思科云 / 混合邮件安全概述

发布日期：2017 年 7 月 28 日
修订日期：2018 年 7 月 23 日

思科系统公司
www.cisco.com
思科在全球设有 200 多个办事处。
有关地址、电话号码和传真号码信息，
可查阅思科网站：
www.cisco.com/go/offices。

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系以获取副本。

思科所采用的 TCP 信头压缩是加州大学伯克莱分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。保留所有权利。© 1981，加州大学董事会。

无论在该手册中是否作出了其他担保，来自这些供应商的所有文档文件和软件都按“原样”提供且仍有可能存在缺陷。思科和上述供应商不承诺所有明示或暗示的担保，包括（但不限于）对特定用途的适销性、适用性、非侵权性以及因交易、使用或商业惯例所衍生的担保。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

CCDE、CCENT、CCSI、Cisco Eos、Cisco HealthPresence、Cisco IronPort、思科徽标、Cisco Nurse Connect、Cisco Pulse、Cisco SensorBase、Cisco StackPower、Cisco StadiumVision、Cisco TelePresence、Cisco Unified Computing System、Cisco WebEx、DCE、Flip Channels、Flip for Good、Flip Mino、Flipshare (Design)、Flip Ultra、Flip Video、Flip Video (Design)、Instant Broadband 和 Welcome to the Human Network 均为商标；Changing the Way We Work, Live, Play, and Learn、Cisco Capital、Cisco Capital (Design)、Cisco:Financed (Stylized)、Cisco Store、Flip Gift Card 和 One Million Acts of Green 是服务商标；Access Registrar、Aironet、AllTouch、AsyncOS、Bringing the Meeting To You、Catalyst、CCDA、CCDP、CCIE、CCIP、CCNA、CCNP、CCSP、CCVP、Cisco、Cisco Certified Internetwork Expert 徽标、Cisco IOS、Cisco Lumin、Cisco Nexus、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems 徽标、Cisco Unity、Collaboration Without Limitation、Continuum、EtherFast、EtherSwitch、Event Center、Explorer、Follow Me Browsing、GainMaker、iLYNX、IOS、iPhone、IronPort、IronPort 徽标、Laser Link、LightStream、Linksys、MeetingPlace、MeetingPlace Chime Sound、MGX、Networkers、Networking Academy、PCNow、PIX、PowerKEY、PowerPanels、PowerTV、PowerTV (Design)、PowerVu、Prisma、ProConnect、ROSA、SenderBase、SMARTnet、Spectrum Expert、StackWise、WebEx 和 WebEx 徽标均为 Cisco Systems, Inc. 和/或其附属公司在美国和其他特定国家/地区的注册商标。

本文档或网站中提及的所有其他商标均属于其各自所有者。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(0910R)

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

思科云混合邮件安全概述
© 2017 - 2018 思科系统公司。保留所有权利。

目 录

了解思科邮件安全服务

思科云邮件安全服务概述

思科云邮件安全提供的基础设施在思科数据中心内维护，这些数据中心具有恢复能力强的特点并且分布于不同的地理位置。 该服务基于“云端”或软件即服务 (SaaS) 模式提供邮件安全。您的组织对基于云的基础设施仍然保有访问权限和可视性 。

在本指南中，“设备”一词用于表示虚拟设备。

思科云邮件安全是一种全包式服务。软件、硬件和支持捆绑在一起。该服务包括以下特性和功能：

- **使用外部威胁源。**借助外部威胁源 (ETF) 框架，思科邮件安全网关可以使用通过 TAXII 协议传输的 STIX 格式的外部威胁信息。
- **发件人域信誉过滤。** 使用发件人域信誉 (SDR) 过滤功能，您可以根据思科 SDR 服务确定的 SDR 过滤经过思科邮件安全网关的邮件。
- **新的防数据丢失 (DLP) 解决方案。**思科现在提供了一种替代 DLP 解决方案，它允许将 RSA DLP 中创建的所有现有 DLP 策略无缝迁移到新的 DLP 引擎。升级后，您可以在 Web 界面中的**邮件策略 > DLP 策略管理器**页面中查看或修改迁移的 DLP 策略。

