

كرحم نأ نامضل ةلاسرج ذومن لاسرلة فيك زاهج يلع هصحف متي تاسوري فلأ ةحفاكم Cisco Email Security Appliance (ESA)

المحتويات

[المقدمة](#)

[كيفية إرسال نموذج رسالة لضمان أن محرك مكافحة الفيروسات يتم فحصه على جهاز Cisco Email Security Appliance \(ESA\)](#)

[إنشاء ملف TXT](#)

[إرسال نموذج رسالة](#)

[واجهة سطر الأوامر \(CLI\) لنظام Unix](#)

[أوت لوك](#)

[التحقق](#)

[معلومات ذات صلة](#)

المقدمة

يوضح هذا المستند كيفية إرسال رسالة نموذجية للتأكد من مسح محرك مكافحة الفيروسات Sophos أو McAfee Anti-virus على جهاز Cisco Email Security Appliance (ESA).

كيفية إرسال نموذج رسالة لضمان أن محرك مكافحة الفيروسات يتم فحصه على جهاز Cisco Email Security Appliance (ESA)

بالإضافة إلى إرسال عينة رسالة مع اختبار حمولة فيروسية من خلال ESA، يمكننا تشغيل محرك Sophos أو McAfee لمكافحة الفيروسات. قبل تنفيذ الخطوات المدرجة في هذا المستند، ستحتاج إلى إعداد نهج البريد الوارد أو الصادر لديك وتكوين نهج البريد لإجراء عمليات إسقاط مكافحة الفيروسات أو عزل الرسائل المصابة بفيروس. يستخدم هذا المستند رمز ASCII المتوفر من www.eicar.org (EICAR) الذي سيقوم بمحاكاة فيروس إختبار كمرفق:

```
*X5O!P%@AP[4\pZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H
```

ملاحظة: بالنسبة لـ EICAR: تم تقديم ملف الاختبار هذا إلى EICAR لتوزيعه بوصفه "ملف إختبار مكافحة الفيروسات القياسي لـ EICAR"، وهو يستوفي جميع المعايير المذكورة أعلاه. ومن المأمون المرور من مكان إلى آخر، لأنه ليس فيروساً، ولا يتضمن أي أجزاء من الشفرة الفيروسية. تتفاعل معظم المنتجات معه كما لو كان فيروساً (على الرغم من أنها عادة ما تبلغ عنه باسم واضح، مثل "EICAR-AV-Test").

إنشاء ملف TXT

باستخدام سلسلة ASCII أعلاه، قم بإنشاء ملف txt ووضع السلسلة كما هو مكتوب كما هو نص الملف. ستتمكن من إرسال هذا الملف كمرفق في الرسالة النموذجية.

إرسال نموذج رسالة

اعتمادا على كيفية عملك، يمكنك إرسال نموذج رسالة عبر ESA بطرق مختلفة. يوجد طريقتان على سبيل المثال عبر واجهة سطر الأوامر (CLI) الخاصة بنظام Unix باستخدام البريد أو من Outlook (أو تطبيق بريد إلكتروني آخر).

واجهة سطر الأوامر (CLI) لنظام Unix

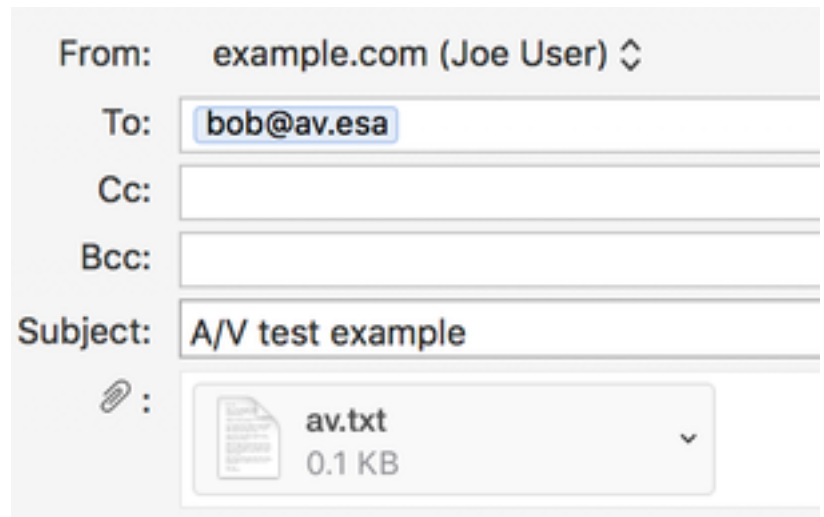
```
joe@unix.local:~$ echo "TEST MESSAGE w/ ATTACHMENT" | mail -s "A/V test example" -A av.txt bob@av.esa
```

