Guide des meilleures pratiques pour les filtres de contenu entrant et sortant

Contenu

Introduction

Les filtres de contenu vous permettent d'examiner les détails complexes d'un e-mail et d'effectuer des actions (ou aucune action) sur l'e-mail. Une fois le filtre de contenu entrant ou sortant créé, vous l'appliquez à une stratégie de messagerie entrante ou sortante. Lorsqu'un e-mail correspond au filtre de contenu, le rapport « Filtres de contenu » sur l'appliance de sécurité de la messagerie Cisco (ESA) et l'appliance de gestion de la sécurité (SMA) peut vous montrer tous les e-mails correspondant à n'importe quel filtre de contenu. Par conséquent, même si aucune action n'est entreprise, c'est un excellent moyen d'obtenir des informations précieuses sur le type d'e-mails entrant et sortant de votre organisation - vous permettant de “ Modèle ” votre flux d'e-mails.

Comme il existe de nombreuses conditions et actions différentes pour les filtres de contenu, ce document vous guidera à travers quelques filtres de contenu entrant et sortant très courants et recommandés.

Présentation des étapes

Étape 1 : Importer les dictionnaires nécessaires

Ce document décrit les étapes nécessaires à la mise en oeuvre de certains filtres de contenu entrant et sortant selon les meilleures pratiques. Les filtres de contenu que nous allons créer référenceront quelques dictionnaires. Nous devrons donc d'abord importer ces dictionnaires. L'ESA est livré avec les dictionnaires et vous n'avez qu'à les importer dans la configuration afin de les référencer dans les filtres de contenu que nous allons créer.

Étape 2 : Créer des quarantaines centralisées

Pour la plupart des filtres de contenu, nous allons créer, nous allons définir l'« Action » pour mettre en quarantaine le courrier électronique (ou une copie du courrier électronique) dans une quarantaine personnalisée (nouvelle) spécifiée. Par conséquent, nous devons d'abord créer ces quarantaines sur le SMA, car ce document suppose que vous avez activé les quarantaines PVO centralisées (stratégies, virus et attaques) entre le ESA et le SMA.

Étape 3 : Créer les filtres de contenu entrant et sortant et appliquer aux stratégies

Une fois les dictionnaires importés et les quarantaines créés, nous créerons les filtres de contenu entrant et les appliquerons aux stratégies de messagerie entrante, puis créerons les filtres de contenu sortant et appliquerons-les aux stratégies de messagerie sortante.

ÉTAPE 1: IMPORTATION DES DICTIONNAIRES NÉCESSAIRES

Importation des dictionnaires que nous allons référencer dans nos filtres de contenu :

- Sur l'appliance ESA, accédez à **« Politiques de messagerie > Dictionnaires »**
- Cliquez sur le bouton **Importer le dictionnaire** " à droite de la page.

Profanation :

- Sélectionnez " **Importer dans le répertoire de configuration de votre appareil IronPort** "
- Sélectionnez " **profanity.txt** " et cliquez sur " **Suivant** ".
- Nom : **Profanité**
- Cliquez sur le " **Correspondance des mots entiers** " (TRÈS IMPORTANT)
- Modifier les termes (ajouter de nouveaux termes ou supprimer des termes indésirables)
- Cliquez sur **"Soumettre ».**

Contenu sexuel :

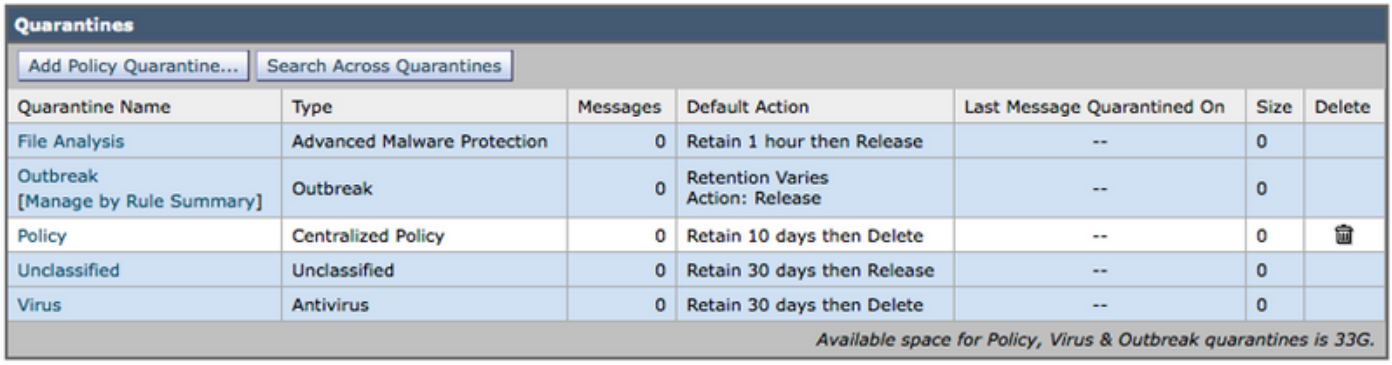
- Sélectionnez " **Importer dans le répertoire de configuration de votre appareil IronPort** "
- Sélectionnez le " **sex_content.txt** " et cliquez sur " **Next** ".
- Nom : **SexualContent**
- Cliquez sur le " **Correspondance des mots entiers** " (TRÈS IMPORTANT)
- Modifier les termes (ajouter de nouveaux termes ou supprimer des termes indésirables)
- Cliquez sur **"Soumettre ».**

