Begrijp de URL Defang en Redirect actie op de beveiligde e-mailgateway

Inhoud

Inleiding

Dit document beschrijft het verschil tussen defang en redirect acties die in het URL-filter worden gebruikt en hoe de beschikbare herschrijfoptie voor het href-kenmerk en de tekst moet worden gebruikt.

Voorwaarden

Vereisten

Om actie te ondernemen op basis van URL-reputatie of om acceptabel gebruiksbeleid met de bericht- en inhoudsfilters af te dwingen, moet de functie Uitbraakfilters wereldwijd worden ingeschakeld.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco beveiligde e-mailgateway
- Uitbraakfilters
- Content- en berichtfilters

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Een van de functies voor URL-filtering is om actie te ondernemen op basis van de URL-reputatie of categorie met het gebruik van bericht- en/of inhoudsfilters. Op basis van het URL-scanresultaat (URL-gerelateerde voorwaarde) kan een van de drie beschikbare acties op een URL worden toegepast:

- Defang URL
- Omleiden naar Cisco security proxy
- URL vervangen met het tekstbericht

De focus van dit document is het uitleggen van het gedrag tussen de opties Defang en Redirect URL. Het biedt ook een korte beschrijving en uitleg van de URL Herschrijfmogelijkheden van niet-virale detectie van bedreigingen van een uitbraakfilter.

Berichtvoorbeeld

Het voorbeeldbericht dat in alle tests wordt gebruikt, is het MIME-berichttype in meerdere delen/alternatieve delen en omvat zowel tekst/vlakte als tekst/html-delen. Deze onderdelen worden gewoonlijk automatisch gegenereerd door e-mailsoftware en bevatten dezelfde soort inhoud die geformatteerd is voor HTML- en niet-HTML-ontvangers. Hiervoor werd de inhoud van tekst/effen en tekst/html handmatig bewerkt.

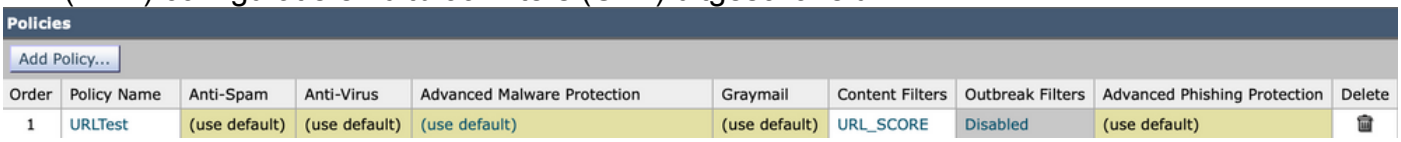
```
Content-Type: multipart/alternative; boundary="===============7781793576330041025==" MIME-
Version: 1.0 From: admin@example.com Date: Mon, 04 Jul 2022 14:38:52 +0200 To: admin@cisco.com
Subject: Test URLs --===============7781793576330041025== Content-Type: text/plain; charset="us-
ascii" MIME-Version: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

Deel I - Defang

Configuraties

In het eerste deel gebruikt de configuratie:

- Mail Policy met standaard anti-spam (AS)/ anti-virus (AV)/ Advanced Malware Protection (AMP) configuratie en uitbraakfilters (OFF) uitgeschakeld



- Inkomende contentfilter: URL_SCORE inhoudsfilter ingeschakeld

De inhoudsfilter gebruikt de URL-reputatievoorwaarde om kwaadaardige URL's aan te passen, de URL's die tussen -6.00 en -10.00 scoren. Als actie wordt de naam van het inhoudfilter vastgelegd en de defang actie **url-reputation-defang** genomen.

Defang Action

Het is belangrijk om duidelijk te maken wat een defang action is. De gebruikershandleiding geeft een toelichting; Defang een URL zodat deze niet kan worden geklikt. Berichtontvangers kunnen de URL nog steeds zien en kopiëren.

Scenario A

Uitbraakfilter voor detectie van niet-virale bedreigingen	Nee
Actie contentfilter	Defang
websecurityadvancedconfig href en tekst herschrijven is ingeschakeld	Nee

Dit scenario verklaart het resultaat van de standaardactie die met standaardinstellingen wordt geconfigureerd. In de standaardinstelling wordt de URL herschreven wanneer alleen de HTML-tags worden gestript. Neem een kijkje bij een HTML-alinea met een aantal URL's erin:

```
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 de eerste twee alinea's wordt de URL weergegeven door een echte HTML A-tag. Het <A>-element bevat de **href=** attribuut dat in de tag zelf is ingesloten en de linkbestemming aangeeft. De inhoud binnen de tagelementen kan ook de koppelingsbestemming aangeven. Dit **text form** van de link kan de URL bevatten. De eerste Link1 bevat dezelfde URL link in zowel href attributen als tekstgedeelte van het element. Je ziet dat die URL's anders kunnen zijn. De tweede Link2 bevat

de juiste URL alleen binnen het href-kenmerk. De laatste alinea bevat geen A-elementen.

> **Opmerking:** Het juiste adres is altijd zichtbaar wanneer u de cursor over de link beweegt of wanneer u de broncode van het bericht bekijkt. Helaas kan de broncode niet gemakkelijk worden gevonden bij een aantal populaire e-mailclients.

