Comment archiver des emails sur l'appliance de sécurité du courrier électronique et opacifier la sécurité du courrier électronique ?

Contenu

Introduction

Ce document décrit les étapes à suivre afin d'archiver des emails sur l'appliance de sécurité du courrier électronique (ESA) et opacifier la sécurité du courrier électronique (CES) pour la récupération et l'examen.

Informations générales

Quand vous archivez des emails sur l'ESA et le CES, il peut être utilisé pour répondre aux exigences réglementaires ou pour fournir des moyens supplémentaires des données pour davantage de diagnostic et d'examen de messagerie. L'archivage envoie agit en tant que mémoire secondaire des emails dans un format de log de mbox dans lui est source d'origine pour des administrateurs afin de récupérer et valider.

- Il est recommandé pour garder les configurations aux valeurs par défaut si vous décidez d'activer l'archivage des emails. Les valeurs par défaut sont 10MB par maximum de log et de 10 logs retenu. Les logs continueront à être ajoutés et roulés plus de basé sur la taille du fichier journal elle-même. Des fichiers journal de mbox d'archives sont remplis ont basé sur le débit du trafic d'email passant cependant l'appliance. Pendant que plus de logs sont créés, des logs plus anciens de mbox d'archives sont retirés sur l'espace libre pour la création du nouveau log.
- Assurez-vous que votre périphérique a le suffisamment d'espace disque avant que vous augmentiez les volumes de fichier journal de mbox d'archives et les fichiers journal maximum retenus.
- Afin d'arrêter les logs de mbox d'archives d'être généré, vous devrez désactiver la fonction d'archives par stratégie.

Note: Des logs de mbox d'archives ESA et de CES ne peuvent pas être récupérés par le SMA et sont enregistrés localement par chaque ESA et CES avec la fonction activée.

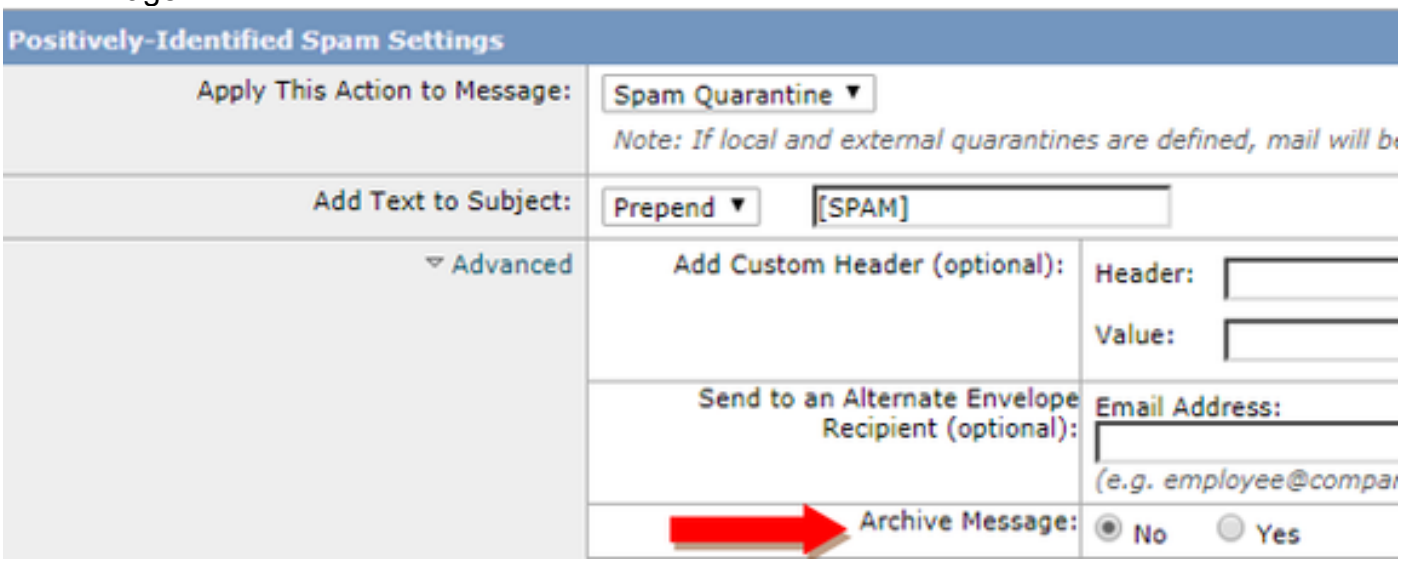
Comment archiver des emails sur l'ESA et le CES ?

L'archivage d'email est disponible avec l'anti-Spam, l'antivirus, les filtres avancés de protection de malware, de Graymail et de message. L'action d'archives peut être configurée dans le GUI et le CLI pour l'anti-Spam, l'antivirus, la protection avancée de malware et le Graymail.

L'action d'archives peut être configurée dans le CLI seulement pour des filtres de message.

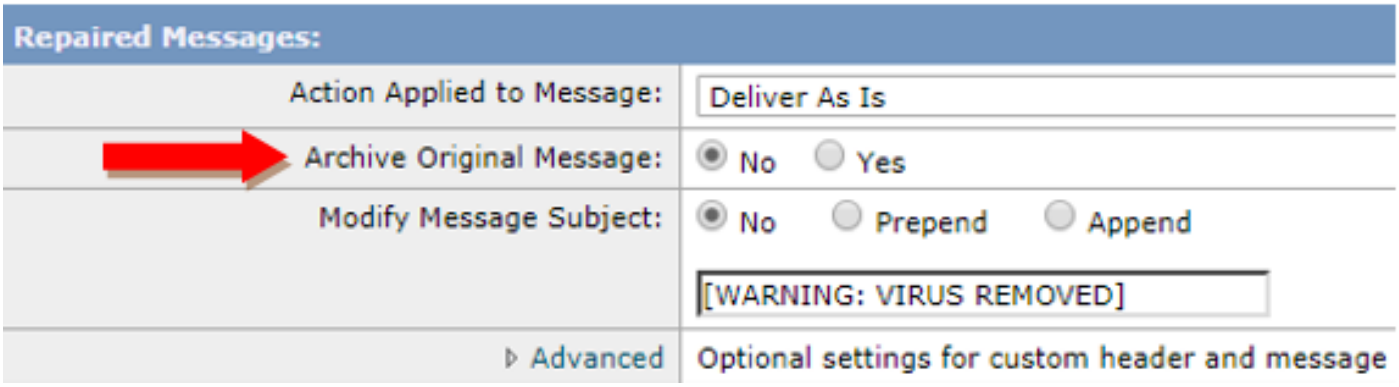
Configurez les archives d'anti-Spam

1. Naviguez vers des **stratégies GUI > de messagerie > des stratégies entrantes/mail sortant**.
2. Cliquez sur en fonction les configurations d'anti-Spam sur la stratégie respective afin de configurer l'archivage d'email.
3. Cliquez sur **avancé** sur les configurations disponibles pour les configurations franchement identifiées de Spam, les configurations suspectées de Spam.
4. Appuyez sur la case d'option à côté de l'oui afin d'archiver des emails avec le verdict respectif d'anti-Spam.
5. La configuration de Submitthe, et commettent ces modifications suivant les indications de l'image.



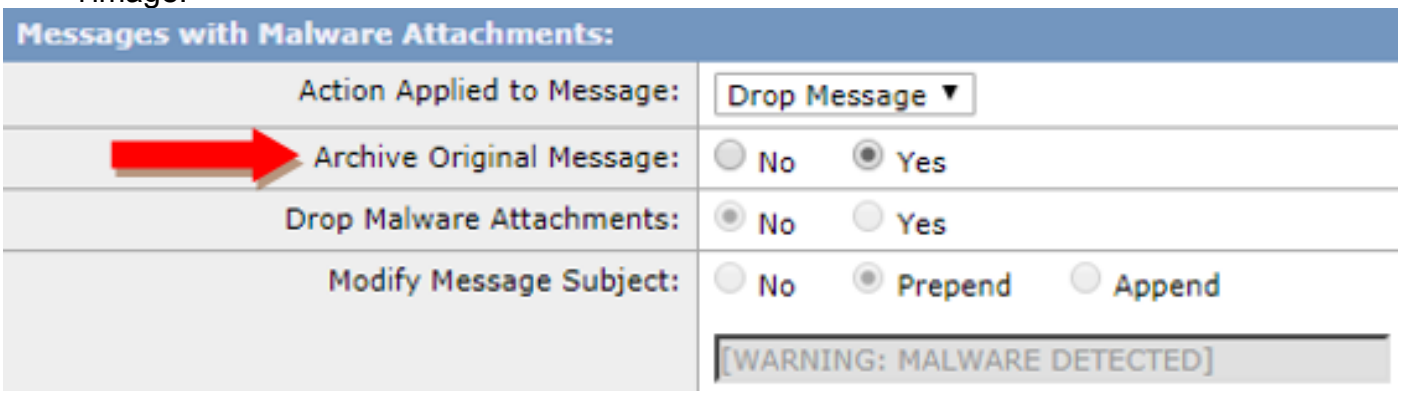
Configurez les archives d'antivirus

1. Naviguez vers des **stratégies GUI > de messagerie > des stratégies entrantes/mail sortant**.
2. Cliquez sur en fonction les configurations d'antivirus sur la stratégie respective afin de configurer l'archivage d'email.
3. Sur chacune de la lecture les verdicts que vous souhaitez archiver le premier message, appuient sur la case d'option à côté de l'oui dans des archives d'orderto.
4. La configuration de Submitthe, et commettent ces modifications suivant les indications de l'image.



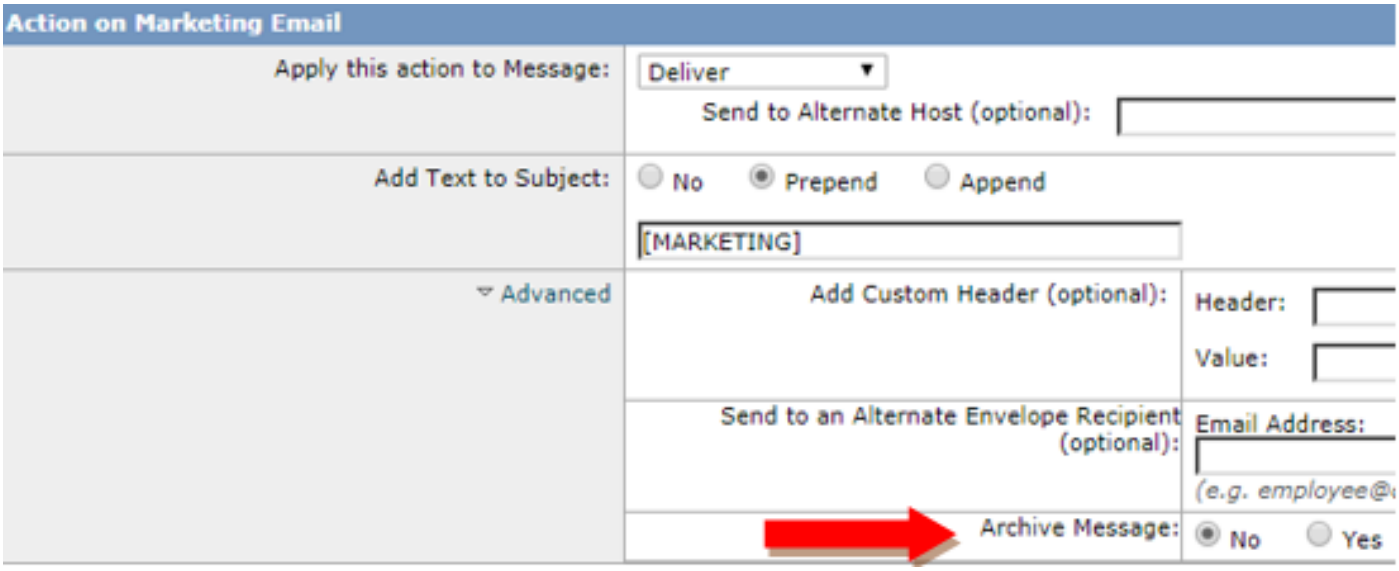
Configurez les archives avancées de protection de malware

1. Naviguez vers des **stratégies GUI > de messagerie > des stratégies entrantes/mail sortant**.
2. Cliquez sur en fonction le malware avancé Protectionsettings sur la stratégie respective afin de configurer l'archivage d'email.
3. Sur chacune de la lecture les verdicts que vous souhaitez afin d'archiver le premier message, appuient sur la case d'option à côté de l'oui afin d'archiver.
4. La configuration de Submitthe, et commettent ces modifications suivant les indications de l'image.



Configurez les archives de Graymail

1. Naviguez vers des **stratégies GUI > de messagerie > des stratégies entrantes/mail sortant**.
2. Cliquez sur en fonction les configurations de Graymail sur la stratégie respective afin de configurer l'archivage d'email.
3. Cliquez sur **Advancedon les** configurations disponibles pour lancer, piratage, le volume.
4. Appuyez sur la case d'option à côté de l'oui afin d'archiver des emails avec le verdict respectif de Graymail.
5. Soumettez la configuration, et commettez ces modifications.



Configurez les archives de filtre de message

> **Note**: Un filtre de message avec l'action d'archives est exigé afin de visualiser les logs archivés. Des filtres de message peuvent seulement être créés dans le CLI.

Filtre témoin :

```
Test_Archive:
if (mail-from == "test1@cisco.com")
{
archive("Test");
}
```

1. Procédure de connexion au périphérique sur le CLI.
2. Créez un filtre de message comme vu dans le filtre témoin fourni.
3. Soumettez ce filtre et commettez vos modifications.

Validez la Disponibilité de logs de Mbox d'archives

Quand la configuration pour des archives est commise pour les services respectifs, les emails archivés sont enregistrés dans un fichier journal de format de mbox. Afin de vérifier si les logs d'archives sont disponibles pour la récupération, naviguez vers des **abonnements GUI > d'administration système > de log**.

Les archives de Services de sécurité créent un log distinct avec un type de log d'archives suivant les indications de l'image :

Configured Log Subscriptions

Add Log Subscription...

Log Settings	Type ▲	Log Files	Rollover Interval
amp	AMP Engine Logs	amp/	None
amparchive	AMP Archive	amparchive/	None
antispam	Anti-Spam Logs	antispam/	None
antivirus	Anti-Virus Logs	antivirus/	None
asarchive	Anti-Spam Archive	asarchive/	None
authentication	Authentication Logs	authentication/	None
avarchive	Anti-Virus Archive	avarchive/	None

Pour le message filtre la configuration d'archives est visualisé du **CLI seulement** :

- **filtres > logconfig**

```
demigod.cisco.com> filters


Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> logconfig

Currently configured logs:
    Log Name           Log Type                    Retrieval          Interval
 ------------------------------------------------------------------------------
 1. Test               Filter Archive Logs         Manual Download    None
```

Récupérez les logs de Mbox

Pour les appliances autonomes ces logs de mbox peuvent être récupérés directement du GUI. Naviguez vers le theGUI **> l'administration système > le log Subscriptionsand** cliquent sur en fonction les **fichiers journal** pour le log d'archives respectif que vous récupèrerez.

Pour les appliances groupées, les logs de mbox peuvent être récupérés avec l'utilisation de la copie FTP/Secure (SCP) comme décrit dans le [thisarticle](https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118315-technote-esa-00....). ([https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118315-technote-esa-00....)](https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118315-technote-esa-00....)

Informations connexes

- [Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur]
- [Quel est format de mbox UNIX (boîte aux lettres) ?]
- [Là où sont les logs enregistrés sur l'appliance de sécurité du courrier électronique de Cisco (ESA) et comment je les accède à]
- [Comment extraire un email du mbox d'archives se connecte]

- Support et documentation techniques - Cisco Systems