Propriétaire :

- Sélectionnez " **Importer dans le répertoire de configuration de votre appareil IronPort** "
- Sélectionnez le " **propriétaire_content.txt** " et cliquez sur " **Suivant** ".
- Nom : **Propriétaire**
- Cliquez sur le " **Correspondance des mots entiers** " (TRÈS IMPORTANT)
- Modifier les termes (ajouter de nouveaux termes ou supprimer des termes indésirables)
- Cliquez sur **« Envoyer »**

ÉTAPE 2: CRÉATION DES QUARANTAINES CENTRALISÉES

- Sur le SMA, accédez à **« Onglet E-mail > Quarantaine de messages > Quarantaines PVO »**
- Voici à quoi devrait ressembler la table Quarantines avant de commencer. Toutes les quarantaines sont par défaut.



- Cliquez sur le bouton *"***Ajouter une quarantaine de stratégie...***"* bouton
- Créez les quarantaines ci-dessous.
- Certains seront utilisés par les filtres de contenu entrant et d'autres par les filtres de contenu sortant. Vous les créez de la même manière.

Quarantaines PVO - utilisées par les filtres de contenu entrant

URL de trafic entrant malveillant :
Name : URL entrante malveillante
Période de rétention : 14 jours
Action par défaut : DELETE
Libérez de l'espace : Activer

Catégorie d'URL entrante :
Name : Catégorie d'URL entrante
Période de rétention : 14 jours
Action par défaut : DELETE
Libérez de l'espace : Activer

Données bancaires entrantes :
Name : Données bancaires entrantes
Période de rétention : 14 jours
Action par défaut : DELETE
Libérez de l'espace : Activer

SSN entrant :
Name : SSN entrant
Période de rétention : 14 jours
Action par défaut : DELETE
Libérez de l'espace : Activer

Entrant inapproprié :
Name : Entrant inapproprié
Période de rétention : 14 jours
Action par défaut : DELETE
Libérez de l'espace : Activer

Échec matériel SPF :
Name : Échec matériel SPF
Période de rétention : 14 jours
Action par défaut : DELETE
Libérez de l'espace : Activer

Échec logiciel SPF :
Name : Échec logiciel SPF
Période de rétention : 14 jours
Action par défaut : DELETE
Libérez de l'espace : Activer

SpoofMail :
Name : MessagerieTromée
Période de rétention : 14 jours
Action par défaut : DELETE
Libérez de l'espace : Activer

Échec matériel DKIM :
Name : Échec matériel DKIM
Période de rétention : 14 jours
Action par défaut : DELETE
Libérez de l'espace : Activer

Entrant protégé par mot de passe :
Name : Pwd Protected Inbound
Période de rétention : 14 jours
Action par défaut : DELETE
Libérez de l'espace : Activer

Quarantaines PVO - utilisées par les filtres de contenu sortants

Données bancaires sortantes :
Name : Données bancaires sortantes
Période de rétention : 14 jours
Action par défaut : DELETE
Libérez de l'espace : Activer

SSN sortant :
Name : SSN sortant
Période de rétention : 14 jours
Action par défaut : DELETE
Libérez de l'espace : Activer

Sortant inapproprié :

URL de trafic sortant malveillant :
Name : URL en sortie malveillante
Période de rétention : 14 jours
Action par défaut : DELETE
Libérez de l'espace : Activer

Catégorie d'URL sortante :
Name : Catégorie d'URL sortante
Période de rétention : 14 jours
Action par défaut : DELETE
Libérez de l'espace : Activer

Sortant protégé par mot de passe :

Name : Sortant inapproprié
Période de rétention : 14 jours
Action par défaut : DELETE
Libérez de l'espace : Activer

