

Best Practices Guide voor inkomende en uitgaande contentfilters

Inhoud

[Inleiding](#)

[Overzicht van de stappen](#)

[STAP 1: DE NODIGE WOORDENBOEKEN IMPORTEREN](#)

[STAP 2: DE GECENTRALISEERDE KWANTINES MAKEN](#)

[STAP 3: DE INKOMENDE CONTENTFILTERS MAKEN](#)

[De inkomende contentfilters op het inkomende postbeleid toepassen](#)

[DKIM-verificatie voor eBay & Paypal en Spraf Email Protection voor uw domein](#)

[STAP 4: DE UITVOERINHOUD-FILTERS MAKEN](#)

[Samenvatting](#)

Inleiding

Met contentfilters kunt u de ingewikkelde details van een e-mail controleren en actie ondernemen (of geen actie) op de e-mail. Zodra het inkomende of uitgaande contentfilter is gemaakt, past u dit toe op een inkomende of uitgaande e-mailbeleid. Wanneer een e-mail overeenkomt met het contentfilter, kan het "Content Filters"-rapport over Cisco Email Security Appliance (ESA) en Security Management-applicatie (SMA) u alle e-mails tonen die overeenkomen met een contentfilter. Daarom is het, ook al wordt er geen actie ondernomen, een uitstekende manier om waardevolle informatie te verkrijgen over het type e-mails dat uw organisatie binnengaat en verlaat. Hiermee kunt u uw e-mailstroom "Patroon" zetten.

Aangezien er veel verschillende Content Filter "Voorwaarden" en "Handelingen" zijn, zal dit document u door een aantal zeer vaak voorkomende en aanbevolen inkomende en uitgaande contentfilters slepen.

Overzicht van de stappen

Stap 1: De benodigde woordenboeken importeren

Dit document biedt de stappen die u nodig hebt om bepaalde Best Practices Inkomend and Off Content Filters te implementeren. De contentfilters die we gaan maken zullen een paar woordenboeken referentie geven - dus moeten we die woordenboeken eerst importeren. De ESA scheppen met de woordenboeken en je hoeft ze alleen maar in de configuratie te importeren om ze in de contentfilters te laten zien die we zullen maken.

Stap 2: Gecentraliseerde gateways maken

Voor de meeste Content Filters maken we, zetten we de "Action" (Actie) in om de e-mail (of een kopie van de e-mail) in een speciale aangepaste (nieuwe) Quarantines te quarantaine, en daarom moeten we eerst die Quarantines op het SMA maken — omdat dit document ervan uitgaat dat u Gecentraliseerde PVO (Policy, Virus en Outbreak) Quarantines tussen het ESA en SMA hebt ingeschakeld.

Stap 3: Inkomende en uitgaande contentfilters maken en toepassen op beleid

Zodra we de woordenboeken hebben geïmporteerd en de Quarantines hebben gemaakt, zullen we de Inbound Content Filters maken en ze toepassen op het inkomende postbeleid. Daarna maken we de uitgaande contentfilters en passen we ze toe op het uitgaande postbeleid.

STAP 1: DE NODIGE WOORDENBOEKEN IMPORTEREN

Woordenboeken importeren waarnaar we in onze contentfilters verwijzen:

- Raadpleeg op het ESR-apparaat "**Mail-beleid > Woordenboeken**"
- Klik op de knop "**Woordenboek importeren**" aan de rechterkant van de pagina.

