Comprendre l'action de redirection et de désactivation d'URL sur la passerelle de messagerie sécurisée

Contenu

Introduction

Ce document décrit la différence entre les actions de désactivation et de redirection utilisées dans le filtre d'URL, et comment utiliser l'option de réécriture disponible pour l'attribut href et le texte.

Conditions préalables

Conditions requises

Pour prendre des mesures en fonction de la réputation des URL ou pour appliquer des stratégies d'utilisation acceptable avec les filtres de messages et de contenu, la fonctionnalité Filtres contre les attaques doit être activée globalement.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Passerelle de messagerie sécurisée Cisco
- Filtres contre les attaques
- Filtres de contenu et de message

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

L'une des fonctionnalités de filtrage d'URL consiste à prendre des mesures en fonction de la réputation ou de la catégorie d'URL à l'aide de filtres de messages et/ou de contenu. En fonction du résultat de l'analyse URL (condition liée à l'URL), l'une des trois actions disponibles sur une URL peut être appliquée :

- URL de définition
- Rediriger vers Cisco Security Proxy
- Remplacer l'URL par le message texte

L'objectif de ce document est d'expliquer le comportement entre les options Defang et Redirect URL. Il fournit également une brève description et une explication des fonctionnalités de réécriture d'URL de la détection de menaces non virales d'un filtre d'attaque.

Exemple de message

L'exemple de message utilisé dans tous les tests est le type de message MIME multipart/alternatif et inclut à la fois des parties text/plain et text/html. Ces parties sont généralement générées automatiquement par un logiciel de messagerie et contiennent le même type de contenu formaté pour les destinataires HTML et non HTML. Pour cela, le contenu de text/plain et text/html a été modifié manuellement.

```
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
```

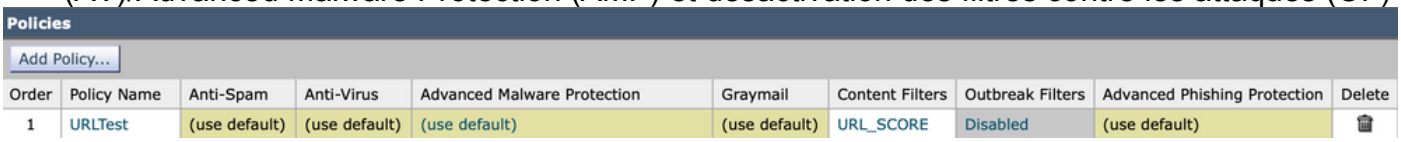
--==========77817935763300410 25==--

Partie I - Defang

Configurations

Dans la première partie, la configuration utilise :

- Politique de messagerie avec configuration par défaut de l'antispam (AS)/antivirus (AV)/Advanced Malware Protection (AMP) et désactivation des filtres contre les attaques (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	Disabled	(use default)	

- Filtre de contenu entrant : Filtre de contenu URL_SCORE activé

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); }		

Le filtre de contenu utilise la condition de réputation d'URL pour faire correspondre les URL malveillantes, celles dont le score est compris entre -6.00 et -10.00. En tant qu'action, le nom du filtre de contenu est consigné et l'action de défense **url-reputation-defang** est prise.

Action Defang

Il est important de clarifier ce qu'est une action de défense. Le guide de l'utilisateur fournit une explication ; Définissez une URL de sorte qu'elle ne soit pas cliquable. Les destinataires du message peuvent toujours voir et copier l'URL.

Scénario A

Détection des menaces non virales grâce au filtre anti-épidémies	Non
Action de filtrage de contenu	Défang
websecurityadvancedconfig href et la réécriture de texte est activée	Non

Ce scénario explique le résultat de l'action debug configurée avec les paramètres par défaut. Dans le paramètre par défaut, l'URL est réécrite lorsque seules les balises HTML sont supprimées. Jetez un oeil à un paragraphe HTML contenant des URL :

```
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
```

Dans les deux premiers paragraphes, l'URL est représentée par une balise A HTML appropriée. L'élément <A> inclut le **href=** qui est inclus dans la balise elle-même et indique la destination du

lien. Le contenu des éléments de balise peut également indiquer la destination du lien. Ceci **text form** du lien peut inclure l'URL. Le premier lien Link1 inclut le même lien URL dans l'attribut href et la partie texte de l'élément. Il est à noter que ces URL peuvent être différentes. Le deuxième lien Link2 inclut l'URL appropriée uniquement dans l'attribut href. Le dernier paragraphe ne contient pas d'éléments A.

> Note: L'adresse correcte est toujours visible lorsque vous déplacez le curseur sur le lien ou lorsque vous affichez le code source du message. Malheureusement, le code source ne peut pas être facilement trouvé avec certains clients de messagerie populaires.

