了解安全邮件网关上的URL防御和重定向操作

目录

简介

本文档介绍URL过滤器中使用的取消和重定向操作之间的差异，以及如何对href属性和文本使用可用的重写选项。

先决条件

要求

要根据URL信誉采取行动，或者对邮件和内容过滤器实施可接受的使用策略，必须全局启用爆发过滤器功能。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全电子邮件网关
- 爆发过滤器
- 内容和邮件过滤器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

URL过滤功能的一个功能是使用消息和/或内容过滤器根据URL信誉或类别采取行动。根据URL扫描结果（URL相关条件），可以应用URL上的三个可用操作之一：

- Defang URL
- 重定向至思科安全代理
- 将URL替换为文本消息

本文档的重点是说明Defang和Redirect URL选项之间的行为。它还提供了爆发过滤器的非病毒威胁检测的URL重写功能的简要描述和说明。

消息示例

所有测试中使用的示例邮件是MIME multipart/alternative邮件类型，包括文本/纯文本和文本/html部分。这些部分通常由电子邮件软件自动生成，包含格式为HTML和非HTML接收器的相同类型的内容。为此，需要手动编辑文本/纯文本和文本/html的内容。

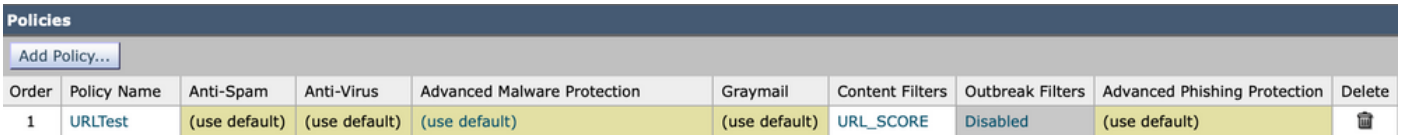
```
Content-Type: multipart/alternative; boundary="===============7781793576330041025==" MIME-
Version: 1.0 From: admin@example.com Date: Mon, 04 Jul 2022 14:38:52 +0200 To: admin@cisco.com
Subject: Test URLs --===============7781793576330041025== Content-Type: text/plain; charset="us-
ascii" MIME-Version: 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

配置

在第一部分，配置使用：

- 禁用默认反垃圾邮件(AS)/防病毒(AV)/高级恶意软件防护(AMP)配置和爆发过滤器(OF)的邮件策略



- 传入内容过滤器：已启用URL_SCORE内容过滤器

内容过滤器使用URL信誉条件来匹配恶意URL，这些URL的分数介于–6.00和–10.00之间。作为操作，将记录内容过滤器名称并取消操作 **url-reputation-defang** 已获取。

Defang操作

澄清什么是防御行动很重要。用户指南提供说明；拆除URL，使其不可单击。邮件收件人仍然可以查看和复制URL。

场景 A

爆发过滤器非病毒威胁检测	无
内容过滤器操作	德芳
websecurityadvancedconfig href和文本重写已启用	无

此场景说明了使用默认设置配置的取消操作的结果。在默认设置中，当仅删除HTML标记时，将重写URL。查看内部包含一些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
```

在前两段中，URL用适当的HTML A标记表示。<A>元素包括 **href=** 标记本身中包含的指示链路目标的属性。标记元素中的内容也可以表示链路目标。此 **text form** 可以包含URL。第一个Link1在元素的href属性和文本部分中都包含相同的URL链接。可以发现，这些URL可能不同。第二个Link2仅在href属性内包含正确的URL。最后一段不包括任何A要素。

> **注意**：将光标移动到链接上方或查看消息的源代码时，始终可以看到正确的地址。遗憾的是，在一些常用的电子邮件客户端上无法轻易找到源代码。

一旦邮件与URL_SCORE过滤器匹配，恶意URL就会被解除。当使用 **OUTBREAKCONFIG** 命令分数和URL可在mail_logs中找到。

```
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'
```

这会导致重写消息：

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

对MIME邮件的text/html部分执行去污操作的结果是删除的A标记，并且标记内容保持不变。在第一个的两个段落中，删除了两个链接，其中删除了HTML代码并保留了元素的文本部分。第一个段落中的URL地址是来自HTML元素文本部分的URL地址。必须注意的是，执行去污操作后，第一个段落中的URL地址仍然可见，但没有HTML A标记，元素不能可单击。第三段不进行缩写，因为此处的URL地址未置于任何A标记之间，并且不视为链接。也许这不是人们想要的行为，原因有二。首先，用户可以轻松查看并复制链接，然后在浏览器中执行。第二个原因是，一些电子邮件软件倾向于在文本内部检测到有效的URL形式，并使其成为可点击链接。

