Verständnis der Aktionen zum Entwerfen und Umleiten von URLs auf dem sicheren E-Mail-Gateway

Inhalt

Einleitung

In diesem Dokument wird der Unterschied zwischen den im URL-Filter verwendeten Vorgabe- und Umleitungsaktionen sowie die Verwendung der verfügbaren Umschreibungsoption für das href-Attribut und den Text beschrieben.

Voraussetzungen

Anforderungen

Um Maßnahmen basierend auf der URL-Reputation zu ergreifen oder Richtlinien zur akzeptablen Nutzung mit Nachrichten- und Inhaltsfiltern durchzusetzen, muss die Outbreak-Filterfunktion global aktiviert werden.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Secure Email Gateway
- Outbreak-Filter
- Content- und Nachrichtenfilter

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Eine der Funktionen für die URL-Filterung besteht darin, anhand der URL-Reputation oder -kategorie mithilfe von Nachrichten- und/oder Content-Filtern Maßnahmen zu ergreifen. Basierend auf dem URL-Scan-Ergebnis (URL-Related Condition) kann eine der drei verfügbaren Aktionen auf eine URL angewendet werden:

- Defang-URL
- Umleitung zu Cisco Security Proxy
- URL durch Textnachricht ersetzen

Im Mittelpunkt dieses Dokuments steht die Erklärung des Verhaltens zwischen den Optionen "Entfang" und "URL umleiten". Es enthält außerdem eine kurze Beschreibung und Erläuterung der URL-Umschreibungsfunktionen für die Erkennung nicht-viraler Bedrohungen durch einen Outbreak-Filter.

Beispiel für eine Nachricht

Die in allen Tests verwendete Beispielnachricht ist der mehrteilige/alternative Nachrichtentyp MIME und umfasst sowohl Text-/Klartext- als auch Text-/HTML-Teile. Diese Teile werden in der Regel automatisch von E-Mail-Software generiert und enthalten die gleiche Art von Inhalten, die für HTML- und Nicht-HTML-Empfänger formatiert sind. Dazu wurde der Inhalt von text/plain und text/html manuell bearbeitet.

```
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
```

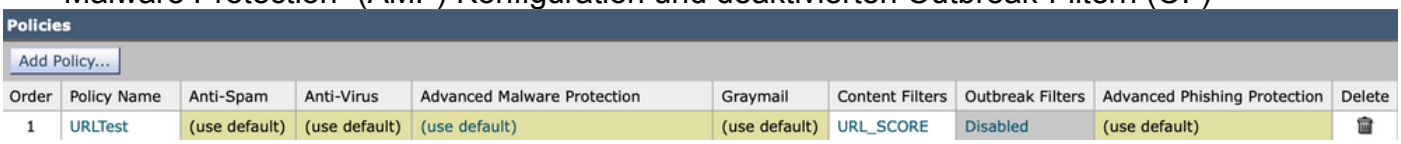
```
Link4: http://cisco.com and some text

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

Teil I - Defang

Konfigurationen

Im ersten Teil wird Folgendes verwendet:

- Mail-Richtlinie mit standardmäßig deaktivierter Anti-Spam- (AS)/Anti-Virus- (AV)/Advanced Malware Protection- (AMP) Konfiguration und deaktivierten Outbreak-Filtern (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)	

- Filter für eingehende Inhalte: URL_SCORE-Inhaltsfilter aktiviert

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); }		

Der Content-Filter verwendet die URL-Reputationsbedingung, um schädliche URLs abzugleichen, d. h. die URLs, die zwischen -6,00 und -10,00 bewertet werden. Als Aktion wird der Content-Filter-Name protokolliert und die Standardaktion festgelegt. **url-reputation-defang** genommen.

Defang-Aktion

Es ist wichtig zu klären, was eine Defang-Aktion ist. Das Benutzerhandbuch bietet eine Erklärung; Entzieh eine URL, sodass sie nicht mehr anklickbar ist. Nachrichtenempfänger können die URL weiterhin sehen und kopieren.

Szenario A

Outbreak-Filter: Erkennung nicht-viraler Bedrohungen	Nein
Content-Filter-Aktion	Defang
websecurityadvancedconfig href und text rewrite ist aktiviert	Nein

In diesem Szenario wird das Ergebnis der mit den Standardeinstellungen konfigurierten Standardaktion erläutert. In der Standardeinstellung wird die URL neu geschrieben, wenn nur die HTML-Tags entfernt werden. Werfen Sie einen Blick auf einen HTML-Absatz mit einigen URLs:

```
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
```

In den ersten beiden Absätzen wird die URL durch ein passendes HTML-A-Tag dargestellt. Das <A>-Element umfasst die **href=** -Attribut, das in das Tag selbst eingeschlossen ist und das Linkziel

angibt. Der Inhalt in den Tag-Elementen kann auch das Linkziel angeben. Diese **text form** des Links kann die URL enthalten. Der erste Link1 enthält den gleichen URL-Link sowohl im href-Attribut als auch im Textteil des Elements. Beachten Sie, dass diese URLs unterschiedlich sein können. Der zweite Link2 enthält den entsprechenden URL nur innerhalb des href-Attributs. Der letzte Absatz enthält keine A-Elemente.

> **Anmerkung:** Die richtige Adresse wird immer angezeigt, wenn Sie den Cursor über den Link bewegen oder den Quellcode der Nachricht anzeigen. Leider ist der Quellcode bei einigen gängigen E-Mail-Clients nicht leicht zu finden.

Sobald die Nachricht vom URL_SCORE-Filter zugeordnet wurde, werden die schädlichen URLs definiert. Wenn die URL-Protokollierung mit dem **OUTBREAKCONFIG** -Befehl die Bewertungen und URLs in mail_logs.

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

Daraus ergibt sich die neu geschriebene Nachricht:

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

Das Ergebnis der Standardaktion für den text/html-Teil der MIME-Nachricht ist ein gestripptes A-Tag, und der Tag-Inhalt bleibt unberührt. In den beiden ersten Absätzen wurden beide Links definiert, wobei der HTML-Code entfernt und der Textteil des Elements belassen wurde. Die URL-Adresse im ersten Absatz ist diejenige aus dem Textteil des HTML-Elements. Es ist zu beachten, dass die URL-Adresse aus dem ersten Absatz nach der Vorgabe noch sichtbar ist, aber ohne die HTML-A-Tags darf das Element nicht anklickbar sein. Der dritte Absatz wird nicht definiert, da die URL-Adresse hier nicht zwischen A-Tags eingefügt wird und nicht als Link angesehen wird. Vielleicht ist es nicht wünschenswert Verhalten aus zwei Gründen. Zum einen kann der Benutzer den Link einfach sehen und kopieren und im Browser ausführen. Der zweite Grund ist, dass einige E-Mail-Software dazu neigt, eine gültige Form von URL innerhalb des Textes zu erkennen und es zu einem anklickbaren Link zu machen.

Werfen wir einen Blick auf den Text der MIME-Nachricht. Der Text-/Klartext-Teil enthält zwei URLs in der Textform. Der Text/Plain wird von MUA angezeigt, das den HTML-Code nicht versteht. In

den meisten modernen E-Mail-Clients wird der Text bzw. die einfachen Teile der Nachricht nicht angezeigt, es sei denn, Sie haben Ihren E-Mail-Client absichtlich so konfiguriert. Normalerweise müssen Sie den Quellcode der Nachricht überprüfen, ein unformatiertes EML-Format der Nachricht, um die MIME-Teile zu sehen und zu untersuchen.

Die Liste hier zeigt URLs aus dem Text-/Plain-Teil der Quellnachricht.

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

Einer dieser beiden Links erhielt eine bösartige Bewertung und wurde defangt. Standardmäßig hat die Standardaktion für den Text/Plain-Teil des MIME-Typs ein anderes Ergebnis als für den Text/HTML-Teil. Es liegt zwischen BLOCKIERTEN Wörtern und allen Punkten zwischen eckigen Klammern.

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

Zusammenfassung:

- Defang run auf dem TEXT/PLAIN Teil schreibt die URL in BLOCKED Blöcke um
- Der Defang-Run auf dem TEXT/HTML-Teil schreibt die URL von einem HTML-A-Tag um, wenn das A-Tag entfernt wird, ohne dass der Text zwischen den A-Tags berührt wird, das kann auch eine URL-Adresse sein

Szenario B

Outbreak-Filter: Erkennung nicht-viraler Bedrohungen	Nein
Content-Filter-Aktion	Defang
websecurityadvancedconfig href und text rewrite ist aktiviert	Ja

Dieses Szenario liefert Informationen darüber, wie sich das Verhalten der defangs-Aktion nach der Verwendung einer der websecurityadvancedconfig-Optionen ändert. Der Befehl websecurityadvancedconfig ist der spezifische CLI-Befehl auf Computerebene, mit dem spezifische Einstellungen für die URL-Suche angepasst werden können. Mit einer der Einstellungen hier können Sie das Standardverhalten der Standardaktion ändern.

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

In der vierten Frage **Do you want to rewrite both the URL text and the href in the message? ..**, die Antwort **Y** gibt an, dass im Fall des HTML-basierten MIME-Teils der Nachricht alle URL-Zeichenfolgen übereinstimmen, unabhängig davon, ob sie im href-Attribut des A-tag-Elements gefunden werden, es sich um einen Textteil oder um eine Ausnahme von Elementen handelt, die neu geschrieben werden. In diesem Szenario wird dieselbe Botschaft erneut übermittelt, allerdings mit einem etwas

anderen Ergebnis.

Werfen Sie noch einmal einen Blick auf den text/html MIME Code mit den URLs und vergleichen Sie ihn mit dem HTML Code, der vom E-Mail Gateway verarbeitet wird.