Une fois que le filtre URL_SCORE correspond au message, les URL malveillantes sont défendues. Lorsque la journalisation d'URL est activée avec **OUTBREAKCONFIG** les scores et les URL sont disponibles dans 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'
```

Il en résulte le message réécrit :

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

Le résultat de l'action de défense effectuée sur la partie texte/html du message MIME est une balise A supprimée et le contenu de la balise est laissé intact. Dans les deux premiers paragraphes, les deux liens ont été définis lorsque le code HTML a été supprimé et que la partie texte de l'élément a été laissée. L'adresse URL du premier paragraphe est celle de la partie texte de l'élément HTML. Il est à noter que l'adresse URL du premier paragraphe est toujours visible après l'action defang, mais sans les balises A HTML, l'élément ne doit pas être cliquable. Le troisième paragraphe n'est pas défini car l'adresse URL n'est pas placée entre les balises A et n'est pas considérée comme un lien. Ce n'est peut-être pas un comportement souhaitable pour deux raisons. Tout d'abord, l'utilisateur peut facilement voir et copier le lien et l'exécuter dans le navigateur. La deuxième raison est que certains logiciels de messagerie tendent à détecter une forme valide d'URL à l'intérieur du texte et en faire un lien cliquable.

Jetons un coup d'oeil à la partie texte/simple du message MIME. La partie texte/ordinaire inclut deux URL dans le formulaire texte. Le texte/clair est affiché par MUA qui ne comprend pas le code

HTML. Dans la plupart des clients de messagerie modernes, vous ne voyez pas les parties texte/clair du message, sauf si vous avez intentionnellement configuré votre client de messagerie pour le faire. En général, vous devez vérifier le code source du message, un format EML brut du message pour voir et examiner les parties MIME.

La liste ci-dessous affiche les URL de la partie texte/ordinaire du message source.

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

L'un de ces deux liens a obtenu un score malveillant et a été mis en échec. Par défaut, l'action defang effectuée sur la partie texte/clair du type MIME a un résultat différent de celui de la partie texte/html. Elle se trouve entre les mots BLOQUÉS et tous les points entre crochets.

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

Résumé :

- Defang exécuté sur la partie TEXT/PLAIN réécrit l'URL en blocs BLOQUÉS
- Defang exécuté sur la partie TEXT/HTML réécrit l'URL à partir d'une balise A HTML lorsque la balise A est supprimée sans que le texte entre les balises A soit touché, qui peut également être une adresse URL

Scénario B

Détection des menaces non virales grâce au filtre anti-épidémies	Non
Action de filtrage de contenu	Défang
websecurityadvancedconfig href et la réécriture de texte est activée	Oui

Ce scénario fournit des informations sur la façon dont le comportement de l'action defangs change après l'utilisation de l'une des options websecurityadvanced config. La commande websecurityadvancedconfig est la commande CLI spécifique à la machine qui permet de régler les paramètres spécifiques à l'analyse URL. L'un des paramètres ici vous permet de modifier le comportement par défaut de l'action debug.

```
> 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
...
```

À la quatrième question, **Do you want to rewrite both the URL text and the href in the message? ..**, la réponse **Y** indique que, dans le cas de la partie MIME HTML du message, toutes les chaînes d'URL qui correspondent, qu'elles se trouvent dans l'attribut href de l'élément A-tag, sont des parties de texte ou en dehors des éléments réécrits. Dans ce scénario, le même message est envoyé, mais avec un résultat légèrement différent.

Examinez à nouveau le code MIME texte/html avec les URL et comparez-le au code HTML traité par la passerelle de messagerie.

