Understand the URL Defang and Redirect Action on the Secure Email Gateway

Contents

Introduction

This document describes the difference between defang and redirect actions used in the URL filter, and how to use the available rewrite option for the href attribute and text.

Prerequisites

Requirements

To take action based on URL reputation, or to enforce acceptable use policies with the message and content filters, the Outbreak Filters feature must be enabled globally.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Email Gateway
- Outbreak Filters
- Content and Message Filters

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

One of the URL filtering feature capabilities is to take action based on the URL reputation or category with the use of message and/or content filters. Based on the URL scan result (URL-Related Condition), one of the three available actions on an URL can be applied:

- Defang URL
- Redirect to Cisco Security Proxy
- Replace URL with the text message

The focus of this document is to explain the behavior between the Defang and Redirect URL options. It also provides a brief description and explanation of the URL Rewrite capabilities of non-viral threat detection of an Outbreak Filter.

Message Sample

The sample message used in all the tests is the MIME multipart/alternative type of message and includes both text/plain and text/html parts. Those parts are usually generated automatically by email software and contain the same kind of content formatted for HTML and non-HTML receivers. For this, the content of text/plain and text/html was manually edited.

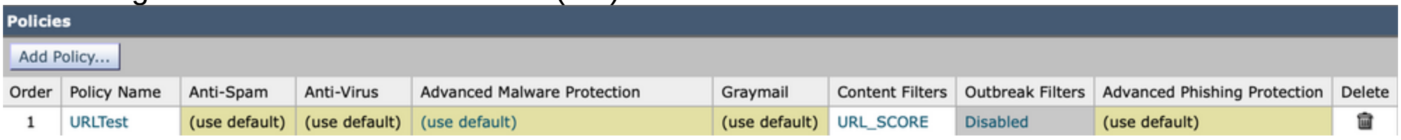
```
Content-Type: multipart/alternative; boundary="===============7781793576330041025==" MIME-
Version: 1.0 From: admin@example.com Date: Mon, 04 Jul 2022 14:38:52 +0200 To: admin@cisco.com
Subject: Test URLs --===============7781793576330041025== Content-Type: text/plain; charset="us-
ascii" MIME-Version: 1.0 Content-Transfer-Encoding: 7bit This is text part of the message Link1:
http://malware.testing.google.test/testing/malware/ and some text Link2: http://cisco.com and
some text --===============7781793576330041025== Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0 Content-Transfer-Encoding: 7bit <html> <head></head> <body> <p>This is an HTML
part of the message</p> <p>Link1: <a
href="http://malware.testing.google.test/testing/malware/">http://malware.testing.google.test/te
sting/malware/</a> and some text</p> <p>Link2: <a
href="http://malware.testing.google.test/testing/malware/">CLICK ME</a> some text</p> <p>Link3:
http://malware.testing.google.test/testing/malware/ and some text</p> <p>Link4: http://cisco.com
and some text</p> </body> </html> --===============7781793576330041025==--
```

Part I - Defang

Configurations

In the first part the configuration uses:

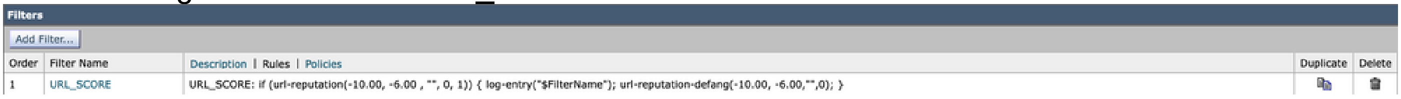
- Mail Policy with default Anti-Spam (AS)/ Anti-Virus (AV)/ Advanced Malware Protection (AMP) configuration and Outbreak Filters (OF) disabled



Policies

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete
1	URLTest	(use default)	(use default)	(use default)	(use default)	URL_SCORE	Disabled	(use default)	🗑

- Incoming Content Filter: URL_SCORE content filter enabled



Filters

Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	URL_SCORE	URL_SCORE: if (url-reputation(-10.00, -6.00 , "", 0, 1)) { log-entry("$FilterName"); url-reputation-defang(-10.00, -6.00,"",0); }	⧉	🗑

The content filter uses the URL reputation condition to match Malicious URLs, the ones that score between -6.00 and -10.00. As an action, the content filter name is logged and the defang action **url-reputation-defang** is taken.

Defang Action

It is important to clarify what is a defang action. The user guide provides an explanation; Defang a URL so that it is unclickable. Message recipients can still see and copy the URL.

Scenario A

Outbreak Filter non-viral threat detection	No
Content Filter Action	Defang
websecurityadvancedconfig href and text rewrite is enabled	No

This scenario explains the result of the defang action configured with default settings. In the default setting, the URL is rewritten when only the HTML tags are stripped. Take a look at an HTML paragraph with some URLs inside:

```
<p>Link1: <a
href="http://malware.testing.google.test/testing/malware/">http://malware.testing.google.test/te
sting/malware/</a> and some text</p> <p>Link2: <a
href="http://malware.testing.google.test/testing/malware/">CLICK ME</a> some text</p> <p>Link3:
http://malware.testing.google.test/testing/malware/ and some text</p>
```

In the first two paragraphs, the URL is represented by a proper HTML A-tag. The <A> element includes the **href=** attribute that is enclosed in the tag itself and indicates the link destination. The content within the tag elements can also indicate the link destination. This **text form** of the link can include the URL. The first Link1 includes the same URL link in both href attribute and text part of the element. It can be noticed that those URLs can be different. The second Link2 includes the proper URL only inside the href attribute. The last paragraph does not include any A-elements.

> **Note**: The correct address can always be seen when you move the cursor over the link or when you view the source code of the message. Unfortunately, the source code cannot be easily found with some popular email clients.

Once the message is matched by the URL_SCORE filter, the malicious URLs are defanged. When URL logging is enabled with the **OUTBREAKCONFIG** command the scores and URLs can be found in mail_logs.

```
Mon Jul 4 14:46:43 2022 Info: MID 139502 URL http://malware.testing.google.test/testing/malware/
has reputation -9.4 matched Cond tion: URL Reputation Rule Mon Jul 4 14:46:43 2022 Info: MID
139502 Custom Log Entry: URL_SCORE Mon Jul 4 14:46:43 2022 Info: MID 139502 URL
http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Acti n: URL
defanged Mon Jul 4 14:46:43 2022 Info: MID 139502 URL
http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Acti n: URL
defanged Mon Jul 4 14:46:43 2022 Info: MID 139502 URL
http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Acti n: URL
defanged Mon Jul 4 14:46:43 2022 Info: MID 139502 rewritten to MID 139503 by url-reputation-
defang-action filter 'URL_SCORE'
```

This results in the rewritten message:

```
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version:
1.0 Content-Transfer-Encoding: 7bit <html> <head></head> <body> <p>This is an HTML part of the
message</p> <p>Link1: http://malware.testing.google.test/testing/malware/ and some text</p>
<p>Link2: CLICK ME some text</p> <p>Link3: http://malware.testing.google.test/testing/malware/
and some text</p> <p>Link4: http://cisco.com and some text</p> </body> </html> --
===============7781793576330041025==--
```

The result of the defang action taken on the text/html part of the MIME message is a stripped A-tag and the tag content is left untouched. In the two first paragraphs, both links were defanged where the HTML code was stripped and the text part of the element was left. The URL address in the first paragraph is the one from the text part of the HTML element. It must be noted the URL address from the first paragraph is still visible after the defang action was taken but without the HTML A-tags, the element must not be clickable. The third paragraph is not defanged as the URL address here is not placed between any A-tags, and is not considered as a link. Perhaps it is not desirable behavior because of two reasons. First, the user can easily see and copy the link and execute it in the browser. The second reason is that some email software tends to detect a valid form of URL inside of the text and make it a clickable link.

Let us have a look at the text/plain part of the MIME message. The text/plain part includes two URLs in the text form. The text/plain is displayed by MUA which does not understand the HTML code. In most modern email clients you do not see the text/plain parts of the message unless you intentionally configured your email client to do so. Usually, you need to check the source code of the message, a raw EML format of the message to see and investigate the MIME parts.

