

Configure Beta ESA to Accept Traffic from Production ESA

Contents

[Introduction](#)

[Background Information](#)

[Prerequisites](#)

[Environment](#)

[Requirements](#)

[Components Used](#)

[Configure Beta Appliance](#)

[Listener Configuration for Beta ESA](#)

[Sender Group for Beta ESA](#)

[Simple Mail Transfer Protocol \(SMTP\) Routes for Beta ESA](#)

[Incoming Relay for Beta ESA \(Optional\)](#)

[Enable log headers to capture the spam verdict in mail logs \(Optional\)](#)

[Configure Production Appliance](#)

[SMTP Routes for Production ESA](#)

[Bounce Profile Creation](#)

[Destination Controls Profile Creation](#)

[Message Filter Construction for Production ESA](#)

[Verify](#)

[Troubleshoot](#)

[Additional Information \(Optional\)](#)

[Related Information](#)

Introduction

This document describes how to configure a Beta Cisco Email Security Appliance (ESA) to receive a copied mail flow from a Production ESA for testing.

Background Information

The procedure configures Beta ESA listeners, relay permissions, and Simple Mail Transfer Protocol (SMTP) routes, then configures a Production ESA message filter to send a BCC copy of messages to the Beta ESA and verifies delivery in **mail_logs**. Expected outcome: the Beta ESA accepts copied inbound and outbound traffic from the Production ESA for testing.

Prerequisites

Environment

- One Production Cisco Email Security Appliance (ESA) and one Beta ESA.
- Beta ESA listeners: Public listener on TCP port 25; Private listener on TCP port 26 (or port 25 only when an additional interface is available). In CES Hosted Beta, port 587 is reserved for outbound mail.
- Applies to copied inbound and outbound mail flow from the Production ESA to the Beta ESA by using a Production ESA message filter (BCC).

Requirements

Administrative access to the ESA GUI and CLI is required.

Components Used

This document is not restricted to specific software and hardware versions.

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.

Configure Beta Appliance

Listener Configuration for Beta ESA

The initial Listener configuration is to be completed on the Beta ESA.

1. From the GUI, navigate to **Network > Listeners**.
2. Select **Add Listener....**
3. Enter the listener name and configure a Public Listener on TCP port 25.
4. Select **Submit**.
5. Repeat Steps 2 through 4 to add a second listener.
6. Enter the listener name and configure a Private Listener on TCP port 26. This listener is used for outbound mail. You can use port 25 only when an additional interface is available and configured for the environment. In CES Hosted Beta, port 587 is reserved for outbound mail.
7. **Submit** to save changes to the Listener.
8. **Commit** to save all changes to the configuration.

Sender Group for Beta ESA

For relayed traffic or outbound messages, add the appropriate IP addresses for the Beta ESA so that it accepts and relays messages from the Production ESA.

1. From the GUI, navigate to **Mail Policies > HAT Overview**.
2. Select the appropriately named Relay Sender Group. (This is usually named RELAY, or RELAYLIST.)
3. Select **Add Sender....**
4. For Sender, use the IP address of the Production ESA.
5. Enter any administrative comments, as needed.
6. **Submit** to save changes to the Relay Sender Group.
7. **Commit** to save all changes to the configuration.

Simple Mail Transfer Protocol (SMTP) Routes for Beta ESA

Configure this SMTP routes on the Beta ESA.

1. From the GUI, navigate to **Network > SMTP Routes**.
2. If current SMTP routes exist, you can need to select them and **Delete** them before you proceed.
Ensure that you review the Beta Lab Setup Guide.
3. Select **Add Route...**
4. Enter **cisco.com** for **Receiving Domain** and **USEDNS** for **Destination**.
5. Select **Submit**.
6. Repeat Steps 3 through 5 to add a second SMTP route.
7. Enter **ironport.com** for **Receiving Domain** and **USEDNS** for **Destination**.
8. Click **Submit**.
9. Select **All Other Domains** for **Receiving Domain**.
10. Enter **/dev/null** for **Destination**. This prevents routing mail from the Beta ESA for any domains that are not configured.
11. Select **Submit**.
12. **Commit** to save all changes to the configuration.

The SMTP routes on the Beta ESA appear as shown in this image.

SMTP Routes List		Items per page 20
Add Route...		Clear All Routes Import Routes...
Receiving Domain	Destination Hosts	All Delete
.ironport.com	usedns	☐
cisco.com	usedns	☐
All Other Domains	/dev/null	☐
Export Routes...		Delete



Note: Add the appropriate routes to deliver emails to test end-users for domains as needed.