Zodra het bericht door het filter URL_SCORE wordt aangepast, worden de kwaadaardige URL's gedefangeerd. Wanneer URL-vastlegging is ingeschakeld met de **OUTBREAKCONFIG** opdracht de scores en URL's kunnen worden gevonden 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'
```

Dit resulteert in het herschreven bericht:

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

Het resultaat van de defang actie die is uitgevoerd op de tekst/html deel van het MIME-bericht is een gestripte A-tag en de tag inhoud wordt onaangeroerd gelaten. In de eerste twee alinea's werden beide links gedefangeerd waar de HTML-code was gestript en het tekstgedeelte van het element was achtergelaten. Het URL-adres in de eerste alinea is dat van het tekstgedeelte van het HTML-element. Het moet worden opgemerkt dat het URL-adres uit de eerste alinea nog zichtbaar is nadat de defang actie is ondernomen maar zonder de HTML A-tags, het element moet niet klikbaar zijn. De derde alinea wordt niet gedefangeerd omdat het URL-adres hier niet tussen A-tags wordt geplaatst en niet als een link wordt beschouwd. Misschien is dat om twee redenen niet wenselijk. Ten eerste kan de gebruiker de link gemakkelijk zien en kopiëren en uitvoeren in de browser. De tweede reden is dat sommige e-mailsoftware een geldige URL in de tekst detecteert en er een link van maakt die je kunt aanklikken.

Laten we eens kijken naar het tekstgedeelte van de MIME-boodschap. Het tekst/vlakke gedeelte bevat twee URL's in het tekstformulier. De tekst/vlakte wordt weergegeven door MUA die de HTML-code niet begrijpt. In de meeste moderne e-mailclients ziet u de tekst/onbewerkte delen van het bericht niet tenzij u uw e-mailclient opzettelijk hebt ingesteld om dit te doen. Normaal gesproken moet u de broncode van het bericht controleren, een onbewerkte EML-indeling van het bericht om de MIME-onderdelen te zien en te onderzoeken.

De lijst hier toont URLs van het tekst/duidelijke deel van het bronbericht.

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

Een van die twee links kreeg een kwaadaardige score en werd gedefaneerd. Door gebrek, heeft de defang actie die op de tekst/vlakke deel van het type MIME wordt gevoerd een verschillend resultaat dan op het tekst/html deel. Het ligt tussen GEBLOKKEERDE woorden en alle punten tussen vierkante haakjes.

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

Samenvatting:

- Defang run op het TEXT/PLAIN onderdeel herschrijft de URL in blokjes
- Defang run op het TEXT/HTML onderdeel herschrijft de URL van een HTML A-tag wanneer de A-tag wordt gestript zonder de tekst tussen A-tags aangeraakt, die ook een URL-adres kan zijn

Scenario B

Uitbraakfilter voor detectie van niet-virale bedreigingen	Nee
Actie contentfilter	Defang
websecurityadvancedconfig href en tekst herschrijven is ingeschakeld	Ja

Dit scenario biedt informatie over hoe het gedrag van de defangs actie verandert na het gebruik van een van de websecurity gevorderde configuratieopties. De websecurity geavanceerde configuratie is de machine-level specifieke CLI opdracht die het mogelijk maakt om instellingen specifiek voor URL scan te stemmen. Een van de instellingen hier staat u toe om het standaardgedrag van de defang actie te veranderen.

```
> 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 de vierde vraag **Do you want to rewrite both the URL text and the href in the message? ..**, het antwoord **Y** geeft aan dat in het geval van het op HTML gebaseerde MIME-deel van het bericht alle URL-strings die overeenkomen met geen kwestie als gevonden in het href-kenmerk van het A-tag-element, het is tekst deel of buiten elementen die worden herschreven. In dit scenario is dezelfde boodschap aanwezig, maar met een iets ander resultaat.

Bekijk de tekst/html MIME-artikelcode met de URL's en vergelijk deze met de HTML-code die door de e-mailgateway wordt verwerkt.

```
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
```

Wanneer de optie href en tekst herschrijven is ingeschakeld, worden alle overeenkomende URL's gedefangeerd, ongeacht of het URL-adres deel uitmaakt van het href-kenmerk of het tekstgedeelte van het A-tag HTML-element, of wordt gevonden in een ander deel van het HTML-document.

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

De defanged URL's worden nu herschreven wanneer het A-tag element wordt gestript samen met een herschrijven van het tekstgedeelte van de link wanneer het overeenkomt met de URL-indeling. Het herschreven tekstgedeelte wordt op dezelfde wijze uitgevoerd als in het tekst/onbewerkte gedeelte van het MIME-bericht. Het item wordt tussen geblokkeerde woorden geplaatst en alle punten tussen vierkante haakjes. Dit verhindert de gebruiker om de URL te kopiëren en te plakken, en sommige e-mail softwareclients maken de tekst klikbaar.

