セキュアEメールゲートウェイでのURLデファングおよびリダイレクトアクションについて

内容

概要

このドキュメントでは、URLフィルタで使用されるdefangアクションとredirectアクションの違い、およびhref属性とテキストに使用可能なrewriteオプションを使用する方法について説明します。

前提条件

要件

URLレピュテーションに基づいてアクションを実行したり、メッセージフィルタやコンテンツフィルタでアクセプタブルユースポリシーを適用するには、アウトブレイクフィルタ機能をグローバルに有効にする必要があります。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure Email Gateway
- アウトブレイク フィルタ
- コンテンツおよびメッセージフィルタ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

URLフィルタリング機能の1つは、メッセージフィルタやコンテンツフィルタを使用して、URLレピュテーションまたはカテゴリに基づいてアクションを実行することです。URLスキャン結果（URL関連条件）に基づいて、URLに対して使用可能な3つのアクションのうちの1つを適用できます。

- URLの最適化
- Ciscoセキュリティプロキシにリダイレクトする
- URLをテキストメッセージに置き換える

このドキュメントでは、Defang URLオプションと Redirect URLオプションの動作について説明します。また、アウトブレイクフィルタの非ウイルス脅威検出のURL書き換え機能について簡単に説明します。

メッセージサンプル

すべてのテストで使用されるサンプルメッセージは、メッセージのMIME multipart/alternativeタイプであり、text/plainとtext/htmlの両方の部分が含まれます。これらの部分は通常、電子メールソフトウェアによって自動的に生成され、HTMLおよび非HTMLの受信者用にフォーマットされた同じ種類のコンテンツが含まれています。このため、text/plainおよびtext/htmlのコンテンツは手動で編集されました。

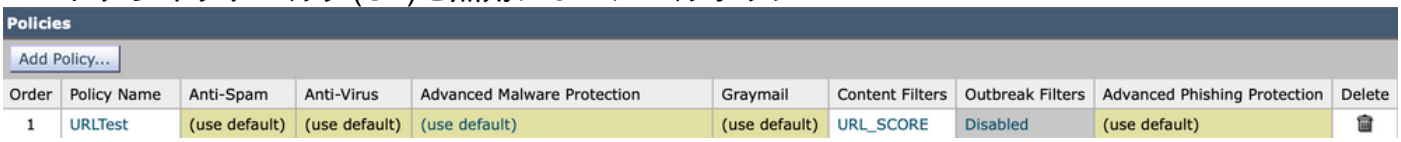
```
Content-Type: multipart/alternative; boundary="===============7781793576330041025==" MIME-
Version: 1.0 From: admin@example.com Date: Mon, 04 Jul 2022 14:38:52 +0200 To: admin@cisco.com
Subject: Test URLs --===============7781793576330041025== Content-Type: text/plain; charset="us-
ascii" MIME-Version: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

パートI – デファン

設定

最初の部分では、設定で次の情報を使用します。

- デフォルトのアンチスパム(AS)/アンチウイルス(AV)/高度なマルウェア防御(AMP)設定とアウトブレイクフィルタ(OF)を無効にしたメールポリシー



- 受信コンテンツフィルタ：URL_SCOREコンテンツフィルタが有効

コンテンツフィルタは、URLレピュテーション条件を使用して、スコアが–6.00 ~ -10.00の悪意のあるURLを照合します。コンテンツフィルタ名が記録され、削除操作が行われます **url-reputation-defang** 取得されます。

Defangアクション

defangアクションとは何かを明確にすることが重要です。ユーザガイドに説明があります。クリックできないようにURLを最適化します。メッセージの受信者は、引き続きURLを表示およびコピーできます。

シナリオA

アウトブレイクフィルタ非ウイルス脅威検出	No
コンテンツフィルタアクション	デファング
websecurityadvancedconfig hrefおよびテキストの書き換えが有効になっています	No

このシナリオでは、デフォルト設定で設定されたdefangアクションの結果について説明します。デフォルト設定では、HTMLタグのみが削除されるとURLが書き換えられます。次のURLを含むHTML段落を見てみましょう。

```
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
```

最初の2つの段落では、URLは適切なHTML Aタグで表されます。<A>要素には、 **href=** タグ自体に囲まれ、リンク先を示す属性。タグ要素内のコンテンツは、リンク先を示すこともできます。これは **text form** URLを含めることができます。最初のLink1は、要素のhref属性とテキスト部分の両方に同じURLリンクを含めます。これらのURLは異なる場合があることに注意してください。2番目のLink2には、href属性の内部にのみ適切なURLが含まれます。最後の段落にはA要素は含まれ

ません。

> **注：**正しいアドレスは、カーソルをリンク上に移動するか、メッセージのソースコードを表示したときに常に表示されます。残念ながら、一部の一般的な電子メールクライアントではソースコードを簡単に見つけることができません。

メッセージがURL_SCOREフィルタに一致すると、悪意のあるURLがデフラグされます。URLロギングが有効で、 **OUTBREAKCONFIG** コマンドを発行すると、mail_logsにスコアとURLが表示されます。

```
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'
```

その結果、メッセージが書き換えられます。