  注 Async0S 11.0 和更高版本不支持 RSA 企业管理器集成。如果在 RSA 企业管理器中创建了 DLP 策略，则升级后必须在设备中重新创建这些策略。

- 网关处的**反垃圾邮件**，通过 SenderBase 信誉过滤器和IronPort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。
- **灰色邮件检测和安全取消订用**。您可以通过思科邮件安全设备：
  - 使用集成的灰色邮件引擎识别灰色邮件，并进行相应的策略控制。
  - 为最终用户提供安全且简单的机制，使其能够使用基于云的取消订用服务取消订用不需要的灰色邮件。
- **Outbreak Filters™**（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。

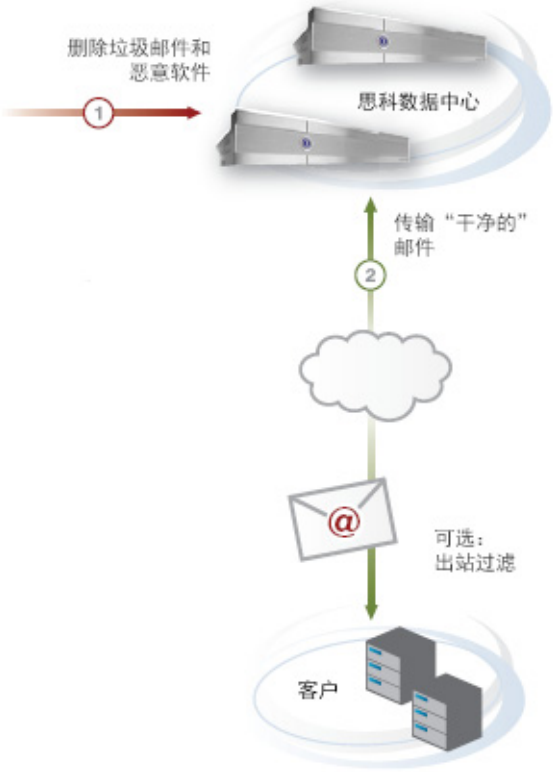
- **策略、病毒和病毒爆发隔离区。**提供一个安全的位置来存储可疑邮件供管理员评估。
- **垃圾邮件隔离区。**为最终用户提供对隔离的垃圾邮件和疑似垃圾邮件的访问。
- **邮件身份验证**。此设备支持各种不同形式的邮件身份验证，包括传入邮件的发件人策略框架 (SPF)、发件人 ID 框架 (SIDF) 和 DomainKeys 确定的邮件 (DKIM) 验证，以及传出邮件的 DomainKeys 和 DKIM 签名。
- **文件信誉过滤和文件分析**。高级恶意软件防护根据以下条件识别传入和传出邮件中新出现的和有针对性的基于文件的威胁：
  - 文件信誉
  - 文件分析（信誉未知的某些文件）
  - 判定更新
- **URL 过滤**。URL 过滤可获取传入和传出邮件中的 URL 的信誉和类别，从而实现一些新功能。
- **S/MIME 安全服务**。通过思科邮件安全设备，组织现可使用 S/MIME 安全地通信，不再要求所有最终用户拥有自己的证书。组织可以在网关级别使用标识组织而非个人的证书处理邮件的签名、加密、验证和解密。
- **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，需要在思科邮件安全设备上配置加密策略并使用托管密钥服务来加密邮件。
- **邮件跟踪**。此设备包含邮件跟踪功能，可帮助轻松获取思科邮件安全设备所处理邮件的状态。
- **邮件流监控。**监控所有入站和出站邮件的邮件流，全面了解企业的所有邮件流量。
- **访问控制。**对入站发件人，基于发件人的 IP 地址、IP 地址范围或域进行访问控制。
- 广泛的**邮件过滤**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。
- **通过基于传输层安全的安全 SMTP 进行邮件加密。**确保对公司基础设施与其他可信主机之间传输的邮件进行加密。

  经过整合的、功能强大的报告选项可以分析来自不同地理位置的基础设施部署的流量数据，从而提供完全集成的安全报告功能。即使是针对世界上数据量最高的网络，思科邮件安全设备的第三代报告技术也可提供前所未有的深入洞察。详细、准确的信息经过汇集加工，生成清晰且信息丰富的报告，适合组织的各个级别。

  邮件跟踪功能可帮助组织近乎实时地把握邮件动态，跟踪邮件处置情况。通过确定邮件的确切位置，此功能可以帮助快速解决支持中心的呼叫问题。您可以使用灵活的跟踪界面来查找邮件，而不必搜索日志文件。

