Secure Email Gateway의 URL Defang 및 Redirect 작업 이해

목차

소개

이 문서에서는 URL 필터에서 사용되는 디펜스 및 리디렉션 작업의 차이점과 href 특성 및 텍스트에 대해 사용 가능한 재작성 옵션을 사용하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

URL 평판을 기반으로 조치를 취하거나 메시지 및 콘텐츠 필터로 사용 제한 정책을 시행하려면 Outbreak Filter 기능을 전역적으로 활성화해야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure Email Gateway
- 신종 바이러스 필터
- 콘텐츠 및 메시지 필터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

URL 필터링 기능 중 하나는 메시지 및/또는 콘텐츠 필터를 사용하여 URL 평판 또는 카테고리에 따라 작업을 수행하는 것입니다. URL 스캔 결과(URL 관련 조건)에 따라 URL에서 사용 가능한 다음 세 가지 작업 중 하나를 적용할 수 있습니다.

- 디팡 URL
- Cisco 보안 프록시로 이동
- URL을 텍스트 메시지로 바꾸기

이 문서에서는 Defang 및 Redirect URL 옵션 간의 동작을 설명합니다. 또한 Outbreak Filter의 비 바이러스성 위협 탐지의 URL 재작성 기능에 대한 간단한 설명과 설명을 제공합니다.

메시지 샘플

모든 테스트에서 사용되는 샘플 메시지는 MIME multipart/alternative 메시지 유형이며 text/plain 및 text/html 부분을 모두 포함합니다. 이러한 부품은 일반적으로 이메일 소프트웨어에 의해 자동으로 생성되며 HTML 및 비HTML 수신기용으로 서식이 지정된 같은 종류의 콘텐츠를 포함합니다. 이를 위해 text/plain 및 text/html의 내용을 수동으로 편집하였다.

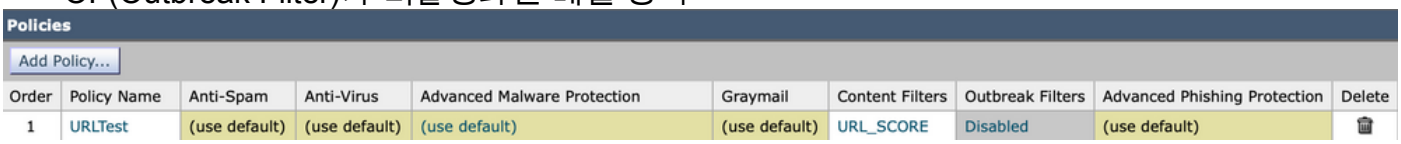
```
Content-Type: multipart/alternative; boundary="===============7781793576330041025==" MIME-
Version: 1.0 From: admin@example.com Date: Mon, 04 Jul 2022 14:38:52 +0200 To: admin@cisco.com
Subject: Test URLs --===============7781793576330041025== Content-Type: text/plain; charset="us-
ascii" MIME-Version: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

I부 - 데팡

설정

첫 번째 부분에서는 컨피그레이션에서 다음을 사용합니다.

- 기본 AS(Anti-Spam)/AV(Anti-Virus)/AMP(Advanced Malware Protection) 컨피그레이션 및 OF(Outbreak Filter)가 비활성화된 메일 정책



- 수신 콘텐츠 필터: URL_SCORE 콘텐츠 필터 사용

콘텐츠 필터는 URL 평판 조건을 사용하여 악의적인 URL(점수가 -6.00에서 -10.00 사이인 URL)과 일치시킵니다. 작업으로 콘텐츠 필터 이름이 기록되고 defang 작업이 수행됩니다 **url-reputation-defang** 있습니다.

디팡액션

무엇이 방어 행위인지를 명확히 하는 것이 중요하다. 사용 설명서에 대한 설명이 나와 있습니다. 클릭할 수 없도록 URL을 정의합니다. 메시지 수신자는 여전히 URL을 보고 복사할 수 있습니다.

시나리오 A

Outbreak Filter 비 바이러스성 위협 탐지	아니요
콘텐츠 필터 작업	디팡
websecurityadvancedconfig href 및 텍스트 재작성이 활성화되어 있습니다.	아니요

이 시나리오에서는 기본 설정으로 구성된 기본 작업의 결과를 설명합니다. 기본 설정에서는 HTML 태그만 제거되면 URL이 다시 작성됩니다. URL이 포함된 HTML 단락을 살펴보십시오.

```
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
```

처음 두 단락에서 URL은 적절한 HTML A-tag로 표시됩니다. <A> 요소에는 **href=** 태그 자체에 포함되고 링크 대상을 나타내는 특성입니다. 태그 요소 내의 콘텐츠는 링크 목적지를 나타낼 수도 있다. 이 **text form** URL을 포함할 수 있습니다. 첫 번째 Link1은 요소의 href 특성 및 텍스트 부분에 동일한 URL 링크를 포함합니다. 이러한 URL은 다를 수 있습니다. 두 번째 Link2는 href 특성 내에서만 적절한 URL을 포함합니다. 마지막 단락은 A 요소를 포함하지 않습니다.

> **참고:** 링크 위로 커서를 이동하거나 메시지의 소스 코드를 볼 때 항상 정확한 주소를 볼 수 있습니다. 안타깝게도 일부 인기 이메일 클라이언트에서는 소스 코드를 쉽게 찾을 수 없습니다.

메시지가 URL_SCORE 필터와 일치하면 악성 URL이 삭제됩니다. URL 로깅이 **OUTBREAKCONFIG** command the scores and URLs can be found 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'
```

이렇게 하면 메시지가 다시 작성됩니다.

