CISCO EMAIL SECURITY APPLIANCE

URL FILTERING

September 2015
Version 1.3

Tobias Mayer

Consulting Systems Engineer

The most current version of this document can be found here:
https://cisco.com/go/emailsecurity-customer

Contents

PURPOSE OF THIS DOCUMENT

The Integration of URL Filtering on the Email Security Appliance (ESA) is expanding the capabilities of email security beyond traditional Anti Spam technology. This Document will show how to activate the feature and where in the ESA it is used.

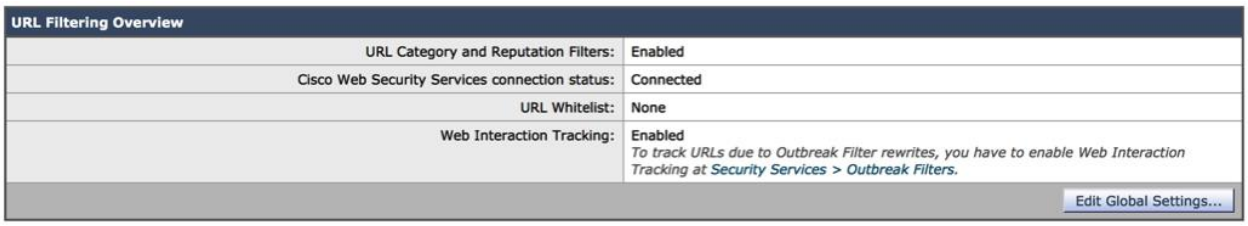
OVERVIEW OF STEPS

This document will provide the steps necessary for you to implement some Best Practices for URL Filtering on the ESA. We will first show how and where in the email pipeline the URL Filtering feature is activated and give some practical examples how to use it and how to combine it with existing filtering criteria.

STEP 1: ACTIVATING URL FILTERING

URL Filtering is a feature that comes with the license of Web Security Essentials and is technically included as a function in the Outbreak Filter.
If you do not have a license for Web Security Essentials (with Outbreak Filter), you will not be able to use this feature!

To activate you need to go to “Security Services” -> “URL Filtering” first.

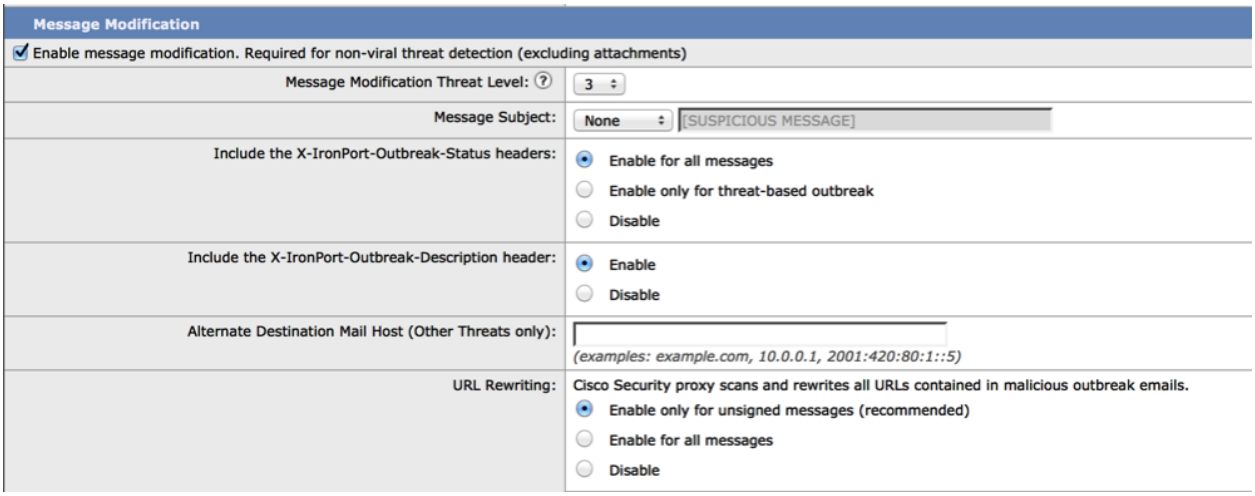


If you have successfully activated the feature , it will show “Connected” in the connection status. This means that the appliance could connect to the Talos Cloud and get the latest Updates on URL categories and URL reputation.

By default, the URL Filtering goes across all URL, but you have the possibility to “whitelist” certain URL. This can be useful for internal domains and URL, that will of course not have a reputation score or a URL Category.

STEP 2: USING URL FILTERING AND MODIFICATION IN OUTBREAK FILTER

The first place to use URL Filtering will be the Outbreak Filter.
Go to your mail policies and click on the Outbreak Filter Tab in the policies:



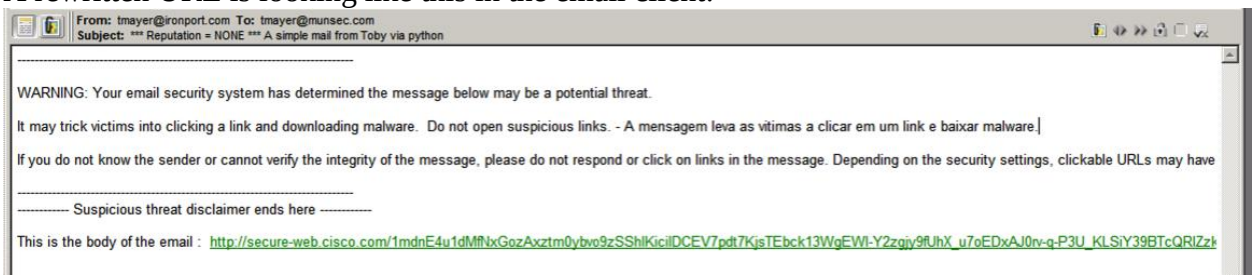
Click on the the “Enable Message Modification” button. Outbreak Filter will now scan URL within Emails.

