瞭解安全電子郵件網關上的URL防禦和重定向操作

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[背景資訊](#)
[消息示例](#)
[第一部分 — 德芳](#)
[組態](#)
[德方行動](#)
[案例A](#)
[案例B](#)
[第II部分 — 重新導向](#)
[組態](#)
[重定向操作](#)
[案例C](#)
[案例D](#)
[第3部分 — 重定向](#)
[組態](#)
[案例E](#)
[案例F](#)
[案例G](#)
[疑難排解](#)
[摘要](#)

簡介

本檔案將說明URL過濾器中使用的取消和重定向操作之間的差異，以及如何對href屬性和文本使用可用的重寫選項。

必要條件

需求

要根據URL信譽採取行動，或者對郵件和內容過濾器實施可接受的使用策略，必須全域性啟用爆發過濾器功能。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全電子郵件閘道
- 爆發過濾器
- 內容和郵件過濾器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

URL過濾功能功能之一是通過使用消息和/或內容過濾器根據URL信譽或類別採取行動。根據URL掃描結果（URL相關條件），可以應用URL上的三個可用操作之一：

- 預設URL
- 重新導向至思科安全代理
- 將URL替換為文本消息

本文的重點是說明「Defang URL」和「Redirect URL」選項之間的行為。它還提供了爆發過濾器的非病毒威脅檢測的URL重寫功能的簡要描述和說明。

消息示例

所有測試中使用的示例消息是MIME multipart/alternative消息型別，包括text/plain和text/html部分。這些部分通常由電子郵件軟體自動生成，並包含格式為HTML和非HTML接收器的相同型別的內容。為此，手動編輯文本/純文字檔案和文本/html的內容。

```
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

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

--===============7781793576330041025==--
```

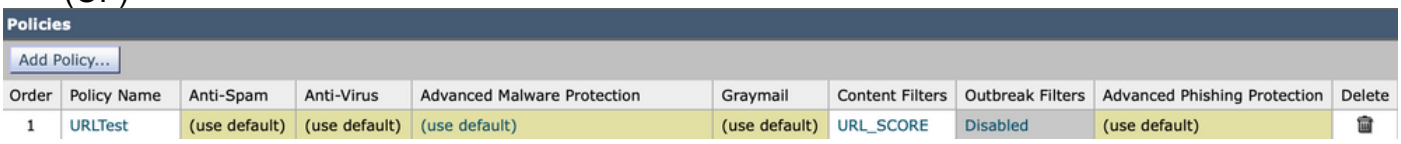
第一部分 — 德芳

組態

在第一部分中，組態使用：

- 郵件策略，預設禁用反垃圾郵件(AS)/防病毒(AV)/高級惡意軟體防護(AMP)配置和爆發過濾器

(OF)



- 傳入內容過濾器：已啟用URL_SCORE內容篩選器

內容過濾器使用URL信譽條件來匹配惡意URL，即得分在–6.00和–10.00之間的惡意URL。作為操作，將記錄內容過濾器名稱並取消操作 **url-reputation-defang** 被拿走了。

德方行動

澄清什麼是防禦行動很重要。使用手冊提供說明；拆除URL使其不可按一下。郵件收件人仍可以檢視和複製URL。

案例A

爆發過濾器非病毒威脅檢測	否
內容篩選器操作	德芳
websecurityadvancedconfig href和文本重寫已啟用	否

此案例說明使用預設設定設定的撤銷操作的結果。在預設設定中，僅刪除HTML標籤時，將重寫URL。請檢視一個包含一些URL的HTML段落：

```
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
```

在前兩段中，URL用正確的HTML A標籤表示。<A>元素包括 **href=** 標籤本身所包含並指示連結目標的屬性。標籤元素中的內容也可以指示連結目標。此 **text form** 可以包含URL。第一個Link1在元素的href屬性和文本部分中都包含相同的URL連結。可以注意到，這些URL可以不同。第二個Link2僅在href屬性內包含正確的URL。最後一段不包括任何A要素。

> **附註**：將游標移動到連結上方或檢視消息的原始碼時，始終可以看到正確的地址。遺憾的是，在一些常用的電子郵件客戶端上找不到原始碼。

一旦郵件與URL_SCORE過濾器匹配，就會對惡意URL進行防禦。當URL日誌記錄與 **OUTBREAKCONFIG** 命令可在mail_logs中找到分數和URL。

```
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'
```

這會導致重寫消息：

```
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version:
1.0 Content-Transfer-Encoding: 7bit

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

--===============7781793576330041025==--
```