يجب إعداد بيئة UNIX بشكل صحيح لإرسال بريد أو ترحيله عبر ESA.

أوت لوك

باستخدام Outlook (أو تطبيق بريد إلكتروني آخر)، لديك خياران في إرسال رمز ASCII عبر: (1) باستخدام ملف txt. الذي تم إنشاؤه، (2) اللصق المباشر لسلسلة ASCII في نص رسالة البريد.

إستخدام ملف txt. كمرفق:



From: example.com (Joe User) ⇅

To: bob@av.esa

Cc:

Bcc:

Subject: A/V test example

📎 : av.txt
0.1 KB

TEST MESSAGE w/ ATTACHMENT

إستخدام سلسلة ASCII في نص رسالة البريد:



From: example.com (Joe User) ⇅

To: bob@av.esa

Cc:

Bcc:

Subject: X5O!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*

يجب إعداد Outlook (أو تطبيق بريد إلكتروني آخر) بشكل صحيح لإرسال بريد أو ترحيله عبر ESA.

التحقق

على واجهة سطر أوامر (ESA (CLI، أستخدم الأمر `tail mail_log` قبل إرسال الرسالة النموذجية. أثناء مشاهدة سجل البريد، سترى الرسالة ممسوحة ضوئياً وملتقطة من قبل McAfee ك "Virus":

```
Wed Sep 13 11:42:38 2017 Info: New SMTP ICID 306 interface Management (10.1.2.84) address
10.1.2.85 reverse dns host zane.local verified yes
Wed Sep 13 11:42:38 2017 Info: ICID 306 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS None country
Australia
Wed Sep 13 11:42:38 2017 Info: Start MID 405 ICID 306
<Wed Sep 13 11:42:38 2017 Info: MID 405 ICID 306 From: <joe@example.com
<Wed Sep 13 11:42:38 2017 Info: MID 405 ICID 306 RID 0 To: <bob@av.esa
'<Wed Sep 13 11:42:38 2017 Info: MID 405 Message-ID '<20170913153801.0EDA1A0121@example.com
'Wed Sep 13 11:42:38 2017 Info: MID 405 Subject 'A/V test attachment
<Wed Sep 13 11:42:38 2017 Info: MID 405 ready 1057 bytes from <joe@example.com
'Wed Sep 13 11:42:38 2017 Info: MID 405 attachment 'av.txt
Wed Sep 13 11:42:38 2017 Info: ICID 306 close
Wed Sep 13 11:42:38 2017 Info: MID 405 matched all recipients for per-recipient policy my_av in
the inbound table
Wed Sep 13 11:42:38 2017 Info: MID 405 interim AV verdict using McAfee VIRAL
'Wed Sep 13 11:42:38 2017 Info: MID 405 antivirus positive 'EICAR test file
Wed Sep 13 11:42:38 2017 Info: MID 405 enqueued for transfer to centralized quarantine "Virus"
((a/v verdict VIRAL
Wed Sep 13 11:42:38 2017 Info: MID 405 queued for delivery
Wed Sep 13 11:42:38 2017 Info: New SMTP DCID 239 interface 10.1.2.84 address 10.1.2.87 port 7025
Wed Sep 13 11:42:38 2017 Info: DCID 239 TLS success protocol TLSv1.2 cipher DHE-RSA-AES256-GCM-
SHA384 the.cpq.host
Wed Sep 13 11:42:38 2017 Info: Delivery start DCID 239 MID 405 to RID [0] to Centralized Policy
Quarantine
Wed Sep 13 11:42:38 2017 Info: Message done DCID 239 MID 405 to RID [0] (centralized policy
(quarantine
'Wed Sep 13 11:42:38 2017 Info: MID 405 RID [0] Response 'ok: Message 49 accepted
