思科安全邮件网关使用入门

本章包含以下部分：

AsyncOS 14.0 中的新增功能

表 *1: AsyncOS 14.0* 中的新增功能

功能	说明
将思科安全邮件网关与思科安全感知云服务集成	通过思科安全感知云服务，您可以有效地部署网络钓鱼模拟和/或感知培训，以便测量和报告结果。它让安全运营团队能够专注于实时威胁，而不是最终用户缓解。 思科安全感知云服务提供重复点击者报告 - 重复单击通过邮件发送的任何 URL 或附件的用户。这些用户通过思科安全感知云服务定义的网络钓鱼模拟活动来加以识别。 将邮件网关与思科安全感知云服务相集成有助于组织： • 提高用户对实际网络钓鱼攻击的意识。 • 允许邮件管理员为被思科安全感知云服务识别为“重复点击者”的一组用户配置严格的策略。 有关详细信息，请参阅 将邮件网关与思科安全感知云服务集成。

功能	说明
改进了邮件网关中的网络钓鱼检测	以下是用于改进邮件网关中网络钓鱼检测的一些增强功能： • 发件人域信誉过滤增强功能 • 默认扫描邮件附件中的 URL **发件人域信誉过滤增强功能**：您可以将邮件网关配置为根据 SMTP 会话级别的 SDR（发件人域信誉）判定来阻止邮件。 您可以使用邮件流策略配置设置来启用或禁用 SDR 验证。 **注释** 默认情况下，为传入邮件流策略启用 SDR 验证，为传出邮件流策略禁用 SDR 验证。 **默认扫描邮件附件中的 URL**：默认情况下，邮件网关会提前（反垃圾邮件引擎之前）在邮件管道中扫描邮件附件中的 URL，以查找任何恶意内容。 根据 SMTP 会话级别的 SDR 判定和邮件附件中 URL 的默认扫描来阻止邮件将有助于组织： • 改进对网络钓鱼和域欺骗的检测效果。 • 根据对 SDR 信誉判定采取的默认操作，在邮件管道中提前检测网络钓鱼攻击。 有关详细信息，请参阅发件人域信誉过滤和使用主机访问表定义允许连接的主机。

功能	说明

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、德语和法语。
	您可以通过以下任一方式创建用户定义的密码，以便打开传入或传出邮件中的受密码保护的附件：
	• Web 界面中的“安全服务 (Security Services) > 扫描行为 (Scan Behavior)”页面。
	• CLI 中的 `scanconfig> protectedattachmentconfig` 子命令。
	在此版本中，内容扫描程序只能扫描以下文件类型的受密码保护的附件内容：
	• Adobe 便携式文档格式 (PDF) 文件。
	• MS Office 文件类型：
	  • Word - 支持 2002 到 2004 版的 .doc 文件格式，以及支持 2007 到 2016 版的 .docx 文件格式。
	  • Excel - 支持 2007 至 2016 版的 .xls 和 .xlsx 文件格式。
	  • PowerPoint - 支持 2007 至 2016 版的 .ppt 或 .pptx 文件格式。
	• 存档文件类型 - .zip 格式。
	有关详细信息，请参阅 使用邮件过滤器实施邮件策略。

功能	说明

简单网络管理协议 (SNMP) 增强功能	以下是对 SNMP 配置设置作出的增强：
	• 添加了用于其他监控的新 SNMP MIB。
	• 支持 SNMPv3 陷阱：
	  • SNMPv3 支持所有三个安全级别 - noAuthNoPriv、authNoPriv 和 authPriv。
	  • 在同时启用 SNMPv3 和 SNMPv2 时，您需要选择所需的陷阱版本。
	  • 在同时启用 SNMPv2 和 SNMPv3 时，在 `snmpconfig` CLI 命令下添加了一个新选项来选择陷阱版本。
	有关详细信息，请参阅使用 CLI 进行管理和监控。

邮件策略详细信息的新报告	新报告 – 在邮件网关的新 Web 界面中添加了**邮件策略详细信息**。使用此报告可查看与已配置的邮件策略匹配的邮件数量。 有关详细信息，请参阅 使用邮件安全监控。
用于邮件策略详细信息的新邮件跟踪过滤器	新的邮件跟踪过滤器 - 在邮件网关的新 Web 界面的“邮件跟踪”(Message Tracking) > “高级搜索”(Advanced Search) > “邮件事件”(Message Event) 选项中添加了**邮件策略 (Mail Policy)**。使用此选项可以搜索与在“邮件策略名称” (Mail Policy Name) 字段中输入的已配置邮件策略名称相匹配的传入或传出邮件。