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

MIME 메시지의 text/html 부분에 대해 수행된 디펜스 작업의 결과는 stripped A-tag이며 태그 내용은 그대로 유지됩니다. 두 개의 첫 번째 단락에서는 HTML 코드가 제거되고 요소의 텍스트 부분이 남아 있는 위치에 두 링크가 모두 정의됩니다. 첫 번째 단락의 URL 주소는 HTML 요소의 텍스트 부분에 있는 주소입니다. 첫 번째 단락의 URL 주소는 디펜스 작업이 수행된 후에도 계속 표시되지만 HTML A-태그가 없으면 요소를 클릭할 수 없어야 합니다. 세 번째 단락은 URL 주소가 A 태그 사이에 위치하지 않으며 링크로 간주되지 않으므로 정의되지 않습니다. 어쩌면 두 가지 이유로 인해 바람직한 행동이 아닐 수도 있다. 첫째, 사용자는 링크를 쉽게 보고 복사하여 브라우저에서 실행할 수 있다. 두 번째 이유는 일부 이메일 소프트웨어가 텍스트 내부의 유효한 형식의 URL을 탐지하여 클릭 가능한 링크로 만드는 경향이 있기 때문입니다.

MIME 메시지의 텍스트/일반 부분을 살펴보겠습니다. 텍스트/일반 부분에는 텍스트 형식의 URL이 2개 있습니다. 텍스트 / 평판은 HTML 코드를 이해 하지 않는 MUA에 의해 표시 됩니다. 대부분의 최신 이메일 클라이언트에서는 의도적으로 이메일 클라이언트를 구성하지 않는 한 메시지의 텍스트/일반 부분이 표시되지 않습니다. 일반적으로 MIME 부분을 보고 조사하려면 메시지의 소스 코드, 메시지의 원시 EML 형식을 확인해야 합니다.

이 목록에는 소스 메시지의 텍스트/일반 부분의 URL이 표시됩니다.

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

그 두 링크 중 하나가 악성 점수를 받아 탈취당했다. 기본적으로 MIME 유형의 text/plain 부분에 대해 수행한 기본 작업은 text/html 부분과 결과가 다릅니다. BLOCKED 단어와 대괄호 안의 모든 점 사이에 있습니다.

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

요약:

- TEXT/PLAIN 부분에서 DEFANG을 실행하면 URL이 차단된 블록에 재작성됩니다.
- TEXT/HTML 부분에서 실행된 Defang은 HTML A-tag에서 URL을 재작성합니다. 이때 A-tag 사이에 텍스트를 건드리지 않고 A-tag를 제거하면 URL 주소일 수도 있습니다

시나리오 B

Outbreak Filter 비 바이러스성 위협 탐지	아니요
콘텐츠 필터 작업	디팡
websecurityadvancedconfig href 및 텍스트 재작성이 활성화되어 있습니다.	예

이 시나리오에서는 websecurityadvancedconfig 옵션 중 하나를 사용한 후 defangs 작업의 동작이 어떻게 변경되는지에 대한 정보를 제공합니다. websecurityadvancedconfig는 URL 스캔과 관련된 설정을 조정할 수 있는 시스템 수준별 CLI 명령입니다. 여기서 설정한 내용 중 하나를 사용하여 기본 동작 정의 동작을 변경할 수 있습니다.

```
> 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
...
```

네 번째 질문은 **Do you want to rewrite both the URL text and the href in the message? ..**, 대답 **Y** 메시지의 HTML 기반 MIME 부분의 경우 A-tag 요소의 href 특성에서 발견된 것과 상관없이 일치하는 모든 URL 문자열이 텍스트 부분이거나 재작성된 요소의 외부에 있음을 나타냅니다. 이 시나리오에서는 동일한 메시지가 재전송되지만 결과는 약간 다릅니다.

URL이 포함된 text/html MIME 부품 코드를 다시 한 번 살펴보고 이메일 게이트웨이에서 처리된 HTML 코드와 비교합니다.

```
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
```

href 및 텍스트 재작성 옵션이 활성화된 경우, URL 주소가 href 특성의 일부이든 A-tag HTML 요소의 텍스트 부분이든 HTML 문서의 다른 부분에 있든 상관없이 필터 URL에 의해 일치하는 모든 URL이 정의됩니다.

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

A-tag 요소가 URL 형식과 일치할 때 링크의 텍스트 부분 재작성과 함께 제거되면 정의된 URL이 다시 작성됩니다. 재작성된 텍스트 부분은 MIME 메시지의 text/plain 부분과 같은 방식으로 수행됩니다. 항목이 차단된 단어 사이에 배치되고 모든 점이 대괄호 사이에 배치됩니다. 이렇게 하면 사용자가 URL을 복사하여 붙여넣을 수 없으며 일부 이메일 소프트웨어 클라이언트는 텍스트를 클릭할 수 있게 만듭니다.

요약:

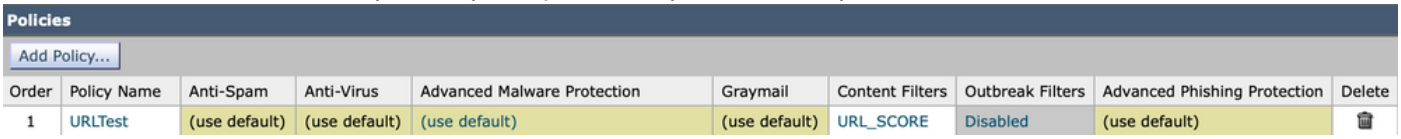
- TEXT/PLAIN 부분에서 DEFANG을 실행하면 URL이 차단된 블록에 재작성됩니다.
- TEXT/HTML 부분에서 실행되면 A 태그가 제거될 때 HTML A 태그에서 URL이 재작성됩니다
- TEXT/HTML 파트에서 실행된 Defang은 차단된 블록으로 일치하는 모든 URL 문자열을 재작성합니다

II부 - 리디렉션

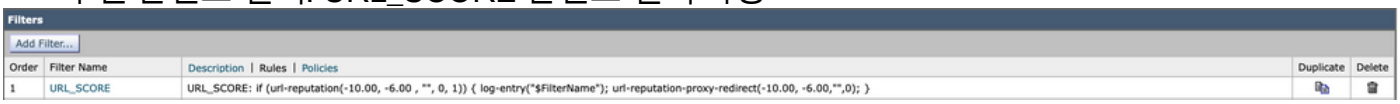
설정

두 번째 부분에서는 컨피그레이션에서 다음을 사용합니다.

