ESA/CES Quarantine Order wanneer getagd door meerdere services

Inhoud

Inleiding

Dit document beschrijft het gedrag van de apparaten van Cisco Email Security (ESA) en Cloud Email Security (CES) wanneer een e-mail wordt gemarkeerd met meerdere services voor quarantaine en de stroom van de e-mail door de rest van de e-mailleiding.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco ESA met AsyncOS 12.1.0 versie.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

E-mails die door de Cisco ESA en CES apparaten voor het filteren stromen volgen de e-mailwerkrijpijplijn. De pijpleiding is statisch en als er meerdere handelingen zijn van meerdere diensten die zijn gedefinieerd om een e-mail te markeren voor de quarantaine, volgt deze niet de volgorde per pijpleiding; In plaats daarvan quaranteert de ESA/CES het in zijn eigen volgorde.

> **Opmerking**: e-mails die worden gemarkeerd met acties die zijn ingesteld op "End Action" (Eindactie) hebben onmiddellijke voorrang en verlaten de werkrijwachtverwerking.

Wat gebeurt er met de e-mail als er meerdere services zijn voor quarantaine?

De e-mail wordt als eerste prioriteerd in de Policy Virus Outbreak (PVO) quarantaine. Er is geen specifieke volgorde voor de quarantaine in het kader van het beleid, aangezien het PVO elke andere quarantaine opsomt waarin de e-mail ook wordt gehouden. Nadat de e-mail is vrijgegeven vanuit één van de PVO-quarantaineines, wordt deze in quarantaine geplaatst, zodat de dieren erop kunnen worden aangegeven.

Nadat de e-mail is vrijgegeven (handmatig of via de timer waar de standaardoptie is ingesteld om hem op te geven) zetten de e-mails vervolgens de spamquarantaine in. Wanneer de e-mail wordt vrijgegeven van de spamquarantaine, wordt deze vervolgens in de leveringswachtrij geplaatst voor de uiteindelijke levering.

> Opmerking: Een e-mail die van één PVO quarantaine is verwijderd, verwijdert de e-mail ook uit alle quarantaine die het in zijn beheer houdt.

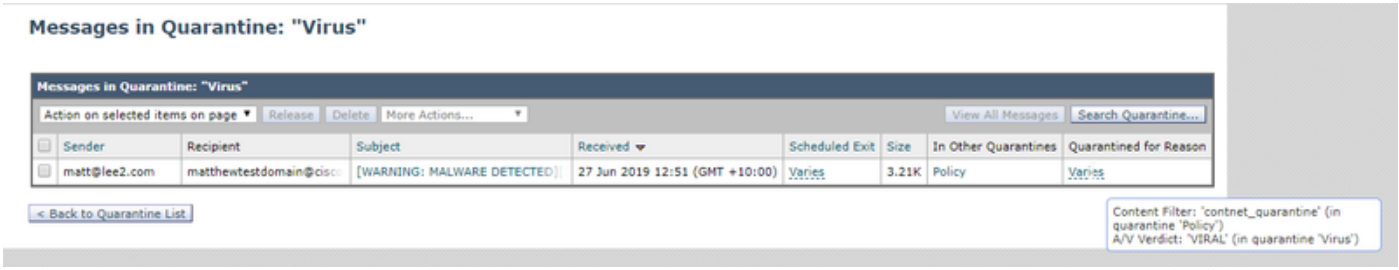
- Berichten die afkomstig zijn van Policy en Virus quarantines worden herroepen door de anti-virus, geavanceerde malware bescherming en grijsmailmotoren.
- Berichten die vrijkomen van de Outbreak quarantaine worden opnieuw gescand door de anti-spam-, anti-virus- en AMP-motoren.
- Berichten die uit de quarantaine van de Bestandsanalyse zijn vrijgegeven, worden opnieuw gescand voor bedreigingen.
- Berichten met bijlagen worden door de dienst bestands reputatie gewist na release van Policy, Virus en Outbreak quarantines.