```
--===============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メッセージのtext/html部分に対して実行されたdefangアクションの結果は、A-tagが削除され、タグの内容は変更されずに残ります。最初の2つの段落では、HTMLコードが削除され、要素のテキスト部分が残された場所で、両方のリンクがデフラグされました。最初の段落のURLアドレスは、HTML要素のテキスト部分のURLアドレスです。最初の段落のURLアドレスは、defangアクションを実行した後も表示されますが、HTMLのAタグがなければ、要素をクリックできないことに注意してください。3番目の段落は、URLアドレスがAタグの間に配置されていないためデフラグされず、リンクとはみなされません。おそらく、次の2つの理由から望ましい動作ではありません。まず、ユーザは簡単にリンクを見てコピーし、ブラウザで実行することができます。2つ目の理由は、一部の電子メールソフトウェアがテキスト内の有効な形式のURLを検出し、クリック可能なリンクにする傾向があるためです。

MIMEメッセージのtext/plain部分を見てみましょう。テキスト/プレーン部分には、テキスト形式で2つのURLが含まれています。テキスト/プレーンは、HTMLコードを理解しないMUAによって表示されます。最近のほとんどの電子メールクライアントでは、意図的に電子メールクライアントを設定しない限り、メッセージのテキストやプレーン部分は表示されません。通常は、メッセージのソースコード、つまりメッセージの生のEML形式を確認して、MIME部分を調べる必要があります。

このリストには、送信元メッセージのテキスト/プレーン部分からのURLが表示されます。

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

この2つのリンクの1つが悪意のあるスコアを獲得し、デフラグされました。デフォルトでは、MIMEタイプのtext/plain部分に対して実行されるdefangアクションの結果は、text/html部分とは異なります。ブロックされた単語の間にあり、角カッコの間のすべてのドットです。

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

まとめ：

- TEXT/PLAIN部分に対して実行されたデフラグにより、URLがBLOCKEDブロックに書き換えられます。
- Defang run on the TEXT/HTML部分は、Aタグ間のテキストをタッチせずにAタグが削除されたときに、HTML AタグからURLを書き換えます。これはURLアドレスにすることもできます

シナリオB

アウトブレイクフィルタ非ウイルス脅威検出	No
コンテンツフィルタアクション	デファング
websecurityadvancedconfig hrefおよびテキストの書き換えが有効になっています	Yes

このシナリオでは、いずれかのwebsecurityadvancedconfigオプションを使用した後にdefangsアクションの動作がどのように変化するかについて説明します。websecurityadvancedconfigは、URLスキャン固有の設定を調整できるマシンレベル固有のCLIコマンドです。ここで設定の1つを使用すると、defangアクションのデフォルト動作を変更できます。

```
> 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
...
```

4番目の質問では **– Do you want to rewrite both the URL text and the href in the message? ..**、解答 **Y** メッセージのHTMLベースのMIME部分の場合、A-tag要素のhref属性に見つかったかどうかに関係なく、一致するすべてのURL文字列がテキスト部分であるか、書き換えられる要素の外側であることを示します。このシナリオでは、同じメッセージが再送信されますが、結果はわずかに異なります。

text/htmlのMIMEパートのコードとURLをもう一度確認し、Eメールゲートウェイで処理されるHTMLコードと比較します。

```
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およびテキスト書き換えオプションが有効な場合、URLアドレスがhref属性の一部であるか、A-tag HTML要素のテキストの一部であるか、またはHTMLドキュメントの別の部分で見つかるかにかかわらず、フィルタURLに一致するものがすべてデフラグされます。

```
--===============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要素がURL形式に一致する場合、リンクのテキスト部分の書き換えと共に取り除かれると、デフラグされたURLが書き換えられます。書き換えられたテキスト部分は、MIMEメッセージのtext/plain部分と同じように行われます。項目はBLOCKED語の間に配置され、すべてのドットは角カッコの間に配置されます。これにより、ユーザはURLをコピーして貼り付けることがなくなり、一部の電子メールソフトウェアクライアントではテキストをクリック可能になります。

まとめ：

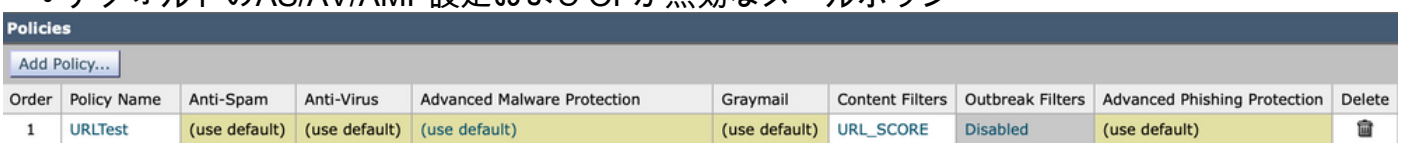
- TEXT/PLAIN部分に対して実行されたデフラグにより、URLがBLOCKEDブロックに書き換えられます。
- Defang run on the TEXT/HTML part rewrites the URL from an HTML A-tag when an A-tag is stripped
- TEXT/HTML部分に対して実行されたデフラグは、BLOCKEDブロックに一致するすべてのURL文字列を書き換えます

