Détectez les messages électroniques charriés sur l'ESA et créez les exceptions pour les expéditeurs qui sont permis pour charrier

Contenu

Introduction

Ce document décrit comment contrôler la mystification d'email sur l'appliance de sécurité du courrier électronique de Cisco (ESA) et comment créer des exceptions pour les utilisateurs permis pour envoyer les emails charriés.

Conditions préalables

Conditions requises

Votre ESA devrait être traitement entrant et mails sortants, et devrait employer une configuration standard de RELAYLIST pour signaler des messages comme sortant.

Composants utilisés

Les informations dans ce document sont basées sur l'ESA avec n'importe quelle version d'AsyncOS. 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 opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Les éléments spécifiques utilisés incluent :

- Dictionnaire : utilisé pour enregistrer tous vos domaines internes.
- Filtre de message : utilisé pour manipuler la logique de détecter l'email charrié et d'insérer une en-tête sur laquelle les filtres satisfaits peuvent agir.
- Quarantaine de stratégie : utilisé pour enregistrer des duplicartes des emails charriés temporairement. Consider ajoutant l'adresse IP des messages libérés au MY_TRUSTED_SPOOF_HOSTS pour empêcher de futurs messages de cet expéditeur d'écrire la stratégie mettent en quarantaine.
- MY_TRUSTED_SPOOF_HOSTS : liste pour mettre en référence vos adresses IP de envoi de confiance. Ajoutant une adresse IP d'un expéditeur à cette liste ignorera la quarantaine et permettra à l'expéditeur pour charrier. Nous plaçons les expéditeurs de confiance dans votre groupe d'expéditeur MY_TRUSTED_SPOOF_HOSTS de sorte que des messages charriés de ces expéditeurs ne soient pas mis en quarantaine.
- RELAYLIST : le répertoriez pour authentifier les adresses IP qui sont permises pour transmettre par relais, ou envoyez l'email sortant. Si l'email est fourni par l'intermédiaire de ce groupe d'expéditeur la supposition est que le message n'est pas un message charrié.

  Remarque: Si le groupe d'expéditeur s'appelle quelque chose différente que MY_TRUSTED_SPOOF_HOSTS ou RELAYLIST, vous devrez modifier le filtre avec le nom de groupe correspondant d'expéditeur. En outre, si vous avez de plusieurs auditeurs, vous pouvez également avoir plus d'un MY_TRUSTED_SPOOF_HOSTS.

Informations générales

La mystification est activée par défaut sur Cisco ESA. Il y a plusieurs, des motifs valables pour permettre à d'autres domaines pour envoyer en fonction votre nom. Un exemple classique, administrateur ESA peut vouloir à contrôler les emails charriés en mettant en quarantaine les messages charriés avant qu'ils soient fournis.

Pour prendre une mesure spécifique telle que la quarantaine sur l'email charrié, vous devez d'abord détecter l'email charrié.

Quelle est mystification d'email ?

La mystification d'email est le contrefaçon d'une en-tête d'email de sorte que le message semble avoir provenu de quelqu'un ou quelque part autre que la source réelle. La mystification d'email est une tactique utilisée dans le phishing et des campagnes de Spam parce que les gens sont pour ouvrir un email quand ils le pensent a été envoyées par une source légitime.

Comment détecter l'email charrié ?

Vous voudrez filtrer tous les messages qui ont un expéditeur d'enveloppe (Messagerie-de) et « amical » (de) de l'en-tête qui contiennent un de vos propres domaines entrants dans l'adresse e-mail.

Comment permettre la mystification pour les expéditeurs spécifiques ?

En mettant en application le filtre de message fourni dans cet article, des messages charriés sont étiquetés avec une en-tête, et le filtre satisfait est utilisé pour agir sur l'en-tête. Pour ajouter une exception, ajoutez simplement l'IP d'expéditeur à MY_TRUSTED_SPOOF_HOSTS.

