여러 서비스에서 플래그 지정된 경우 ESA/CES 격리 순서

목차

소개

이 문서에서는 이메일에 쿼런틴을 위한 여러 서비스에서 플래그가 지정되고 이메일 파이프라인의 나머지 부분을 통해 이메일의 플로우가 전송되는 경우 Cisco ESA(Email Security Appliance) 및 CES(Cloud Email Security) 디바이스의 동작을 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco ESA with AsyncOS 12.1.0 버전을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

필터링용 Cisco ESA 및 CES 디바이스를 통과하는 이메일은 이메일 작업 대기열 파이프라인을 따릅니다.파이프라인은 정적이며, 격리에 대한 이메일에 플래그를 지정하기 위해 여러 서비스에서 여러 작업을 정의한 경우 파이프라인에 따라 순서를 따르지 않습니다.대신 ESA/CES는 자체 주문으로 격리합니다.

> **참고**: (최종 조치)로 설정된 작업으로 플래그가 지정된 이메일은 즉시 우선 순위가 지정되며 작업 대기열 처리를 종료합니다.

Multiple Services for Quarantine으로 플래그가 지정된 이메일은 어떻게 됩니까?

이메일은 먼저 PVO(Policy Virus Outbreak) 격리로 우선 순위가 지정됩니다.PVO는 이메일이 또한 보류된 다른 모든 격리를 나열하므로 어떤 정책 격리가 들어가는지 구체적으로 지시하지 않습니다.이메일이 PVO 쿼런틴 중 하나에서 릴리스되면 해당 격리에서 플래그가 지정되어야 합니다.

이메일이 릴리스된 후(수동으로 또는 기본 작업이 릴리스되도록 설정된 타이머를 통해) 이메일은 스팸 격리를 입력합니다.이메일이 스팸 격리에서 릴리스되면 나중에 최종 전달을 위해 전달 대기열로 전송됩니다.

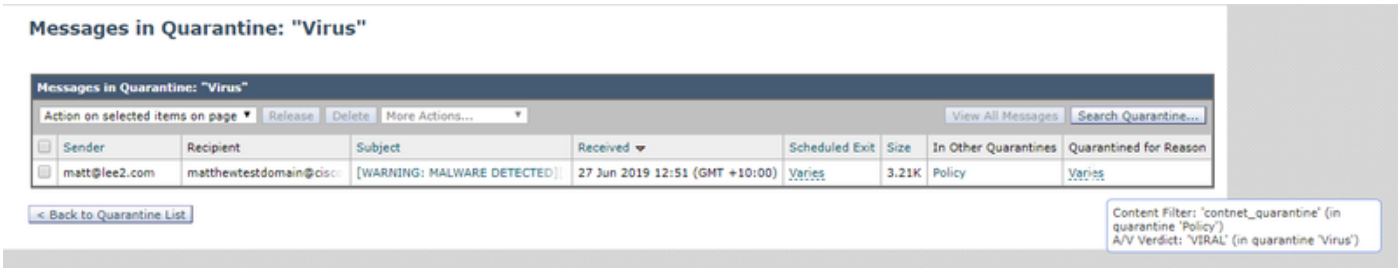
> **참고:**하나의 PVO 격리에서 삭제된 이메일은 해당 격리가 보유한 모든 후속 격리에서 이메일을 제거합니다.

- 정책 및 바이러스 격리에서 릴리스된 메시지는 안티바이러스, 지능형 악성코드 차단 및 그레이메일 엔진에 의해 재검사됩니다.
- Outbreak 격리에서 릴리스된 메시지는 안티스팸, 안티바이러스 및 AMP 엔진에 의해 재검사됩니다.
- File Analysis(파일 분석) 격리에서 릴리스된 메시지는 위협을 재검사합니다.
- 첨부 파일이 있는 메시지는 정책, 바이러스 및 Outbreak 격리에서 릴리스될 때 파일 평판 서비스에 의해 재검사됩니다.

ESA에서 필터링을 통한 초기 이메일 주입이 출력에서는 스팸 격리, 바이러스 격리 및 정책 격리에 의해 플래그가 지정됩니다.