功能	说明
增强的概述和传入邮件报告页面	以下是邮件网关旧 Web 界面中的“概述”(Overview) 和“传入邮件”(Incoming Mail) 报告页面的增强功能： **概述 (Overview)** 报告页面： • 新的邮件类别 - 在“传入邮件摘要”(Incoming Mail Summary) 部分中添加了“由域信誉过滤拦截”(Stopped by Domain Reputation Filtering)。 • 在“传入邮件摘要”(Incoming Mail Summary) 部分中，将“由域信誉过滤拦截”(Stopped by Reputation Filtering) 邮件类别名称更改为“由 IP 信誉过滤拦截”(Stopped by IP Reputation Filtering)。 **传入邮件 (Incoming Mail)** 报告页面： • 添加了新的列 - “传入邮件详细信息”（Incoming Mail Details）部分中的“由域信誉过滤拦截”(Stopped by Domain Reputation Filtering)。 • 在“传入邮件详细信息”(Incoming Mail Details) 部分中，将“由信誉过滤拦截”(Stopped by Reputation Filtering) 列名更改为“由 IP 信誉过滤拦截”(Stopped by IP Reputation Filtering)。 有关详细信息，请参阅 使用邮件安全监控。

功能	说明
增强“邮件流摘要”(Mail Flow Summary) 和“邮件流详细信息”(Mail Flow Details) 报告页面	以下是邮件网关新 Web 界面中对“邮件流摘要”(Mail Flow Summary) 和“邮件流详细信息”(Mail Flow Details) 报告页面的增强： **邮件流摘要 (Mail Flow Summary)** 报告页面： • 添加了新的类别 - “威胁邮件”(Threat Messages) 图形部分中的“由域信誉过滤拦截”(Stopped by Domain Reputation Filtering)。 • 在“威胁消息”(Threat Messages) 图形部分中，将“由信誉过滤拦截”(Stopped by Reputation Filtering) 类别名称更改为“由 IP 信誉过滤拦截”(Stopped by IP Reputation Filtering)。 • 添加了新的列 - “威胁检测摘要”(Threat Detection Summary) 部分中的“由域信誉过滤拦截”(Stopped by Domain Reputation Filtering)。 • 在“威胁检测摘要”(Threat Detection Summary) 部分中，将“由信誉过滤拦截”(Stopped by Reputation Filtering) 列名更改为“由 IP 信誉过滤拦截”(Stopped by IP Reputation Filtering)。 **邮件流详细信息 (Mail Flow Details)** 报告页面： • 添加了新的列 - IP 地址、域和网络所有者的“传入邮件”(Incoming Mails) 部分中的“由域信誉过滤拦截”(Stopped by Domain Reputation Filtering)。 • 在 IP 地址、域和网络所有者的“传入邮件”(Incoming Mails) 部分中，将“由信誉过滤拦截”(Changed Stopped by Reputation Filtering) 列名更改为“由域信誉过滤拦截”(Stopped by Domain Reputation Filtering)。

功能	说明
支持国际化域名 (IDN)	思科安全邮件网关现在可以接收和传送邮件地址包含 IDN 域的邮件。 目前，您的邮件网关仅支持以下语言的 IDN 域： • **印度语区域语言**：印地语、泰米尔语、泰卢固语、卡纳达语、马拉提语、旁遮普语、马拉雅拉姆语、班加利语、古吉拉特语、乌尔都语、阿萨姆语、尼泊尔语、班加拉语、博多语、道格里语、克什米利语、孔卡尼语、迈提利语、马尼普利语、奥里亚语、梵语、圣达里语、信德语和图鲁语。 • **欧洲和亚洲语言**：法语、俄语、日语、德语、乌克兰语、韩语、西班牙语、意大利语、中文、荷兰语、泰语、阿拉伯语和哈萨克语。 有关详细信息，请参阅 系统管理。
安全增强功能	AsyncOS 14.0 包含以下安全增强功能： • 邮件网关现在可通过 TLS 发送思科技术支持请求。如果 SMTP 服务器未使用 TLS，则请求将以纯文本格式发送。 • 您现在可以将邮件网关配置为通过 TLS 发送警报。使用 CLI 中的以下子命令来配置此功能： `alertconfig > SETUP > Do you want to enable TLS support to send alert messages?.` 有关详细信息，请参阅与此版本相关的 CLI 参考指南。
新的补救报告状态小组件	在邮件网关新 Web 界面的“邮件跟踪”(Message Tracking) 页面中搜索和补救邮件时，会添加新的“补救报告状态”(Remediation Report Status) 小组件。 可使用此小组件来检查补救报告生成的状态。有关详细信息，请参阅补救邮箱中的邮件