Wed Sep 13 11:42:38 2017 Info: Message finished MID 405 done
Wed Sep 13 11:42:43 2017 Info: DCID 239 close
نفس الرسالة التي تم إرسالها من خلال Sophos وفحصها:
```

```
Wed Sep 13 11:44:24 2017 Info: New SMTP ICID 307 interface Management (10.1.2.84) address
10.1.2.85 reverse dns host zane.local verified yes
Wed Sep 13 11:44:24 2017 Info: ICID 307 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS None country
Australia
Wed Sep 13 11:44:24 2017 Info: Start MID 406 ICID 307
<Wed Sep 13 11:44:24 2017 Info: MID 406 ICID 307 From: <joe@example.com
<Wed Sep 13 11:44:24 2017 Info: MID 406 ICID 307 RID 0 To: <bob@av.esa
'<Wed Sep 13 11:44:24 2017 Info: MID 406 Message-ID '<20170913153946.E20C7A0121@example.com
'Wed Sep 13 11:44:24 2017 Info: MID 406 Subject 'A/V test attachment
<Wed Sep 13 11:44:24 2017 Info: MID 406 ready 1057 bytes from <joe@example.com
'Wed Sep 13 11:44:24 2017 Info: MID 406 attachment 'av.txt
Wed Sep 13 11:44:24 2017 Info: ICID 307 close
Wed Sep 13 11:44:24 2017 Info: MID 406 matched all recipients for per-recipient policy my_av in
the inbound table
Wed Sep 13 11:44:24 2017 Info: MID 406 interim AV verdict using Sophos VIRAL
'Wed Sep 13 11:44:24 2017 Info: MID 406 antivirus positive 'EICAR-AV-Test
Wed Sep 13 11:44:24 2017 Info: MID 406 enqueued for transfer to centralized quarantine "Virus"
((a/v verdict VIRAL
Wed Sep 13 11:44:24 2017 Info: MID 406 queued for delivery
Wed Sep 13 11:44:24 2017 Info: New SMTP DCID 240 interface 10.1.2.84 address 10.1.2.87 port 7025
Wed Sep 13 11:44:24 2017 Info: DCID 240 TLS success protocol TLSv1.2 cipher DHE-RSA-AES256-GCM-
SHA384 the.cpq.host
Wed Sep 13 11:44:24 2017 Info: Delivery start DCID 240 MID 406 to RID [0] to Centralized Policy
```

Quarantine

Wed Sep 13 11:44:24 2017 Info: Message done DCID 240 MID 406 to RID [0] (centralized policy

(quarantine

'Wed Sep 13 11:44:24 2017 Info: MID 406 RID [0] Response 'ok: Message 50 accepted

Wed Sep 13 11:44:24 2017 Info: Message finished MID 406 done

Wed Sep 13 11:44:29 2017 Info: DCID 240 close

في هذا المختبر ESA، تم تكوين "الرسائل المصابة بالفيروسات" لإجراء عزل "الإجراء المطبق على الرسالة" على نهج البريد المحدد. قد يختلف الإجراء الخاص بـ ESA الخاص بك، بناءً على الإجراء المتخذ للرسائل المصابة بفيروس التي يعالجها برنامج مكافحة الفيروسات على نهج البريد الخاص بك.

معلومات ذات صلة

• [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن م دخت س م ل ل م عد ي و ت م م م دقت ل ة يرش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م م مچرت م ا م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا