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

Inhoud

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)

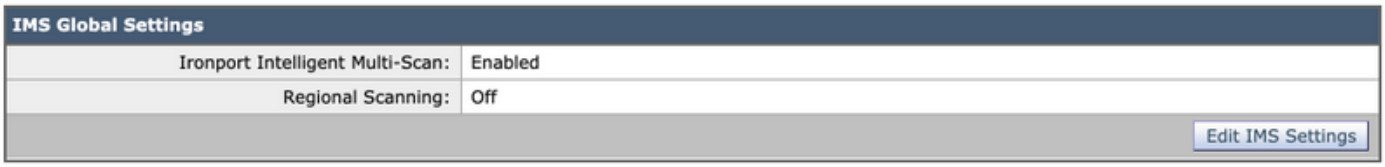
U kunt uw ESA-oplossing licentiëren en inschakelen, maar u kunt deze alleen gebruiken in een bepaald postbeleid. In dit document met beste praktijken zullen wij gebruik maken van de IMS-functie.

Functietoets controleren

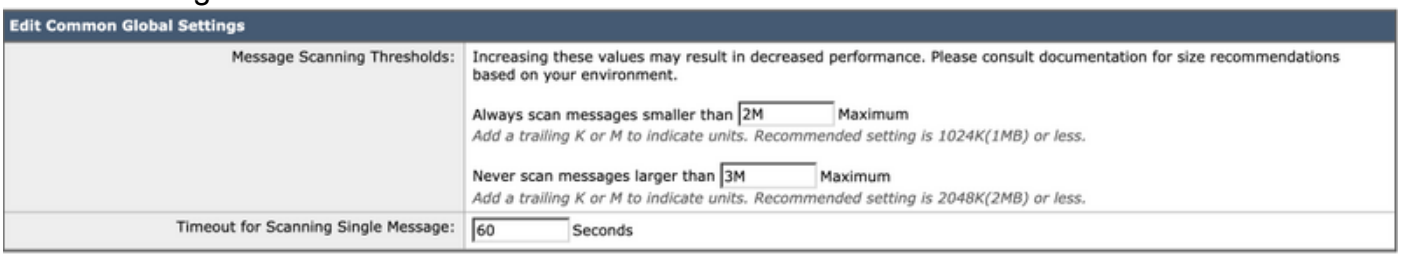
- Raadpleeg in het ESR **systeembeheer > Functietoetsen**
- Zoek de Intelligent Multi-Scan-licentie en controleer of deze actief is.

Intelligent Multi-Scan (IMS) mondiaal inschakelen

- Aan het ESA, navigeren aan **Security Services> IMS en grijsmail**
- Klik het **inschakelen**toets op **IMS Global Settings**:



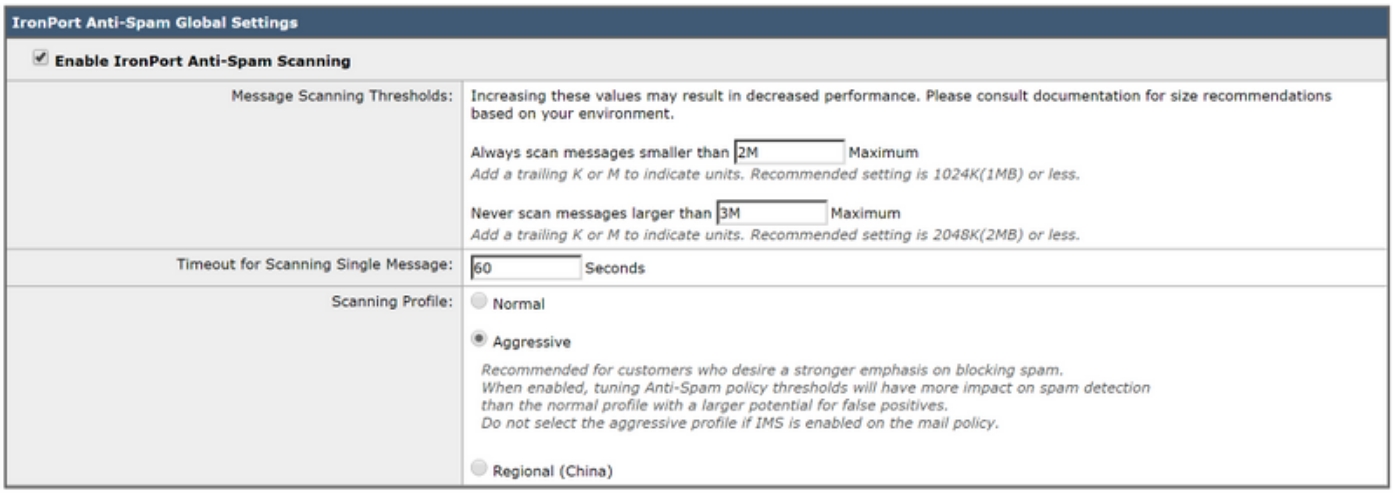
- Zoek naar **Gemeenschappelijke Mondiale Instellingen** en klik op **Global Settings bewerken**
- Hier u kunnen vormen veelvoudig instellingen. Het aanbevolen instellingen zijn getoond in het afbeelding hieronder:



- Klik op **Inzenden**en **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:

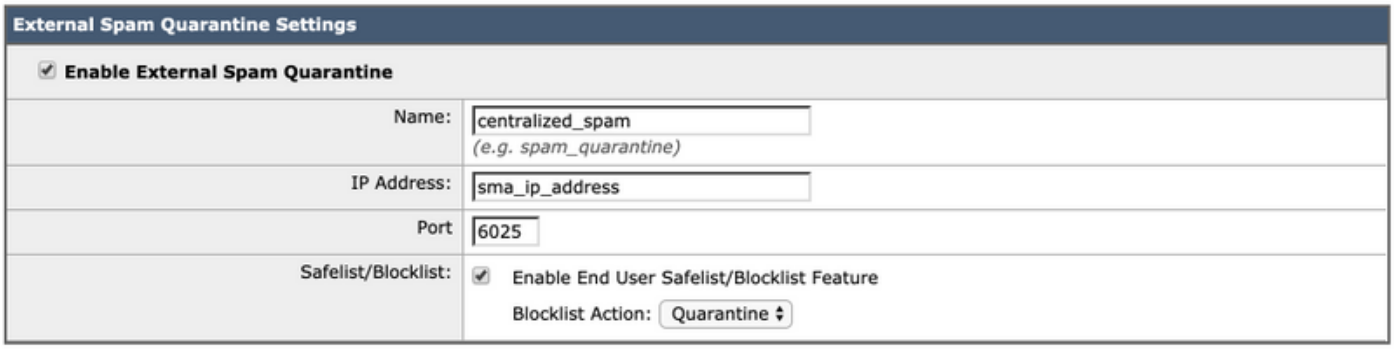


- Cisco raadt aan **Aggressive** Scanning Profile te selecteren voor een klant die een sterke nadruk op het blokkeren van spam wenst.
- Klik op **Inzenden**en **Doe uw wijzigingen**

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 **toelaten**doos en punte quarantain e aan worden gecentraliseerd aan een beveiligingBeheer AApplicatie (SMA) doorvulling in het SMA**Name**en **IP adres.** Het aanbevolen instellingen zijn getoond hieronder:



- Klik op **Inzenden**en **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]

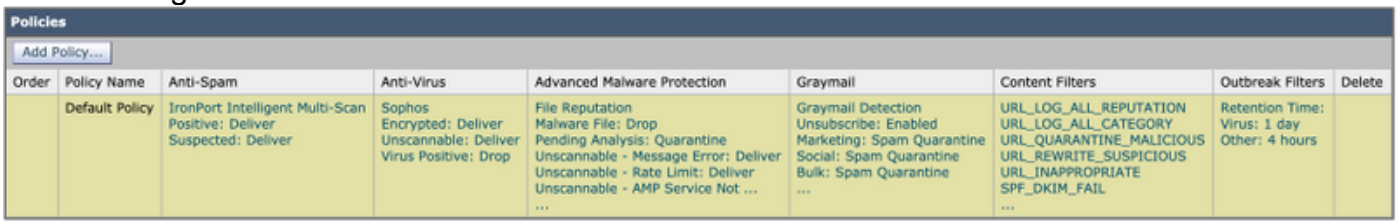
Anti-spam in beleid configureren

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.

