思科邮件安全设备(ESA)反垃圾邮件效力检查表

目录

简介

以下程序和建议是减少通过ESA的垃圾邮件数量的“最佳实践”。请注意，每个客户都不同，其中一些建议可能会增加分类为垃圾邮件的合法电子邮件数量（误报）。

基本设置

1. 确保已打开反垃圾邮件：

   检查以确保所有MX记录（包括较低优先级）MX记录通过ESA中继邮件。确保您的设备具有有效的反垃圾邮件功能密钥。确保为所有适当的传入邮件策略启用反垃圾邮件。

2. 确认您正在接收反垃圾邮件规则更新。检查以确认Security Services > Anti-Spam下更新的最新时间戳是否来自最近2小时内。

3. 确保邮件正被反垃圾邮件扫描：

   检查以下信头的未接垃圾邮件示例：X-IronPort-Anti-Spam-Result:如果缺少该报头：

   检查以确保没有任何允许列表条目或导致垃圾邮件绕过垃圾邮件扫描的过滤器（请参阅下文）。检查以确保邮件不会绕过扫描，因为它们超过了最大邮件扫描大小(默认为262144字节)。减少此设置不会大大提高性能，并且可能导致漏掉垃圾邮件。在评估期间，还必须确保IPAS设置与测试的任何其他产品相同。浏览每个HAT条目，确认所有入站邮件流策略的“spam_check=on”。只要默认设置为“spam_check= on”，且没有任何邮件流策略明确将其关闭，则此配置就正确。请特别注意TRUSTED/allowLIST设置。通常，当客户无意中将发件人添加到其允许列表中以转发垃圾邮件时，例如，通过添加将垃圾邮件和合法邮件转发到allowLIST发件人组的ISP或合作伙伴的域。

   快速检查邮件过滤器，确保没有“跳过垃圾邮件检查”的过滤器。 如果有，请确保他们正在执行应该执行的操作（请记住，匹配一个rcpt-to可以匹配包含30个以上收件人的邮件）。

   查找最近的垃圾邮件示例（时间、日期、rcpt等），并参考mail_logs查看发生的情况。确认反垃圾邮件返回了否定判定。

4. 确保您对垃圾邮件肯定邮件采取所需操作。检查入站邮件策略，了解如何处理反垃圾邮件判定。确保在默认策略中丢弃或隔离SPAM肯定邮件和可疑邮件，并确保所有其他策略使用默认行

为或故意覆盖默认。

5. 如果误报比漏报的垃圾邮件更不令人担心，请应用更严格的垃圾邮件阈值：

   如果误报在“特定”阈值上不引起关注，请将垃圾邮件正阈值降至80（默认为90）。

   如果误报在“可疑”阈值中不存在，则将可疑垃圾邮件阈值降至40（默认为50）。

   如果您的大多数垃圾邮件投诉来自收件人的子集，则可以为具有较低垃圾邮件阈值的这些用户创建单独的邮件策略，以便更积极地过滤仅针对这些收件人。

   这些价值观的变化不应轻视，也不应在没有任何硬数据的情况下实施，以确定其将产生何种复习效果。

   此外，不一定只为了避免误报而调整另一个方向的值。请确保将误报和漏报提交给TAC。

6. 优化SBRS设置和HAT策略：

   大多数组织都乐于将SBRS -10到–3.0添加到其阻止列表，将SBRS -3.0到–1.0添加到其SUSPECTLIST。更积极的客户可以阻止SBRS -10到–2.0，并将–2.0添加到–0.6到SUSPECTLIST。

   在某些情况下，发件人尚未拥有SenderBase信誉得分这一事实表明此发件人可能是垃圾邮件发送者。您可以直接将SBRS“none”添加到获得“Throttled”策略的发件人组，例如，添加到SUSPECT发件人组。

   将“Throttled”策略的每小时最大收件人数更改为5。

   考虑创建多个“限制”策略以强制实施不同收件人每小时的限制 — 例如，SBRS介于–2和–1之间的发件人速率限制为每小时5个收件人，而SBRS介于–1和0到每小时20个收件人的发件人速率限制。

