ESA电子邮件加密配置示例

目录

简介

本文描述如何设置在电子邮件安全工具(ESA)的电子邮件加密。

先决条件

本文档中的信息基于以下软件和硬件版本：

- 型号：所有C系列和X系列
- 信封安装的加密(PostX)功能

配置

启用在ESA的电子邮件加密

完成从GUI的这些步骤：

1. 在安全服务下，请选择**思科IronPort电子邮件加密>enable电子邮件加密**，并且单击**编辑设置**。
2. 单击**添加加密配置文件**为了创建一新的加密配置文件。
3. 选择**思科注册的信封服务**或**思科IronPort加密设备**(如果加密设备采购)关键服务服务类型的。
4. 单击**提交并且确认更改**。
5. 在加密配置文件创建后，您给选项设置它到思科的注册的信封服务(茨雷斯岛)服务器。提供按钮应该在新配置文件旁边显示。点击**提供**。

创建流出的内容过滤器

完成从GUI的这些步骤为了创建一个流出的内容过滤器实现加密配置文件。 在以下示例中，过滤器将触发所有出局信息的加密与字符串“巩固：”在附属的报头：

1. 根据邮件策略，请选择流出的内容过滤器，并且单击**添加过滤器**。
2. 添加一个新的过滤器以附属的报头的情况，附属的== “巩固：”并且Encrypt的操作和当前传送(最后的行动)。单击 **submit**。
3. 根据邮件策略，请选择流出的邮件策略，并且启用此在默认邮件策略或适当的邮件策略的新的过滤器。
4. 确认更改。

验证

此部分描述如何验证加密工作。

1. 为了验证，请生成与**安全的**新的邮件：在主题和请发送电子邮件对Web帐户(Hotmail，Yahoo， Gmail)为了确定是否加密。
2. 检查邮件日志正如下一部分所描述为了保证消息通过流出的内容过滤器加密。

验证处理在Mail_logs的加密过滤器

这些mail_log条目显示消息匹配呼叫Encrypt_Message的加密过滤器。

```
Wed Oct 22 17:06:46 2008 Info: MID 116 was generated based on MID 115 by encrypt
filter 'Encrypt_Message'
Wed Oct 22 17:07:22 2008 Info: MID 118 was generated based on MID 117 by encrypt
filter 'Encrypt_Message'
Wed Oct 22 17:31:21 2008 Info: MID 120 was generated based on MID 119 by encrypt
filter ''Encrypt_Message
```

如此部分所显示，参考的ESA消息处理确定关于关于如何的说明使用**grep**或**findevent**命令为了收集信息从日志。

故障排除

如果加密过滤器不触发，请检查邮件日志测试消息使用的邮件策略。确保过滤器启用在此邮件策略，并且那那里是在与**跳过余留内容**过滤器操作的此策略启用的没有上一个过滤器。

保证在消息跟踪的消息使用正确字符串或选定的附属标记为了触发加密通过内容过滤器。