

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

## Contenu

[Aperçu](#)

[Anti-Spam](#)

[Vérifiez la touche de fonction](#)

[Multi-balayage intelligent d'enable \(IMS\) globalement](#)

[Quarantaine de Spam centralisée par enable](#)

[Configurez l'anti-Spam dans les stratégies](#)

[Antivirus](#)

[Vérifiez les touches de fonction](#)

[Lecture d'antivirus d'enable](#)

[Configurez l'antivirus dans des stratégies de messagerie](#)

[Graymail](#)

[Vérifiez la touche de fonction](#)

[L'enable Graymail et le coffre-fort se désabonnent des services](#)

[Configurez Graymail et le coffre-fort se désabonnent dans les stratégies](#)

[Filtres d'épidémie](#)

[Vérifiez la touche de fonction](#)

[L'épidémie d'enable filtre le service](#)

[Configurez les filtres d'épidémie dans les stratégies](#)

[Conclusion](#)

## 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'**Enable** bouton sur des **paramètres généraux IMS** :

IMS Global Settings	
Ironport Intelligent Multi-Scan:	Enabled
Regional Scanning:	Off
<a href="#">Edit IMS Settings</a>	

- 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 :

Edit Common Global Settings	
Message Scanning Thresholds:	<p>Increasing these values may result in decreased performance. Please consult documentation for size recommendations based on your environment.</p> <p>Always scan messages smaller than <input type="text" value="2M"/> Maximum  <i>Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less.</i></p> <p>Never scan messages larger than <input type="text" value="3M"/> Maximum  <i>Add a trailing K or M to indicate units. Recommended setting is 2048K(2MB) or less.</i></p>
Timeout for Scanning Single Message:	<input type="text" value="60"/> Seconds

- **Validation de Submit** and 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'**Enable** bouton 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 :

IronPort Anti-Spam Global Settings	
<input checked="" type="checkbox"/> <b>Enable IronPort Anti-Spam Scanning</b>	
Message Scanning Thresholds:	<p>Increasing these values may result in decreased performance. Please consult documentation for size recommendations based on your environment.</p> <p>Always scan messages smaller than <input type="text" value="2M"/> Maximum Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less.</p> <p>Never scan messages larger than <input type="text" value="3M"/> Maximum Add a trailing K or M to indicate units. Recommended setting is 2048K(2MB) or less.</p>
Timeout for Scanning Single Message:	<input type="text" value="60"/> Seconds
Scanning Profile:	<p><input type="radio"/> Normal</p> <p><input checked="" type="radio"/> <b>Aggressive</b> <i>Recommended for customers who desire a stronger emphasis on blocking spam. When enabled, tuning Anti-Spam policy thresholds will have more impact on spam detection than the normal profile with a larger potential for false positives. Do not select the aggressive profile if IMS is enabled on the mail policy.</i></p> <p><input type="radio"/> Regional (China)</p>

- 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 **Configure** bouton vous portera à la page suivante.
- Voici que vous pouvez activer la quarantaine en vérifiant l'**enable** box 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 :

External Spam Quarantine Settings	
<input checked="" type="checkbox"/> <b>Enable External Spam Quarantine</b>	
Name:	<input type="text" value="centralized_spam"/> <i>(e.g. spam_quarantine)</i>
IP Address:	<input type="text" value="sma_ip_address"/>
Port:	<input type="text" value="6025"/>
Safelist/Blocklist:	<input checked="" type="checkbox"/> <b>Enable End User Safelist/Blocklist Feature</b> Blocklist Action: <input type="text" value="Quarantine"/>

- 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 :

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
	Default Policy	IronPort Intelligent Multi-Scan Positive: Deliver Suspected: Deliver	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Malware File: Drop Pending Analysis: Quarantine Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not ...	Graymail Detection Unsubscribe: Enabled Marketing: Spam Quarantine Social: Spam Quarantine Bulk: Spam Quarantine ...	URL_LOG_ALL_REPUTATION URL_LOG_ALL_CATEGORY URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE SPF_DKIM_FAIL ...	Retention Time: Virus: 1 day Other: 4 hours	

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** :

Anti-Spam Settings	
<b>Policy:</b>	Default
Enable Anti-Spam Scanning for This Policy:	<input type="radio"/> Use IronPort Anti-Spam service <input checked="" type="radio"/> Use IronPort Intelligent Multi-Scan <i>Spam scanning built on IronPort Anti-Spam.</i> <input type="radio"/> Disabled

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-Identifiant** 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 :

Positively-Identified Spam Settings	
Apply This Action to Message:	Spam Quarantine <input type="button" value="v"/> <i>Note: If local and external quarantines are defined, mail will be sent to local quarantine.</i>
Add Text to Subject:	Prepend <input type="button" value="v"/> <input type="text" value="[SPAM]"/>
<input type="button" value="Advanced"/>	Optional settings for custom header and message delivery.
Suspected Spam Settings	
Enable Suspected Spam Scanning:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Apply This Action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	Prepend <input type="button" value="v"/> <input type="text" value="[SUSPECTED SPAM]"/>
<input type="button" value="Advanced"/>	Optional settings for custom header and message delivery.

- **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** :

Spam Thresholds	
Spam is scored on a 1-100 scale. The higher the score, the more likely a message is a spam.	
IronPort Anti-Spam:	<input checked="" type="radio"/> Use the Default Thresholds <input type="radio"/> Use Custom Settings: Positively Identified Spam: Score > <input type="text" value="90"/> (50 - 100) Suspected Spam: Score > <input type="text" value="50"/> (minimum 25, cannot exceed positive spam score)
IronPort Intelligent Multi-Scan:	<input type="radio"/> Use the Default Thresholds <input checked="" type="radio"/> Use Custom Settings: Positively Identified Spam: Score > <input type="text" value="90"/> (50 - 100) Suspected Spam: Score > <input type="text" value="43"/> (minimum 25, cannot exceed positive spam score)

- 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 :

Sophos Anti-Virus Overview	
Anti-Virus Scanning by Sophos Anti-Virus:	Enabled
Virus Scanning Timeout (seconds):	60
Automatic Updates: (?)	Enabled
<a href="#">Edit Global Settings...</a>	

Current Sophos Anti-Virus files			
File Type	Last Update	Current Version	New Update
Sophos Anti-Virus Engine	Wed Nov 6 10:04:30 2019	3.2.07.377.1_5.68	Not Available
Sophos IDE Rules	Wed Nov 6 12:03:56 2019	2019110602	Not Available
No updates in progress.			<a href="#">Update Now</a>

- 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** :

Anti-Virus Settings	
<b>Policy:</b>	DEFAULT
<b>Enable Anti-Virus Scanning for This Policy:</b>	<input checked="" type="radio"/> Yes <input checked="" type="checkbox"/> Use McAfee Anti-Virus <input checked="" type="checkbox"/> Use Sophos Anti-Virus <input type="radio"/> No

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

Message Scanning	
	Scan for Viruses only <input type="button" value="v"/> <input type="checkbox"/> Drop infected attachments if a virus is found <input checked="" type="checkbox"/> (recommended) Include an X-header with the Anti-Virus scanning results in messages
Repaired Messages:	
Action Applied to Message:	<input type="text" value="Deliver As Is"/>
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input checked="" type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append
	<input type="text" value="[WARNING: VIRUS REMOVED]"/>
<a href="#">Advanced</a>	Optional settings for custom header and message delivery.

- 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 :

Encrypted Messages:	
Action Applied to Message:	Deliver As Is
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[A/V UNSCANNABLE]
▶ Advanced	Optional settings for custom header and message delivery.
Unscannable Messages:	
Action Applied to Message:	Deliver As Is
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[A/V UNSCANNABLE]
▶ Advanced	Optional settings for custom header and message delivery.
Virus Infected Messages:	
Action Applied to Message:	Drop Message
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[WARNING : VIRUS DETECTED]
▶ Advanced	Optional settings for custom header and message delivery.

- **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 Settings** bouton 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 :**

Graymail Global Settings	
Graymail Detection	Enabled
Safe Unsubscribe	Enabled
Automatic Updates <sup>?</sup>	Enabled

[Edit Graymail Settings](#)

- 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** :

Graymail Settings	
<b>Policy:</b>	DEFAULT
<b>Enable Graymail Detection for This Policy:</b>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<b>Enable Graymail Unsubscribing for This Policy:</b>	<input checked="" type="radio"/> Yes <input type="radio"/> No
	Perform this action for: <input checked="" type="radio"/> All Messages (Recommended) <input type="radio"/> Unsigned Messages

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 :

✓ Action on Marketing Email	
Apply this action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[MARKETING]"/>
▸ Advanced	<i>Optional settings for custom header and message delivery.</i>
✓ Action on Social Network Email	
Apply this action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[SOCIAL NETWORK]"/>
▸ Advanced	<i>Optional settings for custom header and message delivery.</i>
✓ Action on Bulk Email	
Apply this action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[BULK]"/>
▸ Advanced	<i>Optional settings for custom header and message delivery.</i>

- 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 :

Outbreak Filters Global Settings	
<input checked="" type="checkbox"/> <b>Enable Outbreak Filters</b>	
Adaptive Rules:	<input checked="" type="checkbox"/> <b>Enable Adaptive Rules</b>
Maximum Message Size to Scan:	<input type="text" value="3M"/> Maximum <i>Add a trailing K or M to indicate units.</i>
Emailed Alerts: (?)	<input checked="" type="checkbox"/> <b>Receive Emailed Alerts</b>
Web Interaction Tracking: (?)	<input checked="" type="checkbox"/> <b>Enable Web Interaction Tracking</b>

- 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 :

Outbreak Filter Settings	
Quarantine Threat Level: ?	3
Maximum Quarantine Retention:	Viral Attachments: 1 Days Other Threats: 4 Hours <input type="checkbox"/> Deliver messages without adding them to quarantine
Bypass Attachment Scanning: ▶	None configured

- 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 :

Message Modification	
<input checked="" type="checkbox"/> Enable message modification. Required for non-viral threat detection (excluding attachments)	
Message Modification Threat Level: ?	3
Message Subject:	Prepend: [[Possible \$threat_category Fraud] <a href="#">Insert Variables</a>   <a href="#">Preview Text</a>
Include the X-IronPort-Outbreak-Status headers:	<input type="radio"/> Enable for all messages <input type="radio"/> Enable only for threat-based outbreak <input checked="" type="radio"/> Disable
Include the X-IronPort-Outbreak-Description header:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Alternate Destination Mail Host (Other Threats only):	<input type="text"/> <small>(examples: example.com, 10.0.0.1, 2001:420:80:1::5)</small>
URL Rewriting:	Cisco Security proxy scans and rewrites all URLs contained in malicious outbreak emails. <input type="radio"/> Enable only for unsigned messages (recommended) <input checked="" type="radio"/> Enable for all messages <input type="radio"/> Disable
Bypass Domain Scanning ?	<input type="text"/> <small>(examples: example.com, crm.example.com, 10.0.0.1, 10.0.0.0/24, 2001:420:80:1::5, 2001:db8::/32)</small>
Threat Disclaimer:	System Generated <a href="#">Preview Disclaimer</a> <small>Disclaimer text will be applied to the top of the message body for Suspicious and Quarantined messages. To create custom disclaimers go to <a href="#">Mail Policies &gt; Text Resources &gt; Disclaimers</a></small>

- **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.