Name : Pwd Protected Outbound
Période de rétention : 14 jours
Action par défaut : DELETE
Libérez de l'espace : Activer

Sortant propriétaire :

Name : Sortant propriétaire
Période de rétention : 14 jours
Action par défaut : DELETE
Libérez de l'espace : Activer

- Voici comment votre table PVO doit gérer la création de 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 DE CONTENU ENTRANTS

Une fois les dictionnaires importés et les quarantaines PVO créées, vous pouvez maintenant commencer à créer les filtres de contenu entrants :

- Accédez à : **« Politiques de messagerie > Filtres de contenu entrant »**
- Voici un tableau des filtres de contenu entrant que vous devez créer. Par exemple, en dessous du tableau se trouve une capture d'écran illustrant comment créer le premier.

Créer ces filtres de contenu entrant

Name : **Données_Banque**
Ajouter deux conditions :
  Corps ou pièce jointe du message :
    Contient l'identificateur Smart : Numéro de routage ABA
    Contient l'identificateur Smart : Numéro de carte de crédit
Ajouter une action :
  Quarantaine :

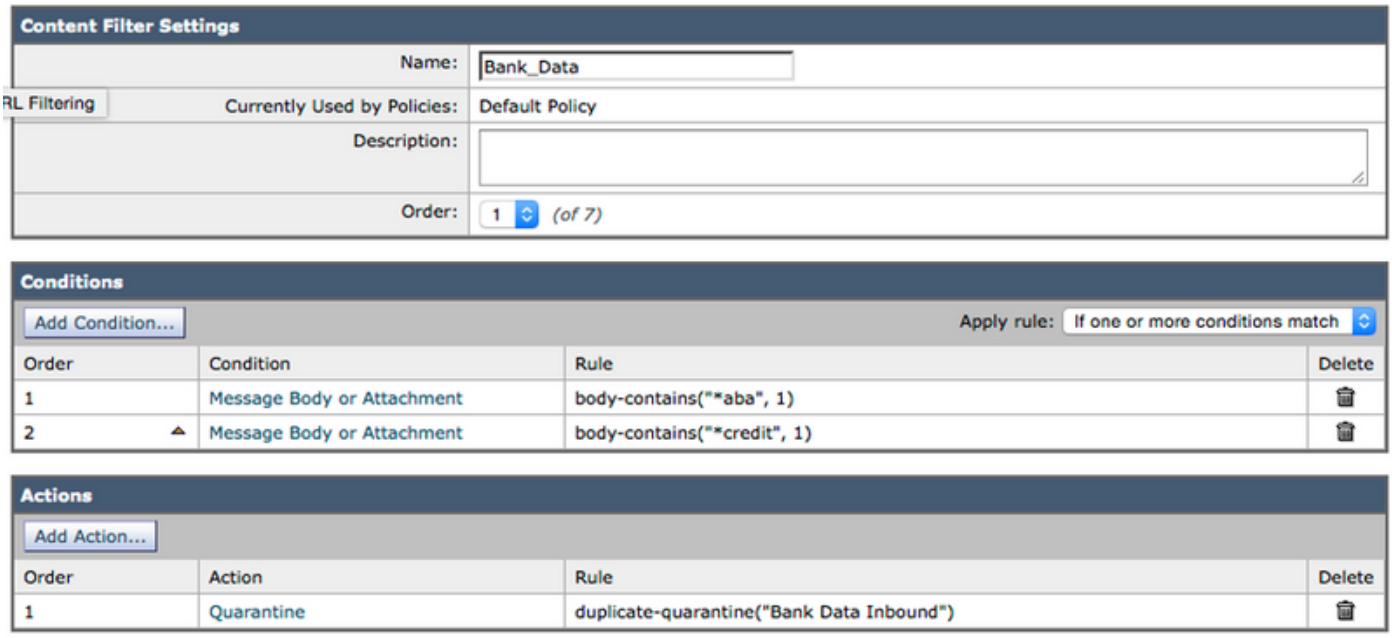
Envoyer le message en quarantaine : ” de données bancaires entrantes “ (centralisé)
Message dupliqué : Activée
(Notez que la règle Apply doit être “ Si une ou plusieurs conditions correspondent ”)