```
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
```

Lorsque l'option href and text rewrite est activée, toutes les URL correspondant au filtre sont définies, que l'adresse URL fasse partie de l'attribut href ou de l'élément HTML A-tag, ou qu'elle se trouve dans une autre partie du document HTML.

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

Les URL définies sont maintenant réécrites lorsque l'élément A-tag est supprimé avec une réécriture de la partie texte du lien lorsqu'il correspond au format de l'URL. La partie texte réécrite est effectuée de la même manière que dans la partie texte/clair du message MIME. L'élément est placé entre des mots BLOQUÉS et tous les points sont placés entre crochets. Cela empêche l'utilisateur de copier et coller l'URL, et certains clients de logiciels de messagerie rendent le texte cliquable.

Résumé :

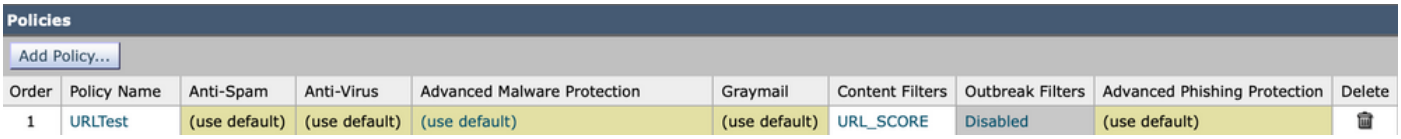
- Defang exécuté sur la partie TEXT/PLAIN réécrit l'URL en blocs BLOQUÉS
- Defang run sur la partie TEXT/HTML réécrit l'URL à partir d'une balise A HTML lorsqu'une balise A est supprimée
- Defang exécuté sur la partie TEXT/HTML réécrit toutes les chaînes d'URL qui correspondent en blocs BLOQUÉS

Partie II - Redirection

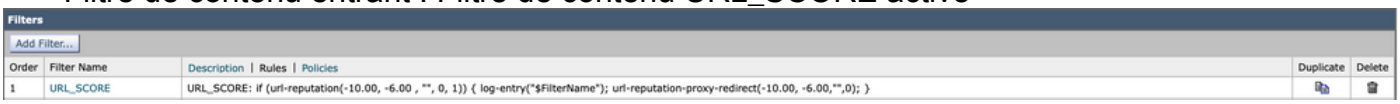
Configurations

Dans la deuxième partie, la configuration utilise :

- Stratégie de messagerie avec configuration AS/AV/AMP par défaut et OF désactivée



- Filtre de contenu entrant : Filtre de contenu URL_SCORE activé



Le filtre de contenu utilise la condition de réputation d'URL pour correspondre aux URL malveillantes, celles dont le score est compris entre -6,00 et -10,00. En tant qu'action, le nom du filtre de contenu est consigné et le **redirect action** est prise.

Action de redirection

Rediriger vers le service Cisco Security Proxy pour l'évaluation du temps de clic permet au destinataire du message de cliquer sur le lien et d'être redirigé vers un proxy de sécurité Web Cisco dans le cloud, qui bloque l'accès si le site est identifié comme malveillant.

Scénario C

Détection des menaces non virales grâce au filtre anti-épidémies	Non
Action de filtrage de contenu	Rediriger
websecurityadvancedconfig href et la réécriture de texte est activée	Non

Ce scénario présente un comportement très similaire à celui du scénario A de la première partie, avec la différence apportée par l'action de filtrage de contenu pour rediriger l'URL au lieu de la définir. Les paramètres websecurityadvanced config sont restaurés à leurs valeurs par défaut, ce qui signifie que **"Do you want to rewrite both the URL text and the href in the message? ..** est défini sur **N**.

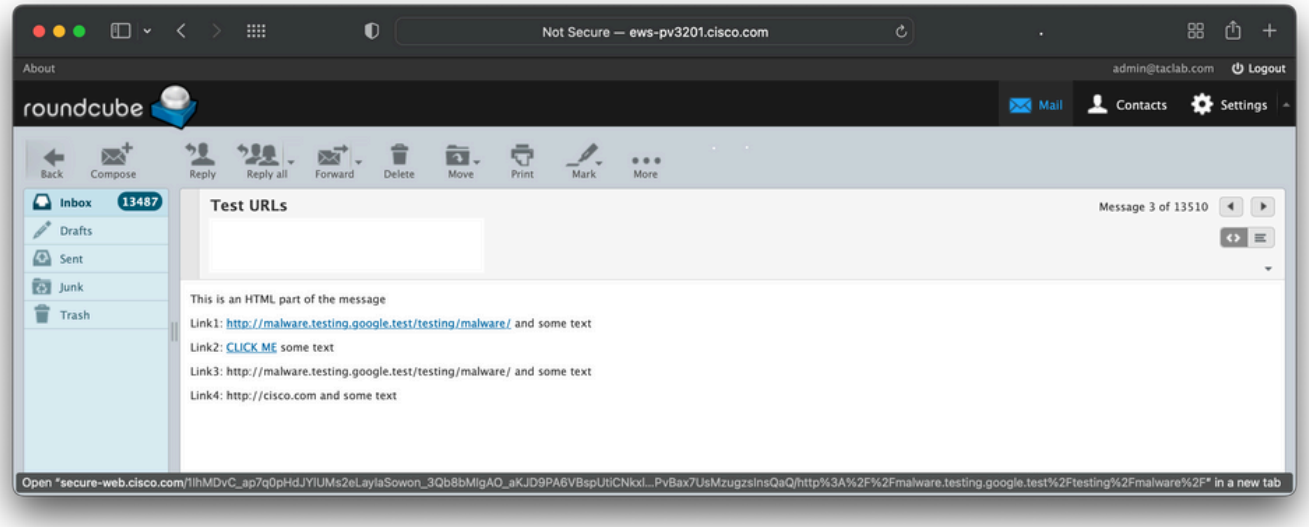
La passerelle de messagerie détecte et évalue chacune des URL. Le score malveillant déclenche la règle de filtre de contenu URL_SCORE et exécute l'action **url-reputation-proxy-redirect-action**