Incoming Relay for Beta ESA (Optional)

Incoming Relay allows the Beta ESA to evaluate the connecting IP address and retrieve a SenderBase Reputation Score (SBRS) beyond what is available from the Production ESA.

Most deployments require one hop.

1. In the GUI, navigate to **Network > Incoming Relay**.
2. Select the **Enable** checkbox.
3. Select **Add Relay**.
4. In the **Name** field, enter a descriptive name.
5. In the **IP Address** field, enter the IP address of the Production ESA that delivers mail to the Beta ESA. Use a partial hostname only when multiple hosts deliver mail.
6. In the **Hop** field, enter **1**.
7. Click **Submit**, then click **Commit**.

You do not need this feature unless you have local MX or MTA relaying mail to your IronPort appliance.

Status: Disabled **Enable**

Add Relay...

No relays defined.

Incoming Relay: Disabled State.

Status: Enabled **Disable**

Incoming Relay: Enabled State, colored white.

Add Relay

Incoming Relay

Name: **Your_Production**

IP Address: **192.1.1.1** → **YOUR Production ESA IP ADDRESS**

Header: ☐ Specify a custom header

☒ Parse the "Received" header

Begin parsing after: (?) from

This will retrieve the sbrs score, one HOP beyond the connecting ip address

Hop: (?) **1**

Incoming Relay: Sample Template

Relay List

You do not need this feature unless you have local MX or MTA relaying mail to your IronPort appliance.

Status: **Enabled** Disable **final preview**

Add Relay...

Name	IP Address	Header	Parse After	Hops	Delete
Your_Production replace with you prod ip	192.1.1.1	Received	from	1	

Incoming Relay: Summary view after Submit.

Sample mail log entry:

Mon Apr 8 12:48:28 2019 Info: MID 2422822 IncomingRelay(PROD_hc2881-52): Header Received found, IP 10.1.

Enable log headers to capture the spam verdict in mail logs (Optional)

1. In the GUI, navigate to **System Administration > Log Subscriptions**.
2. Select **Global Settings** at the bottom of the page.
3. In the **Headers** section, select **Add**.
4. Enter **X-IronPort-Anti-Spam-Result**.
5. Select **Submit**.
6. Click **Commit**.

Log Subscriptions Global Settings

Edit Global Settings

System metrics frequency: 60 seconds

Logging Options:

- ☒ Message-ID headers in Mail Logs
- ☒ Original subject header of each message
- ☒ Remote response text in Mail Logs

Headers (Optional): List any headers you want to record in the log files:

X-IronPort-Anti-Spam-Result

Cancel Submit

Log Spam Headers to Mail Logs

End of beta-side configuration.

Configure Production Appliance

 **Caution:** You are about to make changes to a Production ESA. Ensure that you backup the current configuration.

1. From the Web UI, navigate to **System Administration > Configuration File**.
2. From the Current Configuration section, select one of the options to back up the current configuration as a file:
 - Download file to local computer to view or save.
 - Email file to: <your_email_address@domain.com>
3. Click **Submit**.

SMTP Routes for Production ESA

Add SMTP routes to allow BCC copies of all inbound and outbound email from the Production ESA to the Beta ESA. In this example, **inbound.beta.com** and **outbound.beta.com** are used.

1. From the GUI, navigate to **Network > SMTP Routes**.
2. Select **Add Route....**
3. Enter **inbound.beta.com** for **Receiving Domain**.
4. Enter the IP address of the Beta ESA public listener created earlier for **Destination Hosts**.
5. Enter **25** for the port.
6. Select **Submit**.
7. Repeat Steps 2 through 5 to add the second route.
8. Enter **outbound.beta.com** for **Receiving Domain**.
9. Enter the IP address of the Beta ESA private listener created earlier for **Destination Hosts**.

10. Enter **26** for the port.
11. Select **Submit**.
12. **Commit** to save all changes to the configuration.

The SMTP routes on the Production ESA appear as shown in this image.

SMTP Routes List			Items per page 20
Add Route...		Clear All Routes	Import Routes...
Receiving Domain	Destination Hosts	All ☐ Delete	
cisco.com		☐	
esatest.onmicrosoft.com	smtp.office365.com:587	☐	
inbound.beta.com	172.18.250.222	☐	
ironport.com		☐	
outbound.beta.com	172.18.250.222:26	☐	
All Other Domains	/dev/null	☐	
Export Routes...		Delete	

Bounce Profile Creation

A combination of a Bounce Profile and a Destination Control Profile protects the production mail flow from delays or failures when messages are delivered to the Beta hosts. This configuration applies only to the beta messages.