Outbreak Filter will only scan emails that are considered a “Threat”. The Threat level is set to 3 and above by default, see screenshot

The two sections on “Include Headers” is recommended to be activated. This allows later to track certain messages and determine how Outbreak Filter was treating them.

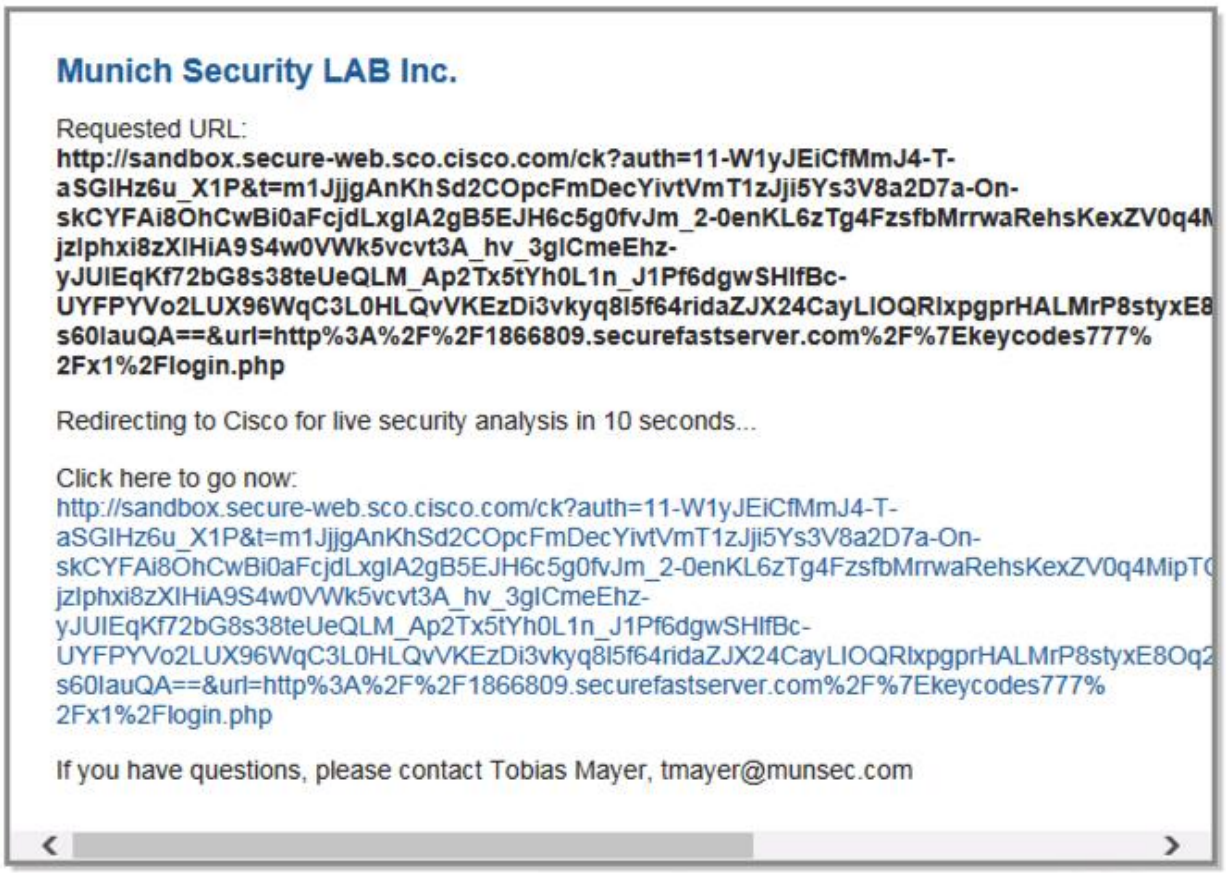
The next important setting is the URL rewriting. Outbreak Filter has the option to “rewrite” a URL. This means, that the URL is no longer pointing directly to the destination but will now be redirected over the Cisco Cloud Web Security Proxy.

