複数のサービスによってフラグを付けられた場合 ESA/CES 検疫順序

目次

概要

この資料はメールが fo のための複数のサービスによって検疫およびフロー メール パイプラインの他を通したメール フラグを付けられるとき Cisco E メール セキュリティ アプライアンス（ESA）およびクラウド E メール セキュリティ（CES）デバイスの動作を記述したものです。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

この資料に記載されている情報は AsyncOS 12.1.0 バージョンの on Cisco 基づいた ESA です。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

メールは Cisco ESA およびフィルタリングのための CES デバイスをフローするメール作業待ち行列パイプラインに続きます。 パイプラインは静的であり、検疫のためのメールにフラグを付けるために定義される複数のサービスから複数のアクションがあればパイプラインによって順序に従いません; その代り、ESA/CES は自身の順序とそれを検疫します。

> **注:** 設定 される操作とフラグを付けられるメールは（最終措置）即時優先し、作業待ち行列処理を終了します。

検疫のための複数のサービスによってフラグを付けられたときメールに何が起こりますか。

メールは最初にポリシー ウイルス発生（PVO）検疫に優先順位をつけられます。 PVO がメールがまた保持されるその他すべての検疫をリストすると同時にポリシー検疫がそれ入る特定の順序がありません。 メールは PVO 検疫の 1 つからリリースされた後、フラグを付けられるべきあらゆるそれぞれ検疫で保持されます。

メールがリリースされた後（手動でまたはデフォルト アクションがリリースする設定 される タイマーを通して）メールはそしてスパム検疫を入力します。 メールはスパム検疫からリリースされるとき、最終的な配信のために配信への transverses その後並べます。

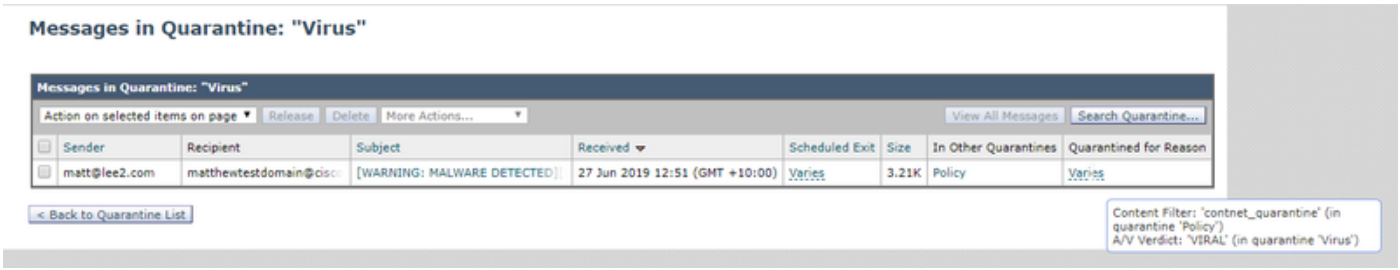
> **注:** 1 つの PVO 検疫を離れて削除されるメールはすべてのそれに続くから、メールを検疫しますそれを同様に保持しました取除きます。

- ポリシーおよびウイルス検疫から発表されるメッセージはアンチウィルスの、高度 malware 保護および graymail エンジンによって再スキャンします。
- 発生検疫から発表されるメッセージは反スパム、アンチウィルスの、および AMP エンジンによって再スキャンします。
- ファイル分析検疫から発表されるメッセージは脅威のために再スキャンします。
- 添付ファイルが付いているメッセージはポリシー、ウイルスおよび発生検疫からのリリースにファイル評判サービスによって再スキャンします。

ESA によってされるフィルタリングの最初のメール インジェクト。 この出力で見ますスパム検疫、ウイルス検疫およびポリシー検疫によってフラグを付けられることを:

