

# ESA FAQ:ESA 안티스팸 기능을 테스트하려면 어떻게 해야 합니까?

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[ESA 안티스팸 기능을 테스트하려면 어떻게 해야 합니까?](#)

[TELNET으로 안티스팸 테스트](#)

[문제 해결](#)

## 소개

이 문서에서는 Cisco ESA(Email Security Appliance) 안티스팸 기능을 테스트하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ESA
- AsyncOS
- Cisco ESA 안티스팸 기능

### 사용되는 구성 요소

이 문서의 정보는 모든 버전의 AsyncOS를 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 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## ESA 안티스팸 기능을 테스트하려면 어떻게 해야 합니까?

ESA Anti-Spam 기능의 기능을 테스트하려면 TELNET 또는 이메일 클라이언트(Microsoft Outlook, Eudora, Thunderbird, Lotus Notes)를 통해 새 메시지를 작성하고 다음 헤더 중 하나를 삽입합니다.

- X-광고:의심
- X-광고:스팸
- X-광고:마케팅

그런 다음 안티스팸 기능이 활성화된 ESA를 통해 메시지를 전송하고 결과를 모니터링할 수 있습니다.

## TELNET으로 안티스팸 테스트

이 섹션에서는 널리 사용 가능한 TELNET 유틸리티를 통해 테스트 메시지를 수동으로 생성하는 방법을 보여 주는 예제를 제공합니다.

TELNET을 통해 테스트 메시지를 생성하려면 다음 예의 정보를 사용합니다. 굵게 표시된 정보를 입력하면 서버가 다음과 같이 응답합니다.

```
telnet hostname.example.com 25
```

```
220 hostname.example.com ESMTTP
```

```
ehlo localhost
```

```
250-hostname.example.com
```

```
250-8BITMIME
```

```
250 SIZE 10485760
```

```
mail from:
```

```
250 sender <sender@example.com> ok
```

```
rcpt to:
```

```
250 recipient <recipient@example.com> ok
```

```
data
```

```
354 go ahead
```

```
X-Advertisement: Marketing
```

```
from: sender@example.com
```

```
to: recipient@example.com
```

```
subject: test
```

```
test
```

```
.
```

```
250 ok: Message 120 accepted
```

mail\_logs를 검토하고 안티스팸 검사 결과를 확인하여 메시지가 기록된 것으로 처리되는지 확인합니다. 이전 예와 같이 기본 인바운드 메일 정책은 메일이 마케팅임을 탐지합니다.

```
Thu Jun 26 22:21:56 2014 Info: New SMTP DCID 66 interface 172.11.1.111 address  
111.22.33.111 port 25
```

```
Thu Jun 26 22:21:58 2014 Info: DCID 66 TLS success protocol TLSv1 cipher  
RC4-SHA
```

```
Thu Jun 26 22:21:58 2014 Info: Delivery start DCID 66 MID 119 to RID [0]
Thu Jun 26 22:21:59 2014 Info: Message done DCID 66 MID 119 to RID [0]
Thu Jun 26 22:21:59 2014 Info: MID 119 RID [0] Response '2.0.0 s5R2LhnL014175
Message accepted for delivery'
Thu Jun 26 22:21:59 2014 Info: Message finished MID 119 done
Thu Jun 26 22:22:04 2014 Info: DCID 66 close
Thu Jun 26 22:22:53 2014 Info: SDS_CLIENT: URL scanner enabled=0
Thu Jun 26 22:25:35 2014 Info: SLBL: Database watcher updated from snapshot
20140627T022535-slbl.db.
Thu Jun 26 22:26:04 2014 Info: Start MID 120 ICID 426
Thu Jun 26 22:26:04 2014 Info: MID 120 ICID 426 From: <sender@example.com>
Thu Jun 26 22:26:10 2014 Info: MID 120 ICID 426 RID 0 To:
<recipient@example.com>
Thu Jun 26 22:26:20 2014 Info: MID 120 Subject 'test'
Thu Jun 26 22:26:20 2014 Info: MID 120 ready 201 bytes from <sender@example.com>
Thu Jun 26 22:26:20 2014 Info: MID 120 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Thu Jun 26 22:26:21 2014 Info: MID 120 interim verdict using engine:
CASE marketing
Thu Jun 26 22:26:21 2014 Info: MID 120 using engine: CASE marketing
Thu Jun 26 22:26:21 2014 Info: MID 120 interim AV verdict using Sophos CLEAN
Thu Jun 26 22:26:21 2014 Info: MID 120 antivirus negative
Thu Jun 26 22:26:21 2014 Info: Message finished MID 120 done
Thu Jun 26 22:26:21 2014 Info: MID 121 queued for delivery
Thu Jun 26 22:26:21 2014 Info: New SMTP DCID 67 interface 172.11.1.111 address
111.22.33.111 port 25
Thu Jun 26 22:26:21 2014 Info: DCID 67 TLS success protocol TLSv1 cipher RC4-SHA
Thu Jun 26 22:26:21 2014 Info: Delivery start DCID 67 MID 121 to RID [0]
Thu Jun 26 22:26:22 2014 Info: Message done DCID 67 MID 121 to RID [0]
Thu Jun 26 22:26:22 2014 Info: MID 121 RID [0] Response '2.0.0 s5R2QQso009266
Message accepted for delivery'
Thu Jun 26 22:26:22 2014 Info: Message finished MID 121 done
Thu Jun 26 22:26:27 2014 Info: DCID 67 close
```

## 문제 해결

메시지가 스팸, 의심되는 스팸 또는 마케팅으로 탐지되지 않은 경우 **Mail Policies(메일 정책) > Incoming Mail Policies(수신 메일 정책) 또는 Mail Policies(메일 정책) > Outgoing Mail Policies(발신 메일 정책)**를 검토합니다. Default Policy(기본 정책) 또는 Policy Name(정책 이름)을 선택하고 Anti-Spam(안티스팸) 열에서 하이퍼링크를 클릭하여 정책에 대한 Anti-Spam 설정 및 컨피그레이션을 확인합니다.

Cisco에서는 양성으로 식별된 스팸 설정, 의심스런 스팸 설정 및/또는 마케팅 이메일 설정을 원하는 대로 활성화할 것을 권장합니다.