让我们看看MIME邮件的文本/纯文本部分。文本/纯文本部分在文本表单中包含两个URL。文本/纯文本由不理解HTML代码的MUA显示。在大多数现代电子邮件客户端中，您不会看到邮件的文本/纯文本，除非您有意将电子邮件客户端配置为这样做。通常，您需要检查邮件的源代码（一种原始邮件的EML格式）才能查看和调查MIME部分。

此处的列表显示源消息文本/纯文本部分的URL。

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

其中一条链路得了恶意得分并被拆除。默认情况下，对MIME类型的text/plain部分采取的去污操作与text/html部分采取的去污操作具有不同的结果。它位于BLOCKED words和方括号之间的所有点之间。

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

总结：

- 在TEXT/PLAIN部分运行Defang会将该URL重写为BLOCKED块
- 当A-tag被剥离，而A-tag之间的文本没有被触及（也可以是URL地址）时，在TEXT/HTML部分上运行的Defang会重写来自HTML A-tag的URL

场景 B

爆发过滤器非病毒威胁检测	无

内容过滤器操作	德芳
websecurityadvancedconfig href和文本重写已启用	Yes

此场景提供有关在使用websecurityadvancedconfig选项之一后防御操作的行为如何更改的信息。websecurityadvancedconfig是计算机级别的特定CLI命令，允许调整特定于URL扫描的设置。使用此处的其中一个设置可以更改取消操作的默认行为。

```
> 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
...
```

在第四个问题中， **Do you want to rewrite both the URL text and the href in the message? ..**，答案 **Y** 表示在邮件中基于HTML的MIME部分的情况下，无论在A-tag元素的href属性中是否找到所有匹配的URL字符串，它都是重写的任何元素的文本部分或外部。在这种情况下，重新发送相同的消息，但结果略有不同。

再次查看带有URL的text/html MIME部分代码，并将其与邮件网关处理的HTML代码进行比较。

```
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
```

