在ESA的常见配置错误

目录

简介

本文描述在电子邮件安全工具(ESA)的常见配置错误。

什么是在ESA的常见配置错误？

您是否设置一个新的评估或在现有配置查找，您能参考常见配置错误此清单。

1. 帽子

- 请勿放正SBRS分数类似+5或+7到WHITELIST。范围9.0-10.0是好的，但是包括更低分数更可能只将使它垃圾邮件将通过。
- 除非真需要并且了解这些，请禁用UNKNOWNLIST，信封发送方DNS验证和连接主机DNS验证。
- 而不是更改消息大小和其他策略设置在每项邮件流量策略，去邮件流量Policies菜单并且选择最后一个选项，“默认策略参数”。
- 限制最大连接到三多数发送方的，并且做这新的邮件流量策略的默认。
- 检查从-10.0的SenderBase分数到-2.0在黑名单包括。文档和设置向导结束保守的;我们当前没有错误肯定在此范围。

2. 策略

- 在谁以后的命名策略获得他们，没有什么他们。所有内容过滤器以什么命名他们执行，并且请使用简称类似Q_basic_attachments， D_spoofers， Strip_Multi-Media，问含义检疫和D含义丢弃。

- 非默认策略如果“请使用默认设置”反垃圾邮件、Anit病毒、内容过滤器和爆发过滤器，除了您真需要特殊设置的地方。如果不是必要的，请勿再创在每项策略的那些设置。

- Untick “丢弃传染了附件”或者您将通过剥离病毒的许多空白电子邮件。

- 出站的抗病毒设置应该通知发送方，不是收件人

- 在出站应该禁用爆发过滤器和反垃圾邮件

3. 流入中继

如果“监视器>概述”表示从您自己的服务器和域的连接，您需要添加他们对流入中继设置。一个非常常见错误，当使用GUI时，是认为您启用流入中继功能，当您执行时的所有是添加条目到表。另外：

- 添加他们的一特殊帽子发送方组，在WHITELIST上，为报告目的。 请勿选择速率限制或DHAP，然而发送消息到新闻组，并且病毒检测是好的。

- 添加一个消息过滤器匹配您的黑名单策略操作。例如：

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

偶然地您再注入电子邮件的地方(例如，重新处理相互用户邮件通过入站邮件策略)，您的过滤器也将需要豁免reinjection接口。通常这不是必要的。

4. DNS

许多客户强制ESA查询他们的内部DNS服务器在习惯外面。在多数安装中，我们需要的100% DNS记录在互联网，不内部DNS的。它有更多意义查询互联网根服务器，减少在内部DNS的转发负载。

5. 消息和内容过滤器

多数常见错误是放置匹配情况在他们没有要求的内容过滤器。 多数过滤器应该列出一些操作，但是情况应该是左空白。过滤器永远将是*真的*和永远运行。用户/策略通过创建新建的流入或流出的邮件策略接收这些操作当必要时的您控制，和应用此过滤器对策略。这是不正确和正确示例：

- 它几乎总是使用的错误rcpt对情况在消息过滤器。正确步骤是写入一个流入内容过滤器，并且使特定为特定用户通过添加一项基于收件人的流入的邮件策略。

- 它几乎总是有的错误附件的出现的内容过滤器测验，然后丢弃附件。正确方法将总是丢弃该附件，没有测试对于其在线状态。

- 它几乎总是使用deliver()的错误。传送含义跳过剩余过滤器，然后传送。如果要传送，无需跳过过滤器的其余，明确操作没有要求(暗示请传送)。

7. 打开中继预防

某些服务将检查发现您的消息传输代理(MTA)是否接受可能潜在导致开放中继情况的地址。因为留下您的MTA作为一个作用的开放中继是坏的，这些站点可能添加您到黑名单，除非拒绝在SMTP会话的这些危险地址。

添加他们的一特殊帽子发送方组，在WHITELIST上，为报告目的。请勿选择速率限制或DHAP，然而允许垃圾邮件和病毒检测。

- 更改对严格地址解析(宽松是默认)。这是必要防止双@签到地址。

- 拒绝(不是小条)无效的字符。这也是必要防止双@签到地址。

- 拒绝(不接受)字面值，并且输入以下字符：*%! \ \/ ?

相关信息

- 技术支持和文档 - Cisco Systems