思科电子邮件安全工具(ESA)反垃圾邮件效力清单

目录

以下步骤和建议是“最佳实践”减少的垃圾邮件获得通过ESA的相当数量。注意每客户不同的，并且其中一些建议可能增加作为垃圾邮件分类的合法电子邮件数量(错误肯定)。

基本设置

1. 确保反垃圾邮件打开：

   检查确保，所有您的MX记录(包括较低优先级) MX记录通过ESAs中继邮件。确保您的设备有一个有效反垃圾邮件功能键。保证反垃圾邮件为所有适当的流入的邮件策略启用。

2. 验证您接收反垃圾邮件规则更新。检查确认更新的最**最近的**时间戳在安全服务>反垃圾邮件下是从最后2个小时的内部。

3. 确保消息由反垃圾邮件扫描：

   检查未接垃圾邮件消息示例以下报头：X IronPort反垃圾邮件结果：如果该报头未命中：

   检查确保您没有造成垃圾邮件的任何Whitelist条目或过滤器绕过垃圾邮件扫描(如下所示)。检查确保，消息不绕过扫描，因为他们超出最大数量消息扫描大小(默认是262144个字节)。减少此设置不非常地改进性能，并且能导致未接垃圾邮件。在评估时，确保IPAS设置是作为测试的其他产品的相同的也是重要的。通过每个帽子条目并且确认“spam_check=on”所有入站邮件流策略的。只要默认没有“在”和邮件流量策略明确地的spam_check=关掉，这适当地配置。注意特别注意TRUSTED/WHITELIST设置。通常计时客户疏忽地添加发送方到例如通过添加ISP或合作伙伴域转发垃圾邮件-，转发垃圾邮件并且使电子邮件合法给WHITELIST发送方组的他们的Whitelist。

   通过消息过滤器进行快速检查确保那里不是“跳过spamcheck”的所有过滤器。如果有，请确保他们执行什么他们应该(记住匹配单个rcpt对在消息能的那配比用30+收件人)。

   查找一最近的垃圾邮件示例(时刻、日期、rcpt等等)，并且参考mail_logs发现发生什么。确认反垃圾邮件返回一个负判决。

4. 确保您采取在垃圾邮件正消息的所需的动作。检查入站邮件策略反垃圾邮件判决如何被处理。确保垃圾邮件正，并且可疑的消息在默认策略丢弃或被检疫，并且那其他策略使用默认行为或故意地改写默认。

5. 如果错误肯定比未命中的垃圾邮件，是无足轻重注意事项请应用更加积极的垃圾邮件阈值：

   使正垃圾邮件阈值降低到80 (默认是90)，如果错误肯定不是注意事项在‘特定的’阈值。

   使怀疑的垃圾邮件阈值降低到40 (默认是50)，如果错误肯定不是注意事项在‘可疑的’阈值。

   如果大多您的垃圾邮件投诉来自收件人的一子集，您能创建这些用户的一项分开的邮件策略以更低垃圾邮件阈值为了为这些收件人积极地过滤。

   不应该应该轻微采取对这些值的更改，亦不他们立法没有任何硬数据查明什么repurcussive作用将是。

   并且，不一定请调整在另一个方向的值只避免错误肯定。请确保错误肯定和假攻击提交对TAC。

6. 优化您的SBRS设置和帽子策略：

   多数组织是对他们的黑名单的方便的添加的对他们的SUSPECTLIST的SBRS -10到-3.0和SBRS -3.0到1.0。更加积极的客户能列入黑名单SBRS -10到-2.0和加-2.0到-0.6到SUSPECTLIST。

   有时，事实发送方没有SenderBase名誉斯克尔是证据此发送方可能是垃圾邮件发送者。您能添加SBRS “无”直接地到获得“被节流的”策略的发送方组，例如到您可疑的发送方组。