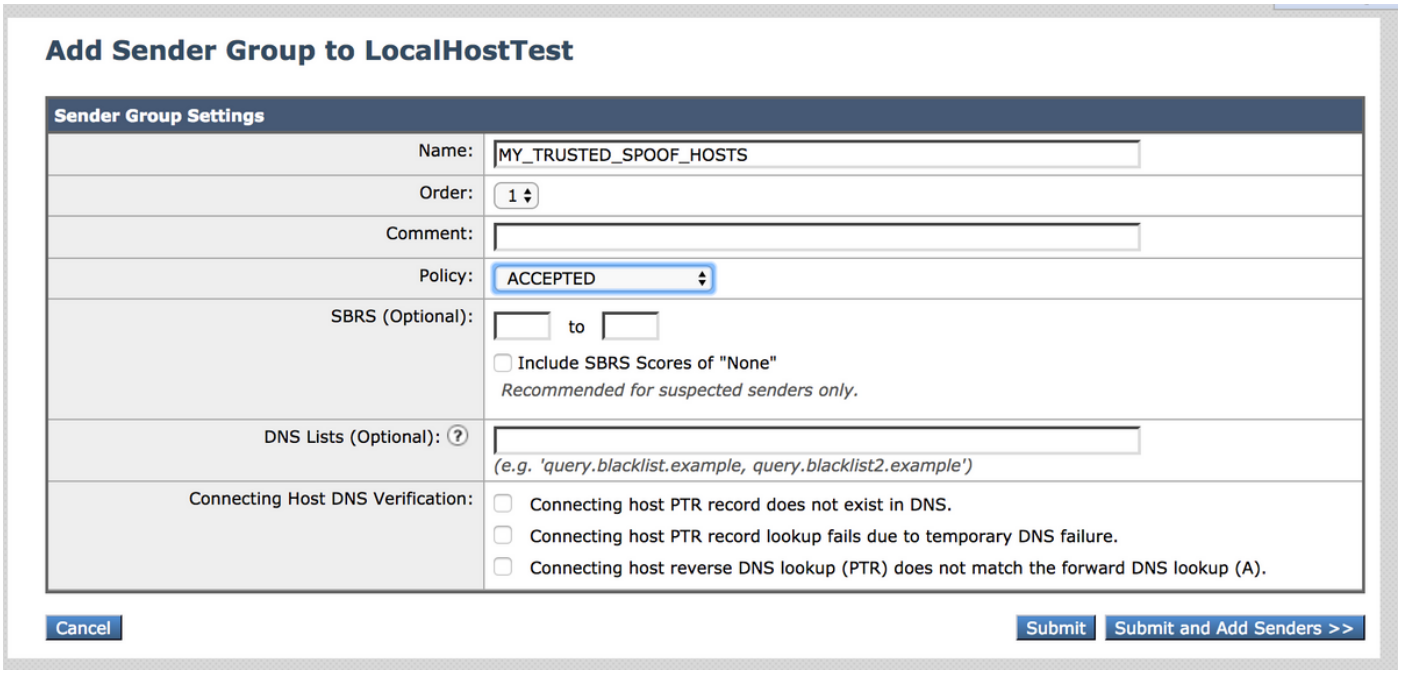
Configurez

Créez un Sendergroup

Créez un dictionnaire pour tous les domaines que vous voulez pour désactiver la mystification pour sur l'ESA :

1. Du GUI ESA, naviguez **pour envoyer par mail des stratégies > l'aperçu de CHAPEAU**
2. Cliquez sur **Add**.
3. Dans le domaine de « nom » spécifiez **MY_TRUSTED_SPOOF_HOSTS**
4. Dans le domaine de « commande » spécifiez **1**
5. Pour le champ de « stratégie », spécifiez **REÇU**
6. Cliquez sur Submit pour sauvegarder des modifications.
7. En conclusion, la **validation de** clic **change** pour sauvegarder la configuration

Exemple
:

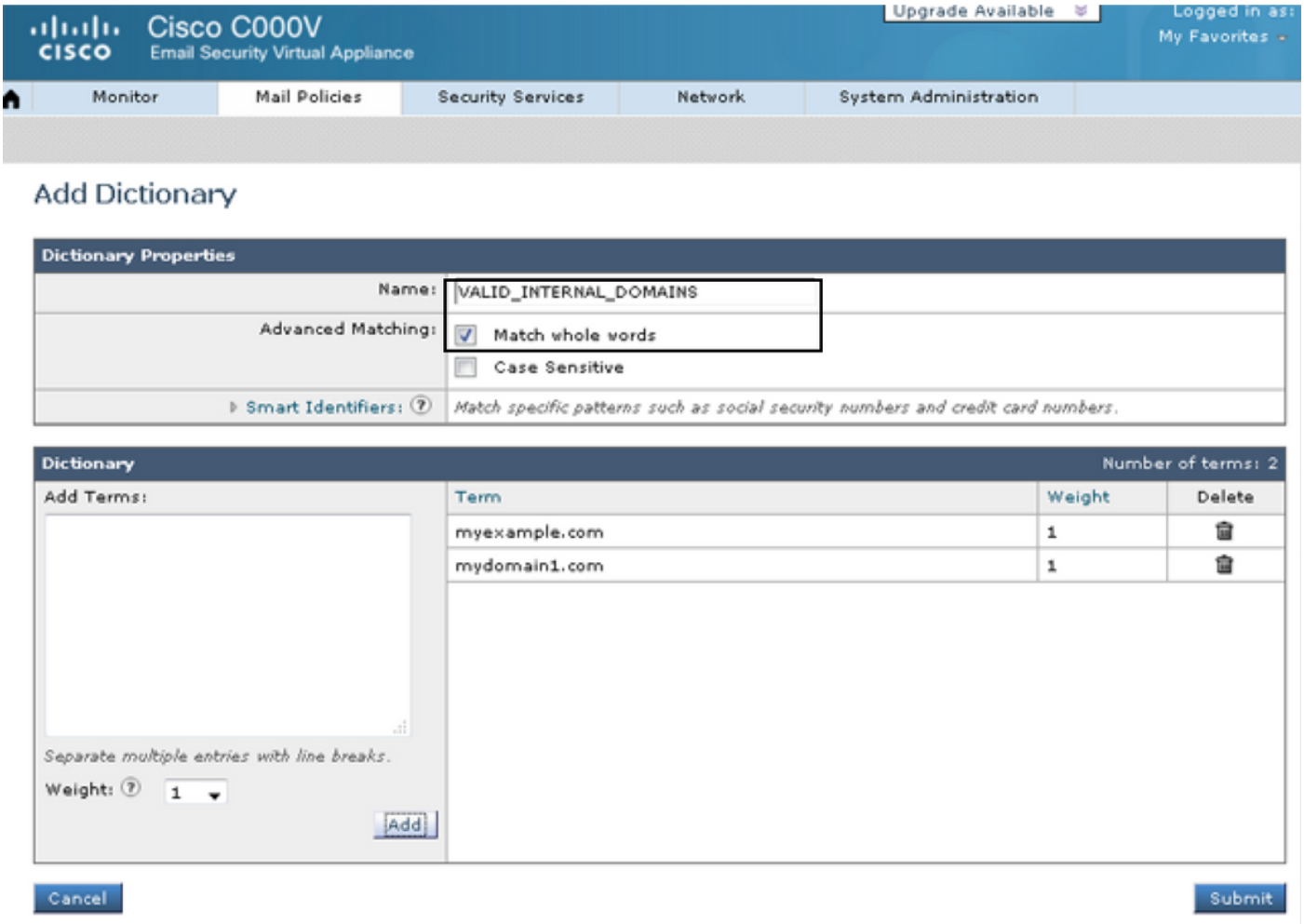


Créez un dictionnaire

Créez un dictionnaire pour tous les domaines que vous voulez pour désactiver la mystification pour sur l'ESA :

1. Du GUI ESA, naviguez **pour envoyer par mail des stratégies > des dictionnaires.**
2. Cliquez sur Add le **dictionnaire.**
3. Dans le domaine de « nom » spécifiez « VALID_INTERNAL_DOMAINS », par exemple.
4. Sous « ajoutez les termes », ajoutent tous les domaines que vous voulez pour détecter la mystification.
5. Cliquez sur Submit pour sauvegarder les modifications de dictionnaire.
6. En conclusion, la **validation de** clic **change** pour sauvegarder la configuration

Exemple :



Créez un filtre de message

Ensuite, vous devrez créer un filtre de message afin d'accroître le dictionnaire juste créé, « VALID_INTERNAL_DOMAINS » :