图 1-1 显示了思科云邮件安全的部署模式。

图 1-1　　思科云邮件安全部署



思科云邮件安全的工作原理如下：

- 邮件安全设备在其他邮件安全设备之间同步配置信息（称为集群配置）。
- 基于云的邮件安全设备集群接收并处理入站邮件。
- 基于云的安全管理设备从云邮件安全设备收集报告和跟踪数据。它可以用作一个集中的位置，用于隔离邮件安全设备集群中按策略隔离或作为垃圾邮件隔离的邮件。
- 集中隔离基于策略过滤的邮件。
- 系统将处理后的邮件直接发送到组件服务器或邮件传输代理 (MTA)，处理来自组件服务器的出站邮件，并提供高级内容过滤和邮件加密。
- （可选）可以通过邮件安全设备集群将出站邮件发送到互联网。

思科混合邮件安全概述

思科混合邮件安全是一种独特的服务产品，它将基于云的邮件安全部署与基于设备的邮件安全部署（本地）相结合，为组织提供最大的选择余地和可控性。基于云的基础设施通常用于入站邮件清理，而本地设备则提供精細控制，通过数据丢失防御 (DLP) 和加密技术保护敏感信息。

与思科云邮件安全服务一样，混合服务也是全包式服务，软件、硬件和支持捆绑在一起。该服务包括以下特性和功能：

- **使用外部威胁源。**借助外部威胁源 (ETF) 框架，思科邮件安全网关可以使用通过 TAXII 协议传输的 STIX 格式的外部威胁信息。

- **发件人域信誉过滤。** 使用发件人域信誉 (SDR) 过滤功能，您可以根据思科 SDR 服务确定的 SDR 过滤经过思科邮件安全网关的邮件。
- **新的防数据丢失 (DLP) 解决方案。**思科现在提供了一种替代 DLP 解决方案，它允许将 RSA DLP 中创建的所有现有 DLP 策略无缝迁移到新的 DLP 引擎。升级后，您可以在 Web 界面中的**邮件策略 > DLP 策略管理器**页面中查看或修改迁移的 DLP 策略。

  注 Async0S 11.0 和更高版本不支持 RSA 企业管理器集成。如果在 RSA 企业管理器中创建了 DLP 策略，则升级后必须在设备中重新创建这些策略。

- 网关处的**反垃圾邮件**，通过 SenderBase 信誉过滤器和IronPort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。
- **灰色邮件检测和安全取消订用**。您可以通过思科邮件安全设备：
  - 使用集成的灰色邮件引擎识别灰色邮件，并进行相应的策略控制。
  - 为最终用户提供安全且简单的机制，使其能够使用基于云的取消订用服务取消订用不需要的灰色邮件。
- **Outbreak Filters™**（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。
- **垃圾邮件隔离区。**为最终用户提供对隔离的垃圾邮件和疑似垃圾邮件的访问。
- **邮件身份验证**。此设备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。
- **文件信誉过滤和文件分析**。高级恶意软件防护根据以下条件识别传入和传出邮件中新出现的和有针对性的基于文件的威胁：
  - 文件信誉
  - 文件分析（信誉未知的某些文件）
  - 判定更新
- **URL 过滤**。URL 过滤可获取传入和传出邮件中的 URL 的信誉和类别，从而实现一些新功能。
- **S/MIME 安全服务**。通过思科邮件安全设备，组织现可使用 S/MIME 安全地通信，不再要求所有最终用户拥有自己的证书。组织可以在网关级别使用标识组织而非个人的证书处理邮件的签名、加密、验证和解密。
- **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，需要在思科邮件安全设备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，用于管理设备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IronPort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。
- **邮件跟踪**。此设备包含邮件跟踪功能，可帮助轻松获取思科邮件安全设备所处理邮件的状态。
- **邮件流监控**。监控所有入站和出站邮件的邮件流，全面了解企业的所有邮件流量。
- **访问控制。**对入站发件人，基于发件人的 IP 地址、IP 地址范围或域进行访问控制。
- 广泛的**邮件过滤**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。

