

Configurazione di Beta ESA per accettare il traffico ESA di produzione

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configura appliance Beta](#)

[Configurazione del listener per Beta ESA](#)

[Gruppo mittente per Beta ESA](#)

[Route SMTP \(Simple Mail Transfer Protocol\) per Beta ESA](#)

[Incoming Relay for Beta ESA](#)

[Abilitare le intestazioni dei log per acquisire il verdetto della posta indesiderata all'interno dei log di posta](#)

[Configura accessorio di produzione](#)

[Route SMTP per Production ESA](#)

[Creazione profilo rimbalzo](#)

[Creazione profilo controlli destinazione](#)

[Costruzione filtro messaggi per produzione ESA](#)

[Creazione profilo rimbalzo](#)

[Creazione profilo controlli destinazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Ulteriori informazioni](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come configurare una Beta Cisco Email Security Appliance (ESA) per accettare il traffico ESA di produzione tramite un filtro messaggi.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configura appliance Beta

Configurazione del listener per Beta ESA

La configurazione iniziale del listener deve essere completata sull'ESA Beta.

1. Dalla GUI, selezionare **Rete > Listener**.
2. Fare clic su **Aggiungi listener...**
3. Assegnare un nome e configurare un listener pubblico in esecuzione sulla porta TCP 25.
4. Per salvare le modifiche apportate al listener pubblico, fare clic su **Sottometti**.
5. Ripetere gli stessi passaggi e aggiungere un secondo listener.
6. Assegnare un nome e impostare un listener privato che viene eseguito sulla porta TCP 26. Questo listener viene utilizzato per la posta in uscita. È possibile utilizzare la porta 25 se è disponibile un'interfaccia aggiuntiva configurata per l'ambiente in uso. L'ambiente CES Hosted Beta ha riservato la porta 587 per l'uscita.
7. **Sottomettere** per salvare le modifiche al listener.
8. **Eseguire il commit** per salvare tutte le modifiche apportate alla configurazione.

Gruppo mittente per Beta ESA

Per il traffico inoltrato o i messaggi in uscita, aggiungere gli indirizzi IP appropriati per l'ESA Beta per accettare e inoltrare i messaggi dall'ESA di produzione.

1. Dalla GUI, selezionare **Mail Policies > HAT Overview** (Policy di posta > Panoramica HAT).
2. Selezionare il gruppo di mittenti di inoltro con il nome appropriato. Questo nome è in genere RELAY o RELAYLIST.
3. Fare clic su **Aggiungi mittente...**
4. Per Mittente, utilizzare l'indirizzo IP dell'ESA di produzione.
5. Immettere eventuali commenti amministrativi, se necessario.
6. **Invia** per salvare le modifiche al gruppo di mittenti di inoltro.
7. **Eseguire il commit** per salvare tutte le modifiche apportate alla configurazione.

Route SMTP (Simple Mail Transfer Protocol) per Beta ESA

Di seguito sono riportate le modifiche da apportare alla route SMTP sull'ESA Beta:

1. Dalla GUI, selezionare **Network > SMTP Routes** (Rete > Route SMTP).
2. Se sono presenti route SMTP correnti, potrebbe essere necessario selezionarle ed **eliminare** prima di procedere. Assicurarsi di consultare la Guida alla configurazione di Beta Lab.
3. Fare clic su **Add Route... (Aggiungi route)**.
4. Impostare il dominio ricevente come **cisco.com** e la destinazione come **USEDNS**.
5. Fare clic su **Invia**.
6. Ripetere gli stessi passaggi e aggiungere una seconda route SMTP.
7. Impostare Dominio di ricezione per **ironport.com** e Destinazione come **USEDNS**.

8. Fare clic su **Invia**.
9. Infine, selezionare **Tutti gli altri domini** da Dominio ricevente.
10. Impostare la destinazione come **/dev/null**. In questo modo si impedisce il routing della posta elettronica dall'appliance Beta per i domini non configurati.
11. Fare clic su **Invia**.
12. **Eseguire il commit** per salvare tutte le modifiche apportate alla configurazione.