Name : **SSN**
Ajouter une condition :
Corps ou pièce jointe du message :
Contient l'identificateur Smart : Numéro de sécurité sociale (SSN)
Ajouter une action :
Quarantaine :
Envoyer le message en quarantaine : “ SSN ” entrant (centralisé)
Message dupliqué : Activée
Name : **Inapproprié**
Ajouter deux conditions :
Corps ou pièce jointe du message :
Contient le terme dans le dictionnaire : Profanité
Contient le terme dans le dictionnaire : Contenu sexuel
Ajouter une action :
Quarantaine :
Envoyer le message en quarantaine : “ Inappropriée ” entrante (centralisée)
Message dupliqué : Activée
Name : **Catégorie_URL**
Ajouter une condition :
Catégorie d'URL :
Sélectionner des catégories :
Adulte, rencontre, évitement de filtre, logiciels gratuits et partagés, jeux d'argent,
Jeux, piratage, lingerie et maillots de bain, nudité non sexuelle,
Domaines garés, transfert de fichiers homologues, pornographie
Ajouter une action :
Quarantaine :
Envoyer le message en quarantaine : ” entrante de catégorie d'URL “ (centralisée)
Message dupliqué : Activée
(Remarque: Ce filtre de contenu nécessite l'activation de “ Security Services ”—> “ URL Filtering ”)
Name : **URL_Malveillant**
Ajouter une condition :
Réputation des URL :
La réputation des URL est la suivante : Malveillant (-10.0 à -6.0)
Ajouter une action :
Quarantaine :
Envoyer le message en quarantaine : “ URL ” de trafic entrant malveillant (centralisé)
Message dupliqué : Désactivé (**** Mettre en quarantaine l'original ****)
Name : **Password_Protected**
Ajouter une condition :
Protection des pièces jointes : Une ou plusieurs pièces jointes sont protégées
Ajouter une action :
Quarantaine :
Envoyer le message en quarantaine : “ ” Pwd Protected Inbound (centralisée)
Message dupliqué : Activée

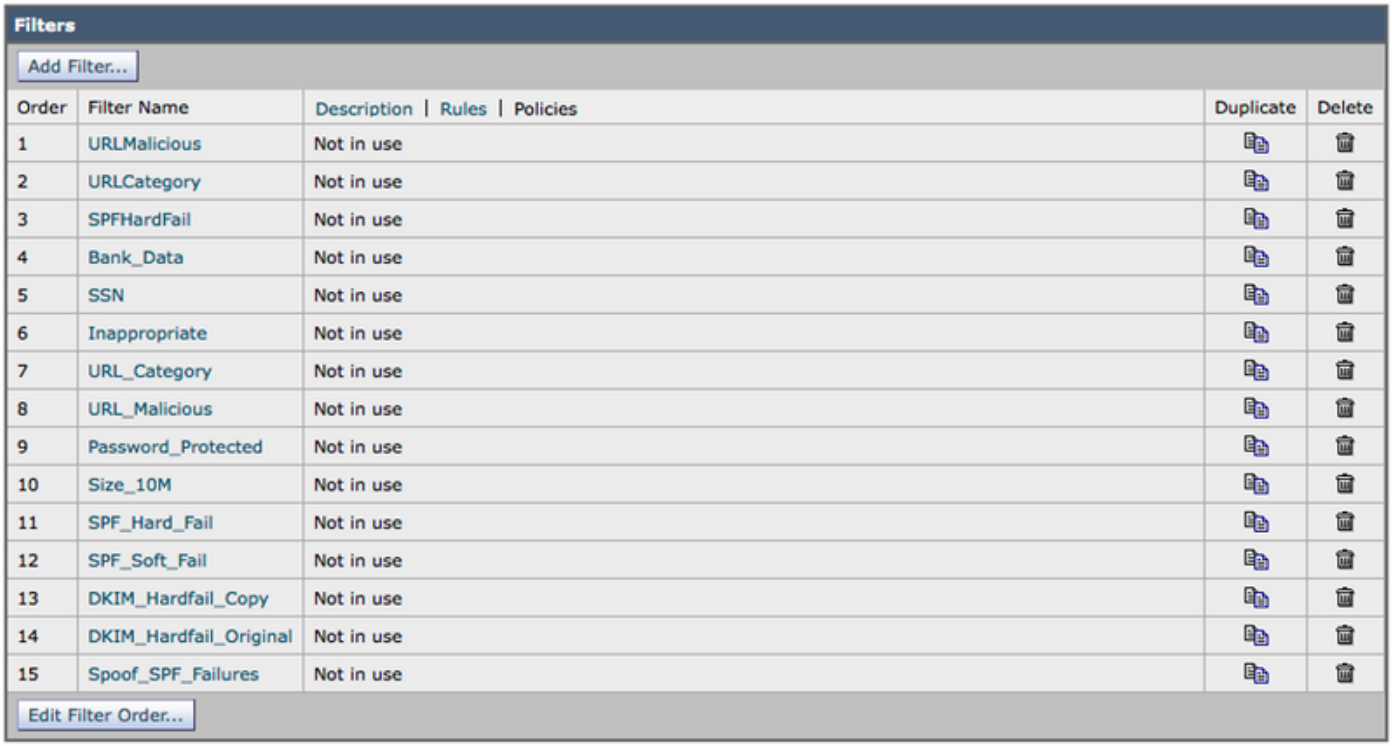
Name : **Taille_10M**
Ajouter une condition :
Taille du message :
Supérieur ou égal à : 10 M
Ajouter une action :
Ajouter une balise de message :
Entrez un terme : NOM
(Remarque: Il doit y avoir une action, donc ici nous “ Tag ” le message pour représenter aucune opération effectuée. Le fait que le filtre de contenu a été “ Correspondant ” le permettra d'apparaître dans les rapports. Aucune « action ” doit être entreprise pour qu'elle apparaisse dans le rapport.)
Name : **SPF_Hard_Fail**
Ajouter une condition :
Vérification SPF : “ est ” Échec
Ajouter une action :
Quarantaine :
Envoyer le message en quarantaine : “ de défaillance matérielle SPF (centralisée)
Message dupliqué : Activée
(Remarque: “ est Fail ” est un échec de SPF dur et cela signifie que le propriétaire du domaine vous dit de supprimer tous les e-mails reçus d'expéditeurs qui ne sont pas répertoriés dans leur enregistrement SPF. Au départ, il est recommandé d'utiliser “ message en double ” et de passer en revue les échecs pendant une semaine ou deux avant de mettre en quarantaine l'original (c'est-à-dire de désactiver le message en double).
Name : **SPF_Soft_Fail**
Ajouter une condition :
Vérification SPF : “ est ” Softfail
Ajouter une action :
Quarantaine :
Envoyer le message en quarantaine : Échec logiciel “ SPF (” centralisée)
Message dupliqué : Activée
Name : **DKIM_Hardfail_Copy**
Ajouter une condition :
Authentification DKIM : “ est ” Hardfail
Ajouter deux actions :
Ajouter/Modifier l'en-tête :
Nom de l'en-tête : Objet
Cliquez sur “ Prépend à la valeur de l'” d'en-tête existant et saisissez : [Copier - Ne pas libérer] ”
Quarantaine :
Envoyer le message en quarantaine : “ DKIM Hard Fail (” centralisée)
Message dupliqué : Activée
(Remarque: Mettre en quarantaine une copie du message initialement.)
Name : **DKIM_Hardfail_Original**
Ajouter une condition :
Authentification DKIM : “ est ” Hardfail
Ajouter une action :
Quarantaine :
Envoyer le message en quarantaine : “ DKIM Hard Fail (” centralisée)
Message dupliqué : Désactivé
(Remarque: Nous allons créer une autre ligne Stratégie de messagerie entrante pour les domaines PayPal et eBay et utiliserons ce filtre de contenu pour les domaines que nous savons réussir la vérification DKIM.)
Name : **Échecs_SPF_Spoof**

