# Les pratiques recommandées guident pour les filtres satisfaits entrants et sortants

## Contenu



## Introduction

Les filtres satisfaits te permettent pour examiner les détails complexes d'un email et pour n'agir (ou aucune mesure) sur l'email. Une fois que le filtre satisfait entrant ou sortant est créé, vous l'appliquez à une stratégie entrante ou de mail sortant. Quand en envoient à des correspondances le filtre satisfait, « les filtres satisfaits » rendent compte de l'appliance de sécurité du courrier électronique de Cisco (ESA) et l'appliance de Gestion de la sécurité (SMA) pourra t'afficher tous les emails qui ont apparié n'importe quel filtre satisfait. Par conséquent, même si aucune mesure n'est prise, c'est un excellent moyen d'obtenir des données de valeur au sujet du type d'emails écrivant et partant de votre organisation - en te permettant « pour modeler » votre email circulez.

Pendant qu'il y a beaucoup le filtre satisfait différent « conditionne » et les « actions », ce document feront un pas vous par quelques filtres satisfaits entrants et sortants très communs et recommandés.

## Vue d'ensemble des étapes

#### Étape 1 : Importez les dictionnaires nécessaires

Ce document fournira les étapes nécessaires pour que vous implémentiez quelques pratiques recommandées entrantes et filtres satisfaits sortants. Les filtres satisfaits que nous allons créer mettront en référence quelques dictionnaires - ainsi nous devrons importer ces dictionnaires d'abord. Les bateaux ESA avec les dictionnaires et vous doivent simplement les importer dans la configuration afin de les mettre en référence dans les filtres satisfaits que nous créerons.

#### Étape 2 : Créez les quarantaines centralisées

Pour la plupart des filtres satisfaits, nous créerons, nous placerons la « action » de mettre en quarantaine l'email (ou une copie de l'email) dans de nouvelles) quarantaines indiquées spécifiées d'une coutume (— et donc, nous devons créer d'abord ces quarantaines sur le SMA — pendant que ce document suppose que vous avez activé PVO centralisé (stratégie, virus, et épidémie) met

en quarantaine entre l'ESA et le SMA.

**Étape 3 : Créez les filtres satisfaits entrants et sortants et appliquez-vous aux stratégies**

Une fois que nous faisons importer les dictionnaires et les quarantaines être créées, nous créerons les filtres satisfaits d'arrivée et les appliquerons aux stratégies de messagerie entrante et puis créerons les filtres satisfaits sortants et les appliquerons aux stratégies de mail sortant.

## ÉTAPE 1 : IMPORTER LES DICTIONNAIRES NÉCESSAIRES

Important les dictionnaires que nous mettrons en référence dans des nos filtres satisfaits :

- Sur l'appliance ESA, naviguez **« pour envoyer par mail des stratégies > des dictionnaires »**
- Cliquez sur le bouton « de **dictionnaire d'importation** » du côté droit de la page.

**Blasphème :**

- « **Importation** choisie **à partir du répertoire de la configuration sur votre appliance d'IronPort** »
- Sélectionnez « **profanity.txt** » et cliquez sur « **ensuite** ».
- *Name :* **Blasphème**
- Cliquez sur les « **mots entiers de correspondance** » (TRÈS IMPORTANTS)
- Modifiez les termes (ajoutez les nouveaux termes ou retirez les termes non désirés)
- Le clic « **soumettent »**

**Contenu sexuel :**

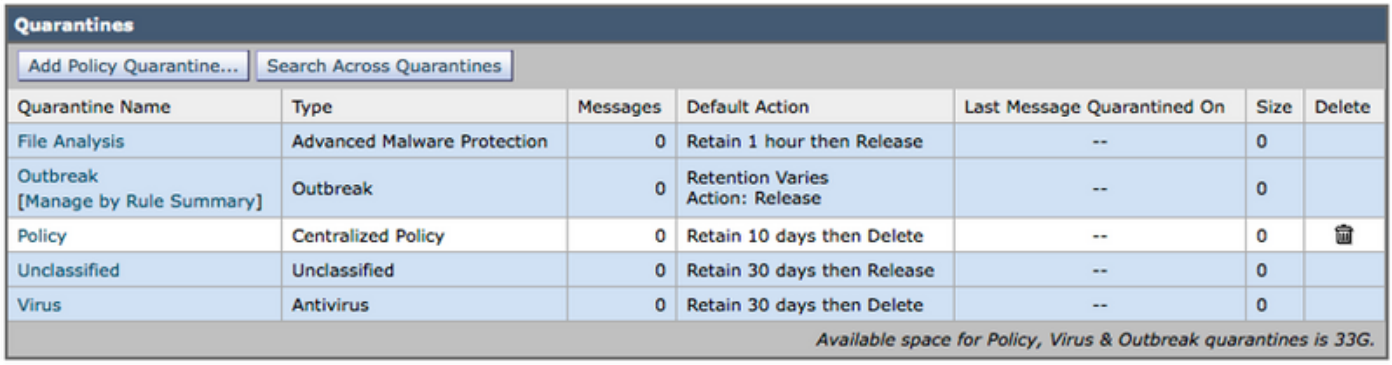
- « **Importation** choisie **à partir du répertoire de la configuration sur votre appliance d'IronPort** »
- Sélectionnez « **sexual_content.txt** » et cliquez sur « **ensuite** ».
- *Name :* **SexualContent**
- Cliquez sur les « **mots entiers de correspondance** » (TRÈS IMPORTANTS)
- Modifiez les termes (ajoutez les nouveaux termes ou retirez les termes non désirés)
- Le clic « **soumettent »**

