CLOUDFLARE
AREA 1 SECURITY

Phishing Protection for Cisco Email Security

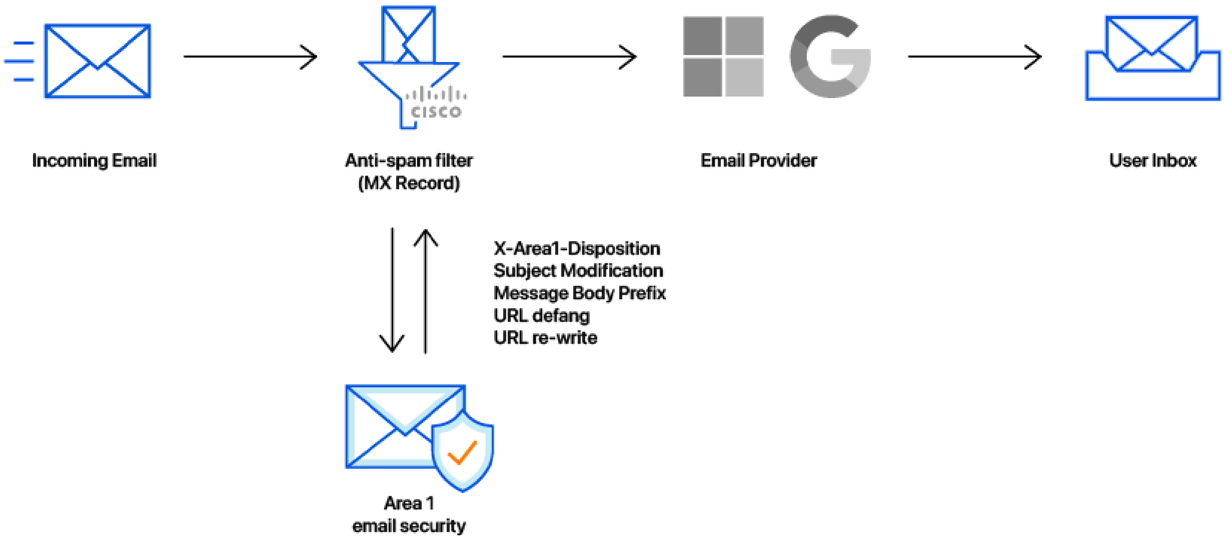
Deployment and Configuration Guide

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.