1. From the Web UI, navigate to **Network > Bounce Profiles > Add Bounce Profile**.
2. Maximum Number of Retries: **15**
3. Maximum time in Queue: **130**
4. Initial time to wait per Message: **60**
5. Maximum time to wait per Message: **60**
6. Send Hard bounce Messages: **NO**
7. Send Delay Warning Messages: **NO**
8. Use Domain Key Signing for Bounce and Delay Messages: **NO**
9. **Submit** to save the changes to this new Bounce Profile.
10. Select **Commit** to save all changes to the configuration.

Add Bounce Profile

Profile Name:	BETA_BOUNCE
Maximum Number of Retries:	15 (between 0 and 10000)
Maximum Time in Queue:	130 seconds (between 0 and 3000000)
Initial Time to Wait per Message:	60 seconds (between 60 and 86400)
Maximum Time to Wait per Message:	60 seconds (between 60 and 86400)

Hard Bounce and Delay Warning Messages:

Send Hard Bounce Messages:

☐ Use Default (Yes) ☐ Yes ☒ No

Use DSN format for bounce messages:

☐ Use Default (Yes) ☒ Yes ☐ No

Message Composition

Message Subject: Delivery Status Notification (Failure)

Parse DSN "Status" field from bounce responses: ☐ Use Default (No) ☐ Yes ☒ No

Notification Template: Bounce Notification Template can be defined at Mail Policies > Text Resources.

Message Language	Template	Preview	Delete
Default	System Generated		

Add Row

Send Delay Warning Messages:

☐ Use Default (No) ☐ Yes ☒ No

Message Composition

Message Subject: Delivery Status Notification (Delay)

Notification Template: Bounce Notification Template can be defined at Mail Policies > Text Resources.

Message Language	Template	Preview	Delete
Default	System Generated		

Add Row

Minimum Interval Between Messages: 14400 seconds

Maximum Number of Messages to Send: 1

Recipient for Bounce and Warning Messages:

☒ Message sender

☐ Alternate:

Use Domain Key Signing for Bounce and Delay Messages:

☒ Use Default (No) ☐ Yes ☐ No

There is no signing profile matching bounce from address MAILER-DAEMON@bluedevil.rtp. Bounce messages will not be signed until you create appropriate signing profile.