Ajouter une condition, mais les deux options Softfail et Hardfail sont cochées :
Vérification SPF : “ est ” Softfail et cliquez également sur “ Fail ”
(vous avez donc coché deux cases “ Softfail ” et “ Fail ”
Ajouter une action :
Quarantaine :
Envoyer le message en quarantaine : “ SpoofMail (centralisé) ”
Message dupliqué : Activer
(Remarque: Nous utiliserons ce filtre de contenu pour prendre des mesures pour les courriels entrants prétendant envoyer à partir de votre propre domaine — usurpation d'adresse. Commencez par l'action définie pour mettre en quarantaine une copie et après quelques semaines de vérification de la quarantaine SpoofMail, vous pouvez modifier votre enregistrement DNS TXT SPF pour ajouter tous les expéditeurs légitimes et, à un moment donné, vous pouvez modifier ce filtre de contenu pour mettre en quarantaine l'original en désactivant la case à cocher des messages en double.)

Par exemple, c'est à cela que doit ressembler le filtre de contenu Bank_Data avant de l'envoyer.



Après avoir créé tous les filtres de contenu entrant, la table doit 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...

Étant donné que la fonction ” Stratégies “ est sélectionnée (vous verrez l'hypertexte Stratégies en haut au milieu), la colonne du milieu affiche les Stratégies de messagerie entrante auxquelles le filtre de contenu a été appliqué. Comme nous ne les avons pas appliqués à une stratégie de messagerie entrante, la “ Non utilisée ” s'affiche.