The listing here shows URLs from the text/plain part of the source message.

```
Link1: http://malware.testing.google.test/testing/malware/ and some text Link2: http://cisco.com
and some text
```

One of those two links got a malicious score and was defanged. By default, the defang action taken on the text/plain part of the MIME type has a different outcome than on the text/html part. It is between BLOCKED words and all dots between square brackets.

```
--===============7781793576330041025== Content-Type: text/plain; charset="us-ascii" MIME-
Version: 1.0 Content-Transfer-Encoding: 7bit This is text part of the message Link1:
BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLOCKED and some text Link2:
http://cisco.com and some text --===============7781793576330041025==
```

Sum Up:

- Defang run on the TEXT/PLAIN part rewrites the URL into BLOCKED blocks
- Defang run on the TEXT/HTML part rewrites the URL from an HTML A-tag when the A-tag is stripped without the text between A-tags touched, that can also be an URL address

Scenario B

Outbreak Filter non-viral threat detection	No
Content Filter Action	Defang
websecurityadvancedconfig href and text rewrite is enabled	Yes

This scenario provides information on how the behavior of the defangs action changes after the use of one of the websecurityadvancedconfig options. The websecurityadvancedconfig is the machine-level specific CLI command that allows to tune settings specific to URL scan. One of the settings here allows you to change the default behavior of the defang action.

```
> websecurityadvancedconfig Enter URL lookup timeout in seconds: [15]> Enter the maximum number
of URLs that can be scanned in a message body: [100]> Enter the maximum number of URLs that can
be scanned in the attachments in a message: [25]> Do you want to rewrite both the URL text and
the href in the message? Y indicates that the full rewritten URL will appear in the email body.
N indicates that the rewritten URL will only be visible in the href for HTML messages. [N]> Y
...
```

In the fourth question, **Do you want to rewrite both the URL text and the href in the message? ..**, the answer **Y** indicates that in the case of the HTML-based MIME part of the message all URL strings that match no matter if found in the href attribute of the A-tag element, it is text part or outside of any elements that are rewritten. In this scenario the same message is resent, but with a slightly different outcome.

Take a look at the text/html MIME part code with the URLs once again and compare it with the HTML code processed by the email gateway.

```
<p>Link1: <a
href="http://malware.testing.google.test/testing/malware/">http://malware.testing.google.test/te
sting/malware/</a> and some text</p> <p>Link2: <a
href="http://malware.testing.google.test/testing/malware/">CLICK ME</a> some text</p> <p>Link3:
http://malware.testing.google.test/testing/malware/ and some text</p> <p>Link4: http://cisco.com
and some text</p>
```

When href and text rewrite option is enabled all matched by the filter URLs are defanged no matter whether the URL address is part of the href attribute or text part of the A-tag HTML element, or is found in another part of the HTML document.

```
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version:
1.0 Content-Transfer-Encoding: 7bit <html> <head></head> <body> <p>This is an HTML part of the
message</p> <p>Link1: BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLOCKED and some
text</p> <p>Link2: CLICK ME some text</p> <p>Link3:
BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLOCKED and some text</p> <p>Link4:
http://cisco.com and some text</p> </body> </html> --===============7781793576330041025==--
```

The defanged URLs are now rewritten when the A-tag element is stripped together with a rewrite of the text part of the link when it matches the URL format. The rewritten text part is done in the same way as in the text/plain part of the MIME message. The item is placed between BLOCKED words and all dots are placed between square brackets. This prevents the user to copy and paste the URL, and some email software clients make the text clickable.

Sum Up:

- Defang run on the TEXT/PLAIN part rewrites the URL into BLOCKED blocks

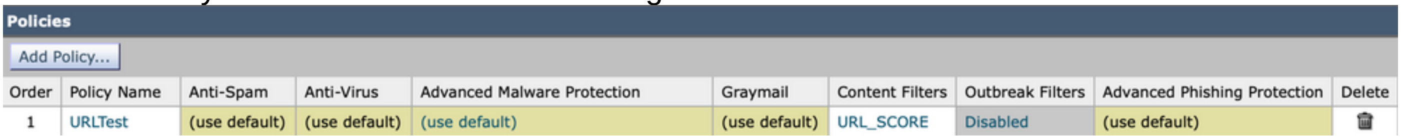
- Defang run on the TEXT/HTML part rewrites the URL from an HTML A-tag when an A-tag is stripped
- Defang run on the TEXT/HTML part rewrites all URL strings that match into BLOCKED blocks

Part II - Redirect

Configurations

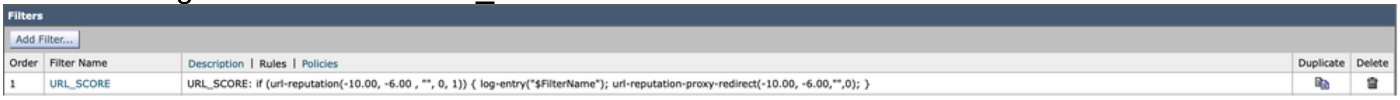
In the second part the configuration uses:

- Mail Policy with default AS/AV/AMP configuration and OF disabled



Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete
1	URLTest	(use default)	(use default)	(use default)	(use default)	URL_SCORE	Disabled	(use default)	🗑

- Incoming Content Filter: URL_SCORE content filter enabled



Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	URL_SCORE	URL_SCORE: if (url-reputation(-10.00, -6.00 , "", 0, 1)) { log-entry("$FilterName"); url-reputation-proxy-redirect(-10.00, -6.00,"",0); }	⧉	🗑

The content filter uses the URL reputation condition to match Malicious URLs, the ones which score between -6.00 and -10.00. As an action, the content filter name is logged and the **redirect action** is taken.

Redirect Action

Redirect to Cisco Security Proxy service for click-time evaluation allows the message recipient to click the link and be redirected to a Cisco web security proxy in the cloud, which blocks access if the site is identified as malicious.

Scenario C

Outbreak Filter non-viral threat detection	No
Content Filter Action	Redirect
websecurityadvancedconfig href and text rewrite is enabled	No

This scenario is very similar in behavior to Scenario A from the first part with the difference made in the content filter action to redirect the URL instead of defang it. The websecurityadvancedconfig settings are restored to default settings, which means the **"Do you want to rewrite both the URL text and the href in the message? ..** is set to **N.**

The email gateway detects and evaluates each of the URLs. The malicious score triggers the URL_SCORE content filter rule and takes the action **url-reputation-proxy-redirect-action**

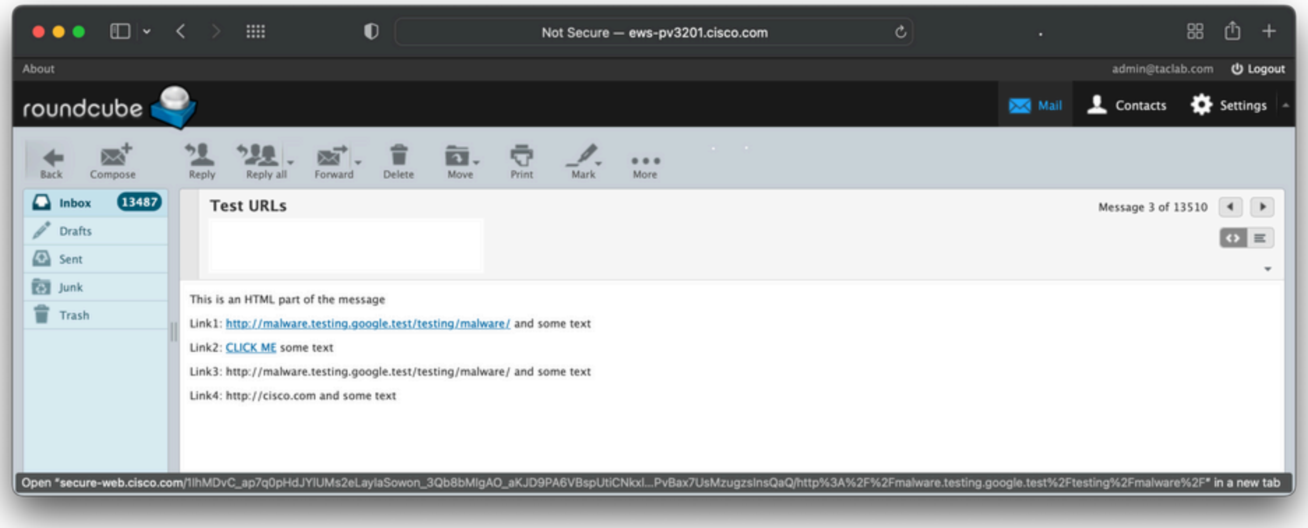
```
Tue Jul 5 12:42:19 2022 Info: MID 139508 URL http://malware.testing.google.test/testing/malware/
has reputation -9.4 matched Condition: URL Reputation Rule Tue Jul 5 12:42:19 2022 Info: MID
139508 Custom Log Entry: URL_SCORE Tue Jul 5 12:42:19 2022 Info: MID 139508 URL
http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL
redirected to Cisco Security proxy Tue Jul 5 12:42:19 2022 Info: MID 139508 URL
```

```
http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL
redirected to Cisco Security proxy Tue Jul 5 12:42:19 2022 Info: MID 139508 URL
http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL
redirected to Cisco Security proxy Tue Jul 5 12:42:19 2022 Info: MID 139508 rewritten to MID
139509 by url-reputation-proxy-redirect-action filter 'URL SCORE'
```