Samenvatting:

- Defang run op het TEXT/PLAIN onderdeel herschrijft de URL in blokjes
- Defang run op het TEXT/HTML onderdeel herschrijft de URL van een HTML A-tag wanneer een A-tag is gestript
- Defang run op het TEXT/HTML onderdeel herschrijft alle URL strings die overeenkomen met BLOKKEERDE blokken

Deel II - Doorverwijzen

Configuraties

In het tweede deel gebruikt de configuratie:

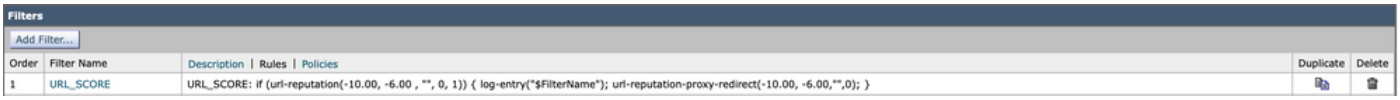
- Mail Policy met standaard AS/AV/AMP configuratie en OFF uitgeschakeld

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)	

- Inkomende contentfilter: URL_SCORE inhoudsfilter ingeschakeld



De inhoudsfilter gebruikt de URL reputatievoorwaarde om kwaadaardige URL's aan te passen, de URL's die tussen -6.00 en -10.00 scoren. Als een actie wordt de naam van de inhoudsfilter vastgelegd en de **redirect action** genomen.

Handeling omleiden

Omleiden naar Cisco Security Proxy-service voor kliktijdevaluatie stelt de ontvanger van het bericht in staat om op de link te klikken en om te leiden naar een Cisco-webbeveiligingsproxy in de cloud, die toegang blokkeert als de site als kwaadaardig wordt geïdentificeerd.

Scenario C

Uitbraakfilter voor detectie van niet-virale bedreigingen	Nee
Actie contentfilter	Doorsturen
websecurityadvancedconfig href en tekst herschrijven is ingeschakeld	Nee

Dit scenario is zeer vergelijkbaar in gedrag met Scenario A van het eerste deel met het verschil gemaakt in de actie van het inhoudfilter om de URL om te leiden in plaats van het te defang. De standaardinstellingen van de websecurity geavanceerde configuratieinstellingen worden hersteld, wat betekent dat de **"Do you want to rewrite both the URL text and the href in the message? ..** is ingesteld op **N**.

De e-mailgateway detecteert en evalueert elk van de URL's. De kwaadaardige score activeert de URL_SCORE content filter regel en voert de actie **url-reputation-proxy-redirect-action**