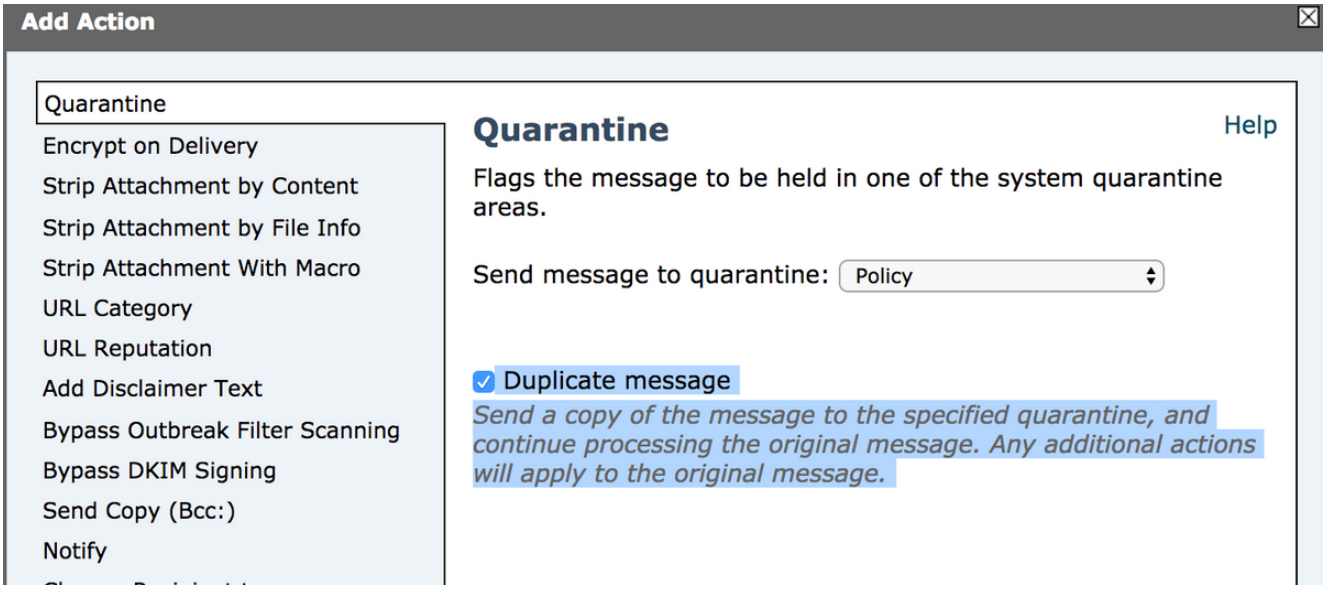
1. Connectez à l'interface de ligne de commande (CLI) de l'ESA.
2. Exécutez les **filtres de** commande.
3. Exécutez la commande **nouvelle** pour créer un nouveau filtre de message.
4. Copiez et collez l'exemple suivant de filtre, faisant édite pour vos noms de groupe réels d'expéditeur si nécessaire :