功能	说明
支持新的内容匹配分类器 - 东南亚国家/地区的国家标识号	您可以使用以下任何一个新的内容匹配分类器（东南亚国家/地区的国家标识号）来创建 DLP 策略： • 印度尼西亚 KTP • 马来西亚 MyKad • 泰国 ID • 菲律宾 UMID • 新加坡 NRIC 您可以在邮件网关 Web 界面的以下页面中选择新的内容匹配分类器： • 转到“邮件策略”(Mail Policies) > “DLP 策略管理器”(DLP Policy Manager) > “添加自定义策略”(Add Custom Policy) 页面 > “预定义的自定义分类器”(Predefined Custom Classifiers) > **策略匹配详细信息 (Policy Matching Details)** 选项。 • 转到“邮件策略”(Mail Policies) > “DLP 策略管理器”(DLP Policy Manager) > “添加自定义策略”(Add Custom Policy) 页面 > “创建自定义分类器”(Create Custom Classifier) > **实体规则 (Entity rule)** 选项。 • 转到“邮件策略”(Mail Policies) > “DLP 策略管理器”(DLP Policy Manager) > “添加 DLP 策略”(Add DLP Policy) 页面 > **隐私保护模板 (Privacy Protection template)**选项。 • 转到“邮件策略”(Mail Policies) > “DLP 策略自定义”(DLP Policy Customizations) > ”添加自定义分类器”(Add Custom Classifier) 页面 > **实体规则 (Entity rule)** 选项。
产品和相关文档中的无偏差术语使用	我们删除了产品和相关文档中的偏差术语。 以下是已用新的无偏差术语替换的偏差术语列表： • “白名单”术语被替换为“允许列表”术语 • “黑名单”术语被替换为“阻止列表”术语 • “master”术语被替换为“primary”术语 • “从属”术语被替换为“辅助”术语 • “blackhole”术语被替换为“sinkhole”术语

功能	说明
对产品及相关文档进行品牌更名	我们对产品和相关文档进行了品牌更名，如下所示： • “思科邮件安全设备”被更改为思科安全邮件网关 • “思科云邮件安全设备”被更改为思科安全邮件云网关 • “思科内容安全管理设备”被更改为思科安全邮件和 *Web* 管理器
AMP 上游代理文件分析设置	您现在可以配置上游代理以进行文件分析。 有关详细信息，请参阅文件信誉过滤和文件分析：
对思科 SecureX 威胁响应中的邮件执行补救操作	在思科 SecureX 威胁响应中，您现在便可对邮件网关处理的邮件进行调查并采取以下补救操作： • 删除 • 转发 • 转发并删除 有关详细信息，请参阅与思科 SecureX 威胁响应集成
内容过滤器 - “附件文件信息”(Attachment File Info) 条件和“按文件信息删除附件”(Strip by Attachment File Info) 操作增强功能	新的选项 - 在“内容过滤器”(Content Filters) 中添加了**文件散列列表 (File Hash List)** - “附件文件信息”(Attachment File Info) 条件和“按文件信息删除附件”(Strip by Attachment File Info) 操作。 使用此选项可配置内容过滤器，以便对与所选文件散列列表中的特定文件 SHA-256 值匹配的邮件附件执行操作。 **注释** 您还可以使用邮件过滤器来配置此功能。 有关详细信息，请参阅内容过滤器和使用邮件过滤器实施邮件策略。