当启用href和文本重写选项时，无论该URL地址是href属性的一部分还是A-tag HTML元素的文本部分，或者是在HTML文档的其他部分中找到，都默认匹配过滤器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: 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==--
```

现在，当A-tag元素与URL格式匹配时，会随链接文本部分的重写一起剥离，并重写该元素时，会重写已取消固定的URL。重写的文本部分以与MIME邮件的文本/纯文本部分相同的方式完成。该项放置在BLOCKED字词之间，所有点都放在方括号之间。这会阻止用户复制和粘贴URL，并且某些电子邮件软件客户端会将该文本设置为可点击。

总结：

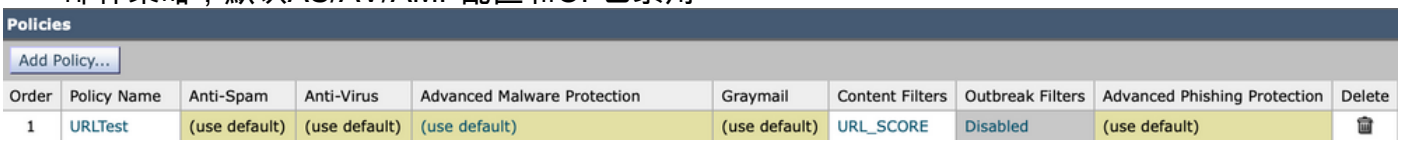
- 在TEXT/PLAIN部分运行Defang会将该URL重写为BLOCKED块
- 当A标记被删除时，在TEXT/HTML部分上运行的取消标记会重写来自HTML A标记的URL
- 在TEXT/HTML部分运行Defang将匹配的所有字符串重写为BLOCKED块

第二部分 — 重定向

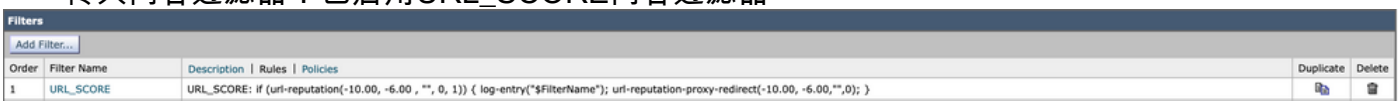
配置

在第二部分中，配置使用：

- 邮件策略，默认AS/AV/AMP配置和OF已禁用



- 传入内容过滤器：已启用URL_SCORE内容过滤器



内容过滤器使用URL信誉条件来匹配恶意URL，这些URL的分数介于–6.00和–10.00之间。作为操作，将记录内容过滤器名称，并且 **redirect action** 已获取。

重定向操作

重定向到用于点击时间评估的思科安全代理服务允许消息收件人点击链接并重定向到云中的思科网络安全代理，如果站点被识别为恶意站点，该代理会阻止访问。

场景 C

爆发过滤器非病毒威胁检测	无
内容过滤器操作	重定向
websecurityadvancedconfig href和文本重写已启用	无

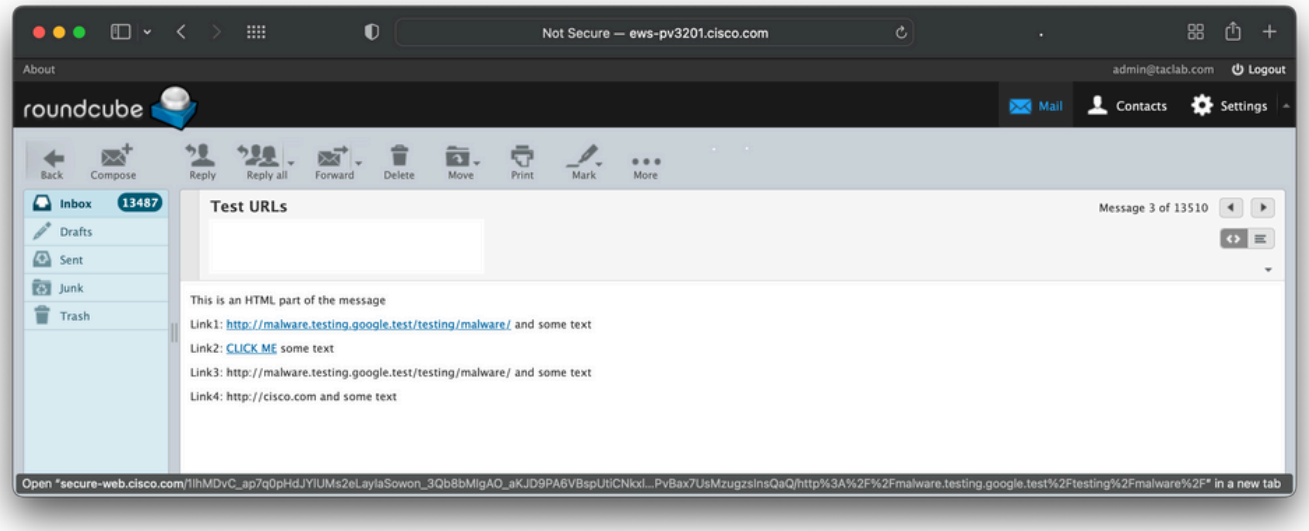
此场景在行为上与第一部分中的场景A非常相似，内容过滤器操作中的差异在于重定向而非取消删除URL。websecurityadvancedconfig设置将还原为默认设置，这意味着 **"Do you want to rewrite both the URL text and the href in the message? ..** 设置为 **N.**

电子邮件网关检测并评估每个URL。恶意评分会触发URL_SCORE内容过滤器规则并执行操作 **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'
```
了解在邮件的HTML部分如何重写URL。与方案A中相同，仅重写A-tag元素的href属性中找到的URL，并跳过在A-tag元素的文本部分中找到的URL地址。使用去污操作，整个A-tag元素被去除，但使用重定向操作，href属性中的URL被重写。

```
--===============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，电子邮件客户端显示两个活动链接：Link1和Link2均指向思科网络安全代理服务，但邮件客户端中显示的消息会显示A-tag的文本部分，默认情况下不会重写。为了更好地理解这一点，请查看显示邮件文本/html部分的Web邮件客户端的输出。



在MIME部分的文本/纯文本部分，重定向看起来更容易理解，因为匹配得分的每个URL字符串都会被重写。

