Mettez en quarantaine 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 Cisco ESA et comment créer des exceptions pour que les utilisateurs envoient les emails charriés.

Conditions préalables

Conditions requises

Votre ESA devrait traiter les deux entrant/mails sortants et devrait employer une configuration standard de RELAYLIST pour signaler des messages comme sortants.

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 la quarantaine a charrié l'email et traiter les exceptions.
- **Quarantaine de stratégie** : utilisé pour enregistrer a charrié des emails temporairement avant la décision pour libérer, ou livrer, le message. Consider ajoutant l'adresse IP des messages sortis au WHITELIST pour empêcher de futurs messages de cet expéditeur d'écrire la stratégie mettent en quarantaine.
- **WHITELIST** : 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 WHITELIST Sendergroup 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 sendergroup la supposition est que le message n'est pas un message charrié.

  Remarque: Si le sendergroup s'appelle quelque chose différente que **WHITELIST** ou **RELAYLIST** vous devrez modifier le filtre avec le nom correspondant de sendergroup. Également si vous avez de plusieurs auditeurs, vous pouvez également avoir plus d'un WHITELIST.

Informations générales

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

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 la création des messages électroniques avec une adresse modifiée d'expéditeur.

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 ?

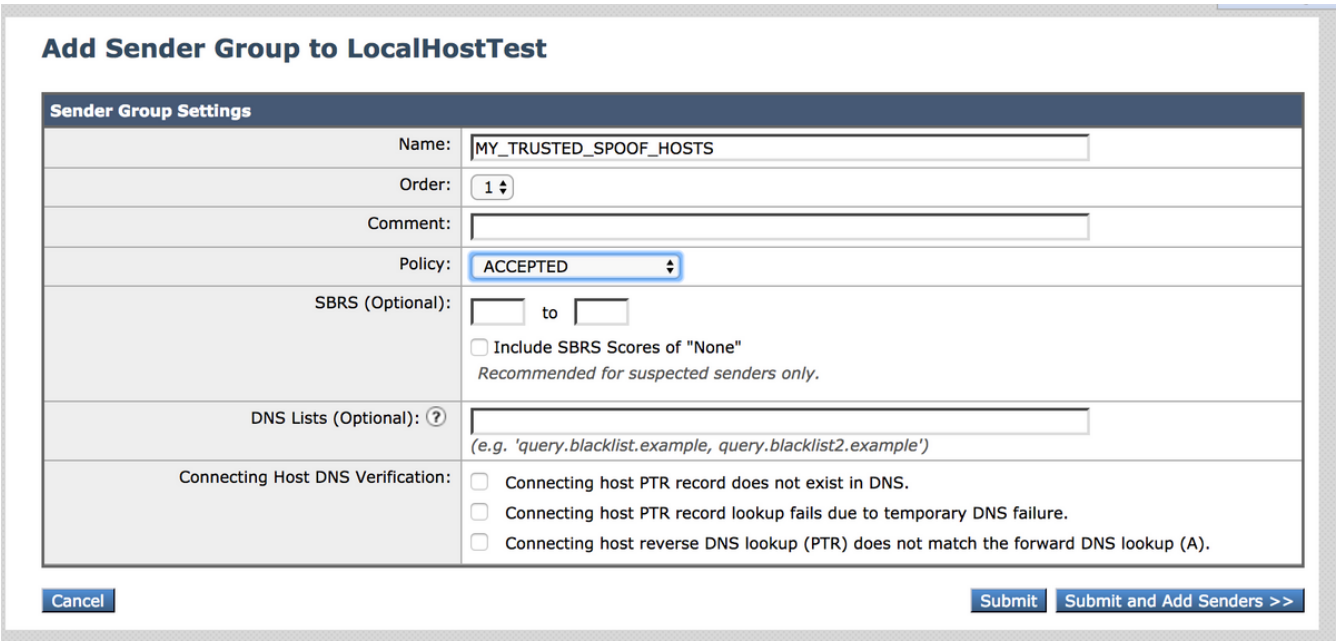
Quand la mise en oeuvre du filtre de message dans ces messages artcile et charriés sont envoyées à la quarantaine de stratégie. Pour ajouter une exception, ajoutez simplement l'IP d'expéditeur à WHITELIST.

Configurez

Créez le dictionnaire

de tous vos domaines pour lesquels vous voulez désactiver la mystification sur l'ESA

- Dans le GUI, naviguez **pour envoyer par mail des stratégies > des dictionnaires.**
- Cliquez sur Add le **dictionnaire.**
- Dans la zone d'identification spécifiez **VALID_INTERNAL_DOMAINS**, par exemple.
- Sous ajoutez les termes, ajoutent tous les domaines pour lesquels vous voudriez désactiver la mystification.
- **Soumettez et commettez les modifications.**
-



Créez le filtre de message

Pour accroître le dictionnaire **VALID_INTERNAL_DOMAINS**

Connectez à la console de l'interface de ligne de commande (CLI) de votre appliance et entrez dans les **filtres de** commande pour obtenir le menu de fiters de message.

