮件网关上启用一个外部垃圾邮件隔离区。

准备工作

- 审查邮件流和外部垃圾邮件隔离区 , on page 2中的信息。
- 查看从本地垃圾邮件隔离区迁移到外部隔离区, on page 3中的信息，并基于此采取操作。
- 将思科安全邮件和 Web 管理器配置为支持集中垃圾邮件隔离区和安全列表/阻止列表功能。请参阅思科安全邮件和 Web 管理器的文档。

- 如果之前已为邮件安全设备配置了其他外部垃圾邮件隔离区，请先禁用该外部垃圾邮件隔离区设置。

在每个邮件网关上完成以下程序。

Procedure

步骤 1 依次选择**安全服务 (Security Services) > 集中服务 (Centralized Services) > 垃圾邮件隔离区 (Spam Quarantine)**。

步骤 2 点击**配置 (Configure)**。

步骤 3 选择**启用外部垃圾邮件隔离区 (Enable External Spam Quarantine)**。

步骤 4 在“名称”(Name) 字段中，输入思科安全邮件和 Web 管理器的名称

名称不是很重要，仅供参考。例如，输入思科安全邮件和 Web 管理器的主机名。

步骤 5 输入 IP 地址和端口号。

它们必须匹配“垃圾邮件隔离区设置”(Spam Quarantines Settings) 页面中在思科安全邮件和 Web 管理器上指定的 IP 地址和端口号（**管理设备 [Management Appliance] > 集中服务 [Centralized Services] > 垃圾邮件隔离区 [Spam Quarantine]**）。

步骤 6 （可选）选中该复选框以启用**外部安全列表/阻止列表 (External Safelist/Blocklist)** 功能，并指定适当的阻止列表操作。

步骤 7 提交并确认更改。

步骤 8 对每个邮件网关重复此程序。

What to do next

如果一直使用本地隔离区，请参阅禁用本地垃圾邮件隔离区以激活外部隔离区 , on page 4。

相关主题

- 本地与外部垃圾邮件隔离区
- 垃圾邮件隔离区
- 管理垃圾邮件和灰色邮件
- 如何配置邮件网关以扫描垃圾邮件

禁用本地垃圾邮件隔离区以激活外部隔离区

如果在启用外部垃圾邮件隔离区之前使用的是本地垃圾邮件隔离区，则必须禁用本地隔离区，才能将邮件发送到外部隔离区。

准备工作

执行启用外部垃圾邮件隔离区和外部安全列表/阻止列表 , on page 3中的所有指导，包括“准备工作”部分的信息。

Procedure

步骤 1 依次选择**监控 (Monitor) > 垃圾邮件隔离区 (Spam Quarantine)**。

步骤 2 在“垃圾邮件隔离区”(Spam Quarantine) 部分，点击**垃圾邮件隔离区 (Spam Quarantine)** 链接。

步骤 3 取消选择**启用垃圾邮件隔离区 (Enable Spam Quarantine)**。

忽略所有由于此更改导致的调整邮件策略警告。如果已配置外部隔离区设置，邮件策略则自动将邮件发送到外部垃圾邮件隔离区。

步骤 4 提交并确认更改。

外部垃圾邮件隔离区故障排除

问题：邮件网关不必重新处理从思科安全邮件和 Web 管理器放行的邮件。

解决方案：如果思科安全邮件和 Web 管理器的 IP 地址发生改变，则会发生这种情况。请参阅邮件流和外部垃圾邮件隔离区 , on page 2。

关于集中策略、病毒和病毒爆发隔离区

集中策略、病毒和病毒爆发隔离区

可以在思科安全邮件和 Web 管理器上集中策略、病毒和病毒爆发隔离区。邮件由邮件网关处理，但存储在思科安全邮件和 Web 管理器上的隔离区中。

集中策略、病毒和爆发隔离区提供以下优势：

- 管理员可以集中于一处来管理多个邮件网关的被隔离邮件。
- 隔离的邮件存储在防火墙后，而不是 DMZ 中，从而降低安全风险。
- 集中隔离区可使用思科安全邮件和 Web 管理器上的标准备份功能进行备份。