A rewritten URL is looking like this in the email client:

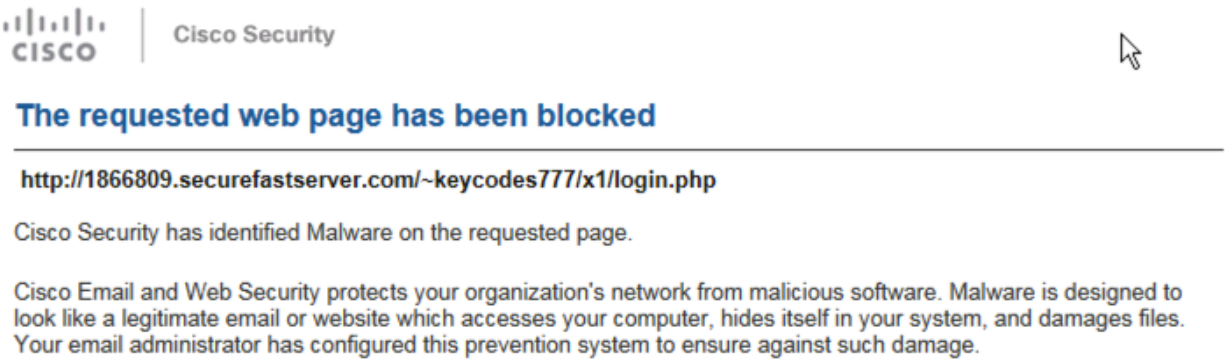


It is recommended to rewrite only URLs that are not signed. If a URL is digitally signed, the rewriting would make the signature no longer valid.

What happens if the user clicks on the URL?
If the user clicks on the URL he will be redirected to the Cloud Web Security Proxy:



The URL is sandboxed and scanned for any malicious content.
If the URL is malicious, the request is blocked:

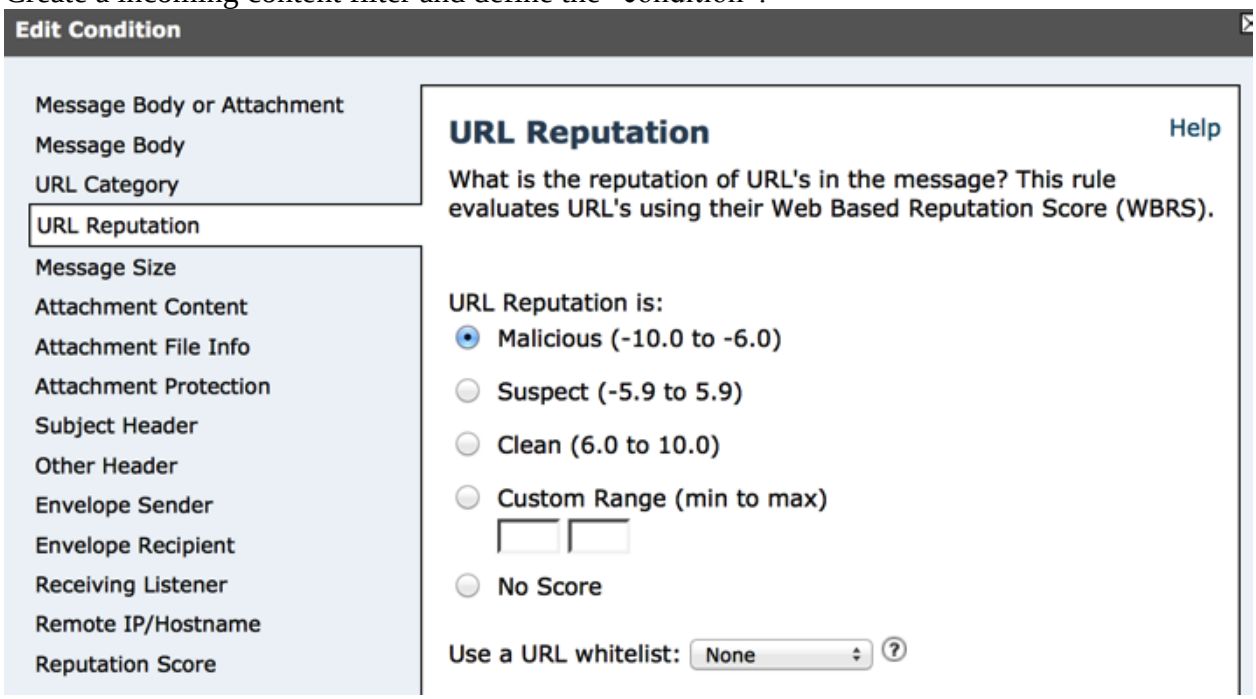


STEP 3: USING URL FILTERING AND MODIFICATION IN MESSAGE & CONTENT FILTERS

URL Filtering can also be used in the various filters on the ESA.

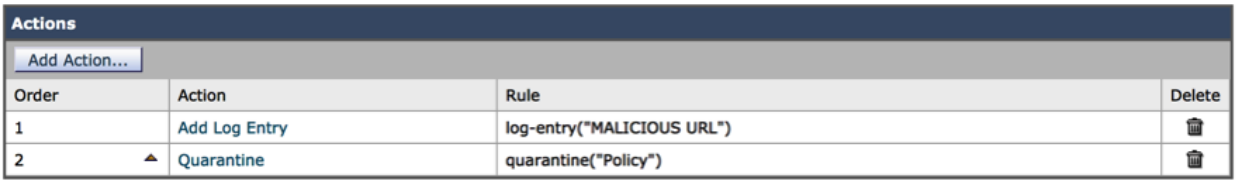
A simple and effective way to use them is shown in this example:
"If a URL has a Web Reputation lower than -6, quarantine the email and log a message"

Create a incoming content filter and define the "condition":



Next step, define the action. You have a full range of actions. You can drop the message, put it in quarantine or take action on the link directly.

In this example we want to log a message and also put the email in quarantine. Our "action" in the filter looks like this:



Now the filter is ready for use and can be applied to a mail policy.