對MIME郵件的text/html部分執行反遮蔽操作的結果是剝離的A標籤，並且標籤內容保持不變。在前面兩段中，兩個連結都進行了縮排，其中刪除了HTML代碼，並且保留了元素的文本部分。第一個段落中的URL地址是HTML元素文本部分中的地址。必須注意的是，執行去汙操作後，第一個段落的URL地址仍然可見，但沒有HTML A標籤，元素不能可按一下。第三段沒有進行縮寫，因為此處的URL地址沒有放在任何A標籤之間，並且不被視為連結。也許這不是人們想要的行為，原因有二。首先，使用者可以方便地檢視並複製連結，然後在瀏覽器中執行。第二個原因是，一些電子郵件軟體傾向於檢測文本內部有效的URL形式，並使其成為可點選連結。

讓我們看一下MIME郵件的文本/純文字檔案部分。文本/純文字檔案部分在文本格式中包括兩個URL。文本/純文字檔案由不理解HTML代碼的MUA顯示。在大多數現代電子郵件客戶端中，您不會看到郵件的文本/純文字檔案部分，除非您有意將電子郵件客戶端配置為這樣做。通常，您需要檢查郵件的原始碼，郵件的原始EML格式，以檢視和調查MIME部分。

此處清單顯示了源消息文本/純文字檔案部分的URL。

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

這兩個連結中的其中一個被惡意得分並拆除。預設情況下，對MIME型別的text/plain部分執行的防禦操作與text/html部分執行操作的結果不同。它位於BLOCKED單詞和方括弧中的所有點之間。

```
--===============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==
```

總結：

- 在TEXT/PLAIN部分上運行的防禦將URL重寫為BLOCKED塊
- Defang在TEXT/HTML部分運行，當刪除了A標籤而沒有A標籤之間的文本（也可以是URL地址）時，會從HTML A標籤中重寫URL

案例B

爆發過濾器非病毒威脅檢測	否
內容篩選器操作	德芳
websecurityadvancedconfig href和文本重寫已啟用	是

此案例提供有關使用其中一個websecurityadvancedconfig選項後，defangs操作的行為如何更改的資訊。websecurityadvancedconfig是特定於電腦級別的CLI命令，允許調整特定於URL掃描的設定。此處其中一個設定允許您更改預設操作的預設行為。

```
> 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
...
```

在第四個問題上， **Do you want to rewrite both the URL text and the href in the message? ..**，答案 **Y** 指示在郵件中基於HTML的MIME部分的情況下，無論在A-tag元素的href屬性中是否找到所有匹配的URL字串，它都是文本部分或重寫的任何元素的外部。在此案例中，相同的訊息重新傳送，但結果略有不同。

再次檢視帶有URL的text/html MIME部分代碼，並將其與電子郵件網關處理的HTML代碼進行比較。

```
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
```

當啟用href和文本重寫選項時，無論該URL地址是href屬性的一部分還是A-tag HTML元素的文本部分，或者是在HTML文檔的其他部分中找到，都會定義與篩選器URL匹配的所有內容。

```
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version: 1.0 Content-Transfer-Encoding: 7bit

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://cisco.com and some text

--===============7781793576330041025==--
```

現在，當A-tag元素與URL格式匹配時，會隨連結文本部分的重寫一起剝離，從而重寫已定義的URL。重寫的文本部分以與MIME消息的文本/純文字檔案部分相同的方式完成。該項放置在BLOCKED單詞之間，所有點都放在方括弧之間。這阻止使用者複製和貼上URL，並且某些電子郵件軟體客戶端使文本可按一下。

總結：

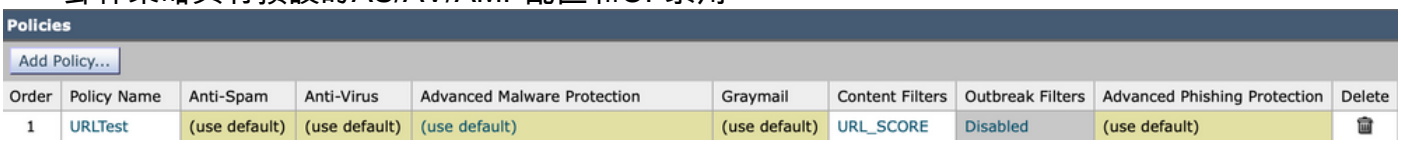
- 在TEXT/PLAIN部分上運行的防禦將URL重寫為BLOCKED塊
- 刪除A標籤時，在TEXT/HTML部件上運行的取消標籤會重寫來自HTML A標籤的URL
- 在TEXT/HTML部分上運行的預設將匹配的所有字串重寫為BLOCKED塊

第II部分 — 重新導向

組態

在第二部分中，組態使用：

- 郵件策略具有預設的AS/AV/AMP配置和OF禁用



Policies

Add Policy...

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)	

- 傳入內容過濾器：已啟用URL_SCORE內容篩選器

Filters

Add Filter...

