Ordine di quarantena ESA/CES se contrassegnato da più servizi

Sommario

Introduzione

Questo documento descrive il comportamento dei dispositivi Cisco Email Security Appliance (ESA) e Cloud Email Security (CES) quando un'e-mail è contrassegnata da più servizi per la messa in quarantena e il flusso della e-mail attraverso il resto della pipeline di posta elettronica.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco ESA con versione AsyncOS 12.1.0.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Le e-mail che passano attraverso i dispositivi Cisco ESA e CES per filtrare seguono la pipeline della coda di lavoro della posta elettronica. La pipeline è statica e, se esistono più azioni da più servizi definiti per contrassegnare un messaggio di posta elettronica per le quarantene, non segue l'ordine indicato dalla pipeline. al contrario, l'ESA/CES lo mette in quarantena con un proprio ordine.

> **Nota**: le e-mail contrassegnate con azioni impostate su (Azione finale) avranno la precedenza immediata e usciranno dall'elaborazione della coda di lavoro.

Cosa succede all'e-mail quando contrassegnato da più servizi per la quarantena?

L'e-mail ha la priorità innanzitutto nella quarantena della Policy Virus Outbreak (PVO). Non c'è un ordine specifico in quale politica di quarantena va in come il PVO elenca ogni altra quarantena in cui è tenuto anche l'e-mail. Dopo che l'e-mail è stata rilasciata da una delle quarantene PVO, viene conservata in ogni quarantena rispettiva per essere contrassegnata.

Dopo il rilascio dell'e-mail (manualmente o tramite il timer dove l'azione predefinita è impostata sul rilascio), le e-mail vengono messe in quarantena. Quando l'e-mail viene rilasciata dalla quarantena della posta indesiderata, viene trasferita nella coda di recapito per essere poi recapitata definitivamente.

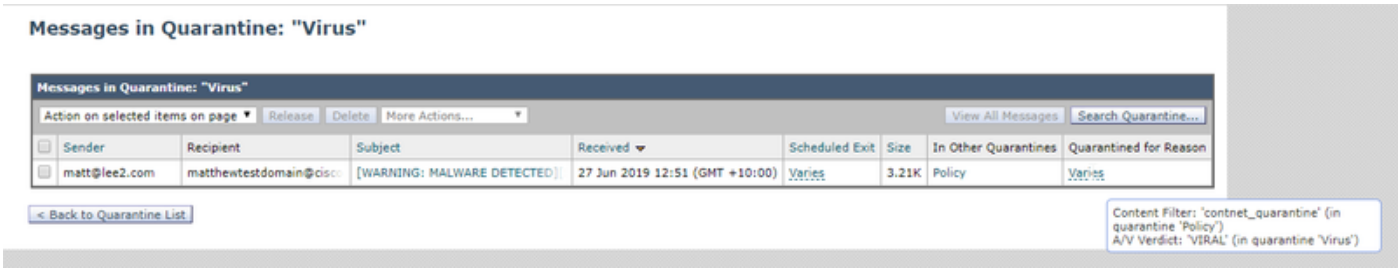
> **Nota:** Un messaggio di posta elettronica eliminato da una quarantena PVO rimuoverà anche il messaggio da tutte le quarantene successive in cui è conservato.

- I messaggi rilasciati dalle quarantene di policy e virus vengono rianalizzati dai motori antivirus, di protezione avanzata dal malware e di posta grigia.
- I messaggi rilasciati dalla quarantena del focolaio vengono nuovamente analizzati dai motori antispam, antivirus e AMP.
- I messaggi rilasciati dalla quarantena di analisi file vengono nuovamente analizzati per rilevare eventuali minacce.
- I messaggi con allegati vengono rianalizzati dal servizio di reputazione dei file al momento del rilascio dalle quarantene per policy, virus ed epidemie.