**Classe des propriétaires :**

- « **Importation** choisie **à partir du répertoire de la configuration sur votre appliance d'IronPort** »
- Sélectionnez « **proprietary_content.txt** » et cliquez sur « **ensuite** ».
- *Name :* **De propriété industrielle**
- Cliquez sur les « **mots entiers de correspondance** » (TRÈS IMPORTANTS)
- Modifiez les termes (ajoutez les nouveaux termes ou retirez les termes non désirés)
- Le clic **« soumettent »**

## ÉTAPE 2 : CRÉATION DES QUARANTAINES CENTRALISÉES

- Sur le SMA, naviguez **« pour envoyer la quarantaine d'onglet > de message > le PVO met en quarantaine »**
- C'est ce qui ressembler à la table de quarantaines devrait avant que nous commencions. Toutes les quarantaines sont par défaut.




- Cliquez sur *« **ajoutent la quarantaine de stratégie…** »* bouton
- Créez les quarantaines ci-dessous.
- Certains seront utilisés par les filtres satisfaits entrants et les autres seront utilisés par les filtres satisfaits sortants. Vous les créez de la même manière.

## Quarantaines PVO - utilisées par les filtres satisfaits entrants

**D'arrivée malveillant URL :**
*Name :* D'arrivée malveillant URL
Période de validité : 14 jours
Action par défaut : Effacement
Libérez l'espace : Enable

**Catégorie URL d'arrivée :**
*Name :* Catégorie URL d'arrivée
Période de validité : 14 jours
Action par défaut : Effacement
Libérez l'espace : Enable

**Données de banque d'arrivée :**
*Name :* Données de banque d'arrivée
Période de validité : 14 jours
Action par défaut : Effacement
Libérez l'espace : Enable

**SSN d'arrivée :**
*Name :* SSN d'arrivée
Période de validité : 14 jours
Action par défaut : Effacement
Libérez l'espace : Enable

**D'arrivée inadéquat :**
*Name :* D'arrivée inadéquat
Période de validité : 14 jours
Action par défaut : Effacement
Libérez l'espace : Enable

**Échouer dur SPF :**
*Name :* Échouer dur SPF
Période de validité : 14 jours
Action par défaut : Effacement
Libérez l'espace : Enable

**Échouer doux SPF :**
*Name :* Échouer doux SPF
Période de validité : 14 jours
Action par défaut : Effacement
Libérez l'espace : Enable

**SpoofMail :**
*Name :* SpoofMail
Période de validité : 14 jours
Action par défaut : Effacement
Libérez l'espace : Enable

**Échouer dur DKIM :**
*Name :* Échouer dur DKIM
Période de validité : 14 jours
Action par défaut : Effacement
Libérez l'espace : Enable

**D'arrivée protégé par mot de passe :**
*Name :* D'arrivée protégé par pwd
Période de validité : 14 jours
Action par défaut : Effacement
Libérez l'espace : Enable

## Quarantaines PVO - utilisées par les filtres satisfaits sortants

**Données de banque sortantes :**
*Name :* Données de banque sortantes
Période de validité : 14 jours
Action par défaut : Effacement
Libérez l'espace : Enable

**SSN sortant :**
*Name :* SSN sortant
Période de validité : 14 jours
Action par défaut : Effacement
Libérez l'espace : Enable

**Sortant inadéquat :**

**Sortant malveillant URL :**
*Name :* Sortant malveillant URL
Période de validité : 14 jours
Action par défaut : Effacement
Libérez l'espace : Enable

**Catégorie URL sortante :**
*Name :* Catégorie URL sortante
Période de validité : 14 jours
Action par défaut : Effacement
Libérez l'espace : Enable

**Sortant protégé par mot de passe :**

*Name :* Sortant inadéquat
Période de validité : 14 jours
Action par défaut : Effacement
Libérez l'espace : Enable

*Name :* Sortant protégé par pwd
Période de validité : 14 jours
Action par défaut : Effacement
Libérez l'espace : Enable

**Sortant de propriété industrielle :**
*Name :* Sortant de propriété industrielle
Période de validité : 14 jours
Action par défaut : Effacement
Libérez l'espace : Enable

- Voici comment votre table PVO devrait s'occuper de créer toutes les quarantaines PVO.

