Guide de pratique recommandée pour l'anti-Spam, l'antivirus, le Graymail et les filtres d'épidémie

Contenu

Aperçu

L'immense majorité de menaces, d'attaques, et de gênes faites face par une organisation par l'email été livré sous forme de Spam, de malware, et d'attaques mélangées. L'appliance de la sécurité du courrier électronique de Cisco (ESA) inclut plusieurs différentes Technologies et caractéristiques pour couper ces menaces à la passerelle avant qu'elles écrivent l'organisation. Ce document décrira les approches de pratique recommandée pour configurer l'anti-Spam, l'antivirus, le Graymail et les filtres d'épidémie, sur l'écoulement d'arrivée et sortant d'email.

Anti-Spam

La protection d'anti-Spam adresse une gamme complète de menaces connues comprenant des attaques de Spam, de phishing et de zombie, aussi bien que dur-à-détecte le bas volume, des menaces de courte durée d'email telles que « 419" des escroqueries. En outre, la protection d'anti-Spam identifie nouveau et évoluer des menaces mélangées telles que des attaques de Spam distribuant le contenu malveillant par un URL de téléchargement ou un exécutable.

La sécurité du courrier électronique de Cisco offre les solutions suivantes d'anti-Spam :

- Filtrage d'anti-Spam d'IronPort (IPAS)
- Filtrage intelligent de Multi-balayage de Cisco (IMS)

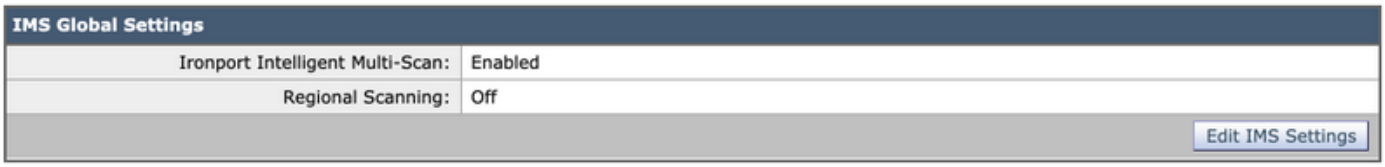
Vous pouvez autoriser et activer les deux solutions sur votre ESA mais seulement pouvez utiliser un dans une stratégie particulière de messagerie. Afin de ce document de pratique recommandée, nous allons utiliser la caractéristique IMS.

Vérifiez la touche de fonction

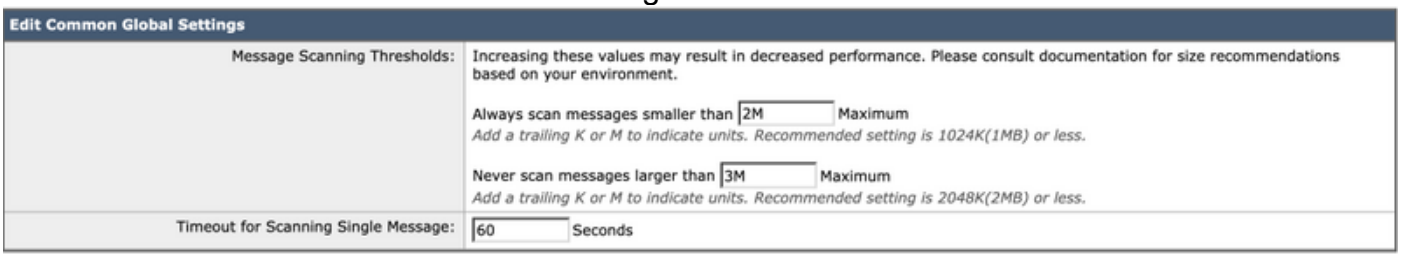
- Sur l'ESA, naviguez vers l'**administration système** > les **touches de fonction**
- Recherchez le permis intelligent de Multi-balayage et assurez-vous qu'il est en activité.

Multi-balayage intelligent d'enable (IMS) globalement

- Sur l'ESA, naviguez vers les **Services de sécurité** > l'**IMS et le Graymail**
- Cliquez sur l'**Enablebutton** sur des **paramètres généraux IMS** :