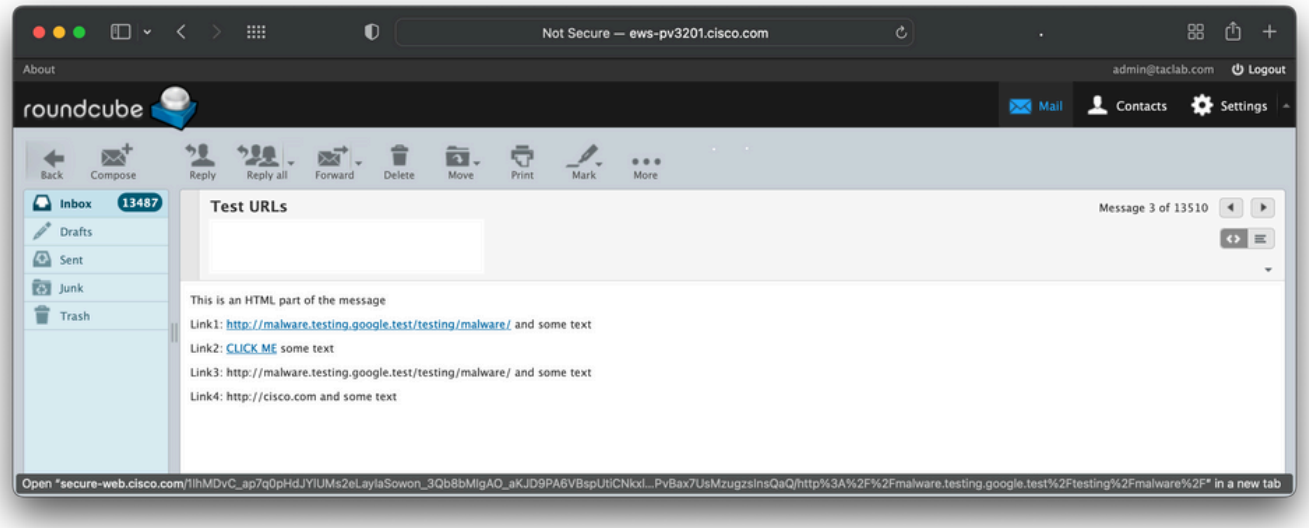
```
Tue Jul 5 12:42:19 2022 Info: MID 139508 URL http://malware.testing.google.test/testing/malware/
has reputation -9.4 matched Condition: URL Reputation Rule Tue Jul 5 12:42:19 2022 Info: MID
139508 Custom Log Entry: URL_SCORE Tue Jul 5 12:42:19 2022 Info: MID 139508 URL
http://malware.testing.google.test/testing/malware/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

Neem een kijkje hoe de URL's worden herschreven in het HTML-gedeelte van het bericht. Net als in Scenario A worden alleen de URL's in het href-kenmerk van een A-tag-element herschreven en worden de URL-adressen in het tekstgedeelte van het A-tag-element overgeslagen. Met een defang actie wordt een volledig A-tag element gestript, maar met een omleiding actie wordt de URL in het href attribuut herschreven.

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

Als gevolg hiervan worden op de e-mailclient twee actieve links weergegeven: Link1 en Link2 verwijzen beide naar de Cisco Web Security Proxy-service, maar het bericht dat wordt weergegeven in de e-mailclient toont het tekstgedeelte van de A-tag dat niet standaard wordt herschreven. Om beter onder dit te zijn neem een kijkje bij de output van de webmail client die de tekst/html deel van het bericht toont.



In het tekst/vlakke deel van het MIME-deel, ziet de omleiding er makkelijker te begrijpen uit omdat elke URL-string die overeenkomt met de score wordt herschreven.

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

Samenvatting:

- Redirect run op het TEXT/PLAIN-onderdeel herschrijft de URL-string die overeenkomt met de Cisco Web Secure-proxyservice
- Redirect run op het TEXT/HTML onderdeel herschrijft de URL van een HTML A-tag href attribuut met de Cisco Web Secure proxy service maar verlaat alle andere URL strings die overeenkomen met ongewijzigd

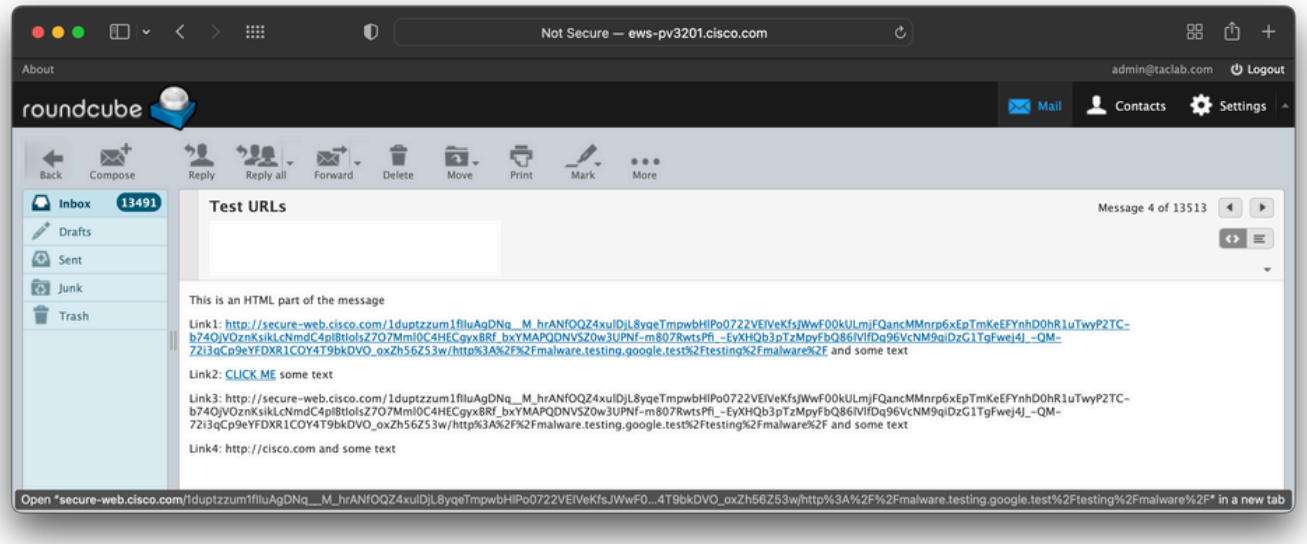
Scenario D

Uitbraakfilter voor detectie van niet-virale bedreigingen	Nee
Actie contentfilter	Doorsturen
websecurityadvancedconfig href en tekst herschrijven is ingeschakeld	Ja

Dit scenario is vergelijkbaar met scenario B van deel één. Alle URL-strings die overeenkomen met het HTML-gedeelte van het bericht worden herschreven. Dit gebeurt met de opdracht websecurity advancedConfig wanneer u Y beantwoordt voor de **"Do you want to rewrite both the URL text and the href in the message? ..** vraag.

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

Zodra href en tekst herschrijven is ingeschakeld, worden alle URL-strings die overeenkomen met de voorwaarden van het inhoudsfilter omgeleid. Het bericht in de e-mailclient wordt nu gepresenteerd met alle omleiding. Om dit beter te begrijpen, bekijk de output van de webmailclient die het tekst/html deel van het bericht toont.



Het tekst/vlakke deel van het MIME-bericht is hetzelfde als in Scenario C, aangezien de websecurity gevorderde verandering in configuratie geen invloed heeft op de tekst/vlakke delen van het bericht.

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

Samenvatting:

- Redirect run op het TEXT/PLAIN-onderdeel herschrijft de URL-strings die overeenkomen met de Cisco Web Secure-proxyservice
- Omleiden run op het TEXT/HTML onderdeel herschrijft de URL van een HTML A-tag href attribuut samen met het tekst onderdeel, evenals een andere URL string die overeenkomt in de HTML body met de Cisco Web Secure proxy service

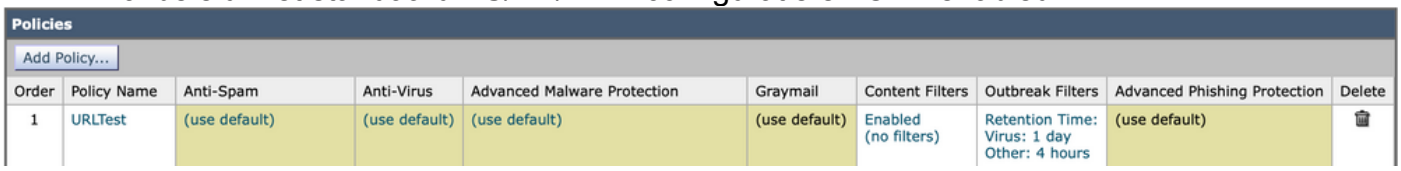
Deel 3 - VAN doorverwijzing

Dit deel bevat informatie over de manier waarop instellingen voor niet-virale detectie van effecten op URL-scans worden uitgevoerd.

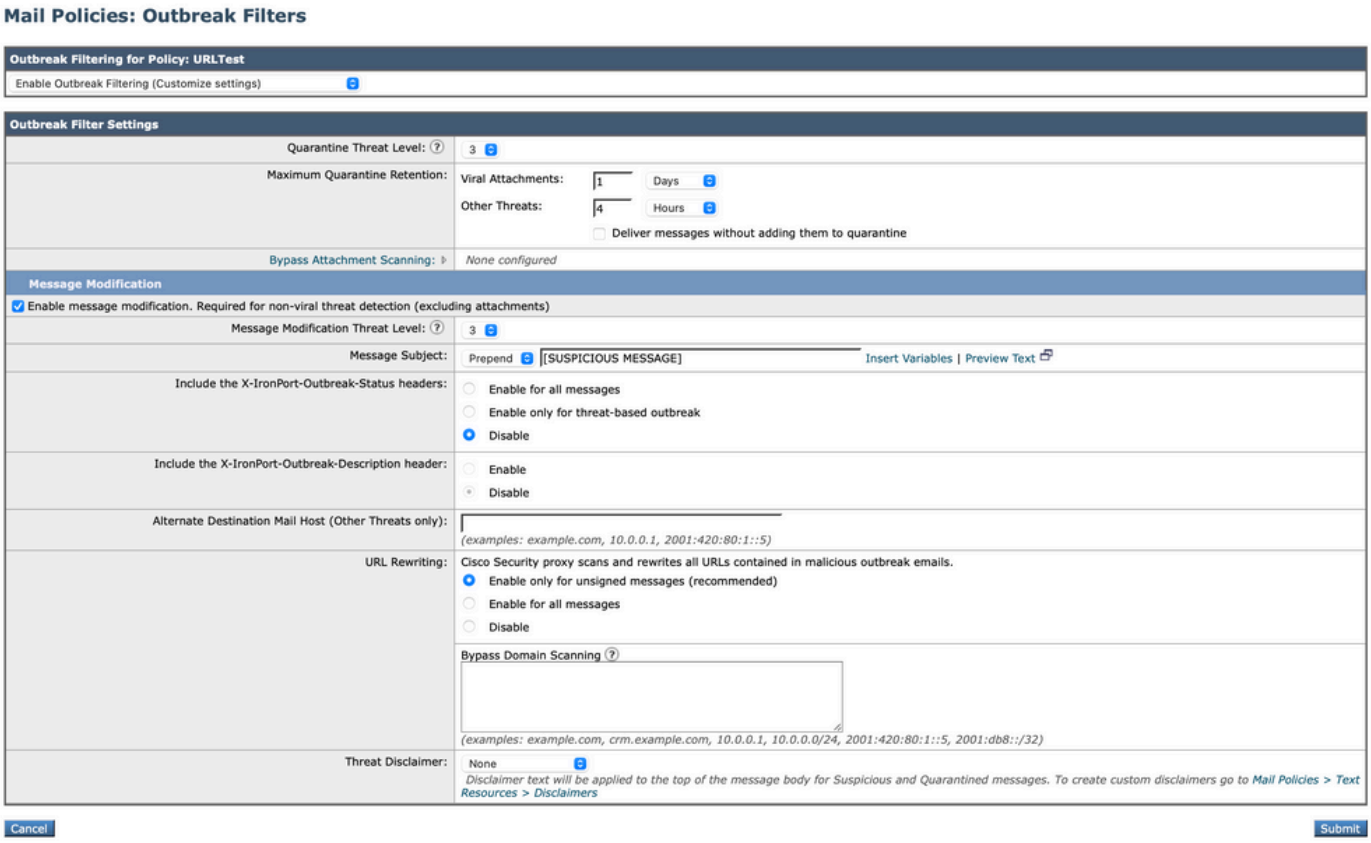
Configuratie

Hiervoor wordt het in de eerste twee delen gebruikte inhoudsfilter uitgeschakeld.

- E-mailbeleid met standaard AS/AV/AMP-configuratie en OFF-enabled



- De Uitbraakfilters scannen voor niet-virale detectie van bedreigingen is geconfigureerd met een URL Rewrite set om alle URL's in kwaadaardige e-mails te herschrijven



Wanneer het bericht is geclassificeerd door OF als kwaadaardig, worden alle URL's binnen opnieuw geschreven met de Cisco Web Secure-proxyservice.

Scenario E

Uitbraakfilter voor detectie van niet-virale bedreigingen	Ja
Actie contentfilter	Nee
websecurityadvancedconfig href en tekst herschrijven is ingeschakeld	Nee

Dit scenario toont hoe het bericht herschrijven werkt met alleen van ingeschakeld en websecurity geavanceerd config href en tekst herschrijven uitgeschakeld.

