ESA/CES检疫顺序，当标记由多个服务

目录

简介

本文描述Cisco电子邮件安全工具(ESA)和Cloud电子邮件安全(CES)设备的行为，当电子邮件由检疫和流的fo多个服务标记电子邮件通过电子邮件渠道的其余时。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据与AsyncOS 12.1.0版本的Cisco ESA。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

流经的电子邮件过滤的Cisco ESA和CES设备跟随电子邮件工作队列渠道。渠道是静态的，并且，如果有从定义的多个服务的多样行动标记检疫的一电子邮件，不根据渠道遵从命令;反而，ESA/CES检疫它与其自己的顺序。

> **Note**: 标记与设置的操作的电子邮件(最后的行动)将获得立即优先权并且退出工作队列处理。

什么发生在电子邮件，当标记由检疫的多个服务？

电子邮件优先安排到首先策略病毒爆发(PVO)检疫。没有策略检疫它进入的特定顺序，当PVO列出电子邮件也保持的其他检疫。在电子邮件从其中一PVO检疫当中后发布，在将被标记的所有各自检疫保持。

在电子邮件发布后(手工或通过默认操作设置发布)的计时器电子邮件然后输入垃圾邮件检疫。当电子邮件从垃圾邮件检疫时发布， transverses到交付里为最终交付尔后排队。

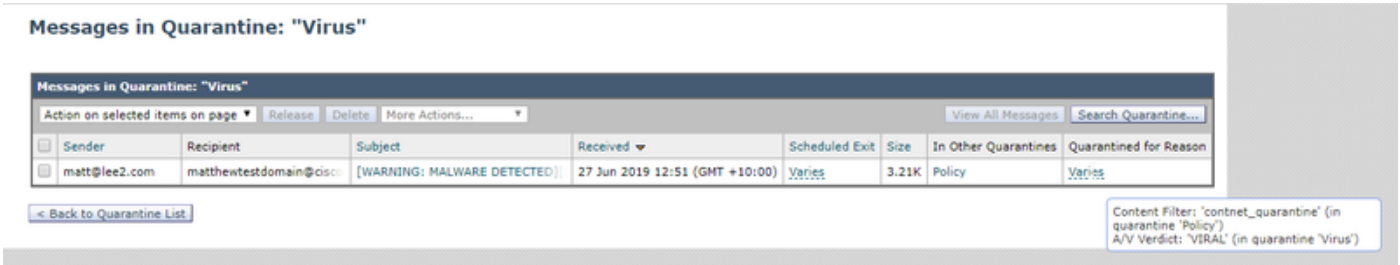
Note:删除一PVO检疫的电子邮件，从所有随后将删除电子邮件检疫它保持。

- 从策略和病毒检疫发布的消息乘抗病毒，先进的恶意软件保护和graymail引擎重新扫描。
- 从爆发检疫发布的消息乘反垃圾邮件，抗病毒和AMP引擎重新扫描。
- 从文件分析检疫发布的消息为威胁被重新扫描。
- 消息用附件由在版本的文件名誉服务重新扫描从策略、病毒和爆发检疫。

与ESA完成的过滤的最初的电子邮件射入。在此输出中您看到由垃圾邮件检疫、病毒检疫和策略检疫标记：

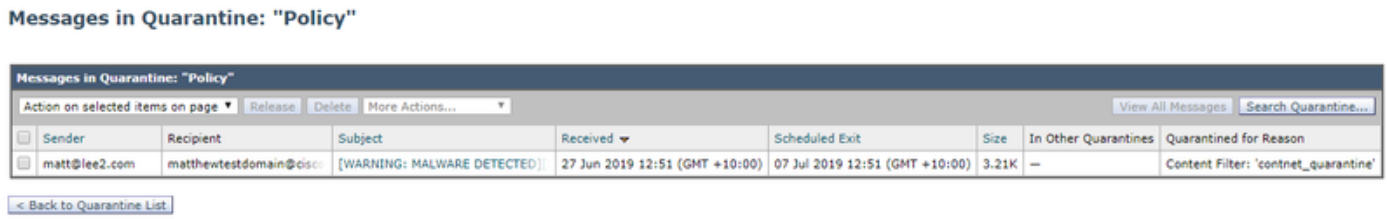
```
Thu Jun 27 12:51:03 2019 Info: Start MID 378951 ICID 391696
Thu Jun 27 12:51:03 2019 Info: MID 378951 ICID 391696 From: <matt@lee2.com>
Thu Jun 27 12:51:10 2019 Info: MID 378951 ICID 391696 RID 0 To: <matthewtestdomain@cisco.com>
Thu Jun 27 12:51:14 2019 Info: MID 378951 Subject 'Test email with 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
```