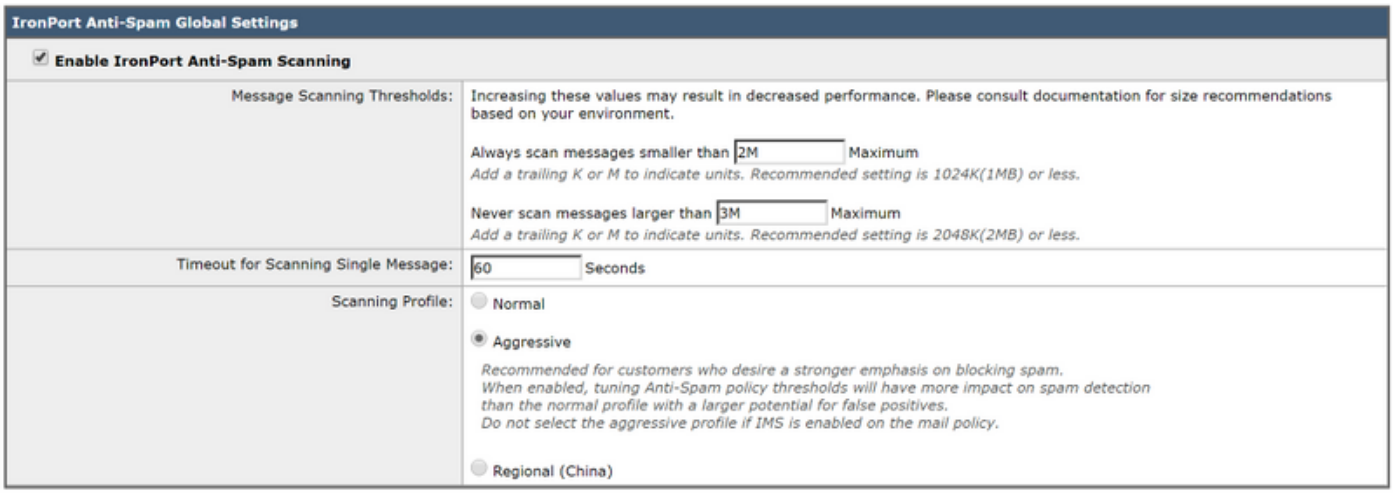
- Recherchez les **paramètres généraux communs** et cliquez sur Edit les **paramètres généraux**
- Voici que vous pouvez configurer de plusieurs configurations. Les configurations recommandées sont affichées dans l'image ci-dessous :



- **Validation de Submitand de** clic **vos modifications**.

Si vous n'avez pas un abonnement de permis IMS :

- Naviguez vers les **Services de sécurité > l'anti-Spam d'IronPort**
- Cliquez sur l'**Enablebutton** sur la **vue d'ensemble d'anti-Spam d'IronPort**
- Cliquez sur Edit les **paramètres généraux**
- Voici que vous pouvez configurer de plusieurs configurations. Les configurations recommandées sont affichées dans l'image ci-dessous :

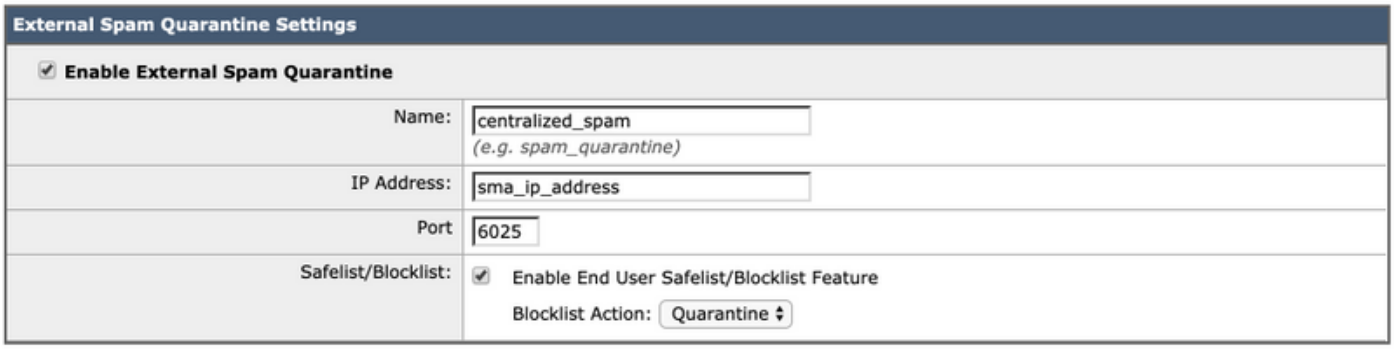


- Cisco recommande sélectionner le profil **agressif de** lecture pour un client qui désire un accent fort sur bloquer le Spam.
- **Validation de Submitand de** clic **vos modifications**

Quarantaine de Spam centralisée par enable

Puisque l'anti-Spam a l'option d'être envoyé pour mettre en quarantaine, il est important de s'assurer que la quarantaine de Spam est installée :

- Naviguez vers des **Services de sécurité** > la **quarantaine de Spam**
- Cliquer sur le **Configurebutton** vous portera à la page suivante.
- Voici que vous pouvez activer la quarantaine en vérifiant l'**enablebox** et diriger la quarantaine à centraliser sur une appliance de SecurityManagement (SMA) byfilling dans l'**IP address** SMANAMEAND. Les configurations recommandées sont affichées ci-dessous :



- **Validation de Submitand de** clic **vos modifications**

Pour plus d'informations sur l'établissement et les quarantaines centralisées, référez-vous s'il vous plaît au document de pratiques recommandées :

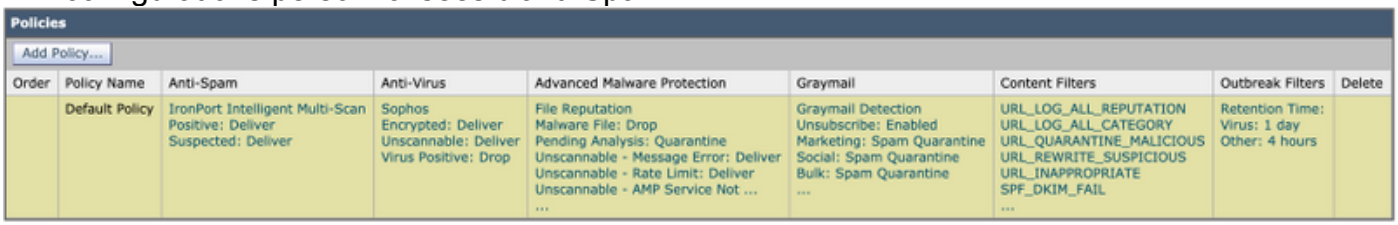
[Pratiques recommandées pour la stratégie, l'installation de quarantaines de virus et d'épidémie, et le transfert centralisés de l'ESA à SMA]

Configurez l'anti-Spam dans les stratégies

Une fois que le Multi-balayage intelligent a été
configuré globalement, vous pouvez maintenant appliquer le Multi-balayage intelligent pour envoyer par mail des stratégies :

- Naviguez **pour envoyer par mail des stratégies** > des **stratégies de messagerie entrante**
- Les stratégies de messagerie entrante utilisent des configurations d'anti-Spam d'IronPort par défaut.

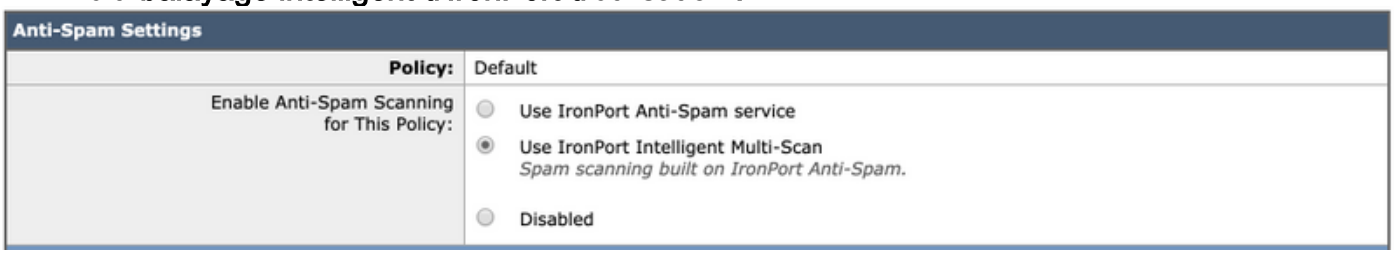
- Cliquer sur le lien bleu sous l'**anti-Spam** tiendra compte pour que cette stratégie particulière utilise les configurations personnalisées d'anti-Spam.
- Au-dessous de vous verra un exemple qui affiche la stratégie par défaut utilisant les configurations personnalisées d'anti-Spam :



Personnalisez les configurations d'anti-Spam pour une stratégie de messagerie entrante en cliquant sur le lien bleu sous l'**anti-Spam** pour la stratégie que vous souhaitez personnaliser.

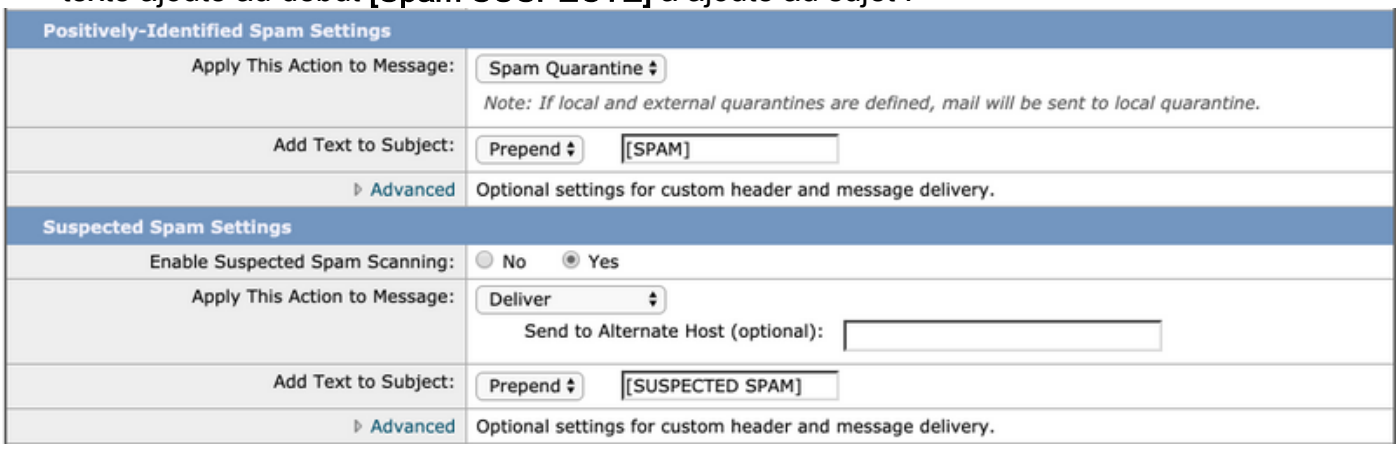
Voici que vous pouvez sélectionner l'option de lecture d'anti-Spam
que vous souhaitez activer pour cette stratégie.

- Aux fins de ce document de pratique recommandée, cliquez sur la case d'option à côté du Multi-**balayage intelligent d'IronPort d'**utilisation **:**

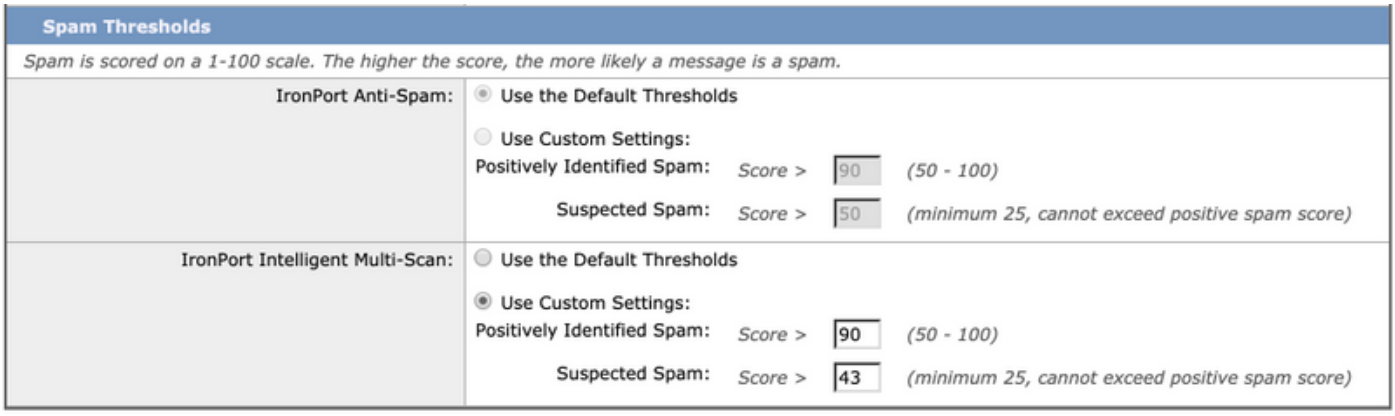


Les deux prochaines sections incluent les **configurations Positif-identifiées de Spam** et les **configurations suspectées de Spam :**

- La pratique recommandée recommandée est de configurer l'action de **quarantaine** sur la configuration de **Spam Positif-Identifier** avec le texte ajouté au début **[Spam]** ajouté au sujet et ;
- Appliquez **pour livrer** comme l'action pour des **configurations de Spam Suspected** avec le texte ajouté au début **[Spam SUSPECTÉ]** a ajouté au sujet :



- **La définition de seuil de Spam** peut être changée, et les configurations recommandées sont de personnaliser le score Positif-**identifié de Spam à 90** et le score **suspecté de Spam à 43** :



- **Validation de Submitand de** clic **vos modifications**

Antivirus

La protection antivirus est assurée par deux engines de tiers – Sophos et McAfee. Ces engines filtreront toutes les menaces malveillantes connues, les relâchant, nettoyant ou mettant en quarantaine comme configurées.

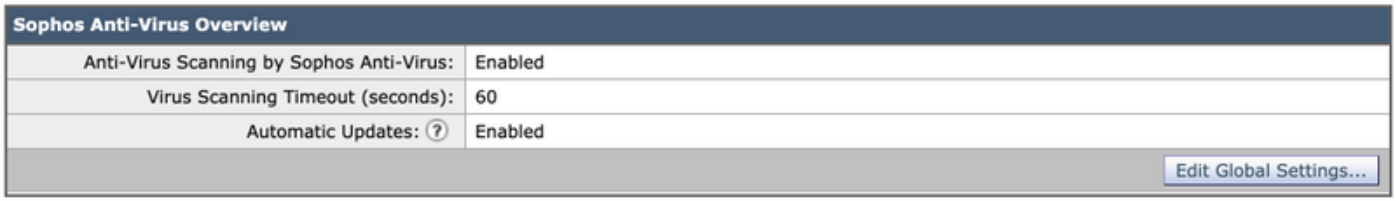
Vérifiez les touches de fonction

Pour vérifier que les deux touches de fonction sont activées et active :

- Allez à l'**administration système** > aux **touches de fonction**
- Assurez-vous que les permis d'**antivirus** et de **McAfee de Sophos** sont en activité.

Lecture d'antivirus d'enable

- Naviguez vers les **Services de sécurité** > l'**antivirus - Sophos**
- Cliquez sur l'**Enablebutton**.
- Assurez-vous que la **mise à jour automatique est activée** et la mise à jour de fichiers d'antivirus de Sophos fonctionne bien. S'il y a lieu, **mise à jour de** clic **maintenant** pour initier la mise à jour des fichiers immédiatement :



- **Validation de Submitand de** clic **vos modifications**.

Si le permis de McAfee est en activité aussi bien, naviguez vers les **Services de sécurité** > l'**antivirus - McAfee**

- Cliquez sur l'**Enablebutton**.

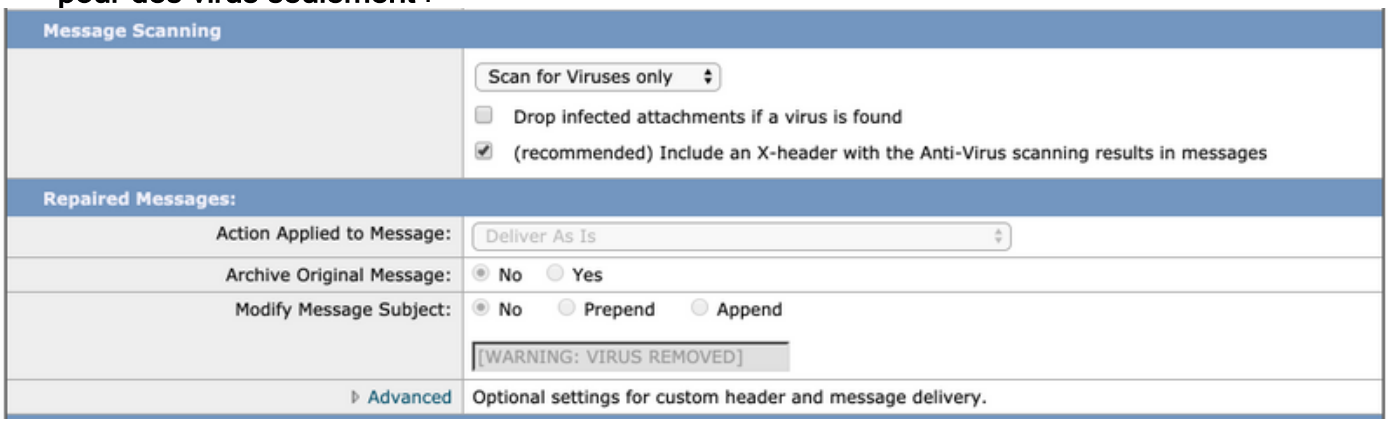
- Assurez-vous que la **mise à jour automatique est activée** et la mise à jour de fichiers d'antivirus de McAfee fonctionne bien. S'il y a lieu, **mise à jour de** clic **maintenant** pour initier la mise à jour des fichiers immédiatement.
- **Validation de Submitand de** clic **vos modifications**

Configurez l'antivirus dans des stratégies de messagerie

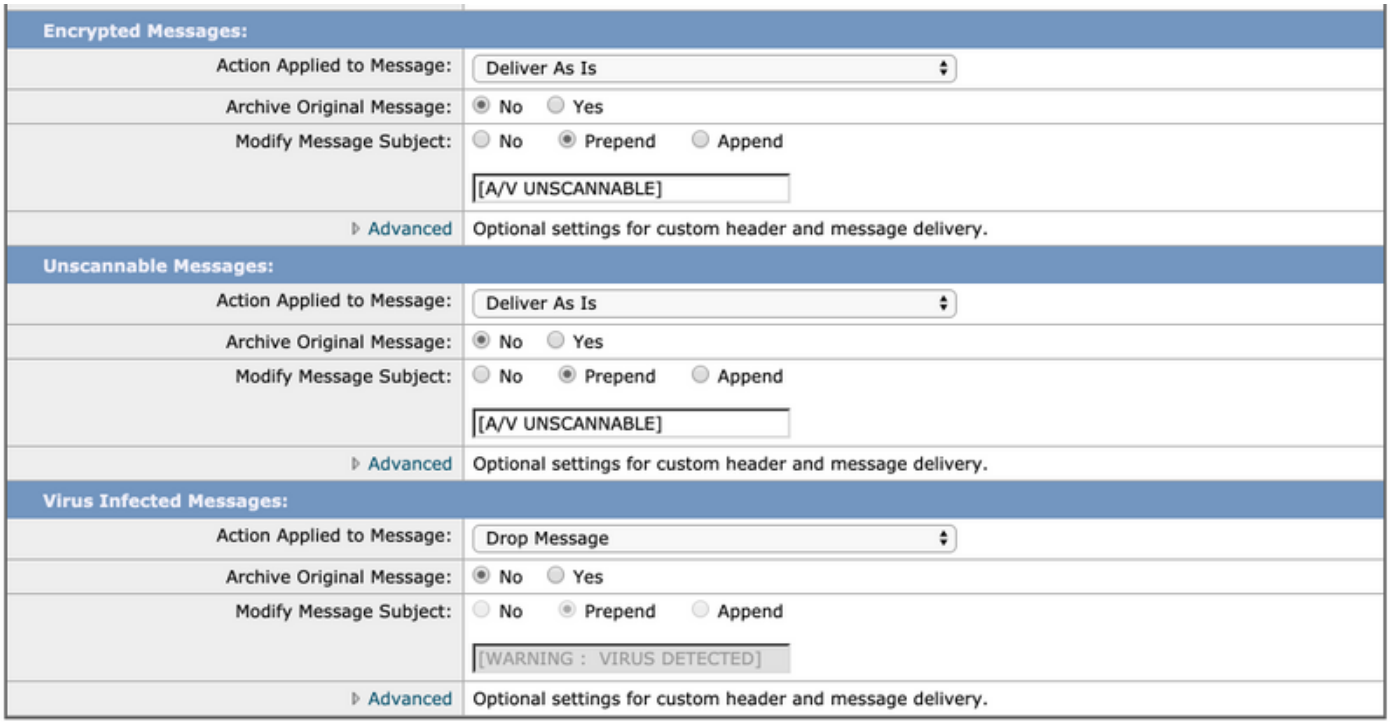
Sur une stratégie de messagerie entrante, ce qui suit est recommandé :

- Naviguez **pour envoyer par mail des stratégies >** des **stratégies de messagerie entrante**
- Personnalisez les configurations d'**antivirus** pour une stratégie de messagerie entrante en cliquant sur le lien bleu sous l'antivirus pour la stratégie que vous souhaitez personnaliser.
- Voici que vous pouvez sélectionner l'option de lecture d'antivirus que vous souhaitez activer pour cette stratégie.
- Aux fins de ce document de pratique recommandée, sélectionnez **McAfee** et **antivirus de Sophos** :

- Nous ne tentons pas de réparer un fichier, ainsi les restes de lecture de message **balayent pour des virus seulement** :



- L'action recommandée pour les **messages chiffré** et d'**Unscannable** est **de livrer réel** avec un champ objet modifié à leur attention.
- La stratégie recommandée pour l'antivirus est **baisse** tous les **messages infectés par le virus** suivant les indications de l'image ci-dessous :



- **Validation de Submitand de** clic **vos modifications**

Une stratégie semblable est recommandée pour des stratégies de mail sortant, cependant, nous ne recommandons pas modifier le champ objet sur l'email sortant.

Graymail

La solution de Gestion de graymail dans l'appliance de sécurité du courrier électronique comporte de deux composants : une engine intégrée de lecture de graymail et un basé sur nuage se désabonnent le service. La solution de Gestion de graymail permet à des organismes pour identifier le graymail utilisant l'engine intégrée de graymail et appliquer des contrôles appropriés de stratégie et fournir un mécanisme facile pour que les utilisateurs se désabonnent des messages indésirables utilisant désabonnez-vous le service.

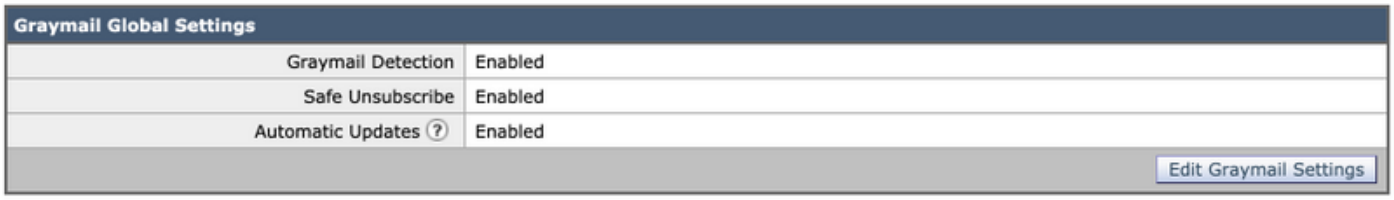
Les catégories de Graymail incluent l'email de vente, l'email social de réseau et l'email en vrac. Les options avancées incluent ajouter une en-tête faite sur commande, l'envoi à un hôte alternatif et archiver le message. Pour cette pratique recommandée, nous activerons le coffre-fort de Graymail nous désabonnons la caractéristique pour la stratégie par défaut de messagerie.

Vérifiez la touche de fonction

- Sur l'ESA, naviguez vers l'**administration système** > les **touches de fonction**
- Recherchez **Graymail Unsubscription sûr** et assurez-vous qu'il est en activité.

L'enable Graymail et le coffre-fort se désabonnent des services

- Sur l'ESA, naviguez vers les **Services de sécurité** > l'**IMS et le Graymail**
- Cliquez sur l'**éditer Graymail Settingsbutton** sur des **paramètres généraux de Graymail**
- Sélectionnez toutes les options - **Activez la détection de Graymail**, le **coffre-fort d'enable se désabonnent** et **activent les mises à jour automatiques** :



- **Validation de Submitand de** clic **vos modifications**

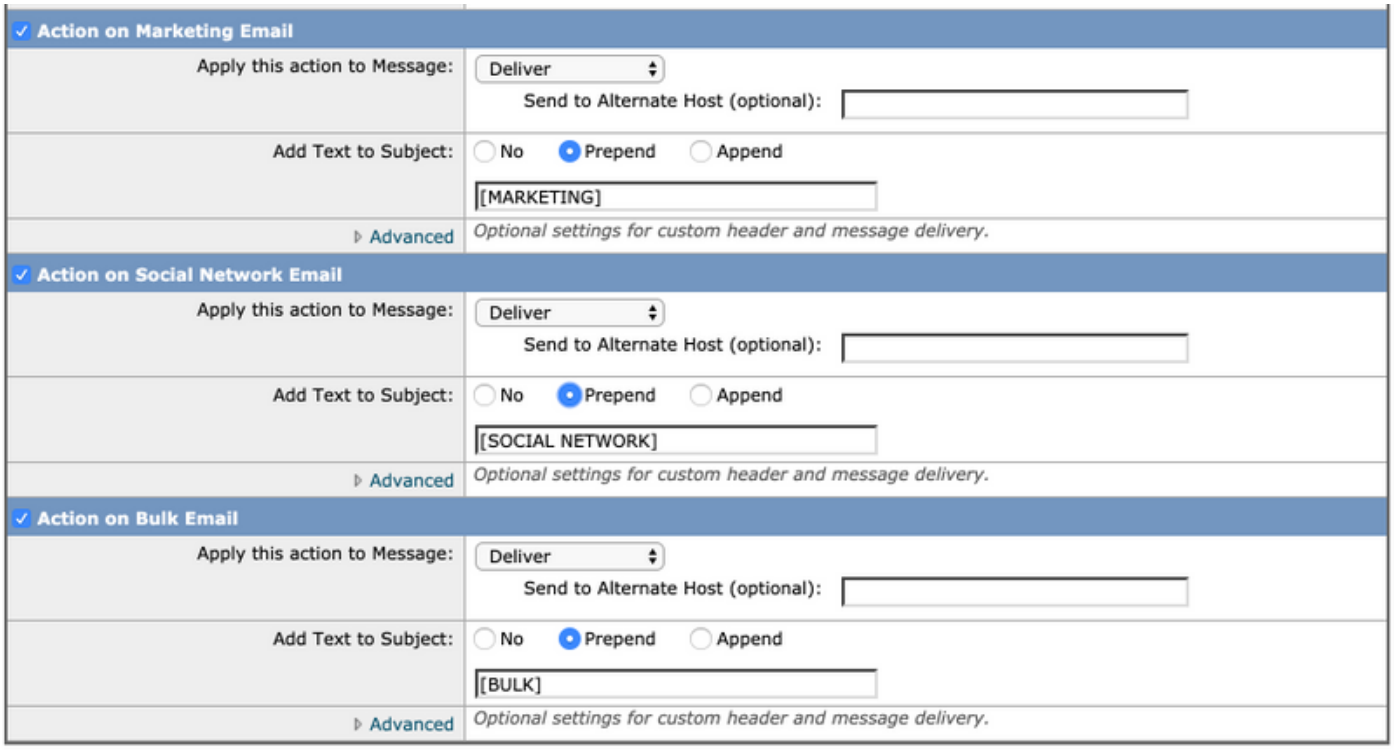
Configurez Graymail et le coffre-fort se désabonnent dans les stratégies

Une fois que Graymail et coffre-fort Unsubscribe a été
configuré globalement, vous pouvez maintenant appliquer ces services pour envoyer par mail des stratégies.

- Naviguez **pour envoyer par mail des stratégies >** des **stratégies de messagerie entrante**
- Cliquer sur le lien bleu sous **Graymail** tiendra compte pour que cette stratégie particulière utilise les configurations personnalisées de Graymail.
- Voici que vous pouvez sélectionner le Graymailoptions
  que vous souhaitez activer pour cette stratégie.
- Aux fins de ce document de pratique recommandée, cliquez sur la case d'option à côté de la **détection de Graymail d'enable pour cette stratégie** et **activez Graymail se désabonnant pour cette stratégie** :

Les trois prochaines sections incluent l'**action sur des configurations d'email de vente**, l'**action sur les configurations sociales d'email de réseau** et l'**action sur les configurations en vrac d'email**.

- La pratique recommandée recommandée est d'activer tous et de rester l'action comme **livrent** avec ajouté au début le texte ajouté au sujet en ce qui concerne les catégories comme affiché ci-dessous :



- **Validation de Submitand de** clic **vos modifications**

La stratégie de mail sortant devrait faire rester **Graymail** dans la condition **handicapée**.

Filtres d'épidémie

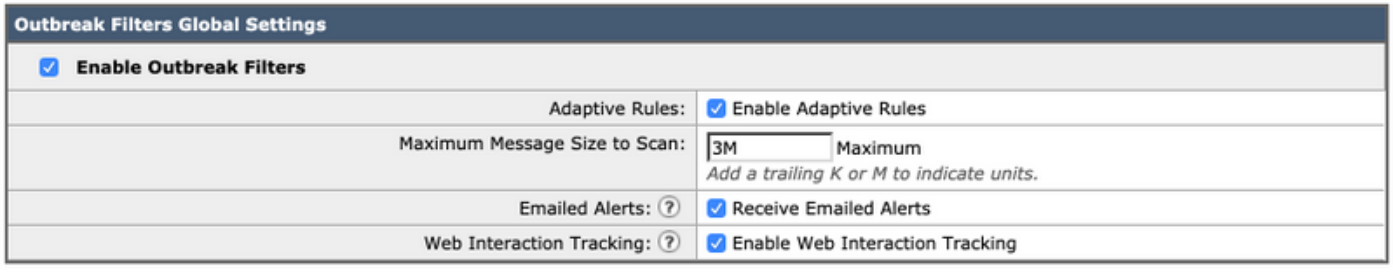
Les filtres d'épidémie combinent des déclencheurs dans l'engine d'anti-Spam, lecture URL et Technologies et plus de détection pour étiqueter correctement les éléments qui tombent en dehors de la véritable catégorie de Spam – par exemple, le phishing envoie et les emails d'escroquerie et les manipule convenablement avec des notifications ou la quarantaine d'utilisateur.

Vérifiez la touche de fonction

- Sur l'ESA, naviguez vers l'**administration système** > les **touches de fonction**
- Recherchez les **filtres d'épidémie** et assurez-vous qu'il est en activité.

L'épidémie d'enable filtre le service

- Sur l'ESA, naviguez vers des **Services de sécurité** > des **filtres d'épidémie**
- Cliquez sur l'**Enablebutton** sur la **vue d'ensemble de filtres d'épidémie**
- Voici que vous pouvez configurer de plusieurs configurations. Les configurations recommandées sont affichées dans l'image ci-dessous :

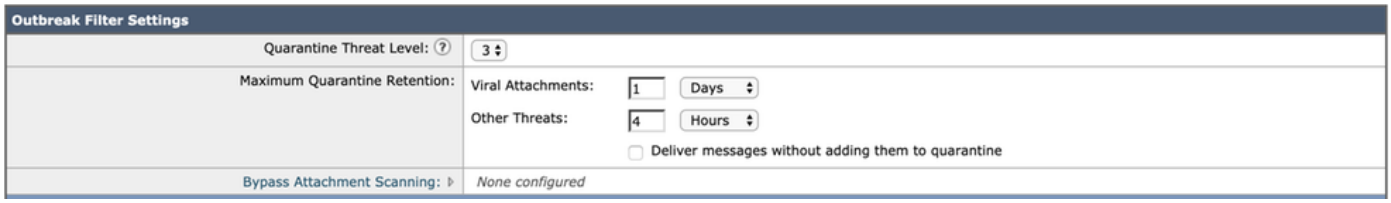


- **Validation de Submitand de** clic **vos modifications**.

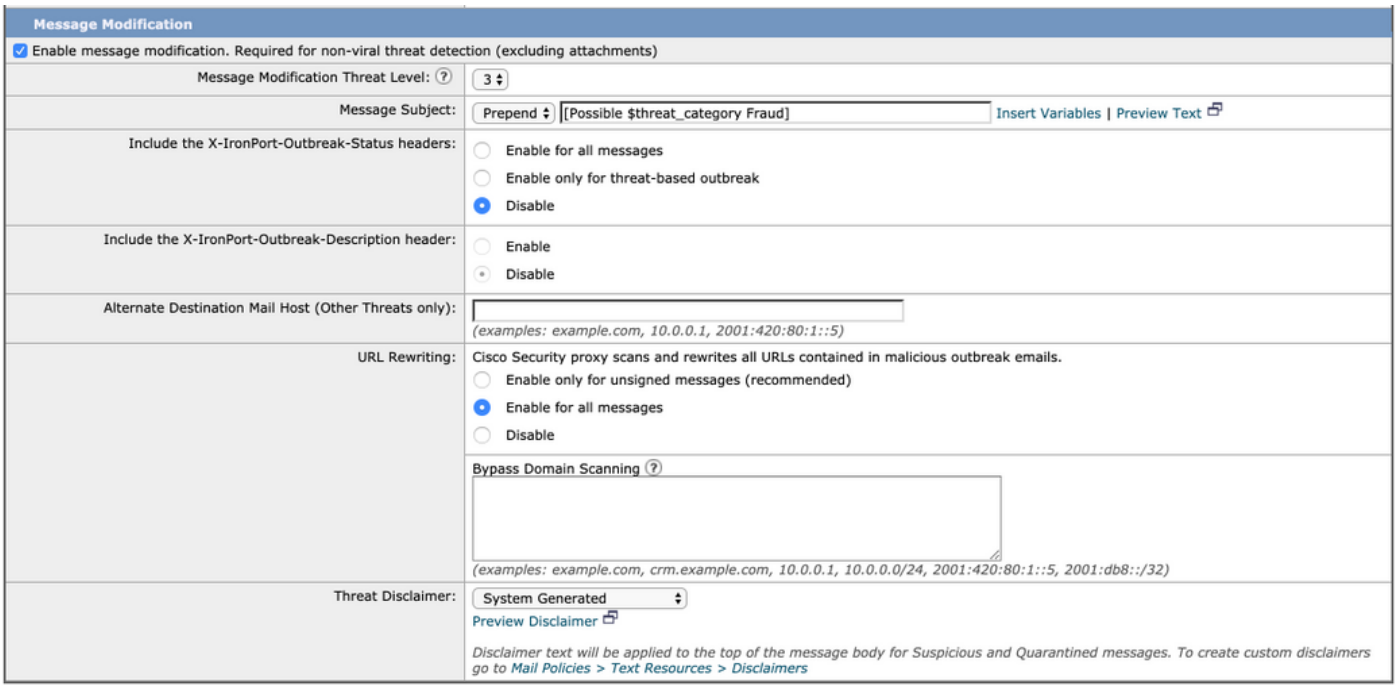
Configurez les filtres d'épidémie dans les stratégies

Une fois que l'épidémie Filtershas configuré globalement, vous peut maintenant appliquer des stratégies de ce tomail de caractéristique.

- Naviguez **pour envoyer par mail des stratégies** > des **stratégies de messagerie entrante**
- Cliquer sur le lien bleu sous des **filtres d'épidémie** tiendra compte pour que cette stratégie particulière utilise les configurations personnalisées de filtres d'épidémie.
- Aux fins de ce document de pratique recommandée, nous gardons les paramètres de filtre d'épidémie avec des valeurs par défaut :



- Les filtres d'épidémie peuvent réécrire l'URLs s'ils sont considérés malveillants, suspects, ou phish. Sélectionnez la **modification de message d'enable** pour détecter et réécrire des menaces basées par URL.
- Assurez-vous que l'option de **réécriture URL** est **enable** pour tous les messages comme suivant affiché :



- **Validation de Submitand de** clic **vos modifications**

La stratégie de mail sortant devrait faire rester des **filtres d'épidémie** dans la condition **handicapée**.

Conclusion

Ce document a visé à décrire le par défaut, ou des configurations de pratique recommandée pour l'anti-Spam, l'antivirus, le Graymail et les filtres d'épidémie dans l'appliance de sécurité du courrier électronique (ESA). Tous ces filtres sont disponibles sur les stratégies d'arrivée et sortantes d'email, et la configuration et le filtrage sont recommandés sur chacun des deux – tandis que la partie de la protection est pour d'arrivée, le filtrage de l'écoulement sortant assure la protection contre les emails transmis par relais ou les attaques malveillantes internes.