Configurer Bêta ESA pour accepter le trafic provenant de Production ESA

Table des matières

- Introduction
- Informations générales
- Conditions préalables
  - Environnement
  - Exigences
  - Composants utilisés
- Configurer l'appliance bêta
  - Configuration de l'écouteur pour Bêta ESA
  - Groupe d'expéditeurs pour Bêta ESA
  - Routes SMTP (Simple Mail Transfer Protocol) pour Bêta ESA
  - Relais entrant pour Bêta ESA (facultatif)
  - Activer les en-têtes de journal pour capturer le verdict de spam dans les journaux de messagerie (facultatif)
- Configurer l'appliance de production
  - Routes SMTP pour ESA de production
  - Création du profil de renvoi
  - Création du profil des contrôles de destination
  - Construction de filtre de message pour la production ESA
- Vérifier
- Dépannage
- Informations supplémentaires (facultatif)
- Informations connexes

Introduction

Ce document décrit comment configurer un appareil de sécurité de la messagerie électronique Cisco (ESA) bêta pour recevoir un flux de messages copié d'un ESA de production à des fins de test.

Informations générales

La procédure configure les écouteurs Bêta ESA, les autorisations de relais et les routes SMTP (Simple Mail Transfer Protocol), puis configure un filtre de messages Production ESA pour envoyer une copie BCC des messages à la Bêta ESA et vérifie la remise dans mail_logs. Résultat escompté : La version bêta de l'ESA accepte le trafic entrant et sortant copié de l'ESA de production pour test.

Conditions préalables

Environnement

- Un appareil de sécurité de la messagerie Cisco (ESA) de production et un ESA bêta.
- Écouteurs Bêta ESA : Écouteur public sur le port TCP 25 ; Écouteur privé sur le port TCP 26 (ou le port 25 uniquement lorsqu'une interface supplémentaire est disponible). Dans la version bêta hébergée CES, le port 587 est réservé au courrier sortant.
- S'applique au flux de courrier entrant et sortant copié de l'ESA de production vers l'ESA bêta à l'aide d'un filtre de messages ESA de production (BCC).

Exigences

Un accès administratif à l'interface graphique utilisateur et à la CLI ESA est requis.

Composants utilisés

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

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configurer l'appliance bêta

Configuration de l'écouteur pour Bêta ESA

La configuration initiale de l'écouteur doit être effectuée sur le ESA bêta.

1. Dans l'interface graphique utilisateur, accédez à Network > Listeners.
2. Sélectionnez Ajouter un écouteur....
3. Entrez le nom de l'écouteur et configurez un écouteur public sur le port TCP 25.
4. Sélectionnez Envoyer.
5. Répétez les étapes 2 à 4 pour ajouter un second écouteur.
6. Entrez le nom du processus d'écoute et configurez un processus d'écoute privé sur le port TCP 26. Ce processus d'écoute est utilisé pour le courrier sortant. Vous pouvez utiliser le port 25 uniquement lorsqu'une interface supplémentaire est disponible et configurée pour l'environnement. Dans la version bêta hébergée CES, le port 587 est réservé au courrier sortant.
7. Envoyer pour enregistrer les modifications apportées au récepteur.
8. Validez pour enregistrer toutes les modifications apportées à la configuration.

Groupe d'expéditeurs pour Bêta ESA

Pour le trafic relayé ou les messages sortants, ajoutez les adresses IP appropriées pour le ESA bêta afin qu'il accepte et relaie les messages du ESA de production.

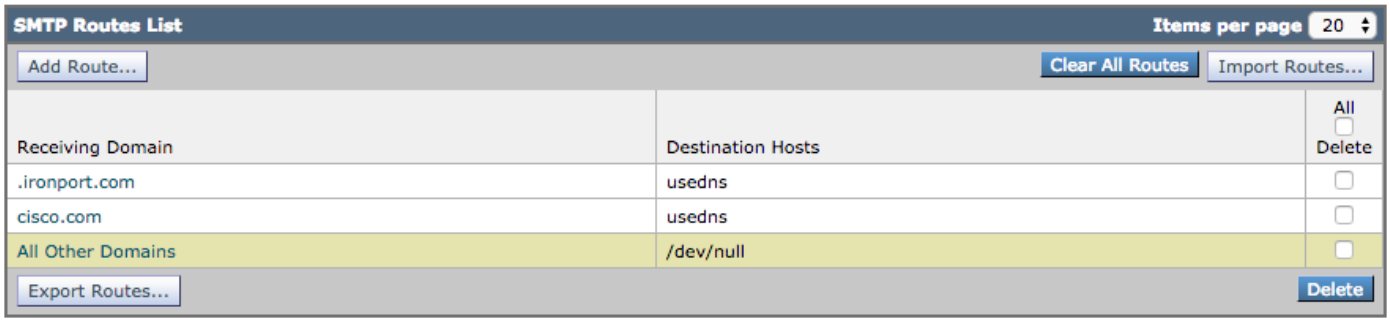
1. Dans l'interface graphique utilisateur, accédez à Politiques de messagerie > Vue d'ensemble de HAT.
2. Sélectionnez le groupe d'expéditeurs relais approprié. (généralement appelé RELAY ou RELAYLIST).
3. Sélectionnez Ajouter un expéditeur....
4. Pour l'expéditeur, utilisez l'adresse IP de l'ESA de production.
5. Saisissez les commentaires administratifs, le cas échéant.
6. Envoyer pour enregistrer les modifications apportées au groupe d'expéditeurs relais.
7. Validez pour enregistrer toutes les modifications apportées à la configuration.