Winstgevendheid:

- Selecteer "**Importeren uit de configuratiemap in uw IronPort-apparaat**"
- Selecteer "**profanity.txt**" en klik op "**Volgende**".
- Naam: **Religieid**
- Klik op "**gehele woorden afstemmen**" (**ZEER BELANGRIJK**)
- De bepalingen wijzigen (nieuwe bepalingen toevoegen of ongevraagde bepalingen verwijderen)
- Klik op "**Inzenden**"

Seksuele inhoud:


- Selecteer "**Importeren uit de configuratiemap in uw IronPort-apparaat**"
- Selecteer "**sexueel_content.txt**" en klik op "**Volgende**".
- Naam: **SexualContent**
- Klik op "**gehele woorden afstemmen**" (**ZEER BELANGRIJK**)
- De bepalingen wijzigen (nieuwe bepalingen toevoegen of ongevraagde bepalingen verwijderen)
- Klik op "**Inzenden**"

Gepatenteerd:

- Selecteer "**Importeren uit de configuratiemap in uw IronPort-apparaat**"
- Selecteer de "**propriseed_content.txt**" en klik op "**Next**".
- Naam: **Gepatenteerd**
- Klik op "**gehele woorden afstemmen**" (**ZEER BELANGRIJK**)
- De bepalingen wijzigen (nieuwe bepalingen toevoegen of ongevraagde bepalingen verwijderen)
- Klik op "**Inzenden**"

STAP 2: DE GECENTRALISEERDE KWANTINES MAKEN

- Raadpleeg in het SMA "**Email Tab > Berichtlijn > PVO Quarantines**"
- Zo zou de Quarantines-tafel moeten zijn voordat we beginnen. Alle quarantaine's zijn standaard.

Quarantines						
Add Policy Quarantine...		Search Across Quarantines				
Quarantine Name	Type	Messages	Default Action	Last Message Quarantined On	Size	Delete
File Analysis	Advanced Malware Protection	0	Retain 1 hour then Release	--	0	
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release	--	0	
Policy	Centralized Policy	0	Retain 10 days then Delete	--	0	
Unclassified	Unclassified	0	Retain 30 days then Release	--	0	
Virus	Antivirus	0	Retain 30 days then Delete	--	0	

Available space for Policy, Virus & Outbreak quarantines is 33G.

- Klik op het "Beleidsquarantaine toevoegen..." knoop
- Maak de onderstaande Quarantines.
- Sommigen zullen door Inkomende Filters van de Inhoud worden gebruikt en sommige zullen door Uitgaande Filters van de Inhoud worden gebruikt. Je maakt ze op dezelfde manier.

PVO Quarantines - gebruikt door inkomende contentfilters

URL kwaadaardig inkomende:

Name: URL kwaadaardig binnenkomend

Bewaarperiode: 14 dagen

Standaardactie: Verwijderen

Vrij ruimte: inschakelen

URL-categorie inkomend:

Name: URL-categorie ingesloten

Bewaarperiode: 14 dagen

Standaardactie: Verwijderen

Vrij ruimte: inschakelen

Bankgegevens binnenkomend:

Name: Bankgegevens binnenkomend

Bewaarperiode: 14 dagen

Standaardactie: Verwijderen

Vrij ruimte: inschakelen

SSN-ingang:

Name: SSN-uitgang

Bewaarperiode: 14 dagen

Standaardactie: Verwijderen

Vrij ruimte: inschakelen

Ongeschikt binnenkomend:

Name: ongeschikt binnenkomend

Bewaarperiode: 14 dagen

Standaardactie: Verwijderen

Vrij ruimte: inschakelen

Vaste SFP-fout:

Name: SFP-harde fout

Bewaarperiode: 14 dagen

Standaardactie: Verwijderen

Vrij ruimte: inschakelen

SFP zachte fout:

Name: SPF zachte handgreep

Bewaarperiode: 14 dagen

Standaardactie: Verwijderen

Vrij ruimte: inschakelen

SpoofMail:

Name: SpoofMail

Bewaarperiode: 14 dagen

Standaardactie: Verwijderen

Vrij ruimte: inschakelen

Harde fout DKIM:

Name: DKIM harde fout

Bewaarperiode: 14 dagen

Standaardactie: Verwijderen

Vrij ruimte: inschakelen

Wachtwoord beveiligd.

