ESA에서 DKIM 확인을 기반으로 수신 필터 구성

소개

이 문서에서는 수신 콘텐츠 필터 또는 메시지 필터 구성을 통해 DKIM(Domain Keys Identified Email) 확인에 대한 작업을 수행하기 위해 ESA(Email Security Appliance)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ESA
- 콘텐츠 필터 구성에 대한 기본 지식
- 메시지 필터 구성에 대한 기본 지식
- 정책, 바이러스 및 Outbreak 격리 구성 지식 중앙 집중화

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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.

구성

1단계. DKIM 확인 구성

DKIM 확인이 활성화되었는지 확인합니다.Mail Policies(**메일 정책) > Mail Flow Policies(메일 플로우 정책)로 이동합니다**.

ESA에서 DKIM 확인을 구성하려면 SPF 확인과 유사합니다.메일 흐름 정책의 **기본 정책 매개변수**에서 DKIM Verification(DKIM 확인)을 **On(켜기)으로** 설정하면 됩니다.

2단계. 최종 조치 확인

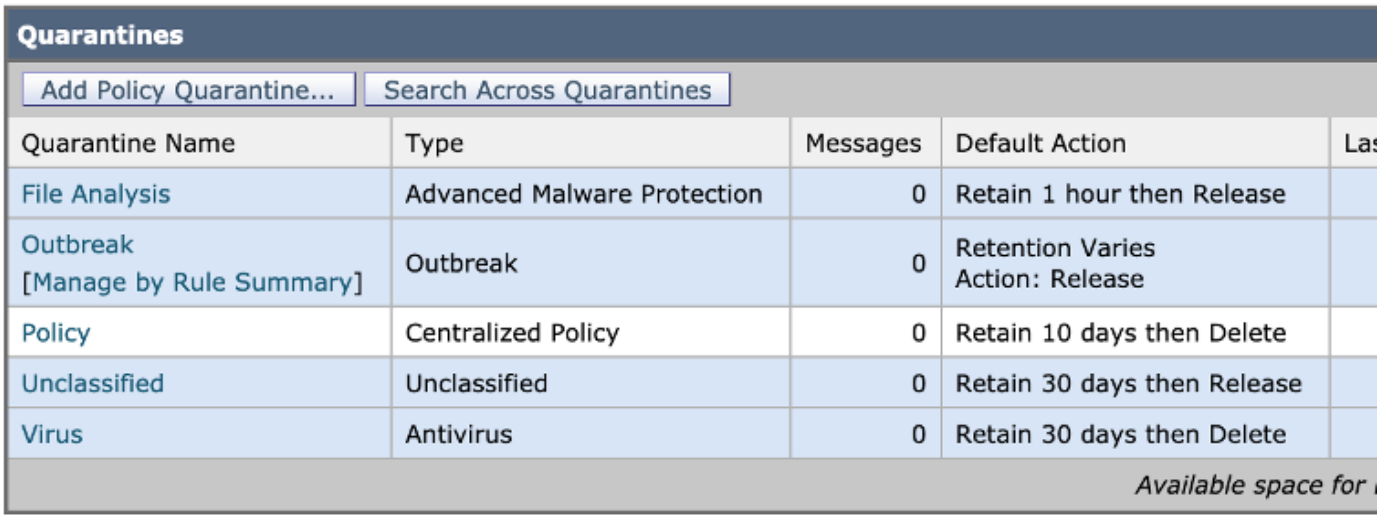
먼저 DKIM 확인에 따라 수행할 작업을 식별합니다.예:삭제, 태그 또는 격리를 추가합니다.최종 작업이 메일을 격리하는 경우 구성된 격리를 검토합니다.

- 중앙 집중식 관리를 사용하지 않는 경우

ESA **>Monitor> Policy, Virus and Outbreak Quarantines로 이동합니다**.

- 중앙 집중식 관리(SMA)를 구성한 경우:

이미지에 표시된 대로 **SMA >Email > Message Quarantine >Policy, Virus and Outbreak Quarantines**로 이동합니다.