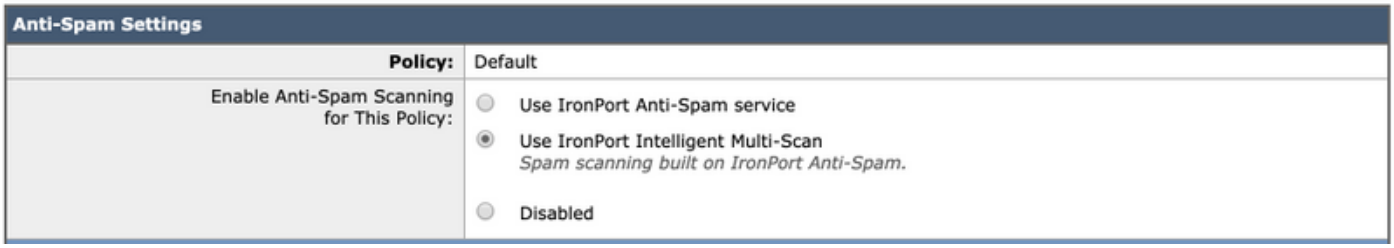
- Hieronder ziet u een voorbeeld dat het Standaardbeleid toont met aangepaste anti-spam-instellingen:



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.

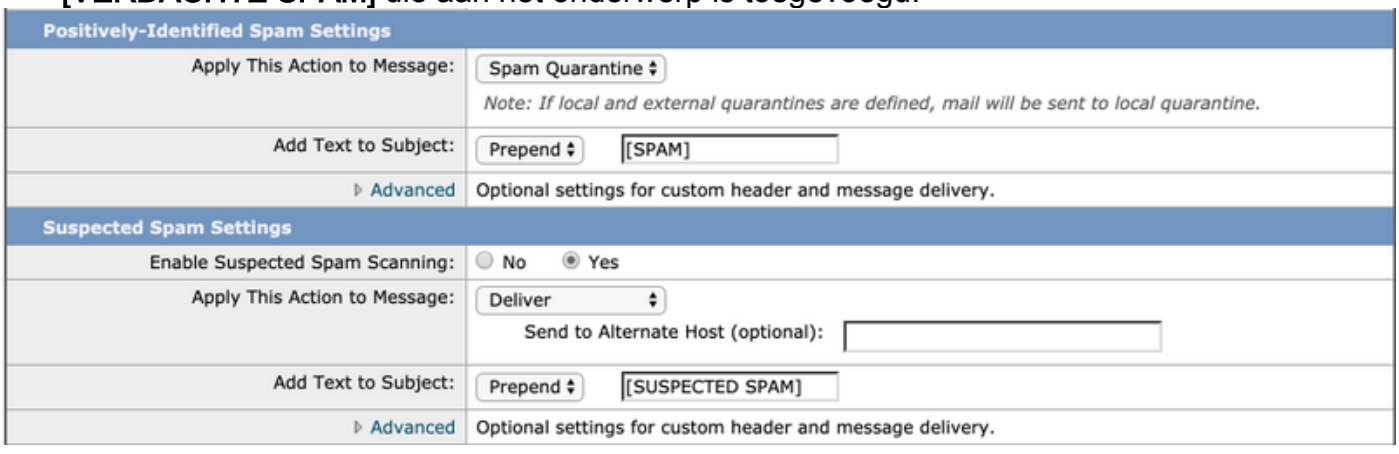
Hier u kunnen selecteren het tegenstander-
Spam Scannen accessoire u wensen aan toelaten voor dit beleid.

