Cisco Secure Email Gateway使用入门

本章包含以下部分：

AsyncOS 15.5.1 中的新增功能

表 *1: AsyncOS 15.5.1* 中的新增功能

特性	说明
识别违反邮件结尾 RFC 标准的邮件	您的邮件网关现在可以识别和过滤违反邮件结尾 RFC 标准的邮件（即，<CRLF.CRLF> ）以检测威胁。 当邮件网关收到包含无效邮件结尾序列的邮件时，它会向该连接内的所有邮件 ID (MID) 添加 **X-Ironport-Invalid-End-Of-Message** 扩展信头 (X-Header)，直到收到符合消息结尾 RFC 标准的 。 您可以在内容过滤器中配置策略，以便对这些邮件执行必要的操作。 有关配置 CR 和 LF 处理字段的详细信息，请参阅 通过使用 Web 界面创建侦听程序侦听连接请求。

特性	说明
监控 Vault Service 和发送警报	现在，您的邮件网关会监控 Vault 服务并跟踪其状态（无论其是否已初始化）。它还会发送相应的警报消息并将状态信息记录到 error_logs 中。 您可以使用以下方式之一访问警报日志： • 导航至 Web 界面上的 **系统管理** > **警报** 页面，然后点击 **查看排名靠前的警报** 按钮。 • 在 CLI 中使用 `displayalerts` 命令。 如果 Vault Service 由于任何问题而无法初始化，您会收到警报消息（在邮件中、Web 界面上和 CLI 中），指示 Vault Service 已关闭，并且您必须执行 Vault 恢复过程以恢复 Vault Service。 **注释** 如果在升级到 AsyncOS 15.5.1 时升级失败，则应在 upgrade_logs 中检查 Vault Service 错误。如果识别出 Vault Service 错误，则必须恢复 Vault Service 或继续升级过程，而不保存配置。 在以下情况下，您将收到警报消息： • 如果在升级到 AsyncOS 15.5.1 后 Vault Service 无法初始化，您将通过邮件、Web 界面和 CLI 收到警报消息。 • 如果您的邮件网关的任何服务使用无法初始化的 Vault 服务，您将通过邮件、Web 界面和 CLI 收到警报消息。发送的警报消息取决于加密状态。可以使用 `fipsconfig` > `encryptconfig` 子命令检查加密状态。 保管库监控机制每 75 分钟检查一次 Vault 服务。如果 Vault 服务关闭，则会发送警报消息，直到 Vault 服务恢复为止。 有关成功的保管库运行状况检查和初始化日志条目示例的信息，请参阅 保管库运行状况检查和初始化成功。 要恢复 Vault Service，您必须执行 Vault 恢复过程。 **注释** 如果启用了加密 (CLI > `fipsconfig` > `encryptconfig`)，请确保始终保存并保留邮件网关配置的副本，以避免数据丢失。 有关如何保存邮件网关配置的详细信息，请参阅版本说明中的保存邮件网关的配置部分。 有关如何执行 Vault 恢复过程的信息，请参阅版本说明中的“执行 Vault 恢复过程以解决 Vault 问题”部分。