```
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
```

Wenn die Option zum Umschreiben von href und text aktiviert ist, werden alle von den Filter-URLs übereinstimmenden URLs definiert, unabhängig davon, ob die URL-Adresse Teil des href-Attributs oder des Textteils des A-tag-HTML-Elements oder in einem anderen Teil des HTML-Dokuments ist.

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

Die vordefinierten URLs werden jetzt neu geschrieben, wenn das A-Tag-Element mit einem Umschreiben des Textteils des Links entfernt wird, wenn es mit dem URL-Format übereinstimmt. Der neu geschriebene Textteil erfolgt auf die gleiche Weise wie im Text/Plain-Teil der MIME-Nachricht. Das Element wird zwischen BLOCKIERTEN Wörtern und alle Punkte zwischen eckigen Klammern platziert. Dadurch wird verhindert, dass der Benutzer die URL kopieren und einfügen kann, und einige E-Mail-Software-Clients machen den Text klickbar.

Zusammenfassung:

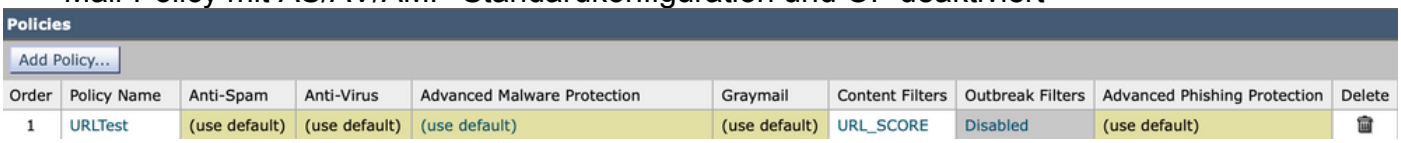
- Defang run auf dem TEXT/PLAIN Teil schreibt die URL in BLOCKED Blöcke um
- Der Defang-Run auf dem TEXT/HTML-Teil schreibt die URL von einem HTML-A-Tag um, wenn ein A-Tag entfernt wird
- Der Defang-Run auf den TEXT/HTML-Teil schreibt alle URL-Strings, die in BLOCKED-Blöcke passen, neu

Teil II: Weiterleitung

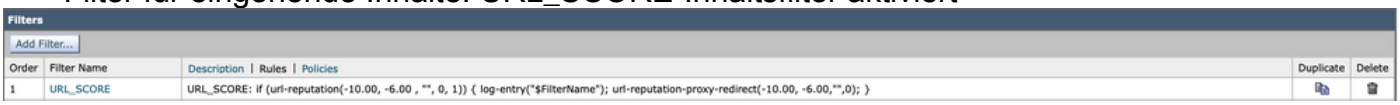
Konfigurationen

Im zweiten Teil wird Folgendes verwendet:

- Mail-Policy mit AS/AV/AMP-Standardkonfiguration und OF deaktiviert



- Filter für eingehende Inhalte: URL_SCORE-Inhaltsfilter aktiviert



Der Content-Filter verwendet die URL-Reputationsbedingung, um schädliche URLs abzugleichen, d. h. die URLs, deren Punktzahl zwischen -6,00 und -10,00 liegt. Als Aktion wird der Content-Filter-Name protokolliert und die **redirect action** genommen.

Aktion umleiten

Umleitung zum Cisco Security Proxy-Service zur Überprüfung per Mausklick: Der Empfänger kann auf den Link klicken und an einen Cisco Web Security Proxy in der Cloud umgeleitet werden, der den Zugriff blockiert, wenn die Website als schädlich identifiziert wird.

Szenario C

Outbreak-Filter: Erkennung nicht-viraler Bedrohungen	Nein
Content-Filter-Aktion	Umleiten
websecurityadvancedconfig href und text rewrite ist aktiviert	Nein

Dieses Szenario ähnelt Szenario A aus dem ersten Teil mit dem Unterschied in der Inhaltsfilteraktion, die URL umzuleiten, anstatt sie zu definieren. Die websecurityadvancedconfig-Einstellungen werden auf die Standardeinstellungen zurückgesetzt, d. h. die **"Do you want to rewrite both the URL text and the href in the message? ..** ist auf **N**.

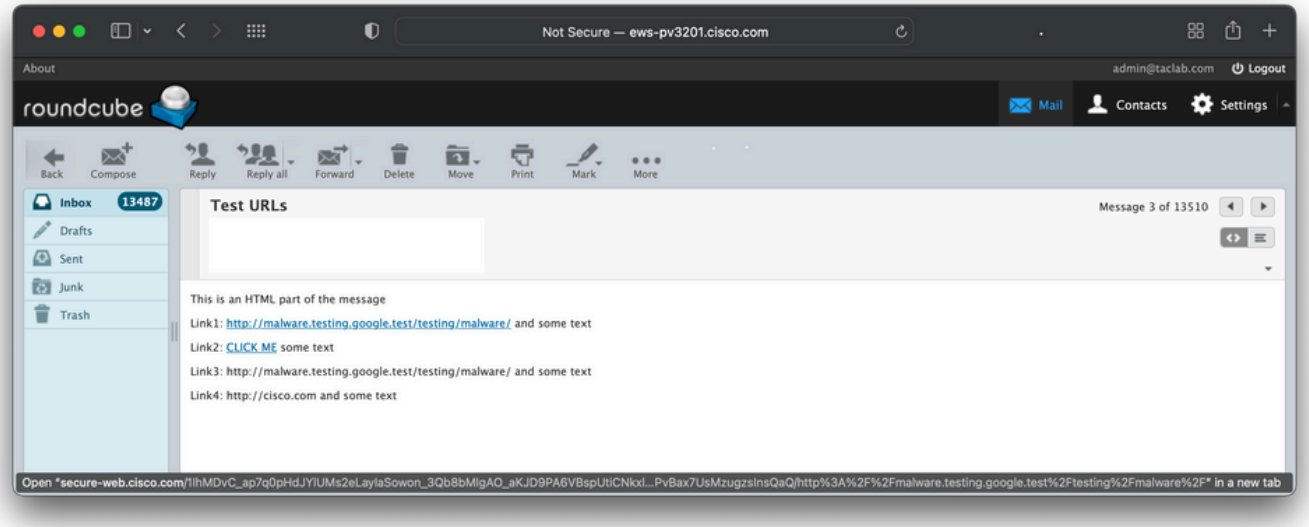
Das E-Mail-Gateway erkennt und wertet jede URL aus. Die schädliche Bewertung löst die URL_SCORE-Inhaltsfilterregel aus und ergreift die erforderlichen Maßnahmen. **url-reputation-proxy-redirect-action**