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); }		

內容過濾器使用URL信譽條件來匹配惡意URL，即得分在–6.00和–10.00之間的惡意URL。作為操作，將記錄內容過濾器名稱， **redirect action** 被拿走了。

重定向操作

重定向到用於點選時間評估的思科安全代理服務允許消息收件人點選連結並重定向到雲中的思科網路安全代理，如果站點被識別為惡意站點，該代理會阻止訪問。

案例C

爆發過濾器非病毒威脅檢測	否
內容篩選器操作	重新導向
websecurityadvancedconfig href和文本重寫已啟用	否

此情境的行為與第一部分的情境A非常相似，因為內容篩選動作與重新導向URL而不是取消它的方式不同。websecurityadvancedconfig設定將還原為預設設定，這意味著 **"Do you want to rewrite both the URL text and the href in the message? ..** 設定為 **N.**

電子郵件網關檢測並評估每個URL。惡意得分觸發URL_SCORE內容過濾器規則並執行操作 **url-reputation-proxy-redirect-action**

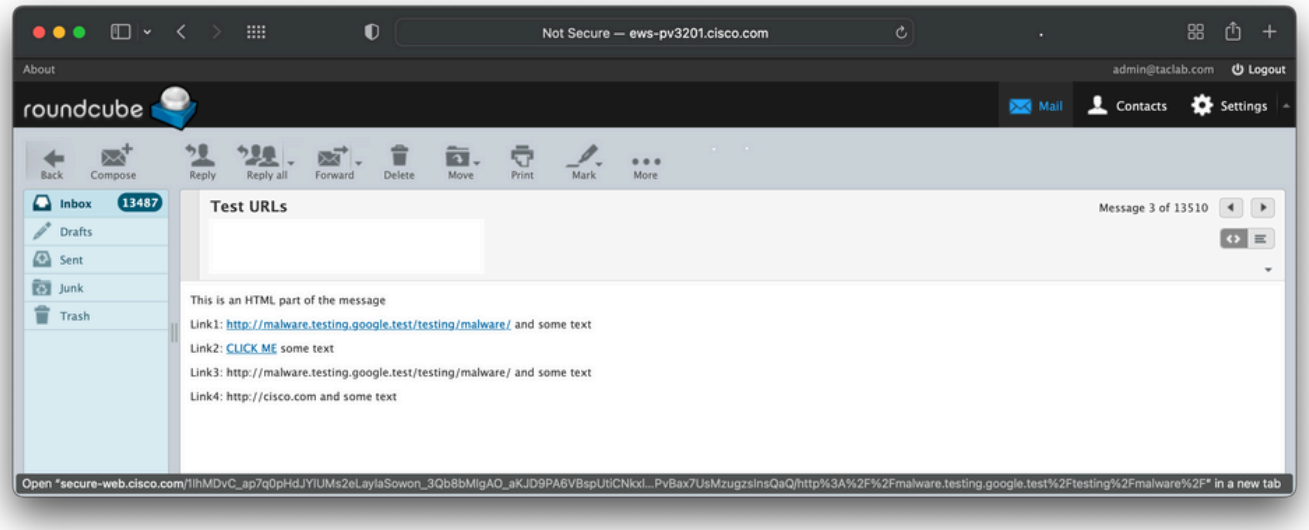
```
Tue Jul 5 12:42:19 2022 Info: MID 139508 URL http://malware.testing.google.test/testing/malware/
has reputation -9.4 matched Condition: URL Reputation Rule Tue Jul 5 12:42:19 2022 Info: MID
139508 Custom Log Entry: URL_SCORE Tue Jul 5 12:42:19 2022 Info: MID 139508 URL
http://malware.testing.google.test/testing/malware/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

請看一下URL在郵件的HTML部分是如何重寫的。與場景A中的情況相同：僅重寫A標籤元素的href屬性中找到的URL，並跳過在A標籤元素的文本部分中找到的URL地址。使用反方向操作將刪除整個A-tag元素，但使用重定向操作將重寫href屬性中的URL。

```
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version:
1.0 Content-Transfer-Encoding: 7bit

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

--===============7781793576330041025==--
```

因此，電子郵件客戶端顯示兩個活動連結：Link1和Link2均指向思科網路安全代理服務，但電子郵件客戶端中顯示的消息顯示A標籤的文本部分，預設情況下不重寫。為了更好地理解這一點，請檢視顯示郵件文本/html部分的Web郵件客戶端的輸出。



在MIME部分的文本/純文字檔案部分，重定向看起來更容易理解，因為每個與分數匹配的URL字串都會被重寫。