特性	说明
通过 CLI 重启 API 服务器	现在，您可以使用新的CLI子命令`API_SERVER`重新启动API服务器。您可以使用`API_SERVER`子命令重新启动并查看API服务器的状态。 `API_SERVER` 子命令添加到 `diagnostic` > `Services` 子命令下。 有关`diagnostic`命令及其子命令的详细信息，请参见《CLI参考指南》的“命令参考样例”章节中的“diagnostic”章节。
配置威胁扫描程序进行威胁检测	在 AsyncOS 15.0 版本中，引入了威胁扫描程序功能来检测传入邮件中的威胁。在此版本中，您无法直接配置威胁扫描程序来检测威胁，它已在后端进行了配置。 从此版本开始，您可以配置威胁扫描程序来检测邮件网关上的传入威胁。您可以为每个传入邮件策略启用或禁用威胁扫描程序。启用威胁扫描程序时，它会扫描传入邮件并影响反垃圾邮件判定。 **前提条件：**您必须启用**灰色邮件全局设置 (Graymail Global Settings)** 才能启用威胁扫描程序。 您可以通过以下方式按策略来配置威胁扫描程序： • **Web 界面：**导航至**邮件策略 (Mail Policies)** > **传入邮件策略 (Incoming Mail Policies)**，然后点击邮件策略的**反垃圾邮件 (Anti-Spam)** 列下的链接，以便打开**邮件策略：反垃圾邮件 (Mail Policies: Anti-Spam)** 页面。您可以选中或取消选中**启用威胁扫描程序 (Enable Threat Scanner)** 复选框。 • **CLI：**使用 `policyconfig` 命令。 **安装和升级情景** 在安装邮件网关或从 AsyncOS 15.0 或更早版本升级到 AsyncOS 15.5.1 版本时，默认情况下将禁用威胁扫描程序。 有关详细信息，请参阅定义反垃圾邮件策略。

特性	说明
强制要求本地用户使用思科智能软件许可	从此版本（AsyncOS 15.0 之后的所有版本）开始，Cisco Secure Email Gateway**必须**使用思科智能软件许可。 **注释** 从 AsyncOS 15.5.1 开始，将**不再支持本地用户**的经典许可。您将无法再在经典许可模式下订购新功能许可证或续订现有功能许可证。 **前提条件**：确保在思科智能软件管理器门户中创建智能账户，并在邮件网关上启用思科智能软件许可。有关详细信息，请参阅 智能软件许可。 在启用思科智能软件许可后，您可以将邮件网关升级到此版本，并在智能许可模式下继续使用现有功能许可证。
包括其他属性以提高 SDR 服务的效力	现在，您的邮件网关默认将**其他属性 (Additional Attributes)**（显示名称和完整邮件地址 - 用户名和域）作为遥测数据的一部分发送到思科 TAC 进行信誉分析，以提高发件人域信誉 (SDR) 服务的效率。 当管理员登录到邮件网关时，您将收到一条警告消息，通知您在 SDR 中**包括其他属性 (Include Additional Attributes)** 选项已默认启用，以便遥测数据包括个人数据的处理。 **注释** 仅当启用发件人域信誉过滤时，才会默认启用**包括其他属性 (Include Additional Attributes)** 选项。 如果要禁用**包括其他属性 (Include Additional Attributes)** 选项： 1. 导航到**安全服务 (Security Services)** > **域信誉 (Domain Reputation)**。 2. 点击**编辑全局设置 (Edit Global Settings)** 并取消选中**包括其他属性 (Include Additional Attributes)** 复选框。 有关详细信息，请参阅在邮件网关上启用发件人域信誉过滤。

