Détecter les e-mails frauduleux sur ESA et créer des exceptions

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

- En quoi consiste la mystification des e-mails
- Détection des e-mails frauduleux
- Autorisation de l'usurpation pour des expéditeurs spécifiques

Configurer

- Créer un groupe d'expéditeurs
- Créer un dictionnaire
- Créer un filtre de message
- Ajouter des exceptions d'usurpation à MY_TRUSTED_SPOOF_HOSTS

Vérifier

- Vérifier que les messages usurpés sont mis en quarantaine
- Vérification de la remise des messages d'exception d'usurpation

Informations connexes

Introduction

Ce document décrit comment contrôler l'usurpation d'e-mail sur Cisco ESA et comment créer des exceptions pour les utilisateurs autorisés à envoyer des e-mails usurpés.

Conditions préalables

Exigences

Votre appareil de sécurité de la messagerie électronique (ESA) doit traiter les messages entrants et sortants et utiliser une configuration standard de RELAYLIST pour marquer les messages comme sortants.

Composants utilisés

Les composants spécifiques utilisés sont les suivants :

- Dictionnaire : utilisé pour stocker tous vos domaines internes.
- Filtre de message : utilisé pour gérer la logique de détection des e-mails frauduleux et insérer un en-tête sur lequel les filtres de contenu peuvent agir.
- Quarantaine des stratégies : utilisé pour stocker temporairement des doublons d'e-mails usurpés. Pensez à ajouter l'adresse IP des messages libérés à MY_TRUSTED_SPOOF_HOSTS pour empêcher les messages futurs de cet expéditeur d'entrer dans la quarantaine de la stratégie.
- MY_TRUSTED_SPOOF_HOSTS : pour référencer vos adresses IP d'envoi approuvées. L'ajout de l'adresse IP d'un expéditeur à cette liste ignore la quarantaine et permet à l'expéditeur de se tromper. Vous placez les expéditeurs approuvés dans votre groupe d'expéditeurs MY_TRUSTED_SPOOF_HOSTS afin que les messages usurpés de ces expéditeurs ne soient pas mis en quarantaine.
- RELAYLIST : pour authentifier les adresses IP autorisées à relayer ou à envoyer des e-mails sortants. Si l'e-mail est remis via ce groupe d'expéditeurs, il est supposé qu'il ne s'agit pas d'un message usurpé.

Remarque : Si l'un des groupes d'expéditeurs est appelé différemment de MY_TRUSTED_SPOOF_HOSTS ou RELAYLIST, vous devez modifier le filtre avec le nom de groupe d'expéditeurs correspondant. En outre, si vous avez plusieurs écouteurs, vous avez également plusieurs MY_TRUSTED_SPOOF_HOSTS.

Les informations contenues dans ce document sont basées sur l'ESA avec n'importe quelle version d'AsyncOS.

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.

Informations générales

La mystification est activée par défaut sur Cisco ESA. Il existe plusieurs raisons valables d'autoriser d'autres domaines à envoyer en votre nom. Par exemple, ESA Administrator souhaite contrôler les e-mails usurpés en mettant en quarantaine les messages usurpés avant leur remise.

Pour effectuer une action spécifique, telle que la mise en quarantaine sur les e-mails usurpés, vous devez d'abord détecter les e-mails usurpés.

En quoi consiste la mystification des e-mails

L'usurpation d'e-mail est la falsification d'un en-tête d'e-mail de sorte que le message semble provenir de quelqu'un ou d'un autre endroit que la source réelle. L'usurpation d'adresse e-mail est une tactique utilisée dans les campagnes d'hameçonnage et de spam, car les utilisateurs sont plus susceptibles d'ouvrir un e-mail lorsqu'ils pensent qu'il a été envoyé par une source légitime.

Détection des e-mails frauduleux

Vous voulez filtrer tous les messages qui ont un expéditeur d'enveloppe (Mail-From) et un en-tête convivial de (From) qui contiennent l'un de vos propres domaines entrants dans l'adresse e-mail.

Autorisation de l'usurpation pour des expéditeurs spécifiques

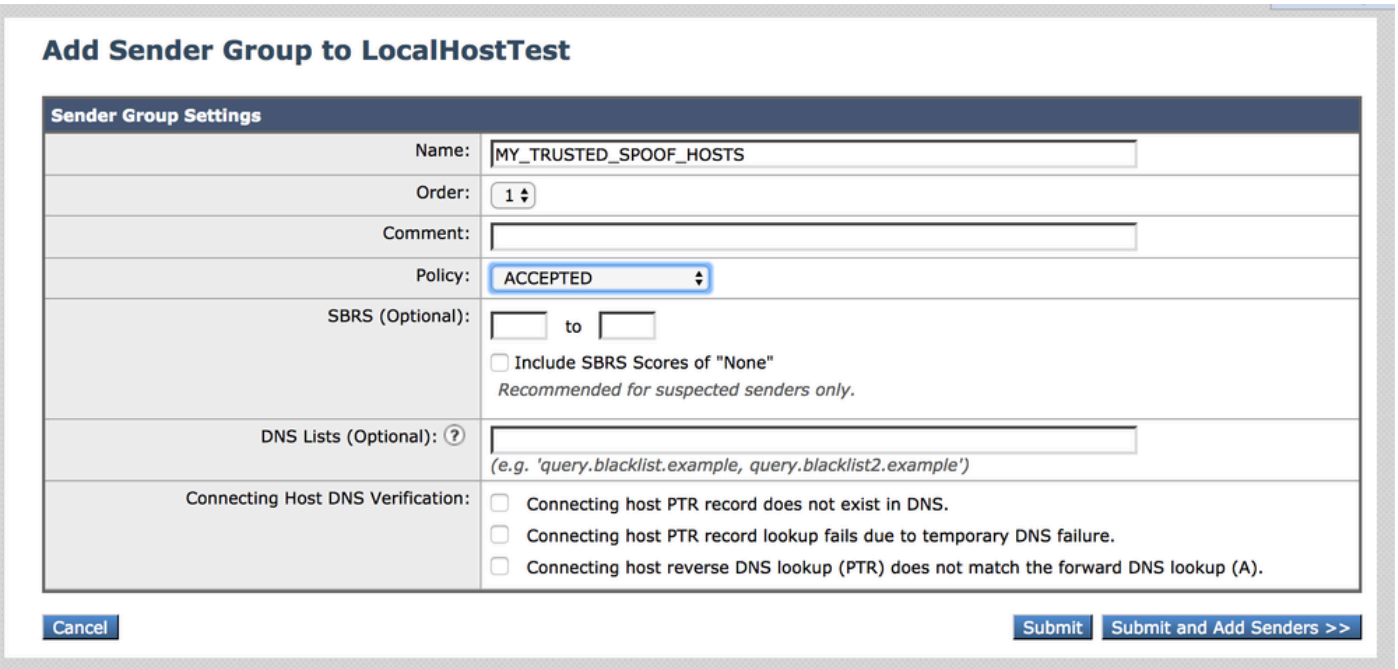
Lorsque vous implémentez le filtre de messages fourni dans cet article, les messages usurpés sont marqués d'un en-tête et le filtre de contenu est utilisé pour exécuter une action sur l'en-tête . Pour ajouter une exception, ajoutez simplement l'adresse IP de l'expéditeur à MY_TRUSTED_SPOOF_HOSTS.