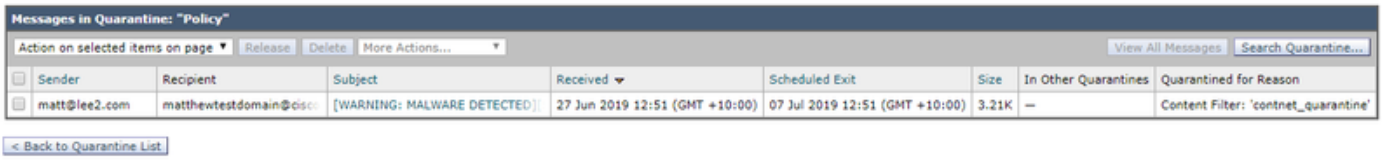
```
Thu Jun 27 12:51:03 2019 Info: Start MID 378951 ICID 391696
Thu Jun 27 12:51:03 2019 Info: MID 378951 ICID 391696 From: <matt@lee2.com>
Thu Jun 27 12:51:10 2019 Info: MID 378951 ICID 391696 RID 0 To: <matthewtestdomain@cisco.com>
Thu Jun 27 12:51:14 2019 Info: MID 378951 Subject 'Test email with AV EICAR and other triggers'
Thu Jun 27 12:51:15 2019 Info: MID 378951 ready 3292 bytes from <matt@lee2.com>
Thu Jun 27 12:51:15 2019 Info: MID 378951 matched all recipients for per-recipient policy matt
in the inbound table
Thu Jun 27 12:51:15 2019 Info: MID 378951 interim verdict using engine: CASE spam positive
Thu Jun 27 12:51:15 2019 Info: MID 378951 using engine: CASE spam positive
Thu Jun 27 12:51:15 2019 Info: ISQ: Tagging MID 378951 for quarantine
Thu Jun 27 12:51:15 2019 Info: MID 378951 interim AV verdict using Sophos VIRAL
Thu Jun 27 12:51:15 2019 Info: MID 378951 antivirus positive 'EICAR-AV-Test'
Thu Jun 27 12:51:15 2019 Info: MID 378951 AMP file reputation verdict : MALWARE
Thu Jun 27 12:51:15 2019 Info: MID 378951 attachment 'testAV.txt'
Thu Jun 27 12:51:15 2019 Info: MID 378951 URL https://ihaveabadreputation.com has reputation -
9.3 matched Condition: URL Reputation Rule
Thu Jun 27 12:51:15 2019 Info: MID 378951 Custom Log Entry:  - Match whole word filter
Thu Jun 27 12:51:15 2019 Info: ISQ: Tagging MID 378951 for quarantine (X-Ironport-Quarantine)
Thu Jun 27 12:51:15 2019 Info: MID 378951 quarantined to "Policy" (content
filter:contnet_quarantine)
Thu Jun 27 12:51:15 2019 Info: MID 378951 quarantined to "Virus" (a/v verdict:VIRAL)
Thu Jun 27 12:51:15 2019 Info: Message finished MID 378951 done
Thu Jun 27 12:51:15 2019 Info: ICID 391696 close
```