特性	说明
支持用于 DKIM 验证的大密钥大小值	您可以在邮件网关中使用以下大密钥大小值进行 DKIM 验证： • 3072 密钥位大小 • 4096 密钥位大小 您可以通过以下方式为DKIM验证选择新的大密钥大小值： • **Web 界面**：转到“邮件策略”(Mail Policies)>“验证配置文件”(Verification Profiles)>“添加配置文件或默认值”(Add Profile or Default)，然后从“接受的最小密钥：”(Smallest Key to be Accepted:) 或“接受的最大密钥：”(Largest Key to be Accepted:) 下拉列表字段中选择 3072 或 4096。 • **CLI**：使用 `domainkeysconfig > keys > new` 或编辑 `(edit) > 输入可接受的最小密钥 (Enter the smallest key to be accepted)` 或输入可接受的最大密钥 `(Enter the largest key to be accepted)` 选项并输入与特定 DKIM 验证配置文件的 3072 或 4096 对应的所需值。
新 DKIM 验证配置文件不支持 512 和 768 密钥大小值	从此版本开始，在创建新的 DKIM 验证配置文件时，不再支持 512 和 768 密钥位大小值。 **注释** 升级到此版本后，仍支持使用 512 和 768 密钥大小值来创建的现有 DKIM 验证配置文件
TLS 1.3 对 SSL 服务的支持	现在，您可以在邮件网关中为以下 TLS 服务配置 TLS 1.3： • GUI HTTPS • 入站 SMTP • 出站 SMTP 仅当为“GUI HTTPS”、“入站 SMTP”和“出站 SMTP”TLS 服务配置 TLS 1.3 时，邮件网关才支持以下 TLS 密码： • `TLS_AES_128_GCM_SHA256` • `TLS_AES_256_GCM_SHA384` • `TLS_CHACHA20_POLY1305_SHA256` **注释** 邮件网关不允许修改用于 TLS 1.3 的密码。 在配置 TLS 1.3 后，您可以在邮件网关的旧版或新版 Web 界面与 API 服务之间使用 TLS 进行通信。

特性	说明
使用 AsyncOS API 获取文件散列列表、RAT 和 SMTP 路由，保存和加载配置、地址列表和传入邮件策略用户信息	现在，您可以使用 AsyncOS API 在邮件网关中获取有关文件散列列表、收件人访问表 (RAT) 条目、SMTP 路由、保存和加载配置、地址列表和传入邮件策略用户的信息。 有关更多信息，请参阅《适用于思科安全电子邮件网关的 *AsyncOS 15.5.1 API* - 入门指南》的“配置 API”部分。
在发件人或收件人级别对传出邮件实施 TLS	现有的“目标控制”(Destination Controls) 配置允许您按域覆盖 TLS 模式（例如 TLS 强制、TLS 首选等）。 如果需要根据其他条件（例如发件人、收件人等）对传出邮件实施 TLS，您现在可以使用 `X-ESA-CF-TLS-Mandatory` 信头。 您可以配置“内容过滤器 - 添加/编辑信头”(Content Filter – Add/Edit Header) 操作，以根据任何内容过滤器条件在“信头名称：”(Header Name:) 字段中添加 `X-ESA-CF-TLS-Mandatory` 信头，并将内容过滤器附加到传出邮件策略。
在不同集群的计算机之间同步配置更改	您可以将对一个集群中已登录计算机所做的配置更改同步到远程集群中的所有计算机。仅当两个集群位于同一区域的相同或不同数据中心时，才会发生同步过程。 **注释** 只能在集群级别同步计算机之间的配置更改，而不能在组或计算机级别同步。 **注释** 您必须将计算机移动到组级别，以避免通过集群间同步 SPAM 隔离区 IP 配置。 要启用此功能，请联系您的思科客户经理。 **前提条件：**在请求思科客户经理启用此功能之前，请确保集群中所有计算机的配置相同。 同步过程完成后，如果您在一台计算机上进行了配置更改，相同的配置会自动复制到集群中的所有计算机。您可以在系统日志中查看相同的配置。有关详细信息，请参阅日志记录。 **注释** 集群间连接过程完成后，不得再修改集群名称。确保集群具有唯一的名称。

