

Use Content Filter to Divert Emails to the Spam Quarantine in ESA

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Related information](#)

Introduction

This document describes the configuration to divert emails that are not marked spam to the Spam Quarantine.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Cisco Secure Email Gateway (SEG / ESA)
- Content Filters Knowledge
- Quarantines Knowledge
- Spam Quarantine Knowledge

Components Used

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

- Email Security Appliance

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

The purpose for Spam Quarantine is to quarantine emails marked as spam, however, in relation to your organizations needs you can divert emails which are not classified as spam to the Spam Quarantine.

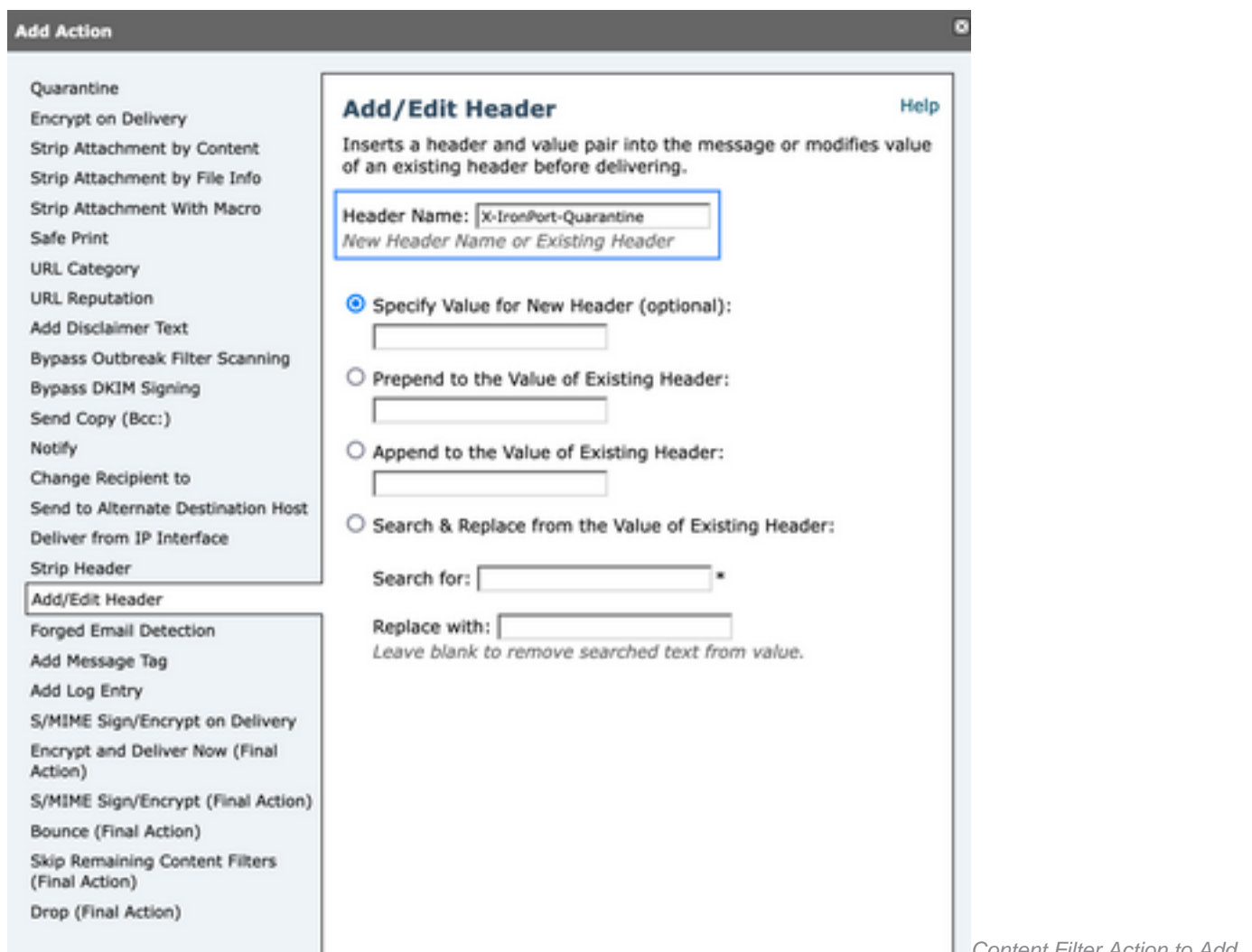
Caution: Ensure you understand End-User Quarantine Access.

Configure

Create the content filter on the ESA:

1. Navigate to **Mail Policies > Incoming/Outgoing content filters**
2. Click **Add Filter**
3. Name the filter
4. Add condition desired and
5. Click **Add Action**
6. Choose **Add/Edit Header**
7. Use **X-IronPort-Quarantine** for the **Header Name** value box
8. **Submit and Commit**

As shown in the image:



Add Action

Quarantine
Encrypt on Delivery
Strip Attachment by Content
Strip Attachment by File Info
Strip Attachment With Macro
Safe Print
URL Category
URL Reputation
Add Disclaimer Text
Bypass Outbreak Filter Scanning
Bypass DKIM Signing
Send Copy (Bcc:)
Notify
Change Recipient to
Send to Alternate Destination Host
Deliver from IP Interface
Strip Header
Add/Edit Header
Forged Email Detection
Add Message Tag
Add Log Entry
S/MIME Sign/Encrypt on Delivery
Encrypt and Deliver Now (Final Action)
S/MIME Sign/Encrypt (Final Action)
Bounce (Final Action)
Skip Remaining Content Filters (Final Action)
Drop (Final Action)

Add/Edit Header [Help](#)

Inserts a header and value pair into the message or modifies value of an existing header before delivering.

Header Name:
New Header Name or Existing Header

Specify Value for New Header (optional):

Prepend to the Value of Existing Header:

Append to the Value of Existing Header:

Search & Replace from the Value of Existing Header:

Search for: *

Replace with:
Leave blank to remove searched text from value.

Content Filter Action to Add

Header

To finish, apply this filter to the desired Incoming/Outgoing Mail Policy.

Related information

- [End user guides ESA](#)