```
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'
```

Regardez comment les URL sont réécrites dans la partie HTML du message. Identique au scénario A, seules les URL trouvées dans l'attribut href d'un élément de balise A sont réécrites et les adresses URL trouvées dans la partie texte de l'élément de balise A sont ignorées. Avec une action de défang, un élément A-tag entier est supprimé, mais avec une action de redirection, l'URL dans l'attribut href est réécrite.

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

Par conséquent, le client de messagerie affiche deux liens actifs : Link1 et Link2, tous deux pointent vers le service Cisco Web Security Proxy, mais le message affiché dans le client de messagerie affiche la partie texte de la balise A qui n'est pas réécrite par défaut. Pour mieux comprendre ce message, consultez la sortie du client de messagerie Web qui affiche la partie texte/html du message.



Dans la partie texte/clair de la partie MIME, la redirection semble plus facile à comprendre, car chaque chaîne d'URL correspondant au score est réécrite.

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

Résumé :

- La redirection exécutée sur la partie TEXT/PLAIN réécrit la chaîne d'URL qui correspond au service proxy Cisco Web Secure
- La redirection exécutée sur la partie TEXT/HTML réécrit l'URL à partir d'un attribut href de balise A HTML avec le service proxy Cisco Web Secure, mais laisse toutes les autres chaînes d'URL qui correspondent non modifiées

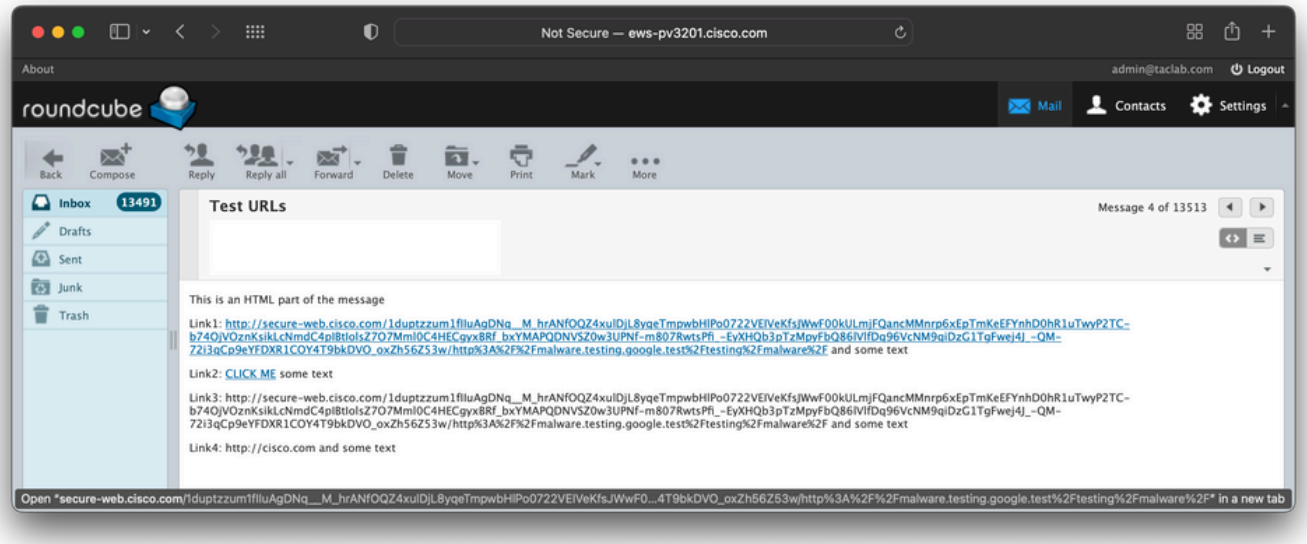
Scénario D

Détection des menaces non virales grâce au filtre anti-épidémies	Non
Action de filtrage de contenu	Rediriger
websecurityadvancedconfig href et la réécriture de texte est activée	Oui

Ce scénario est similaire au scénario B de la première partie. Pour réécrire toutes les chaînes d'URL qui correspondent dans la partie HTML du message est activé. Pour ce faire, utilisez la commande websecurityadvancedconfig lorsque vous répondez Y pour le **"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

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==--
```

Une fois la réécriture href et text activée, toutes les chaînes d'URL qui correspondent aux conditions du filtre de contenu sont redirigées. Le message du client de messagerie est maintenant présenté avec toute la redirection. Pour mieux comprendre cela, regardez la sortie du client de messagerie Web qui affiche la partie texte/html du message.