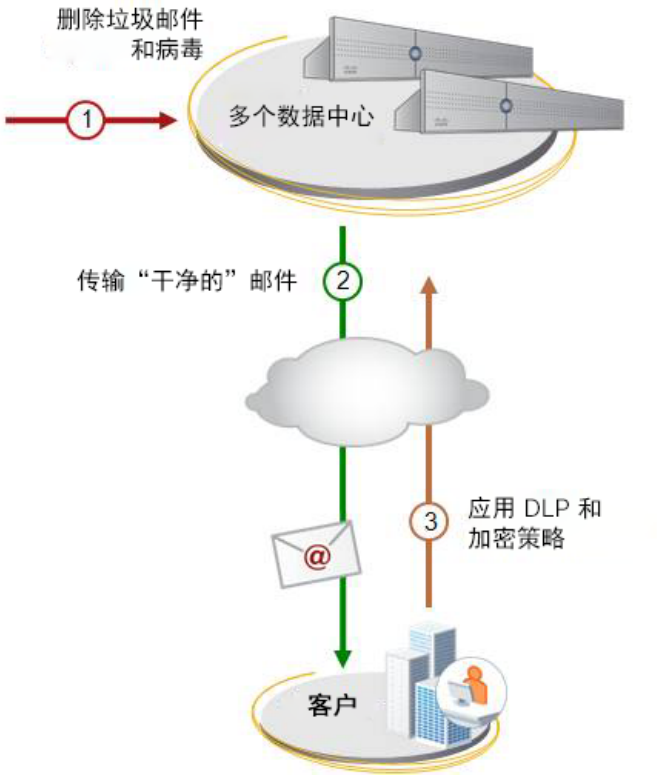
- **通过基于传输层安全的安全 SMTP 进行邮件加密。**确保对公司基础设施与其他可信主机之间传输的邮件进行加密。

  经过整合的、功能强大的报告选项可以分析来自不同地理位置的基础设施部署的流量数据，从而提供完全集成的安全报告功能。即使是针对世界上数据量最高的网络，思科邮件安全设备的第三代报告技术也可提供前所未有的深入洞察。详细、准确的信息经过汇集加工，生成清晰且信息丰富的报告，适合组织的各个级别。

  邮件跟踪功能可帮助组织近乎实时地把握邮件动态，跟踪邮件处置情况。通过确定邮件的确切位置，此功能可以帮助快速解决支持中心的呼叫问题。您可以使用灵活的跟踪界面来查找邮件，而不必搜索日志文件。跟踪同时跨越基于云的设备和本地设备。

图 1-2 显示了思科混合邮件安全的部署模式。

图 1-2　　思科混合邮件安全部署



思科混合邮件安全的工作原理如下：

- 邮件安全设备在其他邮件安全设备之间同步配置信息（称为集群配置）。
- 云邮件安全设备接收并处理入站邮件。系统将处理后的邮件发送到本地邮件安全设备，由其执行其他内容过滤，以便按策略过滤邮件。
- 基于云的安全管理设备从云邮件安全设备以及本地邮件安全设备收集报告和跟踪数据。
- 基于云的安全管理设备可以用作集中隔离区，用于隔离来自基于云的邮件安全设备的垃圾邮件。
- 根据策略过滤的邮件在过滤该邮件的思科安全管理设备上隔离。
- 本地邮件安全设备将邮件传送到组件服务器，处理来自组件服务器的出站邮件，并提供高级内容过滤和邮件加密。
- 本地邮件安全设备将出站邮件发送到互联网。

强烈建议您不要允许基于云的设备批量中转出站邮件，例如群发的营销邮寄广告。相反，您可以将中转流量仅限于事务邮件。容量保证不包括生成程序或实体的营销通信或邮件。

管理思科邮件安全服务

您可以直接使用设备来管理并更改基于云的邮件安全服务。

您可以使用设备执行以下操作：

- 查看并跟踪有关基于云的邮件安全服务的信息。
- 访问报告。
- 访问并修改基于云的设备的配置。

服务与支持

注　要获得思科云邮件安全 (CES) 的支持服务，请在致电思科 TAC 时提前准备好您的合同编号。

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

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

对于普通问题，您还可以从设备上访问客户支持。有关说明，请参阅用户指南或在线帮助。

设置云环境

访问云设备

访问 Web 界面和命令行界面

您可以直接通过设备访问所有云设备的 Web 界面，也可以使用欢迎函中提供的 URL 对这些 Web 界面进行访问。

您可以使用欢迎函中提供的详细信息，通过命令行界面 (CLI) 访问所有云设备。

配置云邮件安全设备

配置邮件身份验证

要对邮件进行身份验证，您可以使用发件人策略框架 (SPF) 或 DomainKey 识别的邮件 (DKIM)。

DKIM 基于发件人使用的签名密钥验证邮件的真实性。SPF 基于 DNS 文本记录验证邮件的真实性。通过 SPF，互联网域的所有者可使用特定格式的 DNS 记录指定哪些计算机获得发送该域邮件的权限。