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

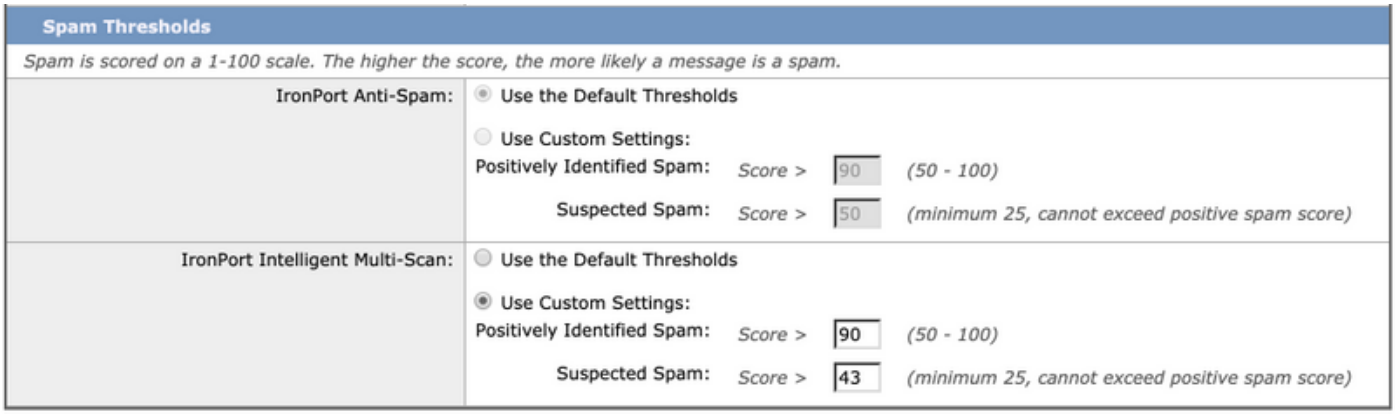


De volgende twee delen omvatten **positief-geïdentificeerde Spam** instellingen en **verdachte Spam-instellingen:**

- 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:



- **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**:



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

tegen het virus

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

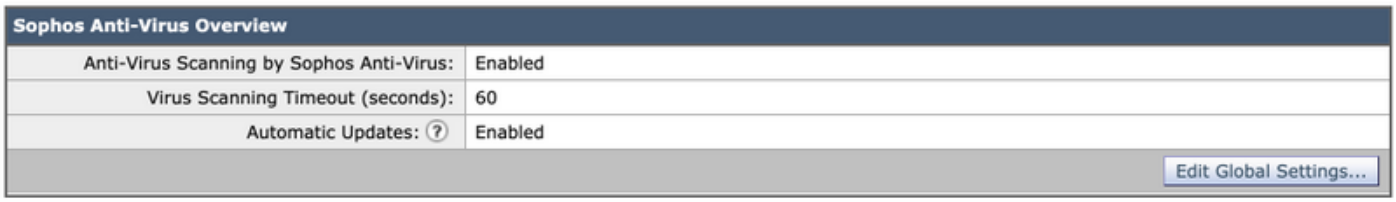
Controleer de functietoetsen

U kunt controleren of beide functietoetsen ingeschakeld en actief zijn:

- Ga naar **systeembeheer > 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 Sofo's Anti-Virus werkt prima. Indien nodig klikt u op **Nu bijwerken** om het bestand direct te uploaden:



- Klik op **Inzenden**en **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.