有关完整信息，请参阅思科安全邮件和 Web 管理器的用户指南或联机帮助。

集中策略、病毒和爆发隔离区的限制和局限性

- 在每个邮件网关上，所有策略、病毒和爆发隔离区都必须集中管理，或必须存储在本地。
- 因为在思科安全邮件和 Web 管理器中未提供扫描引擎，您无法手动测试策略、病毒或爆发隔离区中的邮件是否含有病毒。

在集群配置中集中策略、病毒和病毒爆发隔离区的要求

可以在集群设备的任何级别启用集中策略、病毒和爆发隔离区。

要求：

- 在特定级别（计算机、组或集群）在邮件网关上启用集中策略、病毒和爆发隔离区之前，属于同一级别的所有设备都必须先添加到思科安全邮件和 Web 管理器。
- 内容和邮件过滤器及 DLP 邮件操作必须在同一级别配置，且它们在低于该级别的任何级别不会被覆盖。
- 集中策略、病毒和爆发隔离区设置必须在同一级别配置，且它们在低于所配置级别的任何级别不会被覆盖。
- 确保要用于与思科安全邮件和 Web 管理器进行通信的接口在组或集群中的所有设备上拥有相同的名称。

例如：

如果要在集群或组级别启用集中策略、病毒和爆发隔离区，但连接到集群的邮件网关的这些设置是在计算机级别定义的，则您必须删除在计算机级别配置的集中隔离区设置，才能在集群或组级别启用此功能。

关于策略、病毒和爆发隔离区的迁移

当您集中策略、病毒和爆发隔离区时，邮件网关上的现有策略、病毒和爆发隔离区将迁移到思科安全邮件和 Web 管理器。

您将在思科安全邮件和 Web 管理器上配置迁移，但是当您确认更改，在邮件网关上启用集中策略、病毒和爆发隔离区时，会发生迁移。

在确认更改时，将会出现以下情况：

- 禁用邮件网关上的本地策略、病毒和爆发隔离区。所有进入这些隔离区的新邮件都将在思科安全邮件和 Web 管理器上隔离起来。
- 从现有非垃圾邮件隔离区向思科安全邮件和 Web 管理器的迁移开始。
- 删除所有本地策略、病毒和爆发隔离区。如果您配置的是自定义迁移，则选择不迁移的任何本地策略隔离区也会被删除。有关删除策略隔离区的影响，请参阅关于删除策略隔离区。
- 迁移前位于多个隔离区中的邮件，在迁移后将位于对应的集中隔离区。
- 迁移在后台进行。所需的时间取决于隔离区大小和网络。当您在邮件网关上启用集中隔离区时，您可以输入一个或多个邮件地址，以便在迁移完成时接收通知。
- 这些邮件将应用集中隔离区中的设置，而不是始发本地隔离区的设置。但是，每封邮件仍沿用初始到期时间。

Note 迁移期间自动创建的所有集中隔离区均采用默认隔离区设置。

集中策略、病毒和病毒爆发隔离区

Before you begin

Note 请在维护窗口或非高峰时段执行此过程。

- 您必须先为集中策略、病毒和爆发隔离区配置思科安全邮件和 Web 管理器。请参阅思科安全邮件和 Web 管理器联机帮助或用户指南中“集中策略、病毒和爆发隔离区”一章的“集中策略、病毒和爆发隔离区”部分的表格。
- 如果思科安全邮件和 Web 管理器上分配给集中隔离区的空间比现有本地隔离区占用的总空间小，邮件将根据思科安全邮件和 Web 管理器上的隔离区设置提前到期。在迁移之前，请考虑手动执行操作以减小隔离区空间。有关提前到期的详细信息，请参阅自动处理的隔离邮件的默认操作。
- 如果您已选择自动迁移，或者将自定义迁移配置为在迁移过程中创建集中隔离区，请注意邮件网关上的当前隔离区设置，以便将这些设置用作集中隔离区配置准则。
- 如果在集群配置中部署了邮件网关，请参阅在集群配置中集中策略、病毒和病毒爆发隔离区的要求 , on page 6。
- 注意在此程序中确认更改时将发生的变化。请参阅关于策略、病毒和爆发隔离区的迁移 , on page 6。

Procedure

步骤 1 依次选择**安全服务 (Security Services) > 集中服务 (Centralized Services) > 策略、病毒和爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**。

步骤 2 点击**启用 (Enable)**。

步骤 3 输入要用于与思科安全邮件和 Web 管理器通信的接口和端口。

确保可从思科安全邮件和 Web 管理器访问接口和端口。

如果邮件网关加入集群，则选择的接口必须在集群中的所有计算机上都可用。

步骤 4 要在迁移完成时收到通知，请输入一个或多个邮件地址。

步骤 5 验证要迁移的隔离区的相关信息，确保这是您所需的内容。

步骤 6 如果要执行自定义迁移，请注意在确认此过程中的更改时将删除任何隔离区。

步骤 7 确认有关内容和邮件过滤器及 DLP 邮件操作的信息将按预期方式更新。

Note 对于集群配置，只有在特定级别已定义过滤器和邮件操作，且它们在低于该级别的任何级别上不会被覆盖，系统才会在该级别自动更新过滤器和邮件操作。迁移后，可能需要使用集中隔离区名称手动重新配置过滤器和邮件操作。

步骤 8 如果需要重新配置迁移映射，请执行以下操作：

a) 返回思科安全邮件和 Web 管理器。

b) 重新配置迁移映射。

在思科安全邮件和 Web 管理器上，选择要重新映射的隔离区，然后点击**从集中隔离区中删除 (Remove from Centralized Quarantine)**。然后，可以重新映射隔离区。

c) 在思科安全邮件和 Web 管理器上提交新迁移配置。

d) 从开始执行此程序。

重要提示！请务必重新依次加载**安全服务 (Security Services) > 集中服务 (Centralized Services) > 策略、病毒和爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**。

步骤 9 点击**提交 (Submit)**。

步骤 10 如果需要重新配置迁移映射，请按照步骤 8 中的过程执行操作。

步骤 11 确认您的更改。

Note 在迁移进行时，避免在邮件网关或思科安全邮件和 Web 管理器上进行配置更改。

步骤 12 查看页面顶部可监控迁移状态；如果在配置迁移时输入了邮件地址，请等待邮件通知您迁移完成。

What to do next

执行思科安全邮件和 Web 管理器联机帮助或用户指南中“集中策略、病毒和爆发隔离区”主题的表格中所述的剩余任务。

相关主题

- 可访问策略、病毒和爆发隔离区的用户组

关于禁用集中策略、病毒和爆发隔离区

当您在邮件网关上禁用集中策略、病毒和爆发隔离区时：

- 邮件网关上的本地隔离区会自动启用。
- 系统创建的隔离区以及邮件过滤器、内容过滤器和 DLP 邮件操作所引用的隔离区会在邮件网关上自动创建。病毒、爆发和未分类隔离区使用集中隔离区之前使用的设置创建，包括分配的用户角色。所有其他隔离区均采用默认设置创建。
- 新隔离的邮件将立即转到本地隔离区。
- 禁用集中隔离区时其中包含的邮件将保留在原处，直到出现以下情况之一：
  - 手动删除邮件或邮件到期自动删除。
  - 手动放行邮件，或自动放行邮件，前提是同时满足下列条件之一：

* 在思科安全邮件和 Web 管理器上配置了备用放行设备。请参阅思科安全邮件和 Web 管理器的联机帮助或文档。

* 集中隔离区在邮件网关上再次启用。

禁用集中策略、病毒和爆发隔离区

Before you begin

- 了解禁用集中策略、病毒和爆发隔离区的影响。
- 执行以下操作之一：
  - 处理集中策略、病毒和爆发隔离区中当前的所有邮件。
  - 确保已指定备用放行设备，用来在禁用集中隔离区后处理从集中隔离区放行的邮件。有关信息，请参阅思科安全邮件和 Web 管理器的联机帮助或用户指南。

