ESA上的常见配置错误

目录

简介

本文档介绍邮件安全设备(ESA)上的常见配置错误。

ESA上常见的配置错误有哪些？

无论您是设置新评估还是查看现有配置，您都可以参阅此常见配置错误核对表。

HAT

- 请勿将+5或+7等正SBRS得分放入ALLOWLIST。9.0-10.0范围可以，但如果分数较低，垃圾邮件更有可能通过。
- 除非您确实需要并了解这些，否则禁用UNKNOWNLIST、信封发件人DNS验证和连接主机DNS验证。
- 不更改每个邮件流策略中的邮件大小和其他策略设置，而是转到邮件流策略菜单并选择最后一个选项“默认策略参数”。
- 对于大多数发件人，将最大连接数限制为3，并将此设置为新邮件流策略的默认值。
- 检查阻止列表中是否包含从–10.0到–2.0的SenderBase分数。文档和设置向导过于保守；目前此范围内没有误报。

策略

- 根据谁获得策略，而不是策略所执行的操作来命名策略。在内容过滤器执行的操作后命名任何内容过滤器，并使用缩写，如Q_basic_attachments、D_spookers、Strip_Multi-Media，其中Q表示隔离，D表示丢弃。
- 非默认策略应为反垃圾邮件、防病毒、内容过滤器和爆发过滤器使用默认设置，但您确实需要特殊设置的除外。如果不需要，请勿在每个策略中重新创建这些设置。
- 取消勾选“删除受感染的附件”，否则，您将在许多已删除病毒的空白邮件中传递。
- 出站的防病毒设置应通知发件人，而不是收件人
- 应在出站时禁用爆发过滤器和反垃圾邮件

传入中继

如果“监控>概述”显示来自您自己的服务器和域的连接，则需要将其添加到传入中继设置。使用GUI时，一个非常常见的错误是认为您在将条目添加到表中时启用了传入中继功能。此外：

- 在ALLOWLIST上方为其添加特殊的HAT发件人组以用于报告目的。 选择无速率限制或DHAP，但垃圾邮件和病毒检测正常。
- 添加邮件过滤器以匹配BLOCKLIST策略操作。例如：

```
Drop_Low_Reputation_Relayed_Mail:
if reputation <= -2.0
{ drop();}
```

在极少数情况下，您会重新注入电子邮件（例如，通过入站邮件策略重新处理订户间邮件），您的过滤器还需要免除重新注入接口。通常不需要这样做。

DNS

许多客户强制ESA查询其内部DNS服务器，这是出于习惯。在大多数安装中，我们需要的DNS记录100%都在Internet上，而不是在内部DNS中。查询Internet根服务器更有意义，可减少内部DNS的转发负载。

邮件和内容过滤器

最常见的错误是将匹配条件置于不需要的内容过滤器中。 大多数过滤器应列出一些操作，但条件应留空。过滤器将始终为true，并且始终运行。您可以根据需要创建新的传入或传出邮件策略，并将此过滤器应用于策略，从而控制哪些用户/策略接收这些操作。以下是不正确且正确的示例：

- 在邮件过滤器中使用rcpt-to条件几乎总是一个错误。正确的步骤是编写传入内容过滤器，并通过添加基于收件人的传入邮件策略使其针对特定用户。
- 对附件是否存在进行内容过滤器测试，然后删除附件几乎总是一种错误。正确的方法是始终丢弃该附件，而不测试其存在。
- 使用deliver()几乎总是一个错误。 “传送”是指跳过任何剩余的过滤器，然后传送。如果只想在不跳过其余过滤器的情况下传送，则无需执行任何明确操作（隐含传送）。

开放中继保护

某些服务将检查消息传输代理(MTA)是否接受可能导致中继条件打开的地址。由于将MTA保留为正常的开放中继是不好的，因此这些站点可能会将您添加到阻止列表，除非您在SMTP会话中拒绝这些危险地址。

在ALLOWLIST上方为其添加特殊的HAT发件人组以用于报告目的。选择不限速或DHAP，但允许垃圾邮件和病毒检测。

- 更改为严格地址解析（默认为Loose）。 这是防止地址中出现双@符号的必要条件。
- 拒绝（非删除）无效字符。这也是防止地址中出现双@符号的必要条件。
- 拒绝（不接受）文字，并输入以下字符：*%!\\/?

相关信息

- 技术支持和文档 - Cisco Systems