```
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)
```

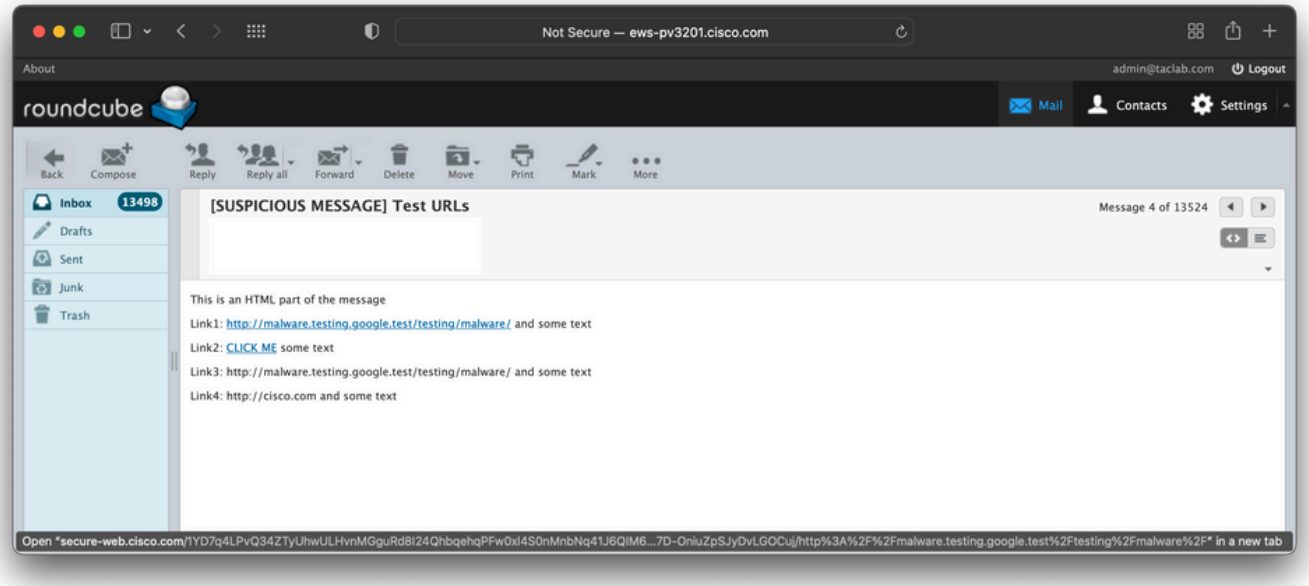
Laten we beginnen met de tekst/effen MIME-onderdeel. Na een snelle controle, kan worden opgemerkt dat alle URL's in het tekst/duidelijke deel worden herschreven naar de Cisco Web Secure-proxyservices. Het gebeurt omdat URL herschrijven is ingeschakeld voor alle URL's in het bericht van de uitbraak.

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

Dit is het verwerkte tekst/html deel van het MIME-bericht.

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



Het eerste wat hier kan worden opgemerkt is waarom Link4 niet is herschreven. Als je het artikel zorgvuldig leest, weet je het antwoord al. Het tekst/html deel van MIME evalueert en manipuleert standaard alleen de href-kenmerken van de A-tag-elementen. Als een soortgelijk gedrag als voor tekst/onbewerkte deel wordt gewenst, moet websecurity geavancedconfig href en tekst herschrijven worden toegelaten. Het volgende scenario doet precies dit.Samenvatting:

- Van doorverwijzing uitvoeren op het TEXT/PLAIN-onderdeel herschrijft alle URL-string die overeenkomt met de Cisco Web Secure-proxyservice
- VAN doorsturen in het TEXT/HTML onderdeel herschrijft alleen de URL van een HTML A-tag href attribuut met de Cisco Web Secure proxy service

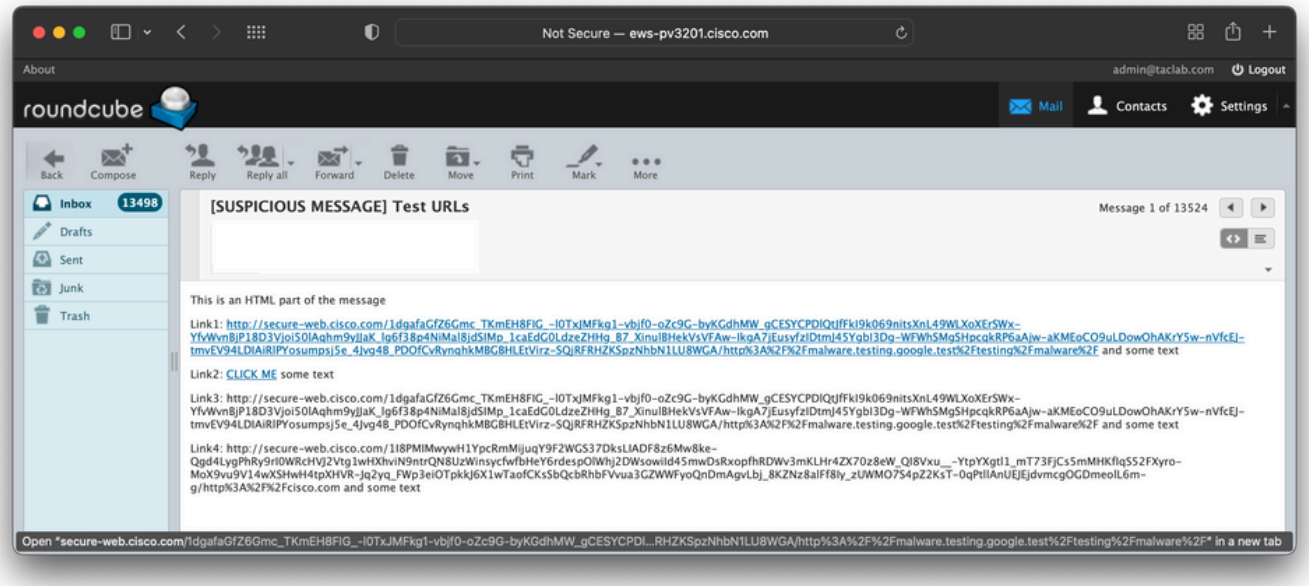
Scenario F

Uitbraakfilter voor detectie van niet-virale bedreigingen	Ja
Actie contentfilter	Nee
websecurityadvancedconfig href en tekst herschrijven is ingeschakeld	Ja

Dit scenario laat websecurityadvancedconfig href en tekst herschrijven toe om te tonen hoe het gedrag in URL herschrijven verstrekt door van niet-virale bedreigingsopsporing verandert. Op dit moment moet worden begrepen dat de websecurity geavanceerdeConfig geen invloed heeft op tekst/effen MIME-onderdelen. Laten we alleen het tekst/html-deel evalueren en zien hoe het gedrag is veranderd.