```
--===============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==
```

總結：

- 在TEXT/PLAIN部分上運行的重定向會重寫與Cisco Web Secure Proxy服務匹配的URL字串
- 在TEXT/HTML部分上運行的重定向使用Cisco Web安全代理服務重寫來自HTML A-tag href屬

性的URL，但保留所有匹配的URL字串未修改

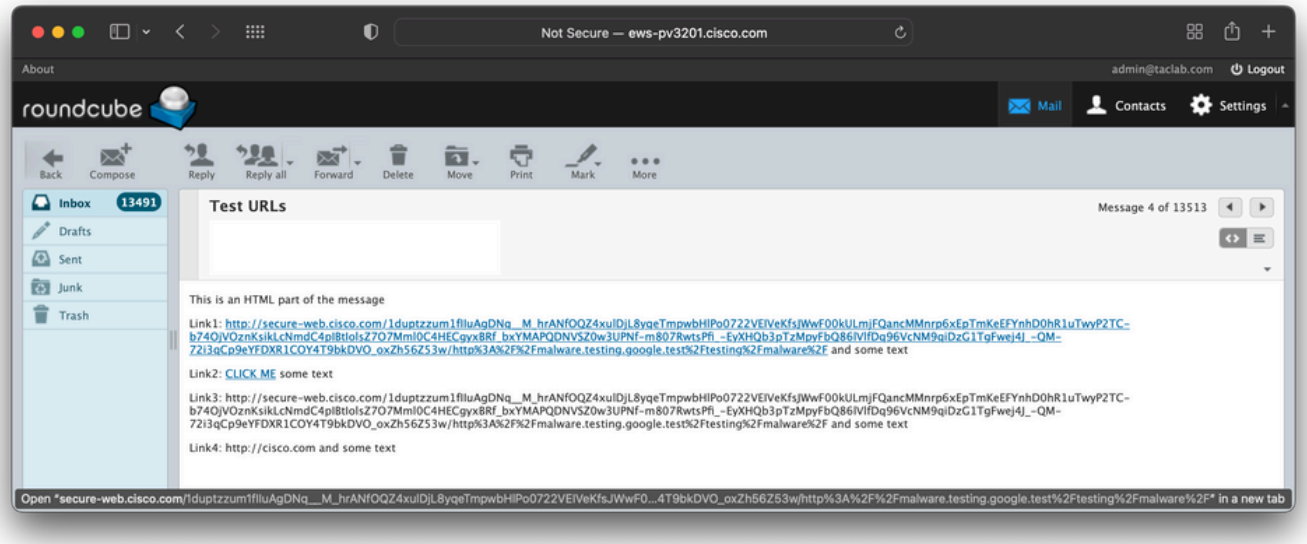
案例D

爆發過濾器非病毒威脅檢測	否
內容篩選器操作	重新導向
websecurityadvancedconfig href和文本重寫已啟用	是

此案例類似第一部分中的案例B。重新寫入消息的HTML部分中匹配的所有URL字串已啟用。當您對 **"Do you want to rewrite both the URL text and the href in the message? ..** 問題。

```
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version:
1.0 Content-Transfer-Encoding: 7bit

This is an HTML 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: CLICK ME some text

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

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

--===============7781793576330041025==--
```

啟用href和文本重寫後，所有與內容過濾器條件相匹配的URL字串都會被重定向。現在，電子郵件客戶端中的郵件會顯示所有重新導向。要更好地理解這一點，請檢視顯示郵件文本/html部分的Web郵件客戶端的輸出。



MIME郵件的文本/純文字檔案部分與場景C中的相同，因為websecurityadvancedconfig更改對郵件的文本/純文字檔案部分沒有任何影響。