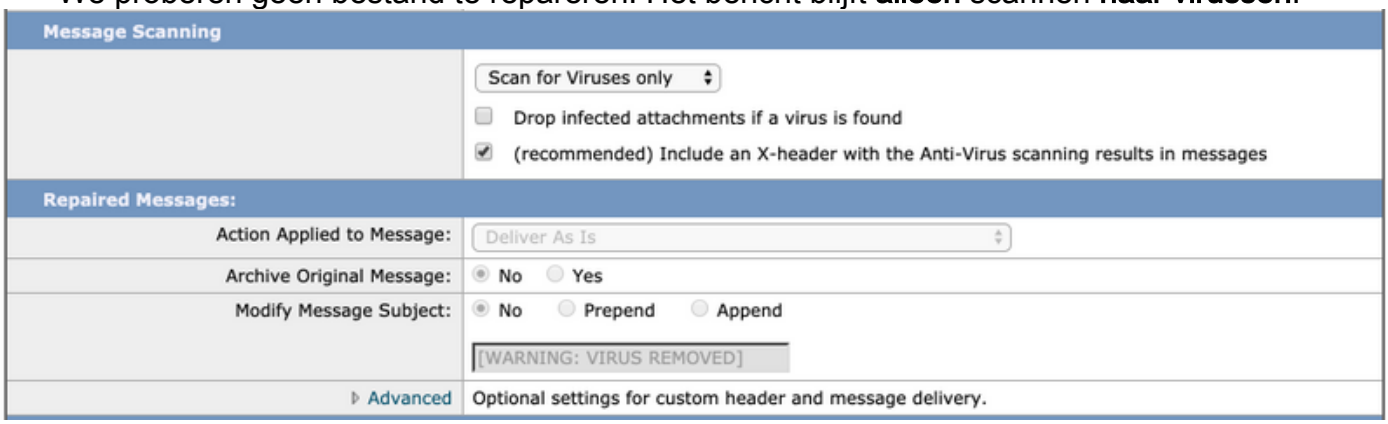
- Klik op **Inzendenen** **Doe uw wijzigingen**

Anti-virus instellen in postbeleid

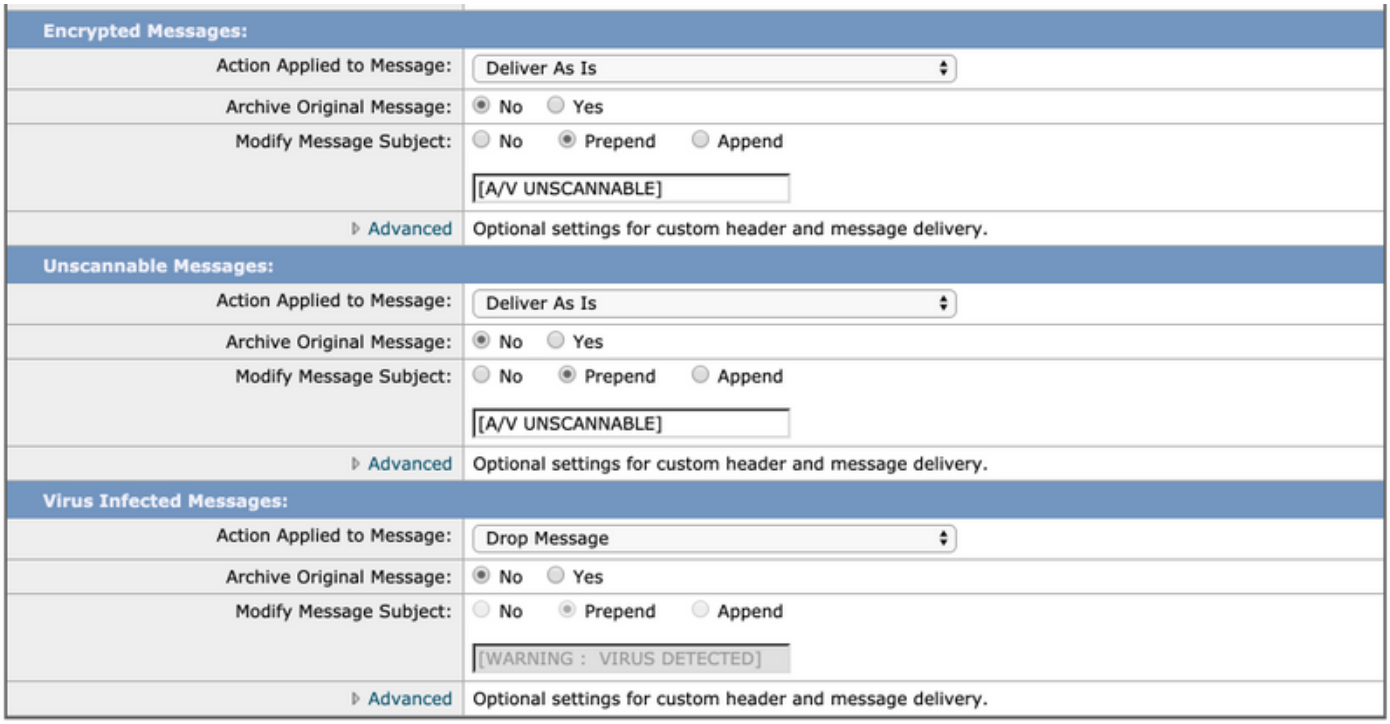
Op een inkomend postbeleid, wordt het volgende aanbevolen:

- 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**:

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



- 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 geïnfecteerde berichten** zoals in de afbeelding hieronder wordt getoond:



- Klik op **Inzenden**en **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.

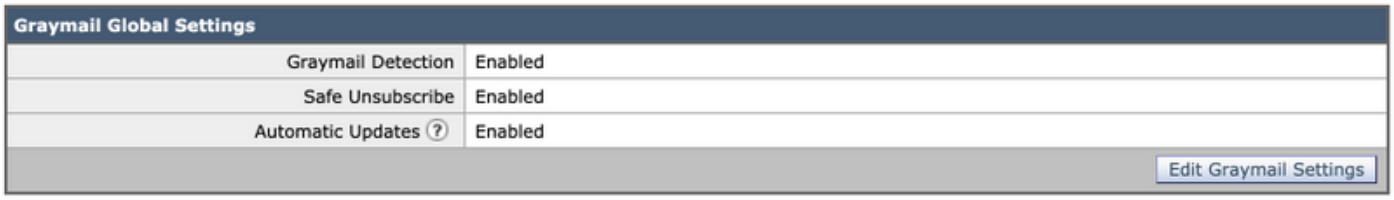
De categorieën Grijsmail omvatten marketing e-mail, sociaal netwerk e-mail en bulkmail. Geavanceerde opties omvatten het toevoegen van een aangepaste header, het verzenden naar een alternatieve host en het archiveren van het bericht. Voor deze beste praktijk zullen we de optie Safe Unsubscribe van Graymail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

Functietoets controleren

- Raadpleeg in het ESR **systeembeheer > 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**:



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

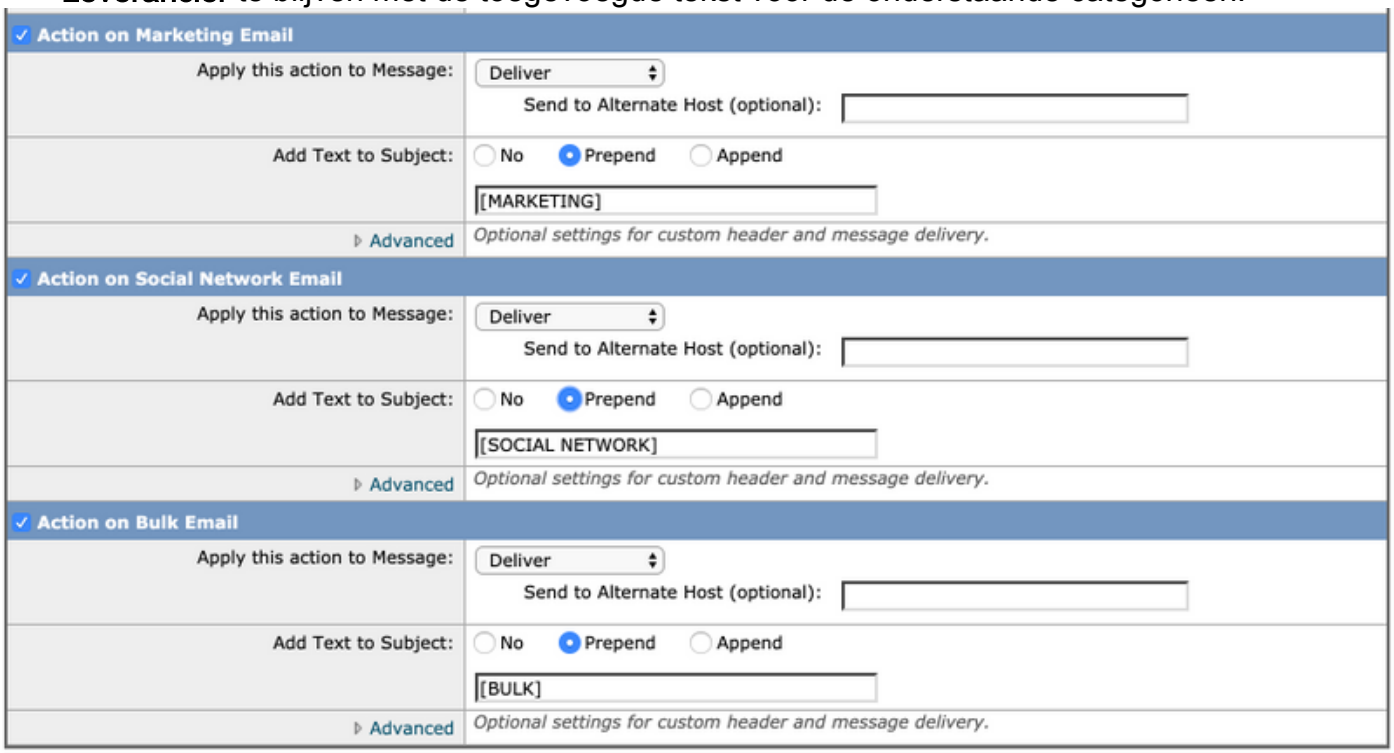
Graymail en Safe unsubscript in beleid configureren