Take a look at how the URLs are rewritten in the HTML part of the message. Same as in Scenario A only the URLs found in the href attribute of an A-tag element are rewritten and URL addresses found in the text part of the A-tag element are skipped. With a defang action an entire A-tag element is stripped but with a redirect action the URL in the href attribute is rewritten.

```
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version:
1.0 Content-Transfer-Encoding: 7bit <html> <head></head> <body> <p>This is an HTML part of the
message</p> <p>Link1: <a href="http://secure-
web.cisco.com/1IhMDvC_ap7q0pHdJYlUMs2eLayIaSowon_3Qb8bMIgAO_aKJD9PA6VBspUtiCNkxlKc5eJlNhOtEfr39J
CzxxvtcBL1Afs_iV01OL_vXFE30zOmEEVYX8djFTJ1T9seDtxmxF8beciVywF2xlokkRSP8SolTEtSJyveaHblr8uI4gcXBU
rhul0C3rfjHzH92GySnz9Fh7Waj8cv67P7WHi4qCTYzzEXbGh4DXbIig8VD6PHCMsezaN-
79nWaAy6GeFPvBax7UsMzugzsInsQaQ/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F"
>http://malware.testing.google.test/testing/malware/</a> and some text</p> <p>Link2: <a
href="http://secure-
web.cisco.com/1IhMDvC_ap7q0pHdJYlUMs2eLayIaSowon_3Qb8bMIgAO_aKJD9PA6VBspUtiCNkxlKc5eJlNhOtEfr39J
CzxxvtcBL1Afs_iV01OL_vXFE30zOmEEVYX8djFTJ1T9seDtxmxF8beciVywF2xlokkRSP8SolTEtSJyveaHblr8uI4gcXBU
rhul0C3rfjHzH92GySnz9Fh7Waj8cv67P7WHi4qCTYzzEXbGh4DXbIig8VD6PHCMsezaN-
79nWaAy6GeFPvBax7UsMzugzsInsQaQ/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F"
>CLICK ME</a> some text</p> <p>Link3: http://malware.testing.google.test/testing/malware/ and
some text</p> <p>Link4: http://cisco.com and some text</p> </body> </html> --
===============7781793576330041025==--
```

As a result, the email client displays two active links: Link1 and Link2, both point to the Cisco Web Security Proxy service but the message displayed in the email client displays the text part of the A-tag which is not rewritten by default. To better under this please take a look at the output from the webmail client that displays the text/html part of the message.



Test URLs

This is an HTML part of the message

Link1: http://malware.testing.google.test/testing/malware/ and some text

Link2: CLICK ME some text

Link3: http://malware.testing.google.test/testing/malware/ and some text

Link4: http://cisco.com and some text

Open "secure-web.cisco.com/1IhMDvC_ap7q0pHdJYlUMs2eLaylaSowon_3Qb8bMIgAO_aKJD9PA6VBspUtiCNkxl...PvBax7UsMzugzsInsQaQ/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F" in a new tab

In the text/plain part of the MIME part, the redirection looks easier to understand because every URL string that matches the score is rewritten.

```
--===============7781793576330041025== Content-Type: text/plain; charset="us-ascii" MIME-
Version: 1.0 Content-Transfer-Encoding: 7bit This is text part of the message Link1:
http://secure-
web.cisco.com/1duptzzum1fIIuAgDNq__M_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF00kULmjFQancMMn
rp6xEpTmKeEFYnhD0hR1uTwyP2TC-
```

```
b74OjVOznKsikLcNmdC4pIBtIolsZ7O7Mml0C4HECgyxBRf_bxYMAPQDNVSZ0w3UPNf-m807RwtsPfi_-
EyXHQb3pTzMpyFbQ86lVlfDq96VcNM9qiDzG1TgFwej4J_-QM-
72i3qCp9eYFDXR1COY4T9bkDVO_oxZh56Z53w/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalwa
re%2F and some text Link2: http://cisco.com and some text --===============7781793576330041025==
```

Sum Up:

- Redirect run on the TEXT/PLAIN part rewrites the URL string that matches with the Cisco Web Secure proxy service
- Redirect run on the TEXT/HTML part rewrites the URL from an HTML A-tag href attribute with the Cisco Web Secure proxy service but leaves all other URL strings that match unmodified

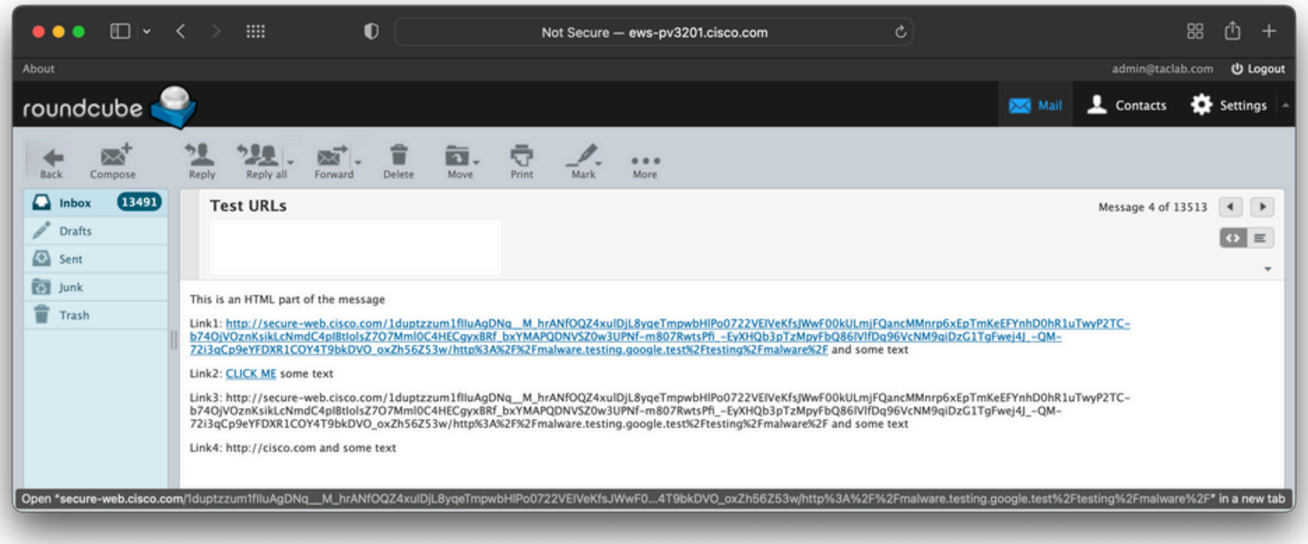
Scenario D

Outbreak Filter non-viral threat detection	No
Content Filter Action	Redirect
websecurityadvancedconfig href and text rewrite is enabled	Yes

This scenario is similar to Scenario B from part one. To rewrite all the URL strings that match in the HTML part of the message is enabled. This is done with the websecurityadvancedconfig command by when you answer Y for the **"Do you want to rewrite both the URL text and the href in the message?** .. question.

```
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version:
1.0 Content-Transfer-Encoding: 7bit <html> <head></head> <body> <p>This is an HTML part of the
message</p> <p>Link1: <a href="http://secure-
web.cisco.com/1duptzzum1fIIuAgDNq__M_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF00kULmjFQancMMn
rp6xEpTmKeEFYnhD0hR1uTwyP2TC-
b74OjVOznKsikLcNmdC4pIBtIolsZ7O7Mml0C4HECgyxBRf_bxYMAPQDNVSZ0w3UPNf-m807RwtsPfi_-
EyXHQb3pTzMpyFbQ86lVlfDq96VcNM9qiDzG1TgFwej4J_-QM-
72i3qCp9eYFDXR1COY4T9bkDVO_oxZh56Z53w/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalwa
re%2F">http://secure-
web.cisco.com/1duptzzum1fIIuAgDNq__M_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF00kULmjFQancMMn
rp6xEpTmKeEFYnhD0hR1uTwyP2TC-
b74OjVOznKsikLcNmdC4pIBtIolsZ7O7Mml0C4HECgyxBRf_bxYMAPQDNVSZ0w3UPNf-m807RwtsPfi_-
EyXHQb3pTzMpyFbQ86lVlfDq96VcNM9qiDzG1TgFwej4J_-QM-
72i3qCp9eYFDXR1COY4T9bkDVO_oxZh56Z53w/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalwa
re%2F</a> and some text</p> <p>Link2: <a href="http://secure-
web.cisco.com/1duptzzum1fIIuAgDNq__M_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF00kULmjFQancMMn
rp6xEpTmKeEFYnhD0hR1uTwyP2TC-
b74OjVOznKsikLcNmdC4pIBtIolsZ7O7Mml0C4HECgyxBRf_bxYMAPQDNVSZ0w3UPNf-m807RwtsPfi_-
EyXHQb3pTzMpyFbQ86lVlfDq96VcNM9qiDzG1TgFwej4J_-QM-
72i3qCp9eYFDXR1COY4T9bkDVO_oxZh56Z53w/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalwa
re%2F">CLICK ME</a> some text</p> <p>Link3: http://secure-
web.cisco.com/1duptzzum1fIIuAgDNq__M_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF00kULmjFQancMMn
rp6xEpTmKeEFYnhD0hR1uTwyP2TC-
b74OjVOznKsikLcNmdC4pIBtIolsZ7O7Mml0C4HECgyxBRf_bxYMAPQDNVSZ0w3UPNf-m807RwtsPfi_-
EyXHQb3pTzMpyFbQ86lVlfDq96VcNM9qiDzG1TgFwej4J_-QM-
72i3qCp9eYFDXR1COY4T9bkDVO_oxZh56Z53w/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalwa
re%2F and some text</p> <p>Link4: http://cisco.com and some text</p> </body> </html> --
===============7781793576330041025==--
```

Once the href and text rewrite is enabled, all URL strings that match the content filter conditions are redirected. The message in the email client is now presented with all the redirection. To better understand this, look at the output of the webmail client that displays the text/html part of the message.



