



CISCO EMAIL SECURITY APPLIANCE

BEST PRACTICES:

INCOMING & OUTGOING CONTENT FILTERS

September 2015
Version 1.0.1

Dalton Hamilton
Cisco Sales Engineer

THE MOST RECENT VERSION OF THIS DOCUMENT CAN BE FOUND HERE:

<https://cisco.com/go/emailsecurity-customer>

ESA Incoming and Outgoing Content Filters - Best Practices

| | |
|--------------------------------------------------------------------|-----------|
| THE MOST RECENT VERSION OF THIS DOCUMENT CAN BE FOUND HERE: | 1 |
| PURPOSE OF THIS DOCUMENT | 3 |
| OVERVIEW OF STEPS | 3 |
| STEP 1: IMPORTING THE NEEDED DICTIONARIES | 4 |
| STEP 2: CREATING THE CENTRALIZED QUARANTINES | 5 |
| STEP 3: CREATING THE INCOMING CONTENT FILTERS | 7 |
| STEP 4: CREATING THE OUTGOING CONTENT FILTERS | 15 |
| NEXT STEPS AND SUMMARY | 18 |

PURPOSE OF THIS DOCUMENT

Content Filters allow you to inspect the intricate details of an Email and take Actions (or no Action) on the Email. Once the Incoming or Outgoing Content Filter is created, you apply it to a Incoming or Outgoing Mail Policy. When any Email matches the Content Filter, the 'Content Filters' Report on the ESA and SMA will be able to show you all email that matched any Content Filter. Therefore, even if no Action is taken, it is an excellent way to obtain valuable information about the type of emails entering and leaving your organization — allowing you to “Pattern” your email flow.

As there are many different Content Filter ‘Conditions’ and ‘Actions’, this document will step you through some very common and recommended Incoming and Outgoing Content Filters.

OVERVIEW OF STEPS

Step1: Import the needed dictionaries:

This document will provide the steps necessary for you to implement some Best Practices Incoming and Outgoing Content Filters. The Content Filters we are going to create will reference a few dictionaries — so we will need to import those dictionaries first. The ESA ships with the dictionaries and you merely need to import them into the configuration in order to reference them in the Content Filters we will create.

Step2: Create the Centralized Quarantines

For most of the Content Filters we will create, we will set the ‘Action’ to Quarantine the Email (or a copy of the Email) into a specified designated custom (new) Quarantines — and therefore, we need to first create those Quarantines on the SMA — as this document assumes you have enabled Centralized PVO (Policy, Virus, and Outbreak) Quarantines between the ESA and SMA.

Step3: Create the Incoming and Outgoing Content Filters and Apply to Policies

Once we have the dictionaries imported and the Quarantines created, we will create the Inbound Content Filters and apply them to the Incoming Mail Policies and then create the Outgoing Content Filters and apply them to the Outgoing Mail Policies.

STEP 1: IMPORTING THE NEEDED DICTIONARIES

Importing the Dictionaries that we will be referencing in our Content Filters:

On the ESA appliance, Navigate to: *Mail Policies > Dictionaries*

Click the “*Import Dictionary*” button on the right side of the page.

Profanity:

- Select “*Import from the configuration directory on your IronPort appliance*”
- Select “*profanity.txt*” and click “*Next*”.
- Name: Profanity
- Click the “*Match whole words*” (VERY IMPORTANT)
- Modify the terms (add new terms or remove unwanted terms)
- Click *Submit*

SexualContent:

- Select “*Import from the configuration directory on your IronPort appliance.*” Select the “*sexual_content.txt*” and click “*Next*”.
- Name: SexualContent
- Click the “*Match whole words*” (VERY IMPORTANT)
- Modify the terms (add new terms or remove unwanted terms)
- Click *Submit*

Proprietary:

- Select “*Import from the configuration directory on your IronPort appliance.*” Select the “*proprietary_content.txt*” and click “*Next*”.
- Name: Proprietary
- Click the “*Match whole words*” (VERY IMPORTANT)
- Modify the terms (add new terms or remove unwanted terms)
- Click *Submit*

STEP 2: CREATING THE CENTRALIZED QUARANTINES

On the SMA, navigate to: *Email Tab > Message Quarantine > PVO Quarantines*

This is what the Quarantines table should look like before we start. All quarantines are default.

| 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.

