如何为垃圾邮件隔离区服务启用ESA和SMA之间的TLS

目录

简介

本文档介绍如何在邮件安全设备(ESA)和安全管理设备(SMA)之间为垃圾邮件隔离区服务启用传输层安全(TLS)。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

请注意，此功能不是官方支持的功能，因此，在集成该功能时，您可以按照下一说明完成此任务，并为此创建一些增强请求。

配置

1. 使用未屏蔽的密码从SMA下载最新的配置文件。
2. 在文本编辑器中打开配置文件。
3. 在配置**文件中找**到euq_listener:

4. 向下滚动几行，直到找到默认HAT设置的部分：

值0表示TLS已关闭，未提供STARTTLS。值1表示首选TLS，值2表示需要TLS。

5. 将值更改为例如1，保存配置文件，然后再次将其上传到SMA。
6. 在ESA上，导航至**Mail Policies > Destination Controls，**然后为域添加新条目：.euq.queue，选择**TLS Support Preferred**。
7. 通过从ESA到端口6025上的SMA IP运行手动telnet测试，验证是否提供了STARTTLS

注意：the.euq.queue是最终用户隔离区的传送队列的特殊名称。

当邮件发送到集中垃圾邮件隔离区时，ESA现在应尝试建立TLS连接并通过加密的SMTP会话传送邮件。