Test URLs

This is an HTML part of the message

Link1: http://secure-web.cisco.com/1duptzzum1fIIuAgDNq__M_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF00kULmjFQancMMnrp6xEpTmKeEFYnhD0hR1uTwyP2TC-b74OjVOznKsikLcNmdC4pIBtIolsZ7O7Mml0C4HECgyxBRf_bxYMAPQDNVSZ0w3UPNf-m807RwtsPfi_-EyXHQb3pTzMpyFbQ86lVlfDq96VcNM9qiDzG1TgFwej4J_-QM-72i3qCp9eYFDXR1COY4T9bkDVO_oxZh56Z53w/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F and some text

Link2: CLICK ME some text

Link3: http://secure-web.cisco.com/1duptzzum1fIIuAgDNq__M_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF00kULmjFQancMMnrp6xEpTmKeEFYnhD0hR1uTwyP2TC-b74OjVOznKsikLcNmdC4pIBtIolsZ7O7Mml0C4HECgyxBRf_bxYMAPQDNVSZ0w3UPNf-m807RwtsPfi_-EyXHQb3pTzMpyFbQ86lVlfDq96VcNM9qiDzG1TgFwej4J_-QM-72i3qCp9eYFDXR1COY4T9bkDVO_oxZh56Z53w/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F and some text

Link4: http://cisco.com and some text

Open "secure-web.cisco.com/1duptzzum1fIIuAgDNq__M_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF0...4T9bkDVO_oxZh56Z53w/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F" in a new tab

The text/plain part of the MIME message is the same as in Scenario C as the websecurityadvancedconfig change does not have any impact on the text/plain parts of the message.

```
--===============7781793576330041025== Content-Type: text/plain; charset="us-ascii" MIME-
Version: 1.0 Content-Transfer-Encoding: 7bit This is text part of the message Link1:
http://secure-
web.cisco.com/1duptzzum1fIIuAgDNq__M_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF00kULmjFQancMMn
rp6xEpTmKeEFYnhD0hR1uTwyP2TC-
b74OjVOznKsikLcNmdC4pIBtIolsZ7O7Mml0C4HECgyxBRf_bxYMAPQDNVSZ0w3UPNf-m807RwtsPfi_-
EyXHQb3pTzMpyFbQ86lVlfDq96VcNM9qiDzG1TgFwej4J_-QM-
72i3qCp9eYFDXR1COY4T9bkDVO_oxZh56Z53w/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalwa
re%2F and some text Link2: http://cisco.com and some text --===============7781793576330041025==
```

Sum Up:

- Redirect run on the TEXT/PLAIN part rewrites the URL strings that match with the Cisco Web Secure proxy service
- Redirect run on the TEXT/HTML part rewrites the URL from an HTML A-tag href attribute together with the text part as well as any other URL string that matches in the HTML body with the Cisco Web Secure proxy service

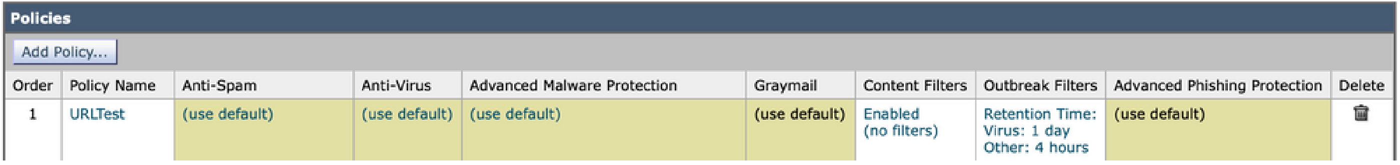
Part 3 - OF Redirect

This part provides information on how OF settings for non-viral threat detection impact URL scans.

Configuration

For this purpose, the content filter used in the first two parts is disabled.

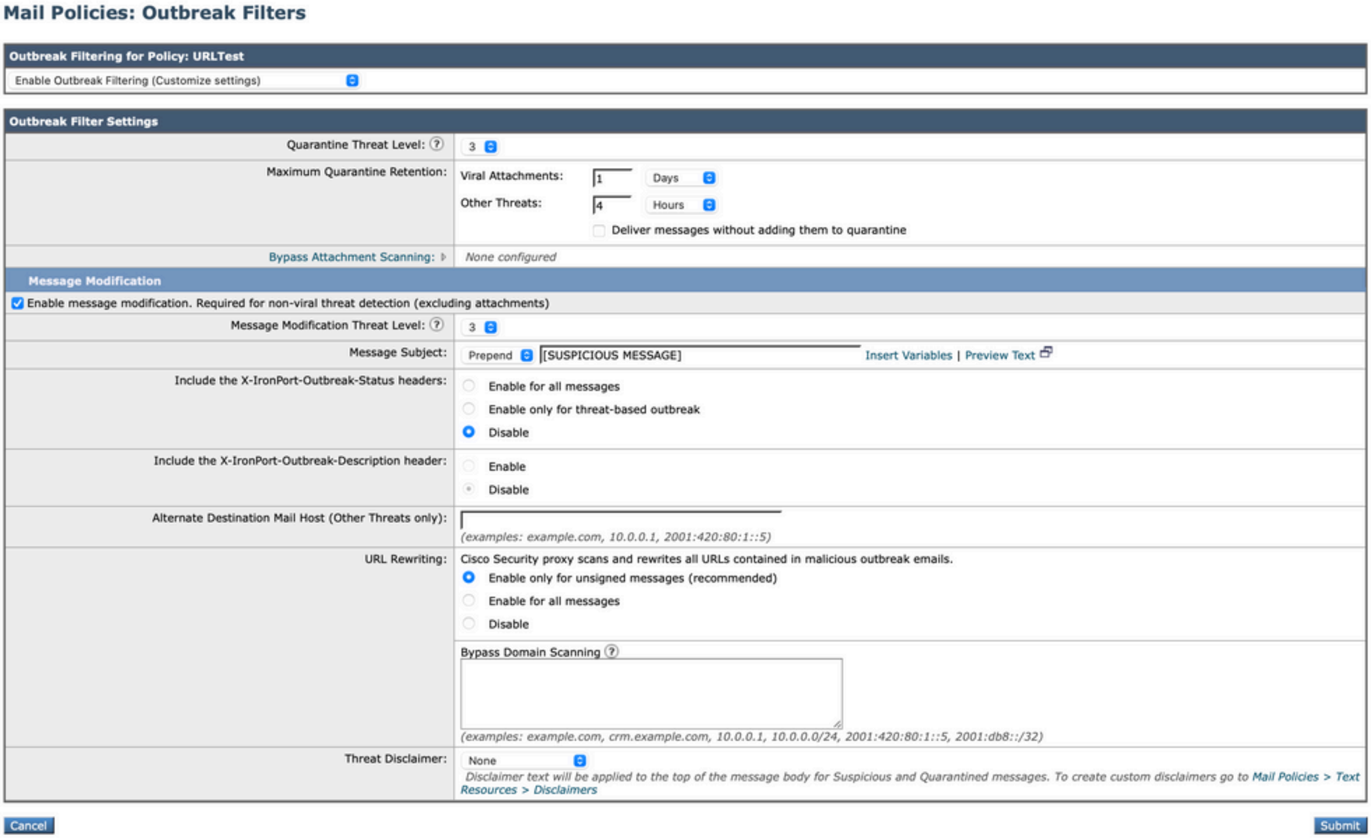
- Mail Policy with default AS/AV/AMP configuration and OF enabled



Policies

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete
1	URLTest	(use default)	(use default)	(use default)	(use default)	Enabled (no filters)	Retention Time: Virus: 1 day Other: 4 hours	(use default)	🗑

- The Outbreak Filters scan for non-viral threat detection is configured with a URL Rewrite set to rewrite all URLs contained in malicious emails



Mail Policies: Outbreak Filters

Outbreak Filtering for Policy: URLTest

Enable Outbreak Filtering (Customize settings)