```
--===============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==
```

總結：

- 在TEXT/PLAIN部分上運行的重定向會重寫與Cisco Web Secure Proxy服務匹配的URL字串
- 在TEXT/HTML部分上執行的重定向將重寫來自HTML A-tag href屬性的URL，同時重寫文本部分以及任何與Cisco Web Secure代理服務在HTML正文中匹配的URL字串

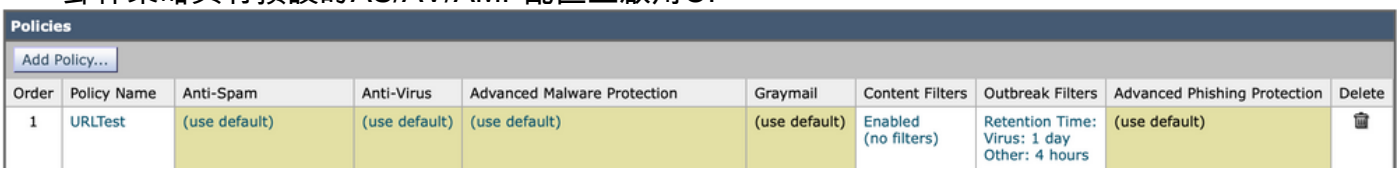
第3部分 — 重定向

本部分提供有關非病毒威脅檢測OF設定如何影響URL掃描的資訊。

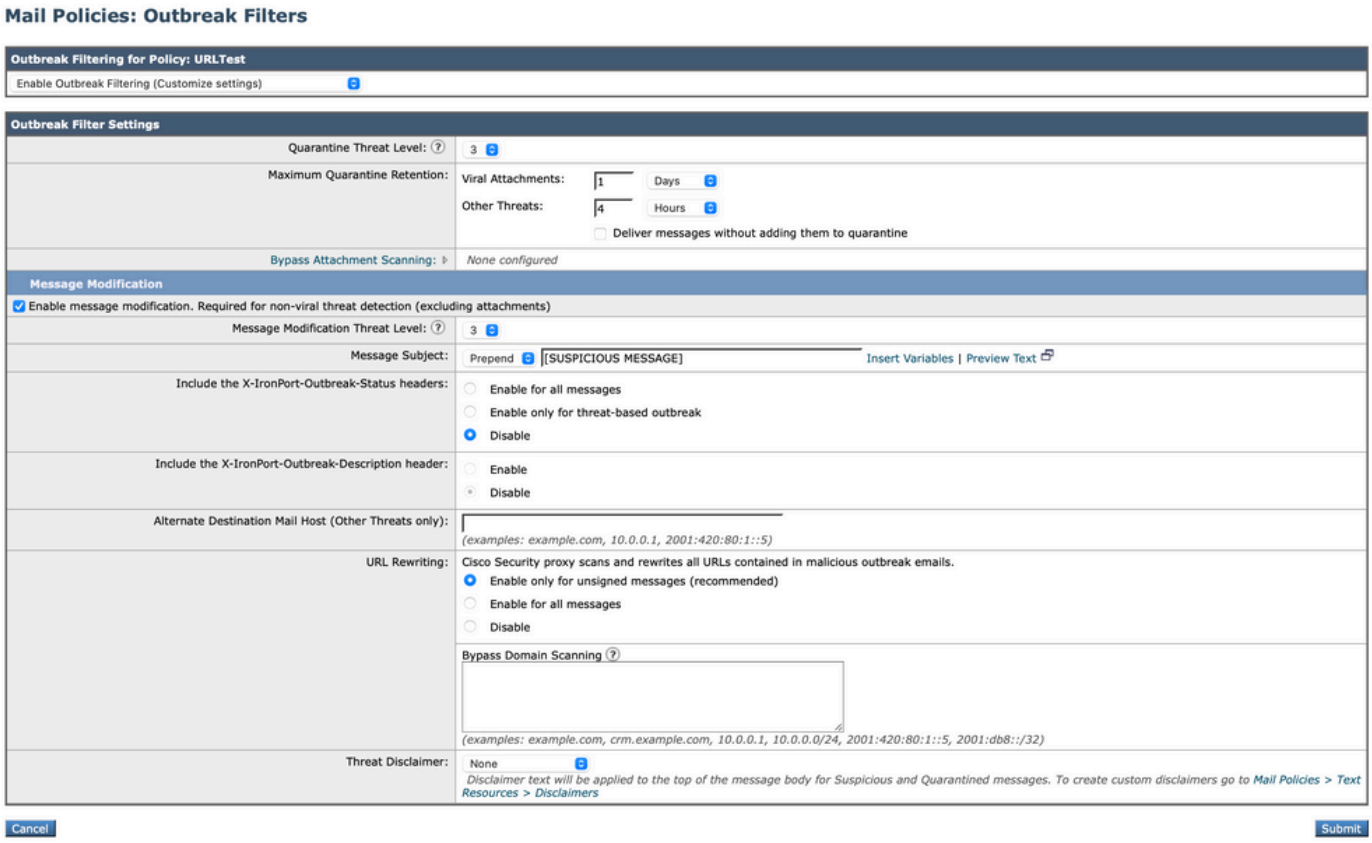
組態

為此，禁用前兩個部分中使用的內容過濾器。

- 郵件策略具有預設的AS/AV/AMP配置並啟用OF



- 用於非病毒威脅檢測的爆發過濾器掃描已配置URL重寫集，以重寫惡意電子郵件中包含的所有URL



如果郵件被歸類為OF（惡意），則其中的所有URL都將使用Cisco Web Secure Proxy服務重新寫入。

案例E

爆發過濾器非病毒威脅檢測	是
內容篩選器操作	否
websecurityadvancedconfig href和文本重寫已啟用	否

此案例顯示只啟用OF並禁用websecurityadvancedconfig href和文本重寫的情況下，消息重寫如何工作。

```
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)
```

讓我們從文本/純MIME部分開始。快速檢查後，可以觀察到，文本/純文字檔案部分內的所有URL都重新寫入到Cisco Web Secure Proxy服務。發生這種情況是因為對爆發惡意消息內的所有URL都啟用了URL重寫。