Appliquer les filtres de contenu entrant aux stratégies de messagerie entrante

- Accédez à : **"Politiques de messagerie > Politiques de messagerie entrante »**
- Cliquez sur le texte **“ Désactivé** dans la cellule Filtres de contenu pour la **« Stratégie par défaut »**.
- Le bouton du menu déroulant est défini sur **“ Désactiver ” filtres de contenu**.
- Cliquez sur le bouton et sélectionnez **Activer les filtres de contenu ”** et vous recevrez immédiatement tous les filtres de contenu entrants qui ont été créés.
- Activez tous les filtres à l'exception de DKIM_Hardfail_Original et Spoof_SPF_Failures.
- **« Envoyer »** et **"Valider »**.

Vérification de DKIM pour eBay et la protection contre les spams et les spams pour votre domaine

Ces deux rubriques concernent les filtres de contenu 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. Activer la vérification DKIM et SPF dans les stratégies de flux de courrier

- Accédez à : **« Politiques de messagerie > Politiques de flux de courrier »**
- Activez la vérification DKIM et SPF dans toutes les stratégies de flux de messages qui ont “ comportement de connexion ” de “ Accepter ”.
- Cliquez sur l'hypertexte du bas “ Paramètres de stratégie par défaut ” et définissez **“ Vérification DKIM ”** sur **“ Sur ”** et **“ Vérification SFP/SIDF** sur .
- Cliquez sur **« Soumettre »** et **« Valider »**.

- Le tableau Politiques de flux de messages s'affiche maintenant. Examinez la colonne nommée **“ Comportement ”** et modifiez toute stratégie de flux de messages avec le comportement défini sur **“ Relay ”**
- Désactivez **“ ”** Vérification DKIM et SPF pour ces stratégies de flux de messages.
- Cliquez sur **« Soumettre »** et **« Valider »**.

Nous ne voulons pas que l'ESA effectue la vérification DKIM ou SPF pour les e-mails reçus dans l'ESA à partir de votre en-tête Exchange Mail Server sortant. Dans la plupart des configurations, la stratégie de flux de messages ” RELAIS “ est la seule ligne ayant le comportement du relais.

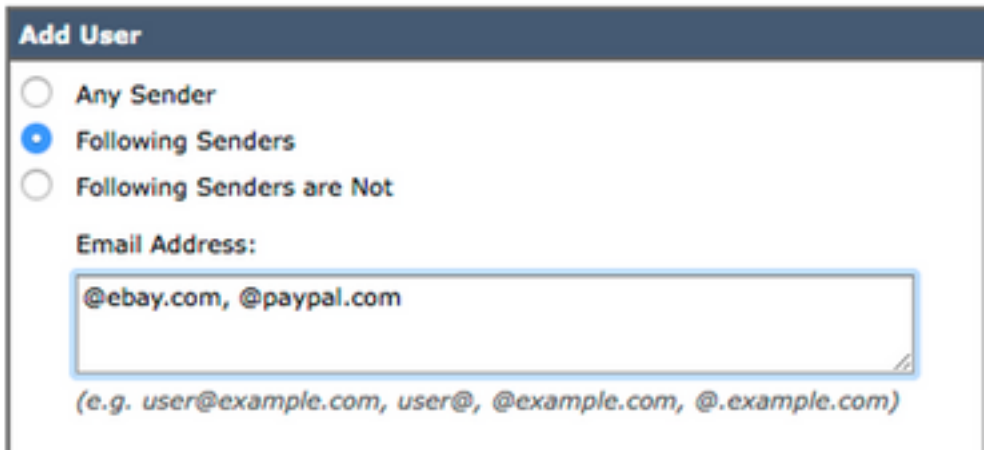
2. Créer une nouvelle stratégie de flux de messages entrants pour eBay et Paypal

Les e-mails entrants reçus d'eBay et de Paypal doivent toujours réussir la vérification DKIM. Nous allons donc créer une autre stratégie de messagerie entrante pour utiliser le filtre de contenu entrant DKIM_Hardfail_Original pour un e-mail provenant de ces domaines.

- Accédez à : **"Politiques de messagerie > Politiques de messagerie entrante »**
- Cliquez sur le bouton **Ajouter une stratégie**.
- Saisissez le nom : **« DKIM Hardfail Original »**
- Cliquez sur le bouton **“ Ajouter un utilisateur... ”** bouton.

Le panneau de configuration suivant vous permet de définir les messages qui correspondent à cette nouvelle stratégie de messagerie entrante. Nous voulons uniquement définir les critères de l'expéditeur (partie gauche du panneau de configuration).

- Cliquez sur **“ ” d'expéditeurs suivants** et dans le tableau Adresses e-mail, saisissez **“@ebay.com, @paypal.com ”**



- Cliquez sur le bouton **“ OK ”** en bas.
- Cliquez sur **"Envoyer »**.