Outbreak Filter Settings

Quarantine Threat Level: 3

Maximum Quarantine Retention: Viral Attachments: 1 Days; Other Threats: 4 Hours

□ Deliver messages without adding them to quarantine

Bypass Attachment Scanning: None configured

Message Modification

☑ Enable message modification. Required for non-viral threat detection (excluding attachments)

Message Modification Threat Level: 3

Message Subject: Prepend [SUSPICIOUS MESSAGE]

Include the X-IronPort-Outbreak-Status headers:
○ Enable for all messages
○ Enable only for threat-based outbreak
● Disable

Include the X-IronPort-Outbreak-Description header:
○ Enable
● Disable

Alternate Destination Mail Host (Other Threats only):
(examples: example.com, 10.0.0.1, 2001:420:80:1::5)

URL Rewriting: Cisco Security proxy scans and rewrites all URLs contained in malicious outbreak emails.
● Enable only for unsigned messages (recommended)
○ Enable for all messages
○ Disable

Bypass Domain Scanning
(examples: example.com, crm.example.com, 10.0.0.1, 10.0.0.0/24, 2001:420:80:1::5, 2001:db8::/32)

Threat Disclaimer: None
Disclaimer text will be applied to the top of the message body for Suspicious and Quarantined messages. To create custom disclaimers go to Mail Policies > Text Resources > Disclaimers

When the message is classified by OF as Malicious, all the URLs inside are rewritten with the Cisco Web Secure proxy service.

Scenario E

Outbreak Filter non-viral threat detection	Yes
Content Filter Action	No
websecurityadvancedconfig href and text rewrite is enabled	No

This scenario shows how the message rewrite works with only OF enabled and websecurityadvancedconfig href and text rewrite disabled.

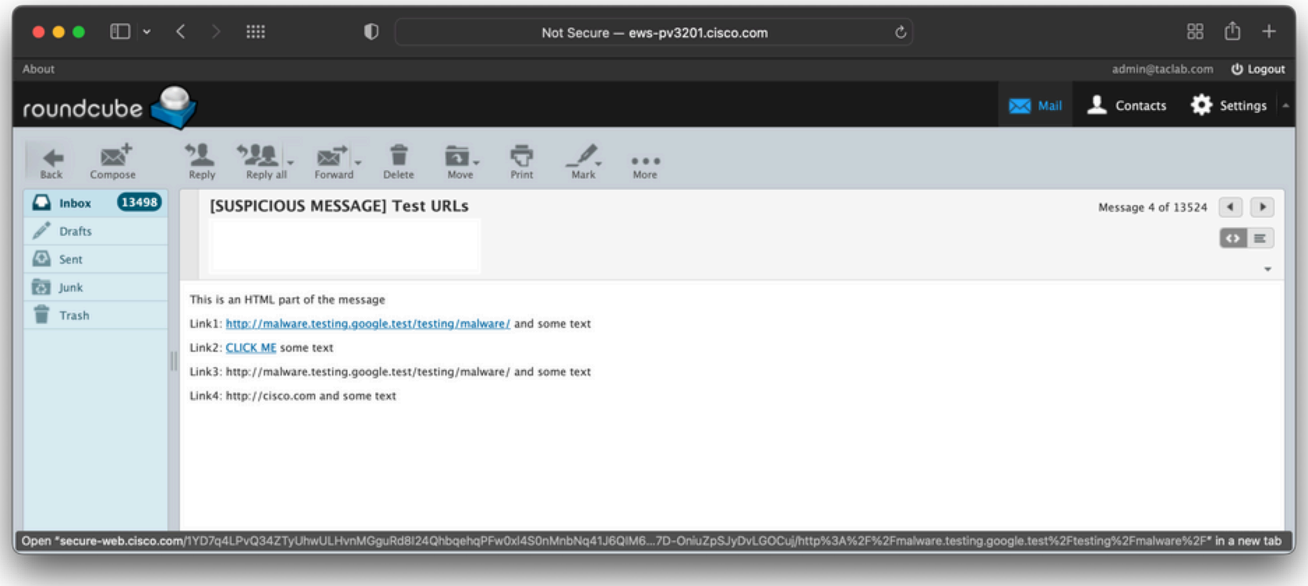
```
Wed Jul 6 14:09:19 2022 Info: MID 139514 Outbreak Filters: verdict positive Wed Jul 6 14:09:19
2022 Info: MID 139514 Threat Level=5 Category=Phish Type=Phish Wed Jul 6 14:09:19 2022 Info: MID
139514 rewritten URL u'http://malware.testing.google.test/testing/malware/' Wed Jul 6 14:09:19
2022 Info: MID 139514 rewritten URL u'http://cisco.com' Wed Jul 6 14:09:19 2022 Info: MID 139514
rewritten URL u'http://malware.testing.google.test/testing/malware/' Wed Jul 6 14:09:19 2022
Info: MID 139514 rewritten URL u'http://malware.testing.google.test/testing/malware/' Wed Jul 6
14:09:19 2022 Info: MID 139514 rewritten to MID 139515 by url-threat-protection filter 'Threat
Protection' Wed Jul 6 14:09:19 2022 Info: Message finished MID 139514 done Wed Jul 6 14:09:19
2022 Info: MID 139515 Virus Threat Level=5 Wed Jul 6 14:09:19 2022 Info: MID 139515 quarantined
to "Outbreak" (Outbreak rule:Phish: Phish)
```

Let us start with the text/plain MIME part. After a quick check, it can be observed that all URLs inside the text/plain part are rewritten to the Cisco Web Secure proxy services. It happens because URL rewrite is enabled for all URLs inside the Outbreak malicious message.

```
--===============7781793576330041025== Content-Type: text/plain; charset="us-ascii" MIME-
Version: 1.0 Content-Transfer-Encoding: quoted-printable This is text part of the message Link1:
http://secure-web.cisco.com/11ZWFnZYM5Rp_tvvnco4I3GtnExIEFqpirK= f5WBmD_7X-
8wSvnm0QxYNYhb4aplEtOXp_-0CMTnyw6WX63xZIFnj5S_n0vY18F9GOJWCSoVJpK= 3OEq8lB-jcbjx9BWlZaNbl-t-
uTOLj107Z3j8XCAdOwHe1t7GGF8LFt1GNFRCVLEM_wQZyo-uxh= UfkhZVETXPZAdddg6-
uCeoeimiRZUOAzqvgw2axm903AUpieDdfeMHYXpmzeMwu574FRGbbr7uV=
tB65hfy29t2r_VyWA24b6nyaKyJ_hmRf2A4PBWOTe37cRLveONF9cI3P51GxU/http%3A%2F%2F=
malware.testing.google.test%2Ftesting%2Fmalware%2F and some text Link2: http://secure-
web.cisco.com/1o7068d-d0bG3Sqwcifil89X-tY7S4csHT6=
LsLToTUYJqWzfLfODch91yXWfJ8aOxPq1PQBSACgJlDt4hCZipXXmC1XI3-XdNLGBMd0bLfj1cB= hY_OWlBfLD-
zC86M02dm_fOXCqKT0tDET3RD_KAeUWTWhWZvN9i8lLPcwBBBi9TLjMAMnRKPmeg= En_YQvDnCzTB4qYkG8aUQlFsecXB-
V_HU1vL8IRFRP-uGINjhHp9kWCnntJBJEm0MheA1T6mBJJ= ZhBZmfymfOddXs-
xIGiYXn3juN1TvuOlCceo3YeaiVrbOXc0lZs3FO8xvNjOnwVKN181yGKPQ9Y= cn5aSWvg/http%3A%2F%2Fcisco.com
and some text --===============7781793576330041025==
```

This is the processed text/html part of the MIME message.

```
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version:
1.0 Content-Transfer-Encoding: quoted-printable <html> <head></head> <body> <p>This is an HTML
part of the message</p> =20 <p>Link1: <a href=3D"http://secure-
web.cisco.com/1YD7q4LPvQ34ZTyUhwULH=
vnMGguRd8I24QhbqehqPFw0xl4S0nMnbNq41J6QIM6zDb1r_PFdS2LGUpWQcvGTivdd_WSFsc32=
jfhbrQ9yQsKFerMUioP3BdNXH0UtTGoSE5qLY120lJGhOD2Q7KuRVXTtGu06v17VO10dISpwtuq=
ZqRH1LnImVjUPQLr9dRex3xC1cnZdILPQjPn9zwe4lC7YQD5zmqxPMWsZCnTDA6UrxCuk1ETwZX= 6n4PQSOAoBQd-
BZH4kMIy7Z_bZJacnLYCBg28tL3m8JFD5ZKWlo2LKL7D-OniuZpSJyDvLGOCuj=
/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F">http://ma=
lware.testing.google.test/testing/malware/</a> and some text</p> <p>Link2: <a
href=3D"http://secure-web.cisco.com/1YD7q4LPvQ34ZTyUhwULH=
vnMGguRd8I24QhbqehqPFw0xl4S0nMnbNq41J6QIM6zDb1r_PFdS2LGUpWQcvGTivdd_WSFsc32=
jfhbrQ9yQsKFerMUioP3BdNXH0UtTGoSE5qLY120lJGhOD2Q7KuRVXTtGu06v17VO10dISpwtuq=
ZqRH1LnImVjUPQLr9dRex3xC1cnZdILPQjPn9zwe4lC7YQD5zmqxPMWsZCnTDA6UrxCuk1ETwZX= 6n4PQSOAoBQd-
BZH4kMIy7Z_bZJacnLYCBg28tL3m8JFD5ZKWlo2LKL7D-OniuZpSJyDvLGOCuj=
/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F">CLICK ME<= /a> some text</p>
<p>Link3: http://malware.testing.google.test/testing/malware/ and some= text</p> <p>Link4:
http://cisco.com and some text</p> </body> </html> =20 --===============7781793576330041025==--
```