パートII：リダイレクト

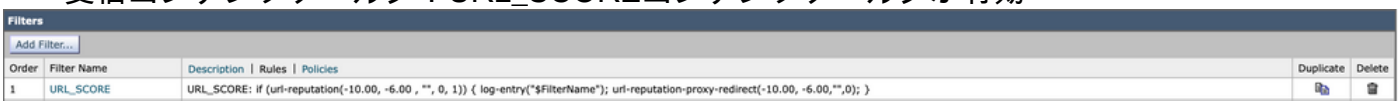
設定

2番目の部分では、設定で次の情報を使用します。

- デフォルトのAS/AV/AMP設定およびOFが無効なメールポリシー



- 受信コンテンツフィルタ：URL_SCOREコンテンツフィルタが有効



コンテンツフィルタは、URLレピュテーション条件を使用して、スコアが–6.00 ~ -10.00の悪意のあるURLを照合します。コンテンツフィルタ名が記録され、 **redirect action** 取得されます。

リダイレクトアクション

「Cisco Security Proxyサービスによるクリック時評価にリダイレクトする」を選択すると、メッセージ受信者はリンクをクリックしてクラウド内のCisco Webセキュリティプロキシにリダイレクトされ、サイトが悪意のあるサイトとして識別された場合はアクセスがブロックされます。

シナリオC

アウトブレイクフィルタ非ウイルス脅威検出	No
コンテンツフィルタアクション	リダイレクト（Redirect）
websecurityadvancedconfig hrefおよびテキストの書き換えが有効になっています	No

このシナリオは、最初の部分のシナリオAと動作が非常によく似ていますが、URLをデフラグする代わりにリダイレクトするコンテンツフィルタアクションで違いがあります。
websecurityadvancedconfig設定がデフォルト設定に復元されます。つまり、 **"Do you want to rewrite both the URL text and the href in the message? ..** に設定されている **N.**

電子メールゲートウェイは、各URLを検出して評価します。悪意のあるスコアはURL_SCOREコンテンツフィルタルールをトリガーし、アクションを実行します **url-reputation-proxy-redirect-action**