La partie texte/simple du message MIME est la même que dans le scénario C, car la modification de websecurityadvancedconfig n'a aucun impact sur la partie texte/simple du 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==
```

Résumé :

- La redirection exécutée sur la partie TEXT/PLAIN réécrit les chaînes d'URL qui correspondent au service proxy Cisco Web Secure
- L'exécution de redirection sur la partie TEXT/HTML réécrit l'URL à partir d'un attribut href de balise A HTML avec la partie text ainsi que toute autre chaîne URL qui correspond dans le corps HTML avec le service proxy Cisco Web Secure

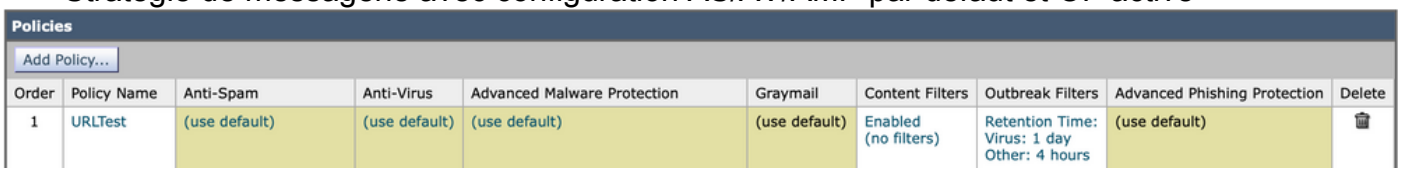
Partie 3 - Redirection de OF

Cette partie fournit des informations sur l'impact des paramètres de détection des menaces non virales sur les analyses d'URL.

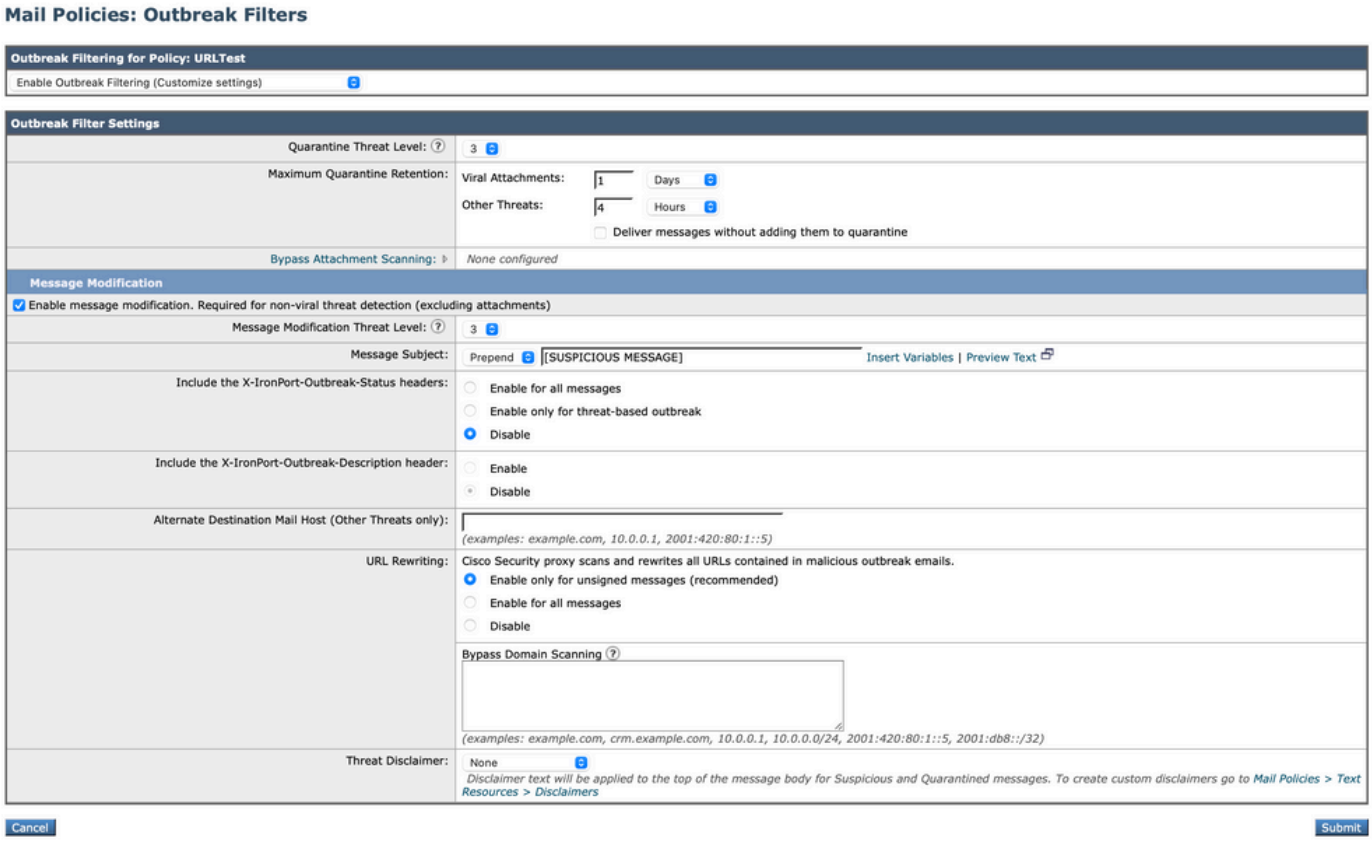
Configuration

Àcet effet, le filtre de contenu utilisé dans les deux premières parties est désactivé.

- Stratégie de messagerie avec configuration AS/AV/AMP par défaut et OF activé



- L'analyse des filtres contre les attaques pour la détection des menaces non virales est configurée avec un jeu de réécriture d'URL pour réécrire toutes les URL contenues dans les e-mails malveillants



Lorsque le message est classé par OF comme malveillant, toutes les URL qu'il contient sont réécrites avec le service proxy Cisco Web Secure.

Scénario E

Détection des menaces non virales grâce au filtre anti-épidémies	Oui
Action de filtrage de contenu	Non
websecurityadvancedconfig href et la réécriture de texte est activée	Non

Ce scénario montre comment la réécriture du message fonctionne uniquement avec OF activé et websecurityadvancedconfig href et text rewrite désactivés.