```
--===============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==
```
总结：

- 对TEXT/PLAIN部分运行的重定向会重写与Cisco Web Secure代理服务匹配的URL字符串
- 在TEXT/HTML部分上运行的重定向使用Cisco Web Secure代理服务从HTML A-tag href属性重

写URL，但保留所有匹配未修改的URL字符串

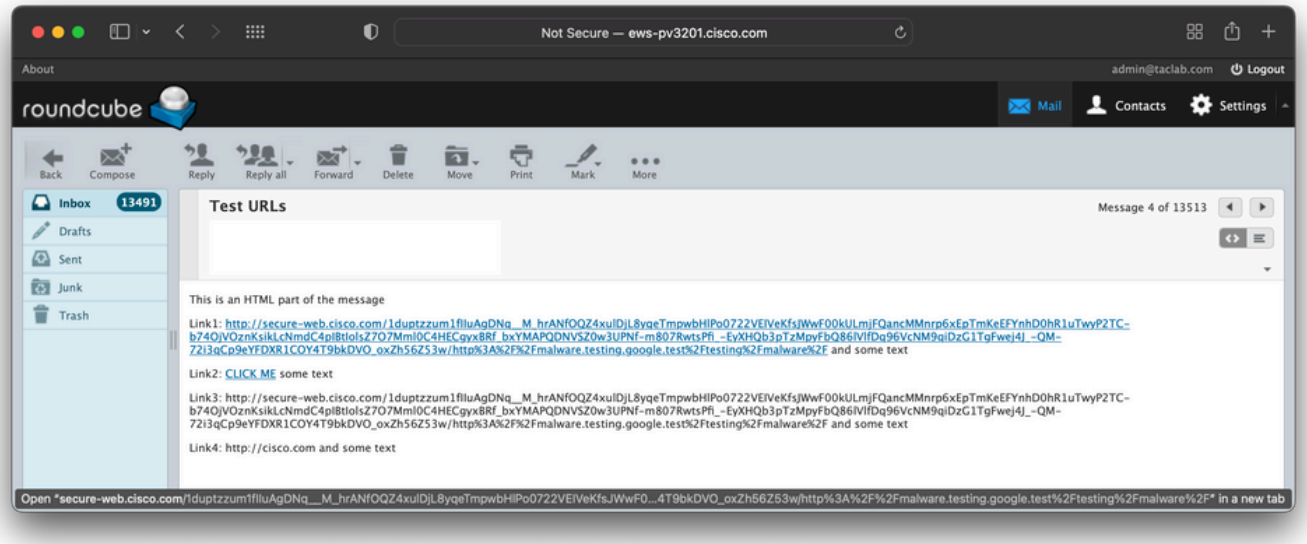
场景D

爆发过滤器非病毒威胁检测	无
内容过滤器操作	重定向
websecurityadvancedconfig href和文本重写已启用	Yes

此场景与第一部分的场景B类似。重新写入消息的HTML部分中匹配的所有URL字符串已启用。当您对 **"Do you want to rewrite both the URL text and the href in the message? ..** 问题。

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

启用href和文本重写后，会重定向所有与内容过滤器条件匹配的URL字符串。邮件客户端中的邮件现在显示所有重定向。为了更好地理解这一点，请查看显示消息文本/html部分的Web邮件客户端的输出。



MIME邮件的文本/纯文本部分与场景C中的相同，因为websecurityadvancedconfig更改对邮件的文本/纯文本部分没有任何影响。