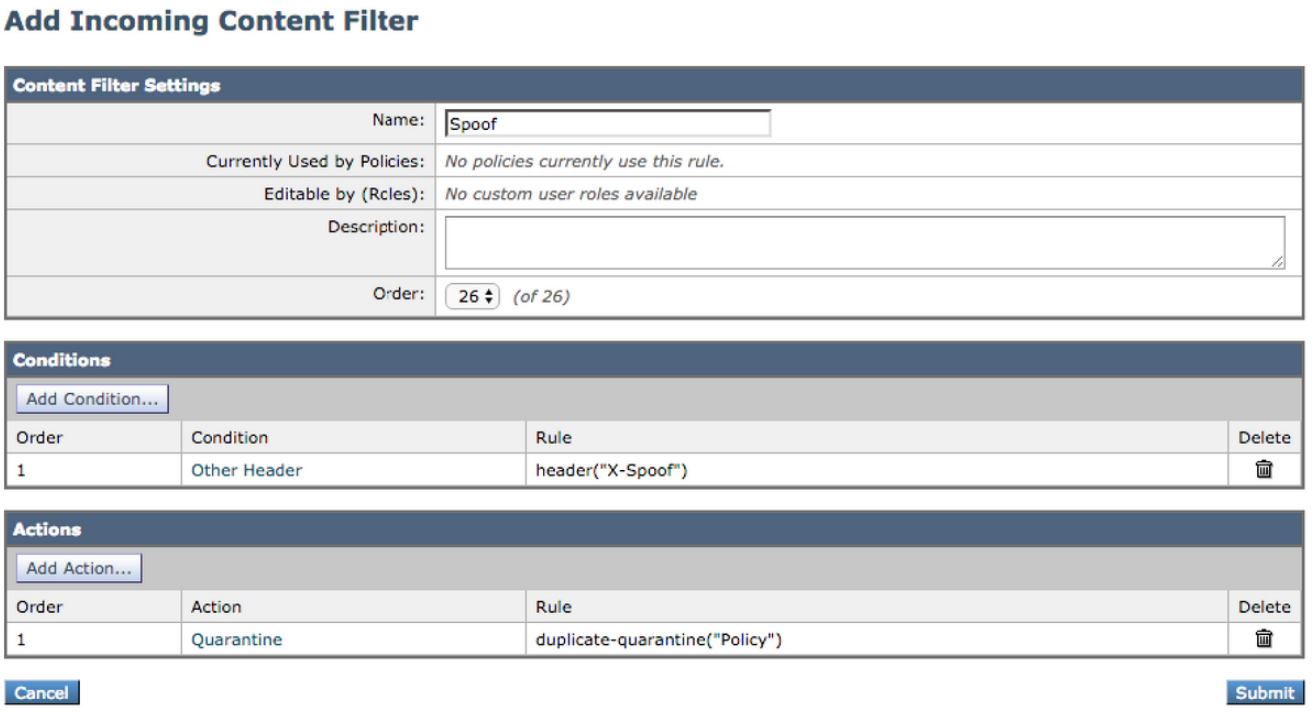
```
mark_spoofed_messages:
if(
(mail-from-dictionary-match("VALID_INTERNAL_DOMAINS", 1))
OR (header-dictionary-match("VALID_INTERNAL_DOMAINS","From", 1)))
AND ((sendergroup != "RELAYLIST")
AND (sendergroup != "MY_TRUSTED_SPOOF_HOSTS")
)
{
insert-header("X-Spoof", "");
}
```

5. Revenez à la demande CLI et à la **validation** principales de passage pour sauvegarder la

configuration.

6. Naviguez vers des stratégies GUI > de messagerie > les filtres satisfaits entrants
7. Créez le filtre satisfait entrant qui agit sur l'en-tête de charrier X-charrient : Ajoutez l'action : doublon-quarantaine (« stratégie ").
   Remarque: La caractéristique en double de message affichée ici gardera une copie du message, et continue à envoyer le premier message au destinataire.





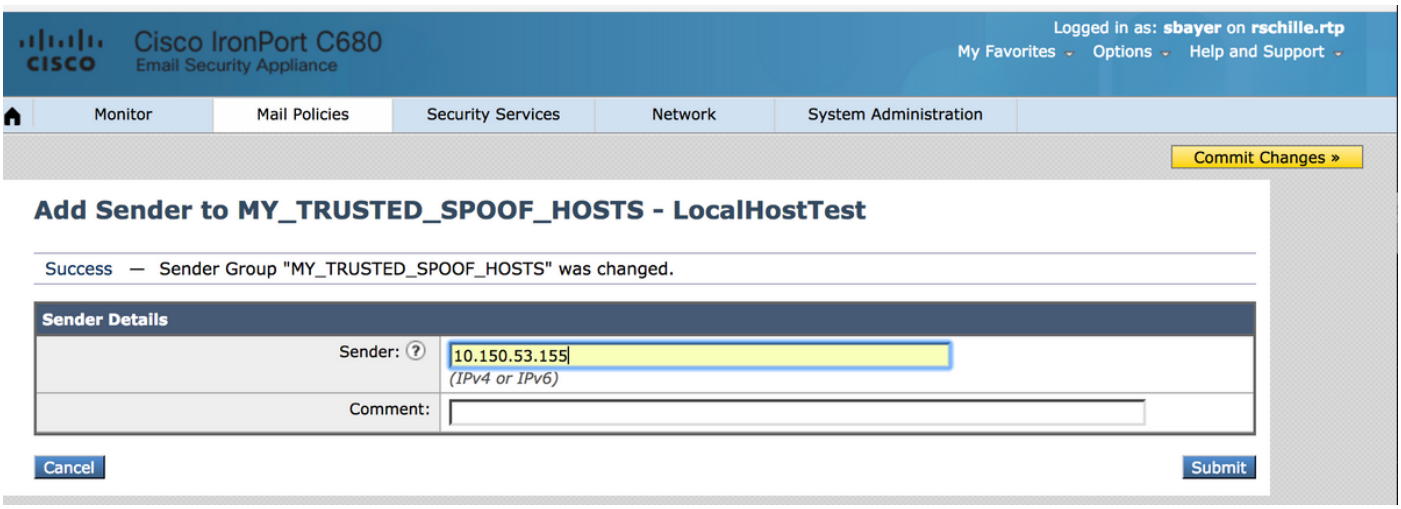
8. Filtre satisfait de lien aux stratégies de messagerie entrante à stratégies de messagerie entrante de Policies> GUI > de messagerie
9. Soumettez et commettez les modifications

