配置ESA反垃圾邮件设置以改进垃圾邮件检测

目录

[简介](#)

[基本设置](#)

[启用SBNP](#)

[SBRS原理](#)

简介

本文档介绍如何提高思科邮件安全设备(ESA)反垃圾邮件效果并减少绕过过滤的垃圾邮件。

问题

垃圾邮件绕过ESA过滤，或未按预期由入站邮件策略进行处理。

环境

- 已启用反垃圾邮件功能且具有有效反垃圾邮件功能密钥的思科邮件安全设备(ESA)。
- 在单独的侦听程序上配置入站和出站邮件流（建议用于SenderBase设置）。
- 部署中可用的SenderBase信誉得分(SBRS)和SenderBase网络参与(SBNP)。

分辨率

完成以下部分中的步骤以验证反垃圾邮件操作、确认扫描、调整阈值以及优化SBRS和邮件流策略。

原因

- 禁用反垃圾邮件、缺少功能密钥或规则更新不是最新更新。
- 由于允许列表、邮件过滤器或扫描大小限制，邮件绕过扫描。
- 允许主机访问表(HAT)策略或SBRS阈值。
- 垃圾邮件数量随着时间的推移而增加。

设置

过程 1:验证是否已启用反垃圾邮件

1. — 确保所有邮件交换(MX)记录（包括优先级较低的MX记录）通过ESA转发邮件。

2. — 验证设备是否具有有效的反垃圾邮件功能密钥。

3. — 确保为所有适当的传入邮件策略启用反垃圾邮件。

过程 2:验证反垃圾邮件规则更新

导航到安全服务(Security Services)>反垃圾邮件(Anti-Spam)，并验证最近的规则更新时间戳是否在最近2小时内。

过程 3:验证邮件是否被反垃圾邮件扫描

1. — 检查标题X-IronPort-Anti-Spam-Result的未命中垃圾邮件示例：

2. — 如果缺少报头，请完成以下检查：

- 确认没有允许列表条目或过滤器会绕过垃圾邮件扫描。
- 验证邮件是否由于最大邮件扫描大小（默认值为262144字节）而绕过扫描。
- 检查每个主机访问表(HAT)条目，并确认已为入站邮件流策略设置spam_check=on。
- 检查邮件过滤器并验证除非需要，否则没有过滤器使用skip-spamcheck。
- 使用最近的垃圾邮件示例（时间、日期、收件人）并查看mail_logs以确认Anti-Spam返回了否定判定。

过程 4:验证垃圾邮件阳性邮件的操作

检查入站邮件策略，并确认在默认策略中丢弃或隔离了垃圾邮件和疑似垃圾邮件，并且其他策略会继承默认行为或故意覆盖默认行为。

过程 5:调整垃圾邮件阈值（可选）

1. — 当误报在某一阈值可接受时，将垃圾邮件正阈值降低至80（默认值为90）。

2. — 当可疑阈值可接受的误报时，将可疑垃圾邮件阈值降至40（默认值为50）。

3.当投诉仅限于一部分收件人时，为阈值较低的收件人创建单独的邮件策略。

过程 6:优化SBRS设置和HAT策略

1. — 根据组织对误报的容忍度，调整阻止列表和可疑发件人组的SBRS范围。

2. — 当策略需要更严格的验证时，将SBRS none添加到使用受限策略的可疑发件人组。

3. — 将限制策略每小时的最大收件人数设置为5。

4. —（可选）为不同的SBRS范围创建具有不同每小时收件人限制的多个受限策略。

过程 7:为受限邮件流启用发件人验证

1. — 当策略需要更严格的验证时，请将域名系统(DNS)不存在或配置不当的发件人添加到可疑发件人组。

2. — 考虑单独的邮件流策略，该策略返回自定义4xx响应，指示邮件被拒绝的原因。

过程 8:启用LDAP接受和目录搜集攻击保护

1. — 启用轻量级目录访问协议(LDAP)接受以减少发送到无效收件人的垃圾邮件。

2. — 如果已启用LDAP接受，请为每个入站侦听程序配置目录搜集攻击保护(DHAP)，每个IP的最大无效尝试次数介于5到10之间。

过程 9:启用内容词典（可选）

ESA包括两个内容词典：profanity.txt和sexual_content.txt。仅在需要时应用这些字典，因为它们可能会增加误报。

过程 10:报告错误分类邮件

将误报和漏报提交到Cisco TAC进行分析。

过程 11:禁用出站扫描的SBRS

启用SBNP

1. — 确保入站和出站邮件位于不同的侦听程序上。

2. — 禁用出站邮件的SenderBase查找。导航到Network > Listeners。选择出站侦听器。单击Advanced。清除Use SenderBase IP profiling复选框。

SenderBase网络参与(SBNP)可以提高信誉过滤器、反垃圾邮件和病毒爆发过滤器的效率。启用反垃圾邮件后，SBNP对性能没有明显影响，并且是安全的。



注意：您的组织收到的垃圾邮件数量随时间而变化。可能更多垃圾邮件通过ESA，只是因为组织收到的垃圾邮件比过去更多。通过查看“传入邮件概述”(Incoming Mail Overview)页面并添加通过信誉过滤拦截的邮件和检测到的垃圾邮件行项目，在一段时间内跟踪此行为。

SBRS原理

误报的主要问题是重要电子邮件可能会丢失。在这种情况下，隔离或丢弃垃圾邮件的邮件可能会带来问题。如果合法电子邮件被发送到隔离区或垃圾邮件文件夹，则需要主动搜索以识别合法电子邮件被错误分类为垃圾邮件。

相反，阻止列表和速率限制电邮的方式是立即通知发件人。如果此发件人不是垃圾邮件发送者，则此发件人可能会找到其他联系方式。事实上，作为一项整体策略，默认阻止然后根据请求接受受信任的合作伙伴，对于某些企业而言是更好的选择。

如果设置得当，限制很少会对合作伙伴产生影响，但会提供保护，防止域感染病毒。限制也让垃圾邮件发送者感到不快。已知的一种垃圾邮件制造者技术是，购买大量IP，生成足够好的电子邮件以得到不错的SBRS得分，然后开始发送垃圾邮件。较大的可疑列表范围会捕获垃圾邮件，限制其造成的损害，最终可能导致它们停止向您的域发送垃圾邮件。

相关内容

- 如何确定SenderBase信誉得分(SBRS)？它们是什么意思？

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。