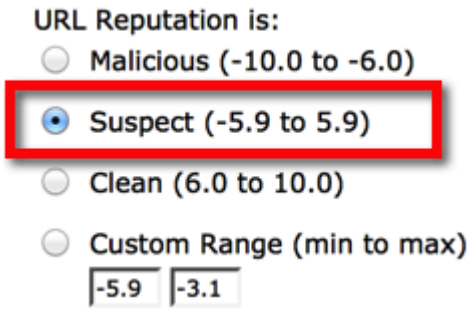
The same result can be achieved through a message filter, the syntax would look like this:

```
Enforce_Web_Reputation:
If url-reputation(-10,-6)
{
 log-entry('MALICIOUS URL');
 quarantine ("Policy");
}
```

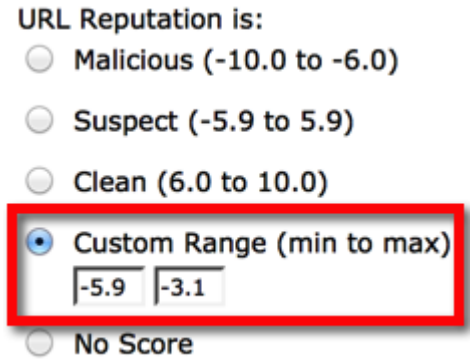
From the CLI, go to “filters” and choose “NEW”. Then, copy or type in the filter above and end the input with a single “.”

Note:

In the URL Reputation Condition there is a Section called “Suspect URL”. Due to a recent change in our Talos Backend Cloud, the “Suspect Range” is no longer from -5.9 to 5.9 as shown here.

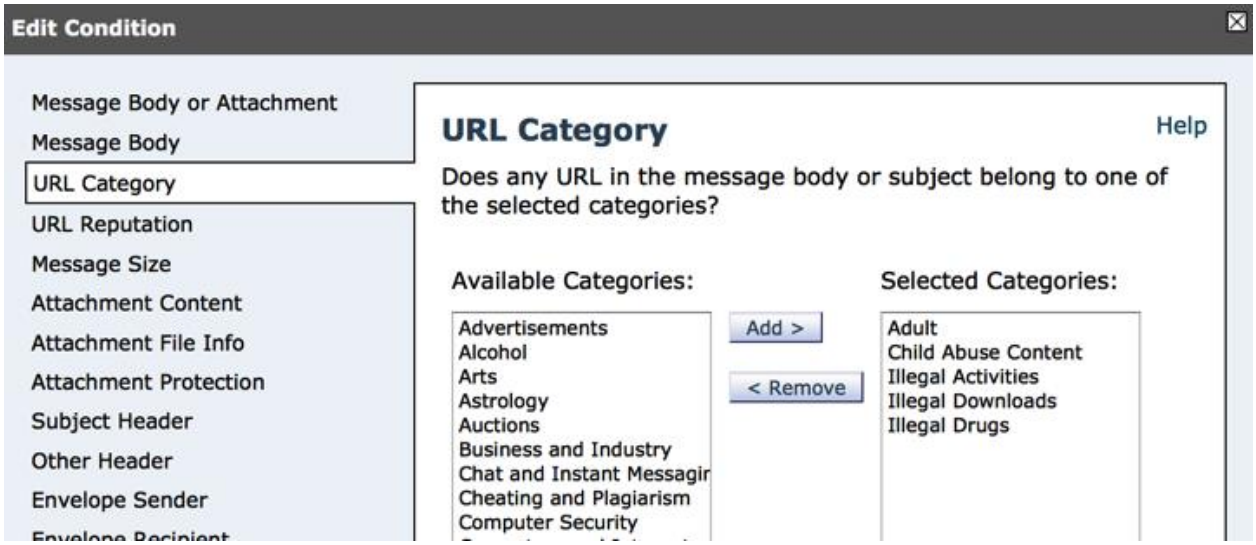


Instead, use a custom range from -5.9 to -3.1 to mark “suspect URLs”