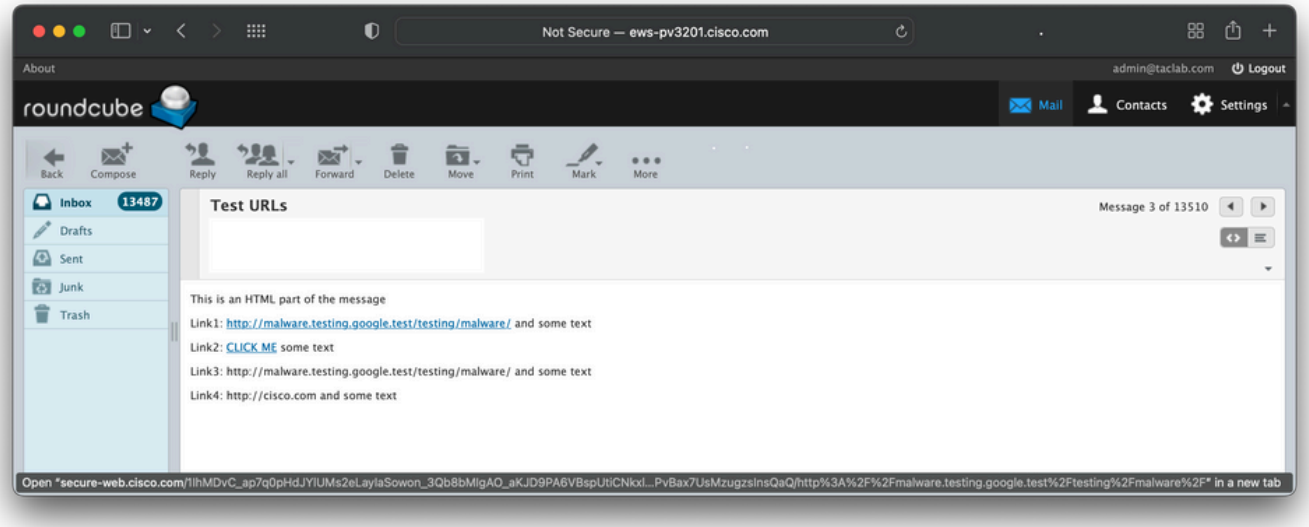
```
Tue Jul 5 12:42:19 2022 Info: MID 139508 URL http://malware.testing.google.test/testing/malware/
has reputation -9.4 matched Condition: URL Reputation Rule Tue Jul 5 12:42:19 2022 Info: MID
139508 Custom Log Entry: URL_SCORE Tue Jul 5 12:42:19 2022 Info: MID 139508 URL
http://malware.testing.google.test/testing/malware/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

メッセージのHTML部分でURLがどのように書き換えられるのかを見てみましょう。シナリオAと同様に、A-tag要素のhref属性で見つかったURLのみが書き換えられ、A-tag要素のテキスト部分で見つかったURLアドレスはスキップされます。defangアクションではA-tag要素全体が削除されますが、redirectアクションではhref属性のURLが書き換えられます。

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

その結果、電子メールクライアントには次の2つのアクティブリンクが表示されます。Link1と

Link2は両方ともCisco Web Security Proxyサービスを指していますが、電子メールクライアントに表示されるメッセージには、デフォルトでは書き換えられないAタグのテキスト部分が表示されます。この問題を解決するには、メッセージのtext/html部分を表示するWebメールクライアントからの出力を調べてください。



MIMEパートのtext/plain部分では、スコアに一致するすべてのURL文字列が書き換えられるので、リダイレクトが理解しやすいように見えます。

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

まとめ：

- TEXT/PLAIN部分に対するリダイレクト実行は、Cisco Web Secureプロキシサービスと一致するURL文字列を書き換えます
- TEXT/HTML部分に対するリダイレクトの実行では、HTML A-tag href属性のURLがCisco Web Secureプロキシサービスに書き換えられますが、一致する他のすべてのURL文字列は変更されずに残ります

シナリオD

アウトブレイクフィルタ非ウイルス脅威検出	No
コンテンツフィルタアクション	リダイレクト（Redirect）
websecurityadvancedconfig hrefおよびテキストの書き換えが有効になっています	Yes

このシナリオは、第1部のシナリオBに似ています。メッセージのHTML部分に一致するすべてのURL文字列を書き換えるには、有効にします。これは、websecurityadvancedconfigコマンドを使用して、 **"Do you want to rewrite both the URL text and the href in the message? ..** 質問.

--===============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

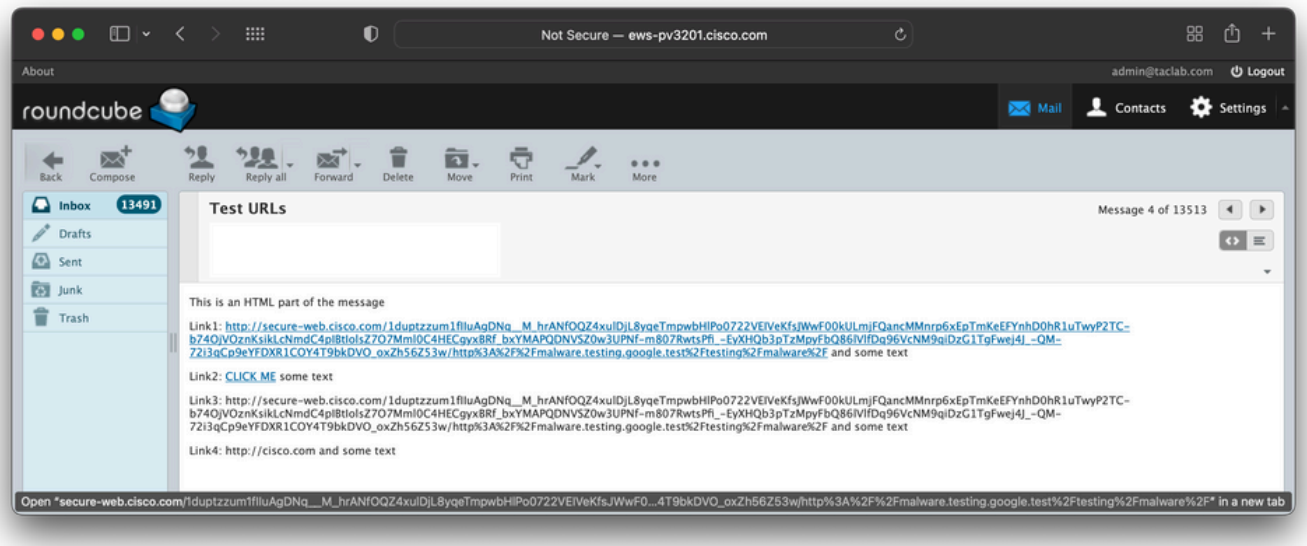
Link2: CLICK ME some text

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とテキストの書き換えが有効になると、コンテンツフィルタ条件に一致するすべてのURL文字列がリダイレクトされます。電子メールクライアントのメッセージに、すべてのリダイレクトが表示されます。これをより理解するには、メッセージのtext/html部分を表示するWebメールクライアントの出力を調べます。



MIMEメッセージのテキスト/プレーン部分は、シナリオCと同じです。これは、websecurityadvancedconfigの変更がメッセージのテキスト/プレーン部分に影響を与えないためです。

--===============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%2Fmalwa
re%2F and some text Link2: http://cisco.com and some text --===============7781793576330041025==
```

まとめ：

- TEXT/PLAIN部分に対するリダイレクト実行は、Cisco Web Secureプロキシサービスと一致するURL文字列を書き換えます
- TEXT/HTML部分に対するリダイレクト実行は、HTML A-tag href属性からのURLをテキスト部分と共に書き換えるほか、Cisco Web SecureプロキシサービスとHTML本文で一致するその他のURL文字列を書き換えます

