ESA Email Encryption Configuration Example

Document ID: 117863

Contributed by Kevin Luu, Robert Sherwin, and Andreas Mueller, Cisco TAC Engineers.
Jun 26, 2014

Contents

Introduction

This document describes how to set up email encryption on the Email Security Appliance (ESA).

Prerequisites

The information in this document is based on these software and hardware versions:

- Model: All C−Series and X−Series
- Envelope Encryption (PostX) Feature installed

Configure

Enable Email Encryption on the ESA

Complete these steps from the GUI:

1. Under Security Services, choose ***Cisco IronPort Email Encryption > Enable Email Encryption***, and click ***Edit Settings***.

2. Click ***Add Encryption Profile*** in order to create a new Encryption Profile.

3. Choose ***Cisco Registered Envelope Service*** or ***Cisco IronPort Encryption Appliance*** (if the Encryption Appliance is purchased) for the Key Service Type.

4. Click ***Submit and Commit Changes***.

5. After the Encryption Profile has been created, you are given the option to Provision it to the Cisco's Registered Envelope Service (CRES) server. A Provision button should display next to the new profile. Click ***Provision***.

Create an Outgoing Content Filter

Complete these steps from the GUI in order to create an outgoing content filter to implement the Encryption Profile. In the following example, the filter will trigger encryption for any outgoing message with the string "Secure:" in the subject header:

1. Under Mail Policies, choose the Outgoing Content Filters, and click ***Add Filter***.
2. Add a new filter with condition of Subject Header as subject == "Secure:" and action of Encrypt and Deliver Now (Final Action). Click ***Submit***.
3. Under Mail Policies, choose the Outgoing Mail Policies, and enable this new filter in the default mail policy or the appropriate mail policies.
4. Commit changes.

Verify

This section describes how to verify that encryption works.

1. In order to verify, generate a new mail with ***Secure:*** in the subject and send the email to a web account (Hotmail, Yahoo, Gmail) in order to determine if it is encrypted.
2. Check the mail logs as described in the next section in order to ensure that the message is encrypted via the Outgoing Content Filter.

Validate Encryption Filter Processing in the Mail_logs

These mail_log entries show that the messages matched the encryption filter called Encrypt_Message.

```
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
```

Refer to ESA Message Disposition Determination for instruction on how to use the ***grep*** or ***findevent*** commands in order to gather information from the logs as shown in this section.

Troubleshoot

If the encryption filter does not trigger, check the mail logs for the mail policy the test message uses. Make sure the filter is enabled in this mail policy, and also that there is no previous filter enabled in this policy with a ***Skip Remaining Content Filters*** action.

Ensure that the message(s) in message tracking use the correct string or designated subject tagging in order to trigger encryption through the content filter.

Updated: Jun 26, 2014 Document ID: 117863