Iniezione iniziale via email con filtraggio effettuato dall'ESA. In questo output viene segnalato dalla quarantena per posta indesiderata, dalla quarantena per virus e dalla quarantena per criteri:

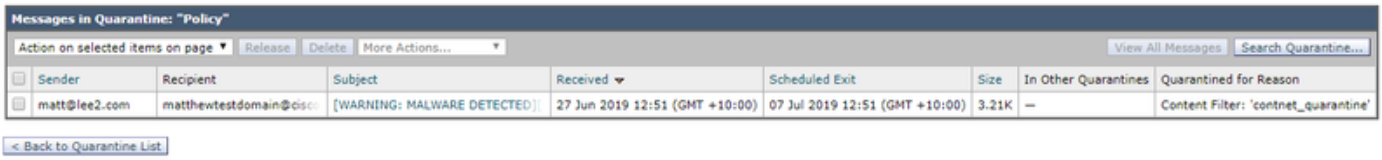
```
Thu Jun 27 12:51:03 2019 Info: Start MID 378951 ICID 391696
Thu Jun 27 12:51:03 2019 Info: MID 378951 ICID 391696 From: <matt@lee2.com>
Thu Jun 27 12:51:10 2019 Info: MID 378951 ICID 391696 RID 0 To: <matthewtestdomain@cisco.com>
Thu Jun 27 12:51:14 2019 Info: MID 378951 Subject 'Test email with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

Una volta analizzato all'interno della quarantena, vengono visualizzate le e-mail conservate nella quarantena PVO contrassegnata e tutte le altre quarantene in cui è contrassegnato.



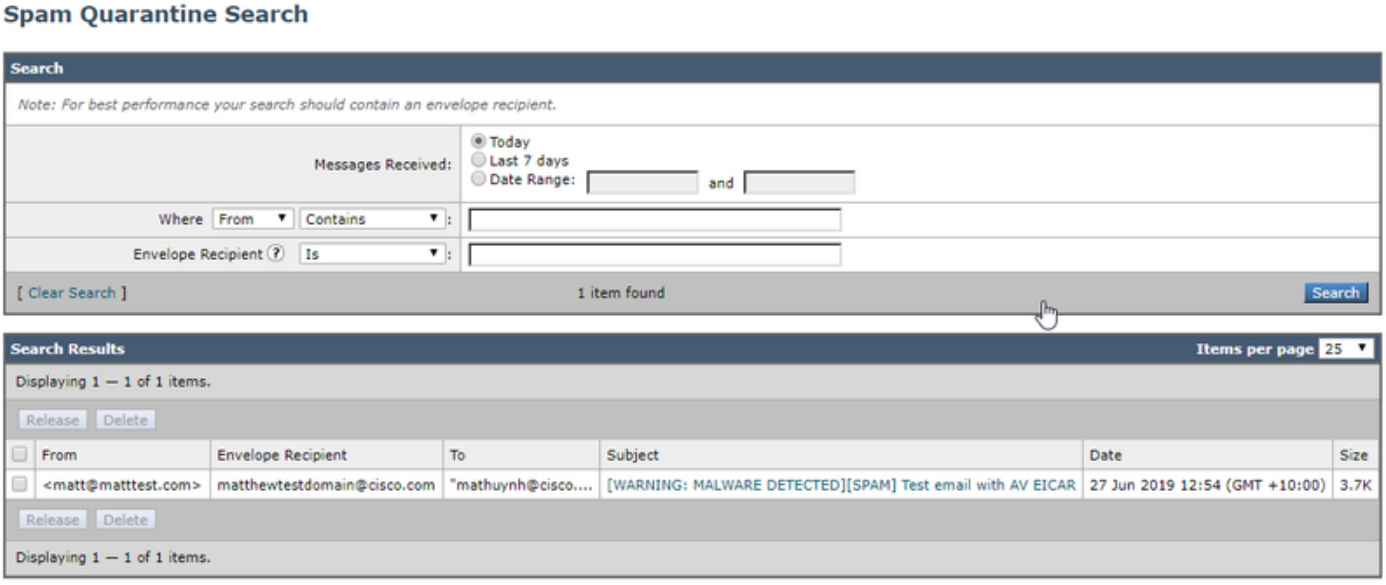
Dopo il rilascio dalla quarantena, l'evento viene registrato nei **log_posta** e si riflette sulle altre quarantene e sul fatto che non è più disponibile nell'altra quarantena.

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



Rilasciarlo dalla quarantena PVO che rimane e consentire ai messaggi di posta elettronica di raggiungere la quarantena di posta indesiderata contrassegnata.

```
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
```



Qui, nella versione finale della quarantena, l'e-mail è destinata alla coda di recapito.

```
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
```

Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Documentazione e supporto tecnico – Cisco Systems