Ajoutez les Charrier-exceptions à MY_TRUSTED_SPOOF_HOSTS

En conclusion, vous devrez ajouter des charrier-exceptions (des adresses IP ou des adresses Internet) au sendergroup MY_TRUSTED_SPOOF_HOSTS.

1. Naviguez par l'intermédiaire du GUI de Web : **Stratégies de messagerie > aperçu de CHAPEAU**
2. Cliquez sur et ouvrez le groupe d'expéditeur MY_TRUSTED_SPOOF_HOSTS.
3. Cliquez sur en fonction « ajoutent l'expéditeur… » pour ajouter une adresse IP, une plage, un nom d'hôte, ou un nom d'hôte partiel.
4. Cliquez sur Submit pour sauvegarder les modifications d'expéditeur.
5. En conclusion, la **validation de** clic **change** pour sauvegarder la configuration.

Exemple :



Vérifiez

Vérifiez les messages charriés sont mis en quarantaine

Envoyez un message-test spécifiant un de vos domaines comme expéditeur d'enveloppe. Validez le filtre fonctionne comme prévu en exécutant une piste de message sur ce message. Le résultat prévu est que le message obtiendra mis en quarantaine parce que nous n'avons créé aucune exception pourtant pour ces expéditeurs qui sont permis pour charrier.

```
Thu Apr 23 07:09:53 2015 Info: MID 102 ICID 9 RID 0 To: <test_user@domain.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 Subject 'test1'
Thu Apr 23 07:10:07 2015 Info: MID 102 ready 177 bytes from <user_1@example.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Thu Apr 23 07:10:11 2015 Info: MID 102 interim verdict using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:10:11 2015 Info: MID 102 antivirus negative
Thu Apr 23 07:10:12 2015 Info: MID 102 quarantined to "Policy" (message
filter:quarantine_spoofed_messages)
Thu Apr 23 07:10:12 2015 Info: Message finished MID 102 done
```

Vérifiez les messages de Charrier-exception sont livrés

Les expéditeurs de « Charrier-exception » sont des adresses IP dans vos groupes d'expéditeur référencés dans le filtre ci-dessus.

RELAYLIST est mis en référence parce qu'il est utilisé par l'ESA pour envoyer la messagerie sortante. Les messages envoyé par RELAYLIST sont messagerie en général sortante, et pas comprenant ceci créeraient des faux positifs, ou des messages sortants mis en quarantaine par le filtre ci-dessus.

Exemple de cheminement de message d'une adresse IP de « Charrier-exception » qui a été ajoutée à MY_TRUSTED_SPOOF_HOSTS. L'action prévue est livrent et pas mettent en quarantaine. (On permet à cet IP pour charrier).

```
Thu Apr 23 07:25:57 2015 Info: Start MID 108 ICID 11
Thu Apr 23 07:25:57 2015 Info: MID 108 ICID 11 From: <user_1@example.com>
Thu Apr 23 07:26:02 2015 Info: MID 108 ICID 11 RID 0 To: <test_user@domain.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 Subject 'test2'
Thu Apr 23 07:26:10 2015 Info: MID 108 ready 163 bytes from <user_1@example.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Thu Apr 23 07:26:10 2015 Info: MID 108 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:26:10 2015 Info: MID 108 antivirus negative
Thu Apr 23 07:26:10 2015 Info: MID 108 queued for delivery
Thu Apr 23 07:26:10 2015 Info: Delivery start DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: Message done DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: MID 108 RID [0] Response '2.0.0 t58EVG9N031598 Message accepted
for delivery'
Thu Apr 23 07:26:11 2015 Info: Message finished MID 108 done
```

Informations connexes

- Filtrage de messagerie charrié par ESA
- Charriez la protection utilisant la vérification d'expéditeur