Routes SMTP (Simple Mail Transfer Protocol) pour Bêta ESA

Configurez ces routes SMTP sur la Bêta ESA.

1. Dans l'interface utilisateur graphique, accédez à Network > SMTP Routes.
2. Si des routes SMTP actuelles existent, vous pouvez avoir besoin de les sélectionner et de les supprimer avant de continuer. Assurez-vous de consulter le guide de configuration des travaux pratiques bêta.
3. Sélectionnez Ajouter une route....
4. Entrez cisco.com pour le domaine de réception et USEDNS pour la destination.
5. Sélectionnez Envoyer.
6. Répétez les étapes 3 à 5 pour ajouter une deuxième route SMTP.
7. Entrez ironport.com pour le domaine de réception et USEDNS pour la destination.
8. Cliquez sur Submit.
9. Sélectionnez Tous les autres domaines pour le domaine de réception.
10. Entrez /dev/null pour Destination. Cela empêche le routage des messages à partir de la Bêta ESA pour tous les domaines qui ne sont pas configurés.
11. Sélectionnez Envoyer.
12. Validez pour enregistrer toutes les modifications apportées à la configuration.

Les routes SMTP sur la Bêta ESA apparaissent comme illustré dans cette image.



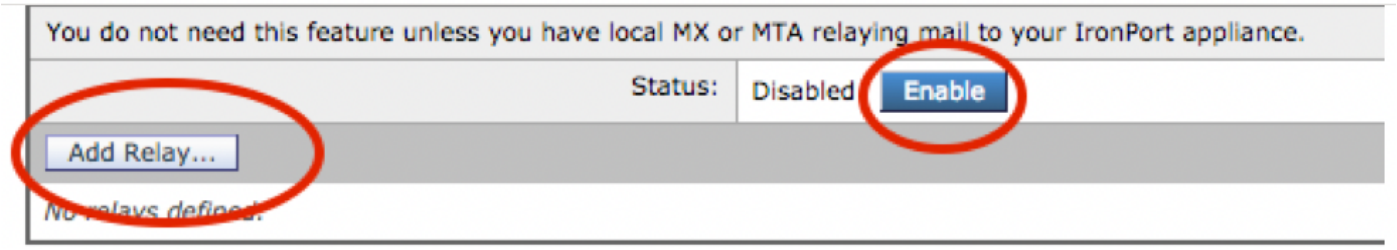
Remarque : Ajoutez les routes appropriées pour envoyer des e-mails afin de tester les domaines des utilisateurs finaux, le cas échéant.

Relais entrant pour Bêta ESA (facultatif)

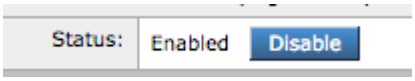
Le relais entrant permet à l'ESA bêta d'évaluer l'adresse IP de connexion et de récupérer un SenderBase Reputation Score (SBRS) au-delà de ce qui est disponible à partir de l'ESA de production.

La plupart des déploiements nécessitent un seul saut.