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

Het kan worden opgemerkt dat de output zeer gelijkaardig is aan die van Scenario D met het enige verschil dat alle URLs, niet alleen de kwaadaardige degenen zijn herschreven. Alle URL-strings die overeenkomen met het HTML-deel, samen met de niet-schadelijke strings worden hier aangepast.



Samenvatting:

- VAN doorsturen van het uitvoeren op het TEXT/PLAIN-onderdeel herschrijft alle URL-strings die overeenkomen met de Cisco Web Secure-proxyservice
- Van doorverwijzing uitvoeren op het TEXT/HTML-onderdeel herschrijft de URL van een HTML A-tag href-kenmerk samen met het tekstgedeelte van het element en alle andere URL-strings die overeenkomen met de Cisco Web Secure-proxyservice

Scenario G

Uitbraakfilter voor detectie van niet-virale bedreigingen	Ja
Actie contentfilter	Defang
websecurityadvancedconfig href en tekst herschrijven is ingeschakeld	Ja

Dit laatste scenario valideert de configuratie.

- E-mailbeleid met standaard AS/AV/AMP-configuratie en OFF-enabled

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)	

- De OFF scan voor niet-virale detectie van bedreigingen is geconfigureerd met URL Rewrite ingesteld om alle URL's in kwaadaardige e-mails te herschrijven (hetzelfde als in eerdere scenario's)
- Inkomende contentfilter: URL_SCORE inhoudsfilter ingeschakeld

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); }		

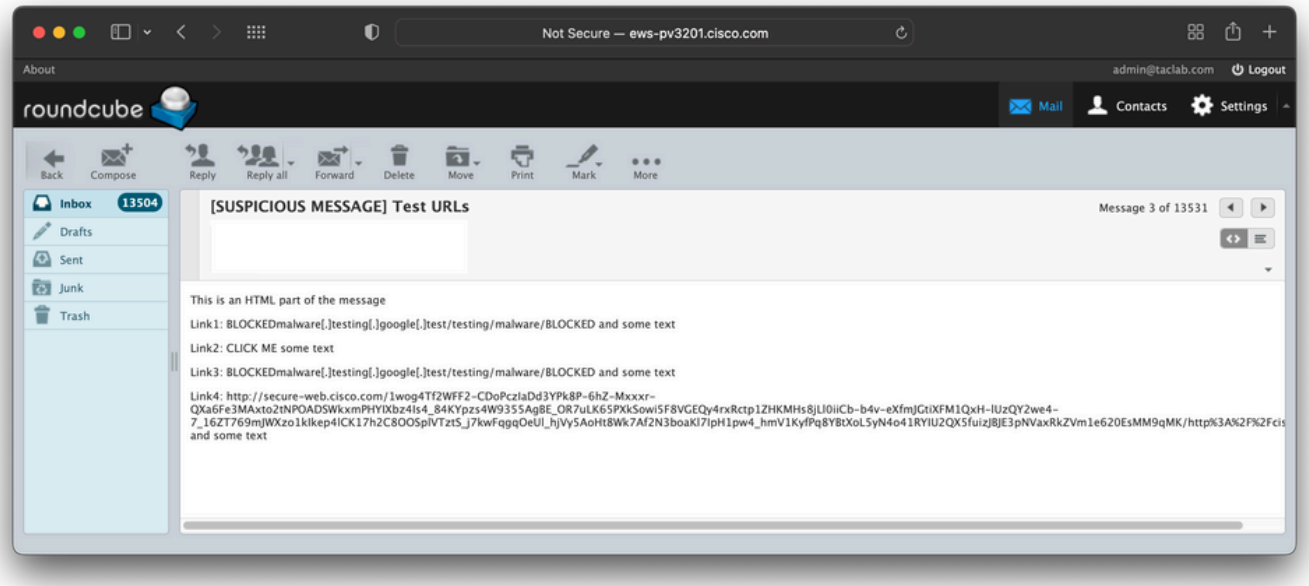
De inhoudsfilter gebruikt de URL-reputatievoorwaarde om kwaadaardige URL's aan te passen, de URL's die tussen -6.00 en -10.00 scoren. Als actie wordt de naam van het inhoudfilter vastgelegd en de defang actie **url-reputation-defang** genomen.

Het zelfde exemplaar van het bericht wordt verzonden en door de e-mailgateway met de resultaten geëvalueerd:

```
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
```

De e-mailpijpleiding legt uit dat het bericht eerst wordt geëvalueerd door de inhoudsfilters, waar de URL_SCORE filter wordt geactiveerd en URL-reputatie-defang-actie wordt toegepast. Deze actie defect alle kwaadaardige URLs in zowel tekst/vlakte als tekst/html MIME-delen. Omdat websecurityadvanceconfig href en tekst herschrijven is ingeschakeld, worden alle URL-strings die overeenkomen met de HTML-hoofdtekst gedefangeerd wanneer alle A-tag-elementen zijn gestript en tekstdelen van de URL tussen geblokkeerde woorden herschrijven en alle punten tussen vierkante haakjes plaatsen. Hetzelfde gebeurt met andere kwaadaardige URL's die niet in A-tag HTML-elementen zijn geplaatst. Het Uitbraakfilter verwerkt vervolgens het bericht. Het OCR detecteert kwaadaardige URL's en identificeert het bericht als kwaadaardig (Threat Level=5). Dientengevolge, herschrijft het alle kwaadwillige en niet kwaadwillige URLs die binnen het bericht worden gevonden. Omdat de actie van het inhoudfilter reeds die URLs wijzigde herschrijft het KIP slechts de rest van niet-kwaadwillige URLs aangezien het opzettelijk werd gevormd om het te doen. Het bericht weergegeven in de e-mailclient als deel van de kwaadaardige URL's defanged en een deel van de niet-kwaadaardige URL omgeleid.

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



Hetzelfde wordt toegepast op het tekst/onbewerkte deel van het MIME-bericht. Alle niet-schadelijke URL's worden omgeleid naar Cisco Web Secure proxy en de schadelijke URL's worden gedefangeerd.

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

Samenvatting:

- CF-defang die op het TEXT/PLAIN-onderdeel wordt uitgevoerd, herschrijft de URL in geblokkeerde blokken
- CF defang uitgevoerd op het TEXT/HTML onderdeel herschrijft de URL van een HTML A-tag wanneer een A-tag is gestript
- CF-defang die wordt uitgevoerd op het TEKST/HTML-onderdeel herschrijft alle URL-strings die overeenkomen met GEBLOKKEERDE blokken
- Van doorverwijzing uitvoeren op het TEXT/PLAIN-onderdeel herschrijft alle URL-strings die overeenkomen met de Cisco Web Secure-proxyservice (niet-kwaadaardig)
- Van doorverwijzing uitvoeren op het TEXT/HTML-onderdeel herschrijft de URL van een HTML A-tag href-kenmerk samen met het tekstgedeelte van het element en alle andere URL-strings die overeenkomen met de Cisco Web Secure-proxyservice (niet-kwaadaardig)

Problemen oplossen

Volg deze punten als er een noodzaak is om het probleem te onderzoeken met URL rewrite.

- URL-logboekregistratie inschakelen in uw mail_logs. Voer uit **OUTBREAKCONFIG** bevel en antwoord **Y** in **Do you wish to enable logging of URL's?** [N]>"
- Verifiëren **WEBSECURITYADVANCECONFIG** instellingen onder elk e-mailgateway cluster lid en zorg

ervoor dat de href en tekst herschrijven optie is ingesteld dienovereenkomstig en hetzelfde op elke machine. Houd in gedachten deze opdracht is machine-level specifiek en wijzigingen die hier worden uitgevoerd hebben geen invloed op de instellingen van de groep of cluster.
- Controleer de voorwaarden en activiteiten van uw content filter en zorg ervoor dat de content filter is ingeschakeld en toegepast op het juiste inkomende mail beleid. Controleer of er geen andere inhoudsfilter verwerkt is met een laatste handeling die kan overslaan om andere filters te verwerken.
- Onderzoek de ruwe kopie van de bron en het definitieve bericht. Houd in gedachten om het bericht op te halen in EML-formaat, de eigen formaten zoals MSG zijn niet betrouwbaar als het gaat om berichtonderzoek. Sommige e-mailclients staan u toe om het bronbericht te bekijken en proberen om de kopie van het bericht op te halen met een andere e-mailclient. Zo kunt u met MS Outlook voor Mac de bron van het bericht bekijken, terwijl u met de Windows-versie alleen de kopregels kunt bekijken.

Samenvatting

Het doel van dit artikel is om te helpen in beter begrip van beschikbare configuratieopties wanneer het over URL herschrijven komt. Het is belangrijk om te onthouden dat moderne berichten worden gebouwd door de meeste e-mail software met de MIME standaard. Het betekent dat dezelfde kopie van het bericht op verschillende manieren kan worden weergegeven, afhankelijk van de mogelijkheden van de e-mailclient of/en de ingeschakelde modi (tekst vs HTML-modus). Standaard gebruiken de meeste moderne e-mailclients HTML om berichten weer te geven. Wanneer het gaat om HTML en URL herschrijven, houd dan in gedachten door standaard e-mail gateway herschrijft alleen URL's gevonden binnen de href attributen van het A-tag element. In veel gevallen is dat niet genoeg en moet worden overwogen om zowel href als tekst te herschrijven met de opdracht WEBSECURITYADVANCEDECONFIG. Onthoud dat dit een opdracht op machineniveau is en dat de wijziging voor consistentie over het cluster afzonderlijk moet worden toegepast op elk van de clusterleden.