あるためにフラグを付ける見られるマークした PVO 検疫で保持される検疫、メール、また他の検疫の中で調査されて。



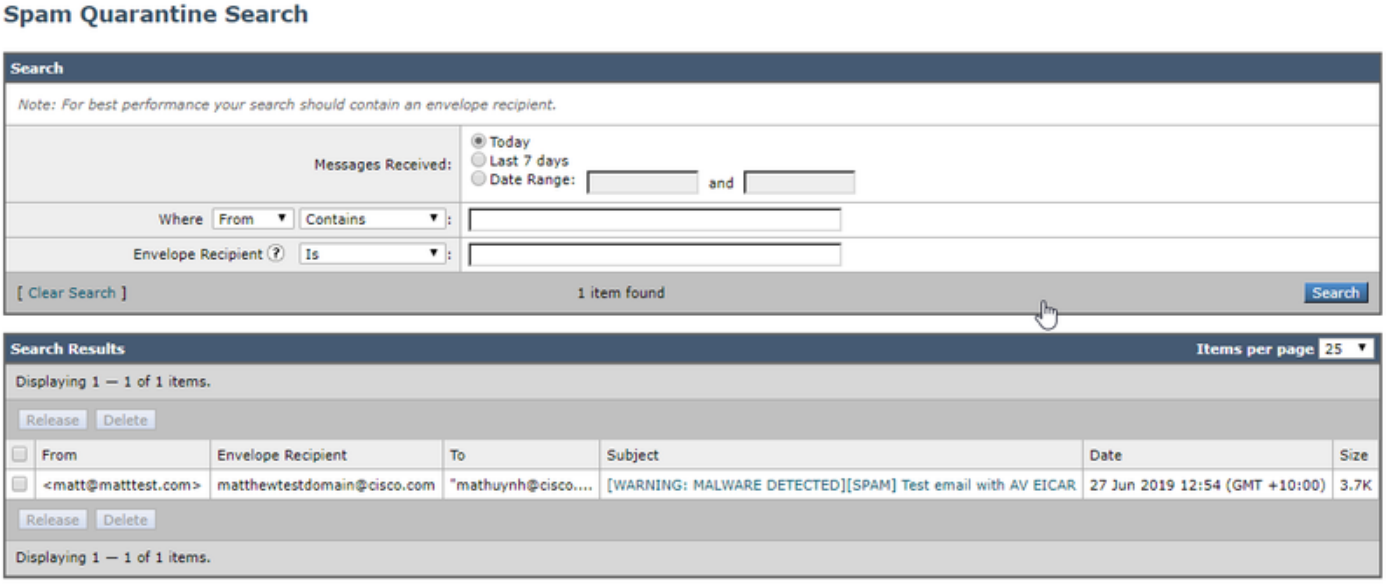
それはこの検疫からリリースした後、他の検疫で利用できなくならないことを mail_logs のこのイベントを記録 し、他の検疫に同様に反映します。

```
Thu Jun 27 12:52:59 2019 Info: MID 378951 released from quarantine "Virus" (manual) t=104
```



メール割り当てにフラグを付けられたスパム検疫にその後移動する残る PVO 検疫からそれをリリースして下さい。

```
Thu Jun 27 12:54:15 2019 Info: MID 378951 released from quarantine "Policy" (manual) t=180
Thu Jun 27 12:54:15 2019 Info: MID 378951 released from all quarantines
Thu Jun 27 12:54:15 2019 Info: MID 378951 matched all recipients for per-recipient policy matt
in the inbound table
Thu Jun 27 12:54:15 2019 Info: MID 378951 interim AV verdict using Sophos VIRAL
Thu Jun 27 12:54:15 2019 Info: MID 378951 antivirus positive 'EICAR-AV-Test'
Thu Jun 27 12:54:15 2019 Info: MID 378951 AMP file reputation verdict : MALWARE
Thu Jun 27 12:54:15 2019 Info: ISQ: Tagging MID 378951 for quarantine (X-Ironport-Quarantine)
Thu Jun 27 12:54:15 2019 Info: MID 378951 queued for delivery
Thu Jun 27 12:54:15 2019 Info: RPC Delivery start RCID 13914 MID 378951 to local IronPort Spam
Quarantine
Thu Jun 27 12:54:15 2019 Info: ISQ: Quarantined MID 378951
Thu Jun 27 12:54:15 2019 Info: RPC Message done RCID 13914 MID 378951
Thu Jun 27 12:54:15 2019 Info: Message finished MID 378951 done
```



そこにスパム検疫の最終リリースで、メールは配信キューに向かいます。

```
Thu Jun 27 12:55:33 2019 Info: Start MID 378952 ICID 0 (ISQ Released Message)
Thu Jun 27 12:55:33 2019 Info: ISQ: Reinjected MID 378951 as MID 378952
Thu Jun 27 12:55:33 2019 Info: MID 378952 ICID 0 From: <matt@lee2.com>
Thu Jun 27 12:55:33 2019 Info: MID 378952 ICID 0 RID 0 To: <matthewtestdomain@cisco.com>
Thu Jun 27 12:55:33 2019 Info: MID 378952 Subject '[WARNING: MALWARE DETECTED][SPAM] Test email
with AV EICAR'
Thu Jun 27 12:55:33 2019 Info: MID 378952 ready 9661 bytes from <matt@lee2.com>
Thu Jun 27 12:55:33 2019 Info: MID 378952 queued for delivery
```

関連情報

- Cisco 電子メール セキュリティ アプライアンス - エンド ユーザ ガイド
- テクニカル サポートとドキュメント – Cisco Systems