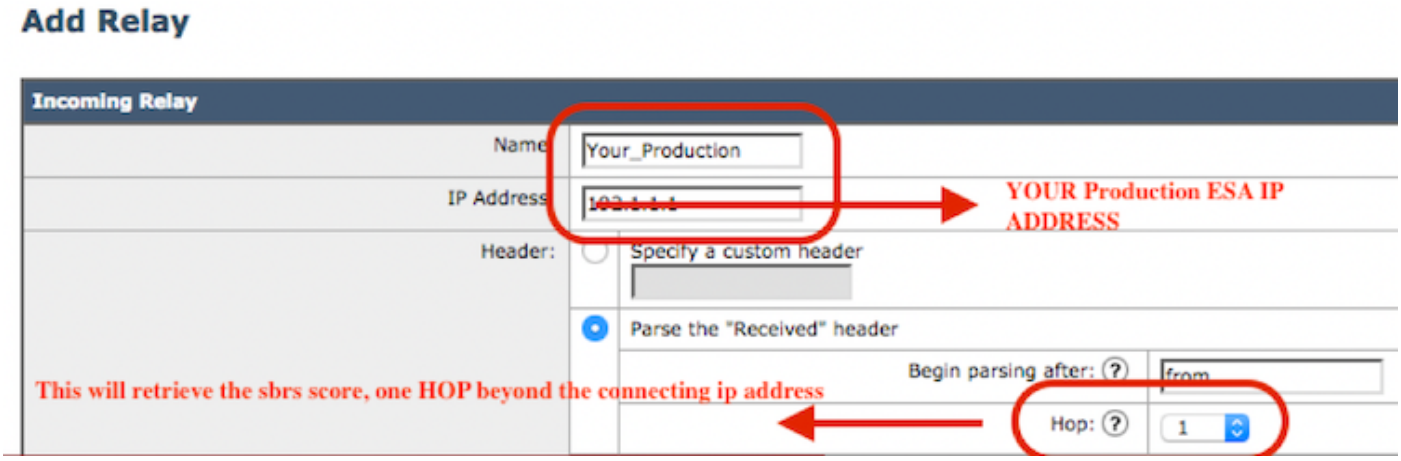
1. Dans l'interface graphique utilisateur, accédez à Network > Incoming Relay.
2. Cochez la case Activer.
3. Sélectionnez Ajouter un relais.
4. Dans le champ Nom, entrez un nom descriptif.
5. Dans le champ IP Address, saisissez l'adresse IP de l'ESA de production qui livre le courrier à l'ESA bêta. Utilisez un nom d'hôte partiel uniquement lorsque plusieurs hôtes envoient des messages.
6. Dans le champ Saut, saisissez 1.
7. Cliquez sur Submit, puis sur Commit.



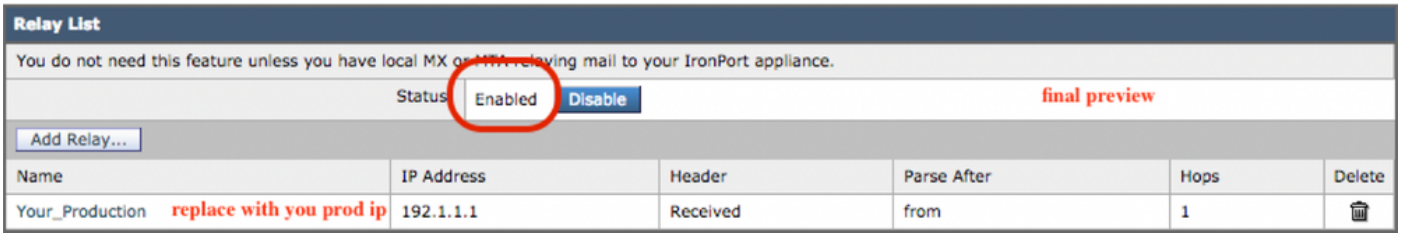
Relais entrant : État Désactivé.



Relais entrant : État activé, couleur blanche.



Relais entrant : Exemple de modèle



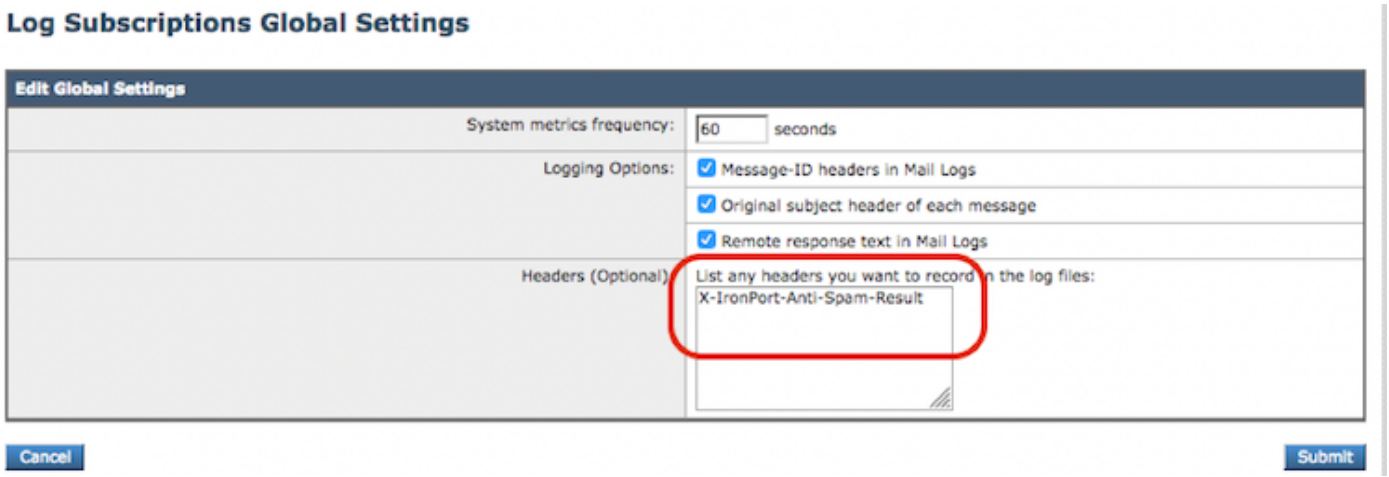
Relais entrant : Vue récapitulative après envoi.