```
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)
```

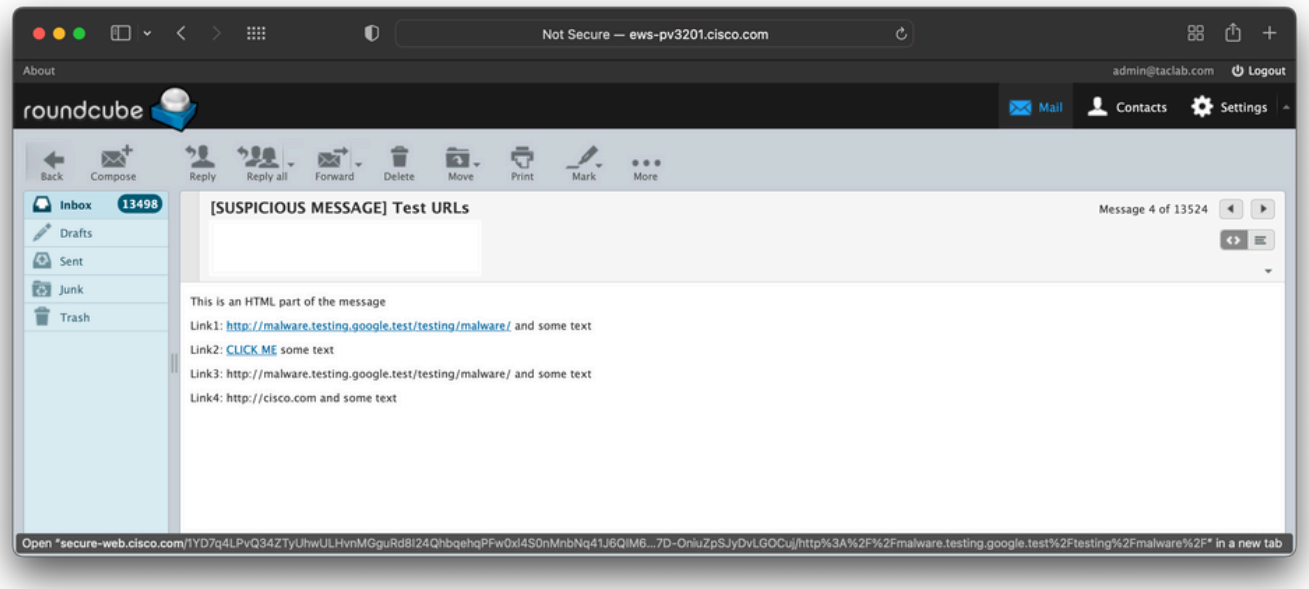
Commençons par la partie texte/MIME simple. Après une vérification rapide, on peut observer que toutes les URL à l'intérieur de la partie texte/clair sont réécrites dans les services proxy Cisco Web

Secure. Cela se produit parce que la réécriture d'URL est activée pour toutes les URL dans le message malveillant d'attaque.

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

Il s'agit de la partie texte/html traitée du message MIME.

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



La première chose à noter ici est la raison pour laquelle Link4 n'est pas réécrit. Si vous lisez attentivement l'article, vous connaissez déjà la réponse. Par défaut, la partie texte/html de MIME évalue et manipule uniquement les attributs href des éléments de balise A. Si un comportement similaire à celui de la pièce texte/ordinaire est souhaité, les commandes websecurityadvancedconfig href et text rewrite doivent être activées. Le scénario suivant fait exactement cela.Résumé :

- OF redirect exécuté sur la partie TEXT/PLAIN réécrit toute la chaîne d'URL correspondant au service proxy Cisco Web Secure
- OF redirect exécuté sur la partie TEXT/HTML réécrit uniquement l'URL à partir d'un attribut href de balise A HTML avec le service proxy Cisco Web Secure

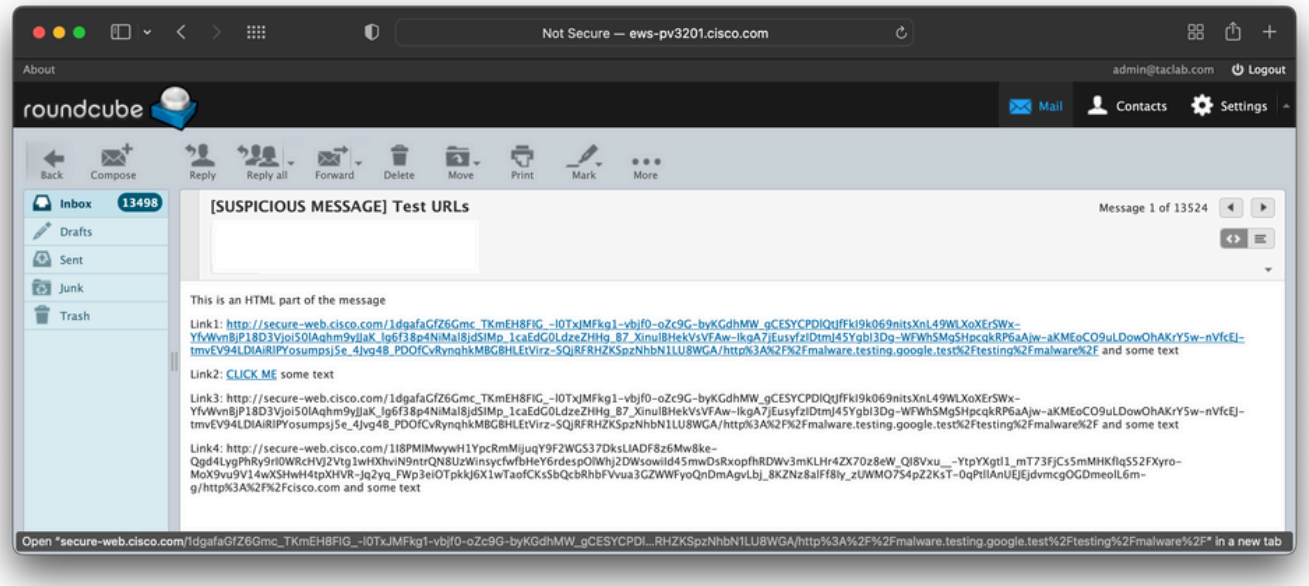
Scénario F

Détection des menaces non virales grâce au filtre anti-épidémies	Oui
Action de filtrage de contenu	Non
websecurityadvancedconfig href et la réécriture de texte est activée	Oui

Ce scénario active websecurityadvancedconfig href et text rewrite pour montrer comment le comportement de la réécriture d'URL fournie par la détection de menaces non virales OF change. À ce stade, il faut comprendre que websecurityadvancedconfig n'affecte pas les parties MIME texte/clair. Évaluons uniquement la partie text/html et voyons comment le comportement a changé.

