

# ESR geeft geen informatie over bijlagen bij e-mail in de berichtentracing weer

## Inhoud

[Inleiding](#)

[Probleem](#)

[Oplossing](#)

[Filters voorbeeld](#)

## Inleiding

Dit document beschrijft een probleem met de Cisco Email Security Appliance (ESA) wanneer e-mailbijlage geen informatie geeft in het volgen van het bericht en beschrijft een aantal mogelijke oplossingen voor het probleem.

## Probleem

U ontvangt een e-mail met een geldige bijlage. Als er geen bodyscanner is of als er geen scanberichtfilters of contentfilters zijn geïnstalleerd, dan verschijnt de e-mailbijlage niet in het volgende bericht. In het volgende bericht ziet u **Attachments: N.v.t.:**

Envelope and Header Summary	
Received Time:	17 Mar 2014 09:41:59 (GMT +00:00)
MID:	332
Message Size:	929 (Bytes)
Subject:	test
Envelope Sender:	@cisco.com
Envelope Recipients:	@cisco.com
Message ID Header:	<op.xcv3i5pbiv2o52@_cisco.com>
SMTP Auth User ID:	N/A
Attachments:	N/A
Sending Host Summary	
Reverse DNS Hostname:	
IP Address:	
SBRS Score:	

Indien de informatie over de bijlage niet in het bericht wordt weergegeven, geeft dit niet aan dat de ESA de bijlage heeft laten vallen. De bijlage is nog zichtbaar, maar het apparaat heeft niet de benodigde scanners om de e-mailtekst te scannen om de bijlage te kunnen identificeren.

## Oplossing

Dit probleem doet zich voor omdat de scanmachine van de inhoud geen bijlagen actief scant. Volg deze stappen om het bericht te volgen om de bijlageinformatie weer te geven:

1. Configureer ten minste één bericht of contentfilter dat u voor informatie over de bijlage, naam, type of grootte kunt scannen. U kunt ook de gewenste wijzigingen in de bijlagen aanbrengen.
2. Configuratie een lichaamsscanner die voor de namen, koorden, tekens en afmetingen controleert.
3. Configureer een disclaimer (of vergelijkbaar) die nieuwe informatie uit de voetregels of kopregels in de inhoud van de e-mail afdrucken of een wijziging van het e-maillichaam uitvoeren.

## Filters voorbeeld

In dit gedeelte worden een aantal mogelijke filteropties beschreven. U kunt een van de filters gebruiken die door de vakjes in de volgende afbeelding worden omlijnd, omdat het apparaat een of andere vorm van scannen van bijlagen of organen moet uitvoeren:

**Edit Condition**

Message Body or Attachment  
Message Body  
Message Size  
Attachment Content  
Attachment File Info  
Attachment Protection  
Subject Header  
Other Header  
Envelope Sender  
Envelope Recipient  
Receiving Listener  
Remote IP/Hostname  
Reputation Score  
DKIM Authentication  
SPF Verification

**Attachment File Info** Help

Does the message contain an attachment of a filetype matching a specific filename or pattern based on its fingerprint (similar to a UNIX file command)? Does the declared MIME type of an attachment match, or does the IronPort Image Analysis engine find a suspect or inappropriate image?

**Filename:**  
Ends With


**Filename contains term in content dictionary:**  
email\_address

**File type is:**  
Is

**MIME type is:**  
Is

Image Analysis Verdict:

Zodra u de filter(en) hebt gemaakt, dient de e-mailbijlage bij de tracerings te worden aangegeven:

Message Details	
<b>Envelope and Header Summary</b>	
Received Time:	17 Mar 2014 09:54:24 (GMT +00:00)
MID:	333
Message Size:	929 (Bytes)
Subject:	test
Envelope Sender:	@cisco.com
Envelope Recipients:	@cisco.com
Message ID Header:	<op.xcv33tgiiv2o52@.cisco.com>
SMTP Auth User ID:	N/A
 Attachments:	test.vbs
<b>Sending Host Summary</b>	
Reverse DNS Hostname:	
IP Address:	
SBRS Score:	