

Die ESA zeigt keine E-Mail-Anhangsdaten in der Nachrichtenverfolgung an.

Inhalt

[Einführung](#)

[Problem](#)

[Lösung](#)

[Beispielfilter](#)

Einführung

Dieses Dokument beschreibt ein Problem mit der Cisco E-Mail Security Appliance (ESA), wenn die E-Mail-Anhang-Informationen nicht in der Nachrichtenverfolgung enthalten sind und beschreibt einige mögliche Lösungen für das Problem.

Problem

Sie erhalten eine E-Mail mit einem gültigen Anhang. Wenn kein Body-Scanner vorhanden ist oder keine Filter für Nachrichten zum Scannen von Anhängen oder Inhalte vorhanden sind, wird der E-Mail-Anhang nicht in der Nachrichtenverfolgung angezeigt. In der Nachrichtenverfolgung sehen Sie **Anhänge: K/A**:

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:	

Wenn die Anhangsdaten in der Nachrichtenverfolgung nicht angezeigt werden, bedeutet dies nicht, dass die ESA den Anhang verworfen hat. Der Anhang ist noch sichtbar, aber die Appliance verfügt nicht über die erforderlichen Scanner für Versuche, den E-Mail-Text zu scannen, um den Anhang zu identifizieren.

Lösung

Dieses Problem tritt auf, weil das Content-Scan-Modul Anhänge nicht aktiv scannt. Gehen Sie wie folgt vor, damit die Nachrichtenverfolgung die Informationen des Anhangs anzeigen kann:

1. Konfigurieren Sie mindestens einen Nachrichten- oder Content-Filter, der nach Anhangsdaten, Namen, Typ oder Größe suchen kann. Sie können auch erforderliche Änderungen an den Anhängen vornehmen.
2. Konfigurieren Sie einen Body-Scanner, der nach Namen, Zeichenfolgen, Zeichen und Größen sucht.
3. Konfigurieren Sie einen Haftungsausschluss oder Ähnliches, der neue Informationen von den Fußzeigern oder Kopfzeilen in den Text der E-Mail ausgibt oder eine Form der Änderung des E-Mail-Textkörpers ausführt.

Beispielfilter

In diesem Abschnitt werden einige mögliche Filteroptionen beschrieben. Sie können jeden der Filter verwenden, der von den Feldern im nächsten Bild umrissen wird, da die Appliance eine Form von Anhängen oder Körperscannen ausführen muss:

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:

Sobald Sie die Filter erstellt haben, sollte die Nachrichtenverfolgung die E-Mail-Anhänge wie folgt anzeigen:

Message Details

Envelope and Header Summary	
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
Sending Host Summary	
Reverse DNS Hostname:	
IP Address:	
SBRS Score:	