[SUSPICIOUS MESSAGE] Test URLs

Message 4 of 13524

This is an HTML part of the message

Link1: http://malware.testing.google.test/testing/malware/ and some text

Link2: CLICK ME some text

Link3: http://malware.testing.google.test/testing/malware/ and some text

Link4: http://cisco.com and some text

Open "secure-web.cisco.com/1YD7q4LPvQ34ZTyUhwULHvnMGguRd8I24QhbqehqPFw0xl4S0nMnbNq41J6QIM6...7D-OniuZpSJyDvLGOCuj/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F" in a new tab

The first that can be noted here is why Link4 is not rewritten. If you read the article carefully you already know the answer. The text/html part of MIME by default evaluates and manipulates only the href attributes of the A-tag elements. If a similar behavior as for text/plain part is desired, the websecurityadvancedconfig href and text rewrite must be enabled. The next scenario does exactly this.

Sum Up:

- OF redirect run on the TEXT/PLAIN part rewrites all the URL string that matches with the Cisco Web Secure proxy service
- OF redirect run on the TEXT/HTML part rewrites only the URL from an HTML A-tag href attribute with the Cisco Web Secure proxy service

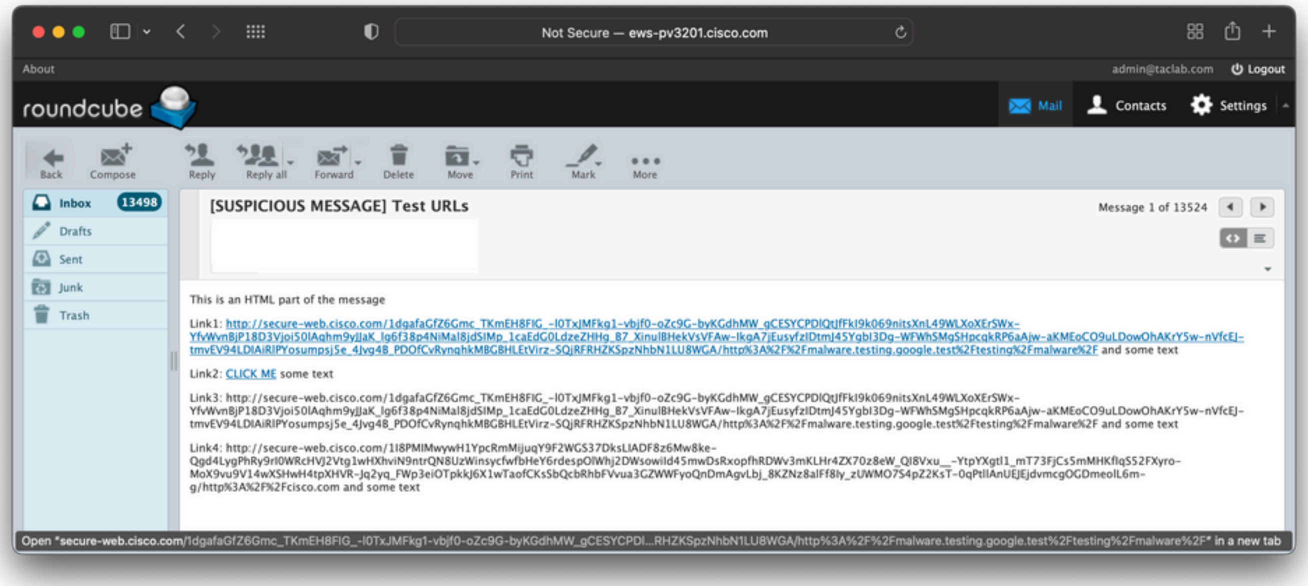
Scenario F

Outbreak Filter non-viral threat detection	Yes
Content Filter Action	No
websecurityadvancedconfig href and text rewrite is enabled	Yes

This scenario enables websecurityadvancedconfig href and text rewrite to show how the behavior in URL rewrite provided by OF non-viral threat detection changes. At this moment it must be understood that the websecurityadvancedconfig does not affect text/plain MIME parts. Let us evaluate only the text/html part and see how the behavior has changed.

```
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version:
1.0 Content-Transfer-Encoding: quoted-printable <html> <head></head> <body> <p>This is an HTML
part of the message</p> =20 <p>Link1: <a href=3D"http://secure-
web.cisco.com/1dgafaGfZ6Gmc_TKmEH8F= IG_-l0TxJMFkg1-vbjf0-oZc9G-
byKGdhMW_gCESYCPDlQtJfFkI9k069nitsXnL49WLXoXErSW= x-
YfvWvnBjP18D3Vjoi50lAqhm9yJJaK_lg6f38p4NiMal8jdSIMp_1caEdG0LdzeZHHg_B7_Xi= nulBHekVsVFAw-
IkgA7jEusyfzIDtmJ45YgbI3Dg-WFWhSMgSHpcqkRP6aAjw-aKMEoCO9uLDow= OhAKrY5w-nVfcEJ-
tmvEV94LDIAiRlPYosumpsj5e_4Jvg4B_PDOfCvRynqhkMBGBHLEtVirz-S=
QjRFRHZKSpzNhbN1LU8WGA/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2=
Fmalware%2F">http://secure-web.cisco.com/1dgafaGfZ6Gmc_TKmEH8FIG_-l0TxJMFkg= 1-vbjf0-oZc9G-
byKGdhMW_gCESYCPDlQtJfFkI9k069nitsXnL49WLXoXErSWx-YfvWvnBjP18=
D3Vjoi50lAqhm9yJJaK_lg6f38p4NiMal8jdSIMp_1caEdG0LdzeZHHg_B7_XinulBHekVsVFAw= -
IkgA7jEusyfzIDtmJ45YgbI3Dg-WFWhSMgSHpcqkRP6aAjw-aKMEoCO9uLDowOhAKrY5w-nVfc= EJ-
tmvEV94LDIAiRlPYosumpsj5e_4Jvg4B_PDOfCvRynqhkMBGBHLEtVirz-SQjRFRHZKSpzNh=
bN1LU8WGA/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F</= a> and some
text</p> <p>Link2: <a href=3D"http://secure-web.cisco.com/1dgafaGfZ6Gmc_TKmEH8F= IG_-l0TxJMFkg1-
vbjf0-oZc9G-byKGdhMW_gCESYCPDlQtJfFkI9k069nitsXnL49WLXoXErSW= x-
YfvWvnBjP18D3Vjoi50lAqhm9yJJaK_lg6f38p4NiMal8jdSIMp_1caEdG0LdzeZHHg_B7_Xi= nulBHekVsVFAw-
IkgA7jEusyfzIDtmJ45YgbI3Dg-WFWhSMgSHpcqkRP6aAjw-aKMEoCO9uLDow= OhAKrY5w-nVfcEJ-
tmvEV94LDIAiRlPYosumpsj5e_4Jvg4B_PDOfCvRynqhkMBGBHLEtVirz-S=
QjRFRHZKSpzNhbN1LU8WGA/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2= Fmalware%2F">CLICK
ME</a> some text</p> <p>Link3: http://secure-web.cisco.com/1dgafaGfZ6Gmc_TKmEH8FIG_-l0TxJMF=
kg1-vbjf0-oZc9G-byKGdhMW_gCESYCPDlQtJfFkI9k069nitsXnL49WLXoXErSWx-YfvWvnBjP=
18D3Vjoi50lAqhm9yJJaK_lg6f38p4NiMal8jdSIMp_1caEdG0LdzeZHHg_B7_XinulBHekVsVF= Aw-
IkgA7jEusyfzIDtmJ45YgbI3Dg-WFWhSMgSHpcqkRP6aAjw-aKMEoCO9uLDowOhAKrY5w-nV= fcEJ-
tmvEV94LDIAiRlPYosumpsj5e_4Jvg4B_PDOfCvRynqhkMBGBHLEtVirz-SQjRFRHZKSpz=
NhbN1LU8WGA/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F= and some text</p>
<p>Link4: http://secure-web.cisco.com/1I8PMIMwywH1YpcRmMijuqY9F2WGS37D= ksLIADF8z6Mw8ke-
Qgd4LygPhRy9rI0WRcHVJ2Vtg1wHXhviN9ntrQN8UzWinsycfwfbHeY6rde=
spOlWhj2DWsowiId45mwDsRxopfhRDWv3mKLHr4ZX70z8eW_QI8Vxu__-YtpYXgtl1_mT73FjCs= 5mMHKfIqS52FXyro-
MoX9vu9V14wXSHwH4tpXHVR-Jq2yq_FWp3eiOTpkkJ6X1wTaofCKsSbQcb=
RhbFVvua3GZWWFyoQnDmAgvLbj_8KZNz8alFf8Iy_zUWMO7S4pZ2KsT-0qPtllAnUEJEjdvmcgO= GDmeolL6m-
g/http%3A%2F%2Fcisco.com and some text</p> </body> </html> =20 --
===============7781793576330041025==--
```

It can be noted that the output is very similar to the one from Scenario D with the only difference that all URLs have been rewritten, not only the malicious ones. All URL strings that match in the HTML part together with the non-malicious ones are modified here.



