How do I bypass encryption in a content filter and DLP?

TAC **Document ID: 118560**

Contributed by Cisco TAC Engineers.
Oct 13, 2014

Contents

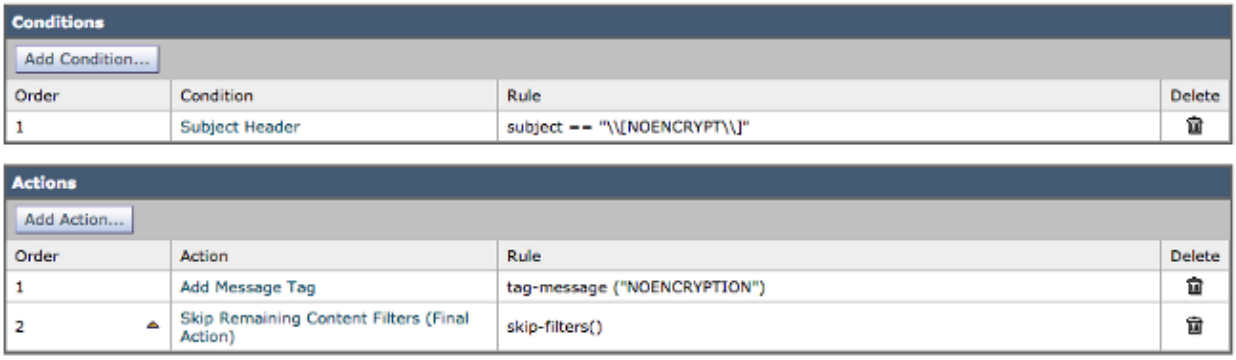
Introduction

This document describes how to bypass encryption in a content filter and DLP.

How do I bypass encryption in a content filter and DLP?

On the Cisco Email Security Appliance (ESA), you have an environment that is required to encrypt based on a subject field and DLP policy. There are instances that you want to bypass both encryption triggers for a message.

1. Create an outgoing content filter that precedes the one that does encryption. From the GUI ***Mail Policy > Outgoing Content Filters > Add Filters...***
2. The condition will be to look for the keyword "[NOENCRYPT]" in the subject. Choose ***Add Condition...*** and select ***Subject Header***, with "Contains" \[NOENCRYPT\]. (The "\" are for the literal use of "[", so please enter them.)
3. The first actions is to "Add message−tag" and it's value is "NOENCRYPTION." (This will be used in the DLP policy steps later).
4. Finally the last action is to "Skip Remaining content filters (Final Action)." (Note, this filter and the encrypt filter should be the last two in the order list and this filter precedes the encrypt content filter.) This should look similar to:



5. Submit and Commit your changes at this point.
6. From the GUI ***Mail Policies > Outgoing Mail Policies***, click on content filter (enable if disabled) and put a check mark for your new content filter to enable it.
7. From the GUI, ***Mail Policies > DLP Policy Manager*** click on your existing DLP policy that does the encryption.

8. Scroll down until you see the *Filter Message Tags* section, and enter ***NOENCRYPTION*** in the field, and from the drop−down choose *absent* next to it from drop down. (So this means if this value is absent, then perform the encryption, otherwise skip encryption.)
9. Submit and commit your changes.

Related Information

- ***Cisco Email Security Appliance − End−User Guides***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Oct 13, 2014 Document ID: 118560