- 기본 AS/AV/AMP 컨피그레이션 및 OF가 비활성화된 메일 정책



- 수신 콘텐츠 필터: URL_SCORE 콘텐츠 필터 사용



콘텐츠 필터는 URL 평판 조건을 사용하여 악의적인 URL(점수가 -6.00에서 -10.00 사이임)과 일치시킵니다. 작업으로 콘텐츠 필터 이름이 기록되고 **redirect action** 있습니다.

리디렉션 작업

클릭 시 평가를 위한 Cisco Security Proxy 서비스로 리디렉션하면 메시지 수신자가 링크를 클릭하여 클라우드의 Cisco 웹 보안 프록시로 리디렉션할 수 있습니다. 그러면 사이트가 악성으로 식별된 경우 액세스가 차단됩니다.

시나리오 C

Outbreak Filter 비 바이러스성 위협 탐지	아니요
콘텐츠 필터 작업	리디렉션
websecurityadvancedconfig href 및 텍스트 재작성이 활성화되어 있습니다.	아니요

이 시나리오는 첫 번째 부분의 시나리오 A와 동작이 매우 유사하며, URL을 정의하는 대신 리디렉션하는 콘텐츠 필터 작업의 차이점이 있습니다. websecurityadvancedconfig 설정이 기본 설정으로 복원되므로 **"Do you want to rewrite both the URL text and the href in the message? ..** 다음으로 설정됨 **N.**

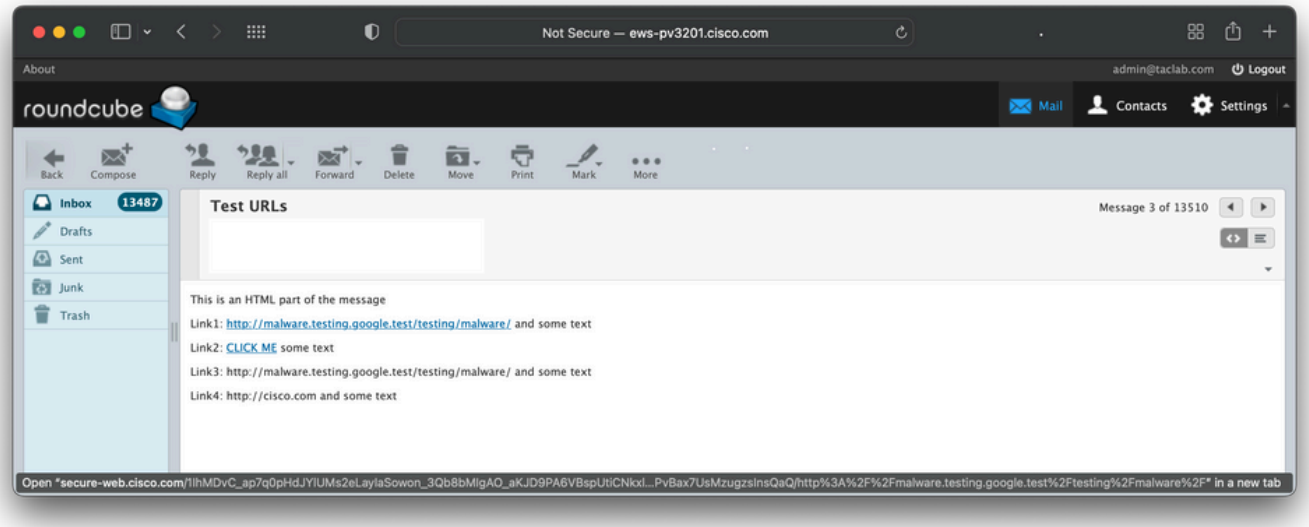
이메일 게이트웨이는 각 URL을 탐지하고 평가합니다. 악의적인 점수는 URL_SCORE 콘텐츠 필터 규칙을 트리거하고 작업을 수행합니다 **url-reputation-proxy-redirect-action**

```
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'
```

메시지의 HTML 부분에서 URL이 어떻게 재작성되는지 살펴보십시오. 시나리오 A와 마찬가지로 A-tag 요소의 href 특성에 있는 URL만 재작성되고 A-tag 요소의 텍스트 부분에 있는 URL 주소는 건너뜁니다. defang 작업을 수행하면 전체 A-tag 요소가 제거되지만 리디렉션 작업을 수행하면 href 특성의 URL이 다시 작성됩니다.

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

그 결과 이메일 클라이언트에는 두 개의 활성 링크가 표시됩니다. Link1 및 Link2는 모두 Cisco Web Security Proxy 서비스를 가리키지만 이메일 클라이언트에 표시되는 메시지에는 기본적으로 재작성되지 않는 A-tag의 텍스트 부분이 표시됩니다. 이 기능을 더 잘 사용하려면 메시지의 text/html 부분을 표시하는 웹 메일 클라이언트의 출력을 확인하십시오.



MIME 부분의 text/plain 부분에서는 점수와 일치하는 모든 URL 문자열이 재작성되므로 리디렉션을 쉽게 이해할 수 있습니다.