配置 DKIM

有关配置 DKIM 及定义内容过滤器和邮件过滤器规则的说明，请参阅*《思科邮件安全设备 AsyncOS 用户指南》中的以下章节：*

- 邮件验证
- 使用邮件过滤器实施邮件策略

配置 SPF

思科会对您的 DNS 文本记录提供建议的 SPF 条目，但不会管理客户拥有的域的 DNS，例如邮件安全设备的收件人访问表。记录的格式如下：

`v=spf1 -exists:%{i}.spf.<unique_name>.iphmx.com -all`

请参阅服务与支持（第 1-6 页）。

将 SPF 记录添加到 DNS 后，您可以设置 SPF 验证并定义内容过滤器和邮件过滤器规则。请参阅*《思科邮件安全设备 AsyncOS 用户指南》中的以下章节：*

- 邮件验证
- 使用邮件过滤器实施邮件策略

路由出站邮件

对于通过云邮件安全设备出站的邮件，您必须配置设备以确保基于云的服务器能代表您中转邮件。请参阅《*思科邮件安全设备 AsyncOS 用户指南*》中的以下章节：“配置路由和传送功能”。

存档日志

思科不存储云设备中的日志。历史日志不会存档，而且可能因日志滚动而被覆盖。如果您想保留日志，请将基于云的设备上的日志订阅配置为使用 SCP 推送（或远程服务器上的 SCP）作为日志检索方法。此方法可将日志文件定期推送到远程计算机上的 SCP 服务器。

此方法要求在远程计算机上存在使用 SSH1 或 SSH2 协议的 SSH SCP 服务器。这种订阅需要提供远程计算机上的用户名、SSH 密钥和目的目录，并且日志文件将根据您设置的滚动计划传输。