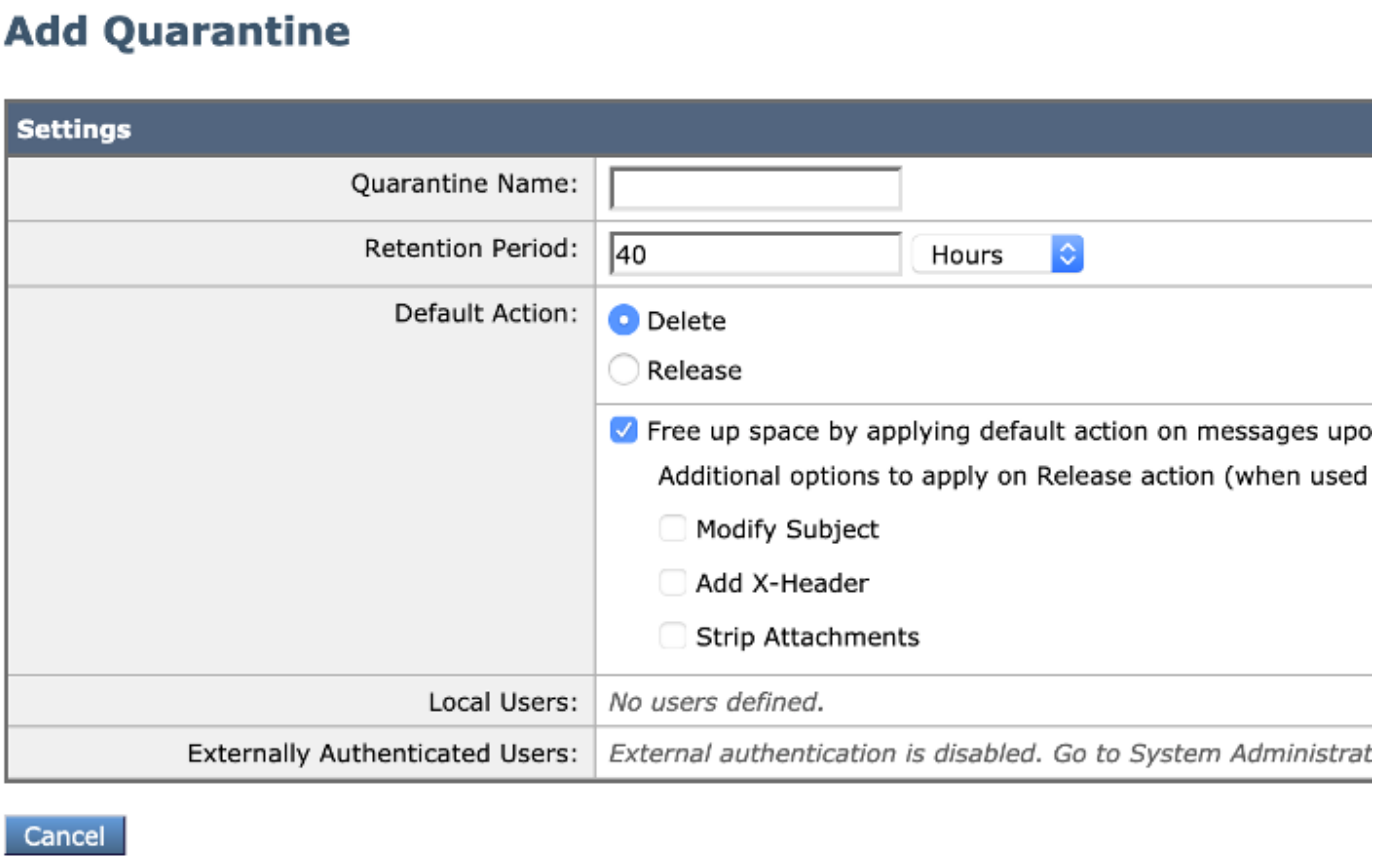


DKIM/**도메인 기반 메시지 인증**, 보고 및 적합성(DMARC)/SPF(Sender Policy Framework) 서비스에 대한 특정 격리가 없는 경우하나를 생성하는 것이 좋습니다.

Policy(정책), Virus(바이러스) 및 Outbreak Quarantines(Outbreak 격리)에서 Add Policy Quarantine(**정책 격리 추가)을** 선택합니다.

여기에서 다음을 설정할 수 있습니다.

- 쿼런틴 이름: 예: DkimQuarantine
- 보존 기간:조직의 요구 사항과 기본 작업에 따라 달라집니다.이메일의 보존 기간이 지나면 이미지에 표시된 대로 선택한 내용에 따라 이메일이 삭제되거나 릴리스되고 전달됩니다.



3단계. ESA용 수신 필터

a.ESA에 대한 수신 콘텐츠 필터 생성:

ESA > **Mail Policies > Incoming Content Filters > Add Filter로 이동합니다**.

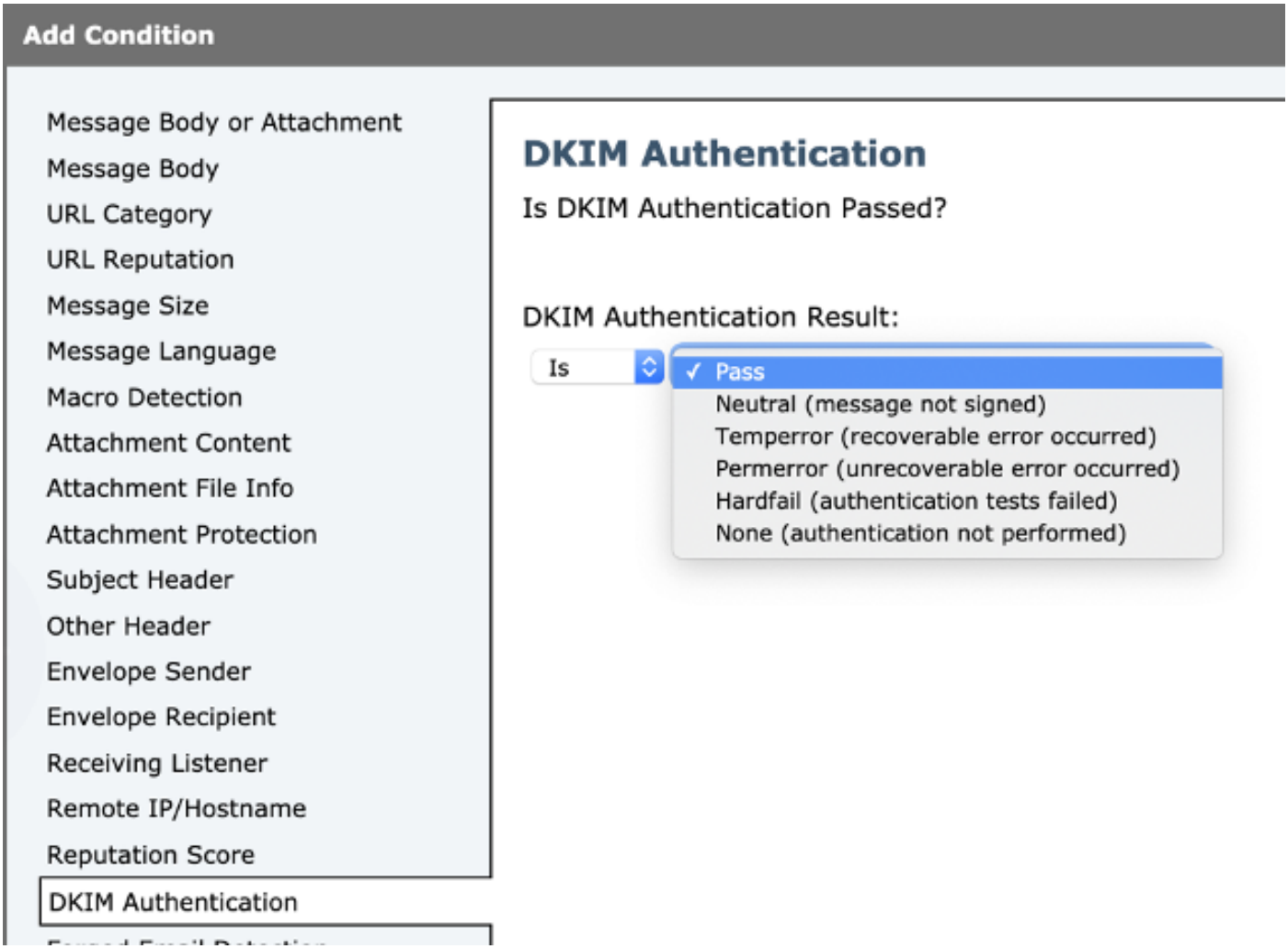
- 첫 번째 섹션:필터의 **Name**, **Description** 및 **Order**를 구성할 수 있습니다.