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

요약:

- TEXT/PLAIN 부분에서 리디렉션 실행은 Cisco Web Secure 프록시 서비스와 일치하는 URL 문자열을 재작성합니다
- TEXT/HTML 부분에 대한 리디렉션 실행은 HTML A-tag href 특성에서 Cisco Web Secure 프록시 서비스로 URL을 재작성하지만 수정되지 않은 것과 일치하는 다른 모든 URL 문자열은 남겨둡니다

시나리오 D

Outbreak Filter 비 바이러스성 위협 탐지	아니요
콘텐츠 필터 작업	리디렉션
websecurityadvancedconfig href 및 텍스트 재작성이 활성화되어 있습니다.	예

이 시나리오는 1부의 시나리오 B와 유사합니다. 메시지의 HTML 부분에서 일치하는 모든 URL 문자열을 재작성하려면 이 활성화됩니다. 이 작업은 websecurityadvancedconfig 명령을 사용하여 **"Do you want to rewrite both the URL text and the href in the message? ..** 질문.

```
--===============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_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF00kULmjFQancMMnrp6xEpTmKeEFYnhD0hR1uTwyP2TC-b74OjVOznKsikLcNmdC4pIBtIolsZ7O7Mml0C4HECgyxBRf_bxYMAPQDNVSZ0w3UPNf-m807RwtsPfi_-EyXHQb3pTzMpyFbQ86lVlfDq96VcNM9qiDzG1TgFwej4J_-QM-72i3qCp9eYFDXR1COY4T9bkDVO_oxZh56Z53w/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F and some text

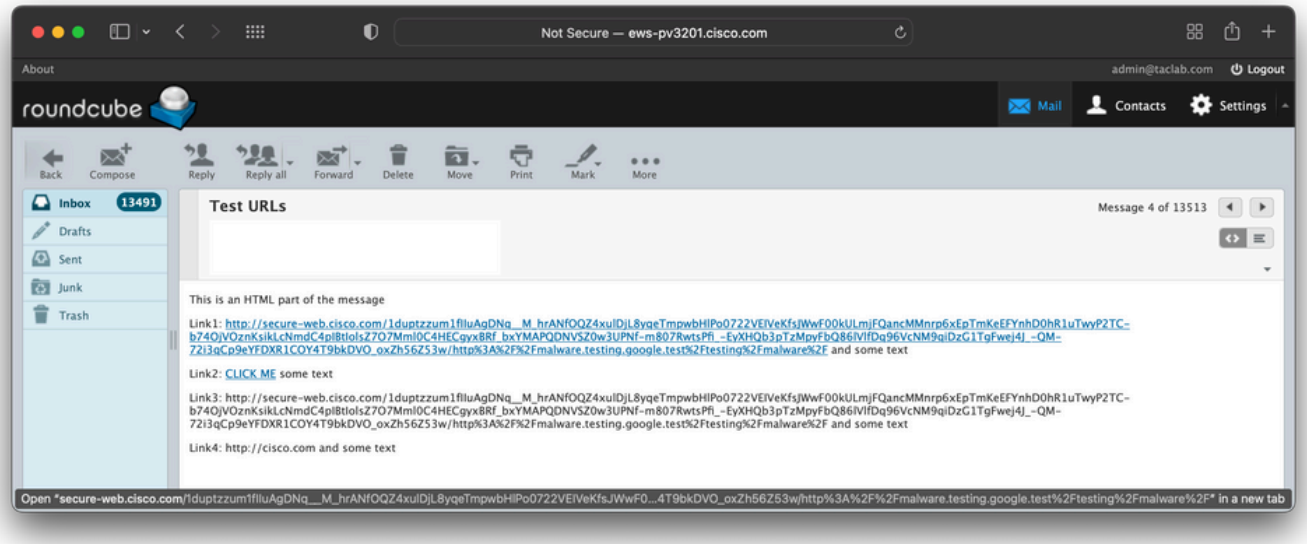
Link2: CLICK ME some text

Link3: http://secure-web.cisco.com/1duptzzum1fIIuAgDNq__M_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF00kULmjFQancMMnrp6xEpTmKeEFYnhD0hR1uTwyP2TC-b74OjVOznKsikLcNmdC4pIBtIolsZ7O7Mml0C4HECgyxBRf_bxYMAPQDNVSZ0w3UPNf-m807RwtsPfi_-EyXHQb3pTzMpyFbQ86lVlfDq96VcNM9qiDzG1TgFwej4J_-QM-72i3qCp9eYFDXR1COY4T9bkDVO_oxZh56Z53w/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F and some text

