思科邮件安全设备 AsyncOS 9.7 版本说明

发布日期：2015 年 10 月 26 日

目录

新增内容

特性	说明
内容扫描引擎更新	此版本更新了内容扫描引擎。在后续版本中，所有内容扫描引擎更新均可通过更新服务器自动获取。
图像分析扫描引擎更新	此版本更新了图像分析扫描引擎。
Cloudmark 反垃圾邮件引擎更新	此版本更新了 Cloudmark 反垃圾邮件引擎。
非垃圾邮件隔离区	您可以为所有策略、病毒和爆发隔离区（包括文件分析隔离区）指定保留时间（以分钟为单位）。

LDAP	在新版本中，当 LDAP 查询返回“不可用”(Unavailable)、“系统繁忙”(Busy) 或“操作错误”(Operations Error) 等特定错误代码时，它将回退到列出的后续 LDAP 服务器，以进行故障切换。之前，仅当与 LDAP 服务器连接失败时，才进行故障切换。
可选择是接受还是拒绝包含组播地址的 ARP 应答	在新版本中，您可以在 CLI 中使用 `etherconfig` 命令配置以太网介质设置时，指定是接受还是拒绝包含组播地址的 ARP 应答。
RAR 5.0 存档格式支持	在新版本中，思科邮件安全设备将支持扫描 RAR 5.0 文件。
SMTP Call-Ahead 服务器配置文件设置的变化	在新版本中，您可以在设置 SMTP Call-Ahead 服务器配置文件时，将设备配置为拒绝因验证失败而连接自定义 SMTP 响应（代码和文本）。

行为变化

爆发过滤器设置的变化	在新版本中，即使“URL 重写”(URL Rewriting) 被禁用或未设置“威胁免责声明”(Threat Disclaimer)，您也可以在启用邮件策略中的“爆发过滤器”(Outbreak Filter) 时，将设备配置为修改邮件主题。
呈现 CPU 使用率	在新版本中，为更好地呈现 CPU 使用率，参数“CPU 总使用率”(Total CPU Utilization) 将更改为“CPU 总负载平均值”(Overall CPU Load Average)（可在 Web 界面上导航至“监控”[Monitor] > “系统状态”[System Status] > “CPU 使用率”[CPU Utilization] 或在 CLI 中运行 `system status` 命令）。“CPU 总负载平均值”(Overall CPU Load Average) 是设备在过去一分钟内的 CPU 负载平均值。
Authentication-Results 报头的变化	在新版本中，Authentication-Results 报头将包括 SPF、DKIM 和 DMARC 验证的身份验证结果。 此外，在新版本中，为了符合 RFC5451，如果已启用 DKIM 验证且邮件为非 DKIM 签名邮件，则设备将在 Authentication-Result 报头中添加“none”。
URL 过滤的变化	在新版本中，之前标记为“可疑”(Suspicious) 的 URL 将标记为“不确定”(Neutral)。仅标记发生变化；底层逻辑和处理没有变化。
接收和处理来自 DMARC 记录格式不正确的域的邮件	在新版本中，思科邮件安全设备将能够接收和处理来自 DMARC 记录格式不正确的域的邮件。但是，该设备将不会对此类邮件执行 DMARC 验证。
去除了 SMTP 路由目标主机名的字符限制	在新版本中，您可以在设置 SMTP 路由时，指定超过 45 个字符的目标主机名。
内容扫描程序行为	为增强性能，如果图像分析功能未启用，内容扫描程序不会提取嵌入到附件文件中的图像。

升级路径

您可以从以下版本升级到 9.7.0-125 版本：

- 8.5.7-043
- 9.1.0-032
- 9.1.1-023
- 9.1.1-025
- 9.6.0-042
- 9.6.0-051
- 9.7.0-041
- 9.7.0-119

安装和升级说明

阅读并考虑本部分中列出的安装和升级影响。

当您通过 Web 界面或命令行界面 (CLI) 升级 AsyncOS 时，相应配置会保存到 /configuration/upgrade 目录中的文件。您可以使用 FTP 客户端访问升级目录。每个配置文件名都附有版本号，而且配置文件中的密码是屏蔽的，因此无法人为识别。