Name: PWD beschermd binnenkomend

Bewaarperiode: 14 dagen

Standaardactie: Verwijderen

Vrij ruimte: inschakelen

PVO Quarantines - gebruikt door uitgaande contentfilters

Uitgaande bankgegevens:

Name: Uitgaande bankgegevens

Bewaarperiode: 14 dagen

Standaardactie: Verwijderen

Vrij ruimte: inschakelen

Uitgaand SSN:

Name: SSN-uitgang

Bewaarperiode: 14 dagen

Standaardactie: Verwijderen

Vrij ruimte: inschakelen

Onjuist uitgaande:

URL Malicious Outbound:

Name: URL kwaadaardig uitgaande

Bewaarperiode: 14 dagen

Standaardactie: Verwijderen

Vrij ruimte: inschakelen

Uitgaande URL-categorie:

Name: Uitgaande URL-categorie

Bewaarperiode: 14 dagen

Standaardactie: Verwijderen

Vrij ruimte: inschakelen

Wachtwoord beveiligd tegen Uitvoer:

Name: Onjuist uitgaande
Bewaarperiode: 14 dagen
Standaardactie: Verwijderen
Vrij ruimte: inschakelen

Name: PWD beschermd uitgaande
Bewaarperiode: 14 dagen
Standaardactie: Verwijderen
Vrij ruimte: inschakelen

Gepatenteerd uiteinde:

Name: Gepatenteerd uitgaande
Bewaarperiode: 14 dagen
Standaardactie: Verwijderen
Vrij ruimte: inschakelen

- Hier volgt hoe je PVO-tabel eruit moet zien als je alle PVO Quarantines creëert.

Quarantines						
Add Policy Quarantine...		Search Across Quarantines				
Quarantine Name	Type	Messages	Default Action	Last Message Quarantined On	Size	Delete
Bank Data Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Bank Data Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
DKIM Hard Fail	Centralized Policy	0	Retain 14 days then Delete	--	0	
File Analysis	Advanced Malware Protection	0	Retain 1 hour then Release	--	0	
Inappropriate Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Inappropriate Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release	--	0	
Policy	Centralized Policy	0	Retain 10 days then Delete	--	0	
Proprietary Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Pwd Protected Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Pwd Protected Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
SPF Hard Fail	Centralized Policy	0	Retain 14 days then Delete	--	0	
SPF Soft Fail	Centralized Policy	0	Retain 14 days then Delete	--	0	
SpoofMail	Centralized Policy	0	Retain 14 days then Delete	--	0	
SSN Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
SSN Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Unclassified	Unclassified	0	Retain 30 days then Release	--	0	
URL Category Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
URL Category Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
URL Malicious Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
URL Malicious Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Virus	Antivirus	0	Retain 30 days then Delete	--	0	

Available space for Policy, Virus & Outbreak quarantines is 33G.

STAP 3: DE INKOMENDE CONTENTFILTERS MAKEN

Nadat de woordenboeken zijn geïmporteerd en de PVO Quarantines zijn gemaakt, kunt u nu beginnen met het maken van de inkomende contentfilters:

- Navigeren in: **"Mail Policies > Inkomend contentfilters"**
- Hier is een tabel met inkomende contentfilters die u moet maken. Onder de tabel staat bijvoorbeeld een screenshot dat laat zien hoe u de eerste serie maakt.

Deze inkomende contentfilters maken

Name: **Bank_data**

Voeg twee voorwaarden toe:

Tekst of bijlage van het bericht:

Bevat slimme identificator: ABA-routingnummer

Bevat slimme identificator: Creditkaartnummer

Voeg één actie toe:

Quarantine:

Bericht naar quarantaine sturen: "Bank Data Inbound (gecentraliseerd)"
Dubbel bericht: Ingeschakeld
(Let erop dat de Toepassingsregel "Als een of meer voorwaarden overeenkomen" is)

Name: **SSN**

Eén voorwaarde toevoegen:

Tekst of bijlage van het bericht:

Bevat slimme identificator: Nummer van de sociale zekerheid (SSN)