Click the “Add Policy Quarantine...” button and Create the below Quarantines. Some will be used by Incoming Content Filters and some will be used by Outgoing Content Filters. You create them in the same manner.

| PVO Quarantines - used by Incoming Content Filters | |
|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| URL Malicious Inbound: Name: URL Malicious Inbound Retention Period: 14 Days Default Action: Delete Free up space: Enable | SPF Hard Fail: Name: SPF Hard Fail Retention Period: 14 Days Default Action: Delete Free up space: Enable |
| URL Category Inbound: Name: URL Category Inbound Retention Period: 14 Days Default Action: Delete Free up space: Enable | SPF Soft Fail: Name: SPF Soft Fail Retention Period: 14 Days Default Action: Delete Free up space: Enable |
| Bank Data Inbound: Name: Bank Data Inbound Retention Period: 14 Days Default Action: Delete Free up space: Enable | SpoofMail: Name: SpoofMail Retention Period: 14 Days Default Action: Delete Free up space: Enable |
| SSN Inbound: Name: SSN Inbound Retention Period: 14 Days Default Action: Delete Free up space: Enable | DKIM Hard Fail: Name: DKIM Hard Fail Retention Period: 14 Days Default Action: Delete Free up space: Enable |
| Inappropriate Inbound: Name: Inappropriate Inbound Retention Period: 14 Days Default Action: Delete Free up space: Enable | Password Protected Inbound: Name: Pwd Protected Inbound Retention Period: 14 Days Default Action: Delete Free up space: Enable |

ESA Incoming and Outgoing Content Filters - Best Practices

| PVO Quarantines - used by Outgoing Content Filters | |
|------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Bank Data Outbound: Name: Bank Data Outbound Retention Period: 14 Days Default Action: Delete Free up space: Enable | URL Malicious Outbound: Name: URL Malicious Outbound Retention Period: 14 Days Default Action: Delete Free up space: Enable |
| SSN Outbound: Name: SSN Outbound Retention Period: 14 Days Default Action: Delete Free up space: Enable | URL Category Outbound: Name: URL Category Outbound Retention Period: 14 Days Default Action: Delete Free up space: Enable |
| Inappropriate Outbound: Name: Inappropriate Outbound Retention Period: 14 Days Default Action: Delete Free up space: Enable | Password Protected Outbound: Name: Pwd Protected Outbound Retention Period: 14 Days Default Action: Delete Free up space: Enable |
| Proprietary Outbound: Name: Proprietary Outbound Retention Period: 14 Days Default Action: Delete Free up space: Enable | |

Here is how your PVO table should look after creating all of the PVO Quarantines.

| Quarantines | | | | | | |
|---------------------------------------------------------|--------------------------------------------------------|----------|-------------------------------------|-----------------------------|------|--------|
| <input type="button" value="Add Policy Quarantine..."/> | <input type="text" value="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.

STEP 3: CREATING THE INCOMING CONTENT FILTERS

Once the Dictionaries have been imported and the PVO Quarantines have been created, you can now start creating the Incoming Content Filters:

Navigate to: *Mail Policies > Incoming Content Filters*

Here is a table of Incoming Content Filters you should create. For example purposes, below the table is a screenshot exemplifying how to create the first one.

