ESA에서 스푸핑된 이메일 메시지 탐지 및 예외 생성

목차

소개

이 문서에서는 Cisco ESA에서 이메일 스푸핑을 제어하는 방법 및 스푸핑된 이메일을 보낼 수 있도록 허용된 사용자에 대한 예외를 생성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

ESA(Email Security Appliance)는 수신 및 발신 메일을 모두 처리하고, RELAYLIST의 표준 컨피그레이션을 사용하여 메시지를 발신으로 플래그 지정해야 합니다.

사용되는 구성 요소

사용되는 특정 구성 요소는 다음과 같습니다.

- 사전: 모든 내부 도메인을 저장하는 데 사용됩니다.
- 메시지 필터 : 스푸핑된 이메일을 탐지하고 콘텐츠 필터가 작동할 수 있는 헤더를 삽입하기 위한 논리를 처리하는 데 사용됩니다.
- 정책 격리: 스푸핑된 이메일의 중복을 임시로 저장하는 데 사용됩니다. 릴리스된 메시지의 IP

주소를 MY_TRUSTED_SPOOF_HOSTS에 추가하여 이 발신자의 향후 메시지가 정책 격리로 들어가지 않도록 하는 것이 좋습니다.
- MY_TRUSTED_SPOOF_HOSTS: 신뢰할 수 있는 전송 IP 주소를 참조하는 목록입니다. 이 목록에 발신자의 IP 주소를 추가하면 격리를 건너뛰고 발신자가 스푸핑할 수 있습니다. MY_TRUSTED_SPOOF_HOSTS 발신자 그룹에 신뢰할 수 있는 발신자를 배치하여 이러한 발신자의 스푸핑된 메시지가 격리되지 않도록 합니다.
- RELAYLIST: 릴레이가 허용된 IP 주소를 인증하거나 아웃바운드 이메일을 보낼 수 있는 목록입니다. 이메일이 이 발신자 그룹을 통해 전달된 경우 메시지가 스푸핑된 메시지가 아닌 것으로 가정합니다.

✎ 참고: 발신자 그룹 중 하나가 MY_TRUSTED_SPOOF_HOSTS 또는 RELAYLIST와 다른 이름으로 호출되는 경우 해당 발신자 그룹 이름으로 필터를 수정해야 합니다. 또한 여러 리스너가 있는 경우 MY_TRUSTED_SPOOF_HOSTS도 두 개 이상 있습니다.

이 문서의 정보는 모든 AsyncOS 버전의 ESA를 기반으로 합니다.

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

배경 정보

스푸핑은 Cisco ESA에서 기본적으로 활성화되어 있습니다. 다른 도메인을 대신 보낼 수 있도록 허용하는 몇 가지 유효한 이유가 있습니다. 한 가지 일반적인 예로, ESA 관리자는 스푸핑된 메시지가 전달되기 전에 격리하여 스푸핑된 이메일을 제어하려고 합니다.

스푸핑된 이메일에 대한 쿼런틴 등의 특정 작업을 수행하려면 먼저 스푸핑된 이메일을 탐지해야 합니다.

이메일 스푸핑이란?

이메일 스푸핑은 이메일 헤더가 위조된 것이므로 메시지가 실제 소스가 아닌 다른 사람이나 다른 곳에서 온 것으로 보입니다. 이메일 스푸핑은 피싱 및 스팸 캠페인에 사용되는 전술입니다. 합법적인 소스에서 이메일을 보냈다고 생각할 때 이메일을 열 가능성이 높기 때문입니다.

스푸핑된 이메일을 탐지하는 방법

이메일 주소에 자체 수신 도메인 중 하나를 포함하는 봉투 발신자(Mail-From) 및 보낸 사람(From) 헤더가 있는 메시지를 필터링하려는 경우