Voeg één actie toe:

Quarantine:

Bericht naar quarantaine sturen: "SSN-inkomende (gecentraliseerd)"

Dubbel bericht: Ingeschakeld

Name: **ongeschikt**

Voeg twee voorwaarden toe:

Tekst of bijlage van het bericht:

Bevat woorden in woordenboek: winstgevendheid

Bevat woorden in woordenboek: Sexual_content

Voeg één actie toe:

Quarantine:

Bericht naar quarantaine sturen: "Ongeschikt binnenkomend (gecentraliseerd)"

Dubbel bericht: Ingeschakeld

Name: **URL_categorie**

Eén voorwaarde toevoegen:

URL-categorie:

Selecteer categorieën:

Volwassenen, drogen, filtervermijding, non-profit en Shareware, gokken,

Spelen, hacken, lingerie en zwempakken, niet-seksuele Nudity,

Geparkeerde domeinen, peer File Transfer, Pornografie

Voeg één actie toe:

Quarantine:

Bericht naar quarantaine sturen: "URL Category inkomende (gecentraliseerd)"

Dubbel bericht: Ingeschakeld

(Opmerking: Voor dit contentfilter dient u "Beveiligingservices"—> "URL-filtering" in te schakelen)

Name: **URL_kwaadaardig**

Eén voorwaarde toevoegen:

URL-reputatie

URL-reputatie is: Kwaadaardig (-10.0 tot -6.0)

Voeg één actie toe:

Quarantine:

Bericht naar quarantaine sturen: "URL Malicious Inbound (gecentraliseerd)"

Dubbel bericht: Uitgeschakeld (**** Quarantine het origineel ****)

Name: **Wachtwoord_beveiligd**

Eén voorwaarde toevoegen:

Aansluitbeveiliging: Een of meer bijlagen zijn beveiligd

Voeg één actie toe:

Quarantine:

Bericht naar quarantaine sturen: "PWD beveiligd tegen inkomende (gecentraliseerd)"

Dubbel bericht: Ingeschakeld

Name: **Grootte_10m**

Eén voorwaarde toevoegen:

Berichtgrootte is:

groter dan of gelijk aan: 10 M

Voeg één actie toe:

Berichtenlabel toevoegen:

Typ een term: OPNIEUW

(Opmerking: Er moet iets gebeuren, dus we "Vraag" de boodschap om geen operatie te laten zien. Het feit dat het filter van de inhoud "aangepast" was zal het in de rapportage mogelijk maken. Er hoeft geen "actie" te worden ondernomen om aan te tonen in de rapportage.)

Name: **SPF_hard_faal**

Eén voorwaarde toevoegen:

Controle van het SFP: "is" fout

Voeg één actie toe:

Quarantine:

Bericht naar quarantaine sturen: "VIDEO VRIJ FALEN (gecentraliseerd)"

Dubbel bericht: Ingeschakeld

(Opmerking: "is Fail" is een mislukking van de harde SPF en dit betekent dat de eigenaar van het domein je vertelt om alle e-mails die ontvangen zijn van verzenders die niet in hun SPF-record staan, te laten vallen. Aanvankelijk is het een goed idee om "Dubbele boodschap" te gebruiken en de fout een week of twee te bekijken voordat u het origineel in quarantaine zet (dit wil zeggen het dubbele bericht uitzetten).

Name: **SPF_Soft_Fail**

Eén voorwaarde toevoegen:

Controle van het SFP: "is" Software

Voeg één actie toe:

Quarantine:

Bericht naar quarantaine sturen: "SFP zachte handboeien (gecentraliseerd)"

Dubbel bericht: Ingeschakeld

Name: **DKIM_Hardfaal_Kopie**

Eén voorwaarde toevoegen:

DKIM-verificatie: "is" Hardfail

Voeg twee acties toe:

Kop toevoegen/bewerken:

Naam header: Betreft

Klik op "Aan de waarde van bestaande kop voorbereiden" en voer het volgende in: [Kopie - niet vrijgeven]"

Quarantine:

Bericht naar quarantaine sturen: "DKIM hard Fail (gecentraliseerd)"

Dubbel bericht: Ingeschakeld

(Opmerking: Laat eerst een kopie van het bericht in quarantaine plaatsen.)