Eenmaal Graymail en Safe unsubscript 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 samenvattingbekortenijs document, klikken het radio knoop Volgende U kunt **Graymail** als volgt **detecteren voor dit beleid** en **u kunt Graymail** niet **ondertekenen voor dit beleid**:

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:



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

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

Outdoorfilters

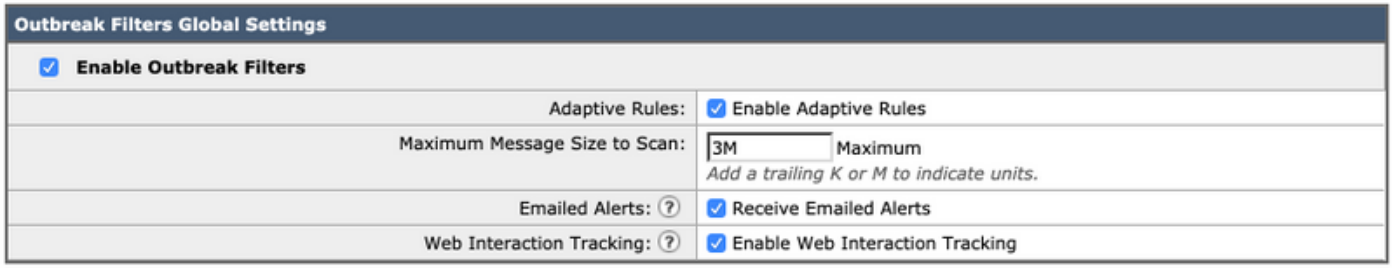
Outdoorfilters combineren triggers in de anti-spam motor, URL scanning en detectietechnologie en meer om items die buiten de echte spamcategorie vallen correct te markeren - bijvoorbeeld phishing e-mails en scam e-mails en ze op juiste wijze te verwerken met gebruikerskennisgevingen of quarantaine.