Exemple d'entrée de journal de messagerie :

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

Activer les en-têtes de journal pour capturer le verdict de spam dans les journaux de messagerie (facultatif)

1. Dans l'interface graphique utilisateur, accédez à Administration système > Inscriptions au journal.
2. Sélectionnez Global Settings en bas de la page.
3. Dans la section En-têtes, sélectionnez Ajouter.
4. Saisissez X-IronPort-Anti-Spam-Result.
5. Sélectionnez Envoyer.
6. Cliquez sur Valider.



Consigner les en-têtes de spam dans les journaux de messagerie

Fin de la configuration côté bêta.

Configurer l'appliance de production

⚠ Mise en garde : Vous êtes sur le point d'apporter des modifications à une ESA de production. Assurez-vous de sauvegarder la configuration actuelle.

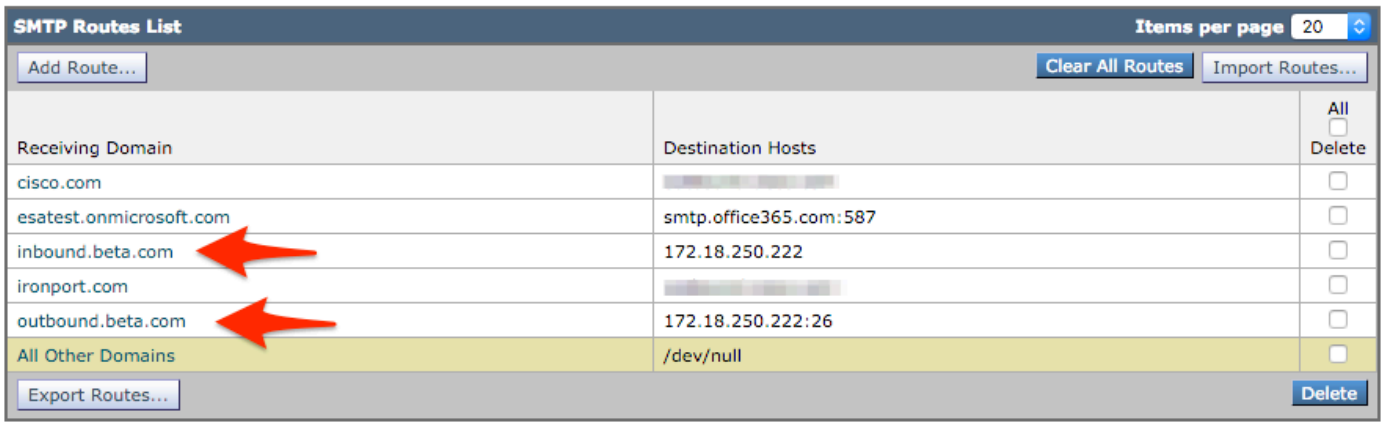
1. Dans l'interface utilisateur Web, accédez à Administration système > Fichier de configuration.
2. Dans la section Current Configuration, sélectionnez l'une des options de sauvegarde de la configuration actuelle sous forme de fichier :
   - Téléchargez le fichier sur l'ordinateur local pour l'afficher ou l'enregistrer.
   - Envoyer le fichier par e-mail : your_email_address@domain.com>
3. Cliquez sur Submit.

Routes SMTP pour ESA de production

Ajoutez des routes SMTP pour autoriser les copies en copie cachée de tous les e-mails entrants et sortants de l'ESA de production vers l'ESA bêta. Dans cet exemple, inbound.beta.com et outbound.beta.com sont utilisés.