특정 발신자에 대한 스푸핑을 허용하는 방법

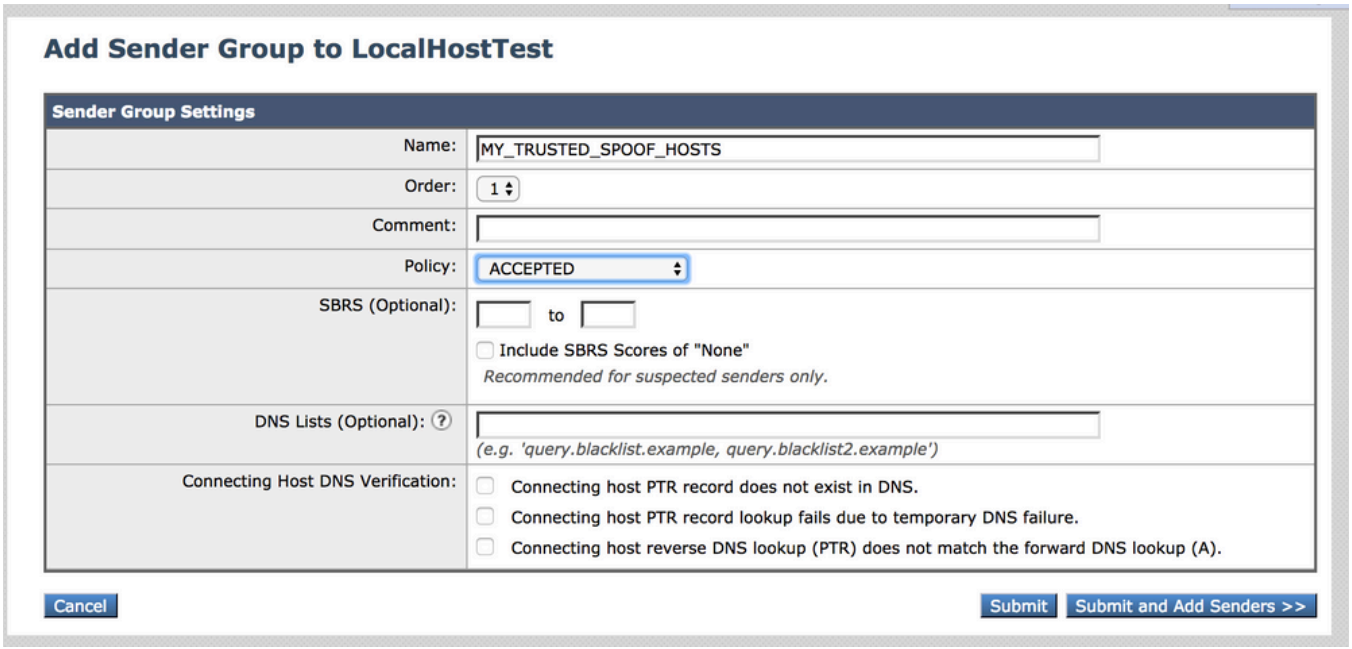
이 문서에 제공된 메시지 필터를 구현하면 스푸핑된 메시지에 헤더가 태그 지정되며, 콘텐츠 필터는 헤더에 대한 작업을 수행하는 데 사용됩니다. 예외를 추가하려면 발신자 IP를 MY_TRUSTED_SPOOF_HOSTS에 추가하기만 하면 됩니다.

구성

발신자 그룹 만들기

1. ESA GUI에서 Mail Policies(메일 정책) > HAT Overview(HAT 개요)로 이동합니다
2. 클릭 추가.
3. Name(이름) 필드에 MY_TRUSTED_SPOOF_HOSTS를 지정합니다.
4. Order(순서) 필드에서 1을 지정합니다.
5. Policy 필드에 ACCEPTED를 지정합니다.
6. Submit(제출)을 클릭하여 변경 사항을 저장합니다.
7. 마지막으로, Commit Changes(변경 사항 커밋)를 클릭하여 컨피그레이션을 저장합니다

예:

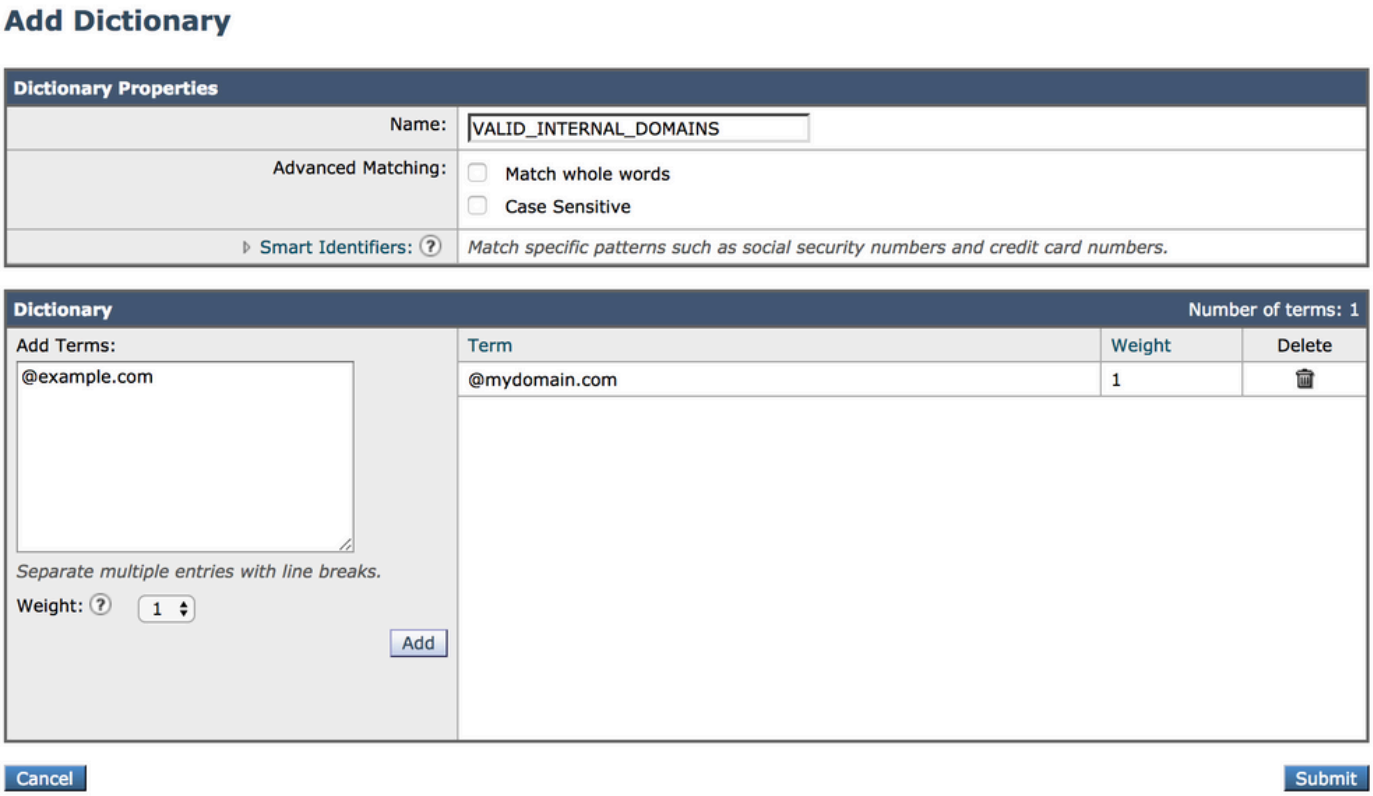


사전 만들기

ESA에서 스푸핑을 비활성화할 모든 도메인에 대한 사전을 생성합니다.

1. ESA GUI에서 Mail Policies(메일 정책) > Dictionaries(사전)로 이동합니다.
2. 클릭 사전을 추가합니다.
3. 메시지 필터 복사 및 붙여넣기를 오류 없이 수행하려면 Name 필드에 'VALID_INTERNAL_DOMAINS'를 지정합니다.
4. 용어 추가에서 스푸핑을 탐지할 모든 도메인을 추가합니다. 도메인 앞에 @ 기호가 있는 도메인을 입력하고 추가를 클릭합니다.
5. 전체 단어 일치 확인란이 선택되지 않았는지 확인합니다.
6. 사전 변경 사항을 저장하려면 Submit(제출)을 클릭합니다.
7. 마지막으로, Commit Changes(변경 사항 커밋)를 클릭하여 컨피그레이션을 저장합니다.