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

--===============7781793576330041025==--

href 및 텍스트 재작성이 활성화되면 콘텐츠 필터 조건과 일치하는 모든 URL 문자열이 리디렉션됩니다. 이제 이메일 클라이언트의 메시지에 모든 리디렉션이 표시됩니다. 이 내용을 더 잘 이해하려면 메시지의 text/html 부분을 표시하는 웹 메일 클라이언트의 출력을 확인합니다.



MIME 메시지의 text/plain 부분은 시나리오 C와 동일하며 websecurityadvancedconfig 변경이 메시지의 text/plain 부분에 영향을 미치지 않습니다.

--===============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_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF00kULmjFQancMMnrp6xEpTmKeEFYnhD0hR1uTwyP2TC-b74OjVOznKsikLcNmdC4pIBtIolsZ7O7Mml0C4HECgyxBRf_bxYMAPQDNVSZ0w3UPNf-m807RwtsPfi_-EyXHQb3pTzMpyFbQ86lVlfDq96VcNM9qiDzG1TgFwej4J_-QM-72i3qCp9eYFDXR1COY4T9bkDVO_oxZh56Z53w/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F and some text Link2: http://cisco.com and some text --===============7781793576330041025==

요약:

- TEXT/PLAIN 부분에서 리디렉션 실행은 Cisco Web Secure 프록시 서비스와 일치하는 URL 문자열을 재작성합니다

- TEXT/HTML 파트에서 실행된 리디렉션은 HTML A-tag href 특성에서 URL을 텍스트 파트와 함께 재작성하고 HTML 본문에서 Cisco Web Secure 프록시 서비스와 일치하는 다른 URL 문자열도 재작성합니다

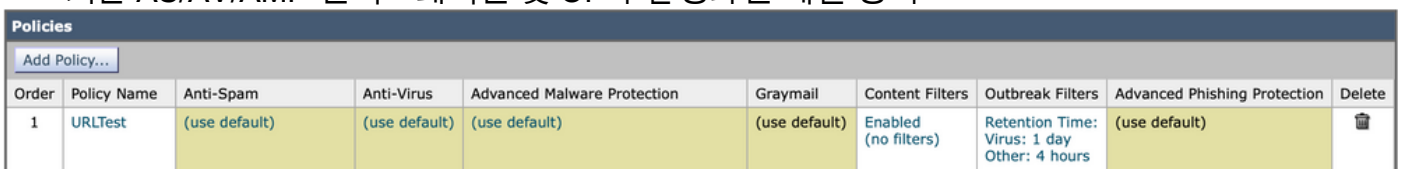
3부 - 리디렉션

이 부분에서는 비 바이러스성 위협 탐지에 대한 OF 설정이 URL 스캔에 미치는 영향에 대한 정보를 제공합니다.

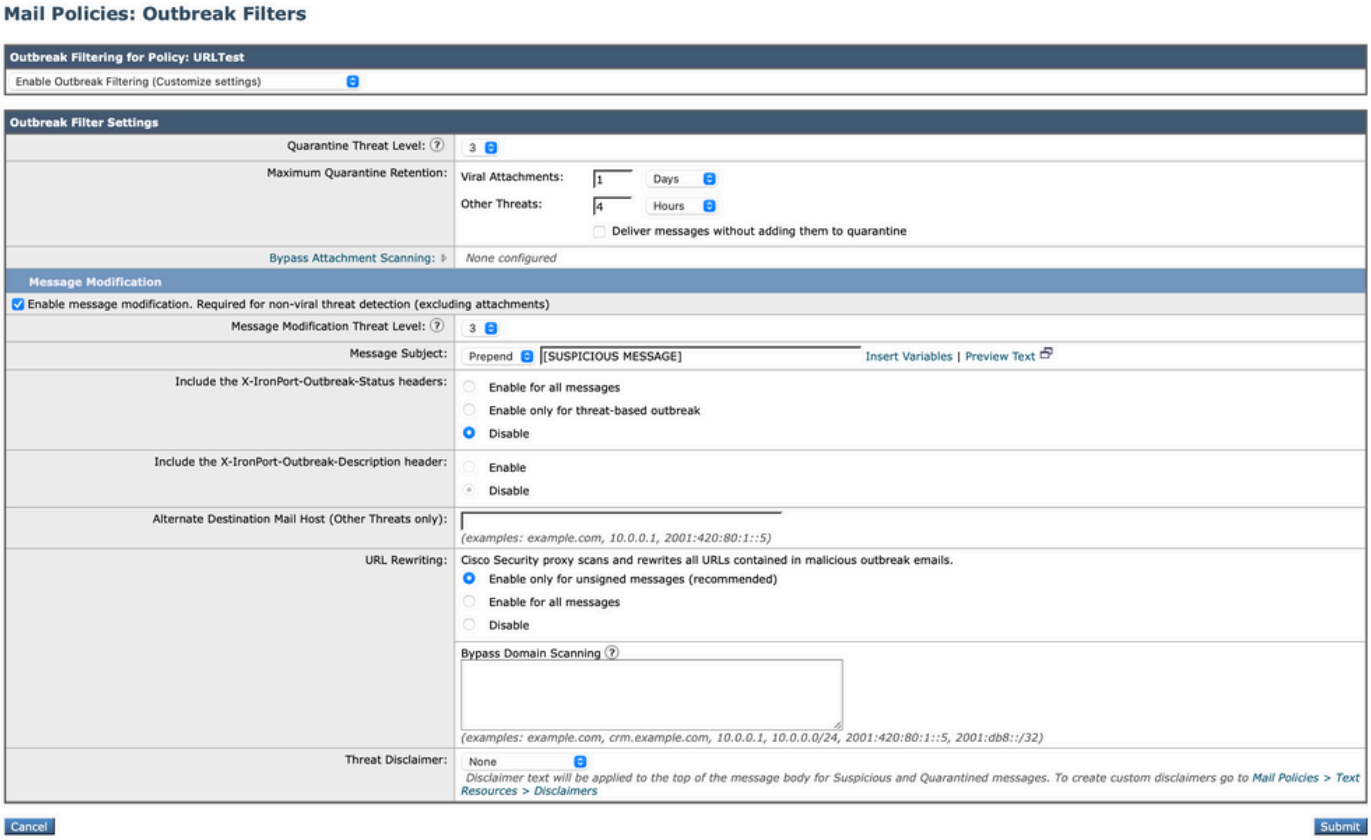
설정

이를 위해, 처음 두 부분에서 사용된 콘텐츠 필터는 비활성화된다.

- 기본 AS/AV/AMP 컨피그레이션 및 OF가 활성화된 메일 정책



- Outbreak Filter에서 비바이러스성 위협 탐지를 검사하려면 악성 이메일에 포함된 모든 URL을 재작성하도록 설정된 URL 재작성을 사용합니다