特性	说明
为单个传入邮件策略配置威胁防御连接器。	现在，您可以为每个传入邮件策略配置威胁防御连接器，并为每个邮件策略使用单独的邮件接收地址。 要使用此功能，您必须在安全邮件网关中配置并启用威胁防御连接器。 转到**邮件策略 (Mail Policies)** > **传入邮件策略 (Incoming Mail Policies)** 以便为单个邮件策略启用或禁用威胁防御连接器。 有关详细信息，请参阅将 Cisco Secure Email Gateway 与威胁防御集成。
扫描邮件中受密码保护的附件	您可以在邮件网关中配置内容扫描程序，以便扫描传入或传出邮件中受密码保护的附件的内容。 在邮件网关中扫描受密码保护的邮件附件将有助于组织： • 检测使用恶意软件作为邮件附件的网络钓鱼活动，并通过密码保护来锁定受限的网络攻击。 • 分析包含针对恶意活动和数据隐私而受密码保护的附件的邮件。 此功能支持以下语言 - 英语、意大利语、葡萄牙语、西班牙语、德语、法语、日语和韩文。 有关详细信息，请参阅使用邮件过滤器实施邮件策略。
用于 URL 追溯服务的基于区域的轮询	您可以配置安全邮件网关连接的 URL 追溯服务区域，以进行判定更新。安全邮件网关 ESA 可以更新追溯服务区域和关联的终端 URL。 有关详细信息，请参阅 设置 URL 过滤。
文件分析服务器区域增强	从此版本开始，文件分析服务器区域支持两个新区域 - 澳大利亚和加拿大。 您可以按照以下方式来配置文件分析服务器区域： • **Web 界面**：导航至**安全服务 (Security Services)** > **文件信誉和分析 (File Reputation and Analysis)**，然后点击**编辑全局设置 (Edit Global Settings)**。 • **CLI**：使用 `ampconfig` > `ADVANCED` 命令。 有关详细信息，请参阅 启用和配置文件信誉和分析服务。

Web 界面比较（新 Web 界面与旧 Web 界面）

下表显示了新 Web 界面与旧版界面的比较：

表 *2:* 新 *Web* 界面与旧版界面的比较

Web 界面页面或元素	新 Web 界面	旧 Web 界面
登录页面	登录到邮件网关后，系统将显示“邮件流摘要”(Mail Flow Summary) 页面。	登录到邮件网关后，系统将显示“我的控制板”(My Dashboard) 页面。
“报告”下拉列表	您可以从“报告”(Reports) 下拉列表中查看邮件网关的报告。	您可以从**监控 (Monitor)** 菜单查看邮件网关的报告。
“我的报告” (My Reports) 页面	从“报告”(Reports) 下拉列表中选择**我的报告 (My Reports)**。	您可以从**监控 (Monitor) > 我的控制面板 (My Dashboard)** 查看“我的报告”(My Reports) 页面。
“邮件流摘要”(Mail Flow Summary) 页面	**邮件流摘要**页面包括传入邮件和传出邮件的趋势图和摘要表。	**传入邮件**包括传入和传出邮件的图和摘要表。
“高级恶意软件保护”报告页面	以下各部分在“报告”菜单的**高级恶意软件保护**报告页面上可用： • 摘要 • AMP 文件信誉 • 文件分析 • 文件追溯 • 邮箱自动补救	邮件网关的**监控 (Monitor)** 菜单下具有以下**高级恶意软件保护 (Advanced Malware Protection)** 报告页面： • 高级恶意软件防护 • AMP 文件分析 • AMP 判定更新 • 邮箱自动补救
“爆发过滤器”(Outbreak Filters) 页面	“过去一年病毒爆发”和“过去一年病毒爆发摘要”在新 Web 界面的**爆发过滤 (Outbreak Filtering)** 报告页面中不可用。	**监控 (Monitor) > 病毒爆发过滤器 (Outbreak Filters)** 页面显示“过去一年病毒爆发”(Past Year Virus Outbreaks) 和“过去一年病毒爆发摘要”(Past Year Virus Outbreak Summary)。