- 두 번째 섹션:조건을 추가합니다.DKIM 확인에 대한 작업을 수행하기 위해 하나 이상의 조건을 추가할 수 있으며 더 많은 콘텐츠 필터를 구성할 수 있습니다.

인증 결과 예상 및 의미:

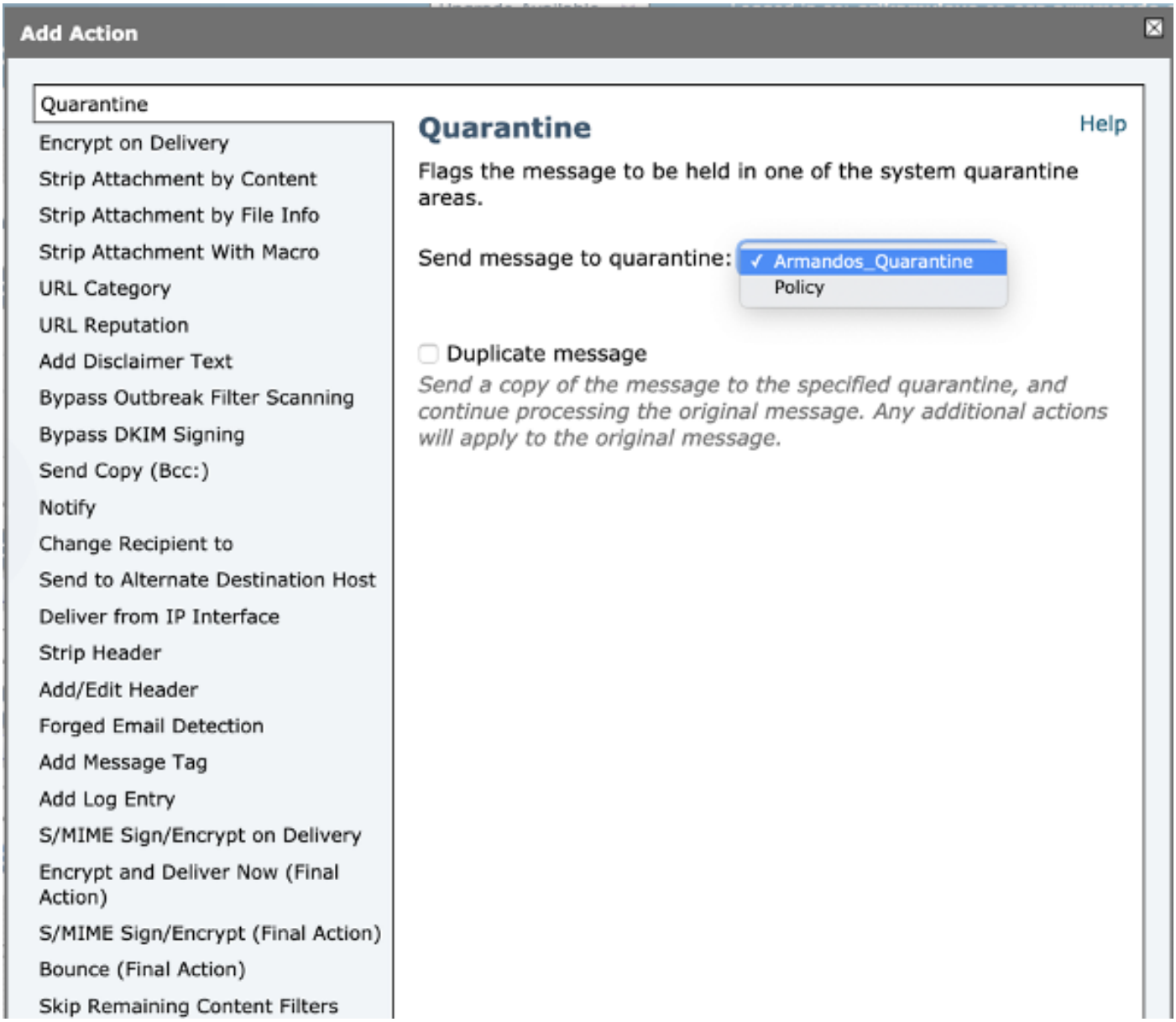
- 통과:메시지가 인증 테스트를 통과했습니다.