Configurer

Créer un groupe d'expéditeurs

1. Dans l'interface graphique utilisateur ESA, accédez à Politiques de messagerie > Vue d'ensemble de HAT
2. Cliquez sur Ajouter.
3. Dans le champ Nom, spécifiez MY_TRUSTED_SPOOF_HOSTS.
4. Dans le champ Commande, spécifiez 1.
5. Pour le champ Policy, spécifiez ACCEPTED.
6. Cliquez sur Submit pour enregistrer les modifications.
7. Enfin, cliquez sur Commit Changes pour enregistrer la configuration

Exemple :

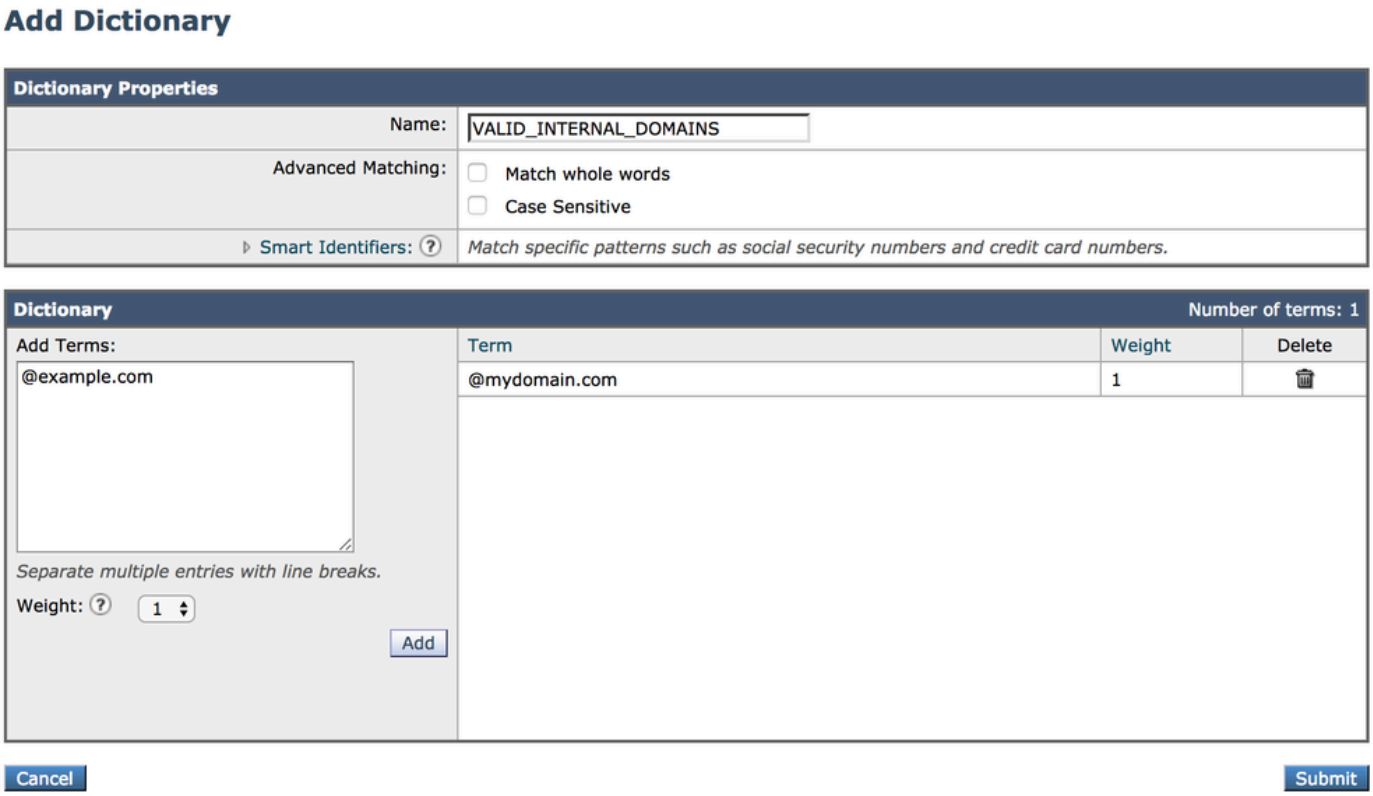


Créer un dictionnaire

Créez un dictionnaire pour tous les domaines pour lesquels vous souhaitez désactiver l'usurpation sur l'ESA :

1. Dans l'interface graphique utilisateur ESA, accédez à Politiques de messagerie > Dictionnaires.
2. Cliquez sur Ajouter un dictionnaire.
3. Dans le champ Nom, spécifiez « VALID_INTERNAL_DOMAINS » pour que la copie et le collage du filtre de message soient exempts d'erreurs.
4. Sous Ajouter des termes, ajoutez tous les domaines pour lesquels vous souhaitez détecter l'usurpation. Entrez le domaine avec le signe @ avant le domaine et cliquez sur add.
5. Assurez-vous que la case Correspondance des mots entiers est décochée.
6. Cliquez sur Submit pour enregistrer les modifications apportées au dictionnaire.
7. Enfin, cliquez sur Commit Changes pour enregistrer la configuration.