功能	说明
智能软件许可增强功能	AsyncOS 14.0 包括以下智能软件许可增强功能： • 在集群配置中，您现在可以启用智能软件许可，并向思科智能软件管理器同时注册所有的计算机。 • 在启用智能软件许可并向思科智能软件管理器注册邮件网关后，思科云服务门户就会自动启用，同时在您的邮件网关上注册。 • 如果思科云服务证书已过期，您现在可以使用 CLI 中的 `cloudserviceconfig > fetchcertificate` 子命令从思科 Talos 情报服务门户下载新的证书。 • 您可以在 CLI 中使用 `smartaccountinfo` 命令来查看在思科智能软件管理器门户中创建的智能帐户的详细信息。 有关详细信息，请参阅系统管理和与思科 SecureX 威胁响应集成。
AsyncOS 14.0 之后版本不支持“发件人域有效期”功能	AsyncOS 14.0 之后版本将不再支持“发件人域有效期”功能。“发件人域有效期”功能将替换为“发件人成熟度”功能。 “发件人成熟度”表示思科 Talos 认为域作为邮件发件人的成熟度。调整成熟度值可以启用有关邮件的威胁检测，并且通常不会反映“基于 Whois 的域有效期”中表示的域有效期。发件人成熟度被设为 90 天限制，如果超过该限制，域就会被视为邮件发件人的成熟地址，并且不会提供进一步的详细信息。 发件人成熟度用于计算发件人信誉。未成熟域的信誉较低。思科 Talos 建议您仅依靠发件人信誉来确定策略操作。对于特定的非标准场景，发件人成熟度会用于优化过滤器。 **注释** 思科 Talos 不会手动调整域的成熟度，而是依靠自动化系统和传感器来确定最合适的值。
生命周期终止 (EOL) 或服务终止 (EOS) AsyncOS 版本或硬件型号的警报或通知横幅	如果您的邮件网关在生命终止 (EOL) 或服务终止 (EOS) AsyncOS 版本或硬件型号上运行，那么现在您将在邮件网关 Web 界面或 CLI 上收到警报或通知横幅消息。
Office 365 或混合（图形 API）补救帐户配置文件配置增强功能	现在，您可以使用在 Azure 管理门户上生成的应用的“客户端密钥”值来验证 Office 365 或混合（图形 API）补救帐户配置文件的客户端凭证。 有关详细信息，请参阅补救邮箱中的邮件 。

功能	说明
亚马逊 Web 服务 (AWS) 的虚拟邮件网关支持	您可以在亚马逊 Web 服务 (AWS) 的亚马逊弹性计算云 (EC2) 上部署思科安全邮件虚拟网关。 请联系思科销售代表并提供您的 AWS 帐户详细信息（用户名和区域），以便调配 AMI 映像。
合并事件日志增强功能	以下是对“合并事件日志”日志类型的增强功能： • 新的日志字段 - 在合并事件日志日志类型中添加了“消息大小”(Message Size)，以便查看单个日志行输出中的消息大小。 • 现在，您可以在单个日志行输出中查看邮件中附件的大小 **步骤：** **1.** 为合并事件日志配置日志订用时，选择“文件详细信息”(File(s) Details) 日志字段。 **2.** 配置邮件过滤器规则，如下所示： `Custom_ Log_Entry: if (true) { log-entry("$filesizes"); }` 或 通过将自定义文本添加为“`$ filesizes`”来配置**添加日志条目 (Add Log Entry)** 内容过滤器操作。
支持云连接器日志记录	邮件网关现在支持一种新的日志订用类型 - **云连接器日志**。使用该日志订用可查看来自思科聚合服务器的 Web 交互跟踪数据的相关信息。信息或警告级别的大多数信息都会显示
文件信誉服务的请求重试方法的增强功能	现在，您可以在配置文件信誉和分析服务（“安全服务”(Security Services) > “文件信誉和分析”(File Reputation and Analysis)）时，将信誉查询超时值设置在 20-30 秒范围内。默认值为 20，这也是最小值。 在配置的查询超时期间，邮件网关会将文件信誉查询发送到 AMP 服务器。如果邮件网关无法从 AMP 服务器接收响应，则它会通过再次向 AMP 服务器发送查询来重试。查询超时包括第一个查询请求和重试请求所用的时间。 如果存在网络延迟或与 AMP 服务器相关的问题时，重试方法会让邮件网关接收响应。

功能	说明
新的思科 Talos 邮件状态门户	思科 Talos 邮件状态门户取代了旧的思科邮件提交和跟踪门户。 思科 Talos 邮件状态门户是一个基于 Web 的工具，用于监控来自最终用户的邮件提交状态。 **重要事项** • 旧门户的用户仍可在新门户中访问之前提交的内容 • 您将无法在新门户中提交可能被邮件网关错误识别的垃圾邮件、网络钓鱼邮件、正常邮件、营销邮件或非营销邮件的样本。有关如何提交邮件样本的详细信息，请参阅 https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/214133-how-to-submit-email-messages-to-cisco.html 上的“如何向思科提交邮件文档”。 有关详细信息，请参阅 管理垃圾邮件和灰色邮件。
身份验证日志增强功能	现在，您可以在身份验证日志中查看已登录用户的用户权限角色详细信息（例如，“admin”、“operator”等）。
定义登录密码的新密码规则	您的邮件网关中添加了新的密码规则，用于定义您的登录密码： 避免使用包含三个或更多重复或连续字符的密码（例如，“AAA@124”、“Abc@123”等）。 您可以通过以下任一方式来配置此密码规则： • “系统”(System) > “管理”(Administration) > “用户”(Users) > “本地用户账号和密码设置”(Local User Account & Passphrase Settings) > Web 界面中的**拒绝包含 3 个或 3 个以上重复或连续字符的密码 (Reject three or more repetitive or sequential characters in passphrases)** 复选框。 • `userconfig` > 策略 `(POLICY)` > 密码强度 `(PASSWORDSTRENGTH)` > 拒绝包含 3 个或 3 个以上重复或连续字符的口令？`(Reject passphrases that contain three or more repetitive or sequential characters?) [Y]>` CLI 中的 命令