- 중립:인증이 수행되지 않았습니다.
- 온도:복구할 수 있는 오류가 발생했습니다.
- 오류:복구할 수 없는 오류가 발생했습니다.
- 하드웨어 장애:인증 테스트에 실패했습니다.
- 없음.메시지가 서명되지 않았습니다.



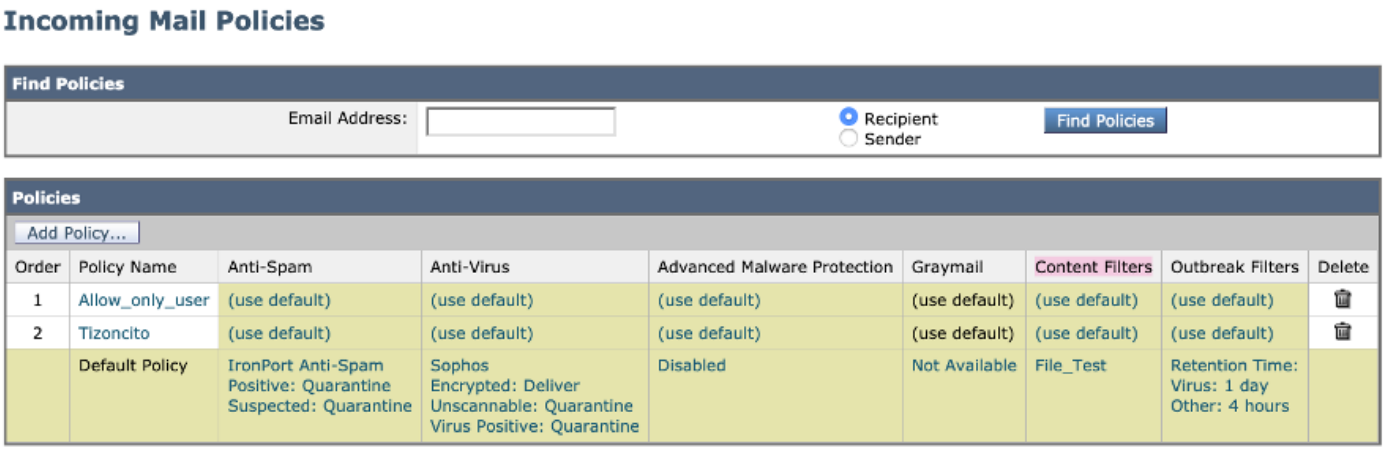
참고:DKIM 확인 요구 사항:발신자가 메시지를 확인하기 전에 서명해야 합니다.전송 도메인에는 확인을 위해 DNS에서 사용할 수 있는 공개 키가 있어야 합니다.

- 세 번째 섹션:작업을 선택합니다.로그 항목 추가, 쿼런틴으로 전송, 이메일 삭제, 알림 등 둘 이상의 작업을 추가할 수 있습니다.이 경우 이미지에 표시된 대로 이전에 구성된 격리를 선택합니다.



메일 플로우 정책에 새 필터 추가:

필터가 생성되면ESA에서 최종 작업으로 DKIM을 확인하려는 각 메일 플로우 정책에 필터를 추가합니다.이미지에 표시된 대로 **ESA> Mail Policies(메일 정책) > Incoming Mail Policies(**수신 메일 정책**)**로 이동합니다.



Content filters(**콘텐츠 필터**) 열 및 **Mail flow policy(메일 플로우 정책**) 행을 클릭합니다.