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

On peut noter que le résultat est très similaire à celui du scénario D avec la seule différence que toutes les URL ont été réécrites, pas seulement les malveillantes. Toutes les chaînes d'URL qui correspondent dans la partie HTML avec celles qui ne sont pas malveillantes sont modifiées ici.



Résumé :

- OF redirect exécuté sur la partie TEXT/PLAIN réécrit toutes les chaînes d'URL qui correspondent au service proxy Cisco Web Secure
- OF redirect exécuté sur la partie TEXT/HTML réécrit l'URL à partir d'un attribut href de balise A HTML avec la partie texte de l'élément et toutes les autres chaînes d'URL qui correspondent au service proxy Cisco Web Secure

Scénario G

Détection des menaces non virales grâce au filtre anti-épidémies	Oui
Action de filtrage de contenu	Défang
websecurityadvancedconfig href et la réécriture de texte est activée	Oui

Ce dernier scénario valide la configuration.

- Stratégie de messagerie avec configuration AS/AV/AMP par défaut et OF activé

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)	

- L'analyse OF pour la détection des menaces non virales est configurée avec la réécriture d'URL définie pour réécrire toutes les URL contenues dans les e-mails malveillants (comme dans les scénarios précédents)
- Filtre de contenu entrant : Filtre de contenu URL_SCORE activé

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); }		

Le filtre de contenu utilise la condition de réputation d'URL pour faire correspondre les URL malveillantes, celles dont le score est compris entre -6.00 et -10.00. En tant qu'action, le nom du

filtre de contenu est consigné et l'action de défense **url-reputation-defang** est prise.

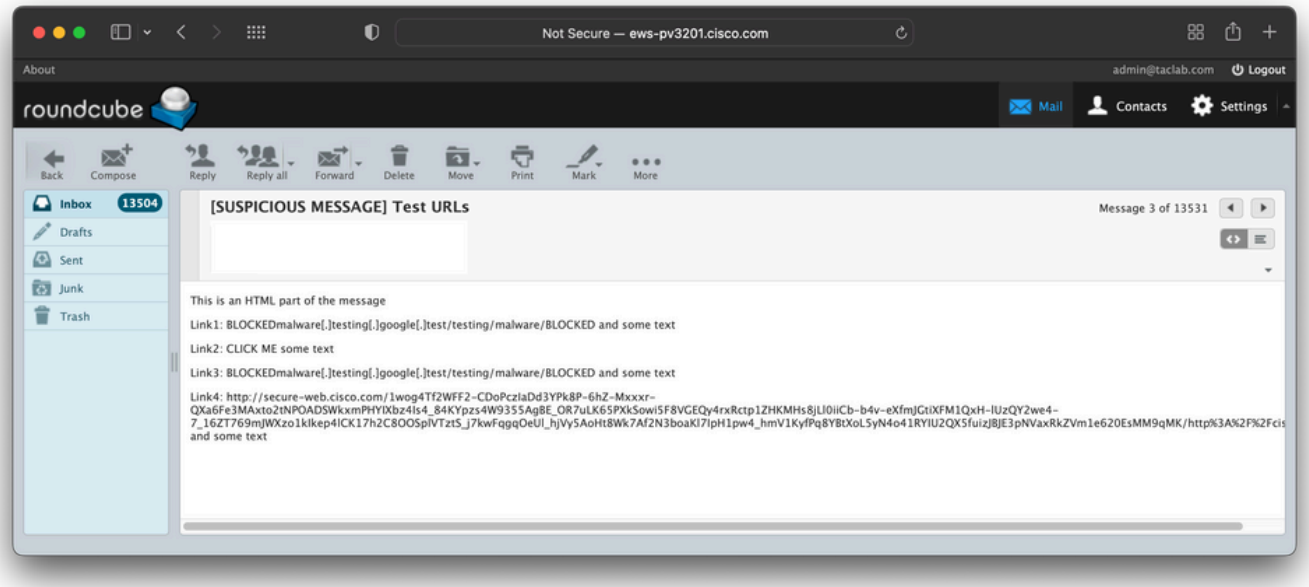
La même copie du message est envoyée et évaluée par la passerelle de messagerie avec les résultats suivants :