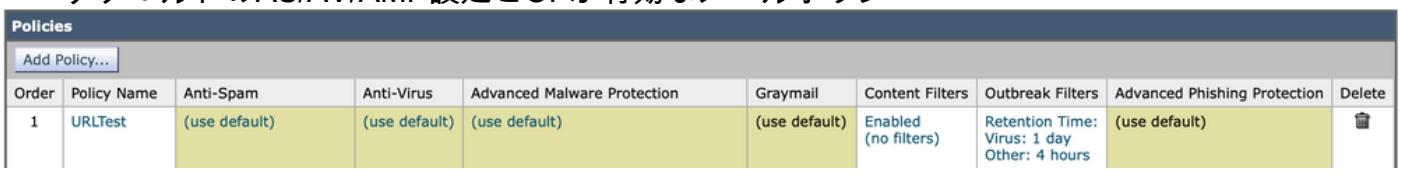
パート3：リダイレクトの

このパートでは、非ウイルス脅威検出のOF設定がURLスキャンにどのように影響するかについて説明します。

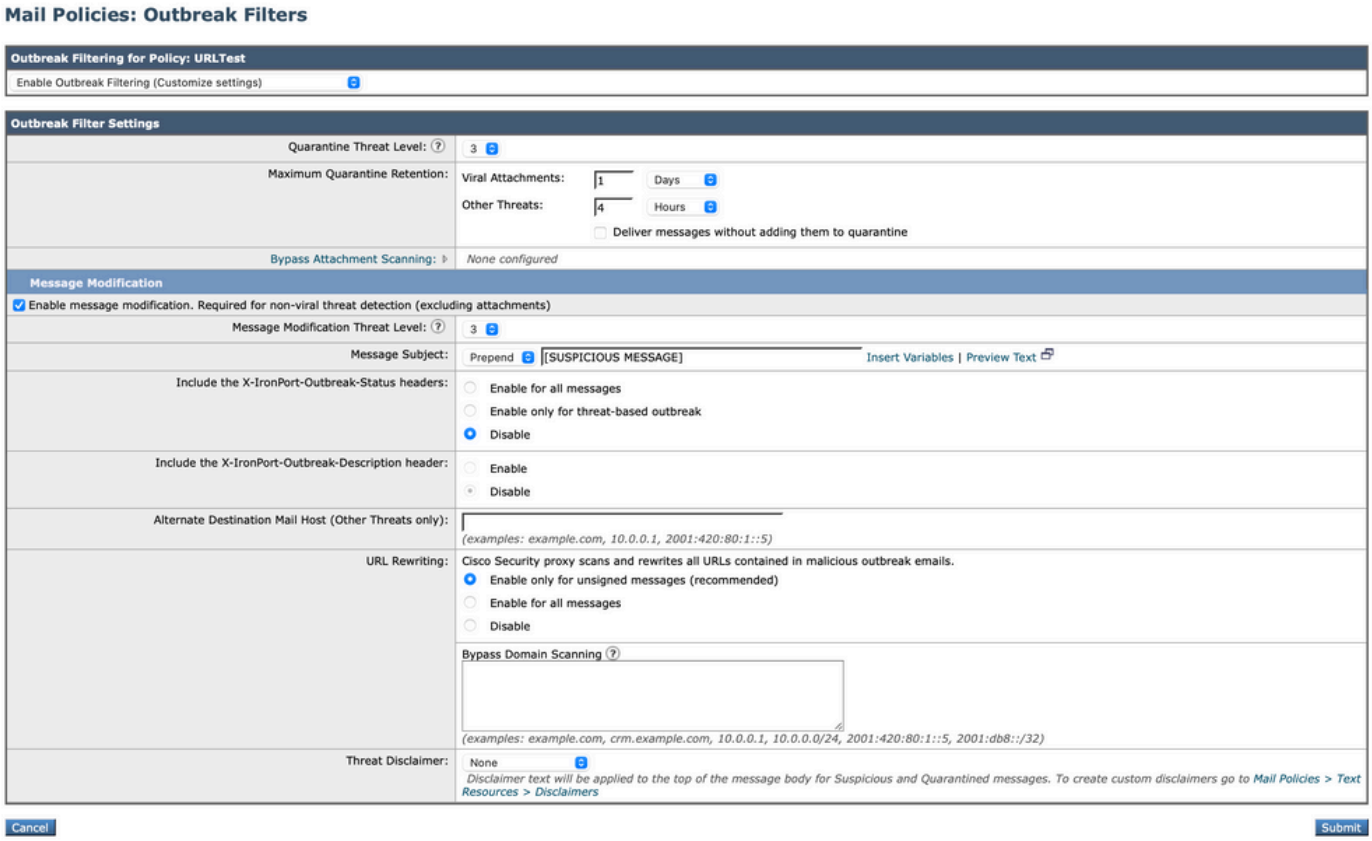
コンフィギュレーション

この目的のために、最初の2つの部分で使用されるコンテンツフィルタが無効になります。

- デフォルトのAS/AV/AMP設定とOFが有効なメールポリシー



- ウイルス以外の脅威の検出をスキャンするアウトブレイクフィルタは、悪意のある電子メールに含まれるすべてのURLを書き換えるようにURL書き換えセットで設定されます



メッセージがOFによってMaliciousとして分類されると、内部のすべてのURLがCisco Web Secureプロキシサービスで書き換えられます。

シナリオE

アウトブレイクフィルタ非ウイルス脅威検出	Yes
コンテンツフィルタアクション	No
websecurityadvancedconfig hrefおよびテキストの書き換えが有効になっています	No

このシナリオでは、メッセージの書き換えが、OFが有効でwebsecurityadvancedconfig hrefとテキストの書き換えが無効な場合にのみ機能する方法を示します。

```
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)
```