Collez et entrez dans le filtre de message ci-dessous.

```
>filters
...
[]> new

Enter filter script.  Enter '.' on its own line to end.

quarantine_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 !=
"WHITELIST")) {
                                quarantine("Policy");
```

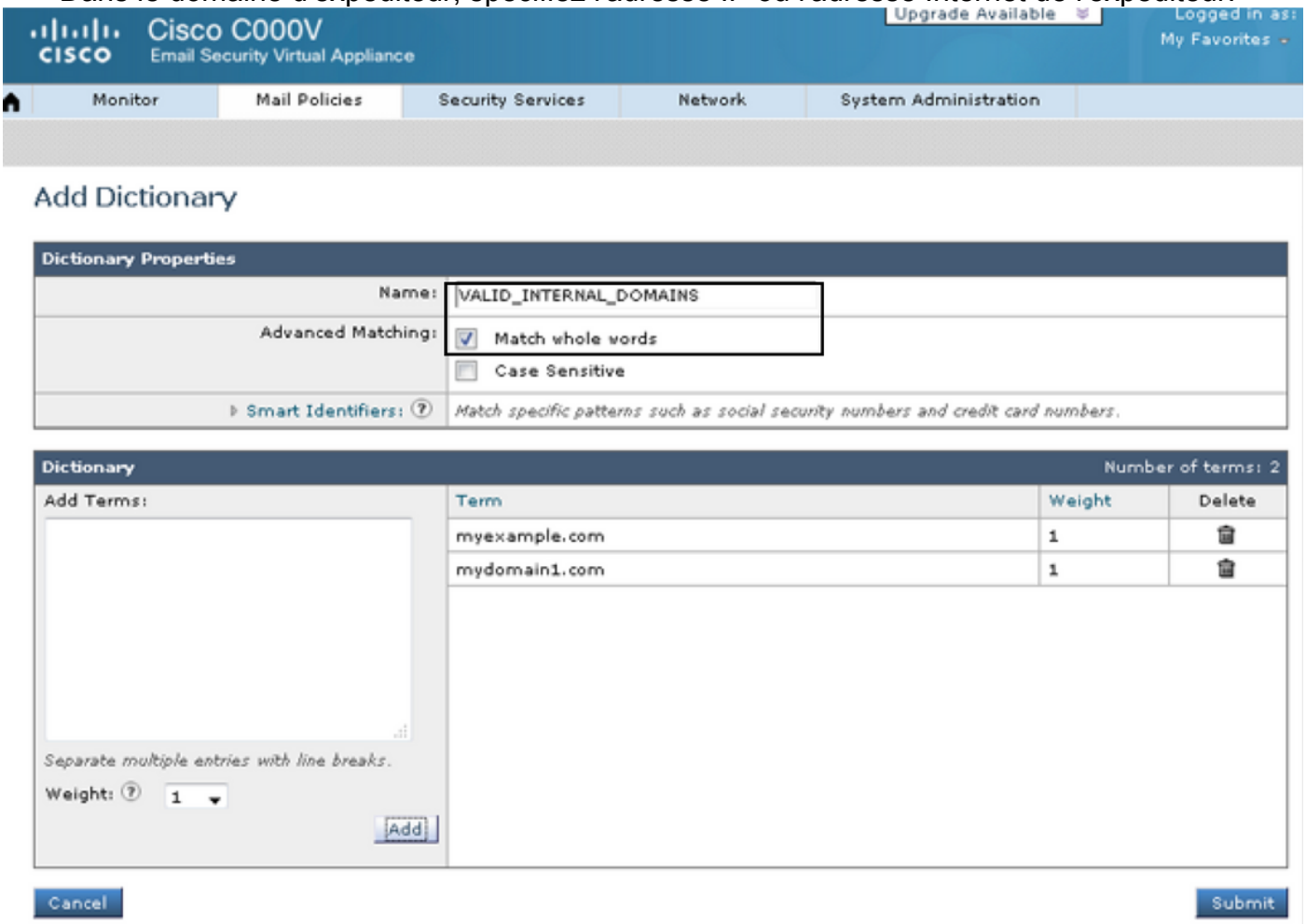
```
                              }
.
1 filters added.
```

Soumettez et commettez les modifications

```
>commit
```

Ajoutez les Charrier-exceptions à WHITELIST

- Naviguez vers des **stratégies de messagerie** GUI **> l'aperçu de CHAPEAU.**
- Ouvrez le **WHITELIST** Sendergroup.
- Dans le domaine d'expéditeur, spécifiez l'adresse IP ou l'adresse Internet de l'expéditeur.



Soumettez et commettez les modifications

```
>commit
```

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: <sbayer@cisco.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 <sbayer@cisco.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 sendergroups 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 WHITELIST. 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: <sbayer@cisco.com>
Thu Apr 23 07:26:02 2015 Info: MID 108 ICID 11 RID 0 To: <sbayer@cisco.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 <sbayer@cisco.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