Web 界面页面或元素	新 Web 界面	旧 Web 界面
垃圾邮件隔离区（管理和最终用户）	在新 Web 界面中点击**隔离区 (Quarantine) > 垃圾邮件隔离区 (Spam Quarantine) > 搜索 (Search)**。 最终用户可以使用以下 URL 访问垃圾邮件隔离区： https://example.com:<https-api-port>/euq-login 其中， example.com 是设备主机名， <https-api-port> 是防火墙上打开的 AsyncOS API HTTPS 端口。	您可以从**监控 (Monitor) > 垃圾邮件隔离区 (Spam Quarantine)** 菜单查看垃圾邮件隔离区。
策略、病毒和爆发隔离区	在新 Web 界面中点击**隔离区 (Quarantine) > 其他隔离区 (Other Quarantine)**。 在新 Web 界面中，您只能查看“策略”、“病毒”和“病毒爆发隔离区”。	在邮件网关上，您可以使用**监控 (Monitor) > 策略、病毒和病毒爆发隔离区 (Policy, Virus and Outbreak Quarantines)** 来查看、配置和修改策略、病毒和病毒爆发隔离区。
为隔离区中的邮件选择所有操作	您可以选择多个（或所有）邮件并执行邮件操作，例如删除、延迟、发布、移动等。	您不能选择多个邮件来执行邮件操作。
附件的最大下载限制	已隔离邮件的附件下载最大限制为 25 MB。	-
受拒连接数	要搜索已拒绝连接，请点击上的**跟踪 (Tracking) > 搜索 (Search) > 已拒绝连接 (Rejected Connection)** 选项卡。	-
查询设置	邮件跟踪功能的查询设置字段在上不可用。	您可以在“邮件跟踪”功能的“查询设置”字段中设置查询超时。
邮件跟踪数据可用性	点击 Web 界面页面右上方的齿轮图标，以访问“邮件跟踪数据可用性”(Message Tracking Data Availability) 页面。	您可以查看邮件网关缺少数据的时间间隔。
显示邮件的更多详细信息	您可以查看邮件的更多详细信息，例如判定图表、上次状态、发件人组、发件人 IP、IP 信誉得分和策略匹配详细信息。	-

Web 界面页面或元素	新 Web 界面	旧 Web 界面
判定图表和上次状态判定	判定图表显示由邮件网关中的每个引擎触发的各种可能判定的信息。 邮件的“上次状态”决定了在引擎的所有可能判定之后触发的最终判定。	邮件的判定图表和上次状态判定不可用。
邮件详细信息中的邮件附件和主机名	在邮件网关上邮件的“邮件详细信息”部分，不显示邮件附件和主机名。	邮件附件和主机名显示在邮件的“邮件详细信息”部分。
邮件详细信息中的发件人组、发件人 IP、IP 信誉得分和策略匹配	邮件的发件人组、发件人 IP、IP 信誉得分和策略匹配的详细信息显示在邮件网关的“邮件详细信息”(Message Details) 部分中。	邮件的发件人组、发件人 IP、IP 信誉得分和策略匹配在邮件的“邮件详细信息”部分不可用。
邮件方向（传入或传出）	邮件网关的邮件跟踪结果页面显示邮件方向（传入或传出）。	“邮件跟踪结果”(Message Tracking Results) 页面不显示邮件方向（传入或传出）。

哪里可以获得详细信息

思科提供以下资源用于了解有关邮件网关的更多信息：

- 文档 , on page 10
- 培训, on page 11
- 思科通知服务 , on page 11
- 知识库, on page 12
- 思科支持社区, on page 12
- 思科客户支持, on page 12
- 第三方贡献者, on page 12
- 思科欢迎您发表意见, on page 13
- 注册思科账户 , on page 13

文档

可通过点击右上角的“帮助和支持”(Help and Support)，直接从设备 GUI 访问联机帮助版本的用户手册。

Cisco Secure Email Gateway的文档集包括以下文档和手册：

- 版本说明
- 思科邮件安全设备模型快速入门指南

- 所用型号或系列的硬件安装或硬件安装与维护指南
- 思科内容安全虚拟设备安装指南
- 适用于*Cisco Secure Email Gateway*思科邮件安全设备的 *AsyncOS* 用户指南（本手册）
- 《适用于*Cisco Secure Email Gateway*的 *AsyncOS CLI* 参考指南》
- 《使用Cisco Secure Email Gateway的 AsyncOS API - 入门指南》