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

总结：

- 在TEXT/PLAIN部分上运行的重定向会重写与Cisco Web Secure代理服务匹配的URL字符串
- 在TEXT/HTML部分上运行的重定向会重写来自HTML A-tag href属性的URL，同时重写文本部分以及与Cisco Web Secure代理服务在HTML正文中匹配的任何其他URL字符串

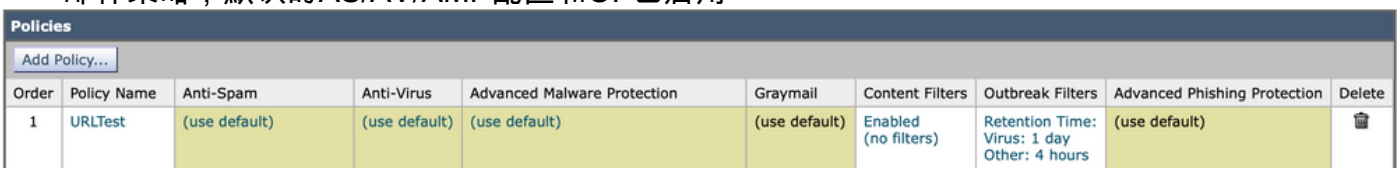
第3部分 — 重定向

本部分提供有关非病毒威胁检测OF设置如何影响URL扫描的信息。

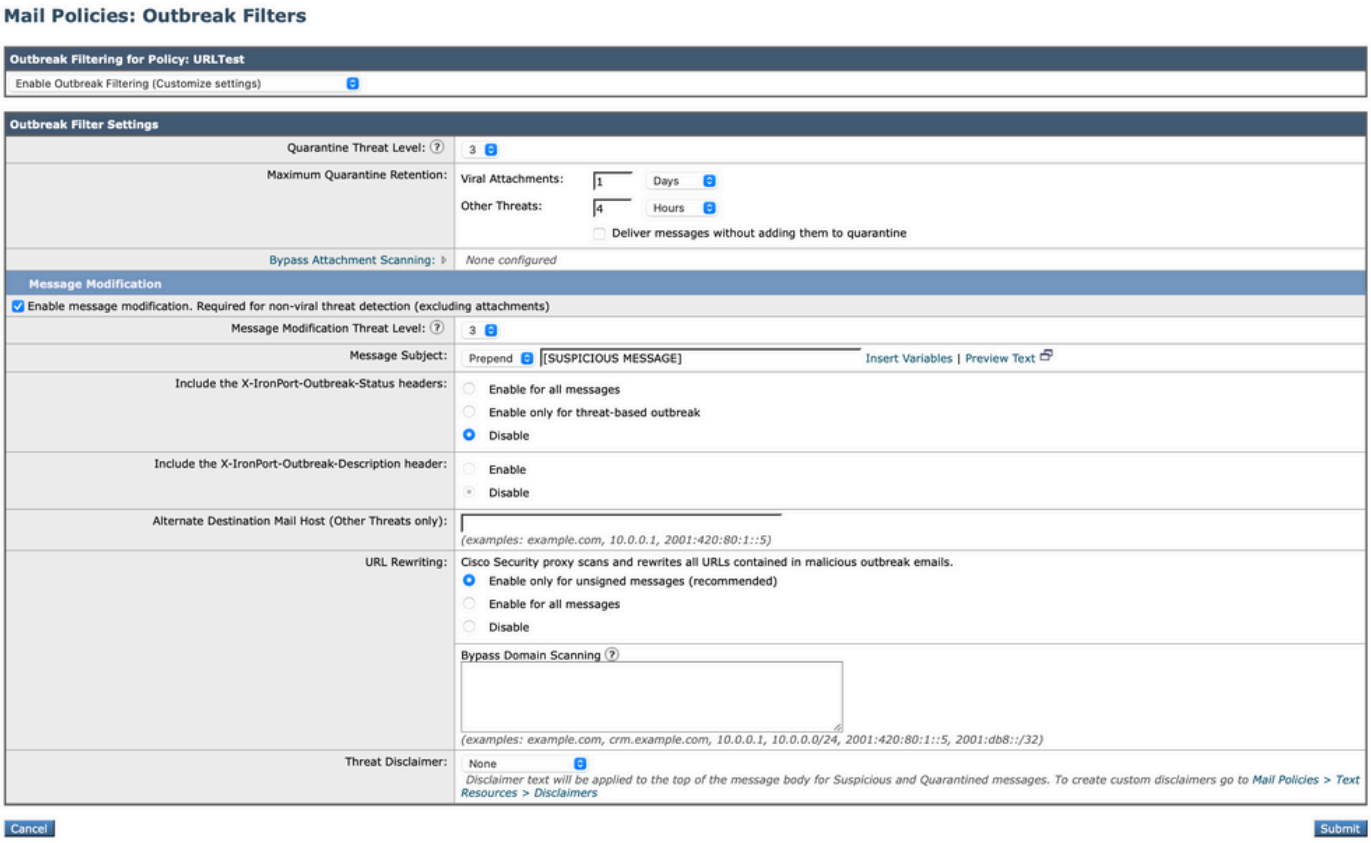
配置

为此，禁用前两个部分中使用的内容过滤器。

- 邮件策略，默认的AS/AV/AMP配置和OF已启用



- 用于非病毒威胁检测的爆发过滤器扫描配置了URL重写集，以重写恶意邮件中包含的所有URL



当邮件被OF分类为“恶意”时，其中的所有URL都使用Cisco Web Secure代理服务重写。

场景E

爆发过滤器非病毒威胁检测	Yes
内容过滤器操作	无
websecurityadvancedconfig href和文本重写已启用	无

此场景显示消息重写如何仅在启用OF且禁用websecurityadvancedconfig href和文本重写的情况下工作。