Cancel Submit

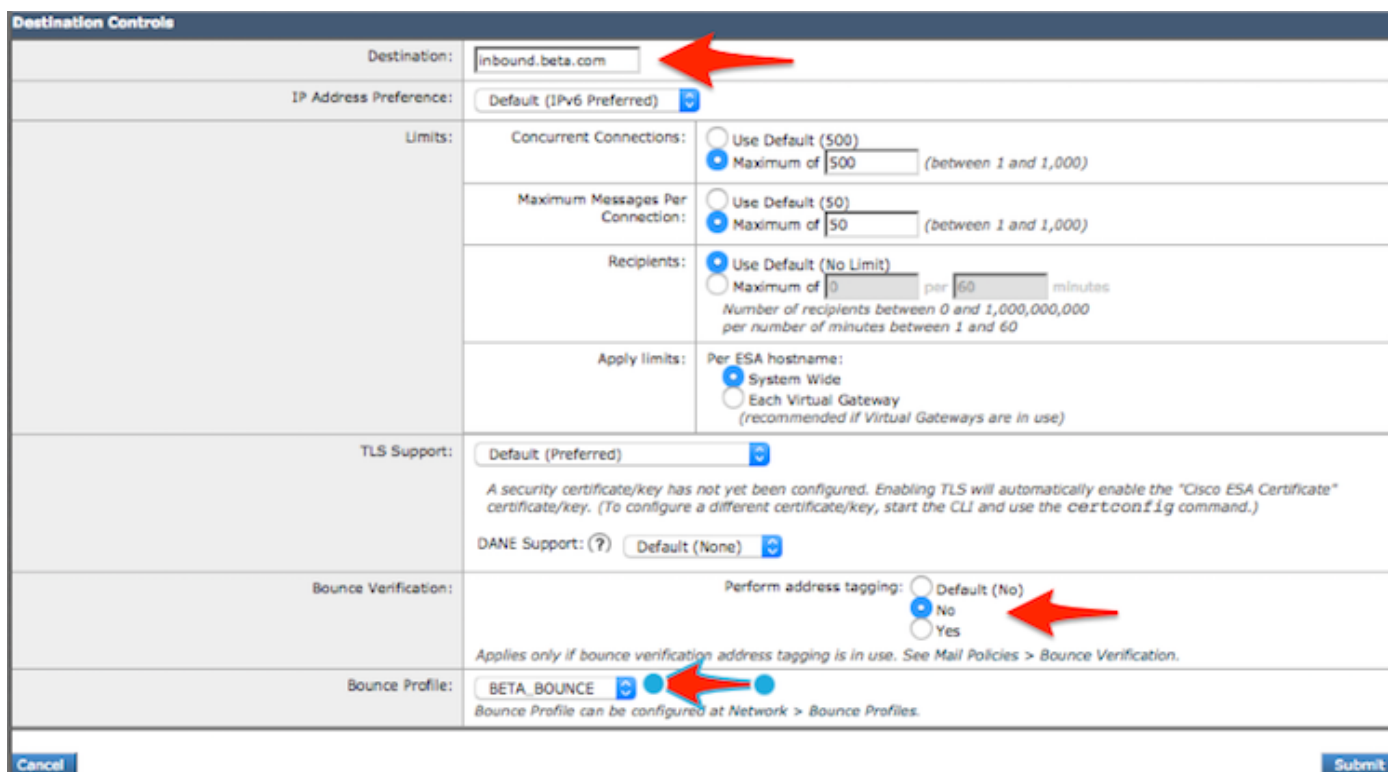
Bounce Profile Creation

Note: The numbered values are configured very aggressively to prevent Delivery Queue Backups in the event of a delivery interruption to the Beta Hosts. The values can be modified to preference. The notification settings are intentionally set to NO to prevent any user notifications from being delivered from the BCC Filters.

Destination Controls Profile Creation

1. From the Web UI, navigate to **Mail Policies > Destination Controls > Add Destination**.
2. Destination: **inbound.beta.com**
3. Bounce Verification: > **Perform address tagging: NO** > or Default (NO)
4. **Bounce Profile: BETA_BOUNCE**
5. Configure the remaining values based on the administrator preference.
6. **Submit** to save the changes to this new Destination Control Profile.

- Repeat Steps 2 through 6 and use **outbound.beta.com** for **Destination**.
- Submit** to save the changes to this new Destination Control Profile.
- Commit** to save all changes to the configuration.



Destination Controls

Destination:

IP Address Preference:

Limits:

- Concurrent Connections: ☐ Use Default (500) ☒ Maximum of (between 1 and 1,000)
- Maximum Messages Per Connection: ☐ Use Default (50) ☒ Maximum of (between 1 and 1,000)
- Recipients: ☒ Use Default (No Limit) ☐ Maximum of per minutes
Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60
- Apply limits: Per ESA hostname: ☒ System Wide ☐ Each Virtual Gateway (recommended if Virtual Gateways are in use)

TLS Support:

A security certificate/key has not yet been configured. Enabling TLS will automatically enable the "Cisco ESA Certificate" certificate/key. (To configure a different certificate/key, start the CLI and use the `certoonfig` command.)

DANE Support:

Bounce Verification: Perform address tagging: ☐ Default (No) ☒ No ☐ Yes

Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.

Bounce Profile:

Bounce Profile can be configured at Network > Bounce Profiles.

Add Destination Control Profiles.

Destination Control Table							Items per page 20
Add Destination...							Import Table
Domain ▲	IP Address Preference	Destination Limits	TLS Support	DANE Support	Bounce Verification *	Bounce Profile	All ☐ Delete
inbound.beta.com	Default	500 concurrent connections, 50 messages per connection, Default recipient limit	Default	Default	Off	BETA_BOUNCE	☐
outbound.beta.com	Default	500 concurrent connections, 50 messages per connection, Default recipient limit	Default	Default	Off	BETA_BOUNCE	☐

Summary View of New Destination Control Profiles.

Message Filter Construction for Production ESA

From the command-line interface (CLI) on the Production ESA, create a message filter that sends BCC copies of email to the appropriate listener on the Beta ESA.

- Navigate to **Filters > NEW**.
- Copy and paste this message filter example, and update the values as needed:

```
bcc-EFT: if sendergroup == "RELAY" {
  bcc ("$envelope recipients", "$Subject", "$EnvelopeFrom", "outbound.beta.com");
  log-entry("<====BCC COPY TO BETA ESA====>");
} else {
  bcc ("$envelope recipients", "$Subject", "$EnvelopeFrom", "inbound.beta.com");
  log-entry("<====BCC COPY TO BETA ESA====>");
}
```

```
}  
.
```

3. **Return** until you are back to the main CLI prompt.
4. **Commit** to save all changes to the configuration.

 **Note:** Limit the traffic copied in the message filter based on sendergroup, recv-listener, mail-from, or other available rules and syntax. Consult the ESA User Guide for complete Message Filter Rules and Filter Rules Summary.

