

Configurez le bêta ESA pour recevoir le trafic ESA de production

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez la bêta appliance](#)

[Configuration d'auditeur pour le bêta ESA](#)

[Groupe d'expéditeur pour le bêta ESA](#)

[Artères de Protocole SMTP \(Simple Mail Transfer Protocol\) pour le bêta ESA](#)

[Configurez l'appliance de production](#)

[Artères de SMTP pour la production ESA](#)

[Construction de filtre de message pour la production ESA](#)

[Vérifiez](#)

[Dépannez](#)

[Informations supplémentaires](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer une bêta appliance de sécurité du courrier électronique de Cisco (ESA) afin de recevoir le trafic ESA de production par l'intermédiaire d'un filtre de message.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Configurez la bêta appliance

Configuration d'auditeur pour le bêta ESA

La configuration initiale d'auditeur doit être terminée sur le bêta ESA.

1. Du GUI, naviguez vers le **réseau > les auditeurs**.
2. Cliquez sur Add l'**auditeur**...
3. Nommez et installez un auditeur public qui s'exécute sur le port TCP 25.
4. Cliquez sur Submit afin de sauvegarder les modifications à l'auditeur public.
5. Répétez les mêmes étapes et ajoutez un deuxième auditeur.
6. Nommez et installez un auditeur privé qui s'exécute sur le port TCP 26. (Cet auditeur est utilisé pour la messagerie sortante.) Vous pouvez utiliser le port 25 s'il y a une interface supplémentaire disponible et configurée pour votre environnement.
7. **Soumettez** pour sauvegarder des modifications à l'auditeur.
8. **La validation** pour épargner toute change en la configuration.

Groupe d'expéditeur pour le bêta ESA

Pour le trafic transmis par relais ou les messages sortants, ajoutez dans l'adresse IP appropriée pour le bêta ESA afin de recevoir et des messages de relais de la production ESA.

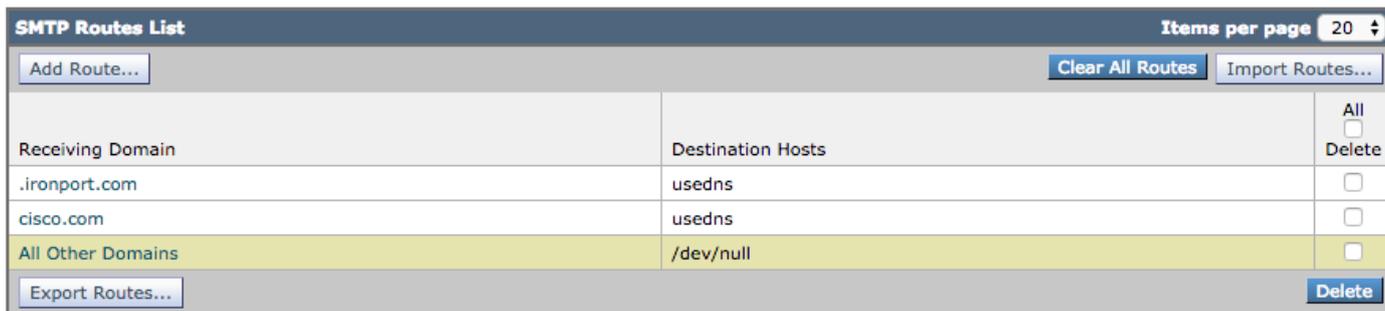
1. Du GUI, naviguez **pour envoyer par mail des stratégies > l'aperçu de CHAPEAU**.
2. Sélectionnez le groupe convenablement Désigné d'expéditeur de relais. (Ceci est habituellement nommé RELAIS, ou RELAYLIST.)
3. Cliquez sur Add l'**expéditeur**...
4. Pour l'expéditeur, utilisez l'adresse IP de la production ESA.
5. Écrivez tous les commentaires administratifs, comme nécessaire.
6. **Soumettez** pour sauvegarder des modifications au groupe d'expéditeur de relais.
7. **La validation** pour épargner toute change en la configuration.

Artères de Protocole SMTP (Simple Mail Transfer Protocol) pour le bêta ESA

Les modifications d'artère de SMTP qui doivent être apportées sur le bêta ESA sont comme suit :

1. Du GUI, naviguez vers le **réseau > les artères de SMTP**.
2. S'il y a les artères en cours de SMTP, vous pouvez devoir sélectionner ceux et l'**effacement** avant que vous poursuiviez. (Assurez pour passer en revue le le bêta guide d'installation de laboratoire.)
3. Cliquez sur Add l'**artère**...
4. Placez le domaine de réception comme **cisco.com** et la destination comme **USEDNS**.
5. Cliquez sur **Submit**.
6. Répétez les mêmes étapes et ajoutez dans une deuxième artère de SMTP.
7. Placez recevoir le domaine pour **ironport.com** et la destination comme **USEDNS**.
8. Cliquez sur **Submit**.
9. En conclusion, sélectionnez **tous autres domaines de recevoir** le domaine.
10. Placez la destination comme **/dev/null**. (Ceci empêche conduire la messagerie de la bêta appliance pour tous les domaines non configurés.)
11. Cliquez sur **Submit**.
12. **La validation** pour épargner toute change en la configuration.