```
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)
```

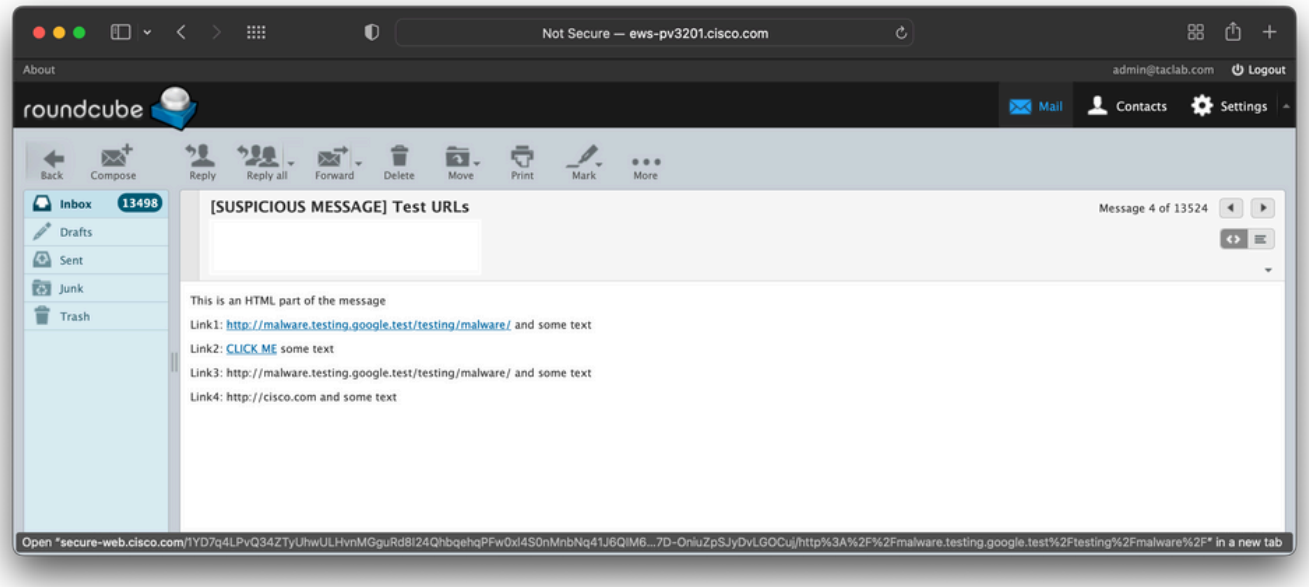
让我们从文本/纯MIME部分开始。快速检查后，可以发现文本/纯文本部分内的所有URL均被重写为Cisco Web Secure代理服务。发生这种情况是因为对爆发恶意消息内的所有URL都启用了URL重写。

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

这是MIME邮件的已处理文本/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==--
```



