CLOUDFLARE
AREA 1 SECURITY

Phishing Protection for Cisco Email Security

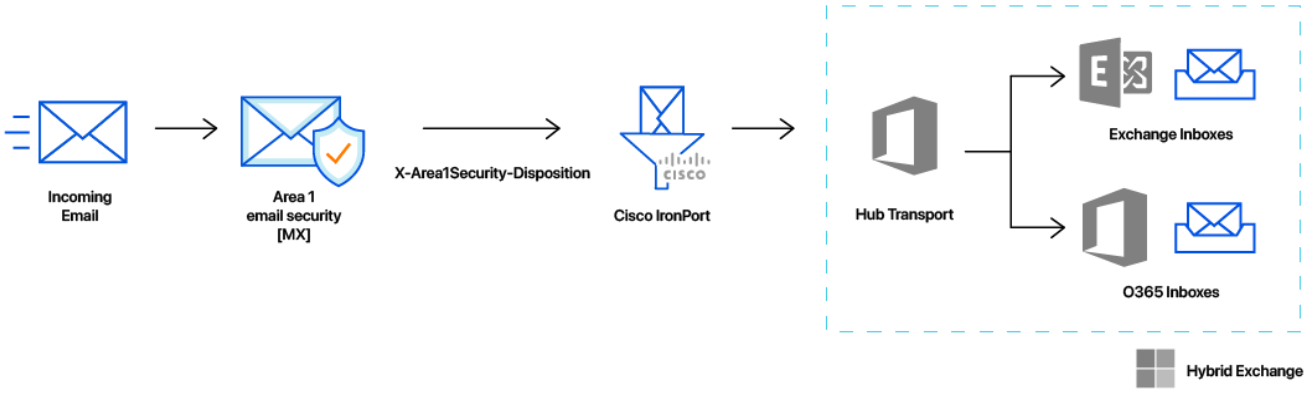
Deployment and Configuration Guide

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

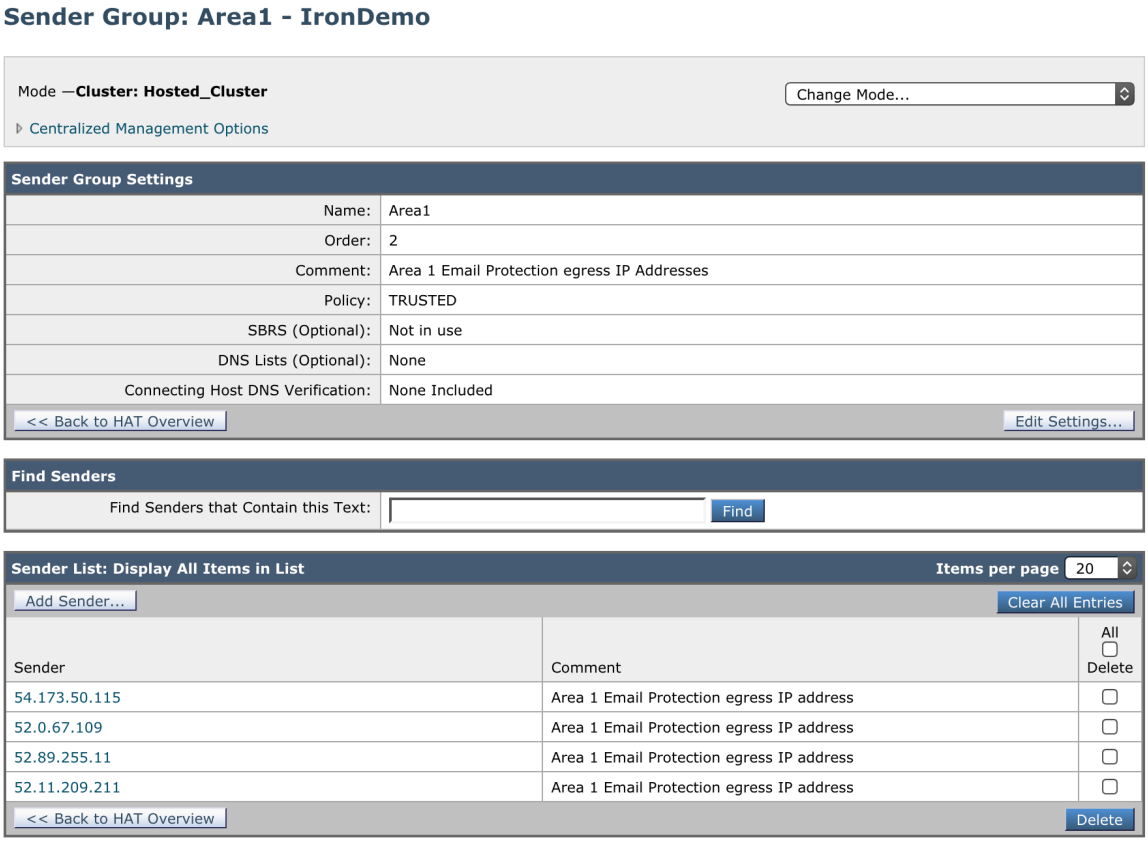
- Step 1: Add a new Sender Group to include Area 1's egress IPs
- Step 2: Configure Incoming Relays
- Step 3: Update domain MX records

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/



Step 2: Configure Incoming Relays

Need access to an IronPort for screenshots

Step 3: Update your domain MX records

Instructions to update your MX records will depend on the DNS provider you are using. In your domain DNS zone, you will want to replace your current MX records with the Area 1 hosts. This will have to be done for every domain where Area 1 will be the primary MX.

Updated your domain MX records using Area 1:

MX Priority	Host
10	mailstream-east.mxrecord.io
10	mailstream-west.mxrecord.io
50	mailstream-central.mxrecord.mx

When configuring the Area 1 MX records, it's important to configure both hosts with the same MX priority, this will allow mail flows to load balance between the hosts.

For European customers, update your MX records to:

MX Priority	Host
10	mailstream-eu1.mxrecord.io
20	mailstream-east.mxrecord.io
20	mailstream-west.mxrecord.io
50	mailstream-central.mxrecord.mx

The European region will be the primary MX, with a fail-over to the US regions. If you wish to exclusively use the European region, simply update with only the European host.
Once the MX records updates complete, the DNS updates may take up to 36 hours to fully propagate around the Internet. Some of the faster DNS providers will start to update records within minutes. The DNS update will typically reach the major DNS servers in about an hour.