**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.*

## ÉTAPE 3 : CRÉATION DES FILTRES SATISFAITS ENTRANTS

Une fois que les dictionnaires ont été importés et les quarantaines PVO ont été créées, vous pouvez maintenant commencer créer les filtres satisfaits entrants :

- Naviguez vers : **« Stratégies de messagerie > filtres satisfaits entrants »**
- Voici une table de satisfait entrant vous filtre devrait créer. Par exemple les buts, au-dessous de la table est un tir d'écran exemplifiant comment créer le premier.

**Créez ces filtres satisfaits entrants**

*Name :* **Bank_Data**
Ajoutez deux conditions :
Corps du message ou connexion :
Contient l'identifiant intelligent : Nombre de routage aba
Contient l'identifiant intelligent : Numéro de carte de crédit
Ajoutez une action :
Quarantaine :

L'envoyez message pour mettre en quarantaine : « Données de banque d'arrivée (centralisé) »
Message en double : Activée
(Notez la règle d'application devrait être « si correspondance d'un ou plusieurs conditions ")

*Name :* **SSN**
Ajoutez une condition :
Corps du message ou connexion :
Contient l'identifiant intelligent : Numéro de sécurité sociale (SSN)
Ajoutez une action :
Quarantaine :
L'envoyez message pour mettre en quarantaine : « SSN d'arrivée (centralisé) »
Message en double : Activée
*Name :* **Inadéquat**
Ajoutez deux conditions :
Corps du message ou connexion :
Contient le terme en dictionnaire : Blasphème
Contient le terme en dictionnaire : Sexual_Content
Ajoutez une action :
Quarantaine :
L'envoyez message pour mettre en quarantaine : « D'arrivée inadéquats (centralisé) »
Message en double : Activée
*Name :* **URL_Category**
Ajoutez une condition :
Catégorie URL :
Catégories choisies :
Adulte, datation, manière d'éviter de filtre, freeware et shareware, jouant,
Jeux, entailler, lingerie et maillots de bain, nudité Non-sexuelle,
Domaines garés, transfert de fichiers de pair, pornographie
Ajoutez une action :
Quarantaine :
L'envoyez message pour mettre en quarantaine : « Catégorie URL d'arrivée (centralisé) »
Message en double : Activée
(Note : Ce filtre satisfait exige que vous activez des « Services de sécurité » — > « Filtrage URL ")
*Name :* **URL_Malicious**
Ajoutez une condition :
Réputation URL :
La réputation URL est : Malveillant (-10.0 à -6.0)
Ajoutez une action :
Quarantaine :
L'envoyez message pour mettre en quarantaine : « D'arrivée malveillants URL (centralisé) »
Message en double : Handicapé (quarantaine de **** le **** d'origine)
*Name :* **Password_Protected**
Ajoutez une condition :
Protection de connexion : Un ou plusieurs connexions sont protégées
Ajoutez une action :
Quarantaine :
L'envoyez message pour mettre en quarantaine : « D'arrivée protégés par pwd

(centralisé) »
Message en double : Activée

*Name :* **Size_10M**
Ajoutez une condition :
La taille de message est :
Supérieur ou égal à : 10m
Ajoutez une action :
Ajoutez la balise de message :
Écrivez un terme : NOOP
(Note : Il doit y avoir une certaine action tellement ici que nous « étiquetons » le message pour ne représenter aucune exécution prise. Le fait que le filtre satisfait « a été apparié » lui permettra pour apparaître dans l'enregistrement. Non « action » doit être pris pour qu'elle affiche dans l'enregistrement.)
*Name :* **SPF_Hard_Fail**
Ajoutez une condition :
Vérification SPF : « est » l'échouer
Ajoutez une action :
Quarantaine :
L'envoyez message pour mettre en quarantaine : « Échouer dur SPF (centralisé) »
Message en double : Activée
(Note : « est l'échouer » est une panne dure SPF et il signifie que le propriétaire du domaine vous dit de relâcher tous les emails reçus des expéditeurs qui ne sont pas répertoriés dans leur enregistrement SPF. Au commencement, c'est une bonne idée d'utiliser « le message en double » et de passer en revue les pannes pendant une semaine ou deux avant de mettre en quarantaine l'original (c.-à-d. arrêtant le message en double).
*Name :* **SPF_Soft_Fail**
Ajoutez une condition :
Vérification SPF : « est » Softfail
Ajoutez une action :
Quarantaine :
L'envoyez message pour mettre en quarantaine : « Échouer doux SPF (centralisé) »
Message en double : Activée
*Name :* **DKIM_Hardfail_Copy**
Ajoutez une condition :
Authentification DKIM : « est » l'incident permanent
Ajoutez deux actions :
En-tête d'Add/Edit :
Nom d'en-tête : Sujet
Cliquez sur « ajoutent à la valeur de l'en-tête existante » et entrent au début : [Copie - Ne font pas la release] »
Quarantaine :
L'envoyez message pour mettre en quarantaine : « Échouer dur DKIM (centralisé) »
Message en double : Activée
(Note : Mettez en quarantaine une copie du message au commencement.)
*Name :* **DKIM_Hardfail_Original**
Ajoutez une condition :
Authentification DKIM : « est » l'incident permanent
Ajoutez une action :
Quarantaine :
L'envoyez message pour mettre en quarantaine : « Échouer dur DKIM (centralisé) »