功能	说明
创建系统生成的密码	除了手动创建登录密码之外，您现在还可以创建系统生成的密码以登录邮件网关。 您可以通过以下任一方式来配置系统生成的密码： • Web 界面中的“选项”(Options)>“更改口令”(Change Passphrase) 页面。 • Web 界面中的“系统管理”(System Administration) >“系统设置向导”(System Setup Wizard) 页面。 • Web 界面中的“系统管理”(System Administration) >“用户”(Users) >“添加本地用户”(Add Local User) 页面。 • CLI 中的 `passphrase` 或 `passwd` 命令 有关详细信息，请参阅 设置和安装。
对证书执行 FQDN 验证	您可以将邮件网关配置为在以下情况下对证书执行 FQDN 验证： • 导入自定义证书。 • 创建自签名 S/MIME 证书。 • 创建自签名证书。 • 导入自定义证书颁发机构 (CA) 列表。 **注释** 您还可以对包含 IDN 域的邮件网关证书执行 FQDN 验证。 有关详细信息，请参阅S/MIME 安全服务和加密与其他 MTA 的通信。

功能	说明
在SSL通信期间为对等证书执行FQDN验证	您可以在 Web 界面的“系统管理”(System Administration) > “SSL 配置”(SSL Configuration) 页面中将邮件网关配置为对等证书执行 FQDN 验证。 FQDN 验证适用于以下服务： • 出站 SMTP • LDAP • 更新程序 • TLS 警报 注释 您可以对仅包含出站 SMTP 服务的 IDN 域的对等证书执行 FQDN 验证。 有关详细信息，请参阅 系统管理。
在 SSL 通信期间为对等证书执行 x509 验证	您可以在 Web 界面的“系统管理”(System Administration) > “SSL 配置”(SSL Configuration) 页面中配置邮件网关，以便为对等证书执行 x509 验证。 x509 验证适用于以下服务： • 出站 SMTP • LDAP • 更新程序 • TLS 警报 有关详细信息，请参阅系统管理。

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。

Web 界面页面或元素	新 Web 界面	旧 Web 界面
“我的报告”页面	从“报告”下拉列表中选择**我的报告**。	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”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”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)。
垃圾邮件隔离区（管理和最终用户）	在新 Web 界面中单击**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。

Web 界面页面或元素	新 Web 界面	旧 Web 界面
策略、病毒和爆发隔离区	在新 Web 界面中单击**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，请单击上的**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	单击 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。	-
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。

Web 界面页面或元素	新 Web 界面	旧 Web 界面
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”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 17
- 培训, on page 18
- 思科通知服务 , on page 18
- 知识库, on page 18
- 思科支持社区, on page 19
- 思科客户支持, on page 19
- 第三方贡献者, on page 19
- 思科欢迎您发表意见, on page 19
- 注册思科账户 , on page 20

文档

可通过单击右上角的“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。

思科安全邮件网关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
- 适用于思科安全邮件网关思科邮件安全设备的 *AsyncOS* 用户指南（本手册）
- 《适用于思科安全邮件网关的 *AsyncOS CLI* 参考指南》
- 《使用思科安全邮件网关的 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。

思科内容安全产品的文档	位置
思科邮件安全	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd- products-support-series-home.html
思科网络安全	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products- support-series-home.html
思科内容安全管理	http://www.cisco.com/c/en/us/support/security/content-security-management- appliance/tsd-products-support-series-home.html
适用于思科内容安全设备的 CLI 参考指南	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
思科 IronPort 加密	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-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 20。

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

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 18
- 知识库, on page 18

思科安全邮件网关概述

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 21

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