In questo momento, le route SMTP sull'accessorio Beta sono indicate nell'immagine:

SMTP Routes List		Items per page 20
Add Route...		Clear All Routes Import Routes...
Receiving Domain	Destination Hosts	All Delete
.ironport.com	usedns	<input type="checkbox"/>
cisco.com	usedns	<input type="checkbox"/>
All Other Domains	/dev/null	<input type="checkbox"/>
Export Routes...		Delete

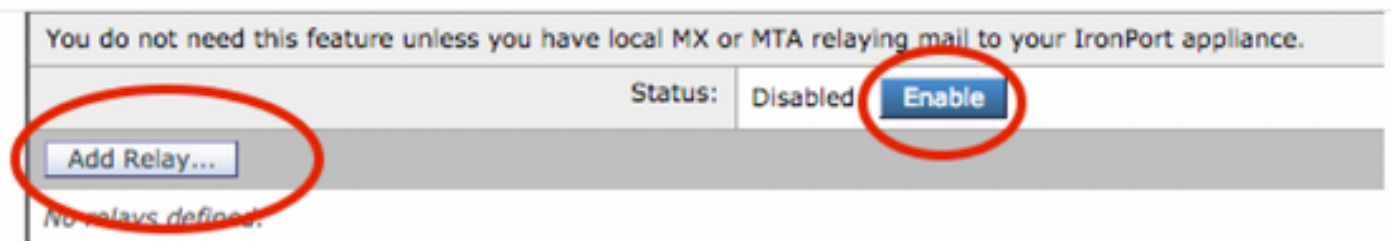
Nota: Aggiungere le route appropriate per recapitare messaggi di posta elettronica agli utenti finali di test per i domini in base alle esigenze.

Incoming Relay for Beta ESA

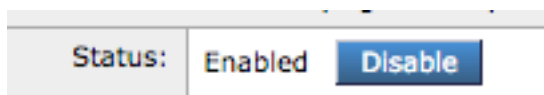
La configurazione del relè in entrata consente alla beta di recuperare il punteggio SBRS oltre quello dell'ESA di produzione.

La maggior parte delle configurazioni funziona con un solo hop.

1. GUI, passare a Network Incoming Relay.
2. Fare clic su "Attiva" per renderlo bianco.
3. Fare clic su Aggiungi inoltra.
4. "Nome" scegliere un nome.
5. Valore "indirizzo IP" dell'ESA di produzione che consegna all'ESA Beta. Il nome host parziale è accettabile se vengono forniti più host.
6. "Hop:" 1
7. Invia e conferma modifiche



Relay in ingresso: Stato disabilitato.



Relay in ingresso: Stato attivato, colore bianco.

Add Relay

Incoming Relay

Name:

IP Address:

Header: Specify a custom header
 Parse the "Received" header

Begin parsing after:

Hop:

YOUR Production ESA IP ADDRESS

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

Relay in ingresso: Modello di esempio

Relay List

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

Status:

final preview

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

Relay in ingresso: Visualizzazione Riepilogo dopo l'invio.

Voce del log di esempio:

Lun Apr 8 12:48:28 2019 Informazioni: MID 2422822 IncomingRelay(PROD_hc281-52): Header Received, IP 54.240.35.22 in uso, SBRS 3.5 paese Stati Uniti

Abilitare le intestazioni dei log per acquisire il verdetto della posta indesiderata all'interno dei log di posta

- Webui > Amministrazione di sistema > Sottoscrizioni dei registri > Impostazioni globali (in basso) > Intestazioni > (aggiungi) Risultato X-IronPort-Anti-Spam

Log Subscriptions Global Settings

Edit Global Settings

System metrics frequency: seconds

Logging Options:

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

Headers (Optional):

Registra intestazioni posta indesiderata nei log di posta

FINE CONFIGURAZIONE LATO BETA.