```
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'
```

Werfen Sie einen Blick darauf, wie die URLs im HTML-Teil der Nachricht umgeschrieben werden. Wie in Szenario A werden nur die URLs im href-Attribut eines A-Tag-Elements neu geschrieben, und die URL-Adressen im Textteil des A-Tag-Elements werden übersprungen. Bei einer Standardaktion wird ein ganzes A-Tag-Element entfernt, bei einer Umleitungsaktion wird jedoch der URL im href-Attribut neu geschrieben.

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

Der E-Mail-Client zeigt daraufhin zwei aktive Links an: Link1 und Link2 verweisen beide auf den Cisco Web Security Proxy-Dienst, die im E-Mail-Client angezeigte Nachricht zeigt jedoch den Text des A-Tags an, der nicht standardmäßig neu geschrieben wird. Um das besser zu machen, schauen Sie sich bitte die Ausgabe des Webmail-Clients an, der den Text/HTML-Teil der Nachricht anzeigt.



Im Text-/Plain-Teil des MIME-Teils erscheint die Umleitung verständlicher, da jede URL-Zeichenfolge, die mit der Punktzahl übereinstimmt, neu geschrieben wird.

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

Zusammenfassung:

- Beim Ausführen der Umleitung für den TEXT/PLAIN-Teil wird die URL-Zeichenfolge, die mit dem Cisco Web Secure-Proxydienst übereinstimmt, neu geschrieben.
- Bei der Ausführung der Umleitung für den TEXT/HTML-Teil wird die URL aus einem HTML A-Tag href-Attribut mit dem Cisco Web Secure-Proxydienst umgeschrieben, alle anderen URL-Zeichenfolgen, die nicht geändert wurden, bleiben jedoch unverändert.

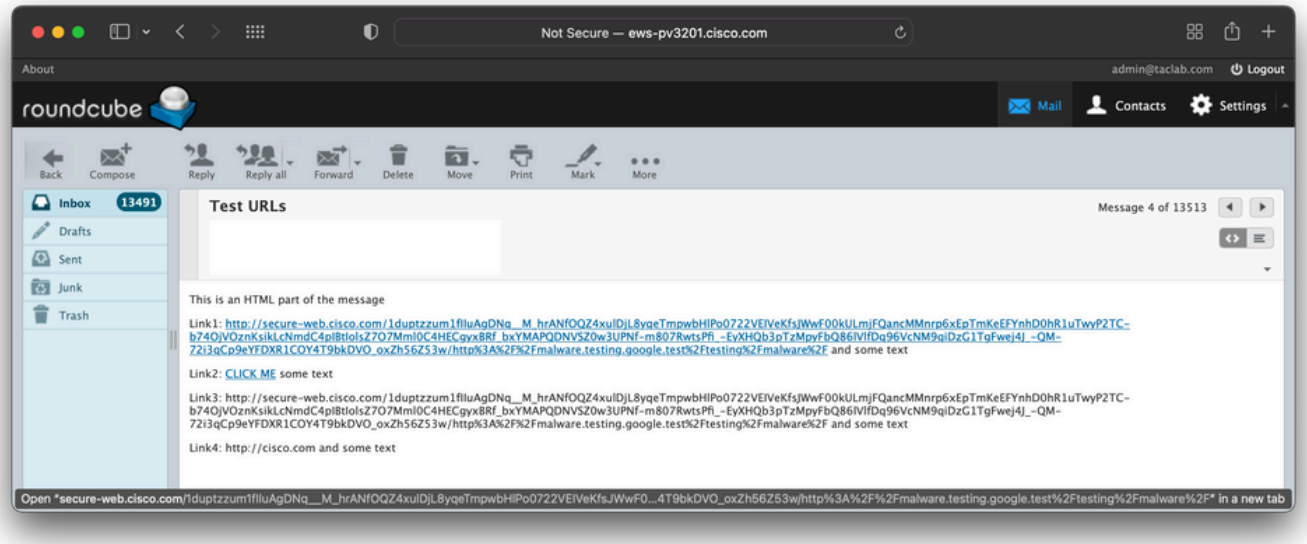
Szenario D

Outbreak-Filter: Erkennung nicht-viraler Bedrohungen	Nein
Content-Filter-Aktion	Umleiten
websecurityadvancedconfig href und text rewrite ist aktiviert	Ja

Dieses Szenario ähnelt Szenario B aus Teil 1. Um alle URL-Zeichenfolgen umzuschreiben, die im HTML-Teil der Nachricht übereinstimmen, ist aktiviert. Dies erfolgt mit dem Befehl websecurityadvancedconfig von, wenn Sie Y für die **"Do you want to rewrite both the URL text and the href in the message? ..** Frage.

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