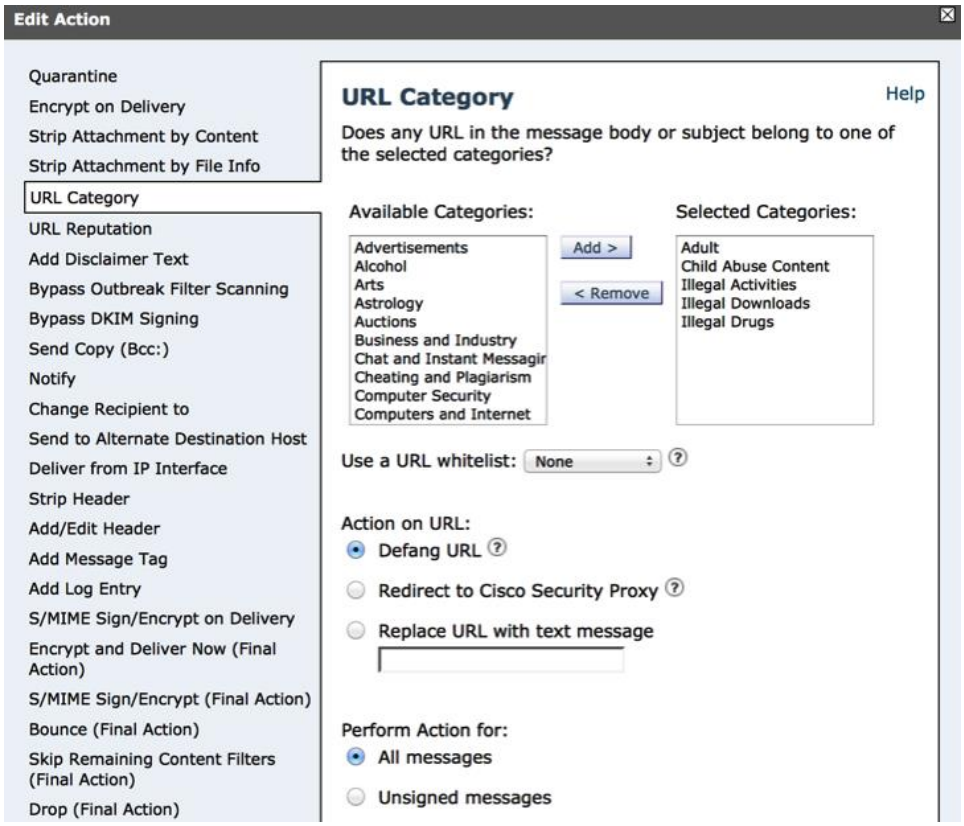


The filters can also work based on URL Categories. For example, you can block emails with unwanted Categories. In this example we select a few Categories in our Content Filter and make the URL no longer clickable.

Define a “Condition”:

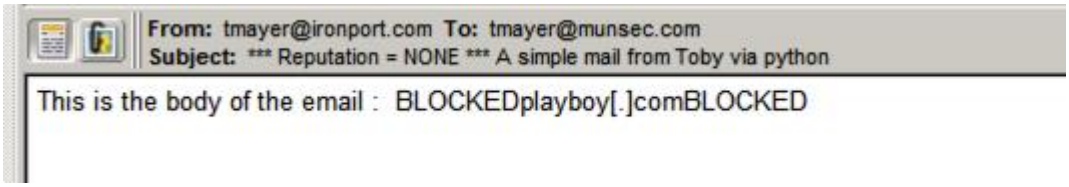


And then define an “Action”:



In this Example we define an Action of “Defang”.

Defang means, the HTML part of the URL is “destroyed” but still visible. It will look like this in the message:



The User can see the URL but can no longer click on them.

STEP 4: WHITELISTING URLS

There are two ways of whitelisting URLs that you do not want to be scanned. You can whitelist them globally or use dedicated whitelist per content filter.

The place to globally whitelist URLs is in “Security Services” -> “URL Filtering”.

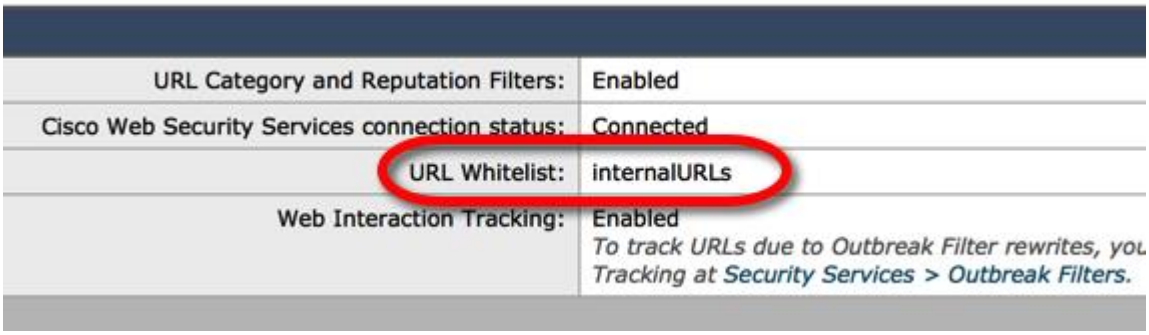
Go to “Mail Policies” -> “URL Lists” and create first a URL List.

Enter the desired URLs to be whitelisted.

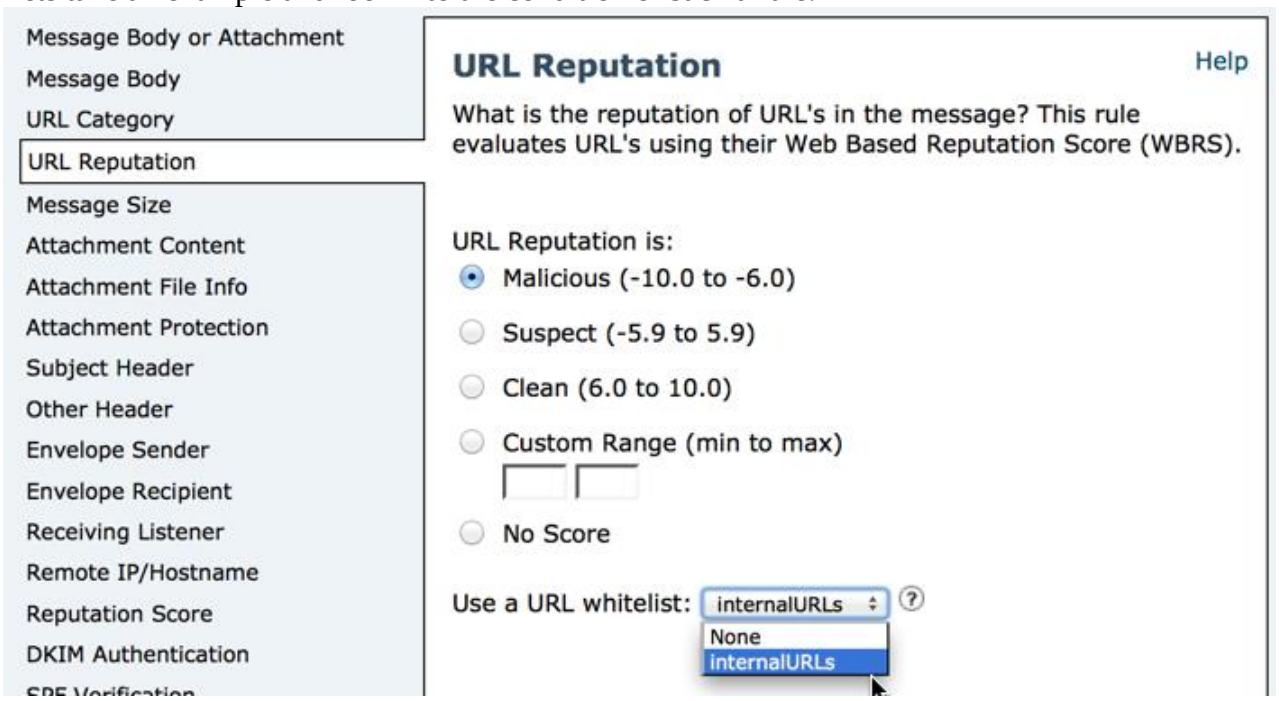
The following formats are allowed:

- Hostnames such as "example.com", "10.1.1.1" or "2001:db8:85a3:8d3:1319:8a2e:370:7348"
- Hostnames with wildcard '*' such as
- "example.com/*" or "example.com/path/*"
- "10.1.1.1/*" or "10.1.1.1/path/*"
- "2001:db8:85a3:8d3:1319:8a2e:370:7348/*" or "2001:db8:85a3:8d3:1319:8a2e:370:7348/path/*"
- Partial hostnames with wildcard '*', such as
- "*.example.com"
- "*.example.com/*"
- "*.example.com/path/*"

Apply the global URL list in the URL SECURITY SERVICE, in this example we called the URL list “internalURLs”



The second place to whitelist is within the Condition Component in the Content Filter Rule. Lets take an example and look into the condition of such a rule:



This is a condition filtering on malicious url. If you want to make sure that some URLs are never filtered you can apply a URL whitelist within this condition by selecting it in the drop down menu.

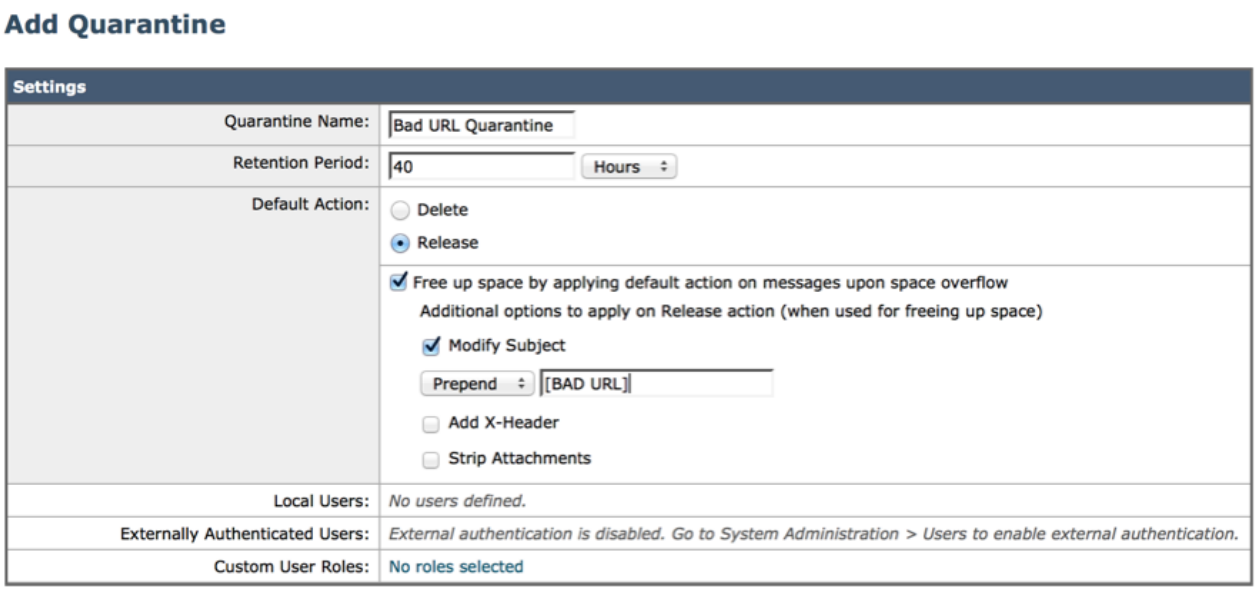
This function applies to the conditions “URL Category” and “URL Reputation.”