메시지가 OF에 의해 악성으로 분류되면 내부의 모든 URL이 Cisco Web Secure 프록시 서비스로 다시 작성됩니다.

시나리오 E

Outbreak Filter 비 바이러스성 위협 탐지	예

콘텐츠 필터 작업	아니요
websecurityadvancedconfig href 및 텍스트 재작성이 활성화되어 있습니다.	아니요

이 시나리오에서는 OF만 활성화되고 websecurityadvancedconfig href 및 텍스트 재작성은 비활성화된 상태에서 메시지 재작성이 작동하는 방식을 보여줍니다.

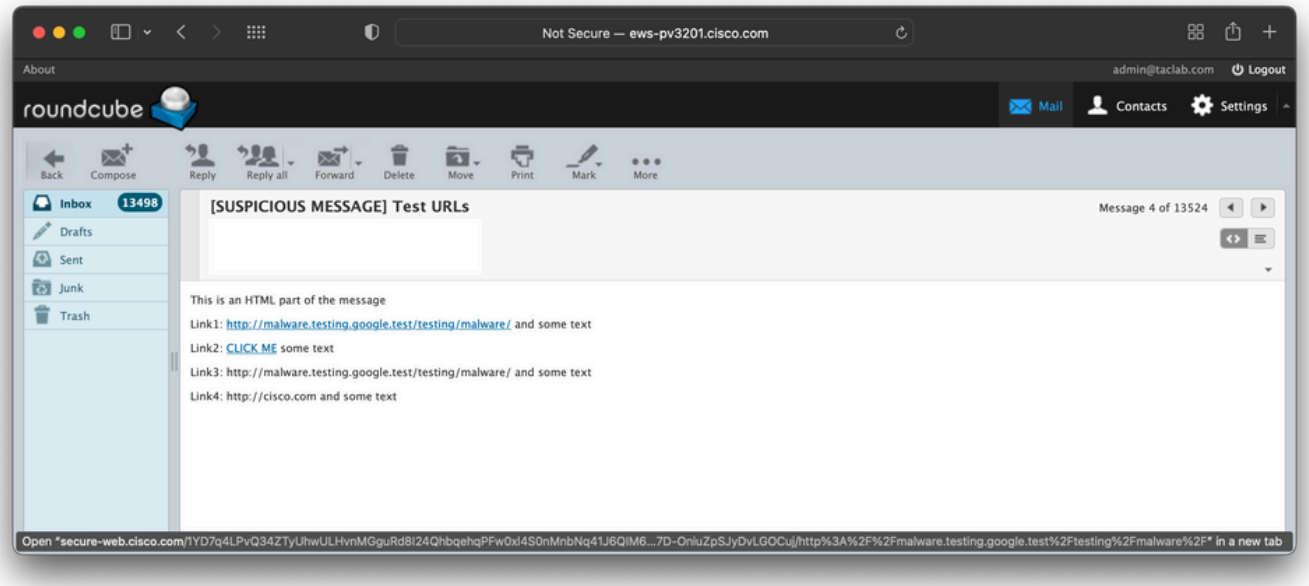
```
Wed Jul 6 14:09:19 2022 Info: MID 139514 Outbreak Filters: verdict positive Wed Jul 6 14:09:19
2022 Info: MID 139514 Threat Level=5 Category=Phish Type=Phish Wed Jul 6 14:09:19 2022 Info: MID
139514 rewritten URL u'http://malware.testing.google.test/testing/malware/' Wed Jul 6 14:09:19
2022 Info: 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)
```

text/plain MIME 부분부터 시작하겠습니다. 빠른 확인 후 텍스트/일반 부분 내부의 모든 URL이 Cisco Web Secure 프록시 서비스에 재작성됩니다. 이는 Outbreak 악성 메시지 내의 모든 URL에 대해 URL 재작성이 활성화되었기 때문입니다.

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

MIME 메시지의 처리된 텍스트/html 부분입니다.

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



여기서 주목할 수 있는 첫 번째 이유는 Link4가 재작성되지 않은 이유입니다. 당신이 그 기사를 주의 깊게 읽었다면, 당신은 이미 답을 알고 있다. MIME의 text/html 파트는 기본적으로 A-tag 요소의 href 특성만 평가하고 조작합니다. 텍스트/일반 부품과 유사한 동작이 필요한 경우 websecurityadvancedconfig href 및 텍스트 재작성을 활성화해야 합니다. 다음 시나리오는 정확히 이렇습니다.요약:

- TEXT/PLAIN 부분에서 실행된 OF 리디렉션은 Cisco Web Secure 프록시 서비스와 일치하는 모든 URL 문자열을 재작성합니다
- TEXT/HTML 파트에서 실행된 OF 리디렉션은 Cisco Web Secure 프록시 서비스를 사용하여 HTML A-tag href 특성에서 URL만 재작성합니다