Message en double : Désactivée

(Note : Nous créerons une autre ligne de stratégie de messagerie entrante pour Paypal et des domaines d'eBay et utiliserons ce filtre satisfait pour les domaines que nous connaissons devrions passer la vérification DKIM.)

*Name :* **Spoof_SPF_Failures**

Ajoutez une condition mais elle fait vérifier Softfail et incident permanent :

Vérification SPF : « est » Softfail et clique sur également en fonction le « échouer »

(ainsi vous avez « Softfail » cliqué sur deux par cases à cocher et « échouez »

Ajoutez une action :

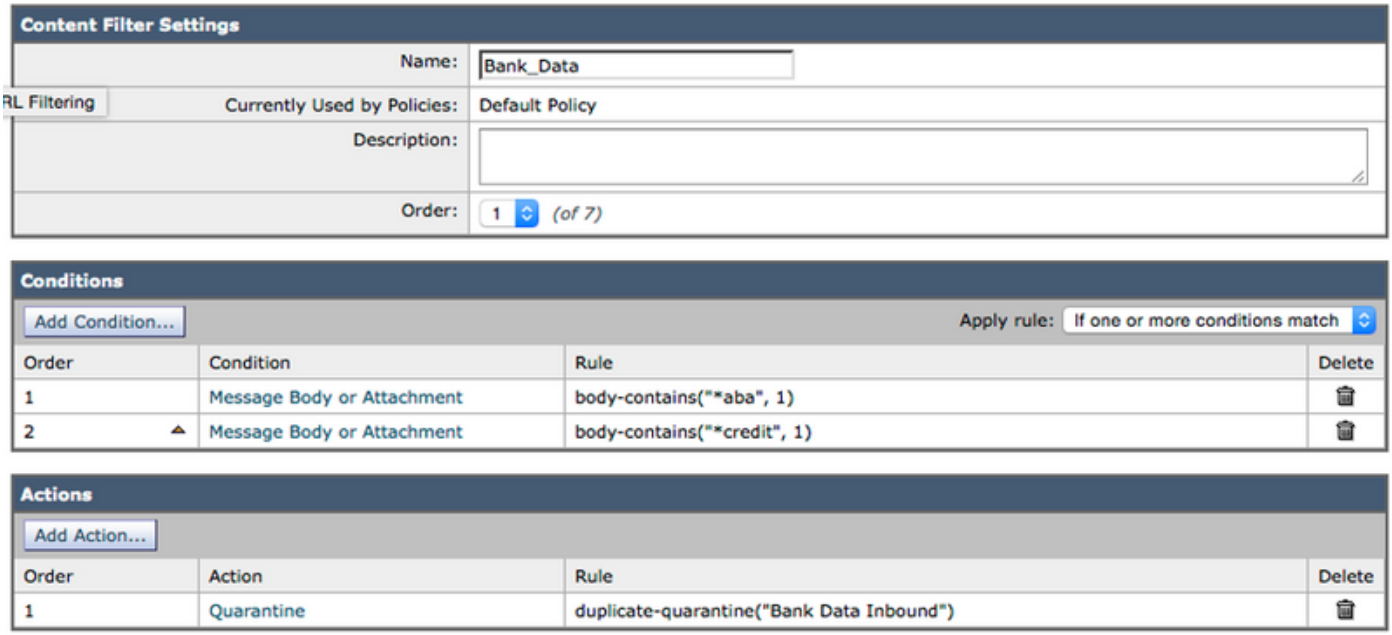
Quarantaine :

L'envoyez message pour mettre en quarantaine : « SpoofMail (centralisé) »

