Bestellung der ESA/CES-Quarantäne bei Markierung durch mehrere Dienste

Inhalt

Einführung

In diesem Dokument wird das Verhalten der Cisco E-Mail Security Appliance (ESA)- und Cloud E-Mail Security (CES)-Geräte beschrieben, wenn eine E-Mail durch mehrere Dienste für die Quarantäne gekennzeichnet wird, und der E-Mail-Fluss durch den Rest der E-Mail-Pipeline.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco ESA-Version mit AsyncOS 12.1.0.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

E-Mails, die zur Filterung über die Cisco ESA- und CES-Geräte gesendet werden, folgen der E-Mail-Warteschlangenpipeline. Die Pipeline ist statisch, und wenn mehrere Aktionen mehrerer Dienste definiert sind, um eine E-Mail-Nachricht für die Quarantäne zu markieren, folgt sie nicht der in der Pipeline angegebenen Reihenfolge. Stattdessen wird sie von der ESA/CES in eigener Reihenfolge unter Quarantäne gestellt.

> **Hinweis**: E-Mails, die mit Aktionen gekennzeichnet sind, die auf "Letzte Aktion" gesetzt sind, haben unmittelbare Priorität und beenden die Verarbeitung der Arbeitswarteschlange.

Was passiert mit der E-Mail, wenn mehrere Dienste für die Quarantäne markiert wurden?

Die E-Mail wird zuerst in die PVO-Quarantäne (Policy Virus Outbreak) priorisiert. Es gibt keine bestimmte Reihenfolge, in der die Richtlinie unter Quarantäne gestellt wird, da das PVO alle anderen Quarantänen auflistet, in denen die E-Mail gespeichert wird. Nachdem die E-Mail aus einer der PVO-Quarantänen freigegeben wurde, befindet sie sich in einer der Quarantänen, in denen die entsprechenden Quarantänen markiert werden sollen.

Nach der Freigabe der E-Mail (manuell oder über den Zeitgeber, in dem die Standardaktion für die Freigabe festgelegt ist) geben Sie die E-Mails in die Spam-Quarantäne ein. Wenn die E-Mail aus der Spam-Quarantäne freigegeben wird, wird sie zur endgültigen Zustellung in die Zustellwarteschlange gestellt.

> **Hinweis**: Eine E-Mail, die von einer PVO-Quarantäne gelöscht wird, entfernt die E-Mail aus allen nachfolgenden Quarantänen, in denen sie ebenfalls gespeichert ist.

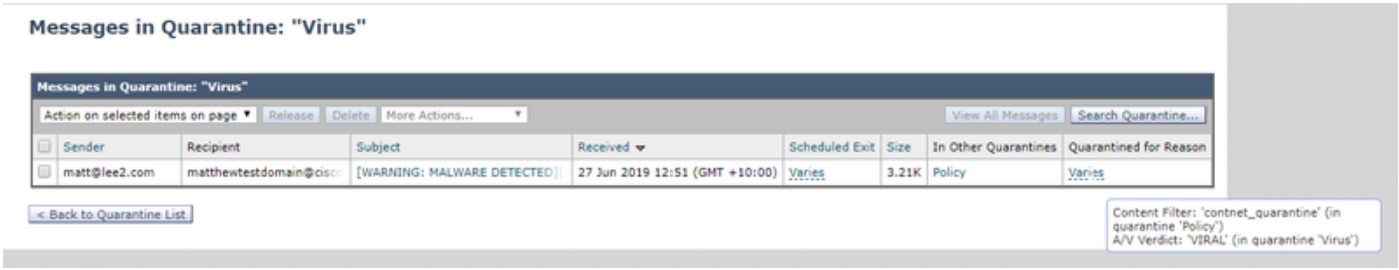
- Nachrichten, die von Richtlinien- und Virenquarantäne freigegeben werden, werden von den Antivirus-, Advanced Malware Protection- und Graustufen-Engines erneut geprüft.
- Von der Outbreak-Quarantäne freigegebene Nachrichten werden von den Anti-Spam-, Anti-Virus- und AMP-Engines erneut geprüft.
- Von der Quarantäne für die Dateianalyse freigegebene Nachrichten werden auf Bedrohungen hin überprüft.
- Nachrichten mit Anhängen werden vom Dateireputations-Service nach Freigabe aus der Quarantäne für Richtlinien, Viren und Outbreaks erneut geprüft.

