

# Best Practice Guide for Anti-Spam, Anti-Virus, Graymail and Outbreak Filters

## Inhoud

[Overzicht](#)

[antispam](#)

[Functietoets controleren](#)

[Intelligent Multi-Scan \(IMS\) mondiaal inschakelen](#)

[Gecentraliseerde spamquarantaine inschakelen](#)

[Anti-spam in beleid configureren](#)

[tegen het virus](#)

[Controleer de functietoetsen](#)

[Het scannen van antivirussen inschakelen](#)

[Anti-virus instellen in postbeleid](#)

[Graymail](#)

[Functietoets controleren](#)

[Graymail en Safe unSubscriber-services inschakelen](#)

[Graymail en Safe unsubscribe in beleid configureren](#)

[Outdoorfilters](#)

[Functietoets controleren](#)

[Inschakelen voor omloopfilters](#)

[Filters voor breuk configureren in beleid](#)

[Conclusie](#)

## Overzicht

De overgrote meerderheid van bedreigingen, aanvallen en overlast waar een organisatie mee te maken heeft via e-mail nemen de vorm aan van spam, malware en gemengde aanvallen. Cisco's e-mail security applicatie (ESA) omvat verschillende technologieën en functies om deze bedreigingen af te sluiten bij de gateway voordat ze de organisatie binnenkomen. In dit document worden de beste werkwijzen beschreven om antispam-, antivirale, grijsmail- en uitbraakfilters te configureren op zowel de inkomende als uitgaande e-mailstroom.

## antispam

Anti-Spam-bescherming richt zich op een volledig scala aan bekende bedreigingen, waaronder aanvallen met spam, phishing en zombie, evenals moeilijk te detecteren kleine, kortstondige e-mailbedreigingen zoals "419". Bovendien identificeert de anti-Spam bescherming nieuwe en evoluerende gemengde bedreigingen zoals spamaanvallen die kwaadwillige inhoud door een download URL of een uitvoerbaar voorwerp verdelen.

Cisco e-mail security biedt de volgende anti-spamoplossingen:

- IronPort Anti-Spam Filtering (IPAS)

- Cisco Intelligent Multi-Scan Filtering (IMS)

U kunt uw ESA-oplossing licentiëren en inschakelen, maar u kunt deze alleen gebruiken in een bepaald postbeleid. In dit document met beste praktijken zullen wij gebruik maken van de IMS-functie.

## Functietoets controleren

- Raadpleeg in het ESR **stelsysteembeheer > Functietoetsen**
- Zoek de Intelligent Multi-Scan-licentie en controleer of deze actief is.

## Intelligent Multi-Scan (IMS) mondiaal inschakelen

- Aan het ESA, navigeren naar **Security Services > IMS** en grijsmail
- Klik het **inschakeltoets** op **IMS Global Settings**:

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

- Zoek naar **Gemeenschappelijke Mondiale Instellingen** en klik op **Global Settings bewerken**
- Hier u kunnen vormen veelvoudig instellingen. Het aanbevolen instellingen zijn getoond in het afbeelding hieronder:

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  <small>Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less.</small></p> <p>Never scan messages larger than <input type="text" value="3M"/> Maximum  <small>Add a trailing K or M to indicate units. Recommended setting is 2048K(2MB) or less.</small></p>
Timeout for Scanning Single Message:	<input type="text" value="60"/> Seconds

- Klik op **Inzenden** **Doe uw wijzigingen**.

Als u geen IMS-licentieserverabonnement hebt:

- Navigatie in naar **security services > IronPort Anti-Spam**
- Klik het **inschakelen**knop op **IronPort Anti-Spam - Overzicht**
- Klik op **Global Settings bewerken**
- Hier u kunnen vormen veelvoudig instellingen. Het aanbevolen instellingen zijn getoond in het afbeelding hieronder:

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  <small>Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less.</small></p> <p>Never scan messages larger than <input type="text" value="3M"/> Maximum  <small>Add a trailing K or M to indicate units. Recommended setting is 2048K(2MB) or less.</small></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>  <small>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.</small></p> <p><input type="radio"/> Regional (China)</p>

- Cisco raadt aan **Aggressive** Scanning Profile te selecteren voor een klant die een sterke nadruk op het blokkeren van spam wenst.
- Klik op **Inzendenen Doe uw wijzigingen**

## Gecentraliseerde spamquarantaine inschakelen

Aangezien anti-spam de mogelijkheid heeft om naar quarantaine te worden overgebracht, is het belangrijk ervoor te zorgen dat de spamquarantaine wordt ingesteld:

- Navigatie in naar **Security Services > Spam Quarantine**
- Klikring het **Configureren**knoop willen nemen u aan het vouwenverschuldigd pagina.
- Hier u kunnen toelaten het quarantaine door controleren het **toelatendoos** en punte quarantaine aan worden gecentraliseerd aan een beveiligingBeheer AApplicatie (SMA) doorvulling in het **SMANamen IP adres**. Het aanbevolen instellingen zijn getoond hieronder:

External Spam Quarantine Settings	
<input checked="" type="checkbox"/> <b>Enable External Spam Quarantine</b>	
Name:	<input type="text" value="centralized_spam"/> <small>(e.g. spam_quarantine)</small>
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"/>

- Klik op **Inzendenen Doe uw wijzigingen**

Raadpleeg voor meer informatie over het instellen en gecentraliseerde quarantaine, het document met de beste praktijken:

[Best Practices for Centralized Policy, Virus and Outbreak Quarantines Setup en Migratie van ESA naar SMA](#)

## Anti-spam in beleid configureren

Eenvoudig intelligent Meervoudig - Scannen heeft zijn ingesteld mondiaal , u kunnen nu toepassen intelligent Meervoudig - Scannen aan post beleid :

- Navigeren in op **e-mailbeleid > Inkomend postbeleid**
- Het inkomende-mailbeleid gebruikt standaard IronPort Anti-Spam-instellingen.
- Als u onder **Anti-Spam** op de blauwe link klikt, kan dat specifieke beleid aangepaste anti-

Spam-instellingen gebruiken.

- Hieronder ziet u een voorbeeld dat het Standaardbeleid toont met aangepaste anti-spam-instellingen:

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	

Pas de anti-spam instellingen voor een inkomend postbeleid aan door op de blauwe link onder **Anti-Spam** te klikken voor het beleid dat u wilt aanpassen.

Hier u kunnen selecteren het tegenstander-Spam Scannen accessoire u wensen aan toelaten voor dit beleid.

- Voor het doel van dit beste uitvoerenijs document, klikken het radio knoop Volgende aan Gebruik **IJzeren poort intelligent multi-modeScannen**:

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

De volgende twee delen omvatten **positief-geïdentificeerde Spam** instellingen en **verdachte Spam**-instellingen:

- De aanbevolen beste praktijk is de **Quarantine**-actie te configureren bij **positief geïdentificeerde** Spam-instelling met de aan het onderwerp toegevoegde tekst **[SPAM]** en
- Toepassen op **Deliver** als de actie voor **verdachte spam-instellingen** met de voorgevulde tekst **[VERDACHTE SPAM]** die aan het onderwerp is toegevoegd:

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="v"/> <b>Advanced</b>	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="v"/> <b>Advanced</b>	Optional settings for custom header and message delivery.

- De instelling **Drempelwaarde** kan worden gewijzigd en de aanbevolen instellingen moeten de **Positive-Identified Spam** score op **90** aanpassen en de **Verdachte Spam**-score op **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)

- Klik op **Inzendenen Doe uw wijzigingen**

## tegen het virus

De bescherming tegen virussen wordt geboden door twee motoren van derden - Sofos en McAfee. Deze motoren filteren alle bekende kwaadaardige bedreigingen, vallen, schoonmaken of in quarantaine plaatsen zoals ze zijn geconfigureerd.

## Controleer de functietoetsen

U kunt controleren of beide functietoetsen ingeschakeld en actief zijn:

- Ga naar **stysteembeheer > Functiesets**
- Controleer of zowel **Sofas Anti-Virus** als **McAfee** licenties actief zijn.

## Het scannen van antivirussen inschakelen

- navigeren aan **Security Services > Antivirus - Sofobie**
- Klik het **inschakelen**-toets.
- Zorg ervoor dat **Automatische update** is **ingeschakeld** en dat de update van Sofos Anti-Virus werkt prima. Indien nodig klikt u op **Nu bijwerken** om het bestand direct te uploaden:

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>

- Klik op **Inzendenen Doe uw wijzigingen**.

Als McAfee-licentie ook actief is, navigeer aan **Security Services > Antivirus - McAfee**

- Klik het **inschakelen**-toets.
- Zorg ervoor dat **Automatische update** is **ingeschakeld** en dat de update van McAfee Anti-Virus prima werkt. Klik indien nodig op **Nu bijwerken** om het bestand direct te uploaden.

- Klik op Inzendenen **Doe uw wijzigingen**

## Anti-virus instellen in postbeleid

Op een inkomend postbeleid, wordt het volgende aanbevolen:

- Navigeren in op **e-mailbeleid > Inkomend postbeleid**
- Pas de instellingen voor **antivirale middelen** aan voor een inkomende e-mailbeleid door op de blauwe link onder Anti-Virus te klikken voor het beleid dat u wilt aanpassen.
- Hier u kunnen selecteren het tegenstander-virus Scannen accessoire u wensen aan toelaten voor dit beleid.
- Voor het doel van deze bnepbekortenijs Selecteer in het document zowel **McAfee** als **Sofoss Anti-Virus**:

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

- We proberen geen bestand te repareren. Het bericht blijft **alleen** scannen **naar virussen**:

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.

- De aanbevolen actie voor zowel **versleutelde** als **niet-scannbare berichten** is **AS-is** met een aangepaste onderwerpregel te **leveren** voor hun aandacht.
- Het aanbevolen beleid voor antivirale middelen is **Drop** alle **via het virus geïnfekteerde berichten** zoals in de afbeelding hieronder wordt getoond:

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.

- Klik op **Inzendenen Doe uw wijzigingen**

Een soortgelijk beleid wordt aanbevolen voor het beleid voor uitgaande e-mail, maar we raden niet aan de onderwerpregel aan te passen op uitgaande e-mail.

## Graymail

De oplossing voor grijsmailbeheer in het e-mailsecurity apparaat bestaat uit twee onderdelen: een geïntegreerde grijsmailscanmachine en een op de cloud gebaseerde Unsubscribe-service. De oplossing voor grijsmailbeheer stelt organisaties in staat om grijsmail te identificeren met behulp van de geïntegreerde grijsmailmotor en passende beleidscontroles toe te passen en een makkelijk mechanisme te bieden voor eindgebruikers om zich te ontkoppelen van ongewenste berichten met behulp van Unsubscribe Service.

De categorieën Grijsmail omvatten marketing e-mail, sociaal netwerk e-mail en bulkmail. Geavanceerde opties omvatten het toevoegen van een aangepaste header, het verzenden naar een alternatieve host en het archiveren van het bericht. Voor deze beste praktijk zullen we de optie Safe Unsubscribe van Graymail voor het standaard postbeleid mogelijk maken.

### Functietoets controleren

- Raadpleeg in het ESR **stelselbeheer > Functietoetsen**
- Zoek **Graymail Safe Unabonnement** en controleer of het actief is.

### Graymail en Safe unSubscriber-services inschakelen

- Aan het ESA, navigeren aan **Security Services> IMS en grijsmail**
- Klik het **Graymail-instellingen bewerken**knop **Global Settings in Graymail**
- Selecteer alle opties - **Graymail-detectie inschakelen, Safe Unsubscribe inschakelen en automatische updates inschakelen:**



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

[Edit Graymail Settings](#)

- Klik op **Inzendenen Doe uw wijzigingen**

## Graymail en Safe unsubscribe in beleid configureren

Eenmaal Graymail en Safe unsubscribe heeft zijn ingesteld mondiaal, u kunnen nu deze diensten toepassen aan post beleid.

- Navigeren in op **e-mailbeleid > Inkomend postbeleid**
- Als u onder **Graymail** op de blauwe link klikt, wordt dat beleid aangepast door aangepaste instellingen voor Graymail te gebruiken.
- Hier u kunnen selecteren de Graymailopties u wensen aan toelaten voor dit beleid.
- Voor het doel van dit beste samenvattingbekortenijis document, klikken het radio knoop Volgende U kunt **Graymail** als volgt **detecteren voor dit beleid** en u kunt **Graymail** niet **ondertekenen voor dit beleid**:

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

De volgende drie onderdelen zijn: **Actie om e-mailinstellingen op de markt te brengen**, **Actie om e-mailinstellingen van sociale netwerken en Actie om e-mailinstellingen op te slaan**.

- De aanbevolen beste praktijk is om deze allemaal in staat te stellen en de actie als **Leverancier** te blijven met de toegevoegde tekst voor de onderstaande categorieën:

<b>✓ Action on Marketing Email</b>	
Apply this action to Message:	Deliver <input type="text" value="↓"/> 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]"/>
<b>Advanced</b>	<i>Optional settings for custom header and message delivery.</i>
<b>✓ Action on Social Network Email</b>	
Apply this action to Message:	Deliver <input type="text" value="↓"/> 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]"/>
<b>Advanced</b>	<i>Optional settings for custom header and message delivery.</i>
<b>✓ Action on Bulk Email</b>	
Apply this action to Message:	Deliver <input type="text" value="↓"/> 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]"/>
<b>Advanced</b>	<i>Optional settings for custom header and message delivery.</i>



- Klik op **Inzendenen Doe uw wijzigingen**

Het vertrekkende Mail-beleid moet **Graymail** in **uitgeschakeld** blijven.

## Outdoorfilters

Outdoorfilters combineren triggers in de anti-spam motor, URL scanning en detectietechnologie en meer om items die buiten de echte spamcategorie vallen correct te markeren - bijvoorbeeld phishing e-mails en scam e-mails en ze op juiste wijze te verwerken met gebruikerskennisgevingen of quarantaine.

### Functietoets controleren

- Raadpleeg in het ESR **systeembeheer > Functietoetsen**
- Zoek naar **Outdoorfilters** en controleer of deze actief is.

### Inschakelen voor omloopfilters

- Aan het ESA, navigeren aan **Security Services> Outdoorfilters**
- Klik het **inschakelen**knop voor **omloopfilters - Overzicht**
- Hier u kunnen vormen veelvoudig instellingen. Het aanbevolen instellingen zijn getoond in het afbeelding hieronder:

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 <small>Add a trailing K or M to indicate units.</small>
Emailed Alerts: (?)	<input checked="" type="checkbox"/> <b>Receive Emailed Alerts</b>
Web Interaction Tracking: (?)	<input checked="" type="checkbox"/> <b>Enable Web Interaction Tracking</b>

- Klik op **Inzendenen Doe uw wijzigingen**.

### Filters voor breuk configureren in beleid

Filters eenmaal uiteinde heeft zijn ingesteld mondiaal , u kunnen nu deze optie toepassen op post beleid.

- Navigeren in op **e-mailbeleid > Inkomend postbeleid**
- Als u op de blauwe link klikt onder **Outdoorfilters**, kunt u dat specifieke beleid gebruiken om aangepaste instellingen voor Outdoorfilters te gebruiken.
- Voor het doel van dit beste uitvoerenijs U kunt als document de standaardinstellingen voor het filter uitzetten:

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

- Outbreak Filters kunnen URL's herschrijven als ze kwaadaardig, verdacht of phish worden geacht. Selecteer **berichtwijziging inschakelen** om URL-gebaseerde bedreigingen te detecteren en te herschrijven.

- Zorg ervoor dat de optie **URL herschrijven** is **Schakel** in voor alle berichten zoals hieronder wordt weergegeven:

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</a> &gt; <a href="#">Text Resources</a> &gt; <a href="#">Disclaimers</a></small>

- Klik op **Inzenden** **Doe uw wijzigingen**

Uitgaande Mail Policy zou moeten zorgen dat **Outbreak Filters** in **uitgeschakeld** toestand blijven.

## Conclusie

Dit document was bedoeld om de standaardinstellingen of de best practice-formaten voor anti-spam-, anti-virus-, graymail- en outbreak-filters in de e-mailsecurity applicatie (ESA) te beschrijven. Al deze filters zijn beschikbaar in zowel het inkomende als de uitgaande e-mailbeleid en configuratie en filtering worden op beide aanbevolen, terwijl het grootste deel van de beveiliging naar binnen moet, terwijl filtering van de uitgaande stroom bescherming biedt tegen relaxed e-mails of interne aanvallen.