```
--===============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==

這是MIME郵件的已處理文本/html部分。

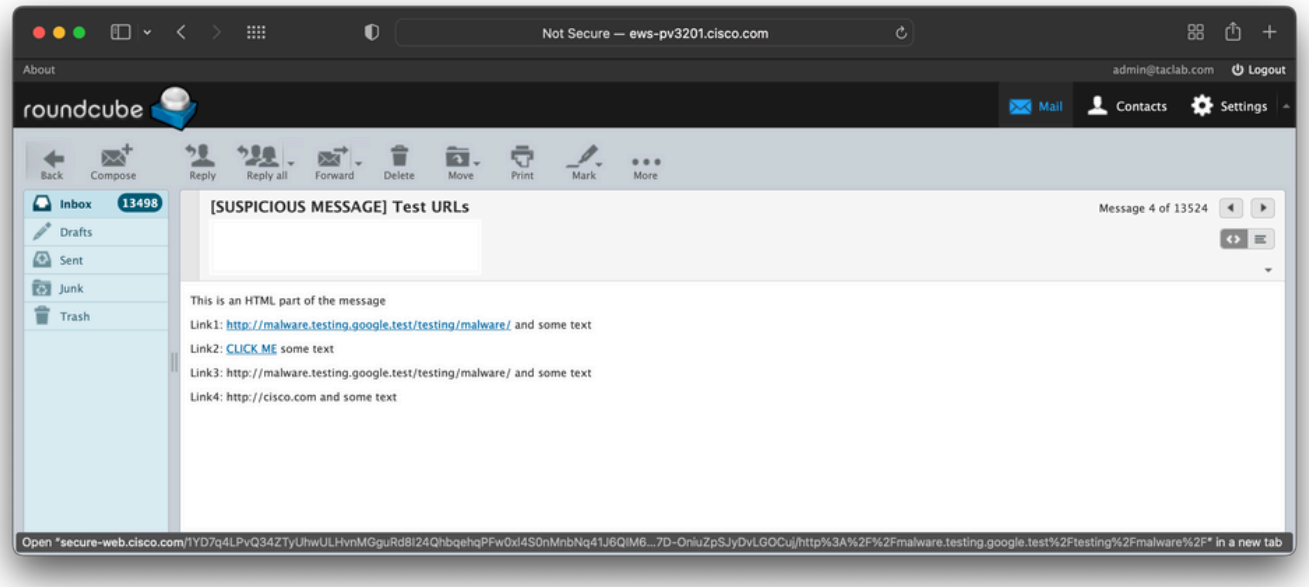
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version: 1.0 Content-Transfer-Encoding: quoted-printable

This is an HTML part of the message

=20
Link1: http://ma= lware.testing.google.test/testing/malware/ and some text

Link2: CLICK ME<= /a> some text

Link3: http://malware.testing.google.test/testing/malware/ and some= textLink4: http://cisco.com and some text=20 --===============7781793576330041025==--



首先要說明的是為什麼沒有重寫Link4。如果你仔細地閱讀這篇文章，你已經知道答案了。預設情況下，MIME的text/html部分僅計算並處理A-tag元素的href屬性。如果需要類似文本/純文字檔案部分的行為，則必須啟用websecurityadvancedconfig href和文本重寫。下一個場景正是如此。總結：

- 在TEXT/PLAIN部分運行的OF重定向重寫所有與Cisco Web Secure Proxy服務匹配的URL字串
- 在TEXT/HTML部分上運行的OF重定向僅重寫來自HTML A-tag href屬性的URL，該屬性帶有Cisco Web Secure代理服務