예:



메시지 필터 만들기

다음으로, 방금 생성한 사전 "VALID_INTERNAL_DOMAINS"를 활용하려면 메시지 필터를 생성해야 합니다.

1. ESA의 CLI(Command Line Interface)에 연결합니다.
2. Filters 명령을 실행합니다.
3. New 명령을 실행하여 새 메시지 필터를 만듭니다.
4. 필요한 경우 실제 발신자 그룹 이름을 편집하여 이 필터 예제를 복사하여 붙여 넣습니다.

```
mark_spoofed_messages:
if(
     (mail-from-dictionary-match("VALID_INTERNAL_DOMAINS", 1))
 OR  (header-dictionary-match("VALID_INTERNAL_DOMAINS","From", 1)))
 AND ((sendergroup != "RELAYLIST")
 AND (sendergroup != "MY_TRUSTED_SPOOF_HOSTS")
  )
{
insert-header("X-Spoof", "");
}
```

5. 기본 CLI 프롬프트로 돌아가 Commit을 실행하여 컨피그레이션을 저장합니다.
6. GUI > Mail Policies(메일 정책) > Incoming Content Filters(수신 콘텐츠 필터)로 이동합니다.
7. 스푸핑 헤더 X-Spoof에 대한 작업을 수행하는 수신 콘텐츠 필터 만들기:

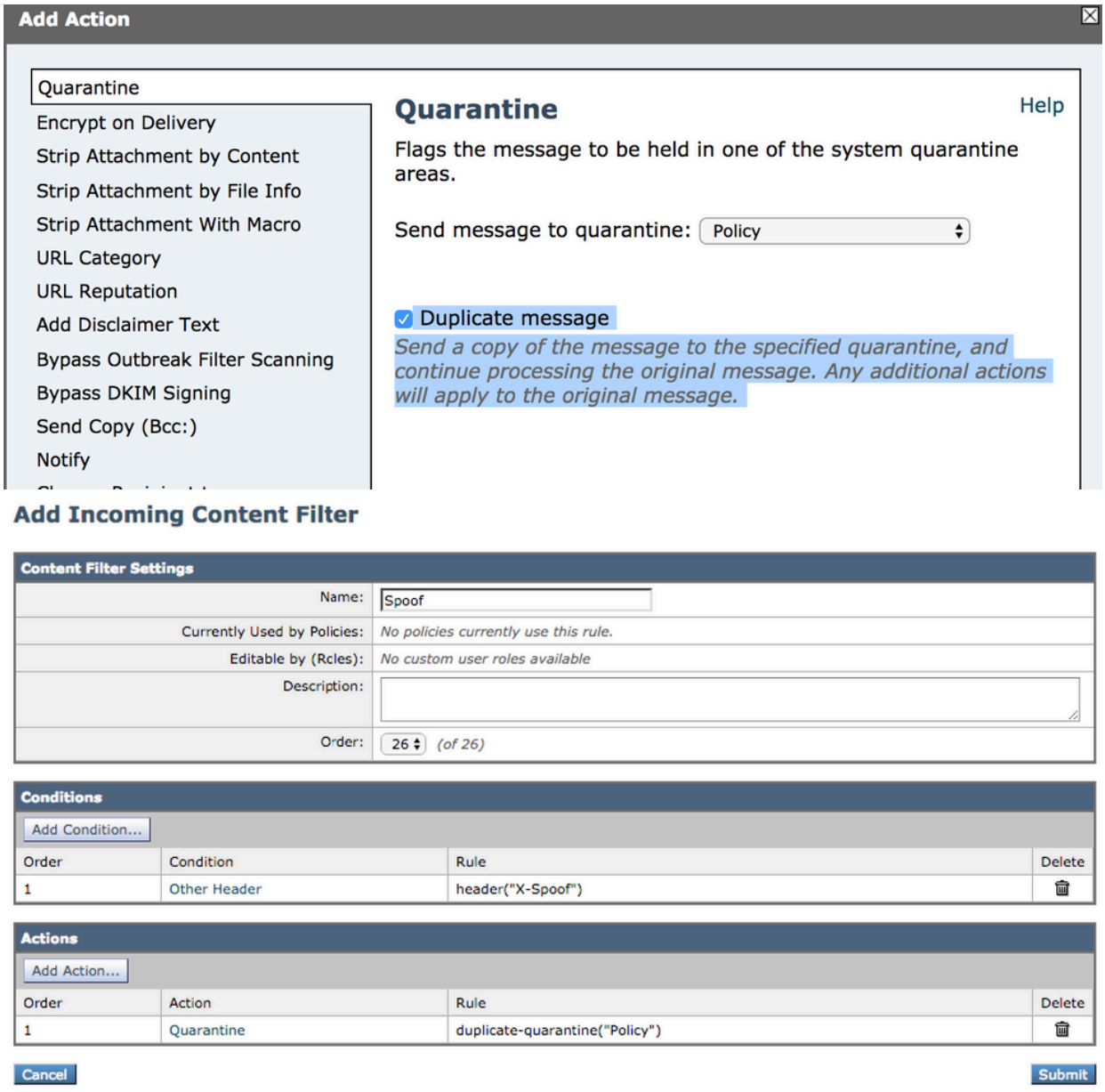
    1. 다른 헤더 추가

2. 헤더 이름: X-Spoof

3. Header exists(헤더 있음) 라디오 버튼

4. 추가 작업: duplicate-quarantine(Policy).

> 참고: 여기에 표시된 메시지 복제 기능은 메시지의 복사본을 보관하며, 원본 메시지를 수신자에게 계속 전송합니다.



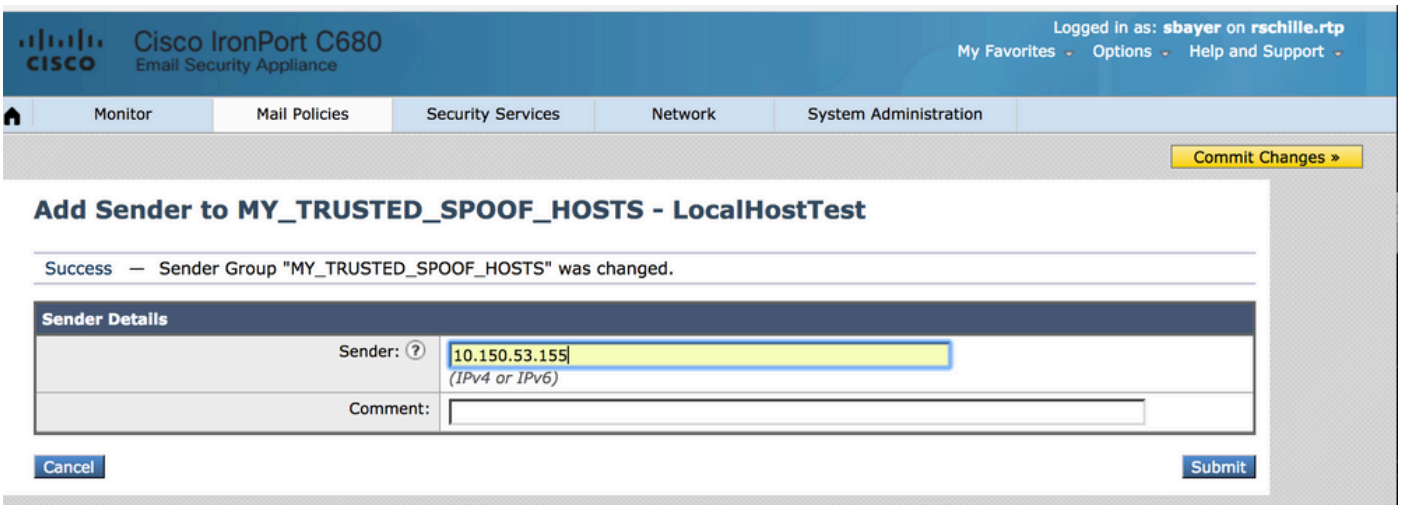
8. GUI > Mail Policies(메일 정책) > Incoming Mail Policies(수신 메일 정책)에서 콘텐츠 필터를 수신 메일 정책에 연결합니다.
9. 변경 사항을 제출 및 커밋합니다.