Email Flow



Configuration Steps

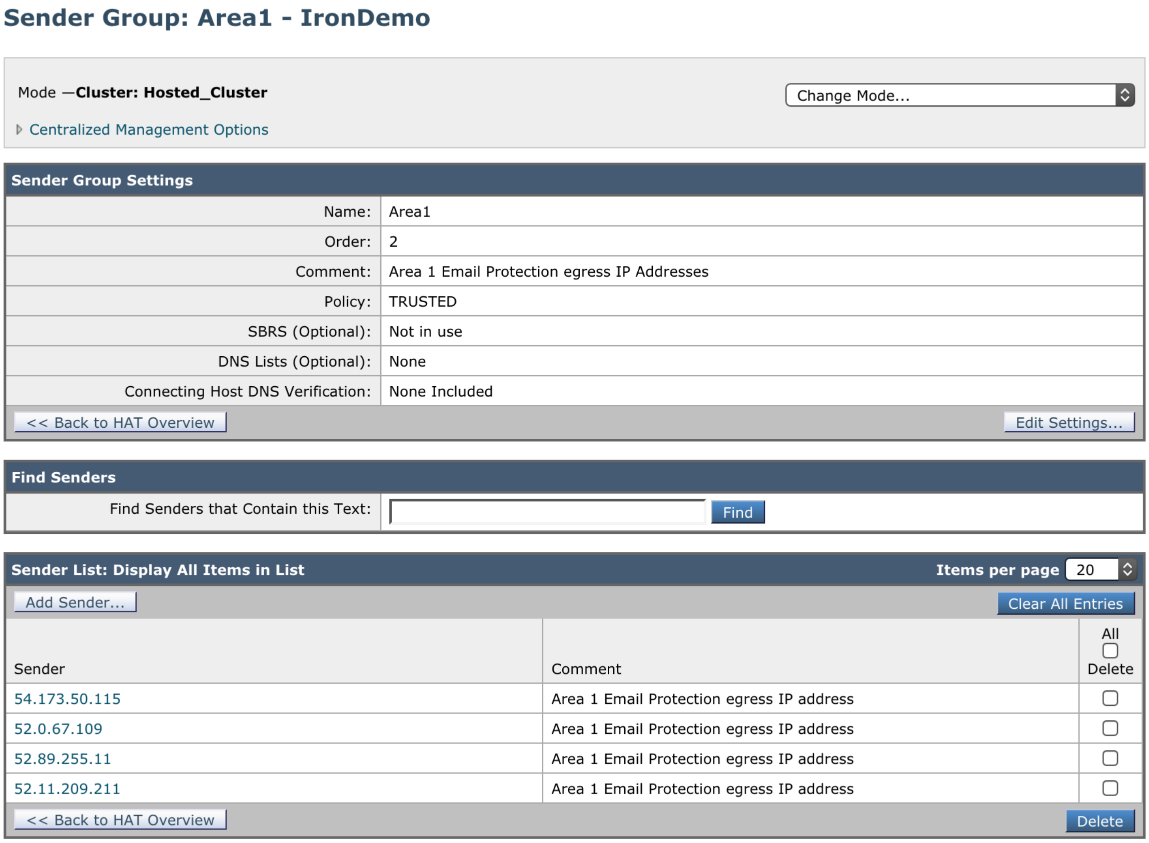
- Step 1: Add a new Sender Group to include Area 1's egress IPs
- Step 2: Add a new SMTP Route for Area 1 Email Protection Service
- Step 3: Add Incoming message filters
  - Redirect all messages to Area 1
  - Detect returning messages from Area 1 and deliver to Email Provider
- Step 4: Apply Incoming message filters to Incoming policies

Step 1: Add a Sender Group for Area 1 Email Protection IPs

To add a new Sender Group:

- Go to “Mail Policies → HAT Overview”
- Click on the “Add Sender Group” button
- Configure the new Sender Group as follows:
    - Name: “Area1”
    - Order: [order above the existing WHITELIST Sender Group]
    - Comment: “Area 1 Email Protection egress IP Addresses”
    - Policy: TRUSTED (by default, spam detection is disabled for this mail flow policy)
    - SBRS: [leave blank]
    - DNS Lists: [leave blank]
    - Connecting Host DNS Verification: [leave all options unchecked]

- Click the “Submit and Add Senders >>” button to add the following IP addresses:
    - 52.11.209.211
    - 52.89.255.11
    - 52.0.67.109
    - 54.173.50.115
    - 158.51.64.0/26
    - 158.51.65.0/26
    - 134.195.26.0/24



Sender Group: Area1 - IronDemo

Mode —**Cluster: Hosted_Cluster**

Sender Group Settings

Name:	Area1
Order:	2
Comment:	Area 1 Email Protection egress IP Addresses
Policy:	TRUSTED
SBRS (Optional):	Not in use
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

Find Senders

Find Senders that Contain this Text:

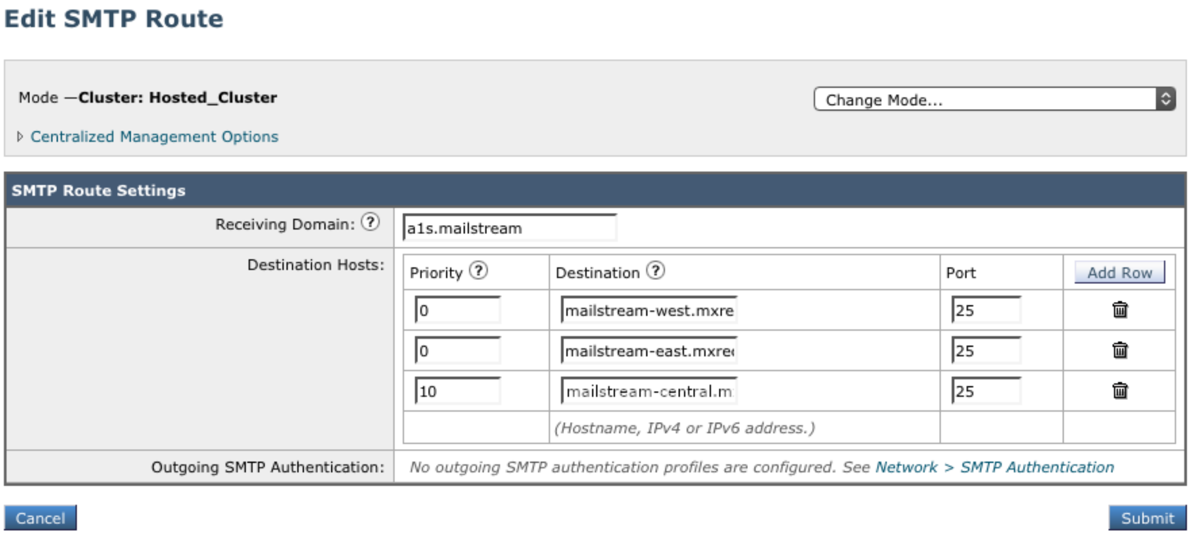
Sender List: Display All Items in List **Items per page** 20

Sender	Comment	All □ Delete
54.173.50.115	Area 1 Email Protection egress IP address	□
52.0.67.109	Area 1 Email Protection egress IP address	□
52.89.255.11	Area 1 Email Protection egress IP address	□
52.11.209.211	Area 1 Email Protection egress IP address	□

Step 2: Add SMTP Route for the Area 1 Email Protection Hosts

To add a new SMTP Route:

- Go to “Network → SMTP Routes”
- Click on the “Add Route…” button
- Configure the new SMTP Route as follows:
    - Receiving Domain: a1s.mailstream
    - Destination Hosts
        - Click the “Add Row” button
        - In the first row:
            - Priority: 0
            - Destination: mailstream-west.mxrecord.io
            - Port: 25
        - In the second row:
            - Priority: 0
            - Destination: mailstream-east.mxrecord.io
            - Port: 25
        - In the third row:
            - Priority:10
            - Destination: mailstream-central.mxrecord.io
            - Port: 25



Edit SMTP Route

Mode —**Cluster: Hosted_Cluster**

SMTP Route Settings

Receiving Domain: a1s.mailstream

Destination Hosts:

Priority	Destination	Port	Add Row
0	mailstream-west.mxre	25	🗑
0	mailstream-east.mxre	25	🗑
10	mailstream-central.m	25	🗑
	(Hostname, IPv4 or IPv6 address.)		

Outgoing SMTP Authentication: *No outgoing SMTP authentication profiles are configured. See Network > SMTP Authentication*