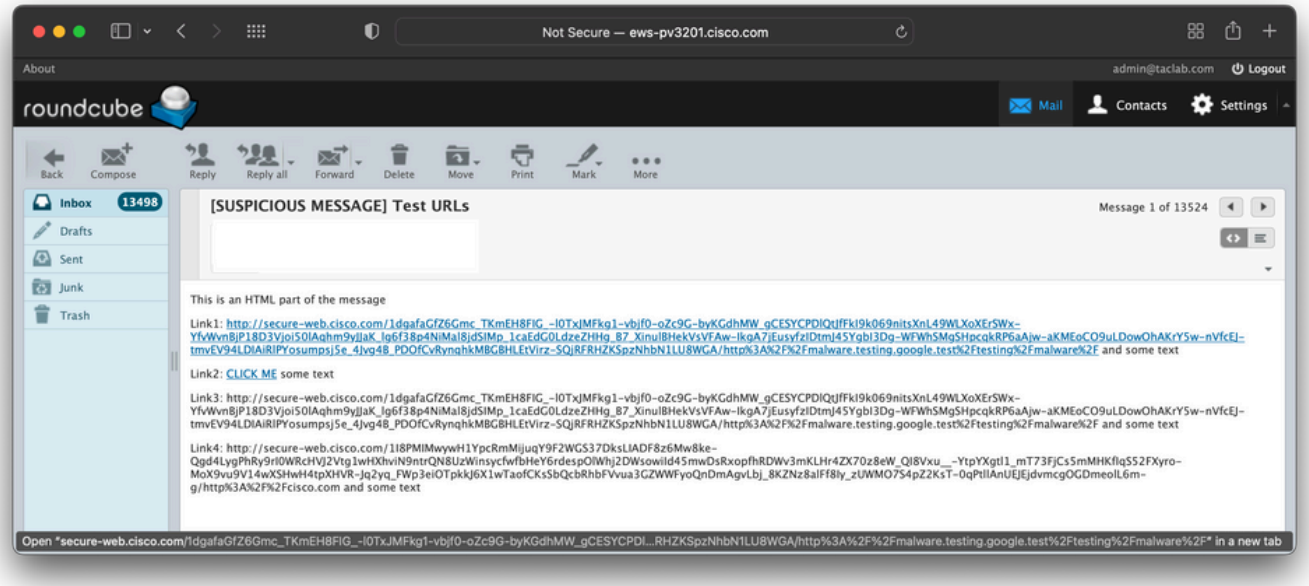
案例F

爆發過濾器非病毒威脅檢測	是
內容篩選器操作	否
websecurityadvancedconfig href和文本重寫已啟用	是

此方案使websecurityadvancedconfig href和文本重寫能夠顯示OF非病毒威脅檢測提供的URL重寫中的行為如何更改。此時必須瞭解，websecurityadvancedconfig不會影響文本/純文MIME部分。讓我們只評估text/html部分，並檢視行為是如何變化的。

```
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version:
1.0 Content-Transfer-Encoding: quoted-printable

This is an HTML part of the message

=20
Link1: 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_and_some_text

Link2: CLICK ME some text

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

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

=20 --===============7781793576330041025==--
```

可以注意到，輸出與場景D的輸出非常相似，唯一的區別是所有URL都被重寫，而不僅僅是惡意的URL。此處將修改HTML部分中與非惡意部分匹配的所有URL字串。



總結：

- 在TEXT/PLAIN部分上運行的OF重定向重寫所有與Cisco Web Secure Proxy服務匹配的URL字串
- 在TEXT/HTML部分上運行的OF重定向會重寫來自HTML A-tag href屬性的URL，以及元素的文本部分和與Cisco Web安全代理服務匹配的所有其他URL字串

案例G

爆發過濾器非病毒威脅檢測	是
內容篩選器操作	德芳
websecurityadvancedconfig href和文本重寫已啟用	是

最後一個方案驗證配置。

- 郵件策略具有預設的AS/AV/AMP配置並啟用OF

Policies

Add Policy...

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)	

- 用於非病毒威脅檢測的OF掃描配置為「URL重寫」設定，以重寫惡意電子郵件中包含的所有URL（與先前的場景相同）
- 傳入內容過濾器：已啟用URL_SCORE內容篩選器

Filters

Add Filter...

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); }		

內容過濾器使用URL信譽條件來匹配惡意URL，即得分在–6.00和–10.00之間的惡意URL。作為操作，將記錄內容過濾器名稱並取消操作 **url-reputation-defang** 被拿走了。

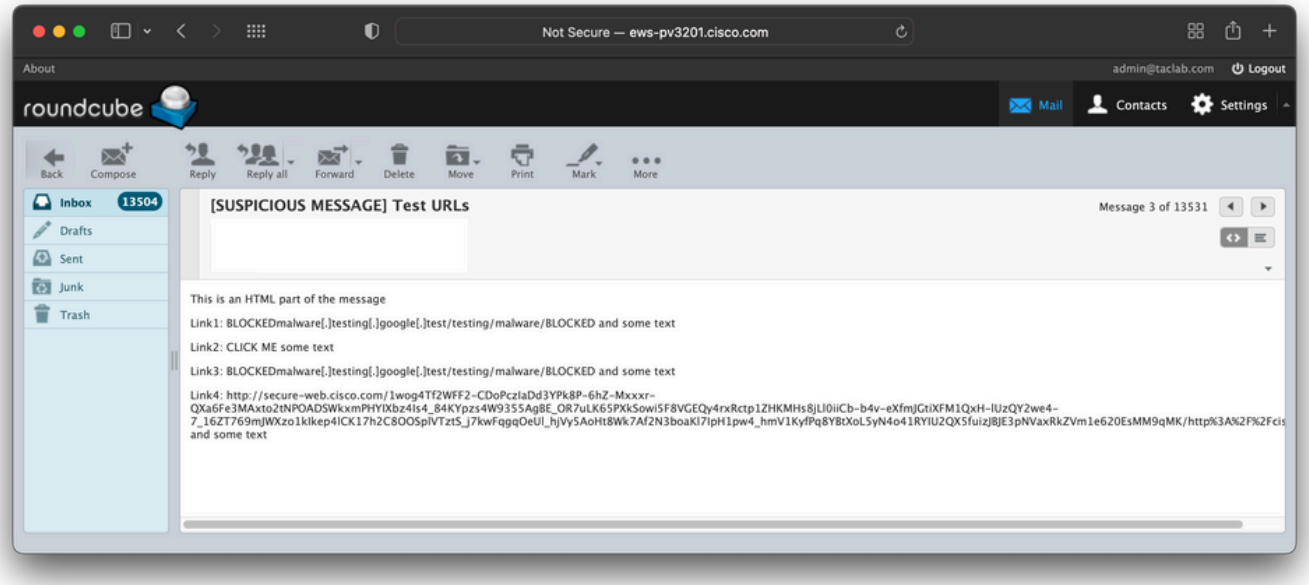
郵件網關傳送和評估郵件的同一副本，結果如下：

```
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
```