如果您的防火墙阻止对您的网络进行 SSH 访问，建议您明确允许来自思科云邮件安全数据中心的入站 SSH 连接。

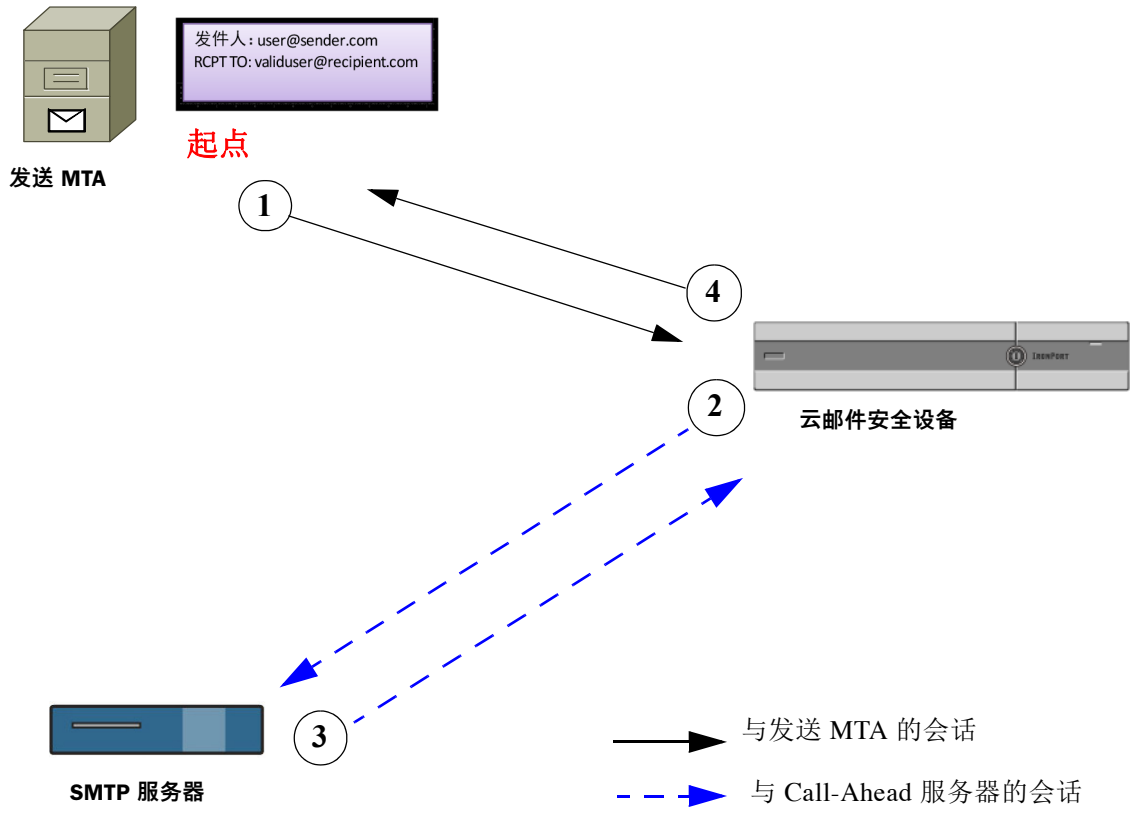
请参阅《*思科邮件安全设备 AsyncOS 用户指南*》。

配置您的服务器

使用 SMTP Call Ahead 验证

思科云邮件安全使用 SMTP Call Ahead 验证来进行收件人验证，这是一种无缝、简洁的方法，可以在最大限度减少管理员开销的同时，对收件人进行验证。此方法对现有解决方案的已有防火墙设置影响最小或没有影响。

图 2-1　　SMTP Call Ahead 服务器会话工作流程



SMTP Call Ahead 的工作原理如下：

步骤 1　发送邮件系统 (MTA) 打开与基于云的邮件安全设备的连接。在初始 SMTP 协议会话的过程中，发件人邮件系统传递 RCPT TO 信息。

步骤 2　基于云的邮件安全基础设施保持传入连接处于打开状态，并向 SMTP 服务器发起呼叫。在此通信过程中，基于云的邮件安全设备将 RCPT TO 信息传递到您的 SMTP 服务器（例如，Microsoft Exchange）。

步骤 3　根据“RCPT TO:”中的用户是有效还是无效，SMTP 服务器分别发送 200 系列状态或 500 系列状态。

为使 SMTP Call Ahead 正常工作，请确保已在您的 MTA 或组件服务器上为指定 IP 地址禁用可能会阻止来自基于云的服务器的连接的发件人验证功能（例如，SPF 检查、TLS 检查和 DHAP 方案）。

步骤 4　云邮件安全设备将恢复 SMTP 会话并向发送 MTA 发送响应，以便基于 SMTP 服务器响应（以及在 SMTP Call-Ahead 配置文件中配置的设置）继续会话或删除连接。

由于邮件管道中的处理顺序，如果特定收件人的邮件被 RAT 拒绝，则不会进行 SMTP Call-Ahead 收件人验证。例如，如果在 RAT 中指定仅接受 *example.com* 的邮件，则在进行 SMTP Call-Ahead 收件人验证之前，会拒绝 *recipient@domain2.com* 的邮件。

有关 SMTP Call-Ahead 验证如何发生的详细信息，请参阅 *《思科邮件安全设备 AsyncOS 用户指南》*。

使用思科最终用户垃圾邮件隔离区

注 本章仅适用于已启用最终用户垃圾邮件隔离区的情况。

了解思科最终用户垃圾邮件隔离区

垃圾邮件包括（但不限于）：

- 广告邮件、非法传销、连锁信和政治宣传
- 令人讨厌的可疑主题，或者辱骂或恐吓邮件
- 包含虚假或误导性的标题、主题行、发件人、回复地址或者发送或传输路径的邮件
- 未经许可擅自使用第三方域名的邮件

通过实施适当的策略和技术，垃圾邮件隔离区可以将垃圾邮件的影响降到最低。已被识别为垃圾邮件的邮件将被隔离。如果邮件并非垃圾邮件，您可以将其从隔离区移走，并将发件人添加到安全列表。或者，如果邮件确实是垃圾邮件， 则不执行任何操作。已隔离的邮件并不计入邮箱容量限制范围内，并会在一定天数后自动被删除。