참고:(기본값 사용) 작업이 기본 정책 설정으로 구성되었음을 의미하지는 않습니다.필요한 필터를 사용하여 각 메일 플로우 정책을 구성합니다.

b.ESA에 대한 메시지 필터 생성:

모든 메시지 필터는 ESA CLI에서 구성됩니다.Filters 명령을 **입력하고** 다음 지침을 따릅니다.

```
ESA. com> filters
Choose the operation you want to perform:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
[]> NEW
Enter filter script.  Enter '.' on its own line to end.
DKIM_Filter:
If (dkim-authentication == "hardfail" )
{
quarantine("DkimQuarantine");
}
.
1 filters added.
```

필터가 생성되면 범례를 검토합니다.**필터 1개가 추가되었습니다**.

구성할 조건 및 작업은 수신 콘텐츠 필터에서 사용하는 조건과 동일합니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

수신 콘텐츠 필터:

- ESA 웹 사용자 인터페이스(WebUI)에서

a.필터가 구성되었는지 확인합니다.

ESA >**Mail Policies(메일 정책) >Incoming Content Filters(수신 콘텐츠 필터)로 이동합니다.**표시된 목록에서 이전에 선택한 순서에 따라 필터를 구성해야 합니다.

b.필터가 적용되었는지 확인합니다.

ESA>**Mail Policies(메일 정책) > Incoming mail policies(수신 메일 정책)로 이동합니다**.

필터 이름은 Content filters(콘텐츠 필터) 열 및 Mail flow(메일 플로우) 정책 행에 표시되어야 합니다.목록이 넓고 이름이 표시되지 않으면 정책에 적용된 필터를 식별하려면 필터 목록을 클릭합니다.

메시지 필터:

```
From ESA CLI:
ESA. com> filters
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
```

```
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> list

Num Active Valid Name

  1           Y      Y     DKIM_Filter
```

목록은 필터가 구성되어 있고 활성화되어 있는지 여부를 보여줍니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

구성 확인:

다음을 확인해야 합니다.

- 메일 흐름 정책에 dkim이 있습니다.확인
- 콘텐츠 필터 또는 메시지 필터에 구성된 작업이 있습니다.
- 콘텐츠 필터의 경우 필터가 메일 흐름과 연결되어 있는지 확인합니다

메시지 추적 확인:

메시지 추적을 통해 다음을 관찰할 수 있습니다.

- DKIM 확인 결과(예:perfail
- 구성된 로그 항목(구성된 경우)
- 필터가 적용되었습니다(이름 및 수행된 작업).

ESA에서 추적:

```
Fri Apr 26 11:33:44 2019 Info: MID 86 ICID 98 From: <user@domain.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 ICID 98 RID 0 To: <userb@domainb.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 Message-ID '<3903af$2r@mgt.esa.domain.com>Fri Apr 26
11:33:44 2019 Info: MID 86 DKIM: permfail body hash did not verify [final]
Fri Apr 26 11:33:44 2019 Info: MID 86 Subject "Let's go to camp!"
Fri Apr 26 11:33:44 2019 Info: MID 86 ready 491 bytes from <user@domain.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 matched all recipients for per-recipient policy
Allow_only_user in the inbound table
Fri Apr 26 11:33:46 2019 Info: MID 86 interim verdict using engine: CASE spam negative
Fri Apr 26 11:33:46 2019 Info: MID 86 using engine: CASE spam negative
Fri Apr 26 11:33:46 2019 Info: MID 86 interim AV verdict using Sophos CLEAN
Fri Apr 26 11:33:46 2019 Info: MID 86 antivirus negative
Fri Apr 26 11:33:46 2019 Info: MID 86 AMP file reputation verdict : UNSCANNABLE
Fri Apr 26 11:33:46 2019 Info: MID 86 using engine: GRAYMAIL negative
Fri Apr 26 11:33:46 2019 Info: MID 86 Custom Log Entry: The content that was found was:
DkimFilter
Fri Apr 26 11:33:46 2019 Info: MID 86 Outbreak Filters: verdict negative
Fri Apr 26 11:33:46 2019 Info: MID 86 quarantined to "DkimQuarantine" by add-footer filter
'DkimFilter '
Fri Apr 26 11:33:46 2019 Info: Message finished MID 86 done
```

관련 정보

- 모범 사례 ESA-SPF-DKIM-DMARC
- Email Security Appliance 최종 사용자 가이드
- DKIM RFC4871
- DKIM RFC8301
- DKIM RFC8463
- 기술 지원 및 문서 – Cisco Systems