STEP 5: RECOMMENDED FILTERS

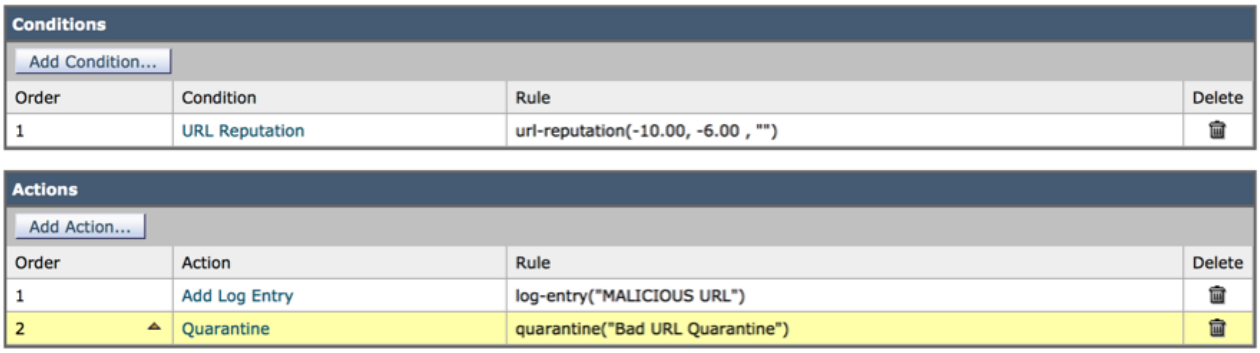
There are some filters that are recommended to use, here are some interesting definitions:

- Quarantine Emails with Bad URLs
  - If url reputation is malicious, Quarantine the email and log a message in the mail_logs

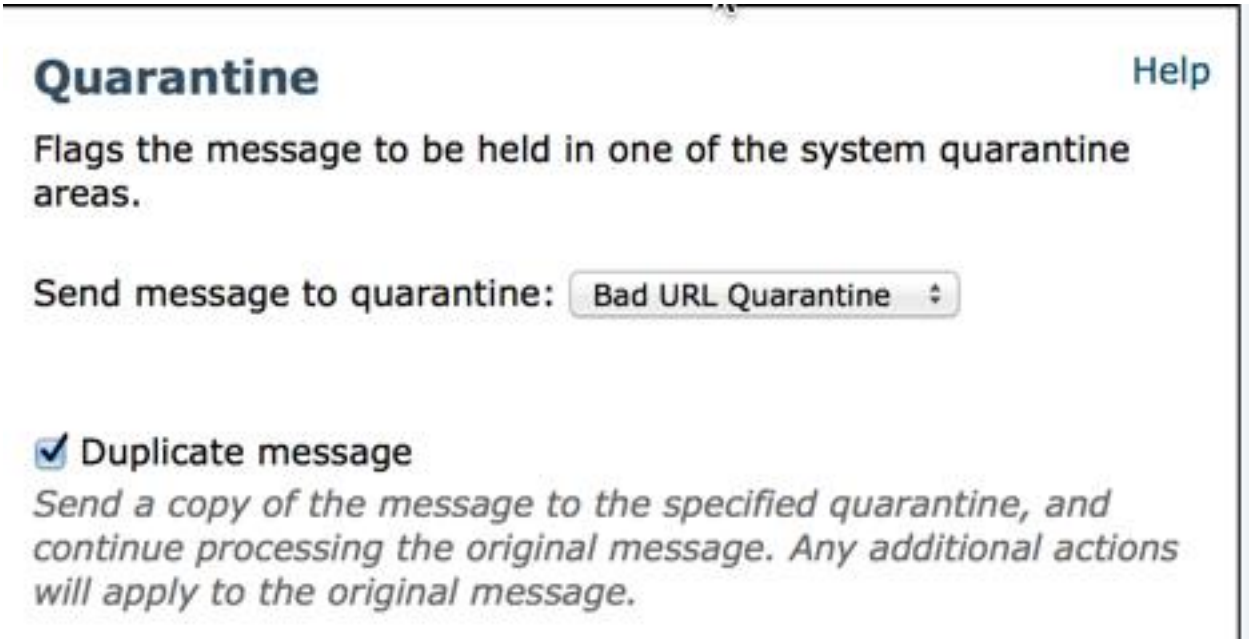
It is a good best Practice that you create a separate quarantine for different messag types. To do so, go to “Monitoring” -> “Policy, Virus and Outbreak Quarantines” and add a new Quarantine. Here, we call it “Bad URL Quarantine”:



In our Rule, we reference the newly created Quarantine.



Note:
If you are very cautious to now block any mail, you can send a copy of the email to the quarantine while delivering the original email to the sender. This is done by selecting the "Duplicate message" button in the "quarantine" action:



- Quarantine Emails with unwanted Categories
  - If url category is XYZ, put message in Quarantine and log a message in the mail_logs

Conditions

Add Condition...

Order	Condition	Rule	Delete
1	URL Category	url-category (['Adult', 'Child Abuse Content', 'Illegal Activities', 'Illegal Downloads', 'Illegal Drugs'], "internalURLs")	

Actions

Add Action...

Order	Action	Rule	Delete
1	Add Log Entry	log-entry("Unwanted URL Category detected")	
2	Quarantine	quarantine("Policy")	

- Modify Subject Header and Log , if message has No Web Reputation Score, no URL Category and Sender has no Email Reputation Score, modify the Subject and defang the URL.