7. 为“Throttled”邮件流策略启用发件人验证：

   客户可以选择将DNS不存在或配置不正确的发件人添加到SUSPECTLIST发件人组。

   DNS中不存在连接主机PTR记录。由于临时DNS故障，连接主机PTR记录查找失败。

   连接主机反向DNS查找(PTR)与正向DNS查找(A)不匹配。

   对于配置错误的DNS，发送方可能存在误报的风险，因此客户可能希望设置单独的邮件流策略，该策略返回自定义4xx响应，指示邮件被拒绝的原因。

   有关发件人验证的详细信息，请参阅联机帮助或AsyncOS用户指南

8. 启用LDAP接受和目录搜集攻击保护：

   许多垃圾邮件发送者将电子邮件发送到大量无效地址，因此阻止发送到无效收件人的发件人也

可以减少垃圾邮件。

如果LDAP接受已启用，请确保为每个入站侦听程序配置目录搜集保护(DHAP)，每个IP的最大无效尝试数在5到10之间。

9. 启用内容词典：

   您的ESA附带两个内容词典：profanity.txt和semor_content.txt。虽然使用这些字典可能会产生误报，但一些客户发现，过滤其邮件流中是否存在不恰当的词语可能会降低“错人”收到“错误邮件”的风险。 这些过滤器只能通过在特定邮件策略中为一组用户启用来应用于“吱吱作响的轮子”。

10. 向思科TAC报告错误分类的邮件。

11. 为防止大量误报，应禁用SBRS进行出站扫描。这是因为SBRS会查看传入IP的信誉，而在内部网络中，这些IP中的大多数是动态的。按照下一节中的步骤操作。

启用SBNP

1. 确保入站和出站邮件位于单独的侦听程序上。

2. 按下面的内容禁用出站电子邮件的SenderBase查找。要从GUI执行此操作，请转到网络(Network)>侦听程序(Listeners)，选择任何出站侦听程序，选择“高级”(Advanced)，并取消选中“使用SenderBase IP分析”(Use SenderBase IP profiling)旁边的框。

   SenderBase网络参与(SBNP)可以显着提高信誉过滤器、反垃圾邮件和病毒爆发过滤器的效力。如果在使用反垃圾邮件时启用SBNP，SBNP也不会对性能产生显着影响，并且安全性高。

   注意：您的组织收到的垃圾邮件数量会随着时间的推移而改变。可能更多垃圾邮件通过ESA，这仅仅是因为您收到的垃圾邮件比过去多。您可以通过查看“传入邮件概述”(Incoming Mail Overview)页面并添加“由信誉过滤拦截”(stopped by reputation filtering)和“检测到垃圾邮件”(spam messages detected)行项目来跟踪此行为。

SBRS原理

误报的主要问题是，重要邮件可能会丢失。在这种情况下，隔离或丢弃垃圾邮件阳性邮件的做法是有问题的。如果将合法电子邮件发送到隔离区或垃圾邮件文件夹，则需要主动搜索才能进入并“注意”火腿被错误分类为垃圾邮件。

相反，阻止列表和速率受限的电子邮件被阻止，以便发送方立即收到通知。如果此发件人不是垃圾邮件发送者，他们可能会找到其他方法与您联系。事实上，作为一项总体政策，默认情况下阻止，然后接受受信任的合作伙伴的请求，对某些企业来说是更好的选择。

如果设置得当，限制极少会影响合作伙伴，但会提供针对感染病毒的域的保护。限制也会对垃圾邮件发送者不利。我们了解到垃圾邮件发送者技术，它可以购买大量IP，生成足够的“好”电子邮件，以获得良好的SBRS分数，然后开始发送垃圾邮件。更大的可疑列表范围应捕获这些内容，限制它们所造成的损害，并可能最终导致它们停止向您的域发送垃圾邮件。