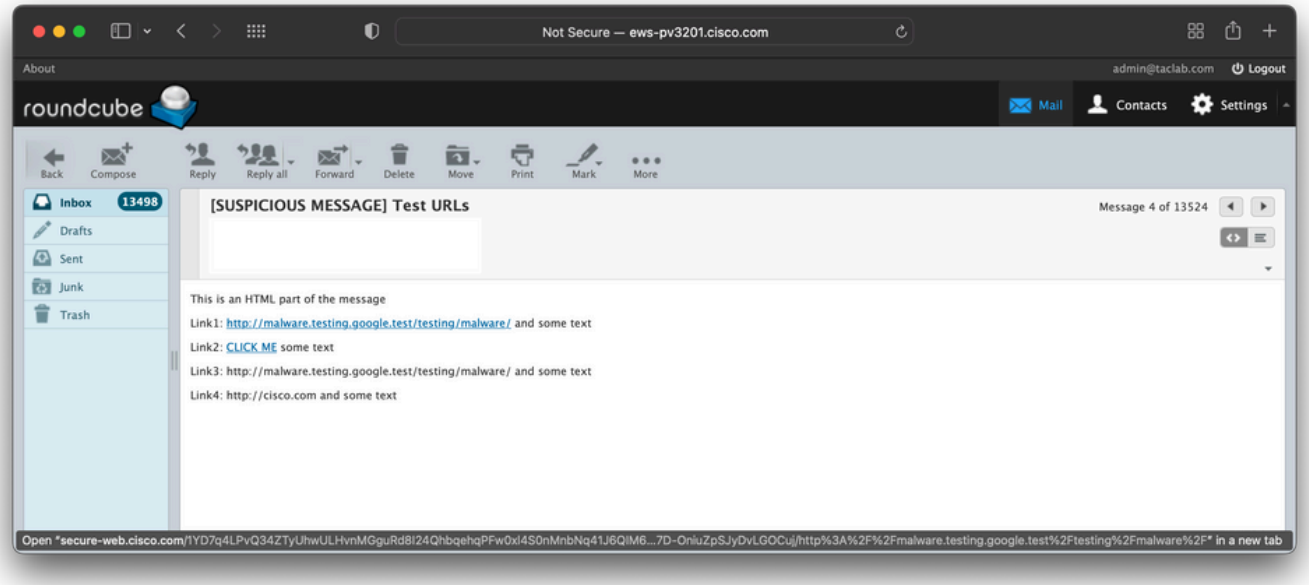
text/plain MIMEの部分から始めましょう。クイックチェックの後、テキスト/プレーン部分の内部にあるすべてのURLがCisco Web Secureプロキシサービスに書き換えられていることがわかります。これは、Outbreak悪意のあるメッセージ内のすべてのURLに対してURL書き換えが有効になっているためです。

```
--================778179357633004102 5== 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 --================778179357633004102 5==
```