Exemple :



Créer un filtre de message

Ensuite, vous devez créer un filtre de message afin d'exploiter le dictionnaire que vous venez de créer, "VALID_INTERNAL_DOMAINS" :

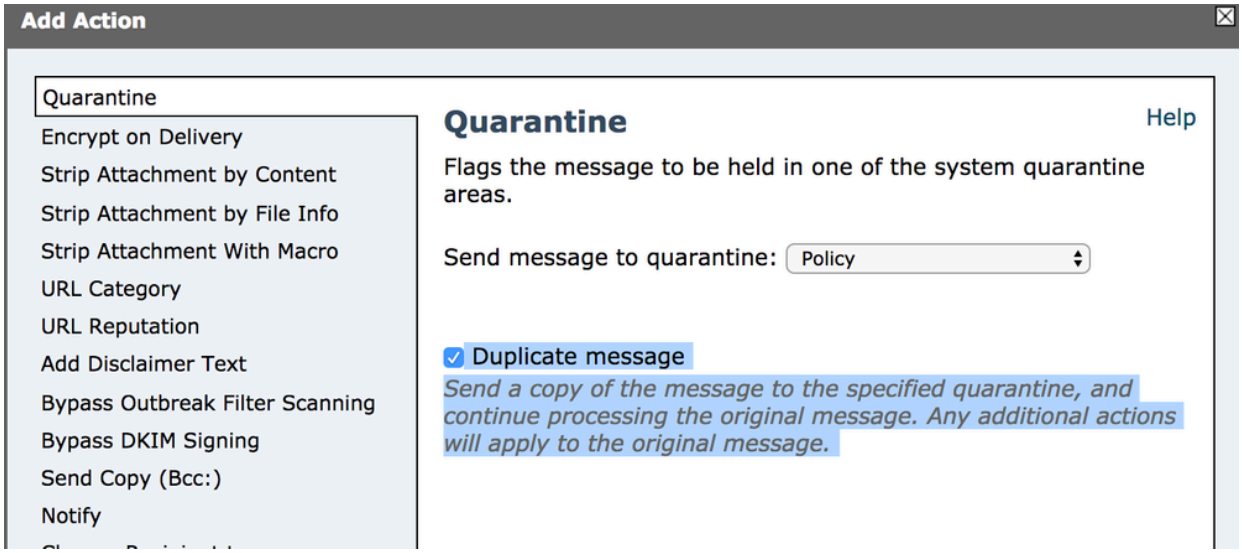
1. Connectez-vous à l'interface de ligne de commande (CLI) de l'ESA.
2. Exécutez la commande Filters.
3. Exécutez la commande New pour créer un nouveau filtre de messages.
4. Copiez et collez cet exemple de filtre, en apportant des modifications à vos noms de groupe d'expéditeurs réels si nécessaire :