Create these Incoming Content Filters:

| Create these Incoming Content Filters |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Name: Bank_Data Add Two Conditions: Message Body or Attachment: Contains Smart Identifier: ABA Routing Number Contains Smart Identifier: Credit Card Number Add One Action: Quarantine: Send message to quarantine: "Bank Data Inbound (centralized)" Duplicate message: Enabled</p> <p>(Note the Apply Rule should be "If one or more conditions match")</p> |
| <p>Name: SSN Add One Condition: Message Body or Attachment: Contains Smart Identifier: Social Security Number (SSN) Add One Action: Quarantine: Send message to quarantine: "SSN Inbound (centralized)" Duplicate message: Enabled</p> |
| <p>Name: Inappropriate Add Two Conditions: Message Body or Attachment: Contains term in dictionary: Profanity Contains term in dictionary: Sexual_Content Add One Action: Quarantine: Send message to quarantine: "Inappropriate Inbound (centralized)" Duplicate message: Enabled</p> |

ESA Incoming and Outgoing Content Filters - Best Practices

Create these Incoming Content Filters

Name: URL_Category

Add One Condition:

URL Category:

Select Categories:

Adult, Dating, Filter Avoidance, Freeware and Shareware, Gambling,
Games, Hacking, Lingerie and Swimsuits, Non-sexual Nudity,
Parked Domains, Peer File Transfer, Pornography

Add One Action:

Quarantine:

Send message to quarantine: "URL Category Inbound (centralized)"

Duplicate message: Enabled

*** Note: This Content Filter requires that you enable "Security Services"—> "URL Filtering"

Name: URL_Malicious

Add One Condition:

URL Reputation:

URL Reputation is: Malicious (-10.0 to -6.0)

Add One Action:

Quarantine:

Send message to quarantine: "URL Malicious Inbound (centralized)"

Duplicate message: Disabled (**** Quarantine the original ****)

Name: Password_Protected

Add One Condition:

Attachment Protection: One or more attachments are protected

Add One Action:

Quarantine:

Send message to quarantine: "Pwd Protected Inbound (centralized)"

Duplicate message: Enabled

Name: Size_10M

Add One Condition:

Message Size is:

Greater than or equal to: 10M

Add One Action:

Add Message Tag:

Enter a Term: NOOP

(Note: There must be some action so here we "Tag" the message to represent no operation taken. The fact that the content filter was "Matched" will allow it to show up in reporting. No 'Action' need be taken for it to show in Reporting.)

ESA Incoming and Outgoing Content Filters - Best Practices

Create these Incoming Content Filters

Name: SPF_Hard_Fail

Add One Condition:

SPF Verification: "is" Fail

Add One Action:

Quarantine:

Send message to quarantine: "SPF Hard Fail (centralized)"

Duplicate message: Enabled

(Note: "is Fail" is a Hard SPF failure and it means the owner of the domain is telling you to drop all emails received from senders that are not listed in their SPF record. Initially, it is a good idea to use "Duplicate message" and review the failures for a week or two before quarantining the original (i.e. turning off duplicate message).

Name: SPF_Soft_Fail

Add One Condition:

SPF Verification: "is" Softfail

Add One Action:

Quarantine:

Send message to quarantine: "SPF Soft Fail (centralized)"

Duplicate message: Enabled

Name: DKIM_Hardfail_Copy

Add One Condition:

DKIM Authentication: "is" Hardfail

Add Two Actions:

Add/Edit Header:

Header Name: Subject

Click "Prepend to the Value of Existing Header" and enter: [Copy - Do Not Release]"

Quarantine:

Send message to quarantine: "DKIM Hard Fail (centralized)"

Duplicate message: Enabled

(Note: Quarantine a copy of the message initially.)

Name: DKIM_Hardfail_Original

Add One Condition:

DKIM Authentication: "is" Hardfail

Add One Action:

Quarantine:

Send message to quarantine: "DKIM Hard Fail (centralized)"

Duplicate message: Disabled

(Note: We will be creating another Incoming Mail Policy row for PayPal and Ebay domains and will use this Content Filter for domains that we know should pass DKIM Verification.)