Procedure

步骤 1 在邮件网关上，依次选择**安全服务 (Security Services) > 集中服务 (Centralized Services) > 策略、病毒和爆发隔离区 (Policy, Virus, and Outbreak Quarantines)**。

步骤 2 禁用集中策略、病毒和爆发隔离区。

步骤 3 提交并确认更改。

步骤 4 自定义新创建的本地隔离区的设置。

集中策略、病毒和病毒爆发隔离区故障排除

如果思科安全邮件和 Web 管理器停止工作

如果在停止工作的思科安全邮件和 Web 管理器上集中策略、病毒和爆发隔离区，应在邮件网关上禁用这些集中隔离区。

如果部署替代思科安全邮件和 Web 管理器，则必须在思科安全邮件和 Web 管理器和每个邮件网关上重新配置隔离区迁移。请参阅思科安全邮件和 Web 管理器联机帮助或用户指南中“集中策略、病毒和爆发隔离区”一章的“集中策略、病毒和爆发隔离区”部分的表格。

配置集中报告

Before you begin

- 在思科安全邮件和 Web 管理器上启用和配置集中报告。请参阅《思科安全邮件和 Web 管理器用户指南》中的前提条件和说明。
- 确保在思科安全邮件和 Web 管理器上为报告服务分配了充足的磁盘空间。

Procedure

步骤 1 依次点击**安全服务 (Security Services) > 报告 (Reporting)**。

步骤 2 在“报告服务”(Reporting Service) 部分，选择“集中报告”(Centralized Reporting) 选项。

步骤 3 提交并确认更改。

高级恶意软件保护报告的要求

有关思科安全邮件和 Web 管理器上高级恶意软件防护（文件信誉和文件分析）功能的完整报告的所需配置，请参阅您的思科安全邮件和 Web 管理器版本的联机帮助或用户指南的邮件报告章节中有关高级恶意软件防护报告的信息。

更改集中报告后报告信息的可用性

在邮件网关上启用集中报告时：

- 邮件网关上用于每月报告的现有数据不会传输到思科安全邮件和 Web 管理器。
- 邮件网关上的存档报告不可用。
- 邮件网关仅存储一周的数据。
- 每月和每年报告的新数据存储在思科安全邮件和 Web 管理器上。
- 邮件网关上的排定报告暂停。
- 您再也无法在邮件网关上访问排定报告配置页面。

关于禁用集中报告

如果在邮件网关上禁用集中报告，则邮件网关会开始存储新的每月报告数据，计划报告恢复，并且您可以访问它的存档报告。禁用集中报告后，设备仅显示过去一小时和一天的数据，但不是过去一周或一个月。这种情况是暂时的。在累积足够的数据后，设备将显示过去一周和一个月的报告。如果邮件网关重新回到集中报告模式，它将在交互式报告中显示上一周的数据。

配置集中邮件跟踪

Before you begin

Note 您不能在邮件网关上启用集中和本地跟踪。

Procedure

步骤 1 依次点击**安全服务 (Security Services) > 邮件跟踪 (Message Tracking)**。

步骤 2 在“邮件跟踪服务”(Message Tracking Service) 部分，点击**编辑设置 (Edit Settings)**。

步骤 3 选中**启用邮件跟踪服务 (Enable Message Tracking Service)** 复选框。

步骤 4 选择“集中跟踪”(Centralized Tracking) 选项。

步骤 5 （可选）选中该复选框可保存被拒绝连接的信息。

Note 保存被拒绝连接的跟踪信息，会对思科安全邮件和 Web 管理器的性能造成负面影响。

步骤 6 提交并确认更改。

后续操作

要使用集中跟踪，您必须在邮件网关和思科安全邮件和 Web 管理器上启用该功能。要在思科安全邮件和 Web 管理器上启用集中跟踪，请参阅《思科安全邮件和 Web 管理器用户指南》。

使用集中服务

有关使用集中服务的说明，请参阅《思科安全邮件和 Web 管理器用户指南》。

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。