此处可以指出的第一个原因是Link4没有重写。如果你仔细地阅读这篇文章，你已经知道答案了。默认情况下，MIME的text/html部分仅评估和处理A-tag元素的href属性。如果需要类似文本/纯文本部分的行为，则必须启用websecurityadvancedconfig href和文本重写。下一个场景正是如此。总结：

- 在TEXT/PLAIN部分运行的OF重定向重写与Cisco Web Secure代理服务匹配的所有URL字符串
- OF在TEXT/HTML部分上运行的重定向仅重写来自HTML A-tag href属性的URL与思科Web安全代理服务

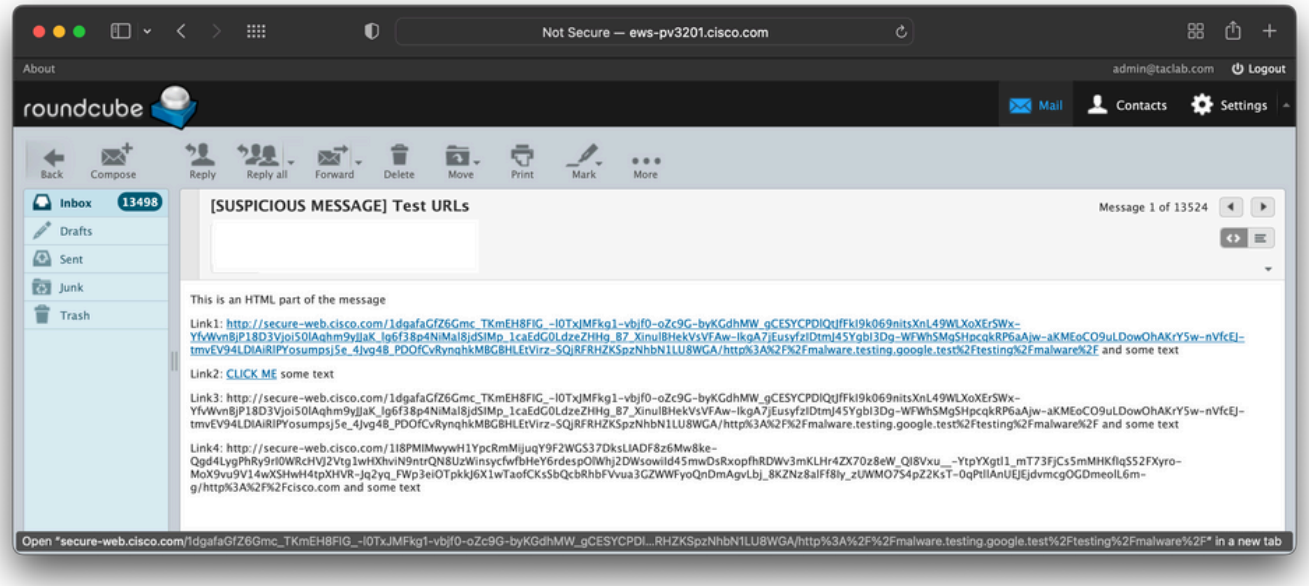
场景F

爆发过滤器非病毒威胁检测	Yes
内容过滤器操作	无
websecurityadvancedconfig href和文本重写已启用	Yes

此场景使websecurityadvancedconfig href和文本重写能够显示OF非病毒威胁检测提供的URL重写行为如何更改。此时必须了解，websecurityadvancedconfig不会影响文本/纯文本MIME部分。让我们只评估text/html部分并查看行为如何变化。

```
--===============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，输出与场景D的输出非常相似，唯一的区别是所有URL（不仅是恶意的URL）都已被重写。HTML部分中匹配的所有与非恶意的URL字符串都在此处修改。



总结：

- 在TEXT/PLAIN部分运行的OF重定向重写所有与Cisco Web Secure代理服务匹配的URL字符串
- 在TEXT/HTML部分运行的OF重定向，会重写来自HTML A-tag href属性的URL，以及元素文本部分和与Cisco Web Secure代理服务匹配的所有其他URL字符串

场景G

爆发过滤器非病毒威胁检测	Yes
内容过滤器操作	德芳
websecurityadvancedconfig href和文本重写已启用	Yes

最后一个场景验证配置。

- 邮件策略，默认的AS/AV/AMP配置和OF已启用

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	Retention Time: Virus: 1 day Other: 4 hours	(use default)	

- 用于非病毒威胁检测的OF扫描配置为“URL重写”(URL Rewrite)设置，以重写恶意邮件中包含的所有URL（与先前场景相同）
- 传入内容过滤器：已启用URL_SCORE内容过滤器

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); }		

内容过滤器使用URL信誉条件来匹配恶意URL，这些URL的分数介于–6.00和–10.00之间。作为操作，将记录内容过滤器名称并取消操作 **url-reputation-defang** 已获取。

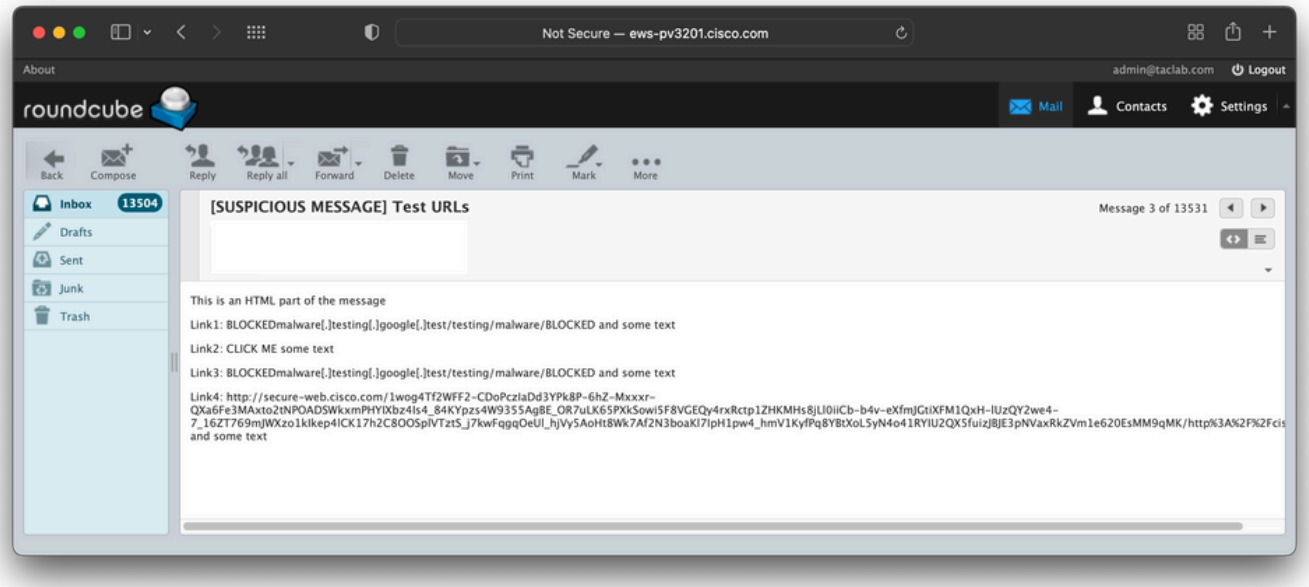
邮件网关发送和评估邮件的同一副本，结果如下：