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:

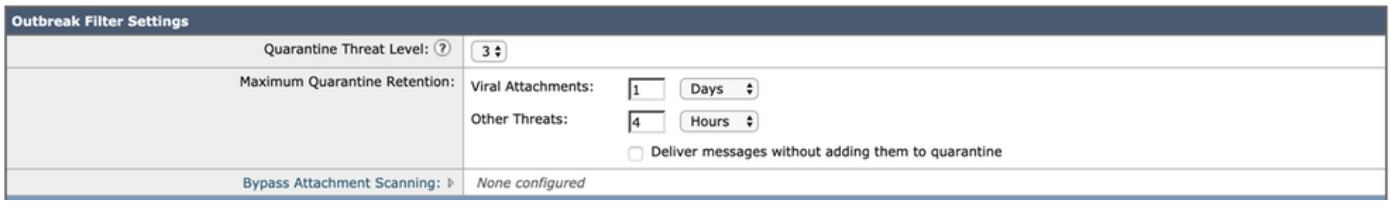


- Klik op **Inzenden**en **Doe uw wijzigingen.**

Filters voor breuk configureren in beleid

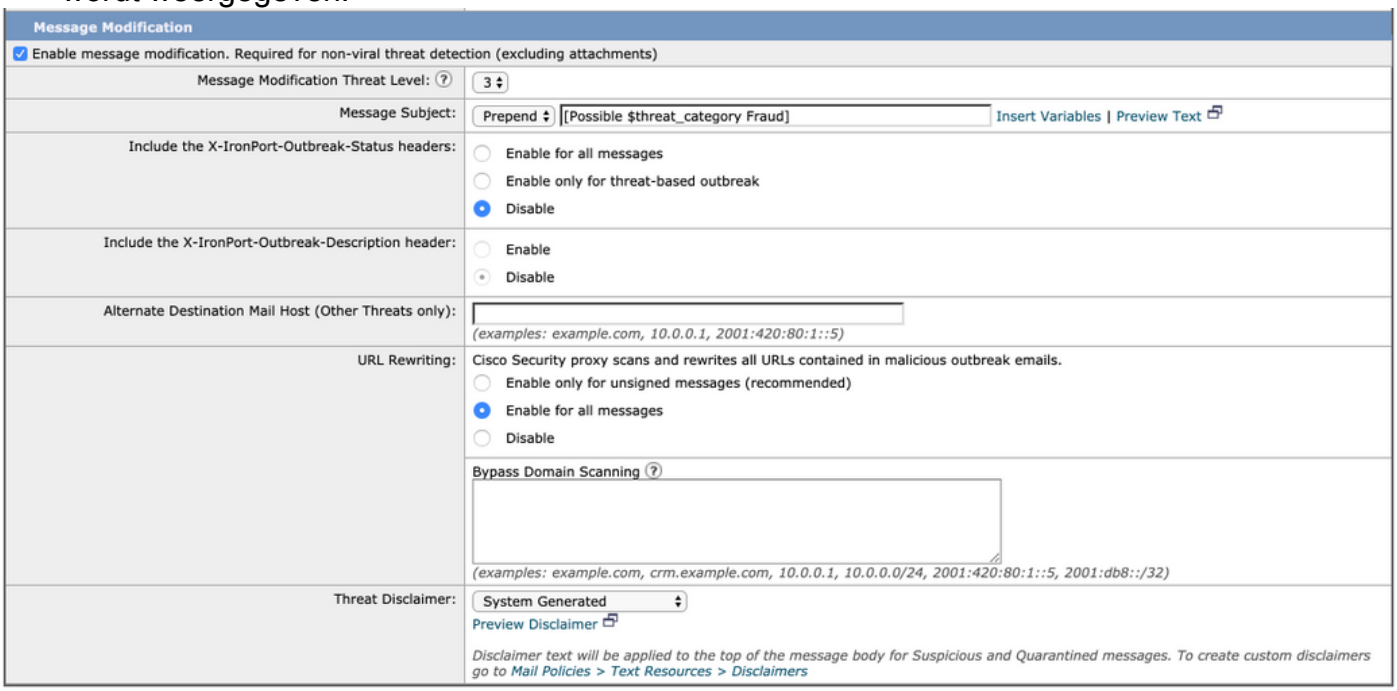
Filters eenmaal uiteinde heeft zijn ingesteld mondiaal , u kunnen nu deze optie toepassen op post beleid.

- 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 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:



- Klik op **Inzenden**en **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.