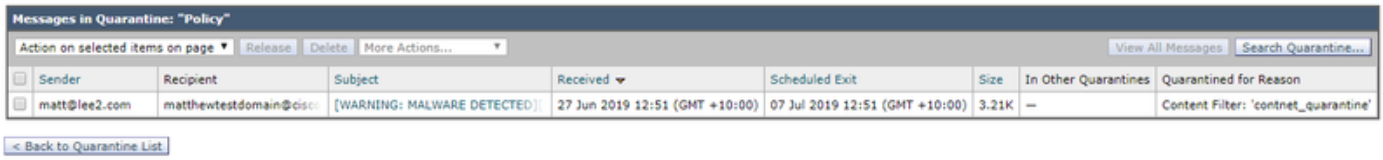
```
Thu Jun 27 12:51:03 2019 Info: Start MID 378951 ICID 391696
Thu Jun 27 12:51:03 2019 Info: MID 378951 ICID 391696 From: <matt@lee2.com>
Thu Jun 27 12:51:10 2019 Info: MID 378951 ICID 391696 RID 0 To: <matthewtestdomain@cisco.com>
Thu Jun 27 12:51:14 2019 Info: MID 378951 Subject 'Test email with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

격리 내부에서 조사한 후, 표시한 PVO 격리에 보관된 이메일은 물론 해당 격리가 포함될 다른 모든 격리도 표시됩니다.



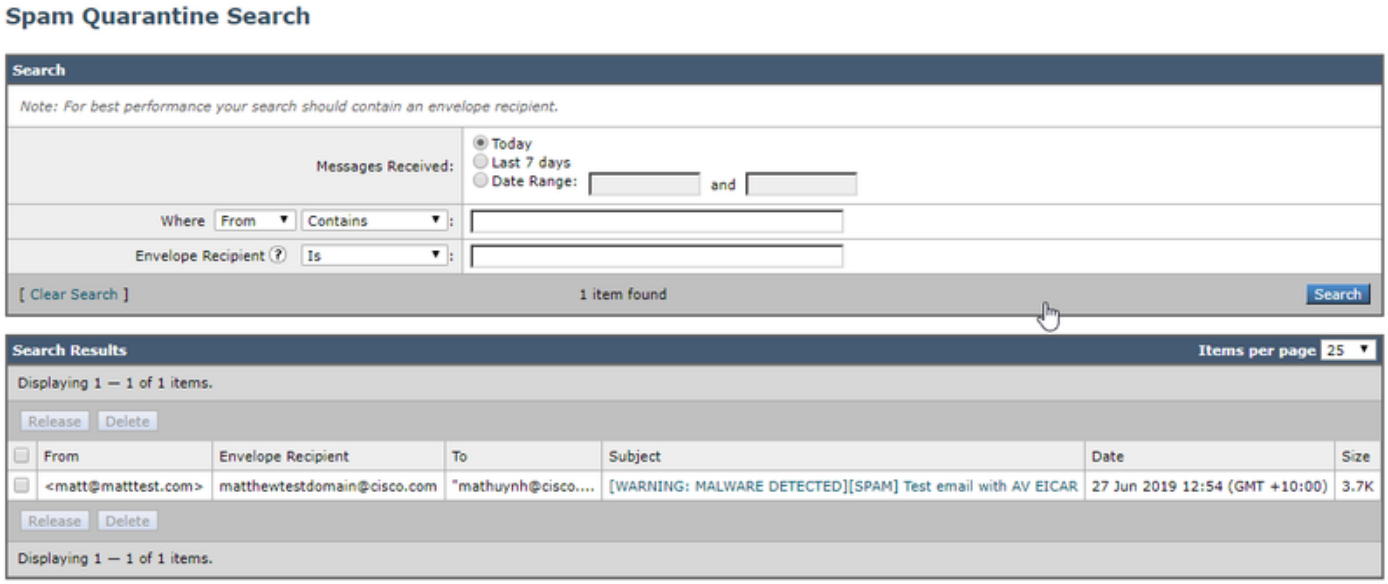
이 격리에서 릴리스된 후에는 이 이벤트를 **mail_logs**에 기록하고 다른 격리에 반영하며 다른 격리에서 더 이상 사용할 수 없습니다.

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



PVO 격리에서 릴리스합니다. 이 경우 이메일이 플래그가 지정된 스팸 격리로 이동할 수 있습니다.

```
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
```



스팸 격리의 최종 릴리스에서는 이메일이 배달 대기열로 이동됩니다.

```
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
```

관련 정보

- Cisco Email Security Appliance – 엔드 유저 가이드
- 기술 지원 및 문서 – Cisco Systems