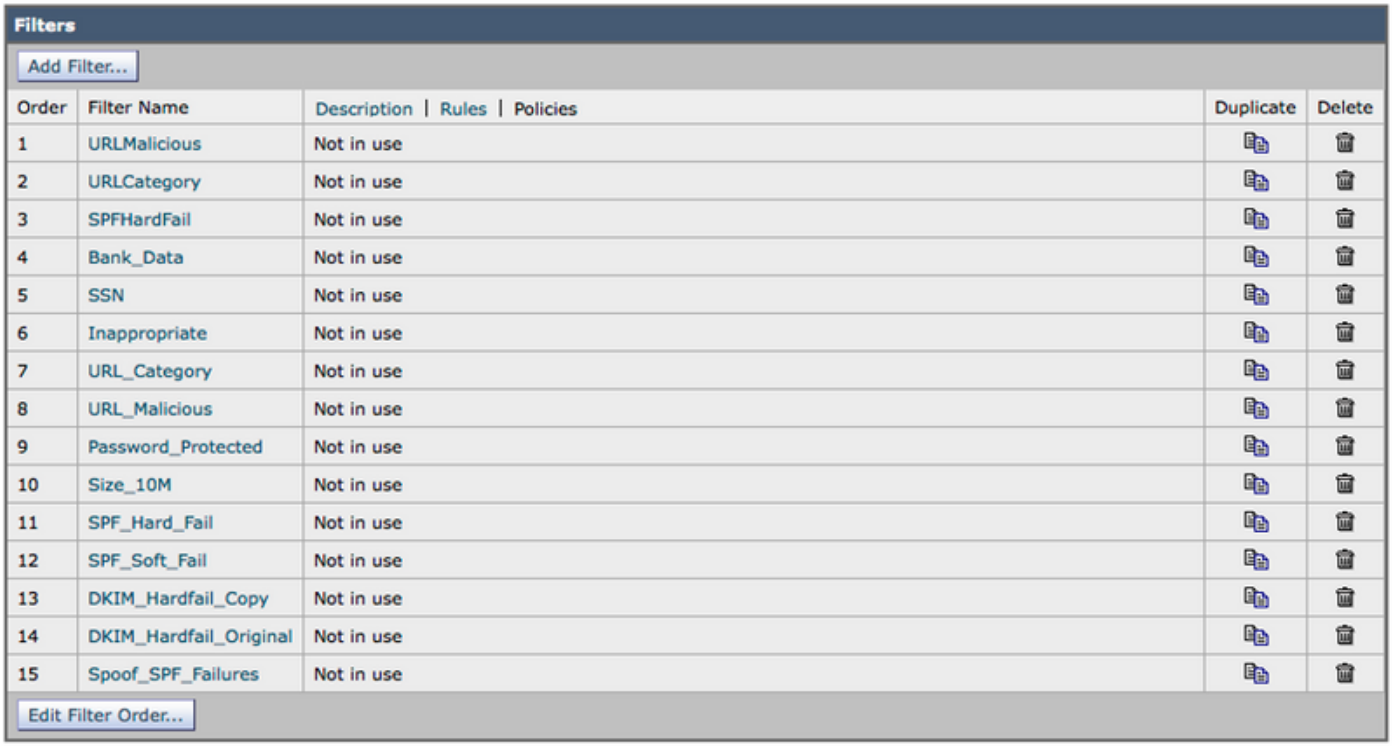
Message en double : Enable

(Note : Nous utiliserons ce filtre satisfait pour agir pour l'email entrant feignant pour envoyer de votre propre domaine — mystification. Début avec le positionnement d'action pour mettre en quarantaine une copie et après que quelques semaines de passer en revue la quarantaine de SpoofMail, vous puissiez modifier votre enregistrement DNS SPF TXT pour ajouter tous les expéditeurs légitimes et à un certain point, vous pouvez changer ce filtre satisfait pour mettre en quarantaine l'original en désactivant la case à cocher en double de message.)

Comme exemple, c'est ce qui ressembler au filtre de contenu de Bank_Data devrait avant que vous soumettiez.




Après création de tous les filtres satisfaits entrants, la table devrait maintenant ressembler à ceci :



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...

Puisque la fonction de « stratégies » est sélectionnée (vous verrez l'hypertexte de stratégies au milieu supérieur) que la colonne moyenne affiche que les stratégies de messagerie entrante le filtre satisfait a été appliquées à. Puisque nous ne les avons appliqués à aucune stratégie de messagerie entrante, le « non utilisable » est affiché.

## Appliquez les filtres satisfaits entrants aux stratégies de messagerie entrante

- Naviguez vers : **« Stratégies de messagerie > stratégies de messagerie entrante »**
- Cliquez sur en fonction **« a désactivé » le** texte dans la cellule de filtres de contenu pour la **« stratégie par défaut »**.
- Le bouton de menu déroulant est placé **« pour désactiver les filtres satisfaits »**.
- Cliquez sur le bouton et placez **« pour activer les filtres satisfaits »** et vous serez immédiatement présenté avec tous les filtres satisfaits entrants qui ont été créés.
- Activez tous les filtres excepté le DKIM_Hardfail_Original, et Spoof_SPF_Failures.
- **« Soumettez »** et « **validation »**.

