多個服務標籤時ESA/CES隔離訂單

目錄

簡介

本文檔介紹當多個用於隔離的服務的郵件被標籤時，思科郵件安全裝置(ESA)和雲郵件安全(CES)裝置的行為，以及郵件通過郵件管道其餘部分的流量。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據搭載AsyncOS 12.1.0版的Cisco ESA。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

流經思科ESA和CES裝置以進行過濾的電子郵件遵循電子郵件工作隊列管道。該管道是靜態的，如果定義了多個服務中的多個操作來標籤用於隔離區的電子郵件，則它不會遵循該管道的順序；相反，ESA/CES用自己的訂單隔離它。

> **注意**：標籤為操作設定為（最終操作）的電子郵件將立即優先並退出工作隊列處理。

當多個服務標籤為隔離時，郵件會發生什麼情況？

該電子郵件首先優先進入策略病毒爆發(PVO)隔離區。由於PVO列出電子郵件所在的所有其他隔離區，因此它進入的策略隔離區沒有特定的順序。電子郵件從其中一個PVO隔離區釋放後，會將其儲存在要標籤的任何相應隔離區中。

在釋放電子郵件後（手動或通過將預設操作設定為釋放的計時器），電子郵件然後進入垃圾郵件隔離區。從垃圾郵件隔離區釋放電子郵件時，它會轉入傳輸隊列中，之後進行最終傳輸。

> **附註**：從一個PVO隔離區中刪除的電子郵件也將從它保留的所有後續隔離區中刪除該電子郵件。

- 從策略和病毒隔離區釋放的郵件由防病毒、高級惡意軟體防護和灰色郵件引擎重新掃描。
- 從爆發隔離區釋放的郵件由反垃圾郵件、防病毒和AMP引擎重新掃描。
- 從File Analysis隔離區釋放的郵件會重新掃描威脅。
- 從策略、病毒和爆發隔離區釋放後，檔案信譽服務會重新掃描帶有附件的郵件。

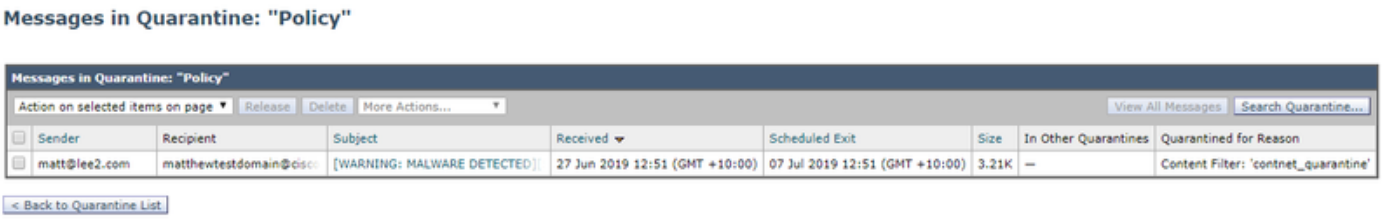
通過ESA完成過濾的初始電子郵件注入。在此輸出中，您會看到垃圾郵件隔離區、病毒隔離區和策略隔離區標籤了它：

```
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
```

在隔離區內調查後，會看到您標籤的PVO隔離區中保留的電子郵件，以及它標籤的任何其他隔離區。

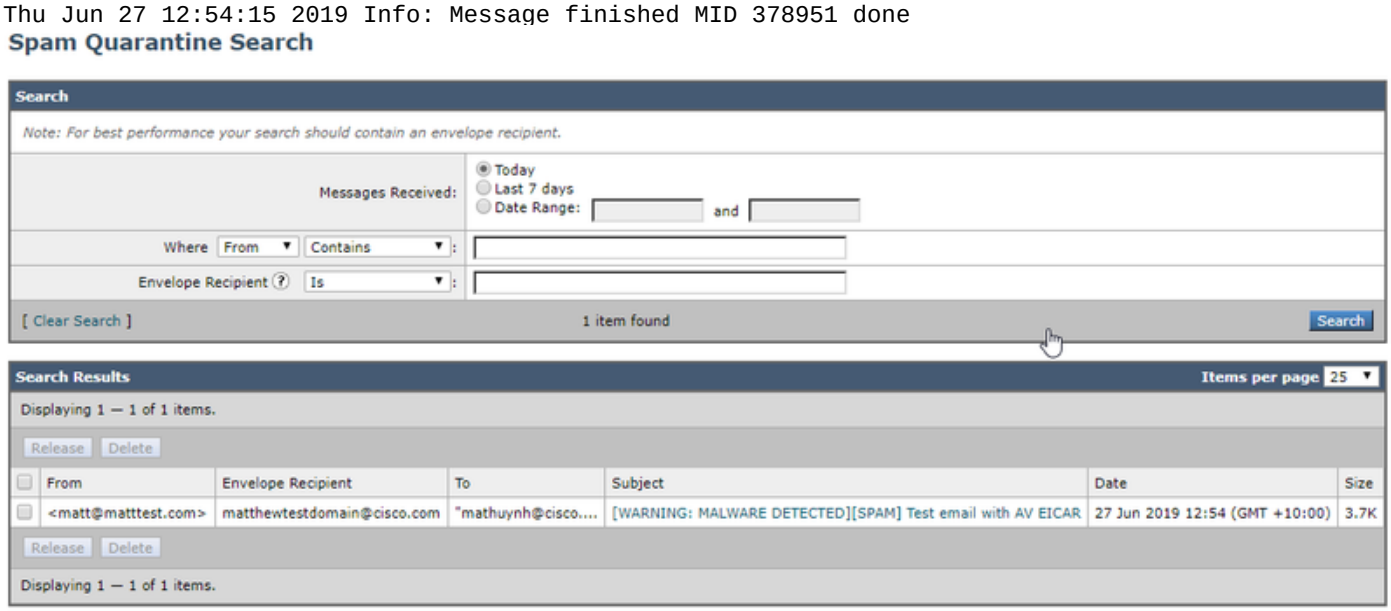
從此隔離區釋放後，它會將此事件記錄到mail_logs中，並在其他隔離區中反映此事件不再可用的情況。

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



將它從PVO隔離區放出，該隔離區將允許電子郵件在之後傳送到已標籤的垃圾郵件隔離區。

```
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
```



在垃圾郵件隔離區的最終版本中，該電子郵件的目的地是傳送隊列。

```
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
```

相關資訊

- Cisco Email Security Appliance — 最終使用手冊
- 技術支援與文件 - Cisco Systems