3. Créer une nouvelle stratégie de flux de messages entrants pour votre domaine (protection contre les erreurs)

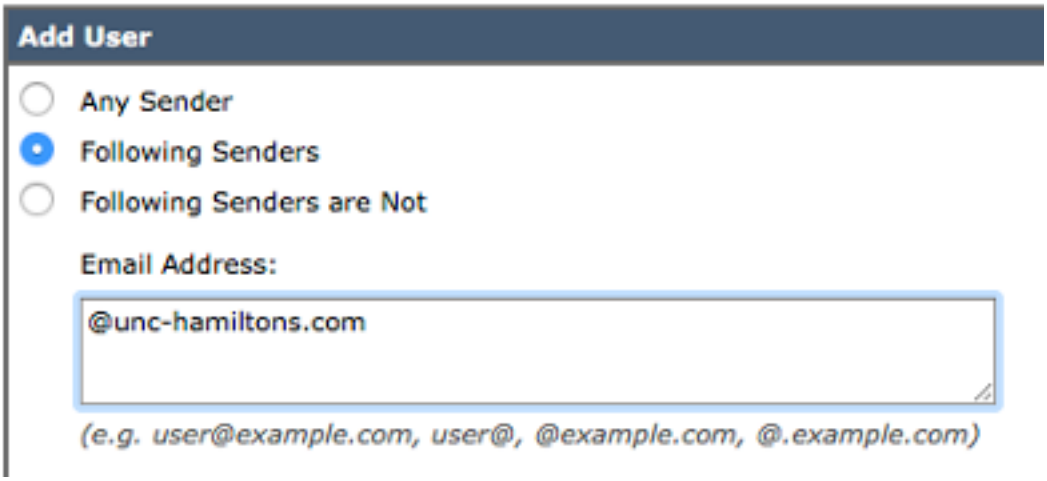
Les étapes de cette section vous permettront d'effectuer des actions sur les e-mails entrants dont l'adresse e-mail de départ de votre propre domaine ne permet pas de vérifier SPF. Bien sûr, cela suppose que vous avez déjà publié votre enregistrement de texte SPF dans DNS. Ignorez ces étapes si vous n'avez pas créé/publié d'enregistrement de ressource de texte SPF pour votre domaine.

- Accédez à : **"Politiques de messagerie > Politiques de messagerie entrante »**
- Cliquez sur le bouton **Ajouter une stratégie**.

- Saisissez le nom : **« Spoof_Protection »**
- Cliquez sur le bouton **“ Ajouter un utilisateur... ”** bouton.

Le panneau de configuration suivant vous permet de définir les messages qui correspondent à cette nouvelle ligne Stratégie de messagerie entrante. Vous voulez uniquement définir les critères de l'expéditeur (qui correspond à la partie gauche du panneau de configuration).

- Cliquez sur le bouton **“ ” d'expéditeurs suivants** puis saisissez votre domaine dans la zone de texte **Adresse e-mail “ : ”**. Pour moi, mon domaine est **“@unc-hamiltons.com ”**



- Cliquez sur **"Envoyer »**.

Le tableau Stratégies de messagerie entrante s'affiche à nouveau, mais vous avez maintenant une deuxième ligne Stratégie de messagerie au-dessus de la Stratégie par défaut.

- Cliquez sur l'hypertexte **(utiliser par défaut)** dans la cellule Filtres de contenu de la nouvelle ligne.
- Retournez le menu déroulant pour **“ Activer les filtres de contenu (paramètres personnalisés) ”** .
- Vérifiez le **” Spoof_SPF_Failures de “** également assurez-vous que **DKIM_Hardfail_Copy »** et **« DKIM_Hardfail_Original »** ne sont pas cochés.
- Cliquez sur **« Envoyer »** et **« Valider les modifications »**.

La table Stratégies de messagerie entrante doit 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 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	

ÉTAPE 4: CRÉATION DES FILTRES DE CONTENU SORTANTS

- Accédez à : **« Politiques de messagerie > Filtres de contenu sortant »**
- Voici un tableau des filtres de contenu sortant que vous devez créer.

