

Phishing Protection for Cisco Email Security

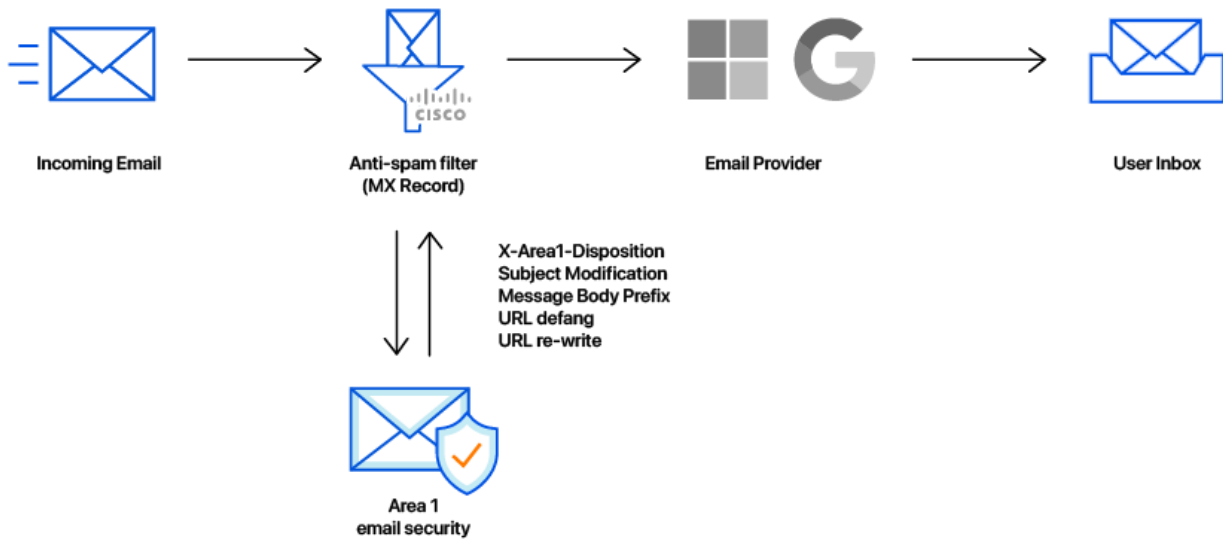
Deployment and Configuration Guide

Cloudflare Area 1 Overview

Phishing is the root cause of upwards of 90% of security breaches that lead to financial loss and brand damage. Cloudflare Area 1 is a cloud-native service that stops phishing attacks, the #1 cybersecurity threat, across all traffic vectors - email, web and network.

With globally distributed sensors and comprehensive attack analytics, Area 1 email security 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 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:
Egress IP’s list can be found here:
<https://developers.cloudflare.com/email-security/deployment/inline/reference/egress-ips/>

Sender Group: Area1 - IronDemo

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

▸ Centralized Management Options

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

[<< Back to HAT Overview](#)

[Edit Settings...](#)

Find Senders

Find Senders that Contain this Text: [Find](#)

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

[Add Sender...](#) [Clear All Entries](#)

Sender	Comment	All <input type="checkbox"/> Delete
54.173.50.115	Area 1 Email Protection egress IP address	<input type="checkbox"/>
52.0.67.109	Area 1 Email Protection egress IP address	<input type="checkbox"/>
52.89.255.11	Area 1 Email Protection egress IP address	<input type="checkbox"/>
52.11.209.211	Area 1 Email Protection egress IP address	<input type="checkbox"/>

[<< Back to HAT Overview](#)

[Delete](#)

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** Change Mode...

▸ [Centralized Management Options](#)

SMTP Route Settings

Receiving Domain:

Destination Hosts:

Priority [?]	Destination [?]	Port	Add Row
<input type="text" value="0"/>	<input type="text" value="mailstream-west.mxre"/>	<input type="text" value="25"/>	
<input type="text" value="0"/>	<input type="text" value="mailstream-east.mxre"/>	<input type="text" value="25"/>	
<input type="text" value="10"/>	<input type="text" value="mailstream-central.m"/>	<input type="text" value="25"/>	
<small>(Hostname, IPv4 or IPv6 address.)</small>			

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

[Cancel](#) [Submit](#)

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 Change Mode...

▶ Centralized Management Options

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

Add Condition...

There are no conditions, so actions will always apply.

Actions

Add Action...

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

Cancel Submit

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:
Egress IP’s list can be found here:
<https://developers.cloudflare.com/email-security/deployment/inline/reference/egress-ips/>

- 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 Change Mode...

▶ Centralized Management Options

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

Add Condition... 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

Add Action...

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

Cancel Submit

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.