## La vérification DKIM pour eBay et le Paypal et charrient la protection de messagerie pour votre domaine

Ces deux thèmes impliqueront les filtres satisfaits qui utilisent la vérification DKIM et la vérification SPF. Par conséquent, nous devons d'abord nous assurer que la vérification DKIM et SPF sont activées.

1. *Enable DKIM et vérification SPF dans des stratégies de flux de courrier*

- Naviguez vers : **« Stratégies de messagerie > stratégies de flux de courrier »**
- Activez la vérification DKIM et SPF dans toutes les stratégies de flux de courrier faites « recevoir » le « comportement de connexion dont ».
- Cliquez sur en fonction l'hypertexte inférieur **« paramètres de stratégie par défaut »** et placez la **« vérification DKIM » vérification "ON"** et à la **« SFP/SIDF » à "ON"**.

- Le clic **« soumettent »** et **« validation »**.
- Vous voyez maintenant la table de stratégies de flux de courrier. Regardez la colonne nommée **« comportement »** et éditez n'importe quelle stratégie de flux de courrier avec le positionnement de comportement **« pour transmettre par relais »**
- Tournez **"OFF"** vérification DKIM et SPF pour ces stratégies de flux de courrier.
- Le clic **« soumettent »** et **« validation »**.

Nous ne voulons pas que l'ESA exécute la vérification DKIM ou SPF pour l'email reçu dans l'ESA de votre se diriger de serveur de messagerie d'échange sortant. Dans la plupart des configurations, la stratégie « TRANSMISE PAR RELAIS » de flux de courrier est la seule ligne avec le comportement du relais.

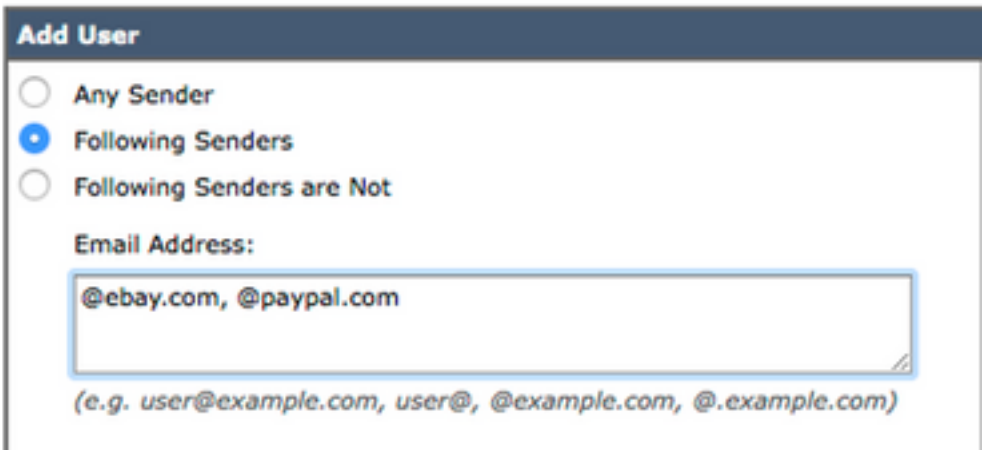
2. *Créez une nouvelle stratégie entrante de flux de courrier pour eBay et Paypal*

L'email d'arrivée reçu d'eBay et le Paypal devraient toujours passer la vérification DKIM. Nous créerons, donc, une autre stratégie de messagerie entrante pour utiliser le filtre satisfait entrant de DKIM_Hardfail_Original pour un email de ces domaines.

- Naviguez vers : **« Stratégies de messagerie > stratégies de messagerie entrante »**
- Cliquez sur le bouton **« ajoutent stratégie »**.
- Écrivez le nom : **« Original d'incident permanent DKIM »**
- Cliquez sur **« ajoutent l'utilisateur… »** bouton.

Le prochain panneau de configuration vous permet de définir quels messages apparieront cette nouvelle stratégie de messagerie entrante. Nous voulons seulement définir les critères pour l'expéditeur (la partie gauche du panneau de configuration).

- La case d'option **« d'expéditeurs suivants » de** clic et dans la table d'adresses e-mail écrivent **« @ ebay.com, @ paypal.com »**




- Cliquez sur le bouton **« correct » au** bas.
- Le clic **« soumettent »**.