1. Dans l'interface utilisateur graphique, accédez à Network > SMTP Routes.
2. Sélectionnez Ajouter une route....
3. Entrez inbound.beta.com comme domaine de réception.
4. Saisissez l'adresse IP de l'écouteur public Bêta ESA créé précédemment pour les hôtes de destination.
5. Saisissez 25 pour le port.
6. Sélectionnez Envoyer.
7. Répétez les étapes 2 à 5 pour ajouter la deuxième route.
8. Entrez outbound.beta.com comme domaine de réception.
9. Saisissez l'adresse IP de l'écouteur privé Bêta ESA créé précédemment pour les hôtes de destination.
10. Saisissez 26 pour le port.
11. Sélectionnez Envoyer.
12. Validez pour enregistrer toutes les modifications apportées à la configuration.

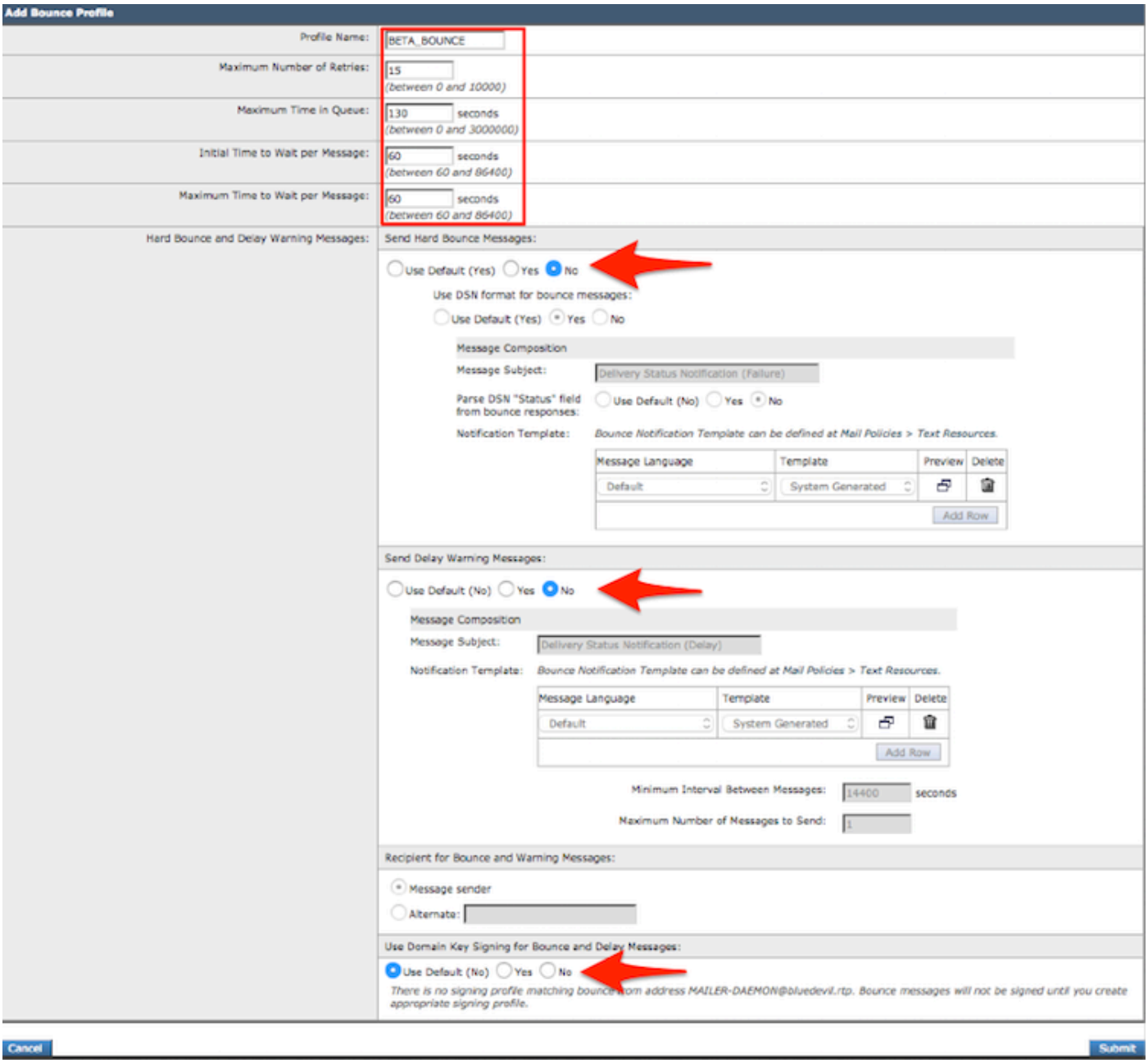
Les routes SMTP sur l'ESA de production apparaissent comme illustré dans cette image.