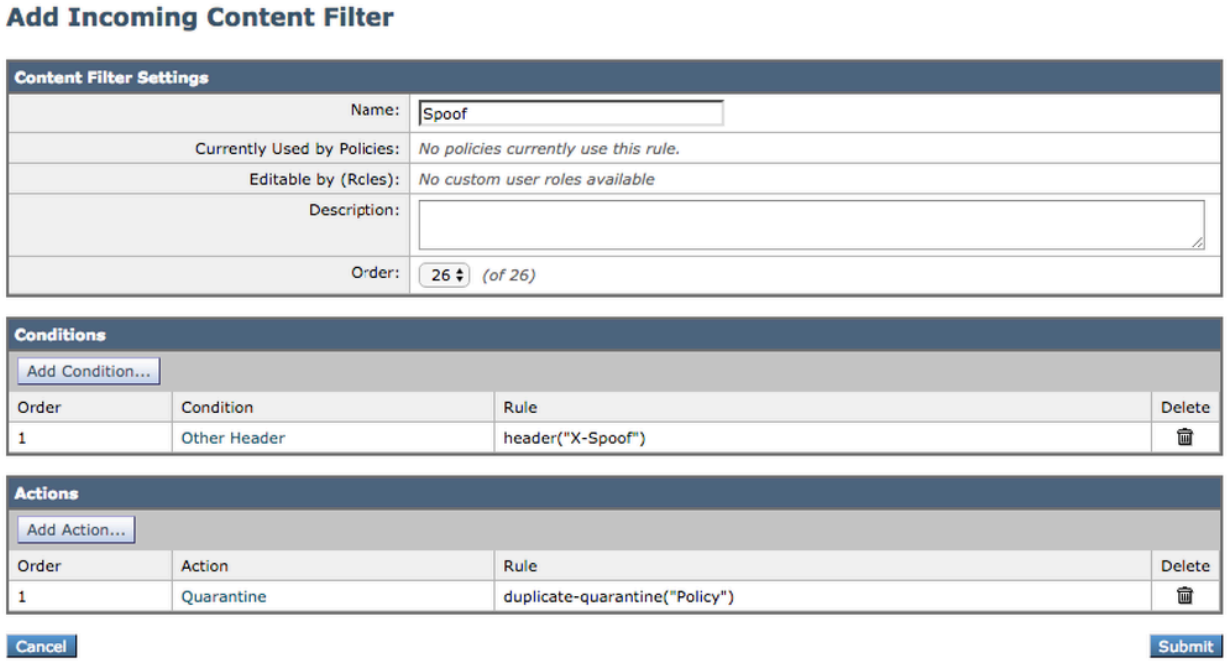
```
mark_spoofed_messages:
if(
     (mail-from-dictionary-match("VALID_INTERNAL_DOMAINS", 1))
 OR  (header-dictionary-match("VALID_INTERNAL_DOMAINS","From", 1)))
 AND ((sendergroup != "RELAYLIST")
 AND (sendergroup != "MY_TRUSTED_SPOOF_HOSTS")
  )
{
insert-header("X-Spoof", "");
}
```

5. Retournez à l'invite de l'interface de ligne de commande principale et exécutez Commit pour enregistrer la configuration.
6. Accédez à GUI > Mail Policies > Incoming Content Filters
7. Créer un filtre de contenu entrant qui exécute une action sur l'en-tête usurpateur X-Spoof :

1. Ajouter un autre en-tête
2. Nom d'en-tête : Usurpation
3. Bouton radio En-tête existant
4. Ajouter une action : duplicate-quarantine(Policy).

> Remarque : la fonctionnalité de message dupliqué affichée ici conserve une copie du message et continue d'envoyer le message d'origine au destinataire.