これは、MIMEメッセージの処理されたtext/html部分です。

```
--================778179357633004102 5== 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==--



ここで最初に注意すべきことは、Link4が書き換えられない理由です。記事を注意深く読めば、既に答えを知っている。デフォルトでは、MIMEのtext/html部分はA-tag要素のhref属性のみを評価して操作します。テキスト/プレーンパーツと同様の動作が必要な場合は、websecurityadvancedconfig hrefとテキストの書き換えを有効にする必要があります。次のシナリオでは、まさにこれをします。まとめ：

- TEXT/PLAIN部分で実行されるOFリダイレクトは、Cisco Web Secureプロキシサービスと一致するすべてのURL文字列を書き換えます
- TEXT/HTMLパーツに対して実行されるOFリダイレクトは、Cisco Web Secureプロキシサービスを使用して、HTML A-tag href属性からのURLのみを書き換えます

シナリオF

アウトブレイクフィルタ非ウイルス脅威検出	Yes
コンテンツフィルタアクション	No
websecurityadvancedconfig hrefおよびテキストの書き換えが有効になっています	Yes

このシナリオでは、websecurityadvancedconfig hrefとテキストの書き換えを有効にして、OF非ウイルス脅威検出によって提供されるURL書き換えの動作がどのように変化するかを示します。現時点では、websecurityadvancedconfigがtext/plain MIME部分に影響を与えないことを理解する必要があります。text/html部分だけを評価して、動作がどのように変化したかを見てみましょう。

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

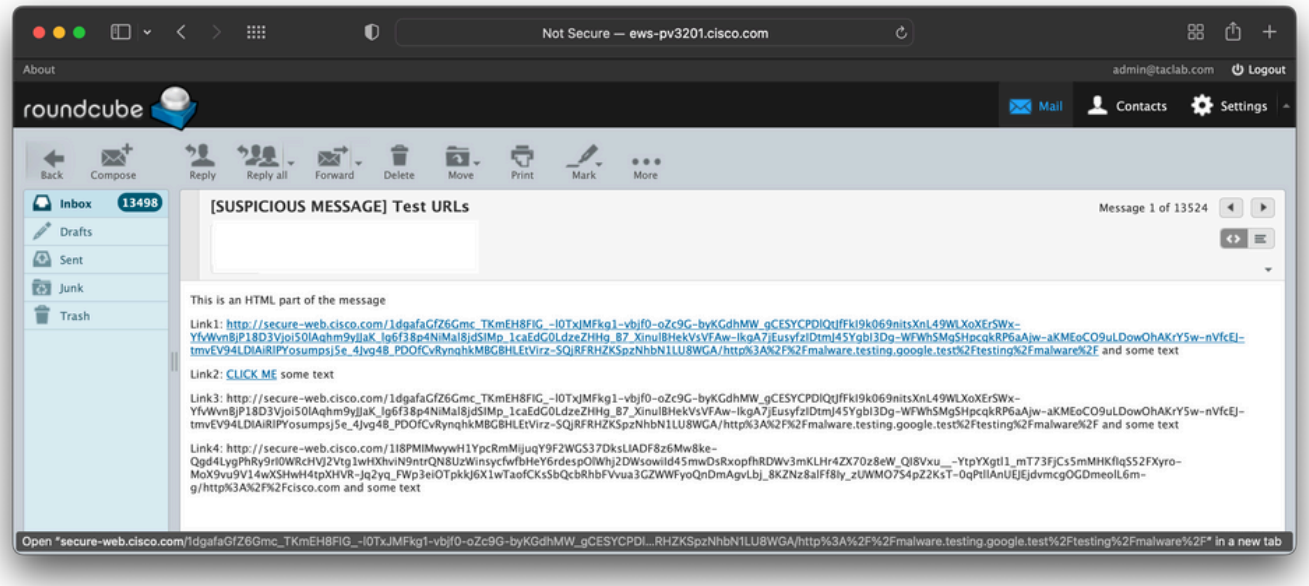
Link2: CLICK ME some text

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==--

出力はシナリオDの出力と非常によく似ており、悪意のあるURLだけでなく、すべてのURLが書き換えられたという唯一の違いがあることに注意してください。HTML部分で一致するURL文字列が、悪意のない文字列と共に修正されます。



まとめ：

- TEXT/PLAIN部分で実行されるOFリダイレクトは、Cisco Web Secureプロキシサービスと一致するすべてのURL文字列を書き換えます
- TEXT/HTML部分で実行されるOFリダイレクトは、HTML A-tag href属性からのURLを、要素のテキスト部分およびCisco Web Secureプロキシサービスと一致するその他すべてのURL文字列とともに書き換えます

シナリオG

アウトブレイクフィルタ非ウイルス脅威検出	Yes
コンテンツフィルタアクション	デファング
websecurityadvancedconfig hrefおよびテキストの書き換えが有効になっています	Yes

この最後のシナリオでは、設定を検証します。

- デフォルトのAS/AV/AMP設定とOFが有効なメールポリシー

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)	

- ウイルス以外の脅威を検出するためのOFスキャンは、悪意のある電子メールに含まれるすべてのURLを書き換えるようにURL書き換え設定で設定されます（以前のシナリオと同じ）
- 受信コンテンツフィルタ：URL_SCOREコンテンツフィルタが有効

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); }		

コンテンツフィルタは、URLレピュテーション条件を使用して、スコアが–6.00 ~ -10.00の悪意のあるURLを照合します。コンテンツフィルタ名が記録され、削除操作が行われます **url-reputation-defang** 取得されます。

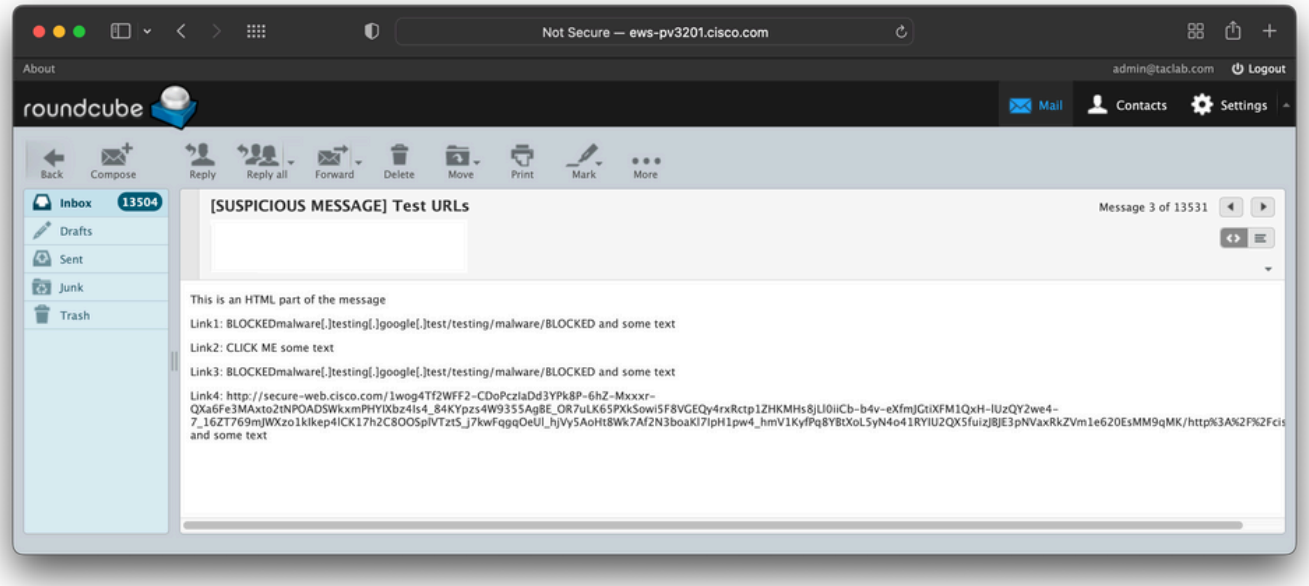
同じメッセージのコピーが送信され、結果とともに電子メールゲートウェイによって評価されます。