```
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
```

邮件管道说明邮件首先由内容过滤器评估，其中触发URL_SCORE过滤器并应用URL-reputation-defang-action。此操作会同时取消文本/纯文本和文本/html MIME部分中的所有恶意URL的标记。由于启用了websecurityadvanceconfig href和文本重写，因此当所有A-tag元素被删除并重写

BLOCKED words之间URL的文本部分并将所有点置于方括号之间时，所有匹配HTML正文内的URL字符串都会被删除。其他未放置在A-tag HTML元素中的恶意URL也会发生同样的情况。 爆发过滤器接下来处理该邮件。OF检测恶意URL并将邮件识别为恶意（威胁级别=5）。 因此，它会重写在邮件中发现的所有恶意和非恶意URL。由于内容过滤器操作已经修改了这些URL，因此OF仅重写其余的非恶意URL，因为它是故意配置为这样做的。作为恶意URL的一部分和作为非恶意URL一部分重定向的邮件客户端中显示的消息。

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



这同样适用于MIME邮件的文本/纯文本部分。所有非恶意URL都重定向到Cisco Web Secure代理，并且恶意URL会进行防御。

```
--===============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==
总结：

- 在TEXT/PLAIN部分上运行的CF去污将该URL重写为BLOCKED块
- 当A标记被剥离时，在TEXT/HTML部分上运行的CF去污会从HTML A标记中重写URL
- 在TEXT/HTML部分上运行的CF取消将匹配到BLOCKED块的所有URL字符串重新写入
- 在TEXT/PLAIN部分运行的OF重定向重写所有与Cisco Web Secure代理服务匹配的URL字符串（非恶意）
- 在TEXT/HTML部分运行的OF重定向，会重写来自HTML A-tag href属性的URL，以及元素文本部分和与思科Web安全代理服务匹配的所有其他URL字符串（非恶意）

故障排除

如果需要调查URL重写问题，请遵循以下要点。

- 在mail_logs中启用URL日志记录。运行 **OUTBREAKCONFIG** 命令和应答 **Y** 到 **Do you wish to enable logging of URL's?** [N]**>**”
- 验证 **WEBSECURITYADVANCECONFIG** 每个邮件网关集群成员下的设置，并确保在每台计算机上相应地设置href和文本重写选项。请记住，此命令是特定于计算机的，并且在此处进行的更改不会影响组或集群设置。
- 验证内容过滤器的条件和活动，并确保内容过滤器已启用并应用于正确的传入邮件策略。验证之前是否未处理任何其他内容过滤器，以通过可跳至处理其他过滤器的最终操作。
- 检查源邮件和最终邮件的原始副本。请记住，要以EML格式检索邮件，MSG等专有格式在邮件调查时不可靠。某些电子邮件客户端允许您查看源邮件，并尝试使用其他电子邮件客户端检索邮件的副本。例如，MS Outlook for Mac允许您查看邮件的源，而Windows版本仅允许您查看信头。

摘要

本文的目的是帮助更好地了解URL重写时可用的配置选项。必须记住，大多数电子邮件软件都采用MIME标准构建现代邮件。这意味着邮件的同一副本可以不同方式显示，这取决于电子邮件客户端功能或/和启用模式（文本模式与HTML模式）。 默认情况下，大多数现代电子邮件客户端使用HTML来显示邮件。对于HTML和URL重写，请记住，默认情况下邮件网关仅重写A-tag元素的href属性内找到的URL。在许多情况下，这还不够，必须考虑使用WEBSECURITYADVANCECONFIG命令启用href和文本重写。 请记住，这是一个计算机级别的命令，为了在整个集群内保持一致，更改必须单独应用于每个集群成员。