Name: **DKIM_Hardfaal_Origineel**

Eén voorwaarde toevoegen:

DKIM-verificatie: "is" Hardfail

Voeg één actie toe:

Quarantine:

Bericht naar quarantaine sturen: "DKIM hard Fail (gecentraliseerd)"

Dubbel bericht: Uitgeschakeld

(Opmerking: We maken een andere inkomende Mail Policy row voor PayPal en eBay domeinen en gebruiken dit Content Filter voor domeinen waarvan we weten dat deze DKIM-verificatie moet doorgeven.)

Name: **Spoof_SPF_failover**

Voeg één voorwaarde toe maar het heeft zowel software als hard gecontroleerd:

Controle van het SFP: "is" Software en klik ook op "Fail"

(dus u hebt twee selectietekens waarop "Software failliet" en "Fail" is geklikt

Voeg één actie toe:

Quarantine:

Bericht naar quarantaine sturen: "SpoofMail (gecentraliseerd)"

Dubbel bericht: inschakelen

(Opmerking: We gebruiken dit Content Filter om actie te ondernemen voor binnenkomende e-mail en te doen alsof we vanuit je eigen domein verzenden — spoofing. Start met de actie die is ingesteld om een kopie in quarantaine te zetten en na een paar weken van het bekijken van de SpoofMail-quarantaine, kunt u uw SPF TXT DNS-record wijzigen om alle legitieme zenders toe te voegen en op een bepaald moment kunt u dit contentfilter in quarantaine zetten door het dubbele venster van het bericht uit te schakelen).

Dit is bijvoorbeeld hoe het filter van de Bank_Data Content zou moeten eruit zien voordat u inzendt.

Content Filter Settings	
Name:	Bank_Data
RL Filtering	Currently Used by Policies: Default Policy
Description:	
Order:	1 (of 7)

Conditions			
Add Condition...			Apply rule: If one or more conditions match
Order	Condition	Rule	Delete
1	Message Body or Attachment	body-contains("**aba", 1)	
2	Message Body or Attachment	body-contains("**credit", 1)	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	Quarantine	duplicate-quarantine("Bank Data Inbound")	

Nadat u alle inkomende contentfilters hebt gemaakt, zou de tabel er nu als volgt moeten uitzien:

Filters						
Add Filter...						
Order	Filter Name	Description	Rules	Policies	Duplicate	Delete
1	URLMalicious	Not in use				
2	URLCategory	Not in use				
3	SPFHardFail	Not in use				
4	Bank_Data	Not in use				
5	SSN	Not in use				
6	Inappropriate	Not in use				
7	URL_Category	Not in use				
8	URL_Malicious	Not in use				
9	Password_Protected	Not in use				
10	Size_10M	Not in use				
11	SPF_Hard_Fail	Not in use				
12	SPF_Soft_Fail	Not in use				
13	DKIM_Hardfail_Copy	Not in use				
14	DKIM_Hardfail_Original	Not in use				
15	Spoof_SPF_Failures	Not in use				

Edit Filter Order...

Omdat de functie "Beleid" is geselecteerd (u zult de hypertext van het beleid in het bovenste midden zien) toont de middelste kolom het Inkomend beleid van de Post waarop het Contentfilter is toegepast. Omdat we ze niet op een inkomend Mail-beleid hebben toegepast, wordt "Not in use" weergegeven.