Step 3: Create Incoming Content Filters

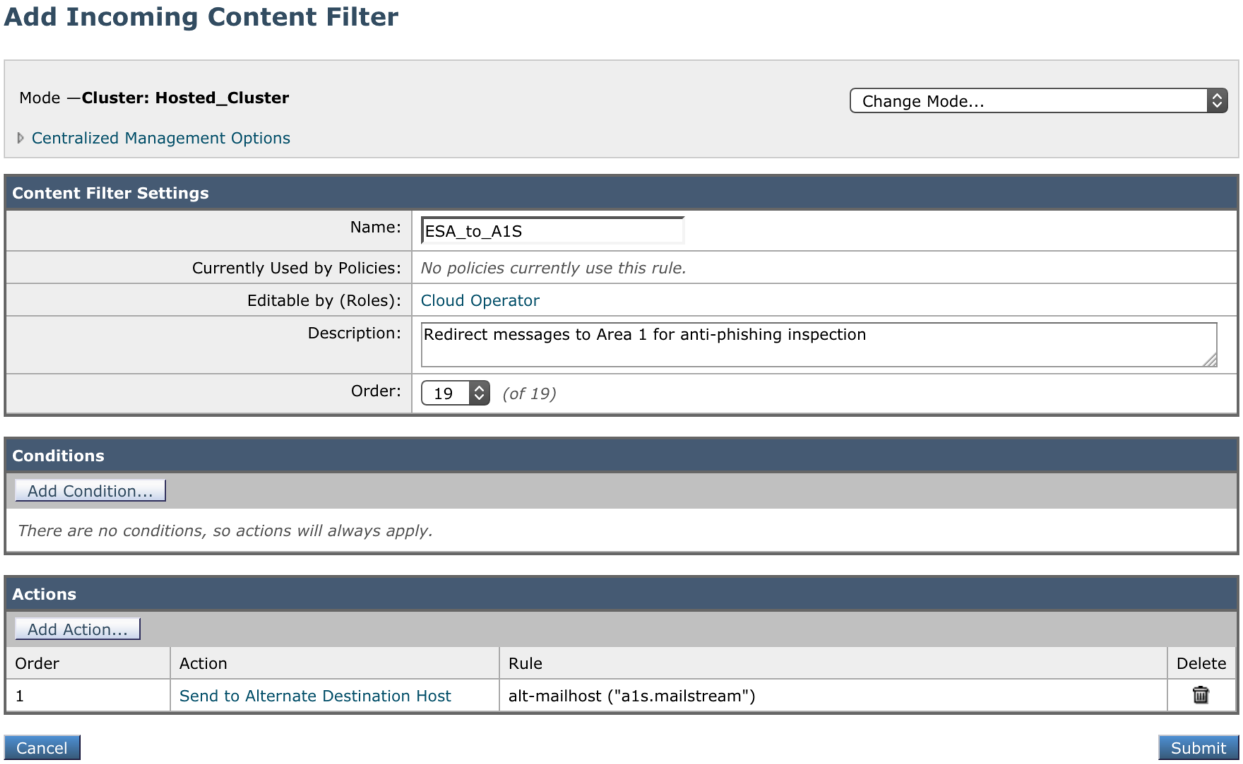
To manage the mail flow between Area 1 and Cisco ESA, 2 filters will be needed:

- A filter to direct all incoming messages to Area 1
- A filter to recognize messages coming back from Area 1 to route for normal delivery

Incoming Content Filter - To Area 1

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: ESA_to_A1S
  - Description: Redirect messages to Area 1 for anti-phishing inspection
  - Order: [this will depend on your other filters but do note the order you select]
  - Condition: [no conditions]
  - Actions:
    - Action: Send to Alternate Destination Host
    - Mail Host: a1s.mailstream (SMTP Route configured in step 2)



Add Incoming Content Filter

Mode —**Cluster: Hosted_Cluster**

Content Filter Settings

Name:	ESA_to_A1S
Currently Used by Policies:	*No policies currently use this rule.*
Editable by (Roles):	Cloud Operator
Description:	Redirect messages to Area 1 for anti-phishing inspection
Order:	19 *(of 19)*

Conditions

There are no conditions, so actions will always apply.