Création du profil de renvoi

La combinaison d'un profil de renvoi et d'un profil de contrôle de la destination protège le flux de messagerie de production contre les retards ou les échecs lors de la remise des messages aux hôtes bêta. Cette configuration s'applique uniquement aux messages bêta.

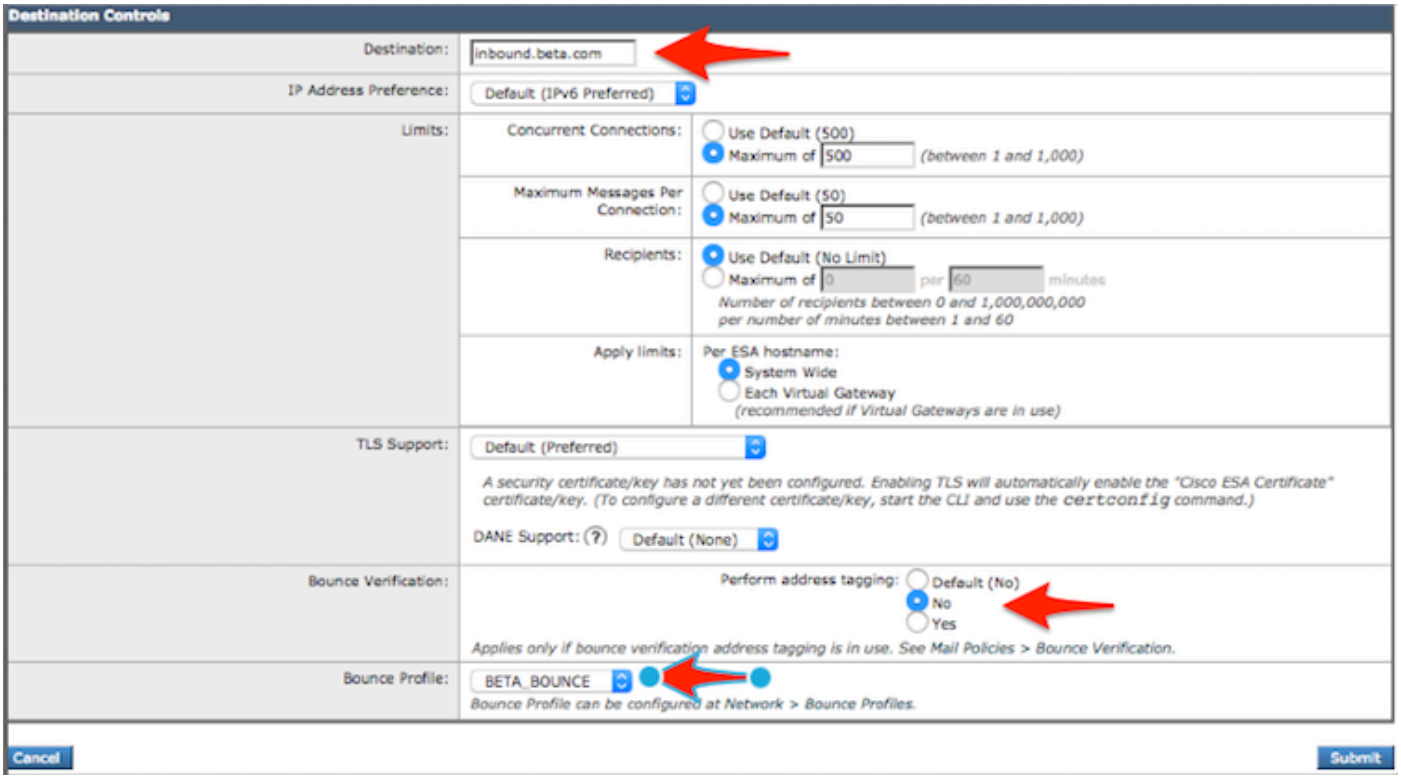
1. Dans l'interface utilisateur Web, accédez à Réseau > Profils de renvoi > Ajouter un profil de renvoi.
2. Nombre maximal de tentatives : 15
3. Temps maximal en file d'attente : 130
4. Délai d'attente initial par message : 60
5. Délai d'attente maximal par message : 60
6. Envoyer des messages de renvoi direct : NON
7. Envoyer des messages d'avertissement de délai : NON
8. Utiliser la signature de clé de domaine pour les messages de renvoi et de délai : NON
9. Soumettre pour enregistrer les modifications apportées à ce nouveau profil de renvoi.
10. Sélectionnez Commit pour enregistrer toutes les modifications apportées à la configuration.