De inkomende contentfilters op het inkomende postbeleid toepassen

- Navigeren in: **"postbeleid > Inkomend-postbeleid"**
- Klik op de tekst **"Uitgeschakeld"** in de cel Content Filters voor het **"Standaardbeleid"**.
- De keuzemenu instelling is ingesteld op **"Content Filters uitschakelen"**.
- Klik op de knop en stel deze in op **"Content Filters inschakelen"** en u wordt direct weergegeven met alle inkomende contentfilters die zijn gemaakt.
- Schakel alle filters in behalve de DKIM_Hardfail_Original en Spoof_SPF_Failures.
- **"Indiening"** en **"Commit"**.

DKIM-verificatie voor eBay & Paypal en Spraof Email Protection voor uw domein

Deze twee onderwerpen zullen contentfilters omvatten die DKIM Verificatie en SPF Verificatie gebruiken. Daarom moeten we er eerst voor zorgen dat zowel DKIM- als SPF-verificatie mogelijk is.

1. Inschakelen van DKIM- en SPF-verificatie binnen het beleid voor Mail Flow

- Navigeren in: **"Mail-beleid > Mail-Flow-beleid"**
- Schakel DKIM- en SPF-verificatie in binnen alle Mail Flow-beleid met "Connection Gedrag" van "Accept".
- Klik op de onderste hypertext **"Default Policy parameters"** en stel **"DKIM Verification"** in op **"On"** en **"SFP/SIDF Verification"** op **"On"**.
- Klik op **"Inzenden"** en **"Commit"**.
- U ziet nu de Mail Flow Policy-tabel. Bekijk de kolom genaamd **"Gedrag"** en bewerk elk beleid

- van de Mail Flow met het Gedrag dat is ingesteld op **"Relay"**
- Schakel **"Off"** zowel DKIM als SPF Verificatie in voor dat Mail Flow-beleid.
- Klik op **"Inzenden"** en **"Commit"**.

We willen niet dat de ESA de DKIM of de SPF verificatie uitvoert voor e-mail die in de ESA wordt ontvangen vanaf de uitgang van de Exchange Mail Server. In de meeste configuraties is het "RELAYED" Mail Flow Policy de enige rij met het gedrag van Relay.

2. Een nieuw instinctbeleid voor eBay en e-mail maken

Inkomend e-mail ontvangen van eBay en Paypal moet altijd de DKIM-verificatie doorgeven. We zullen daarom een ander Inkomend Mail Policy maken om het DKIM_Hardfail_Origineel Inkomen Content Filter te gebruiken voor een e-mail van die domeinen.

- Navigeren in: **"postbeleid > Inkomend-postbeleid"**
- Klik op de knop **"Beleid toevoegen"**.
- Voer de naam in: **"DKIM Hardfail Originator"**
- Klik op het **"Gebruiker toevoegen..."** -toets.

In het volgende configuratiescherm kunt u bepalen welke berichten met dit nieuwe Inkomend Mail-beleid overeenkomen. We willen alleen de criteria voor Sender definiëren (het linkergedeelte van het configuratiescherm).

- Klik **"Volgend senders"** radioknop en in het e-mailadressenbestand **"@ebay.com, @paypal.com"**

The screenshot shows a configuration window titled "Add User". It has three radio button options: "Any Sender", "Following Senders" (which is selected), and "Following Senders are Not". Below these options is a text input field labeled "Email Address:" containing the text "@ebay.com, @paypal.com". At the bottom of the field, there is a small note: "(e.g. user@example.com, user@, @example.com, @.example.com)".

- Klik op het **"Ok"** -toets onderaan.
- Klik op **"Verzenden"**.

3. Maak een nieuw inkomende Mail Flow-beleid voor uw domein (Spoof Protection)

Met de stappen in deze sectie kunt u actie ondernemen bij inkomende e-mail met een From-e-mailadres van uw eigen domein en een FSP-verificatie. Dit is uiteraard afhankelijk van het feit dat u uw SPF-tekstrecord in DNS al hebt gepubliceerd. Ga deze stappen naar als u geen SPF-bestandsindeling voor het tekstgebied hebt gemaakt of gepubliceerd.