```
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
```

電子メールパイプラインでは、最初にコンテンツフィルタによってメッセージが評価され、そこでURL_SCOREフィルタがトリガーされ、URL-reputation-defang-actionが適用されることを説明します。このアクションは、text/plainとtext/htmlの両方のMIME部分のすべての悪意のあるURLをデフラグします。websecurityadvanceconfig hrefとテキストの書き換えが有効であるため、すべてのAタグ要素が削除され、URLのテキスト部分がBLOCKEDワードの間に書き換えられ、すべてのドットが角かっこの間に配置されると、HTML本体内で一致するすべてのURL文字列がデフラグされます。A-tag HTML要素に配置されていない他の悪意のあるURLでも同じことが起こります。 次に、アウトブレイクフィルタがメッセージを処理します。OFは悪意のあるURLを検出し、メッセージを悪意のあるものとして特定します（脅威レベル=5）。 その結果、メッセージ内で見つかったすべての悪意のあるURLと悪意のないURLが書き換えられます。コンテンツフィルタアクションによってこれらのURLがすでに変更されているため、OFは悪意のない残りのURLだけを書き換えます。これは、意図的にURLを書き換えるように設定されているためです。デフラグされた悪意のあるURLの一部およびリダイレクトされた悪意のないURLの一部として電子メールク

ライアントに表示されるメッセージ。

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



同じことがMIMEメッセージのtext/plain部分にも適用されます。悪意のないURLはすべてCisco Web Secureプロキシにリダイレクトされ、悪意のあるURLはデフラグされます。

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

まとめ：

- TEXT/PLAIN部分で実行されるCFデフラグは、URLをBLOCKEDブロックに書き換えます
- TEXT/HTML部分に対して実行されるCFデフラグは、Aタグが削除されたときにHTML AタグからURLを書き換えます

- TEXT/HTML部分で実行されるCFデフラグは、BLOCKEDブロックに一致するすべてのURL文字列を書き換えます
- TEXT/PLAIN部分に対して実行されるOFリダイレクトは、Cisco Web Secureプロキシサービス（悪意のない）と一致するすべてのURL文字列を書き換えます。
- TEXT/HTML部分に対して実行されるOFリダイレクトは、HTML A-tag href属性からのURLを、要素のテキスト部分およびCisco Web Secureプロキシサービスと一致するその他すべてのURL文字列（悪意のない文字列）とともに書き換えます

トラブルシュート

URL書き換えの問題を調査する必要がある場合は、次の点に従ってください。

- mail_logsでURLロギングを有効にします。RUN **OUTBREAKCONFIG** コマンドアンドアンサー **Y** から **Do you wish to enable logging of URL's?** [N]>"
- 確認 **WEBSECURITYADVANCECONFIG** 各eメールゲートウェイクラスタメンバーの設定を確認し、各マシンでhrefとtext rewriteオプションが適切に設定され、同じになっていることを確認します。このコマンドはマシンレベルで固有であり、ここでの変更はグループやクラスタの設定には影響しません。
- コンテンツフィルタの条件とアクティビティを確認し、コンテンツフィルタが有効になっていて、正しい受信メールポリシーに適用されていることを確認します。他のフィルタを処理するためにスキップできる最終的なアクションを使用して、以前に処理された他のコンテンツフィルタがないかどうかを確認します。
- 送信元の生のコピーと最終メッセージを調べます。メッセージをEML形式で取得することを忘れないでください。MSGのような独自の形式は、メッセージの調査に関しては信頼できません。一部の電子メールクライアントでは、送信元メッセージを表示し、別の電子メールクライアントでメッセージのコピーを取得できます。たとえば、MS Outlook for Macではメッセージのソースを表示できますが、Windowsバージョンではヘッダーのみを表示できます。

要約

この記事の目的は、URLの書き換えに関して使用可能な設定オプションを理解しやすくすることです。現代のメッセージは、MIME標準を持つほとんどの電子メールソフトウェアによって構築されていることを覚えておくことが重要です。つまり、同じメッセージのコピーを、電子メールクライアントの機能や有効なモード（テキストとHTMLモード）に応じて異なる方法で表示できます。 デフォルトでは、最近のほとんどの電子メールクライアントはHTMLを使用してメッセージを表示します。HTMLとURLの書き換えでは、デフォルトの電子メールゲートウェイがA-tag要素のhref属性内にあるURLだけを書き換えることに注意してください。多くの場合は十分ではなく、WEBSECURITYADVANCECONFIGコマンドでhrefとtextの両方の書き換えを有効にすることを検討する必要があります。 これはマシンレベルのコマンドであり、クラスタ全体の一貫性を保つために、変更は各クラスタメンバに個別に適用する必要があります。