Erste E-Mail-Injektion mit Filterung durch die ESA durchgeführt. In dieser Ausgabe wird sie durch die Spam-Quarantäne, die Virenquarantäne und die Richtlinienquarantäne gekennzeichnet:

```
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
```

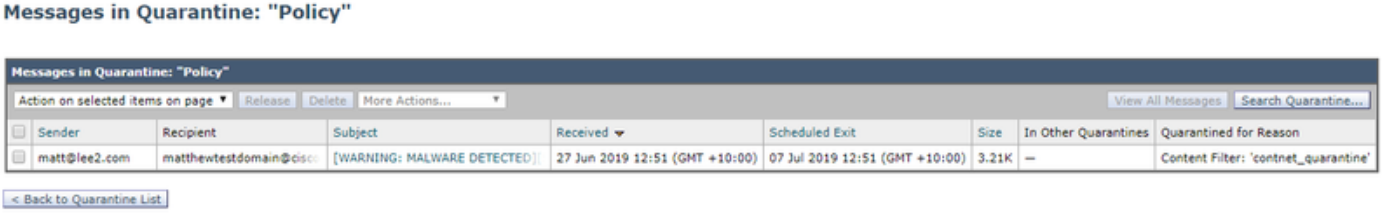
Sobald die E-Mails in der Quarantäne untersucht wurden, werden die E-Mails in der von Ihnen

markierten PVO-Quarantäne sowie alle anderen Quarantänen angezeigt, in denen die Quarantäne markiert werden soll.



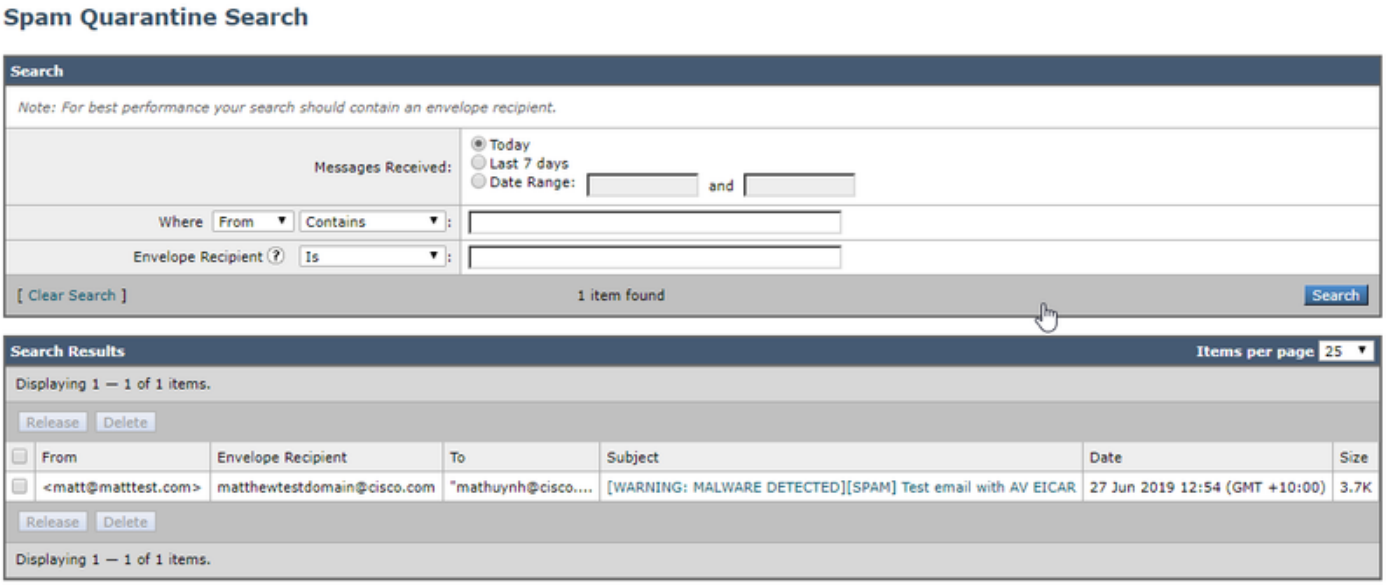
Nachdem es aus dieser Quarantäne freigegeben wurde, protokolliert es dieses Ereignis in Ihren **mail_logs** und reflektiert auch die andere Quarantäne, dass es nicht mehr in der anderen Quarantäne verfügbar ist.

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



Lassen Sie sie aus dem PVO-Quarantänebereich entfernt, sodass die E-Mails anschließend in den markierten Spam-Quarantänebereich verschoben werden können.

```
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
```



In der letzten Version der Spam-Quarantäne ist die E-Mail für die Zustellwarteschlange bestimmt.

```
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
```

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems