How to Enable TLS between ESA and SMA for Spam Quarantine Service

Contents

Introduction

This document describes how to enable Transport Layer Security (TLS) between Email Security Appliance (ESA) and Security Management Appliance (SMA) for Spam Quarantine Service.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Note that this is not an official supported feature hence you can follow the next instructions to accomplish this task while the feature gets integrated, there are some enhancement requests created for this purpose.

Configure

1. Download the latest configuration file from your SMA with unmasked passwords.
2. Open the configuration file in a text editor.
3. Locate the **euq_listener** in the configuration file:

```
<listener_name>euq_listener</listener_name>
```
4. Scroll down a few lines until you find the section for the default HAT settings:

```
<hat_default_tls>0</hat_default_tls>
```
A value of 0 represents that TLS is turned off, no STARTTLS is offered. A value of 1 indicates TLS to be preferred, and a value of 2 represents TLS required.

5. Change the value to for example 1, save the configuration file and upload it again to the SMA.
6. On the ESA, navigate to **Mail Policies > Destination Controls,** and add a new entry for domain: the.euq.queue, select **TLS Support Preferred**.
7. Verify that STARTTLS is offered by running a manual telnet test from your ESA to the SMAs IP on port 6025

   Note: the.euq.queue is a special name for the delivery queue to the end-user quarantine.

When a message is sent to the Centralized Spam Quarantine, the ESA should now try to establish a TLS connection and deliver the message with an encrypted SMTP conversation.