電子郵件管道說明郵件首先由內容過濾器評估，其中觸發URL_SCORE過濾器並應用URL-reputation-defang-action。此操作會將text/plain和text/html MIME部分中的所有惡意URL進行防禦。

由於啟用websecurityadvanceconfig href和文本重寫，因此當刪除所有A-tag元素並重寫URL在BLOCKED單詞之間的文本部分並將所有點置於方括弧之間時，將對HTML正文內匹配的所有所有URL字串進行縮寫。其他未放置在A-tag HTML元素中的惡意URL也會發生同樣的情況。 爆發過濾器接下來處理該消息。OF檢測惡意URL並將郵件識別為惡意（威脅級別=5）。 因此，它會重寫在郵件中找到的所有惡意和非惡意URL。由於內容過濾器操作已經修改了這些URL，因此OF只重寫其餘的非惡意URL，因為它是故意配置為這樣做的。作為惡意URL的一部分而顯示在電子郵件客戶端中的消息，已取消非惡意URL的一部分且已重定向該消息。

```
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version:
1.0 Content-Transfer-Encoding: quoted-printable

This is an HTML part of the message

=20
Link1: BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLO= CKED and some text

Link2: CLICK ME some text

Link3: BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLO= CKED and some text

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

=20 --===============7781793576330041025==--
```



這同樣適用於MIME郵件的文本/純文字檔案部分。所有非惡意URL都會重新導向到Cisco Web Secure Proxy，並且惡意URL會進行防禦。

```
--===============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==
```

總結：

- 在TEXT/PLAIN部分上運行的CF預設將URL重寫為BLOCKED塊
- 剝去A標籤後，TEXT/HTML部件上的CF定義會重寫來自HTML A標籤的URL
- 在TEXT/HTML部分上運行的CF預設將匹配的所有字串重寫為BLOCKED塊
- 在TEXT/PLAIN部分上運行的OF重定向重寫所有與Cisco Web Secure Proxy服務匹配的URL字串（非惡意）
- 在TEXT/HTML部分上執行的OF重新導向會從HTML A-tag href屬性以及元素的文本部分和與Cisco Web安全代理服務相匹配的所有其他URL字串中重新寫入URL（非惡意）

疑難排解

如果需要調查URL重寫問題，請遵循以下幾點。

- 在mail_logs中啟用URL日誌記錄。運行 **OUTBREAKCONFIG** 命令和應答 **Y** 成長至 **Do you wish to enable logging of URL's?** [N]>」
- 驗證 **WEBSECURITYADVANCECONFIG** 在每個電子郵件網關群整合員下的設定，並確保在每台電腦上相應地設定了href和文本重寫選項。請記住，此命令是特定於電腦級別的，在此處進行的更改不會影響組或群集設定。
- 驗證內容過濾器的條件和活動，並確保內容過濾器已啟用且應用於正確的傳入郵件策略。驗證之前是否未處理任何其他內容過濾器，以通過可跳至處理其他過濾器的最終操作。
- 調查源郵件和最終郵件的原始副本。請記住，要以EML格式檢索郵件，MSG等專有格式在郵件調查方面不可靠。某些電子郵件客戶端允許您檢視源郵件，並嘗試使用其他電子郵件客戶端檢索郵件的副本。例如，MS Outlook for Mac允許您檢視郵件的源，而Windows版本僅允許您檢視郵件頭。

摘要

本文的目的是幫助在涉及URL重寫時更好地瞭解可用的配置選項。請務必記住，大多數電子郵件軟體都採用MIME標準構建現代郵件。這表示郵件的同一副本可以不同方式顯示，這取決於電子郵件客戶端功能或/和啟用模式（文本與HTML模式）。 預設情況下，大多數現代電子郵件客戶端使用HTML來顯示郵件。對於HTML和URL重寫，請記住，預設情況下，電子郵件網關僅重寫A-tag元素的href屬性中發現的URL。在許多情況下，這還不夠，必須考慮使用WEBSECURITYADVANCECONFIG命令啟用href和文本重寫。 請記住，這是一個機器級別的命令，為了在整個群集內保持一致性，更改必須分別應用於每個群整合員。