您必须以管理员身份登录才能执行升级。此外，升级完成后必须重启设备。

此版本支持的硬件

- 所有虚拟设备型号。
- 以下硬件型号：
  - C380 或 C680
  - C170
  - 某些 C370、C370D、C670 或 X1070 设备

    要确定您的设备是否受支持，并解决设备当前不兼容的问题（如果有），请访问 http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63931.html。

此版本不支持以下硬件：

C160、C360、C660 和 X1060

部署或升级虚拟设备

如需部署或升级虚拟设备，请参阅《*思科内容安全虚拟设备安装指南*》，可通过以下网址获取：http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html。

升级虚拟设备

如果您当前的虚拟设备版本不支持超过 2 TB 的磁盘空间，但您希望在使用此版本时使用超过 2 TB 的磁盘空间，那么不能只是简单升级虚拟设备，

而必须为此版本部署一个新的虚拟机实例。

如果您选择升级虚拟设备，则现有许可证保持不变。

从硬件设备迁移到虚拟设备

步骤 1 参阅部署或升级虚拟设备（第 3 页）中介绍的文档，使用此 AsyncOS 版本设置您的虚拟设备。

步骤 2 将您的硬件设备升级到此 AsyncOS 版本。

步骤 3 保存已升级硬件设备中的配置文件。

步骤 4 将硬件设备中的配置文件加载到虚拟设备上。

请务必选择与网络设置相关的相应选项。

获取虚拟设备技术支持

有关获取虚拟设备技术支持的要求，请参阅《*思科内容安全虚拟设备的安装指南*》（可从 http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html 下载）。

另请参阅下文的服务与支持（第 8 页）。

从虚拟设备调配和激活思科注册信封服务管理员

有关调配虚拟设备所需的信息，请联系思科技术支持中心 (TAC)。

升级前的注意事项

请在升级之前查看以下内容：

FIPS 合规性

AsyncOS 9.7 版本不符合 FIPS。如果在设备上启用了 FIPS 模式，必须在升级到 AsyncOS 9.7 之前禁用该模式。

利用集中管理升级部署（集群设备）

如果集群包含 C160、C360、C660 或 X1060 硬件设备，请在升级之前从集群中删除这些设备。

集群中的所有机器都必须运行同一 AsyncOS 版本，而 x60 硬件无法升级到此版本。因此，必要时，请为 x60 设备创建单独的集群。

从上一版本以外的版本进行升级

如果是从上一版本以外的主要 (AsyncOS X.0) 或次要 (AsyncOS X.x) 版本进行升级，应查看当前使用的版本和此版本之间所有主要和次要版本的版本说明。

维护版本 (AsyncOS X.x.x) 仅包含漏洞修复。

配置文件

对于主要版本，思科通常不支持配置文件向后兼容。但是对于次要版本，配置文件可向后兼容。旧版本中的配置文件可能与新版本兼容；但可能需要经过修改才能加载。如果对配置文件支持您有任何问题，请联系思科客户支持部门。

升级到此版本

准备工作

- 查看已知和已修复的问题（第 6 页）和安装和升级说明（第 3 页）。
- 如果要升级虚拟设备，请参阅升级虚拟设备（第 4 页）。

程序

参照以下说明升级您的邮件安全设备。

步骤 1 将 XML 配置文件保存到设备外。

步骤 2 如果您使用安全列表/阻止列表功能，请将安全列表/阻止列表数据库导出到设备外部。

步骤 3 暂停所有侦听程序。

步骤 4 等待队列为空。

步骤 5 在“系统管理”(System Administration) 选项卡中，选择“系统升级”(System Upgrade) 页面。

步骤 6 点击**可用的升级 (Available Upgrades)** 按钮。页面会刷新，并显示可用的 AsyncOS 升级版本列表。

步骤 7 点击**开始升级 (Begin Upgrade)** 按钮，即可开始升级。回答出现的问题。

步骤 8 升级完成后，点击**立即重启 (Reboot Now)** 按钮重启设备。

步骤 9 恢复所有侦听程序。

后续操作

查看性能公告（第 6 页）。

性能公告

RSA 邮件 DLP

- 如果在一个对入站邮件运行反垃圾邮件和防病毒扫描的设备上对出站邮件启用 RSA 邮件 DLP，性能将降低不到 10%。
- 相对于上一场景而言，在仅运行出站邮件而未运行反垃圾邮件和防病毒扫描的设备上启用 RSA 邮件 DLP，可能导致性能进一步降低。