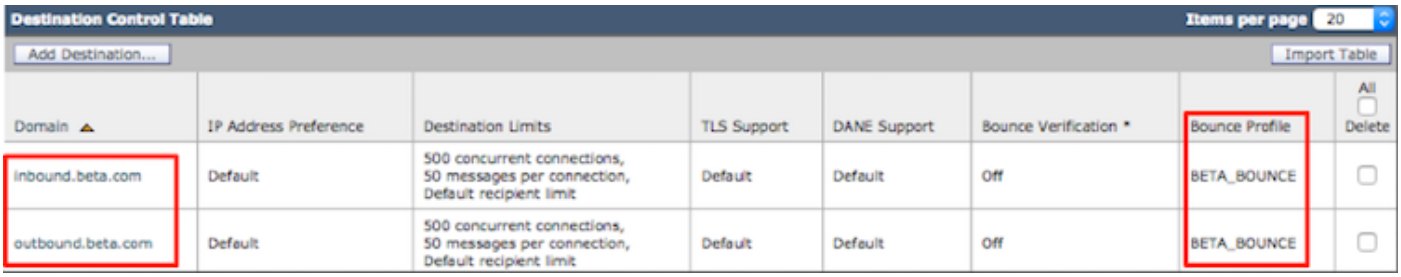
Remarque : les valeurs numérotées sont configurées de manière très agressive pour empêcher les sauvegardes de la file d'attente de remise en cas d'interruption de la remise aux hôtes bêta. Les valeurs peuvent être modifiées à la préférence. Les paramètres de notification sont intentionnellement définis sur NON pour empêcher toute notification utilisateur d'être transmise à partir des filtres CCI.

Création du profil des contrôles de destination

1. Dans l'interface utilisateur Web, accédez à Politiques de messagerie > Contrôles de destination > Ajouter une destination.
2. Destination : inbound.beta.com
3. Vérification du renvoi : > Étiquetage des adresses : NON > ou par défaut (NON)
4. Profil de renvoi : BÊTA_REBOND
5. Configurez les valeurs restantes en fonction des préférences de l'administrateur.
6. Envoyer pour enregistrer les modifications apportées à ce nouveau profil de contrôle de la destination.
7. Répétez les étapes 2 à 6 et utilisez outbound.beta.com pour Destination.
8. Envoyer pour enregistrer les modifications apportées à ce nouveau profil de contrôle de la destination.
9. Validez pour enregistrer toutes les modifications apportées à la configuration.



Ajoutez des profils de contrôle de destination.



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	

Vue récapitulative des nouveaux profils de contrôle de destination.

Construction de filtre de message pour la production ESA

À partir de l'interface de ligne de commande (CLI) de l'ESA de production, créez un filtre de message qui envoie des copies en copie cachée des e-mails à l'écouteur approprié sur l'ESA bêta.

1. Accédez à Filters > NEW.
2. Copiez et collez cet exemple de filtre de message, puis mettez à jour les valeurs si nécessaire :

```
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 reveniez à l'invite CLI principale.
4. Validez pour enregistrer toutes les modifications apportées à la configuration.

Remarque : Limitez le trafic copié dans le filtre de messages en fonction de sendergroup, recv-listener, mail-from ou d'autres règles et syntaxes disponibles. Consultez le Guide de l'utilisateur ESA pour obtenir le récapitulatif complet des règles de filtre de message et des règles de filtre.

Vérifier

Utilisez cette section pour confirmer que la configuration fonctionne comme prévu.

Pour vérifier que la Bêta ESA accepte le trafic de messagerie de la Production ESA, exécutez cette commande à partir de l'interface de ligne de commande sur la Bêta 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
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 outb
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
```

La communication SMTP est établie sur 172.18.250.222 (appliance bêta). Le trafic est envoyé depuis 172.18.250.224 (appareil de production).

Le groupe d'expéditeurs qui reçoit la communication est RELAY pour le trafic relayé du réseau 172.18.250.1/24.

Les entrées restantes indiquent le traitement du message TEST 2.

Sur Production ESA, exécutez cette commande pour vérifier le MID traité :

<#root>

tail mail_logs

L'ESA Production affiche ce résultat :

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

Ce résultat confirme une duplication claire du message et indique que le message a été copié en copie cachée sur le ESA bêta et l'utilisateur final de test comme prévu.