Nach dem Aktivieren von href und text rewrite werden alle URL-Zeichenfolgen, die den Inhaltsfilterbedingungen entsprechen, umgeleitet. Die Nachricht im E-Mail-Client wird jetzt mit der gesamten Umleitung angezeigt. Um dies besser zu verstehen, schauen Sie sich die Ausgabe des Webmail-Clients an, der den Text/HTML-Teil der Nachricht anzeigt.



Der Text-/Klartext-Teil der MIME-Nachricht ist der gleiche wie in Szenario C, da die websecurityadvancedconfig-Änderung keine Auswirkung auf den Text-/Klartext-Teil der Nachricht hat.

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

Zusammenfassung:

- Beim Ausführen der Umleitung für den TEXT/PLAIN-Teil werden die URL-Zeichenfolgen, die mit dem Cisco Web Secure-Proxydienst übereinstimmen, neu geschrieben.
- Bei der Ausführung der Umleitung für den TEXT-/HTML-Teil wird die URL aus einem HTML-A-Tag href-Attribut zusammen mit dem Textteil sowie jeder anderen URL-Zeichenfolge, die mit dem Cisco Web Secure-Proxydienst im HTML-Text übereinstimmt, umgeschrieben.

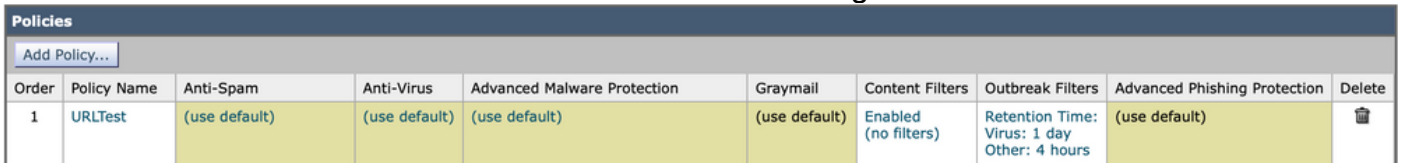
Teil 3 - VON-Umleitung

Dieser Abschnitt enthält Informationen darüber, wie sich OF-Einstellungen für die Erkennung nicht-viraler Bedrohungen auf URL-Scans auswirken.

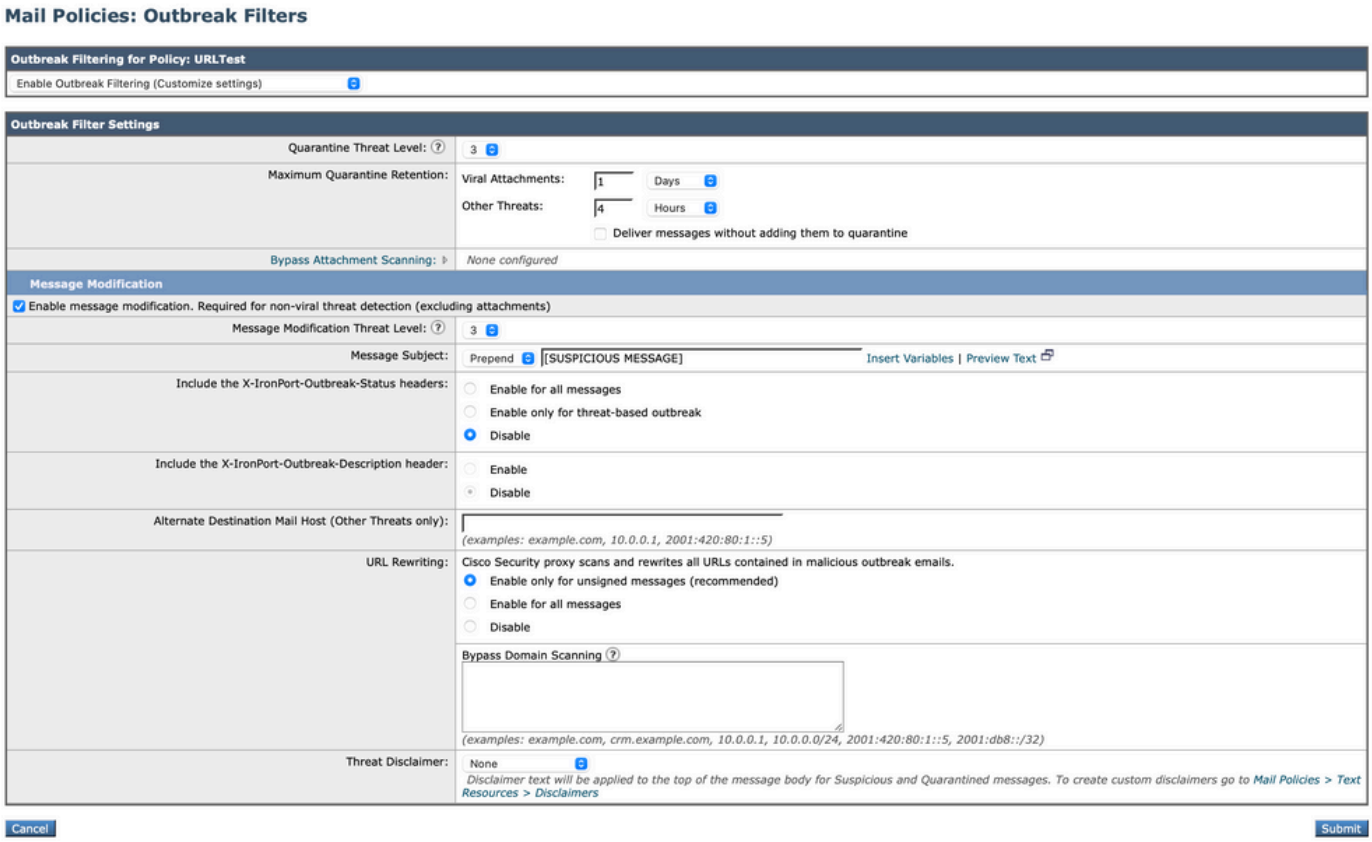
Konfiguration

Dazu wird der in den ersten beiden Teilen verwendete Content-Filter deaktiviert.

- Mail-Richtlinie mit aktivierter AS/AV/AMP-Standardkonfiguration und OF



- Der Outbreak-Filterscan für die Erkennung nicht-viraler Bedrohungen ist mit einem URL-Umschreibungssatz konfiguriert, der alle URLs in bösartigen E-Mails umschreibt



Wenn die Nachricht von OF als "Malicious" (Bösartig) klassifiziert wird, werden alle URLs innerhalb der Nachricht mit dem Cisco Web Secure-Proxydienst neu geschrieben.

Szenario E

Outbreak-Filter: Erkennung nicht-viraler Bedrohungen	Ja
Content-Filter-Aktion	Nein
websecurityadvancedconfig href und text rewrite ist aktiviert	Nein

Dieses Szenario zeigt, wie das Umschreiben von Nachrichten nur mit aktiviertem OF und aktiviertem WebSecurityAdvancedConfig href funktioniert und das Umschreiben von Text deaktiviert ist.