Configura accessorio di produzione

Attenzione: Stai per apportare modifiche a un'ESA di produzione. Accertarsi di eseguire il backup della configurazione corrente.

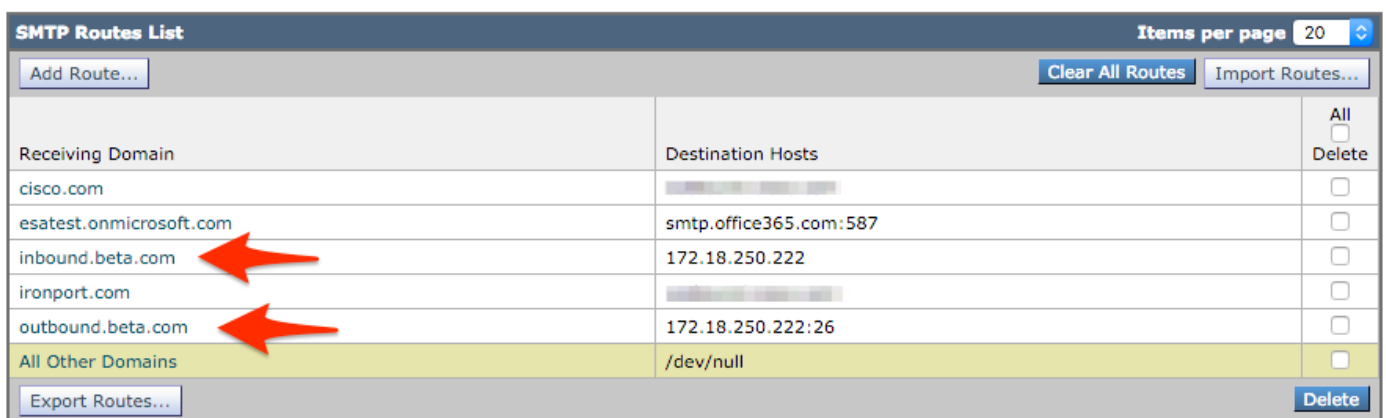
1. Dalla GUI, selezionare **System Administration > Configuration File** (Amministrazione sistema > File di configurazione).
2. Dalla sezione Configurazione corrente, selezionare una delle opzioni per eseguire il backup della configurazione corrente come file: Scaricare il file nel computer locale per visualizzarlo o salvarlo. Invia file tramite posta elettronica a: <your_email_address@domain.com>
3. Fare clic su **Invia**.

Route SMTP per Production ESA

È necessario aggiungere le route SMTP per consentire il calcolo del valore BCC per tutti i messaggi e-mail in entrata e in uscita dall'ESA di produzione all'ESA Beta. Per questo esempio, vengono utilizzati i siti **inbound.beta.com** e **outbound.beta.com**.

1. Dalla GUI, selezionare **Network > SMTP Routes** (Rete > Route SMTP).
2. Fare clic su **Add Route...** (Aggiungi route).
3. Impostare il dominio di ricezione come **inbound.beta.com** con Destination come indirizzo IP del listener pubblico dell'appliance Beta creato in precedenza, con la porta impostata su 25.
4. Fare clic su **Invia** per salvare le modifiche alla nuova route SMTP.
5. Ripetere gli stessi passaggi, **Aggiungi route...**
6. Impostare il dominio di ricezione come **outbound.beta.com**, gli host di destinazione come indirizzo IP del listener privato dell'appliance Beta creato in precedenza e la porta su 26.
7. **Invia** per salvare le modifiche alla nuova route SMTP.
8. **Eseguire il commit** per salvare tutte le modifiche apportate alla configurazione.