一旦调查在您标记看到标记的PVO检疫保持的检疫、电子邮件，以及任何其他检疫里面。



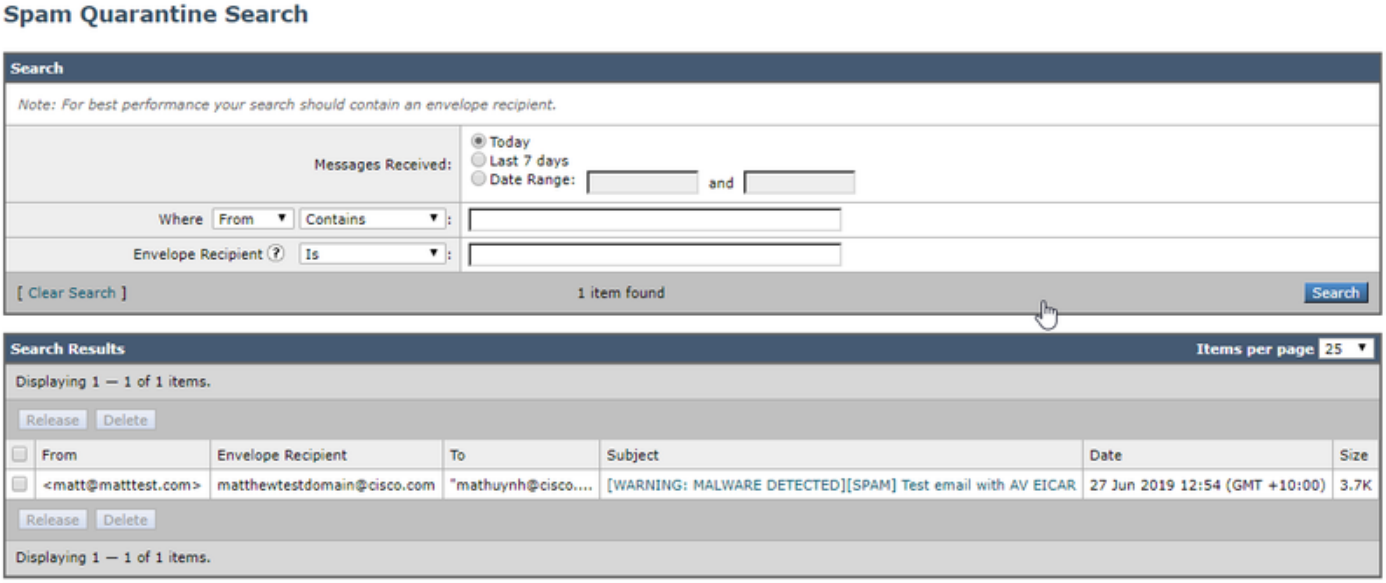
在它从此检疫后发布，在其他检疫记录在您的mail_logs的此事件并且反射不再是可用的在另一检疫。

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



发布它出于依然是允许电子邮件到己标记垃圾邮件检疫尔后移动的PVO检疫。

```
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
```



那里在垃圾邮件检疫的最终版本，电子邮件为交付队列是注定的。

```
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
```

相关信息

- [Cisco电子邮件安全工具-最终用户指南]
- [技术支持和文档 - Cisco Systems]