À ce moment, les artères de SMTP sur la bêta appliance est suivant les indications de l'image :



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"/>

Note: Ajoutez les artères appropriées pour fournir des emails pour examiner des utilisateurs pour des domaines comme nécessaires.

Configurez l'appliance de production

Attention : Vous êtes sur le point d'apporter des modifications à une production ESA. Assurez-vous que vous sauvegarde la configuration en cours.

1. Du GUI, naviguez vers l'**administration système > le fichier de configuration**.
2. De la section de configuration en cours, sélectionnez une des options de sauvegarder la configuration en cours comme fichier : Fichier téléchargé à l'ordinateur local à visualiser ou sauvegarder. Fichier d'email à : < your_email_address@domain.com >
3. Cliquez sur **Submit**.

Artères de SMTP pour la production ESA

Des artères de SMTP doivent être ajoutées afin de permettre BCC pour tous les emails d'arrivée et sortants de la production ESA au bêta ESA. Pour cet exemple, **inbound.beta.com** et **outbound.beta.com** sont utilisés.

1. Du GUI, naviguez vers le **réseau > les artères de SMTP**.
2. Cliquez sur **Add l'artère...**
3. Placez recevoir le domaine comme **inbound.beta.com** avec la destination comme adresse IP de l'auditeur public de bêtas appareils créé plus tôt, avec le port réglé à 25.
4. Cliquez sur **Submit** pour sauvegarder des modifications à cette nouvelle artère de SMTP.
5. Répétez les mêmes étapes, **ajoutez l'artère...**
6. Placez le domaine de réception comme **outbound.beta.com**, les destinations hosts comme adresse IP de l'auditeur privé de bêtas appareils créé plus tôt, et le port à 26.
7. **Soumettez** pour sauvegarder les modifications à cette nouvelle artère de SMTP.
8. **La validation** pour épargner toute change en la configuration.

À ce moment, artères de SMTP sur la production ESA suivant les indications de l'image :

SMTP Routes List		Items per page 20
Add Route...		Clear All Routes Import Routes...
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"/>
Export Routes...		Delete

Construction de filtre de message pour la production ESA

Du CLI sur la production ESA, construisez un filtre de message qui peut des emails BCC à l'auditeur approprié sur le bêta ESA.

1. Naviguez vers des **filtres > NOUVEAU**.
2. Copiez et collez cet exemple de filtre de message et apportez les modifications là où appropriées :

```

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. **Retournez** jusqu'à ce que vous soyez de nouveau à la demande principale CLI.
4. **La validation** pour épargner toute change en la configuration.

Note: Limitez le trafic copié dans le filtre de message basé sur le sendergroup, le recv-auditeur, messagerie-de, ou toutes autres règles et syntaxe disponibles. Consultez le guide utilisateur ESA pour des règles de filtrage de message complet et des règles de filtrage récapitulatives.

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

À ce moment, la bêta appliance reçoit le trafic d'email de l'appliance de production. Afin de vérifier du CLI sur la bêta appliance, exécutez les **mail_logs de queue** :

```

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 transmission de SMTP établit sur 172.18.250.222 (bêta appliance). L'adresse dont le trafic est envoyé est de est 172.18.250.224 (appliance de production).

Le groupe d'expéditeur qui reçoit la transmission est RELAIS, le trafic transmis par relais du réseau 172.18.250.1/24.

Le repos est la transmission du message du TEST 2.

Sur l'appliance de production, vérifiez et exécutez les **mail_logs de queue**. Le MID traité sur la production afficherait :

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

Ce serait un éclatement défini du message électronique comme reçu et BCC'd plus d'à la bêta appliance et examinerait l'utilisateur comme prévu pour la réception.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations supplémentaires

Un filtre satisfait peut être considéré comme afin d'aider à différencier la production contre le bêta trafic d'email pour des utilisateurs de test.

1. Du GUI sur le bêta ESA, naviguez **pour envoyer par mail des stratégies > les filtres satisfaits entrants** ou **pour envoyer par mail des stratégies > les filtres satisfaits sortants**.
 2. Construisez un filtre satisfait de base afin d'exécuter une action d'en-tête d'Add/Edit.
 3. Cliquez sur Submit afin de sauvegarder des modifications au filtre satisfait construit.
 4. **Les stratégies de messagerie > des stratégies de messagerie entrante** ou **des stratégies de messagerie > des stratégies de mail sortant**, enable et ajoutent le nouveau filtre satisfait au nom de stratégie.
 5. Cliquez sur Submit afin de sauvegarder le filtre satisfait à cette stratégie.
 6. Cliquez sur la **validation** afin de sauvegarder toutes les modifications à la configuration.
- À ce moment, le filtre satisfait sur le bêta ESA est suivant les indications des 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")	

[Cancel](#)

[Submit](#)

Maintenant, quand un message électronique est reçu sur le bêta ESA vous pouvez voir ceci dans le champ objet de l'email une fois traité suivant les indications de l'image :

[BETA PROCESSED]TEST 3



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

Wednesday, March 23, 2016 at 3:01 PM

To:

hello

[Informations connexes](#)

- [Comment configurer un ESA/SMA pour les mises à jour de présentation](#)
- [Support et documentation techniques - Cisco Systems](#)