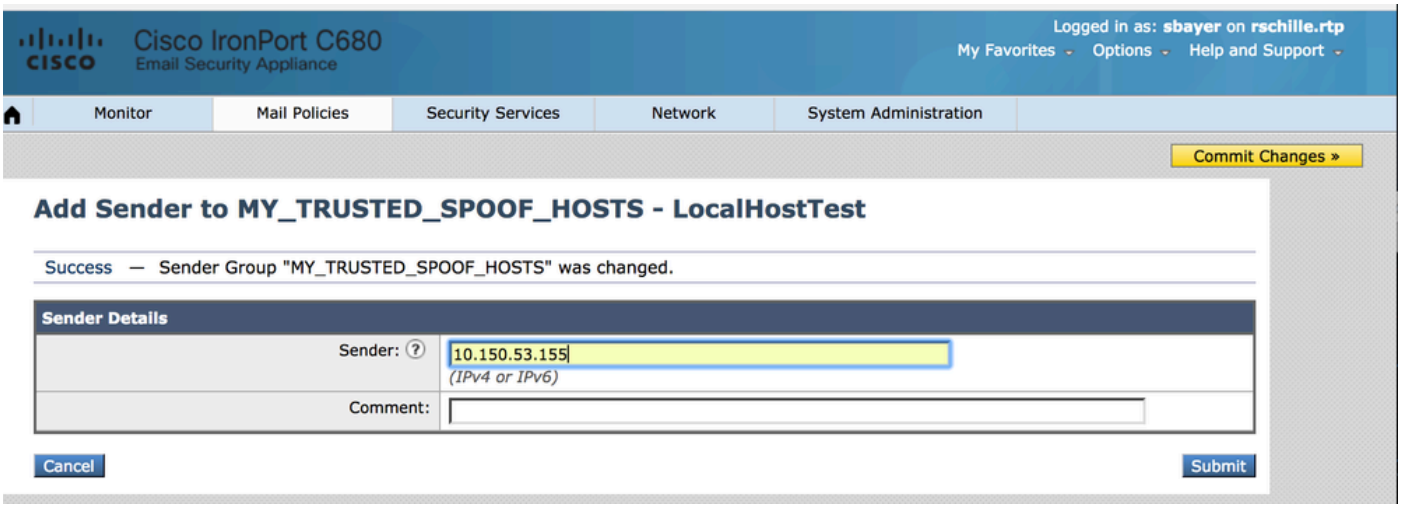
8. Liez le filtre de contenu aux stratégies de messages entrants dans GUI > Politiques de messagerie > Politiques de messages entrants.
9. Soumettre et valider les modifications.

Ajouter des exceptions d'usurpation à MY_TRUSTED_SPOOF_HOSTS

Enfin, vous devez ajouter des exceptions d'usurpation (adresses IP ou noms d'hôte) au groupe d'expéditeurs MY_TRUSTED_SPOOF_HOSTS.

1. Naviguez via l'interface utilisateur graphique Web : Politiques de messagerie > Vue d'ensemble du TAH
2. Cliquez sur et ouvrez le groupe d'expéditeurs MY_TRUSTED_SPOOF_HOSTS.
3. Cliquez sur Ajouter un expéditeur... pour ajouter une adresse IP, une plage, un nom d'hôte ou un nom d'hôte partiel.
4. Cliquez sur Submit pour enregistrer les modifications de l'expéditeur.
5. Enfin, cliquez sur Commit Changes pour enregistrer la configuration.

Exemple :



Vérifier

Vérifier que les messages usurpés sont mis en quarantaine

Envoyez un message test spécifiant l'un de vos domaines comme expéditeur de l'enveloppe. Vérifiez que le filtre fonctionne comme prévu en effectuant un suivi des messages sur ce message. Le résultat attendu est que le message est mis en quarantaine car vous n'avez pas encore créé d'exceptions pour les expéditeurs autorisés à usurper.

<#root>

```
Thu Apr 23 07:09:53 2015 Info: MID 102 ICID 9 RID 0 To: <xxxx_xxxx@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 i
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_messag
```

```
Thu Apr 23 07:10:12 2015 Info: Message finished MID 102 done
```

Vérification de la remise des messages d'exception d'usurpation

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

La liste RELAYLIST est référencée car elle est utilisée par l'ESA pour envoyer des messages sortants. Les messages envoyés par RELAYLIST sont généralement des messages sortants, et le fait de ne pas les inclure créerait des faux positifs ou des messages sortants mis en quarantaine par le filtre ci-dessus.

Exemple de suivi de message d'une adresse IP d'exception d'usurpation ajoutée à MY_TRUSTED_SPOOF_HOSTS. L'action attendue est la livraison et non la mise en quarantaine. (Cette adresse IP est autorisée à usurper).

<#root>

```
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: <user_xxxx@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 i
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 des messages usurpés ESA
- Protection contre les usurpations avec vérification de l'expéditeur

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.