ESA Incoming and Outgoing Content Filters - Best Practices

Create these Incoming Content Filters

Name: Spoof_SPF_Failures

Add One Condition but it has BOTH Softfail and Hardfail checked:

SPF Verification: “is” Softfail and also click on “Fail”
(so you have two checkboxes clicked “Softfail” and “Fail”)

Add One Action:

Quarantine:
Send message to quarantine: “SpoofMail (centralized)”
Duplicate message: Enable

(Note: We will use this Content Filter to take action for incoming email pretending to send from your own domain — spoofing. Start with the action set to quarantine a copy and after a couple of weeks of reviewing the SpoofMail quarantine, you can modify your SPF TXT DNS record to add all legitimate senders and at some point you can change this content filter to quarantine the original by disabling the duplicate message checkbox.)

As an example, this is what the Bank_Data Content Filter should look like before you Submit:

| Content Filter Settings | | | |
|-------------------------|-----------------------------|-------------------------------------------------|--|
| | Name: | <input type="text" value="Bank_Data"/> | |
| URL Filtering | Currently Used by Policies: | Default Policy | |
| | Description: | <input style="width: 100%;" type="text"/> | |
| | Order: | 1 (of 7) | |

| Conditions | | | |
|-------------------------------------------------|----------------------------|----------------------------|--------------------------------------------------------------------------|
| <input type="button" value="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 | | | |
|----------------------------------------------|------------|-------------------------------------------|--------|
| <input type="button" value="Add Action..."/> | | | |
| Order | Action | Rule | Delete |
| 1 | Quarantine | duplicate-quarantine("Bank Data Inbound") | |

After creating all of the Incoming Content Filters, the table should now look like this: Because the “Policies” function is selected (you’ll see the Policies hypertext at the top middle) the middle column shows the Incoming Mail Policies the Content Filter has been applied to. Because we have not applied them to any Incoming Mail Policy, the “Not in use” is displayed.

Apply the Incoming Content Filters to the Incoming Mail Policies:

Navigate to: *Mail Policies > Incoming Mail Policies*

ESA Incoming and Outgoing Content Filters - Best Practices

| 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...](#)

Click on the “Disabled” text in the Content Filters cell for the *Default Policy*.

The pull-down menu button is set to “Disable Content Filters”. Click the button and set to “Enable Content Filters” and you will immediately be presented with all Incoming Content Filters that have been created. Enable all filters except the *DKIM_Hardfail_Original*, and *Spoof_SPF_Failures*.

Submit and Commit

DKIM Verification for Ebay & Paypal and Spoof Email Protection for your domain

Those two topics will involve Content Filters that utilize DKIM Verification and SPF Verification. Therefore, we must first ensure both DKIM and SPF Verification are enabled.

Step 1: Enable DKIM and SPF Verification within Mail Flow Policies

Navigate to: *Mail Policies* → *Mail Flow Policies*

Enable DKIM and SPF Verification within all Mail Flow Policies that have “*Connection Behavior*” of “*Accept*”.

Click on the bottom hypertext “*Default Policy Parameters*” and set “*DKIM Verification*” to “*On*” and “*SFP/SIDF Verification*” to “*On*”.

Click *Submit*.

You now see the Mail Flow Policies table.

Look at the column named “*Behavior*” and edit any Mail Flow Policy with the *Behavior* set to “*Relay*” to turn “*Off*” both DKIM and SPF Verification for those Mail Flow Policies. We do not want the ESA to perform DKIM or SPF verification for email received into the ESA from your Exchange Mail Server heading outbound. In most configurations the “*RELAYED*” *Mail Flow Policy* is the only row with the Behavior of *Relay*.

Step 2: Create a new Incoming Mail Flow Policy for Ebay and Paypal

Inbound Email received from Ebay and Paypal should always pass DKIM verification. We will therefore create another Incoming Mail Policy to use the DKIM_Hardfail_Original Incoming Content Filter for email from those domains.