시나리오 F

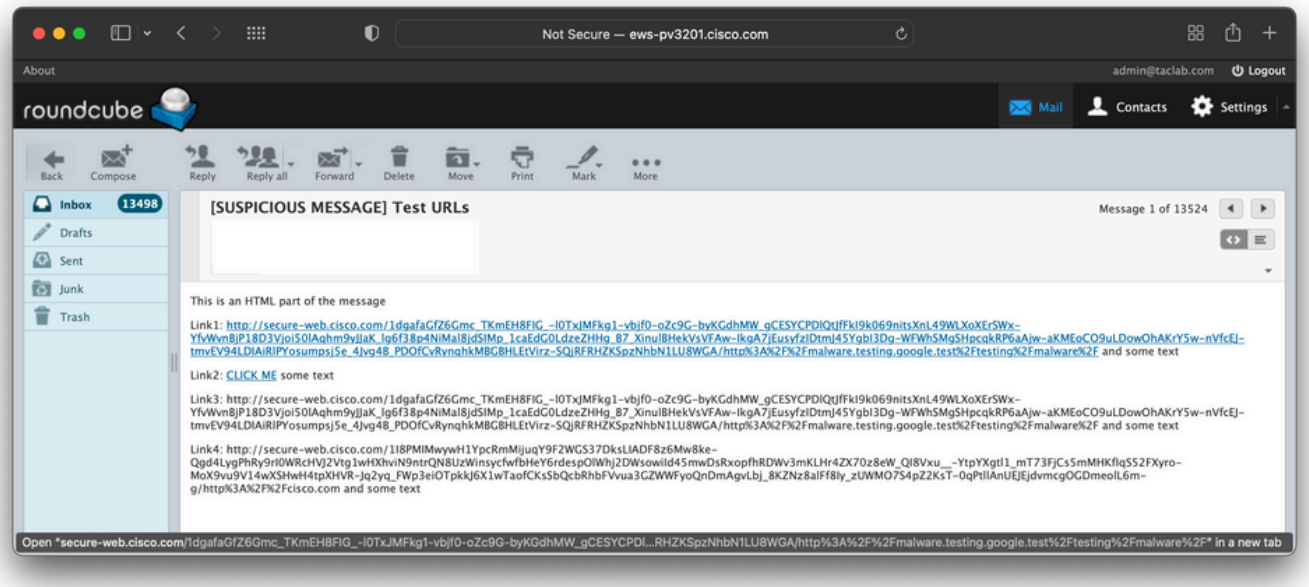
Outbreak Filter 비 바이러스성 위협 탐지	예
콘텐츠 필터 작업	아니요
websecurityadvancedconfig href 및 텍스트 재작성이 활성화되어 있습니다.	예

이 시나리오에서는 websecurityadvancedconfig href 및 텍스트 재작성을 통해 OF 비 바이러스성 위협 탐지에서 제공하는 URL 재작성의 동작이 어떻게 변경되는지 보여줍니다. 이때 websecurityadvancedconfig는 text/plain MIME 부분에 영향을 주지 않습니다. 텍스트/html 부분만 평가하고 동작이 어떻게 변경되었는지 알아보겠습니다.

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

이 출력은 시나리오 D의 출력과 매우 유사하며 악의적인 URL뿐만 아니라 모든 URL이 재작성되었다는 차이점만 있습니다. HTML 부분에서 비악성 문자열과 함께 일치하는 모든 URL 문자열이 여기서 수정됩니다.



요약:

- TEXT/PLAIN 부분에서 실행된 OF 리디렉션은 Cisco Web Secure 프록시 서비스와 일치하는 모든 URL 문자열을 재작성합니다
- TEXT/HTML 부분에서 실행된 OF 리디렉션은 HTML A-tag href 특성에서 URL을 요소의 텍스트 부분 및 Cisco Web Secure 프록시 서비스와 일치하는 다른 모든 URL 문자열과 함께 재작성합니다

시나리오 G

Outbreak Filter 비 바이러스성 위협 탐지	예
콘텐츠 필터 작업	디팡
websecurityadvancedconfig href 및 텍스트 재작성이 활성화되어 있습니다.	예

이 마지막 시나리오에서는 구성을 검증합니다.

- 기본 AS/AV/AMP 컨피그레이션 및 OF가 활성화된 메일 정책

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)	

- 비 바이러스성 위협 탐지에 대한 OF 스캔은 악의적인 이메일에 포함된 모든 URL을 재작성하도록 설정된 URL 재작성으로 구성됩니다(이전 시나리오와 동일)
- 수신 콘텐츠 필터: URL_SCORE 콘텐츠 필터 사용

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); }		

콘텐츠 필터는 URL 평판 조건을 사용하여 악의적인 URL(점수가 -6.00에서 -10.00 사이인 URL)과 일치시킵니다. 작업으로 콘텐츠 필터 이름이 기록되고 defang 작업이 수행됩니다 **url-reputation-defang** 있습니다.

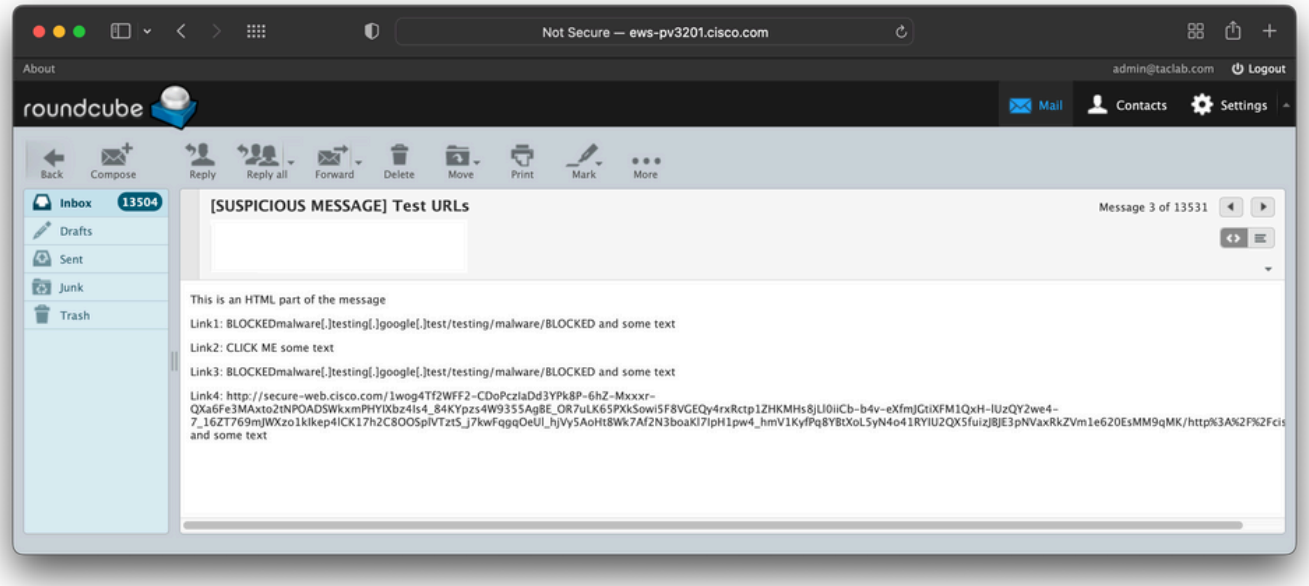
동일한 메시지 복사본이 이메일 게이트웨이에 의해 전송되고 평가되며 결과는 다음과 같습니다.