所有思科内容安全产品的文档均可从以下位置获取：

思科内容安全产品的文档	位置
硬件和虚拟设备	请参阅此表中适用的产品。
Cisco Secure Email Gateway	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd- products-support-series-home.html
Cisco Secure Web Appliance	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products- support-series-home.html
思科安全邮件和 Web 管理器	http://www.cisco.com/c/en/us/support/security/content-security-management- appliance/tsd-products-support-series-home.html
思科安全邮件网关 CLI 参考指南	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
思科安全邮件网关 API 使用入门指南	https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-programming-reference-guides-list.html

培训

有关培训的详细信息可从以下网址获得：

- http://www.cisco.com/c/en/us/training-events/training-certifications/supplemental-training/email-and-web-security.html
- http://www.cisco.com/c/en/us/training-events/training-certifications/overview.html

思科通知服务

注册以接收与思科内容安全设备相关的通知，如安全建议、现场通知、销售终止或支持终止声明，以及有关软件更新和已知问题的信息。

您可以指定通知接收频率和要接收的信息类型等选项。您必须为您所用的每种产品单独注册。

要进行注册，请访问 http://www.cisco.com/cisco/support/notifications.html

需要 Cisco.com 账户才能注册。如果没有，请参阅注册思科账户 , on page 13。

知识库

Procedure

步骤 1 转到主产品页面 (http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html)

步骤 2 查找名称中包含 **TechNotes** 的链接。

思科支持社区

思科支持社区是一个面向思科客户、合作伙伴和员工的在线论坛。它提供了一个讨论常规邮件和网络安全问题以及有关具体思科产品的技术信息的场合。您可以在论坛中发布主题，以咨询问题并与其他用户分享信息。

请通过以下 URL 访问客户支持门户上的思科支持社区：

- 针对邮件安全和相关管理：

  https://supportforums.cisco.com/community/5756/email-security

- 针对网络安全和相关管理：

  https://supportforums.cisco.com/community/5786/web-security

思科客户支持

如需获取有关Cisco Secure Email Gateway 的帮助，请勿联系思科客户支持人员。有关获取云/混合邮件安全设备支持的信息，请参阅《思科 IronPort 托管邮件安全/混合托管邮件安全概述指南》。

Cisco TAC：http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

旧版 IronPort 的支持站点：http://www.cisco.com/c/en/us/services/acquisitions/ironport.html

对于普通问题，您还可以从邮件网关上访问客户支持。有关说明，请参阅用户指南或在线帮助。

第三方贡献者

有关与您的版本对应的开源代码授权信息，请访问以下页面：
http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-release-notes-list.html。

Cisco AsyncOS 的某些软件根据 FreeBSD, Inc.、Stichting Mathematisch Centrum、Corporation for National Research Initiatives, Inc. 及其他第三方贡献者的软件许可协议条款、通知和条件分发，所有此类条款和条件均包含在思科许可协议当中。

这些协议的全文可通过以下网站查看：

https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html。

经 Tobi Oetiker 明确书面同意，Cisco AsyncOS 的部分软件基于 RRDtool。

本文档中部分相关内容的复制已取得 Dell Computer Corporation 的许可。本文档中部分相关内容的复制已取得 McAfee, Inc. 的许可。本文档中部分相关内容的复制已取得 Sophos Plc 的许可。

思科欢迎您发表意见

思科技术出版物团队乐于将努力提高产品文档的质量。我们时刻欢迎您的评论和建议。您可以将评论发送至以下邮件地址：

contentsecuritydocs@cisco.com

请在邮件主题中提供产品名称、版本号和文档发布日期。

注册思科账户

要访问 Cisco.com 上的许多资源，都需要有思科账户。

如果您没有 Cisco.com 用户 ID，可以在此注册一个账户： https://idreg.cloudapps.cisco.com/idreg/register.do