MY_TRUSTED_SPOOF_HOSTS에 스푸핑 예외 추가

마지막으로 MY_TRUSTED_SPOOF_HOSTS 발신자 그룹에 스푸핑 예외(IP 주소 또는 호스트 이름)를 추가해야 합니다.

1. 웹 GUI를 통해 탐색: Mail Policies(메일 정책) > HAT Overview(HAT 개요)
2. MY_TRUSTED_SPOOF_HOSTS 발신자 그룹을 클릭하고 엽니다.
3. IP 주소, 범위, 호스트 이름 또는 부분 호스트 이름을 추가하려면 Add Sender...를 클릭합니다.
4. Submit(제출)을 클릭하여 발신자 변경 사항을 저장합니다.
5. 마지막으로, Commit Changes(변경 사항 커밋)를 클릭하여 컨피그레이션을 저장합니다.

예:



다음을 확인합니다.

스푸핑된 메시지가 격리되었는지 확인

도메인 중 하나를 봉투 발신자로 지정하는 테스트 메시지를 보냅니다. 필터가 예상대로 작동하는지 확인하려면 해당 메시지에 대해 메시지 추적을 수행합니다. 스푸핑이 허용된 발신자에 대한 예외를 아직 만들지 않았으므로 메시지가 격리됩니다.

<#root>

```
Thu Apr 23 07:09:53 2015 Info: MID 102 ICID 9 RID 0 To: <xxxx_xxxx@domain.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 Subject 'test1'
Thu Apr 23 07:10:07 2015 Info: MID 102 ready 177 bytes from <user_1@example.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 matched all recipients for per-recipient policy DEFAULT in the i
Thu Apr 23 07:10:11 2015 Info: MID 102 interim verdict using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:10:11 2015 Info: MID 102 antivirus negative
```

Thu Apr 23 07:10:12 2015 Info: MID 102 quarantined to "Policy" (message filter:quarantine_spoofed_messag

```
Thu Apr 23 07:10:12 2015 Info: Message finished MID 102 done
```

Spoof-Exception 메시지가 전달되고 있는지 확인

Spoof-Exception 발신자는 위의 필터에서 참조하는 발신자 그룹의 IP 주소입니다.

RELAYLIST는 ESA에서 아웃바운드 메일을 보내는 데 사용되므로 참조됩니다. 일반적으로 RELAYLIST가 전송하는 메시지는 아웃바운드 메일입니다. 이를 포함하지 않으면 오탐이 발생하거나 위의 필터에 의해 격리되는 아웃바운드 메시지가 생성됩니다.

MY_TRUSTED_SPOOF_HOSTS에 추가된 Spoof-Exception IP 주소의 메시지 추적 예. 예상되는 작업은 격리가 아닌 배달입니다. (이 IP는 스푸핑할 수 있습니다.)

<#root>

```
Thu Apr 23 07:25:57 2015 Info: Start MID 108 ICID 11
Thu Apr 23 07:25:57 2015 Info: MID 108 ICID 11 From: <user_1@example.com>
Thu Apr 23 07:26:02 2015 Info: MID 108 ICID 11 RID 0 To: <user_xxxx@domain.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 Subject 'test2'
Thu Apr 23 07:26:10 2015 Info: MID 108 ready 163 bytes from <user_1@example.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 matched all recipients for per-recipient policy DEFAULT in the i
Thu Apr 23 07:26:10 2015 Info: MID 108 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:26:10 2015 Info: MID 108 antivirus negative
Thu Apr 23 07:26:10 2015 Info: MID 108 queued for delivery
Thu Apr 23 07:26:10 2015 Info: Delivery start DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: Message done DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: MID 108 RID [0] Response '2.0.0 t58EVG9N031598
```

Message accepted for delivery'

```
Thu Apr 23 07:26:11 2015 Info: Message finished MID 108 done
```

관련 정보

- ESA 스푸핑된 메일 필터링
- 발신자 확인을 사용한 스푸핑 보호

Cisco 내부 정보

이 프로세스를 간소화하기 위해 RAT를 메시지 필터/콘텐츠 필터에 노출시키는 기능 요청이 있습니다.

Cisco 버그 ID CSCus49018 - ENH: RAT(Recipient Access Table)를 필터 조건에 노출

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.