Verify

Use this section to confirm that the configuration works as expected.

To verify that the Beta ESA accepts email traffic from the Production ESA, run this command from the CLI on the Beta ESA:

```
<#root>
```

```
tail mail_logs
```

```
Wed Mar 23 17:28:43 2016 Info: New SMTP ICID 2 interface Management (172.18.250.222) address 172.18.250.222
Wed Mar 23 17:28:43 2016 Info: ICID 2 RELAY SG RELAY match 172.18.250.1/24 SBRS not enabled
Wed Mar 23 17:28:43 2016 Info: Start MID 2 ICID 2
Wed Mar 23 17:28:43 2016 Info: MID 2 ICID 2 From: <test@test.com>
Wed Mar 23 17:28:43 2016 Info: MID 2 ICID 2 RID 0 To: <example@ironport.com>
Wed Mar 23 17:28:43 2016 Info: MID 2 Message-ID '<a033ed$2@9.9.5-038.local>'
Wed Mar 23 17:28:43 2016 Info: MID 2 Subject 'TEST 2'
Wed Mar 23 17:28:43 2016 Info: MID 2 ready 320 bytes from <test@test.com>
Wed Mar 23 17:28:43 2016 Info: MID 2 matched all recipients for per-recipient policy DEFAULT in the out
Wed Mar 23 17:28:43 2016 Info: MID 2 queued for delivery
Wed Mar 23 17:28:43 2016 Info: New SMTP DCID 3 interface 172.18.250.222 address 173.37.93.161 port 25
Wed Mar 23 17:28:43 2016 Info: Delivery start DCID 3 MID 2 to RID [0]
Wed Mar 23 17:28:44 2016 Info: Message done DCID 3 MID 2 to RID [0]
Wed Mar 23 17:28:44 2016 Info: MID 2 RID [0] Response '2.0.0 u2NHSipG018673 Message accepted for delive
Wed Mar 23 17:28:44 2016 Info: Message finished MID 2 done
Wed Mar 23 17:28:48 2016 Info: ICID 2 close
Wed Mar 23 17:28:49 2016 Info: DCID 3 close
```

The SMTP communication is established on 172.18.250.222 (Beta appliance). The traffic is sent from 172.18.250.224 (Production appliance).

The sender group that receives the communication is RELAY for relayed traffic from the 172.18.250.1/24 network.

The remaining entries show the processing of the TEST 2 message.

On the Production ESA, run this command to verify the processed MID:

```
<#root>
```

`tail mail_logs`

The Production ESA shows this output:

Wed Mar 23 14:50:10 2016 Info: MID 242 was generated based on MID 241 by bcc filter 'bcc-EFT'

This output confirms a clear duplication of the message and shows that the message was BCC copied to the Beta ESA and the test end user as intended.

Troubleshoot

If verification fails, review the listener configuration, sender group entries, SMTP routes, incoming relay settings, and message filter configuration on both ESAs. Also review **mail_logs** on both appliances to confirm connection, relay, and delivery events.

Additional Information (Optional)

You can use a content filter to help differentiate Production and Beta email traffic for test end users.

1. From the Web UI on the Beta ESA, navigate to **Mail Policies > Incoming Content Filters** or **Mail Policies > Outgoing Content Filters**.
2. Create a basic content filter that performs the **Add/Edit Header** action.
3. Select **Submit**.
4. Navigate to **Mail Policies > Incoming Mail Policies** or **Mail Policies > Outgoing Mail Policies**.
5. Enable the new content filter and add it to the policy.
6. Select **Submit**.
7. Click **Commit** in order to save all changes to the configuration.

After you complete this step, the content filter on the Beta ESA appears as shown in these images.

Content Filter Settings	
Name:	Bellagio_Subject_Tagging
Currently Used by Policies:	Default Policy
Description:	Prepend BETA PROCESSED tag to subject line for all emails processed through this ESA

Conditions
Add Condition...
<i>There are no conditions, so actions will always apply.</i>

Actions			
Add Action...			
Order	Action	Rule	Delete
1	Add/Edit Header	edit-header-text("Subject", "(.*)", "[BETA PROCESSED]\\1")	Delete

After the Beta ESA processes an email message, the Subject line appears as shown in this image.

[BETA PROCESSED]TEST 3



test@test.com <test@test.com>

Wednesday, March 23, 2016 at 3:01 PM

To:

hello

Related Information

- [How to configure an ESA/SMA for staging updates](#)
- [Technical Support & Documentation - Cisco Systems](#)