[SUSPICIOUS MESSAGE] Test URLs

This is an HTML part of the message

Link1: http://secure-web.cisco.com/1dgafaGfZ6Gmc_TKmEH8FIG_-l0TxJMFkg1-vbjf0-oZc9G-byKGdhMW_gCESYCPDlQtJfFkI9k069nitsXnL49WLXoXErSWx-YfvWvnBjP18D3Vjoi50lAqhm9yJJaK_Ig6f38p4NiMal8jdSIMp_1caEdG0LdzeZHHg_B7_XinulBHekVsVFAw-IkgA7jEusyfzIDtmJ45YgbI3Dg-WFWhSMgSHpcqkRP6aAjw-aKMEoCO9uLDowOhAKrY5w-nVfcEJ-tmvEV94LDIAiRIPYosumpsj5e_4Jvg4B_PDOfCvRynqhkMBGBHLEtVirz-SQjRFRHZKSpzNhbN1LU8WGA/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F and some text

Link2: CLICK ME some text

Link3: http://secure-web.cisco.com/1dgafaGfZ6Gmc_TKmEH8FIG_-l0TxJMFkg1-vbjf0-oZc9G-byKGdhMW_gCESYCPDlQtJfFkI9k069nitsXnL49WLXoXErSWx-YfvWvnBjP18D3Vjoi50lAqhm9yJJaK_Ig6f38p4NiMal8jdSIMp_1caEdG0LdzeZHHg_B7_XinulBHekVsVFAw-IkgA7jEusyfzIDtmJ45YgbI3Dg-WFWhSMgSHpcqkRP6aAjw-aKMEoCO9uLDowOhAKrY5w-nVfcEJ-tmvEV94LDIAiRIPYosumpsj5e_4Jvg4B_PDOfCvRynqhkMBGBHLEtVirz-SQjRFRHZKSpzNhbN1LU8WGA/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F and some text

Link4: http://secure-web.cisco.com/1I8PMIMwywH1YpcRmMijuqY9F2WGS37DksLIADF8z6Mw8ke-Qgd4LygPhRy9rI0WRcHVJ2Vtg1wHXhviN9ntrQN8UzWinsycfwfbHeY6rdespOlWhj2DWsowiId45mwDsRxopfhRDWv3mKLHr4ZX70z8eW_QI8Vxu__-YtpYXgtl1_mT73FjCs5mMHKflqS52FXyro-MoX9vu9V14wXSHwH4tpXHVR-Jq2yq_FWp3eiOTpkkJ6X1wTaofCKsSbQcbRhbFVvua3GZWWFyoQnDmAgvLbj_8KZNz8alFf8ly_zUWMO7S4pZ2KsT-0qPtllAnUEJEjdvmcgOGDmeolL6m-g/http%3A%2F%2Fcisco.com and some text

Open "secure-web.cisco.com/1dgafaGfZ6Gmc_TKmEH8FIG_-l0TxJMFkg1-vbjf0-oZc9G-byKGdhMW_gCESYCPDl...RHZKSpzNhbN1LU8WGA/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F" in a new tab

Sum Up:

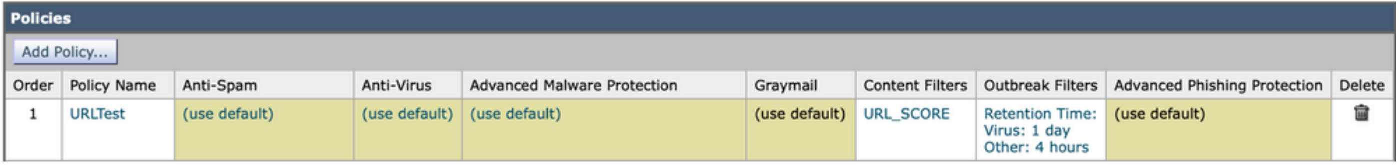
- OF redirect run on the TEXT/PLAIN part rewrites all the URL strings that match with the Cisco Web Secure proxy service
- OF redirect run on the TEXT/HTML part rewrites the URL from an HTML A-tag href attribute together with the text part of the element and all other URL strings that match with the Cisco Web Secure proxy service

Scenario G

Outbreak Filter non-viral threat detection	Yes
Content Filter Action	Defang
websecurityadvancedconfig href and text rewrite is enabled	Yes

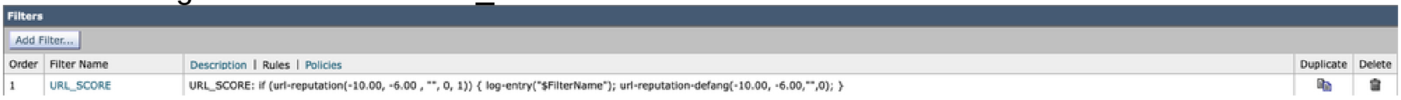
This last scenario validates the configuration.

- Mail Policy with default AS/AV/AMP configuration and OF enabled



Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete
1	URLTest	(use default)	(use default)	(use default)	(use default)	URL_SCORE	Retention Time: Virus: 1 day Other: 4 hours	(use default)	🗑

- The OF scan for non-viral threat detection is configured with URL Rewrite set to rewrite all URLs contained in malicious emails (same as in previous scenarios)
- Incoming Content Filter: URL_SCORE content filter enabled



Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	URL_SCORE	URL_SCORE: if (url-reputation(-10.00, -6.00 , "", 0, 1)) { log-entry("$FilterName"); url-reputation-defang(-10.00, -6.00,"",0); }	⧉	🗑

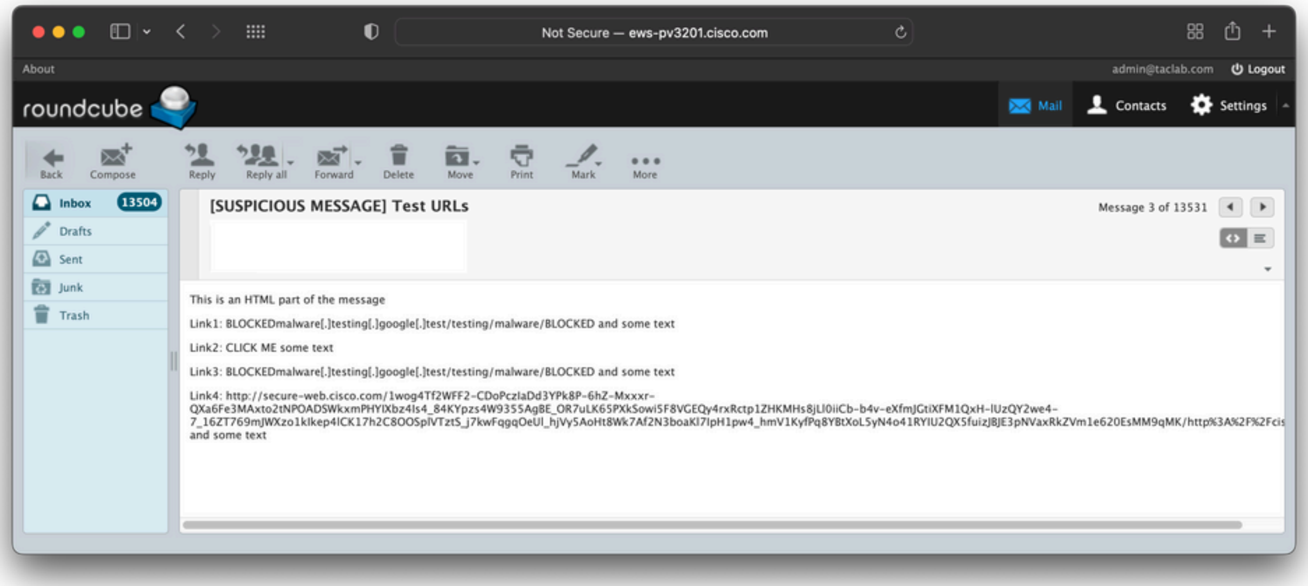
The content filter uses the URL reputation condition to match Malicious URLs, the ones that score between -6.00 and -10.00. As an action, the content filter name is logged and the defang action **url-reputation-defang** is taken.