Conditions

Add Condition... | Apply rule: Only if all conditions match

Order	Condition	Rule	Delete
1	URL Category	url-category (['Uncategorized URLs'], "")	
2	URL Reputation	url-no-reputation("")	
3	Reputation Score	no-reputation	

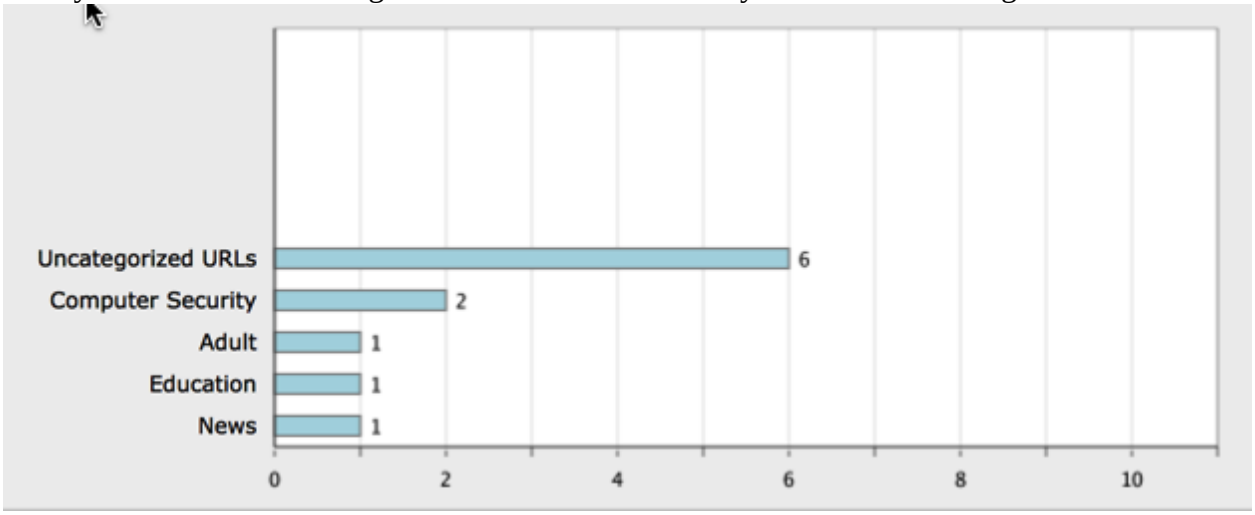
Actions

Add Action...

Order	Action	Rule	Delete
1	Add Log Entry	log-entry("Uncategorized URL from unknown Sender Detected")	
2	Add/Edit Header	edit-header-text("Subject", "(.*)", "[SUSPICIOUS URL INSIDE]\\1")	
3	URL Category	url-category-defang (['Uncategorized URLs'],"",0)	

STEP 6: REPORTING

After the URL Filtering is enabled and filters are defined, there are several reports that you can access.
First place is the dedicated report in the URL filters under Monitoring -> URL Filter
Here you can see which categories of URLs are inside of your received messages:



Further statistics tell you about the amount of malicious URLs:

Summary of Incoming Messages Containing Malicious and Suspicious URLs

Reputation	Messages
Messages with Malicious URLs	9
Messages with Suspicious URLs	9

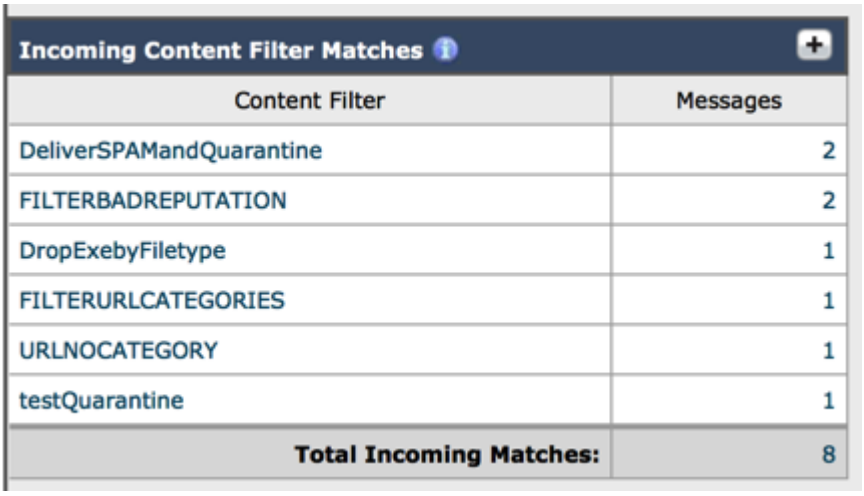
In the far left column, you have a link that leads to the “Message Tracking” of the messages that are listed here.

Another statistic tells you about the Top URLs that were contained in detected Spam messages:

Summary of Top URLs in Incoming Spam Messages

URL	Messages
1866809.securefastserver.com	5
ihaveabadreputation.com	2
lifescience.sysu.edu.cn	1
plcture-store.com	1

Beside the dedicate URL filtering report, you have of course also reports on message and content filters:



Incoming Content Filter Matches

Content Filter	Messages
DeliverSPAMandQuarantine	2
FILTERBADREPUTATION	2
DropExebyFiletype	1
FILTERURLCATEGORIES	1
URLNOCATEGORY	1
testQuarantine	1
Total Incoming Matches:	8

Note:

A good best practice to start with, is to define the filters and put as an “Action” only the “Log Entry”. Messages will not be blocked but still you will get the reports. This can be useful to determine what categories you have in the emails, what reputation they have, if they contain malicious URLs, etc. And at the same time, do not impact your traffic flow.