Navigate to: *Mail Policies* > *Incoming Mail Policies*

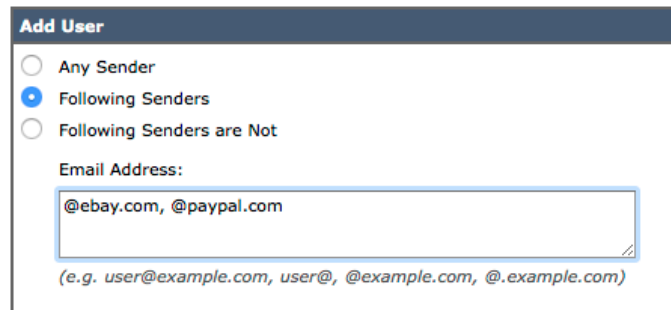
Click the Add Policy button.

Enter the Name: DKIM Hardfail Original

Click “*Add User...*” button.

The next configuration panel lets you define what messages will match this new Incoming Mail Policy. We only want to define criteria for the Sender (the left portion of the configuration panel).

Click “*Following Senders*” radio button and in the Email Addresses table enter “[@ebay.com](#), [@paypal.com](#)”



Add User

Any Sender

Following Senders

Following Senders are Not

Email Address:

@ebay.com, @paypal.com

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

Click the “Ok” button at the bottom.

Click *Submit*.

You are presented with the Incoming Mail Policies table again but now you have a new Mail Policy row above the Default Policy.

Click the *(use default)* hypertext in the Content Filters cell for the new row.

Flip the pulldown menu to “Enable Content Filters (Customized Settings)”.

Uncheck the “DKIM_Hardfail_Copy” and Check the “DKIM_Hardfail_Original”.

Click *Submit* and *Commit* changes.

Step 3: Create a new Incoming Mail Flow Policy for Your Domain (Spoof Protection)

The steps in this section will allow you take action on Incoming email that has a From email address of your own domain and that are failing SPF verification. Of course this relies on you having already published your SPF Text Record in DNS. Skip these steps if you have not created/published a SPF Text Resource record for your domain.

Navigate to: *Mail Policies > Incoming Mail Policies*

Click the Add Policy button.

Enter the Name: Spoof_Protection

Click “Add User...” button.

ESA Incoming and Outgoing Content Filters - Best Practices

The next configuration panel lets you define what messages will match this new Incoming Mail Policy row. You only want to define criteria for the Sender (which is the left portion of the configuration panel).

Click “*Following Senders*” radio button and then enter your domain in the “Email Address:” text box. For me, my domain is “@unc-hamiltons.com”

Click *Submit*.

You are presented with the *Incoming Mail Policies* table again but now you have a second new Mail Policy row above the *Default Policy*.

Click the *(use default)* hypertext in the Content Filters cell for the new row.

Flip the pulldown menu to “*Enable Content Filters (Customized Settings)*”.

Check the “*Spoof_SPF_Failures*” also ensure both *DKIM_Hardfail_Copy* and *DKIM_Hardfail_Original* are not checked.

Click *Submit* and *Commit* changes.

The *Incoming Mail Policies* table should now look like this:

| 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 | |

STEP 4: CREATING THE OUTGOING CONTENT FILTERS

Navigate to: *Mail Policies > Outgoing Content Filters*

Here is a table of Outgoing Content Filters you should create.