Créer ces filtres de contenu sortant

Name : **Données_Banque**
Ajouter deux conditions :
  Corps ou pièce jointe du message :
    Contient l'identificateur Smart : Numéro de routage ABA
    Contient l'identificateur Smart : Numéro de carte de crédit
Ajouter une action :
  Quarantaine :
    Envoyer le message en quarantaine : “ données bancaires ” sortantes (centralisées)
    Message dupliqué : Activée
(Notez que la règle Apply doit être “ Si une ou plusieurs conditions correspondent ”)
Name : **SSN**
Ajouter une condition :
  Corps ou pièce jointe du message :
    Contient l'identificateur Smart : Numéro de sécurité sociale (SSN)
Ajouter une action :
  Quarantaine :
    Envoyer le message en quarantaine : “ SSN ” sortant (centralisé)
    Message en double : activé
Name : **Inapproprié**
Ajouter deux conditions :
  Corps ou pièce jointe du message :
    Contient le terme dans le dictionnaire : Profanité
    Contient le terme dans le dictionnaire : Contenu sexuel
Ajouter une action :
  Quarantaine :
    Envoyer le message en quarantaine : “ ” sortante inappropriée (centralisée)
    Message dupliqué : Activée
Name : **Catégorie_URL**
Ajouter une condition :
  Catégorie d'URL :
    Sélectionner des catégories :
      Adulte, rencontre, évitement de filtre, logiciels gratuits et partagés, jeux d'argent,
      Jeux, piratage, lingerie et maillots de bain, nudité non sexuelle,
      Domaines garés, transfert de fichiers homologues, pornographie
Ajouter une action :
  Quarantaine :
    Envoyer le message en quarantaine : ” sortante de catégorie d'URL “ (centralisée)
    Message dupliqué : Activée
Name : **URL_Malveillant**
Ajouter une condition :
  Réputation des URL :
    La réputation des URL est la suivante : Malveillant (-10.0 à -6.0)
Ajouter une action :
  Quarantaine :
    Envoyer le message en quarantaine : “ URL ” de trafic sortant malveillant (centralisé)
    Message dupliqué : Désactivé (**** Mettre en quarantaine l'original ****)
Name : **Password_Protected**
Ajouter une condition :
  Protection des pièces jointes : Une ou plusieurs pièces jointes sont protégées
Ajouter une action :
  Quarantaine :
    Envoyer le message en quarantaine : “ Pwd Protected Outbound (” centralisée)

Message dupliqué : Activée
Name : **Taille_10M**
Ajouter une condition :
Taille du message :
Supérieur ou égal à : 10 M
Ajouter une action :
Ajouter une balise de message :
Entrez un terme : NOM
(Remarque: Il doit y avoir une action, donc ici nous “ Tag ” le message pour représenter aucune opération effectuée. Le fait que le filtre de contenu a été “ Correspondant ” le permettra d'apparaître dans les rapports. Aucune « action ” doit être entreprise pour qu'elle apparaisse dans le rapport.)
Name : **Propriétaire**
Ajouter une condition :
Corps ou pièce jointe du message :
Contient le terme dans le dictionnaire : Propriétaire
Ajouter une action :
Quarantaine :
Envoyer le message en quarantaine : “ ” propriétaire (centralisé)
Message dupliqué : Activée

Étant donné que la fonction “ Policies ” est sélectionnée (l'hypertexte Policies se trouve au milieu supérieur), la colonne du milieu affiche les Outgoing Mail Policies auxquelles le filtre de contenu a été appliqué. Comme nous ne les avons pas appliqués à une stratégie de messagerie sortante, le ” “ non utilisé s'affiche.

- Accédez à : **"Politiques de messagerie > Politiques de messagerie sortante »**
- Cliquez sur le texte **“ Désactivé** dans la cellule Filtres de contenu de la stratégie par défaut.
- Le bouton du menu déroulant est défini sur “ **Désactiver les** ” **de filtres de contenu**.
- Cliquez sur le bouton et sélectionnez **« Activer les filtres de contenu »** et vous recevrez immédiatement tous les filtres de contenu sortants qui ont été créés.
- **« Activer »** tous les filtres.
- **« Envoyer »** et **"Valider »**.

Résumé

Vous avez maintenant mis en oeuvre les Méthodes Recommandées initiales pour les filtres de contenu entrant et sortant. La plupart (pas tous) des filtres de contenu ont utilisé l'action de quarantaine et ont choisi de cocher (Activer) l'option “ Doublon Message ” - qui place simplement une copie de l'e-mail d'origine et n'empêche pas la remise de l'e-mail. L'objectif de ces filtres de contenu est de vous permettre de recueillir des informations sur les types d'e-mails entrants et sortants vers votre société.

Ceci dit, après avoir exécuté le rapport Filtres de contenu et examiné les copies de courrier enregistrées dans les quarantaines, il peut être prudent de décocher la case “ message en double ” et de commencer ainsi à placer l'e-mail d'origine dans la quarantaine au lieu d'une copie/copie.