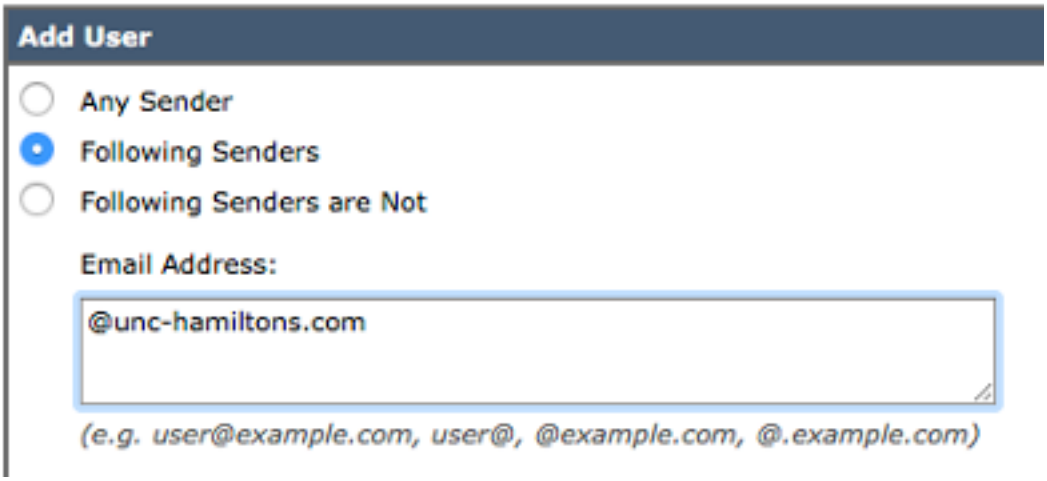
*3. Créez une nouvelle stratégie entrante de flux de courrier pour votre domaine (charriez la protection)*

Les étapes dans cette section te permettront pour agir sur l'email entrant qui a a de l'adresse e-mail de votre propre domaine et qui sont vérification manquante SPF. Naturellement, ceci se fonde sur vous ayant déjà édité votre enregistrement des textes SPF dans des DN. Ignorez ces étapes si vous n'avez pas créé/éditiez un enregistrement de ressource en textes SPF pour votre domaine.

- Naviguez vers : **« Stratégies de messagerie > stratégies de messagerie entrante »**
- Cliquez sur le bouton **« ajoutent stratégie »**.
- Écrivez le nom : **« Spoof_Protection »**
- Cliquez sur **« ajoutent l'utilisateur… »** bouton.

Le prochain panneau de configuration vous permet de définir quels messages apparieront cette nouvelle ligne de stratégie de messagerie entrante. Vous voulez seulement définir les critères pour l'expéditeur (qui est la partie gauche du panneau de configuration).

- Cliquez sur **« les expéditeurs suivants »** case d'option et puis entrez dans votre domaine dans la **« adresse e-mail : »** zone de texte. Pour moi, mon domaine est **« @unc-hamiltons.com »**




- Le clic **« soumettent »**.

Vous êtes présenté avec la table de stratégies de messagerie entrante de nouveau mais maintenant vous avez une deuxième nouvelle ligne de stratégie de messagerie au-dessus de la stratégie par défaut.

- Cliquez sur l'hypertexte **(de par défaut d'utilisation)** dans la cellule de filtres de contenu pour la nouvelle ligne.
- Inversez le menu déroulant **« pour activer les filtres satisfaits (configurations personnalisées) »**.
- Vérifiez le **« Spoof_SPF_Failures »** s'assurent également que « **DKIM_Hardfail_Copy »** et **« DKIM_Hardfail_Original »** ne sont pas vérifiés.
- Le clic **« soumettent »** et **« commettez les modifications »**.

La table de stratégies de messagerie entrante devrait maintenant ressembler à ceci :

**Policies**

Add Policy...

| 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<br>URLCategory<br>SPFHardFail<br>Bank_Data<br>... | (use default) | 🗑 |
| 2 | Spoof_Protection | (use default) | (use default) | (use default) | (use default) | URLMalicious<br>URLCategory<br>SPFHardFail<br>Bank_Data<br>... | (use default) | 🗑 |
| | Default Policy | IronPort Intelligent Multi-Scan<br>Positive: Quarantine<br>Suspected: Quarantine | Sophos<br>Encrypted: Deliver<br>Unscannable: Deliver<br>Virus Positive: Drop | File Reputation<br>Unscannable: Deliver<br>Malware File: Drop<br>Pending Analysis: Deliver | Disabled | URLMalicious<br>URLCategory<br>SPFHardFail<br>Bank_Data<br>... | Retention Time:<br>Virus: 1 day | |

## ÉTAPE 4 : CRÉATION DES FILTRES SATISFAITS SORTANTS

- Naviguez vers : **« Stratégies de messagerie > filtres satisfaits sortants »**
- Voici une table de satisfait sortant vous filtre devrait créer.