The same copy of the message is sent and evaluated by the email gateway with the results:

```
Wed Jul 6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/
has reputation -9.4 matched Condition: URL Reputation Rule Wed Jul 6 15:13:10 2022 Info: MID
139518 Custom Log Entry: URL_SCORE Wed Jul 6 15:13:10 2022 Info: MID 139518 URL
http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL
defanged Wed Jul 6 15:13:10 2022 Info: MID 139518 URL
http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL
defanged Wed Jul 6 15:13:10 2022 Info: MID 139518 URL
http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL
defanged Wed Jul 6 15:13:10 2022 Info: MID 139518 URL
http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL
defanged Wed Jul 6 15:13:10 2022 Info: MID 139518 URL
http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL
defanged Wed Jul 6 15:13:10 2022 Info: MID 139518 rewritten to MID 139519 by url-reputation-
defang-action filter 'URL_SCORE' Wed Jul 6 15:13:10 2022 Info: Message finished MID 139518 done
Wed Jul 6 15:13:10 2022 Info: MID 139519 Outbreak Filters: verdict positive Wed Jul 6 15:13:10
2022 Info: MID 139519 Threat Level=5 Category=Phish Type=Phish Wed Jul 6 15:13:10 2022 Info: MID
139519 rewritten URL u'http://cisco.com' Wed Jul 6 15:13:10 2022 Info: MID 139519 rewritten URL
u'http://cisco.com' Wed Jul 6 15:13:10 2022 Info: MID 139519 rewritten to MID 139520 by url-
threat-protection filter 'Threat Protection' Wed Jul 6 15:13:10 2022 Info: Message finished MID
139519 done Wed Jul 6 15:13:10 2022 Info: MID 139520 Virus Threat Level=5
```

The email pipeline explains the message is first evaluated by the content filters, where the URL_SCORE filter is triggered and URL-reputation-defang-action is applied. This action defangs all malicious URLs in both text/plain and text/html MIME parts. Because websecurityadvanceconfig href and text rewrite is enabled all URL strings that match inside the HTML body are defanged when all A-tag elements are stripped and rewrite text parts of the URL between BLOCKED words and place all the dots between square brackets. The same happens with other malicious URLs not placed in A-tag HTML elements. The Outbreak Filter next processes the message. The OF detects malicious URLs and identifies the message as malicious (Threat Level=5). As a result, it rewrites all the malicious and non-malicious URLs found inside the message. Because the content filter action already modified those URLs the OF rewrites only the rest of the non-malicious URLs as it was intentionally configured to do it. The message displayed in the email client as part of the malicious URLs defanged and part of the non-malicious URL redirected.

```
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version:
1.0 Content-Transfer-Encoding: quoted-printable <html> <head></head> <body> <p>This is an HTML
part of the message</p> =20 <p>Link1:
BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLO= CKED and some text</p> <p>Link2:
CLICK ME some text</p> <p>Link3: BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLO=
CKED and some text</p> <p>Link4: http://secure-web.cisco.com/1wog4Tf2WFF2-CDoPczIaDd3YPk8P-6h=
Z-Mxxxr-QXa6Fe3MAxto2tNPOADSWkxmPHYIXbz4Is4_84KYpzs4W9355AgBE_OR7uLK65PXkSo=
wi5F8VGEQy4rxRctp1ZHKMHs8jLl0iiCb-b4v-eXfmJGtiXFM1QxH-lUzQY2we4-7_16ZT769mJ=
WXzo1kIkep4lCK17h2C8OOSplVTztS_j7kwFqgqOeUl_hjVy5AoHt8Wk7Af2N3boaKl7IpH1pw4=
_hmV1KyfPq8YBtXoL5yN4o41RYIU2QX5fuizJBJE3pNVaxRkZVm1e620EsMM9qMK/http%3A%2F= %2Fcisco.com and
some text</p> </body> </html> =20 --===============7781793576330041025==--
```



[SUSPICIOUS MESSAGE] Test URLs

This is an HTML part of the message

Link1: BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLOCKED and some text

Link2: CLICK ME some text

Link3: BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLOCKED and some text

Link4: http://secure-web.cisco.com/1wog4Tf2WFF2-CDoPczIaDd3YPk8P-6hZ-Mxxxr-QXa6Fe3MAxto2tNPOADSWkxmPHYIXbz4Is4_84KYpzs4W9355AgBE_OR7uLK65PXkSowi5F8VGEQy4rxRctp1ZHKMHs8jLl0iiCb-b4v-eXfmJGtiXFM1QxH-lUzQY2we4-7_16ZT769mJWXzo1kIkep4lCK17h2C8OOSplVTztS_j7kwFqgqOeUl_hjVy5AoHt8Wk7Af2N3boaKl7IpH1pw4_hmV1KyfPq8YBtXoL5yN4o41RYIU2QX5fuizJBJE3pNVaxRkZVm1e620EsMM9qMK/http%3A%2F%2Fcis
and some text

The same is applied to the text/plain part of the MIME message. All non-malicious URLs are redirected to Cisco Web Secure proxy and the malicious URLs are defanged.

```
--===============7781793576330041025== Content-Type: text/plain; charset="us-ascii" MIME-
Version: 1.0 Content-Transfer-Encoding: quoted-printable This is text part of the message Link1:
BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLOCKE= D and some text Link2:
http://secure-web.cisco.com/1wog4Tf2WFF2-CDoPczIaDd3YPk8P-6hZ-M= xxxr-
QXa6Fe3MAxto2tNPOADSWkxmPHYIXbz4Is4_84KYpzs4W9355AgBE_OR7uLK65PXkSowi5=
F8VGEQy4rxRctp1ZHKMHs8jLl0iiCb-b4v-eXfmJGtiXFM1QxH-lUzQY2we4-7_16ZT769mJWXz=
o1kIkep4lCK17h2C8OOSplVTztS_j7kwFqgqOeUl_hjVy5AoHt8Wk7Af2N3boaKl7IpH1pw4_hm=
V1KyfPq8YBtXoL5yN4o41RYIU2QX5fuizJBJE3pNVaxRkZVm1e620EsMM9qMK/http%3A%2F%2F= cisco.com and some
text --===============7781793576330041025==
```

Sum Up:

- CF defang run on the TEXT/PLAIN part rewrites the URL into BLOCKED blocks
- CF defang run on the TEXT/HTML part rewrites the URL from an HTML A-tag when an A-tag is stripped
- CF defang run on the TEXT/HTML part rewrites all URL strings that match into BLOCKED blocks
- OF redirect run on the TEXT/PLAIN part rewrites all the URL strings that match with the Cisco Web Secure proxy service (non-malicious)
- OF redirect run on the TEXT/HTML part rewrites the URL from an HTML A-tag href attribute together with the text part of the element and all other URL strings that match with the Cisco Web Secure proxy service (non-malicious)

Troubleshoot

Follow these points when there is a need to investigate the issue with URL rewrite.

- Enable URL logging in your mail_logs. Run **OUTBREAKCONFIG** command and answer **Y** to **Do you wish to enable logging of URL's?** [N]>"
- Verify **WEBSECURITYADVANCECONFIG** settings under each email gateway cluster member and be sure the href and text rewrite option is set accordingly and the same on each machine. Keep

in mind this command is machine-level specific and changes done here do not affect Group or Cluster settings.

- Verify the conditions and activities of your content filter, and ensure the content filter is enabled and applied to the right incoming mail policy. Verify if there is no other content filter processed before with a final action that can skip to process other filters.
- Investigate the raw copy of the source and final message. Keep in mind to retrieve the message in EML format, the proprietary formats like MSG are not reliable when it comes to message investigation. Some email clients allow you to view the Source message, and try to retrieve the copy of the message with a different email client. For example, MS Outlook for Mac allows you to view the Source of the message while the Windows version allows you only to view the headers.

Summary

The purpose of this article is to help in better understanding available configuration options when it comes to URL rewrite. It is important to remember that modern messages are built by most email software with the MIME standard. It means the same copy of the message can be displayed differently which depends on the email client capabilities or/and enabled modes (text vs HTML mode). By default, most modern email clients use HTML to display messages. When it comes to HTML and URL rewrite, please keep in mind by default email gateway rewrites only URLs found inside the href attribute of the A-tag element. In a lot of cases that is not enough and it must be considered to enable both href and text rewrite with WEBSECURITYADVANCECONFIG command. Remember this is a machine-level command and for consistency across the cluster, the change must be applied separately to each of the cluster members.