Eerste e-mailinjectie met filtering uitgevoerd door de ESA. In deze output zie je dat het wordt gemarkeerd door de spamquarantaine, virusquarantaine en beleidsquarantaine:

```
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
```

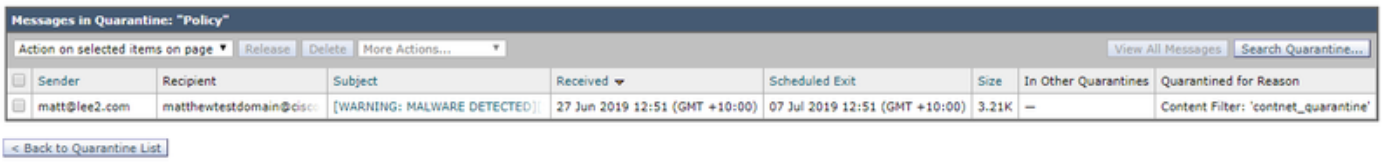
Na onderzoek in de quarantaine worden e-mail die in de door u gemerkte PVO-quarantaine is opgeslagen, en eventuele andere quarantaine-quarantaine's die het aangeeft te zijn ingevoerd,

vertoond.



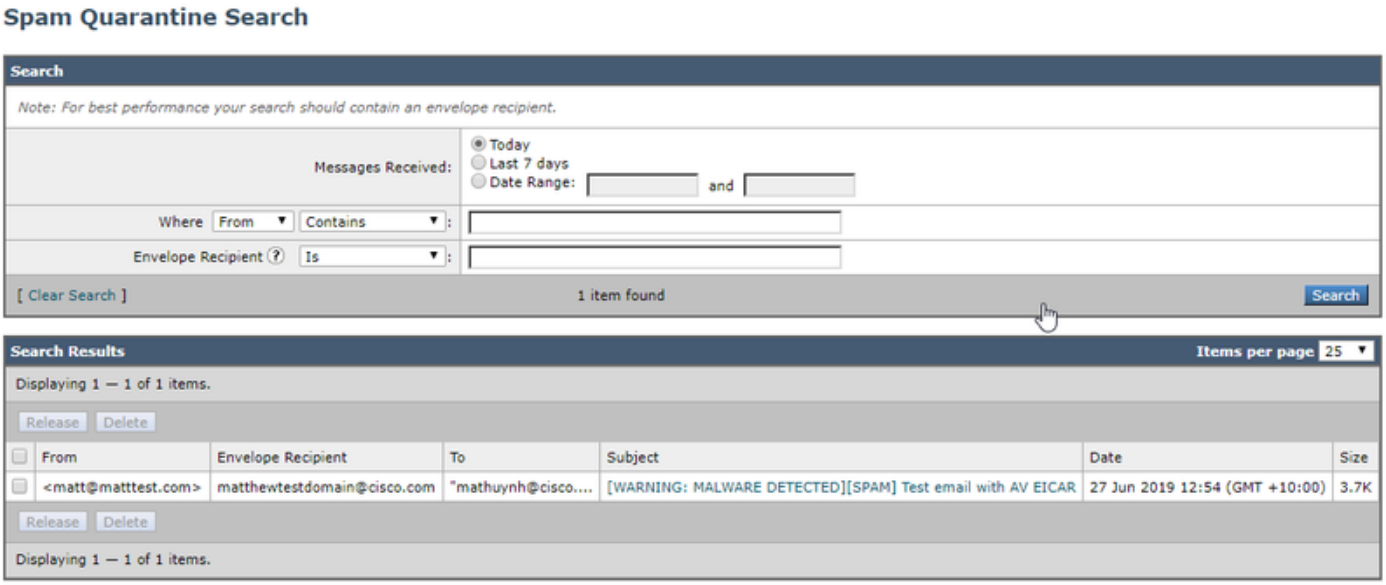
Nadat het uit deze quarantaine is vrijgelaten, registreert het deze gebeurtenis in uw **mail_logs** en reflecteert het op de andere quarantaine evenals dat het niet meer beschikbaar is in de andere quarantaine.

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



Laat het vrij uit de PVO-quarantaine, waardoor de e-mails daarna naar de vlaggengespam-quarantaine kunnen reizen.

```
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
```



Bij de definitieve vrijgave van de spamquarantaine is de e-mail bestemd voor de bezorgingswachtrij.

```
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
```

Gerelateerde informatie

- Cisco e-mail security applicatie - eindgebruikershandleidingen
- Technische ondersteuning en documentatie – Cisco Systems