注 请向管理员了解隔离区会将邮件保留多少天之后再删除。

访问垃圾邮件隔离区不需要特殊的硬件、软件或安全授权。您会定期收到垃圾邮件隔离区通知，列出被识别为垃圾邮件的邮件。

安全列表和阻止列表

您可以创建安全列表和阻止列表，更好地控制应视为垃圾邮件的邮件。使用安全列表可以确保特定用户或域永远不会被视为垃圾邮件，而使用阻止列表则能确保特定用户或域始终被视为垃圾邮件。

注 请向管理员了解您可以添加到安全列表和阻止列表中的最大条目数。

请参阅访问安全列表和阻止列表（第 3-3 页）。

处理垃圾邮件隔离区中的邮件

垃圾邮件隔离区通知提供邮件的详细信息，以便您确定邮件是否确实是垃圾邮件。您可以直接通过垃圾邮件隔离区通知处理邮件，也可以点击通知正文中提供的链接访问垃圾邮件隔离区。

如果邮件是垃圾邮件，则不需要执行任何操作。系统会将邮件在隔离区中保留一定天数（请向管理员核实具体天数），然后删除。

将邮件从垃圾邮件隔离区放行到收件箱

如果邮件不是垃圾邮件，则将邮件从隔离区放行到收件箱。您还可以将发件人添加到安全列表，以防止今后来自该发件人的邮件被隔离。

程序

步骤 1　在垃圾邮件隔离区通知中，点击要放行的邮件旁的**非垃圾邮件**。

步骤 2　在显示的确认消息中，点击**添加发件人至安全列表。**

如果放行邮件但未将发件人添加到安全列表，今后来自该发件人的邮件仍可能被隔离。

查看邮件详细信息

如果您需要除邮件发件人和主题以外的详细信息来确定邮件是否为垃圾邮件，您可以在查看完整邮件后对其执行操作。

程序

步骤 1　在垃圾邮件隔离区通知中，点击邮件的主题链接以显示“邮件详细信息”页面。

注　如果您已对邮件执行操作，此时会显示“找不到邮件”页面。

步骤 2　从下拉列表中选择要执行的操作。选项包括“放行”、“放行并添加至安全列表”和“删除”。

如果不执行任何操作，系统会在一定天数（请向管理员核实具体天数）后将邮件从隔离区删除。

步骤 3　点击**提交。**

步骤 4　在确认消息中，确认您预期的操作。

一次对多封邮件执行操作

程序

步骤 1　在垃圾邮件隔离区通知中，点击相应链接访问垃圾邮件隔离区。

步骤 2　选中您要对其执行操作的每封邮件旁的复选框。

步骤 3　从下拉列表中选择要执行的操作，然后点击**提交。**

如果不执行任何操作，系统会在一定天数（请向管理员核实具体天数）后将邮件从隔离区删除。

步骤 4　在确认消息中，确认您预期的操作。

访问安全列表和阻止列表

可以使用下列格式向安全列表和阻止列表中添加条目:

- `user@domain.com`
- `server.domain.com`
- `domain.com`

不能将发件人或域同时添加到安全列表和阻止列表。不过，如果您将某个域添加到安全列表并将该域中某个用户的邮箱地址添加到阻止列表（反之亦然），则设备会应用这两个规则。例如，如果您将 `example.com` 添加到安全列表，将 `george@example.com` 添加到阻止列表，则设备会发送来自 `example.com` 的所有邮件（而不进行垃圾邮件扫描），但发件人为 `george@example.com` 的邮件会被视为垃圾邮件。

无法使用以下语法允许或阻止某个范围的子域：`.domain.com`。但是，可以使用以下语法明确地阻止特定域：`server.domain.com`。

添加条目到安全列表和阻止列表

程序

步骤 1　在垃圾邮件隔离区通知中，点击相应链接访问垃圾邮件隔离区。

步骤 2　从**选项**下拉列表中，选择**安全列表**或**阻止列表**。

步骤 3　输入邮箱地址或域，然后点击**添加至列表**。

注　与安全列表条目不同，阻止列表条目只能在最终用户垃圾邮件隔离区中从“选项”菜单添加。

搜索隔离区中的邮件

程序

步骤 1　在垃圾邮件隔离区通知中，点击相应链接访问垃圾邮件隔离区。

步骤 2　在**搜索邮件**字段中，输入要搜索的条件，然后点击**搜索**。