Dépannage

Si la vérification échoue, vérifiez la configuration de l'écouteur, les entrées du groupe d'expéditeurs, les routes SMTP, les paramètres de relais entrant et la configuration du filtre de messages sur les deux ESA. Consultez également mail_logs sur les deux appliances pour

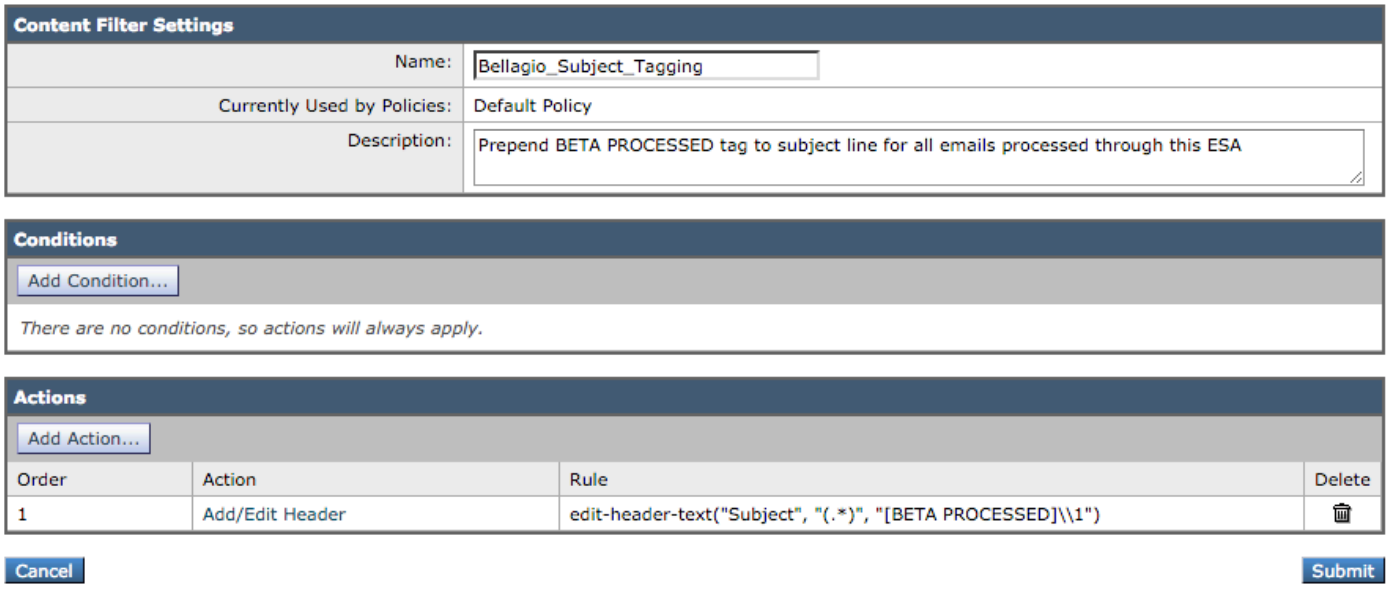
confirmer les événements de connexion, de relais et de livraison.

Informations supplémentaires (facultatif)

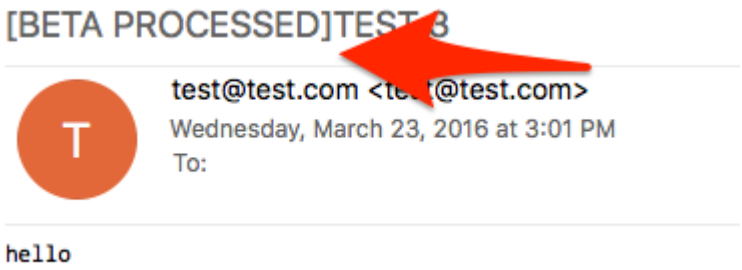
Vous pouvez utiliser un filtre de contenu pour différencier le trafic de messagerie de production et bêta pour les utilisateurs finaux de test.

1. Dans l'interface utilisateur Web de la version Bêta ESA, accédez à Politiques de messagerie > Filtres de contenu entrant ou Politiques de messagerie > Filtres de contenu sortant.
2. Créez un filtre de contenu de base qui exécute l'action Ajouter/Modifier un en-tête.
3. Sélectionnez Envoyer.
4. Accédez à Politiques de messagerie > Politiques de messages entrants ou Politiques de messages > Politiques de messages sortants.
5. Activez le nouveau filtre de contenu et ajoutez-le à la stratégie.
6. Sélectionnez Envoyer.
7. Cliquez sur Commit afin d'enregistrer toutes les modifications apportées à la configuration.

Une fois cette étape terminée, le filtre de contenu de l'ESA bêta apparaît comme illustré dans ces images.



Une fois que la version bêta de l'ESA a traité un e-mail, la ligne d'objet apparaît comme illustré dans cette image.



Informations connexes

- Configuration d'un ESA/SMA pour les mises à jour intermédiaires
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.