```
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)
```

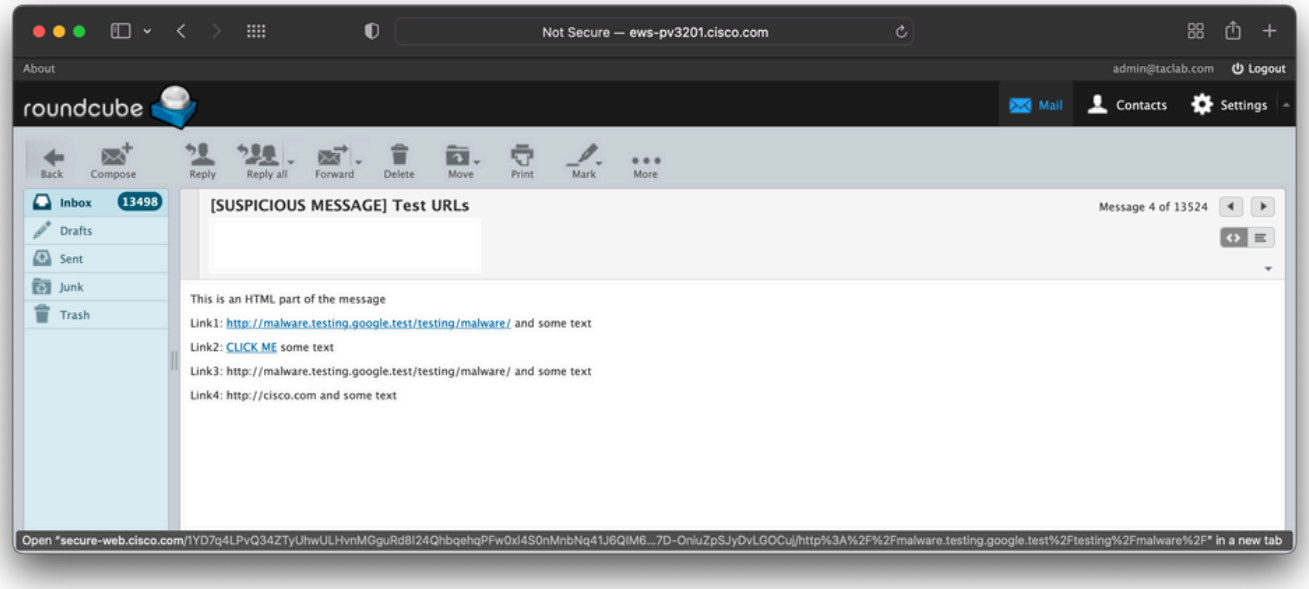
Beginnen wir mit dem Text/Plain MIME Teil. Nach einer kurzen Überprüfung kann festgestellt werden, dass alle URLs im Text-/Plain-Teil in die Cisco Web Secure-Proxydienste neu geschrieben wurden. Der Grund hierfür ist, dass das Umschreiben von URLs für alle URLs in der

Outbreak-Nachricht aktiviert ist.

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

Dies ist der verarbeitete Text/HTML-Teil der MIME-Nachricht.

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



Das erste, das hier bemerkt werden kann, ist, warum Link4 nicht umgeschrieben wird. Wenn Sie den Artikel aufmerksam lesen, kennen Sie die Antwort bereits. Der text/html-Teil von MIME wertet standardmäßig nur die href-Attribute der A-Tag-Elemente aus und bearbeitet diese. Wenn ein ähnliches Verhalten wie bei Text/Plain Part gewünscht wird, müssen websecurancedconfig href und text rewrite aktiviert werden. Das nächste Szenario macht genau das.Zusammenfassung:

- OF redirect run on the TEXT/PLAIN part rewrites all the URL string that match with the Cisco Web Secure proxy service

- OF-Umleitung, die für den TEXT/HTML-Teil ausgeführt wird, schreibt nur die URL eines HTML A-Tag href-Attributs mit dem Cisco Web Secure-Proxydienst um.

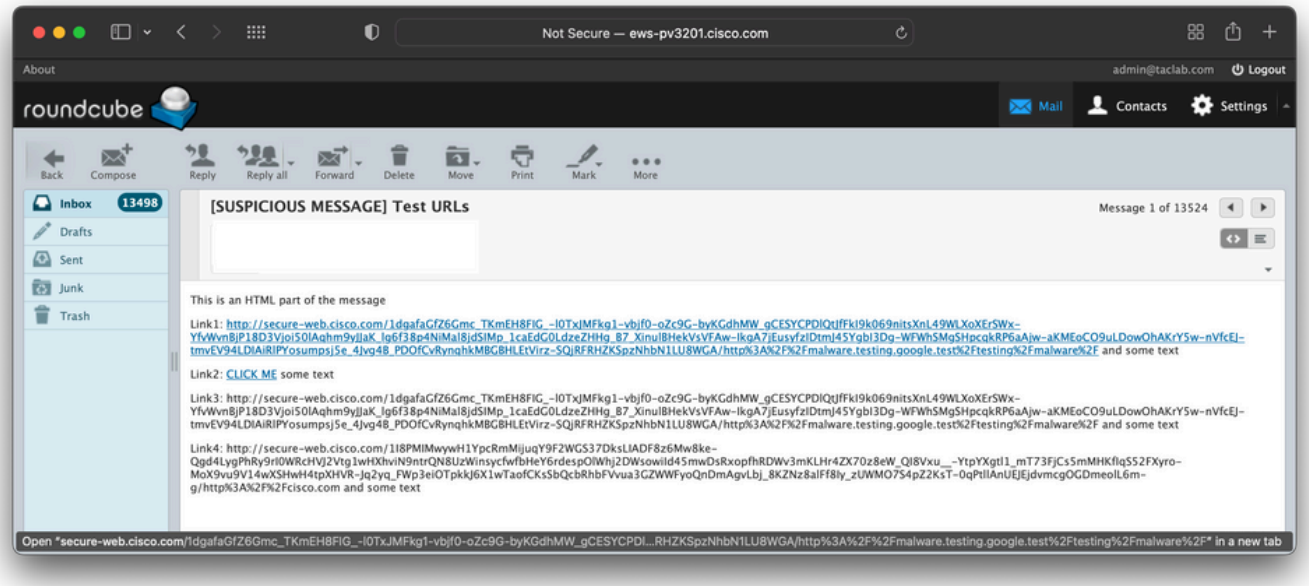
Szenario F

Outbreak-Filter: Erkennung nicht-viraler Bedrohungen	Ja
Content-Filter-Aktion	Nein
websecurityadvancedconfig href und text rewrite ist aktiviert	Ja

Dieses Szenario ermöglicht websecurityadvancedconfig href und text rewrite, um zu zeigen, wie sich das Verhalten in URL-Umschreibungen ändert, die von OF (nicht virale Bedrohungserkennung) bereitgestellt werden. In diesem Moment muss man sich bewusst sein, dass die websecurityadvancedconfig keine Text/Plain-MIME-Teile beeinflusst. Lassen Sie uns nur den text/html Teil bewerten und sehen, wie sich das Verhalten geändert hat.