## Créez ces filtres satisfaits sortants

*Name :* **Bank_Data**
Ajoutez deux conditions :
  Corps du message ou connexion :
    Contient l'identifiant intelligent : Nombre de routage aba
    Contient l'identifiant intelligent : Numéro de carte de crédit
Ajoutez une action :
  Quarantaine :
    L'envoyez message pour mettre en quarantaine : « Données de banque sortantes (centralisé) »
    Message en double : Activée
(Notez la règle d'application devrait être « si correspondance d'un ou plusieurs conditions ")
*Name :* **SSN**
Ajoutez une condition :
  Corps du message ou connexion :
    Contient l'identifiant intelligent : Numéro de sécurité sociale (SSN)
Ajoutez une action :
  Quarantaine :
    L'envoyez message pour mettre en quarantaine : « SSN sortants (centralisé) »
    Message en double :  Activée
*Name :* **Inadéquat**
Ajoutez deux conditions :
  Corps du message ou connexion :
    Contient le terme en dictionnaire : Blasphème
    Contient le terme en dictionnaire : Sexual_Content
Ajoutez une action :
  Quarantaine :
    L'envoyez message pour mettre en quarantaine : « Sortant inadéquat (centralisé) »
    Message en double : Activée
*Name :* **URL_Category**
Ajoutez une condition :
  Catégorie URL :
    Catégories choisies :
      Adulte, datation, manière d'éviter de filtre, freeware et shareware, jouant,
      Jeux, entailler, lingerie et maillots de bain, nudité Non-sexuelle,
      Domaines garés, transfert de fichiers de pair, pornographie
Ajoutez une action :
  Quarantaine :
    L'envoyez message pour mettre en quarantaine : « Catégorie URL sortante (centralisé) »
    Message en double : Activée
*Name :* **URL_Malicious**
Ajoutez une condition :
  Réputation URL :
    La réputation URL est : Malveillant (-10.0 à -6.0)
Ajoutez une action :
  Quarantaine :
    L'envoyez message pour mettre en quarantaine : « Sortant malveillant URL (centralisé) »
    Message en double : Handicapé (quarantaine de **** le **** d'origine)
*Name :* **Password_Protected**
Ajoutez une condition :
  Protection de connexion : Un ou plusieurs connexions sont protégées

Ajoutez une action :
Quarantaine :
L'envoyez message pour mettre en quarantaine : « Sortant protégé par pwd (centralisé) »
Message en double : Activée
*Name :* **Size_10M**
Ajoutez une condition :
La taille de message est :
Supérieur ou égal à : 10m
Ajoutez une action :
Ajoutez la balise de message :
Écrivez un terme : NOOP
(Note : Il doit y avoir une certaine action tellement ici que nous « étiquetons » le message pour ne représenter aucune exécution prise. Le fait que le filtre satisfait « a été apparié » lui permettra pour apparaître dans l'enregistrement. Non « action » doit être pris pour qu'elle affiche dans l'enregistrement.)
*Name :* **De propriété industrielle**
Ajoutez une condition :
Corps du message ou connexion :
Contient le terme en dictionnaire : De propriété industrielle
Ajoutez une action :
Quarantaine :
L'envoyez message pour mettre en quarantaine : « Classe des propriétaires (centralisée) »
Message en double : Activée

Puisque la fonction de « stratégies » est sélectionnée (vous verrez l'hypertexte de stratégies au milieu supérieur) que la colonne moyenne affiche que les stratégies de mail sortant le filtre satisfait a été appliquées à. Puisque nous ne les avons appliqués à aucune stratégie de mail sortant, le « non utilisable » est affiché.

- Naviguez vers : **« Stratégies de messagerie > stratégies de mail sortant »**
- Cliquez sur en fonction **« a désactivé » le** texte dans la cellule de filtres de contenu pour la stratégie par défaut.
- Le bouton de menu déroulant est placé « **pour désactiver les filtres satisfaits** ».
- Cliquez sur le bouton et placez **« pour activer les filtres satisfaits »** et vous serez immédiatement présenté avec tous les filtres satisfaits sortants qui ont été créés.
- **« Activez »** tous les filtres.
- **« Soumettez »** et **« validation »**.

# Résumé

Vous avez maintenant mis en application des pratiques recommandées initiales pour les filtres satisfaits entrants et sortants. La plupart des filtres (de non tout le) contenu ont utilisé l'action de quarantaine et choisis pour vérifier (enable) l'option « de message en double » - qui place simplement une copie de l'email d'origine et n'a pas empêché l'email d'être livrée. L'intention de ces filtres satisfaits est de te permettre pour recueillir des informations au sujet des types d'emails circulant d'arrivée et sortants à votre société.

Ayant a dit que, après s'être exécuté les filtres satisfaits signalent et le regard au-dessus des copies d'email enregistrées dans les quarantaines, il peut être prudent pour décocher l'option de case à cocher « de message en double » et pour commencer de ce fait placer l'email d'origine

dans la quarantaine au lieu d'une copie/de doublon.