Actions

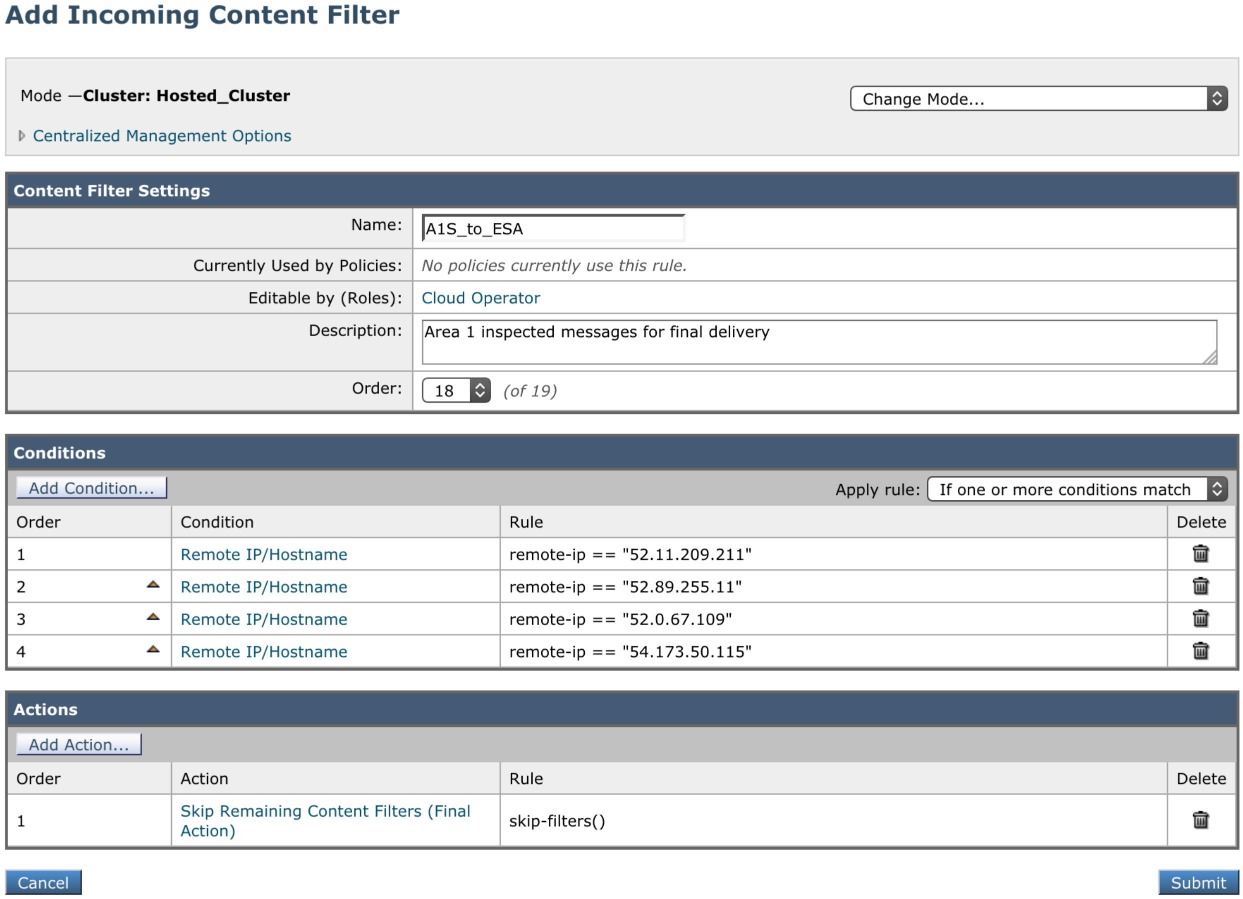
Order	Action	Rule	Delete
1	Send to Alternate Destination Host	alt-mailhost ("a1s.mailstream")	🗑

Incoming Content Filter - From Area 1

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: A1S_to_ESA
    - Description: Area 1 inspected messages for final delivery
    - Order: [this filter MUST be before the previously created filter]
    - Add 7 conditions of type “Remote IP/Hostname” with the following IPs:
        - 52.11.209.211
        - 52.89.255.11
        - 52.0.67.109
        - 54.173.50.115
        - 158.51.64.0/26
        - 158.51.65.0/26
        - 134.195.26.0/24

- Ensure that the “Apply rule:” dropdown is set to “If one or more conditions match”
- Actions:
    - Action: Skip Remaining Content Filters (Final Action)



Add Incoming Content Filter

Mode —**Cluster: Hosted_Cluster**

Content Filter Settings

Name:	A1S_to_ESA
Currently Used by Policies:	*No policies currently use this rule.*
Editable by (Roles):	Cloud Operator
Description:	Area 1 inspected messages for final delivery
Order:	18 *(of 19)*

Conditions

Apply rule: If one or more conditions match

Order	Condition	Rule	Delete
1	Remote IP/Hostname	remote-ip == "52.11.209.211"	🗑
2 ▲	Remote IP/Hostname	remote-ip == "52.89.255.11"	🗑
3 ▲	Remote IP/Hostname	remote-ip == "52.0.67.109"	🗑
4 ▲	Remote IP/Hostname	remote-ip == "54.173.50.115"	🗑

Actions

Order	Action	Rule	Delete
1	Skip Remaining Content Filters (Final Action)	skip-filters()	🗑

Step 4: Add the Incoming Content Filter to the Inbound Policy Table

Assign the Incoming Content Filters created in Step 3 to your primary mail policy in the Incoming Mail Policy table.

Commit your changes to activate the email redirection.