In questo momento, le route SMTP sull'ESA di produzione come mostrato nell'immagine:



Receiving Domain	Destination Hosts	All <input type="checkbox"/> Delete
cisco.com		<input type="checkbox"/>
esatest.onmicrosoft.com	smtp.office365.com:587	<input type="checkbox"/>
inbound.beta.com	172.18.250.222	<input type="checkbox"/>
ironport.com		<input type="checkbox"/>
outbound.beta.com	172.18.250.222:26	<input type="checkbox"/>
All Other Domains	/dev/null	<input type="checkbox"/>

Creazione profilo rimbalzo

Una combinazione di profilo di rimbalzo e profilo di controllo di destinazione protegge il flusso di posta di produzione da complicazioni associate a ritardi o errori nel recapitare i messaggi agli host beta. Questa configurazione verrà applicata solo ai messaggi beta.

1. Dalla GUI, selezionare **Network > Bounce Profiles > Add Bounce Profile** (Rete > Profili di rimbalzo > Aggiungi profilo di rimbalzo).
2. Numero massimo di tentativi: **15**

3. Tempo massimo in coda: **130**
4. Tempo di attesa iniziale per messaggio: **60**
5. Tempo massimo di attesa per messaggio: **60**
6. Invia messaggi di tipo Hard bounce: **NO**
7. Invia messaggi di avviso di ritardo: **NO**
8. Usa firma chiave di dominio per messaggi di rimbalzo e ritardo: **NO**
9. **Invia** per salvare le modifiche al nuovo profilo di rimbalzo.
10. Consente di salvare tutte le modifiche apportate alla configurazione.

Add Bounce Profile

Profile Name:

Maximum Number of Retries:
(between 0 and 10000)

Maximum Time in Queue: seconds
(between 0 and 3000000)

Initial Time to Wait per Message: seconds
(between 60 and 86400)

Maximum Time to Wait per Message: 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:

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		

Send Delay Warning Messages:

Use Default (No) Yes No

Message Composition

Message Subject:

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

Message Language	Template	Preview	Delete
Default	System Generated		

Minimum Interval Between Messages: seconds

Maximum Number of Messages to Send:

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.com address MAILER-DAEMON@bluedevil.rtp. Bounce messages will not be signed until you create appropriate signing profile.

Creazione profilo rimbalzo

Nota: i valori numerati sopra riportati sono configurati in modo molto aggressivo per impedire il backup delle code di recapito in caso di interruzione del recapito agli host beta. I valori possono essere modificati in preferenze. Le impostazioni di notifica sono intenzionalmente impostate su NO per impedire il recapito delle notifiche utente dai filtri Ccn.

Creazione profilo controlli destinazione

1. Dalla GUI, selezionare Mail Policies > Destination Controls > Add Destination.
2. Destinazione: **inbound.beta.com**
3. Verifica Rimbalzo: > **Eseguite la codifica degli indirizzi: NO** > o Predefinito (NO)
4. **Profilo rimbalzo: RIMBALZO**
5. Gli altri valori possono essere configurati in base alle preferenze dell'amministratore.
6. **Invia** per salvare le modifiche al nuovo profilo di controllo della destinazione.
7. **Ripetere** i punti da 2 a 6 utilizzando la destinazione: **outbound.beta.com**
8. **Invia** per salvare le modifiche al nuovo profilo di controllo della destinazione.
9. **Eseguire il commit** per salvare tutte le modifiche apportate alla configurazione.

aggiungere profili di controllo destinazione.

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	<input type="checkbox"/>
outbound.beta.com	Default	500 concurrent connections, 50 messages per connection, Default recipient limit	Default	Default	Off	BETA_BOUNCE	<input type="checkbox"/>

Vista di riepilogo dei nuovi profili di controllo di destinazione.

Costruzione filtro messaggi per produzione ESA

Dalla CLI sull'ESA di produzione, creare un filtro messaggi in grado di inviare e-mail BCC al listener appropriato sull'ESA Beta.