Create these Outgoing Content Filters:

| Create these Outgoing Content Filters |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Name: Bank_Data</p> <p>Add Two Conditions:</p> <ul style="list-style-type: none">Message Body or Attachment:<ul style="list-style-type: none">Contains Smart Identifier: ABA Routing NumberContains Smart Identifier: Credit Card Number <p>Add One Action:</p> <ul style="list-style-type: none">Quarantine:<ul style="list-style-type: none">Send message to quarantine: “Bank Data Outbound (centralized)”Duplicate message: Enabled <p>(Note the Apply Rule should be “If one or more conditions match”)</p> |
| <p>Name: SSN</p> <p>Add One Condition:</p> <ul style="list-style-type: none">Message Body or Attachment:<ul style="list-style-type: none">Contains Smart Identifier: Social Security Number (SSN) <p>Add One Action:</p> <ul style="list-style-type: none">Quarantine:<ul style="list-style-type: none">Send message to quarantine: “SSN Outbound (centralized)”Duplicate message: Enabled |
| <p>Name: Inappropriate</p> <p>Add Two Conditions:</p> <ul style="list-style-type: none">Message Body or Attachment:<ul style="list-style-type: none">Contains term in dictionary: ProfanityContains term in dictionary: Sexual_Content <p>Add One Action:</p> <ul style="list-style-type: none">Quarantine:<ul style="list-style-type: none">Send message to quarantine: “Inappropriate Outbound (centralized)”Duplicate message: Enabled |

Create these Outgoing Content Filters

Name: URL_Category

Add One Condition:

URL Category:

Select Categories:

Adult, Dating, Filter Avoidance, Freeware and Shareware, Gambling,
Games, Hacking, Lingerie and Swimsuits, Non-sexual Nudity,
Parked Domains, Peer File Transfer, Pornography

Add One Action:

Quarantine:

Send message to quarantine: "URL Category Outbound (centralized)"

Duplicate message: Enabled

Name: URL_Malicious

Add One Condition:

URL Reputation:

URL Reputation is: Malicious (-10.0 to -6.0)

Add One Action:

Quarantine:

Send message to quarantine: "URL Malicious Outbound (centralized)"

Duplicate message: Disabled (**** Quarantine the Original ****)

Name: Password_Protected

Add One Condition:

Attachment Protection: One or more attachments are protected

Add One Action:

Quarantine:

Send message to quarantine: "Pwd Protected Outbound (centralized)"

Duplicate message: Enabled

Name: Size_10M

Add One Condition:

Message Size is:

Greater than or equal to: 10M

Add One Action:

Add Message Tag:

Enter a Term: NOOP

(Note: There must be some action so here we "Tag" the message to represent no operation taken. The fact that the content filter was "Matched" will allow it to show up in reporting. No "Action" need be taken for it to show in Reporting.)

ESA Incoming and Outgoing Content Filters - Best Practices

Create these Outgoing Content Filters

Name: Proprietary

Add One Condition:

Message Body or Attachment:

Contains term in dictionary: Proprietary

Add One Action:

Quarantine:

Send message to quarantine: "Proprietary (centralized)"

Duplicate message: Enabled

Because the *"Policies"* function is selected (you'll see the *Polices* hypertext at the top middle) the middle column shows the *Outgoing Mail Policies* the *Content Filter* has been applied to. Because we have not applied them to any *Outgoing Mail Policy*, the *"Not in use"* is displayed.

Navigate to: *Mail Policies > Outgoing Mail Policies*

Click on the *"Disabled"* text in the Content Filters cell for the *Default Policy*.

The pull-down menu button is set to *"Disable Content Filters"*. Click the button and set to *Enable Content Filters* and you will immediately be presented with all Outgoing Content Filters that have been created. Enable all filters.

Submit and Commit

NEXT STEPS AND SUMMARY

You have now implemented initial Best Practices for Incoming and Outgoing Content Filters. Most (not all) Content Filters used the Quarantine Action and elected to check (Enable) “*Duplicate message*” option — which merely places a copy of the Original Email and did not prevent the email from being delivered. The intent of these Content Filters is to allow you to gather information about the types of emails flowing Inbound and Outbound to your company.

Having said that, after running the Content Filters report and looking over the email copies saved in the quarantines, it may be prudent to un-check the “*Duplicate message*” checkbox option and thereby start placing the original email into the quarantine instead of a copy/duplicate.