```
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
```

Le pipeline d'e-mail explique que le message est d'abord évalué par les filtres de contenu, où le filtre URL_SCORE est déclenché et URL-reputation-defang-action est appliqué. Cette action désactive toutes les URL malveillantes dans les parties MIME text/plain et text/html. Étant donné que websecurityadvanceconfig href et la réécriture de texte sont activés, toutes les chaînes d'URL qui correspondent à l'intérieur du corps HTML sont désactivées lorsque tous les éléments de balise A sont supprimés et réécrivent des parties de texte de l'URL entre des mots BLOQUÉS et placent tous les points entre crochets. La même chose se produit avec d'autres URL malveillantes qui ne sont pas placées dans des éléments HTML de balise A. Le filtre anti-épidémies traite ensuite le message. Le OF détecte les URL malveillantes et identifie le message comme malveillant (niveau de menace = 5). Par conséquent, il réécrit toutes les URL malveillantes et non malveillantes trouvées dans le message. Étant donné que l'action de filtrage du contenu a déjà modifié ces URL, le OF réécrit uniquement le reste des URL non malveillantes telles qu'elles ont été configurées intentionnellement pour le faire. Message affiché dans le client de messagerie en tant que partie des URL malveillantes définies et partie de l'URL non malveillante redirigée.

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



Il en va de même pour la partie texte/simple du message MIME. Toutes les URL non malveillantes sont redirigées vers le proxy Cisco Web Secure et les URL malveillantes sont désactivées.

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

Résumé :

- CF defang exécuté sur la partie TEXT/PLAIN réécrit l'URL en blocs BLOQUÉS
- CF defang exécuté sur la partie TEXT/HTML réécrit l'URL à partir d'une balise A HTML lorsqu'une balise A est supprimée
- CF defang exécuté sur la partie TEXT/HTML réécrit toutes les chaînes d'URL qui correspondent en blocs BLOQUÉS
- OF redirect exécuté sur la partie TEXT/PLAIN réécrit toutes les chaînes d'URL qui correspondent au service proxy Cisco Web Secure (non malveillant)
- OF redirect exécuté sur la partie TEXT/HTML réécrit l'URL à partir d'un attribut href de balise A HTML avec la partie texte de l'élément et toutes les autres chaînes d'URL qui correspondent au service proxy Cisco Web Secure (non malveillant)

Dépannage

Suivez ces points lorsqu'il est nécessaire d'étudier le problème de réécriture d'URL.

- Activez la journalisation des URL dans vos journaux de messagerie. Exécutez la commande **OUTBREAKCONFIG** commandement et réponse **Y** par **Do you wish to enable logging of URL's?** [N]>"
- Vérification **WEBSECURITYADVANCECONFIG** paramètres sous chaque membre du cluster de la passerelle de messagerie et assurez-vous que l'option href et text rewrite est définie en

conséquence et identique sur chaque ordinateur. Gardez à l'esprit que cette commande est spécifique à l'ordinateur et que les modifications apportées ici n'affectent pas les paramètres de groupe ou de cluster.
- Vérifiez les conditions et les activités de votre filtre de contenu, et assurez-vous que le filtre de contenu est activé et appliqué à la stratégie de courrier entrant appropriée. Vérifiez s'il n'y a aucun autre filtre de contenu traité avant avec une action finale qui peut sauter pour traiter d'autres filtres.
- Examinez la copie brute du message source et du message final. Gardez à l'esprit pour récupérer le message au format EML, les formats propriétaires comme MSG ne sont pas fiables quand il s'agit de l'investigation de message. Certains clients de messagerie vous permettent d'afficher le message source et d'essayer de récupérer la copie du message avec un autre client de messagerie. Par exemple, MS Outlook pour Mac vous permet d'afficher la source du message tandis que la version Windows vous permet uniquement d'afficher les en-têtes.

Résumé

L'objectif de cet article est d'aider à mieux comprendre les options de configuration disponibles en matière de réécriture d'URL. Il est important de se rappeler que les messages modernes sont créés par la plupart des logiciels de messagerie avec la norme MIME. Cela signifie que la même copie du message peut être affichée différemment, ce qui dépend des capacités du client de messagerie et/ou des modes activés (mode texte ou HTML). Par défaut, la plupart des clients de messagerie modernes utilisent le langage HTML pour afficher les messages. En ce qui concerne la réécriture HTML et URL, gardez à l'esprit que la passerelle de messagerie par défaut réécrit uniquement les URL se trouvant dans l'attribut href de l'élément A-tag. Dans de nombreux cas, cela n'est pas suffisant et il doit être envisagé d'activer à la fois href et text rewrite avec la commande WEBSECURITYADVANCECONFIG. N'oubliez pas qu'il s'agit d'une commande au niveau de l'ordinateur et que, pour des raisons de cohérence dans le cluster, la modification doit être appliquée séparément à chacun des membres du cluster.