SBNP

在此版本中，SenderBase Network Participation 将使用情景自适应扫描引擎 (CASE) 收集数据，以支持 IronPort 信息服务。在某些配置下，客户可能会发现性能略有下降。

爆发过滤器

爆发过滤器使用情景自适应扫描引擎来确定邮件的威胁级别，并基于自适应规则和爆发规则组合对邮件进行评分。在某些配置下，您可能会发现性能略有下降。

IronPort 垃圾邮件隔离区

如果对 C 系列或 X 系列设备启用机上 IronPort 垃圾邮件隔离区，会最大程度降低名义上高负载的设备遭受的系统吞吐量下降。对于在运行时接近或处于峰值吞吐量的设备，活动隔离区中的额外负载可能导致吞吐量降低 10-20%。如果您的系统已达到或接近饱和状态，并且您希望使用 IronPort 垃圾邮件隔离区，请考虑迁移到更大型的 C 系列设备或 M 系列设备。

如果将反垃圾邮件策略从减少垃圾邮件改为隔离垃圾邮件（无论是在机上还是机下），由于系统需要扫描更多垃圾邮件来防范病毒并确保内容安全，所以系统负载会有所增加。如需有关合理调整安装规模的帮助，请与授权支持提供商联系。

已知和已修复的问题

如需了解此版本中已知和已修复的问题，请使用思科漏洞搜索工具进行查找。

- 漏洞搜索工具的要求（第 6 页）
- 已知和已修复问题列表（第 6 页）
- 查找有关已知和已解决问题的信息（第 7 页）

漏洞搜索工具的要求

如果您没有思科帐户，请注册思科帐户。访问 https://tools.cisco.com/RPF/register/register.do。

已知和已修复问题列表

已修复的问题	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=9.7.0&sb=anfr&sts=fd&srtBy=byRel&bt=custV
已知问题	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=9.7.0&sb=anfr&sts=open&srtBy=byRel&bt=custV

查找有关已知和已解决问题的信息

如需了解已知和已解决的缺陷的最新信息，请使用思科漏洞搜索工具进行查找。

准备工作

如果您没有思科帐户，请注册思科帐户。访问 https://tools.cisco.com/RPF/register/register.do。

程序

步骤 1 转到 https://tools.cisco.com/bugsearch/。

步骤 2 使用思科帐户凭证登录。

步骤 3 依次点击**从列表中选择 (Select from list) > 安全 (Security) > 邮件安全 (Email Security) > 思科邮件安全设备 (Cisco Email Security Appliance)**，然后点击**确定 (OK)**。

步骤 4 在“版本”(Releases） 字段中，输入版本号，例如 9.7。

步骤 5 根据您的要求，执行以下操作之一：

- 要查看已解决问题的列表，请从“显示漏洞”(Show Bugs) 下拉列表中选择**这些版本中已修复的问题 (Fixed in these Releases)**。
- 要查看已知问题的列表，请从“显示漏洞”(Show Bugs) 下拉列表中选择**影响这些版本的问题 (Affecting these Releases)**，然后从“状态”(Status) 下拉列表中选择**未解决 (Open)**。

注 如果您有任何疑问或问题，请点击工具右上角的**帮助 (Help)** 或**反馈 (Feedback)** 链接。我们还提供了交互式导览，如需查看，请点击搜索字段上方的橙色信息栏中的链接。

文档更新

《用户指南》PDF 的版本可能要比在线帮助的版本新。要获取用户指南 PDF 和其他有关此产品的文档，请在“在线帮助”(Online Help) 中点击**查看 PDF (View PDF)** 按钮，或访问相关文档（第 7 页）中显示的 URL。

相关文档

思科内容安全产品文档	位置
硬件和虚拟设备	请参阅此表中的相应产品。
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
思科网络安全	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
思科邮件安全	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html

思科内容安全产品文档	位置
思科内容安全设备 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-encryption/tsd-products-support-series-home.html

服务与支持

注意 要获取虚拟设备支持，请在致电思科 TAC 时准备好您的虚拟许可证编号 (VLN)。

思科 TAC：http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

传统 IronPort 的支持站点：http://www.cisco.com/web/services/acquisitions/ironport.html

对于普通问题，您还可以联系设备客户支持人员。有关说明，请参阅用户指南或在线帮助。

本文档需结合“相关文档”部分中列出的文档共同使用。