   更换收件人最大数每个小时到5 “被节流的”策略的。

   例如考虑创建超过一项“被节流的”策略强制执行每小时限额的另外收件人-有SBRS的速率限制发送方在每个小时-2和-1到5有SBRS的收件人和发送方之间在每个小时-1和0到20收件人之间。

7. 启用“被节流的” Mailflow策略的发送方验证：

   客户可能选择添加发送方用不存在或不正确地配置的DNS对SUSPECTLIST发送方组。

   连接主机PTR记录在DNS不存在。连接主机PTR记录查找出故障由于临时DNS失败。

   连接主机逆向DNS查找(PTR)不匹配向前DNS查找(a)。

   有错误肯定某种风险从发送方的用不正确的配置的DNS，因此客户可能要设置返回指示自定义4xx的答复的一项分开的Mailflow策略原因消息拒绝。

   检查在线帮助或AsyncOS用户指南关于发送方验证的更多信息

8. Enable (event) LDAP接受和目录收获攻击保护：

   许多垃圾邮件发送者发送电子邮件到无效的地址大量，如此阻塞发送到无效收件人能也减小垃圾邮件的发送方。

如果LDAP接受已经是，确保目录收获保护(DHAP)为有最大无效尝试的每入站监听程序也配置在5和10之间每个IP。

9. Enable (event)内容字典：

   您的ESA附有两个内容字典：profanity.txt和sexual_content.txt。当曾经这些字典可能生成错误肯定时，一些客户发现过滤他们的不相应的词的邮件数据流可能减小”获得“错误的电子邮件的”“错误的人的风险。这些过滤器可能只应用到“尖叫的轮子”通过启用他们为用户的一组一项特定邮件策略的。

10. 报告对Cisco TAC的被错误分类的消息。

11. 要防止很大数量的错误肯定，应该为出站扫描禁用SBRS。这是因为SBRS查看流入IP的名誉，并且在内部网络，大多这些IP动态。遵从在下一部分的步骤。

启用SBNP

1. 确保入站，并且出站邮件在独立的监听程序。

2. 禁用出站电子邮件的SenderBase查找每下面。从GUI执行此，去网络>监听程序，选择任何出站监听程序，在“使用描出SenderBase的IP旁边选择"Advanced"和非选定方框”。

   SenderBase网络参与(SBNP)能极大增加名誉过滤器、反垃圾邮件和病毒爆发过滤器的效果。SBNP也没有显而易见的性能影响，如果已启用，当曾经反垃圾邮件时并且高度安全。

注意您的组织接收的音量垃圾邮件将随着时间的推移更改。很可能，更多垃圾邮件通过ESAs获得完全由于这样的事实您比以前接收更多垃圾邮件。您能通过查看流入的邮件概述页随着时间的推移跟踪此行为，并且添加“路过的名誉过滤”和“请发送消息到新闻组消息检测的”行项目。

SBRS基本原理

大关心错误肯定是重要电子邮件可能获得丢失。在此上下文，检疫或丢弃垃圾邮件正电子邮件实践是有问题的。如果一合法电子邮件被发送到检疫或垃圾邮件文件夹，要求一积极的搜索参加，并且“请注意”火腿被错误了分类作为垃圾邮件。

相反，黑名单和速率限制电子邮件阻塞，在这种情况下发送方立即通知。如果此发送方不是垃圾邮件发送者，他们可能将查找另一个方式做与您的联系方式。实际上，作为一项整体策略，阻塞默认情况下应要求然后接受委托合作伙伴，是一些企业的一个更加好的位置。

限制，如果适当地设置，很少请应该，如果影响成为伙伴，但是提供从获得被病毒传染的域的防护。throttling也将是反感对垃圾邮件发送者。我们知道垃圾邮件发送者技术采购很大数量的IP，生成足够的"good"电子邮件获得一个正派SBRS分数然后开始滥发。一个更大的可疑的列表范围应该捉住他们造成的这些，限制损害，并且可能最终造成他们停止发送垃圾邮件到您的域。