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

Es ist zu bemerken, dass die Ausgabe sehr ähnlich ist wie die von Szenario D mit dem einzigen Unterschied, dass alle URLs neu geschrieben wurden, nicht nur die bösartigen. Alle URL-Strings, die im HTML-Teil mit den nicht-bösartigen übereinstimmen, werden hier geändert.



Zusammenfassung:

- OF redirect run on the TEXT/PLAIN part rewrites all the URL strings that match with the Cisco Web Secure proxy service
- OF-Umleitungsausführung für den TEXT/HTML-Teil schreibt die URL aus einem HTML A-Tag href-Attribut zusammen mit dem Textteil des Elements und allen anderen URL-Zeichenfolgen, die mit dem Cisco Web Secure-Proxydienst übereinstimmen, um

Szenario G

Outbreak-Filter: Erkennung nicht-viraler Bedrohungen	Ja
Content-Filter-Aktion	Defang
websecurityadvancedconfig href und text rewrite ist aktiviert	Ja

In diesem letzten Szenario wird die Konfiguration validiert.

- Mail-Richtlinie mit aktivierter AS/AV/AMP-Standardkonfiguration und 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)	

- Der OF-Scan für die Erkennung nicht-viraler Bedrohungen ist so konfiguriert, dass URL Rewrite (URL-Umschreibung) so eingestellt ist, dass alle in bösartigen E-Mails enthaltenen URLs umgeschrieben werden (wie in früheren Szenarien).
- Filter für eingehende Inhalte: URL_SCORE-Inhaltsfilter aktiviert

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); }		

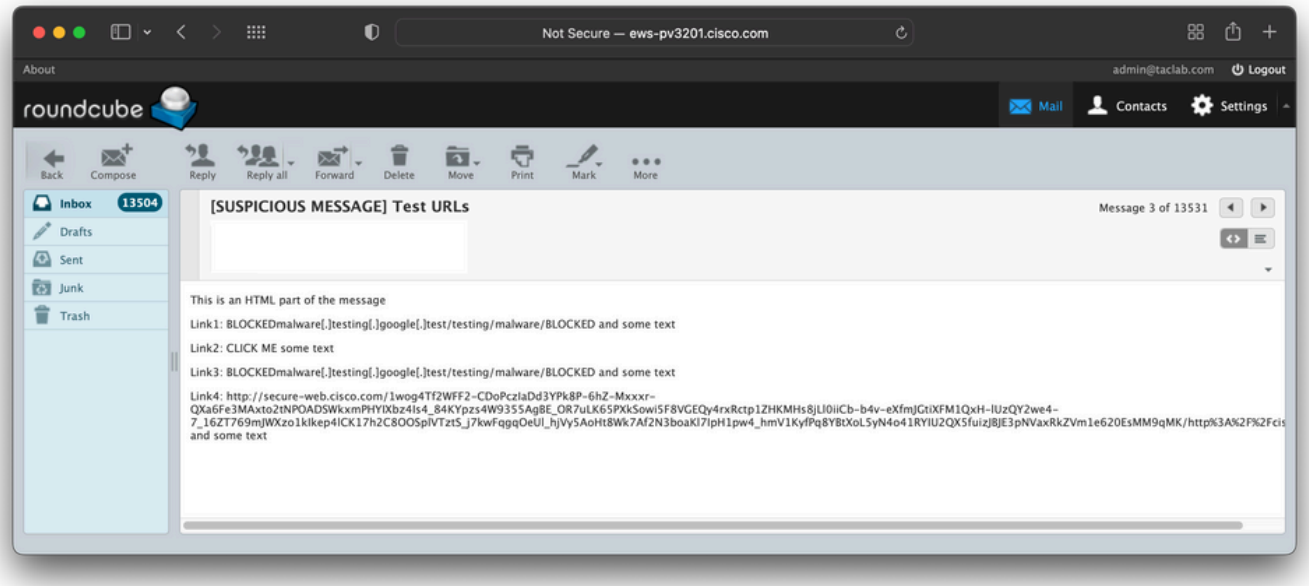
Der Content-Filter verwendet die URL-Reputationsbedingung, um schädliche URLs abzugleichen, d. h. die URLs, die zwischen -6,00 und -10,00 bewertet werden. Als Aktion wird der Content-Filter-Name protokolliert und die Standardaktion festgelegt. **url-reputation-defang** genommen.

Dieselbe Kopie der Nachricht wird vom E-Mail-Gateway versendet und ausgewertet. Das Ergebnis:

```
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
```

In der E-Mail-Pipeline wird erklärt, dass die Nachricht zuerst von den Content-Filtern ausgewertet wird, wo der URL_SCORE-Filter ausgelöst und die URL-Reputations-Definierungsaktion angewendet wird. Mit dieser Aktion werden alle schädlichen URLs in text/plain- und text/html-MIME-Komponenten definiert. Da websecurityadvanceconfig href und text rewrite aktiviert ist, werden alle URL-Zeichenfolgen, die innerhalb des HTML-Textkörpers übereinstimmen, definiert, wenn alle A-Tag-Elemente entfernt werden und Textteile der URL zwischen BLOCKIERTEN Wörtern neu geschrieben und alle Punkte zwischen eckigen Klammern gesetzt werden. Dasselbe geschieht mit anderen schädlichen URLs, die nicht in A-Tag-HTML-Elementen platziert werden. Der Outbreak-Filter verarbeitet die Nachricht anschließend. Der OF erkennt schädliche URLs und identifiziert die Nachricht als schädlich (Bedrohungsstufe=5). Daher werden alle in der Nachricht gefundenen schädlichen und nicht schädlichen URLs neu geschrieben. Da die Inhaltsfilteraktion diese URLs bereits geändert hat, schreibt OF nur den Rest der nicht schädlichen URLs neu, da es absichtlich dafür konfiguriert wurde. Die Nachricht, die im E-Mail-Client als Teil der definierten schädlichen URLs und als Teil der umgeleiteten nicht schädlichen URL angezeigt wird.

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



Dasselbe gilt für den Text-/Plain-Teil der MIME-Nachricht. Alle nicht schädlichen URLs werden an den Cisco Web Secure-Proxy umgeleitet, und die schädlichen URLs werden definiert.

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

Zusammenfassung:

- CF-Standardausführung für den TEXT/PLAIN-Teil schreibt die URL in BLOCKED-Blöcke um
- CF-Standardausführung für den TEXT/HTML-Teil schreibt die URL von einem HTML-A-Tag um, wenn ein A-Tag entfernt wird
- CF-Standardausführung für den TEXT/HTML-Teil schreibt alle URL-Zeichenfolgen, die in BLOCKED-Blöcke passen, neu
- OF redirect run on the TEXT/PLAIN part rewrites all the URL strings that match with the Cisco Web Secure proxy service (non-malicious)
- OF redirect run on the TEXT/HTML part rewrites the URL from an HTML A-tag href attribute together with the text part of the element and all other URL strings that match with the Cisco Web Secure proxy service (non-malicious)

Fehlerbehebung

Befolgen Sie diese Punkte, wenn das Problem mit dem URL-Umschreiben untersucht werden muss.

- Aktivieren Sie die URL-Protokollierung in Ihren mail_logs. Ausgeführt **OUTBREAKCONFIG** Befehl und Antwort **Y** zu **Do you wish to enable logging of URL's?** [N]>"
- Überprüfung **WEBSECURITYADVANCECONFIG** Einstellungen unter jedem E-Mail-Gateway-Cluster-Mitglied. Stellen Sie sicher, dass die Option zum Umschreiben von href- und text-Inhalten auf

jedem Computer entsprechend festgelegt ist. Beachten Sie, dass dieser Befehl maschinenspezifisch ist, und dass sich hier vorgenommene Änderungen nicht auf die Gruppen- oder Clustereinstellungen auswirken.
- Überprüfen Sie die Bedingungen und Aktivitäten Ihres Content-Filters, und stellen Sie sicher, dass der Content-Filter aktiviert ist und auf die richtige Richtlinie für eingehende E-Mails angewendet wird. Überprüfen Sie, ob noch kein anderer Content-Filter verarbeitet wurde. Führen Sie dazu eine abschließende Aktion aus, mit der Sie andere Filter verarbeiten können.
- Untersuchen Sie die Rohkopie der Quell- und Endnachricht. Denken Sie daran, um die Nachricht im EML-Format abzurufen, die proprietären Formate wie MSG sind nicht zuverlässig, wenn es um die Untersuchung von Nachrichten kommt. Einige E-Mail-Clients ermöglichen es Ihnen, die Quellnachricht anzuzeigen und zu versuchen, die Kopie der Nachricht mit einem anderen E-Mail-Client abzurufen. Beispielsweise ermöglicht MS Outlook für Mac die Anzeige der Quelle der Nachricht, während die Windows-Version nur die Anzeige der Header zulässt.

Zusammenfassung

Dieser Artikel soll Ihnen helfen, die verfügbaren Konfigurationsoptionen beim Umschreiben von URLs besser zu verstehen. Es ist wichtig, sich daran zu erinnern, dass moderne Nachrichten von den meisten E-Mail-Software mit dem MIME-Standard erstellt werden. Das bedeutet, dass dieselbe Kopie der Nachricht auf verschiedene Weise angezeigt werden kann, je nach E-Mail-Client-Funktionen oder/und aktiviertem Modus (Text- oder HTML-Modus). Standardmäßig verwenden die meisten modernen E-Mail-Clients HTML, um Nachrichten anzuzeigen. Bei HTML- und URL-Umschreibungen sollten Sie berücksichtigen, dass das E-Mail-Gateway standardmäßig nur URLs umschreibt, die im href-Attribut des A-tag-Elements enthalten sind. In vielen Fällen reicht dies nicht aus, und es muss erwogen werden, sowohl href als auch text rewrite mit dem Befehl WEBSECURITYADVANCECONFIG zu aktivieren. Beachten Sie, dass es sich um einen Befehl auf Computerebene handelt. Aus Gründen der Konsistenz im Cluster muss die Änderung separat auf die einzelnen Cluster-Elemente angewendet werden.