CLOUDFLARE
AREA 1 SECURITY

POV Guide For Cisco Email Security

Bcc Mode

Area 1 Horizon Overview

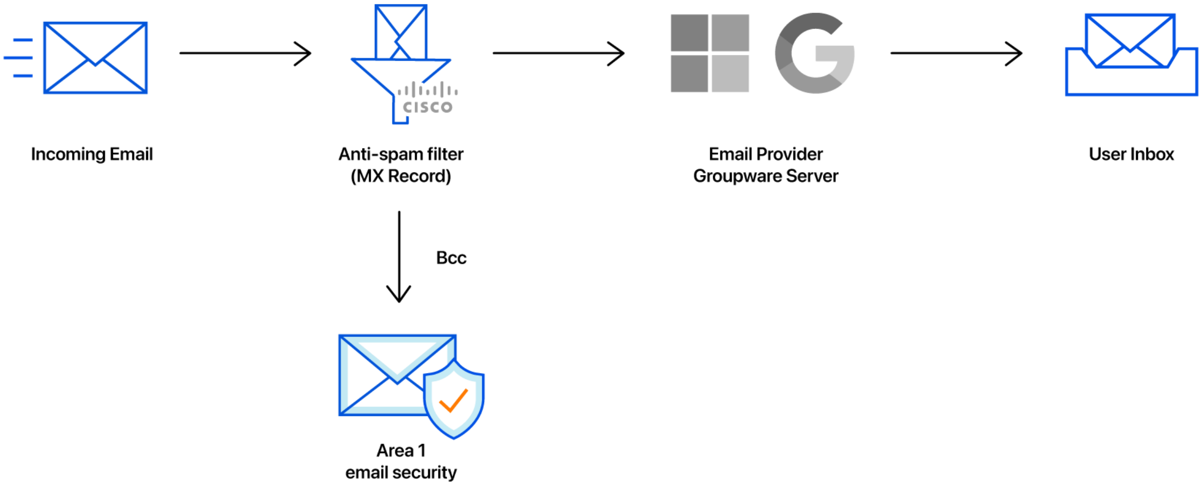
Phishing is the root cause of 95% of security breaches that lead to financial loss and brand damage. Area 1 Horizon is a cloud based service that stops phishing attacks, the #1 cybersecurity threat, across all traffic vectors - email, web and network.

With globally distributed sensors & comprehensive attack analytics, Area 1 Horizon proactively identifies phishing campaigns, attacker infrastructure, and attack delivery mechanisms during the earliest stages of a phishing attack cycle. Using flexible enforcement platforms, Area 1 Horizon allows customers to take preemptive action against these targeted phishing attacks across all vectors - email, web and network; either at the edge or in the cloud.

POV Configuration

This document is intended for customers using Cisco's Email Security Appliances or Cisco Hosted Email Security. The Bcc POV setup with is a simple content filter configuration, where inbound messages are Bcc to Area 1 for phishing inspection and once processed are discarded. The detection reports and details are available through the Area 1 Portal.

POV Email Flow



Configuration Steps

- Step 1: Add Incoming content filter to Bcc message to Area 1
- Step 2: Apply Incoming content filters to an Incoming policies

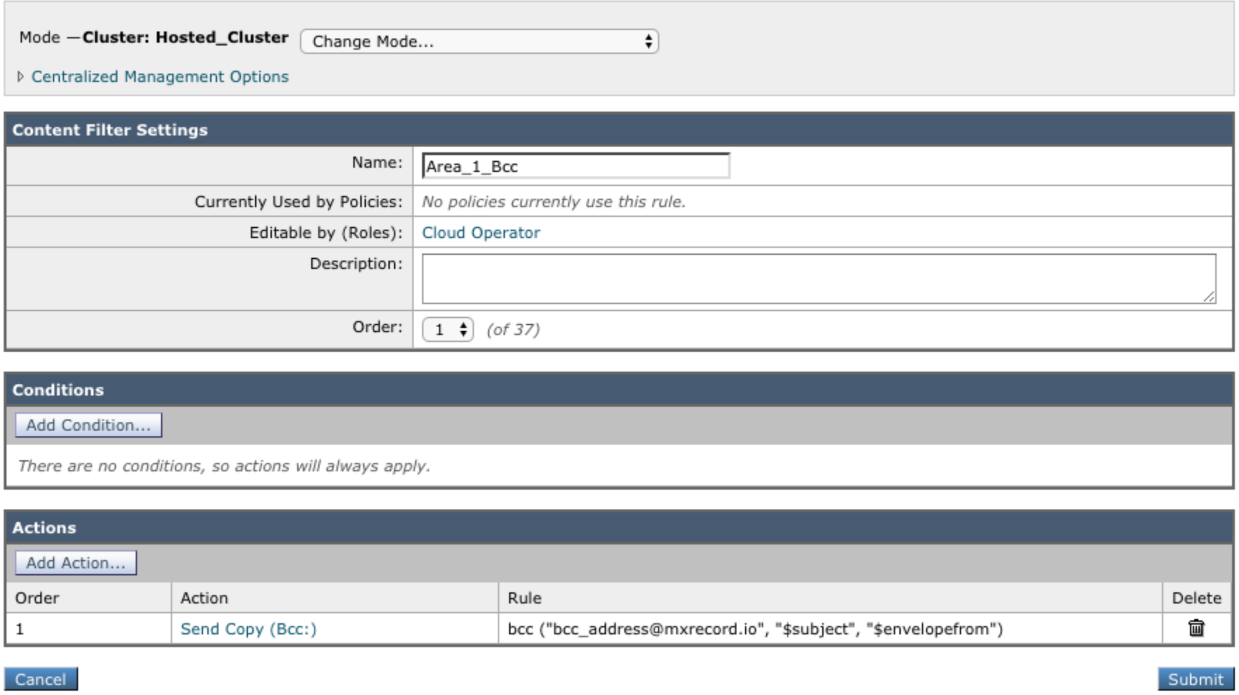
Step 1: Add Incoming content filter to Bcc messages to Area 1

To send a copy of the messages to Area 1, a simple Bcc content filter will need to be configured.

To create a new Content Filter:

- Go to “Mail Policies → Incoming Content Filters”
- Click the “Add Filter…” button to create a new filter
- Configure the new Incoming Content Filter as follows:
  - Name: Bcc_to_Area_1
  - Description: Send a copy of messages to Area 1
  - Order: 1
  - Conditions:
    - Leave blank (i.e. no conditions required)

- Actions:
  - Action: Send Copy (Bcc:)
    - Email Addresses: This address will be provided by Area 1
    - Subject: $subject
    - Return Path: $envelopefrom



Mode —**Cluster: Hosted_Cluster** Change Mode...

▷ Centralized Management Options

Content Filter Settings

Name:	Area_1_Bcc
Currently Used by Policies:	*No policies currently use this rule.*
Editable by (Roles):	Cloud Operator
Description:	
Order:	1 *(of 37)*

Conditions

Add Condition...

There are no conditions, so actions will always apply.

Actions

Add Action...

Order	Action	Rule	Delete
1	Send Copy (Bcc:)	bcc ("bcc_address@mxrecord.io", "$subject", "$envelopefrom")	🗑

Step 2: Add the Incoming Content Filter to the Inbound Policy Table

Assign the Incoming Content Filters created in Step 1 to your primary mail policy in the Incoming Mail Policy table.

Commit your changes to activate the Bcc content filter.

Email Processing & Reports

In the Bcc mode, all emails are put through automated phishing detections by Area 1. Emails that trigger phishing detections are logged for reporting via product portal, email and Slack. Emails that don’t trigger any detections are deleted.