```
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
```

이메일 파이프라인은 메시지가 콘텐츠 필터에 의해 먼저 평가됨을 설명합니다. 콘텐츠 필터에서는 URL_SCORE 필터가 트리거되고 URL-reputation-defang-action이 적용됩니다. 이 작업은 text/plain 및 text/html MIME 부분의 모든 악성 URL을 나타냅니다. websecurityadvanceconfig href 및 텍스트 재작성을 활성화하므로 모든 A-tag 요소가 제거되고 URL의 텍스트 부분을 차단된 단어 사이에 재작성하고 모든 점을 대괄호 사이에 배치하면 HTML 본문 내에서 일치하는 모든 URL 문자열이 정의됩니다. A-tag HTML 요소에 배치되지 않은 다른 악성 URL에서도 마찬가지입니다. 다음으로 Outbreak Filter가 메시지를 처리합니다. OF는 악성 URL을 탐지하고 메시지를 악의적인 것으로 식별합니다(Threat Level=5). 그 결과, 메시지 내부에서 발견된 모든 악성 URL 및 비악성 URL을 재작성합니다. 콘텐츠 필터 작업이 이미 이러한 URL을 수정했기 때문에 OF는 의도적으로 URL을 수정하도록 구성된 나머지 비악성 URL만 재작성합니다. 악성 URL의 일부로 이메일 클라이언트에 표시된 메시지가 무시되었으며 비악성 URL의 일부가 리디렉션되었습니다.

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



MIME 메시지의 text/plain 부분도 마찬가지입니다. 모든 비악성 URL은 Cisco Web Secure 프록시로 리디렉션되고 악성 URL이 정의됩니다.

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

요약:

- TEXT/PLAIN 부분에서 실행된 CF defang은 URL을 차단된 블록에 재작성합니다
- TEXT/HTML 부분에서 실행되는 CF defang은 A 태그가 제거될 때 HTML A-태그에서 URL을 재작성합니다
- TEXT/HTML 부분에서 실행되는 CF defang은 차단된 블록으로 일치하는 모든 URL 문자열을 재작성합니다
- TEXT/PLAIN 부분에서 실행된 OF 리디렉션은 Cisco Web Secure 프록시 서비스(비악성)와 일치하는 모든 URL 문자열을 재작성합니다
- TEXT/HTML 부분에서 실행된 OF 리디렉션은 HTML A-tag href 특성에서 URL을 요소의 텍스트 부분 및 Cisco Web Secure 프록시 서비스와 일치하는 다른 모든 URL 문자열과 함께 재작성합니다(비악성)

문제 해결

URL 재작성 문제를 조사해야 할 경우 다음 사항을 따르십시오.

- mail_logs에서 URL 로깅을 활성화합니다. 실행 **OUTBREAKCONFIG** 명령과 응답 **Y** 수신 **Do you wish to enable logging of URL's?** [N]**>"**
- 다음을 확인합니다. **WEBSECURITYADVANCECONFIG** 각 이메일 게이트웨이 클러스터 멤버의 설정 및 href 및 텍스트 재작성 옵션이 적절하게 설정되어 있고 각 시스템에서 동일한지 확인합니다. 이 명령은 시스템 수준별로 적용되며 여기서 변경한 내용은 그룹 또는 클러스터 설정에 영향을 주지 않습니다.
- 콘텐츠 필터의 조건과 활동을 확인하고 콘텐츠 필터가 활성화되고 올바른 수신 메일 정책에 적용되는지 확인합니다. 다른 필터 처리로 건너뛸 수 있는 최종 작업으로 이전에 처리된 다른 콘텐츠 필터가 없는지 확인합니다.
- 원본 및 최종 메시지의 원시 복사본을 조사합니다. EML 형식으로 메시지를 검색하는 것을 염두에 두십시오, MSG와 같은 독점 형식은 메시지 조사에 관해서 신뢰할 수 없습니다. 일부 이메일 클라이언트에서는 소스 메시지를 볼 수 있으며 다른 이메일 클라이언트에서 메시지의 복사본을 검색하려고 시도합니다. 예를 들어 MS Outlook for Mac에서는 메시지의 소스를 볼 수 있지만 Windows 버전에서는 헤더만 볼 수 있습니다.

요약

이 문서의 목적은 URL 재작성과 관련하여 사용 가능한 컨피그레이션 옵션을 더 잘 이해하는 데 있습니다. 최신 메시지는 MIME 표준이 적용된 대부분의 이메일 소프트웨어에서 구축됩니다. 즉, 동일한 메시지 복사본을 이메일 클라이언트 기능 또는/및 활성화된 모드(텍스트 대 HTML 모드)에 따라 다르게 표시할 수 있습니다. 기본적으로 대부분의 최신 이메일 클라이언트는 HTML을 사용하여 메시지를 표시합니다. HTML 및 URL 재작성의 경우, 기본적으로 이메일 게이트웨이는 A-tag 요소의 href 특성 내에 있는 URL만 재작성합니다. 많은 경우 충분하지 않으며 WEBSECURITYADVANCECONFIG 명령으로 href 및 텍스트 재작성을 모두 활성화하는 것을 고려해야 합니다. 이 명령은 시스템 레벨 명령이며 클러스터 전체에서 일관성을 유지하기 위해 변경 사항을 각 클러스터 멤버에 개별적으로 적용해야 합니다.