1. Selezionare **Filtri > NUOVO**.
2. Copiare e incollare questo esempio di filtro messaggi e apportare le modifiche appropriate:

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

```
log-entry("<====BCC COPY TO BETA ESA====>");
}
```

.

3. **Tornare** al prompt della CLI principale.

4. **Eseguire il commit** per salvare tutte le modifiche apportate alla configurazione.

Nota: Limitare il traffico copiato nel filtro messaggi in base alle regole e alla sintassi di sendergroup, recv-listener, mail-from o altre regole disponibili. Consultare la Guida dell'utente ESA per le regole di filtro dei messaggi e il riepilogo delle regole di filtro.

Creazione profilo rimbalzo

Creazione profilo controlli destinazione

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

A questo punto, l'appliance Beta accetta il traffico e-mail dall'appliance di produzione. Per eseguire la verifica dalla CLI sull'appliance Beta, eseguire **tail mail_logs**:

```
Wed Mar 23 17:28:43 2016 Info: New SMTP ICID 2 interface Management (172.18.250.222) address
172.18.250.224 reverse dns host dhcp-172-18-250-224.cisco.com verified yes
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: <robsherw@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 outbound table
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
delivery'
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
```

La comunicazione SMTP stabilisce il 172.18.250.222 (Beta appliance). L'indirizzo da cui viene inviato il traffico è 172.18.250.224 (apparecchiatura di produzione).

Il gruppo mittente che riceve la comunicazione è RELAY, traffico inoltrato dalla rete 172.18.250.1/24.

Il resto è la comunicazione del messaggio TEST 2.

Nell'accessorio di produzione verificare ed eseguire **tail mail_logs**. Il MID elaborato sulla produzione mostra:

In questo modo, il messaggio e-mail ricevuto viene suddiviso in due parti, che vengono quindi consegnate al dispositivo Beta e testate all'utente finale in base alla destinazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Ulteriori informazioni

È possibile prendere in considerazione un filtro dei contenuti per differenziare il traffico di posta elettronica di produzione da quello beta per gli utenti finali di prova.

1. Dalla GUI sull'ESA Beta, selezionare **Mail Policies > Incoming Content Filters** (Policy di posta > Filtri contenuti in arrivo) o **Mail Policies > Outgoing Content Filters** (Policy di posta > Filtri contenuti in uscita).
2. Creare un filtro del contenuto di base per eseguire un'azione di Aggiungi/Modifica intestazione.
3. Per salvare le modifiche apportate al filtro del contenuto, fare clic su **Submit** (Invia).
4. **Criteri di posta > Criteri posta in arrivo** o **Criteri di posta > Criteri posta in uscita**, abilitare e aggiungere il nuovo filtro contenuto al nome del criterio.
5. Per salvare il filtro contenuti in base al criterio, fare clic su **Submit** (Invia).
6. Per salvare tutte le modifiche apportate alla configurazione, fare clic su **Commit**.

A questo punto, il filtro dei contenuti sull'ESA Beta è come mostrato nelle immagini:

Content Filter Settings	
Name:	<input type="text" value="Bellagio_Subject_Tagging"/>
Currently Used by Policies:	Default Policy
Description:	<input type="text" value="Prepend BETA PROCESSED tag to subject line for all emails processed through this ESA"/>

Conditions
<input type="button" value="Add Condition..."/>
<i>There are no conditions, so actions will always apply.</i>

Actions			
<input type="button" value="Add Action..."/>			
Order	Action	Rule	Delete
1	Add/Edit Header	edit-header-text("Subject", "(.*)", "[BETA PROCESSED]\\1")	

Ora, quando si riceve un messaggio e-mail sull'ESA Beta, è possibile vedere questo nella riga Oggetto dell'e-mail una volta elaborato come mostrato nell'immagine:

[BETA PROCESSED]TEST 3



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

Wednesday, March 23, 2016 at 3:01 PM

To:

hello

Informazioni correlate

- [Come configurare un ESA/SMA per gli aggiornamenti di gestione temporanea](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)