相关主题

- 思科通知服务 , on page 11
- 知识库, on page 12

Cisco Secure Email Gateway概述

AsyncOS™ 操作系统包括以下功能：

- 网关处的**反垃圾邮件**，通过 SenderBase 信誉过滤器和思科反垃圾邮件集成的独特多层方法。
- 网关处的**防病毒**，使用 Sophos 和 McAfee 防病毒扫描引擎。
- **病毒爆发过滤器™**，思科针对新病毒、诈骗和网络钓鱼爆发提供的独特预防保护，可以隔离危险邮件，直到应用新的更新，从而缩短新邮件威胁的漏洞窗口。
- **策略、病毒和病毒爆发隔离区**提供一个安全的位置来存储可疑邮件供管理员评估。
- 内部或外部的**垃圾邮件隔离区**，使最终用户可以访问隔离的垃圾邮件和疑似垃圾邮件。
- **邮件身份验证**。Cisco AsyncOS 支持各种不同形式的邮件身份验证，包括传入邮件的发件人策略框架 (SPF)、发件人 ID 框架 (SIDF) 和 DomainKeys 确定的邮件 (DKIM) 验证，以及传出邮件的 DomainKeys 和 DKIM 签名。
- 思科**邮件加密**。可以加密传出邮件以满足 HIPAA、GLBA 或类似的管理需求。为此，需要在邮件网关上配置加密策略并使用本地密钥服务器或托管密钥服务来加密邮件。
- **邮件安全管理器**，一个综合控制面板，用于管理邮件网关中的所有邮件安全服务和应用。邮件安全管理器可以基于用户组实施邮件安全，以便通过不同的入站和出站策略管理思科信誉过滤器、病毒爆发过滤器、反垃圾邮件、防病毒和邮件内容策略。
- **机上邮件跟踪**。AsyncOS for Email 包含机上邮件跟踪功能，可帮助轻松获取邮件网关所处理邮件的状态。

- 针对所有入站和出站邮件的**邮件流监控**，用于全面了解企业的所有邮件流量。
- 基于发件人的 IP 地址、IP 地址范围或域，针对入站发件人的**访问控制**。
- 广泛的**邮件和内容过滤**技术，用于实施公司策略并在特定邮件进入或离开公司基础设施时执行相应操作。过滤器规则根据邮件或附件内容、有关网络的信息、邮件信封、邮件信头或邮件正文识别邮件。过滤器操作允许删除、退回、存档、密件复制或更改邮件，或者生成通知。
- **通过传输层安全使用安全 SMTP 进行邮件加密**可确保加密在公司基础设施与其他可信主机之间传输的邮件。
- **Virtual Gateway**™ 技术允许邮件网关在单个服务器中用作多个邮件网关，以便划分不同来源或活动中的邮件以通过单独的 IP 地址发送。这样可以确保影响一个 IP 地址的可传送性问题不会影响其他 IP 地址。
- **防止恶意附件和链接**（在邮件中），由多个服务提供。
- 使用**防数据丢失**控制和监控从组织传出的信息。

AsyncOS 支持符合 RFC 2821 标准的简单邮件传输协议 (SMTP)，以接受并传输邮件。

大多数报告、监控和配置命令都可通过基于 Web 的 GUI 和 HTTP 或 HTTPS 使用。此外，还为系统提供了从 Secure Shell (SSH) 或直接串行连接访问的交互式命令行界面 (CLI)。

您还可以设置思科安全邮件和 Web 管理器，以统一管理多个邮件网关的报告、跟踪和隔离管理。

相关主题

- 支持的语言, on page 14

支持的语言

AsyncOS 可使用以下任何语言显示其 GUI 和 CLI：

- 英语
- 法语
- 西班牙语
- 德语
- 意大利语
- 韩语
- 日语
- 葡萄牙语（巴西）
- 中文（简体和繁体）
- 俄语

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。