- Navigeren in: **"postbeleid > Inkomend-postbeleid"**
- Klik op de knop **"Beleid toevoegen"**.
- Voer de naam in: **"Spoof_Protection"**
- Klik op het **"Gebruiker toevoegen..."** -toets.

In het volgende configuratiescherm kunt u bepalen welke berichten overeenkomen met deze nieuwe Beleidslijn Inkomend Mail. U wilt alleen de criteria voor de Zender definiëren (dit is het

linkergedeelte van het configuratiescherm).

- Klik op het "**Volgend senders**" radioknop en voer vervolgens uw domein in in het tekstvak "**E-mailadres:**". Voor mij is mijn domein "**@unc-hamiltons.com**"

Add User

Any Sender

Following Senders

Following Senders are Not

Email Address:

@unc-hamiltons.com

(e.g. user@example.com, user@, @example.com, @.example.com)

- Klik op "**Verzenden**".

U krijgt opnieuw de tabel Inkomend beleid per e-mail, maar nu hebt u een tweede nieuwe rij per e-mail boven het standaardbeleid.

- Klik op de hypertekst (**standaard gebruiken**) in de cel Content Filters voor de nieuwe rij.
- Draai het keuzemenu om "**Content Filters inschakelen (aangepaste instellingen)**".
- Controleer de "**Spoof_SPF_Failures**" ook of "**DKIM_Hardfail_Copy**" en "**DKIM_Hardfail_Original**" niet zijn gecontroleerd.
- Klik op "**Inzenden**" en "**Aankondigen**".

De tabel Inkomend Mail moet er nu als volgt uitzien:

Policies								
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
1	DKIM Hardfail Original	(use default)	(use default)	(use default)	(use default)	URLMalicious URLCategory SPFHardFail Bank_Data ...	(use default)	🗑️
2	Spoof_Protection	(use default)	(use default)	(use default)	(use default)	URLMalicious URLCategory SPFHardFail Bank_Data ...	(use default)	🗑️
	Default Policy	IronPort Intelligent Multi-Scan Positive: Quarantine Suspected: Quarantine	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Unscannable: Deliver Malware File: Drop Pending Analysis: Deliver	Disabled	URLMalicious URLCategory SPFHardFail Bank_Data ...	Retention Time: Virus: 1 day	

STAP 4: DE UITVOERINHOUD-FILTERS MAKEN

- Navigeren in: "**Mail Policies > OutDoorgaande contentfilters**"
- Hier is een tabel met uitgaande contentfilters die u moet maken.

Deze uitgaande contentfilters maken

Name: **Bank_data**

Voeg twee voorwaarden toe:

Tekst of bijlage van het bericht:

Bevat slimme identificator: ABA-routingnummer

Bevat slimme identificator: Creditkaartnummer

Voeg één actie toe:

Quarantine:

Bericht naar quarantaine sturen: "Uitgaande bankgegevens (gecentraliseerd)"

Dubbel bericht: Ingeschakeld

(Let erop dat de Toepassingsregel "Als een of meer voorwaarden overeenkomen" is)

Name: **SSN**

Eén voorwaarde toevoegen:

Tekst of bijlage van het bericht:

Bevat slimme identifier: Nummer van de sociale zekerheid (SSN)

Voeg één actie toe:

Quarantine:

Bericht naar quarantaine sturen: "SSN-uitgang (gecentraliseerd)"

Dubbel bericht: Ingeschakeld

Name: **ongeschikt**

Voeg twee voorwaarden toe:

Tekst of bijlage van het bericht:

Bevat woorden in woordenboek: winstgevendheid

Bevat woorden in woordenboek: Sexual_content

Voeg één actie toe:

Quarantine:

Bericht naar quarantaine sturen: "Ongeschikt uitgaande (gecentraliseerd)"

Dubbel bericht: Ingeschakeld

Name: **URL_categorie**

Eén voorwaarde toevoegen:

URL-categorie:

Selecteer categorieën:

Volwassenen, drogen, filtervermijding, non-profit en Shareware, gokken,

Spelen, hacken, lingerie en zwempakken, niet-seksuele Nudity,

Geparkeerde domeinen, peer File Transfer, Pornografie

Voeg één actie toe:

Quarantine:

Bericht naar quarantaine sturen: "URL Category Outbound (gecentraliseerd)"

Dubbel bericht: Ingeschakeld

Name: **URL_kwaadaardig**

Eén voorwaarde toevoegen:

URL-reputatie

URL-reputatie is: Kwaadaardig (-10.0 tot -6.0)

Voeg één actie toe:

Quarantine:

Bericht naar quarantaine sturen: "URL Malicious Outbound (gecentraliseerd)"

Dubbel bericht: Uitgeschakeld (**** Quarantine het origineel ****)

Name: **Wachtwoord_beveiligd**

Eén voorwaarde toevoegen:

Aansluitbeveiliging: Een of meer bijlagen zijn beveiligd

Voeg één actie toe:

Quarantine:

Bericht naar quarantaine sturen: "PWD beveiligd uitgaande (gecentraliseerd)"

Dubbel bericht: Ingeschakeld

Name: **Grootte_10m**

Eén voorwaarde toevoegen:

Berichtgrootte is:

groter dan of gelijk aan: 10 M

Voeg één actie toe:

Berichtenlabel toevoegen:

Typ een term: OPNIEUW

(Opmerking: Er moet iets gebeuren, dus we "Vraag" de boodschap om geen operatie te laten zien. Het feit dat het filter van de inhoud "aangepast" was zal het in de rapportage mogelijk maken. Er hoeft geen "actie" te worden ondernomen om aan te tonen in de rapportage.)

Name: **eigendom**

Eén voorwaarde toevoegen:

Tekst of bijlage van het bericht:

Bevat woorden in woordenboek: eigendom

Voeg één actie toe:

Quarantine:

Bericht naar quarantaine sturen: "Gepatenteerd (gecentraliseerd)"

Dubbel bericht: Ingeschakeld

Omdat de functie "Beleid" is geselecteerd (u zult de hypertext van het Beleid in het bovenste midden zien) toont de middenkolom het Uitgaande beleid van de Post waarop het Contentfilter is toegepast. Omdat we ze niet op een vertrekend Mail-beleid hebben toegepast, wordt "Not in use" weergegeven.

- Navigeren in: **"postbeleid > Uitgaand postbeleid"**
- Klik op de tekst **"Uitgeschakeld"** in de cel Inhoud Filters voor het Standaardbeleid.
- De keuzemenu -toets wordt ingesteld op **"Content Filters uitschakelen"**.
- Klik op de knop en stel deze in op **"Content Filters inschakelen"** en u wordt direct weergegeven met alle uitgaande contentfilters die zijn gemaakt.
- **"Alle filters inschakelen"**.
- **"Indienen"** en **"beloven"**.

Samenvatting

U hebt nu eerste beste praktijken voor inkomende en uitgaande contentfilters geïmplementeerd. De meeste (niet alle) contentfilters hebben de Quarantine Action (Quarantine Actie) gebruikt en zijn geselecteerd om de "Duplicate Message"-optie (Enable) te controleren - waarbij slechts een kopie van de originele e-mail wordt geplaatst en niet werd voorkomen dat de e-mail wordt afgeleverd. De bedoeling van deze Content Filters is om u toe te staan om informatie te verzamelen over het soort e-mails dat naar binnen en naar buiten naar uw bedrijf gaat.

Niettemin is het, nadat de Content Filters zijn rapport hebben uitgevoerd en de e-mailexemplaren hebben bekeken die in quarantaine zijn opgeslagen, wellicht verstandig om de optie "Duplicate Message" uit te schakelen, zodat de oorspronkelijke e-mail in de quarantaine wordt geplaatst in plaats van een kopie/duplicaat.