Anti-Virus 엔진이 Cisco ESA(Email Security Appliance)에서 스캐닝되고 있는지 확인하기 위해 샘플 메시지를 보내는 방법

목차

[소개](#)
[Anti-Virus 엔진이 Cisco ESA(Email Security Appliance)에서 스캐닝되고 있는지 확인하기 위해 샘플 메시지를 보내는 방법](#)
[TXT 파일 만들기](#)
[샘플 메시지 보내기](#)
[UNIX CLI](#)
[Outlook](#)
[확인](#)
[관련 정보](#)

소개

이 문서에서는 Sophos 안티바이러스 또는 McAfee 안티바이러스 엔진이 Cisco ESA(Email Security Appliance)에서 스캐닝되고 있는지 확인하기 위해 샘플 메시지를 보내는 방법에 대해 설명합니다.

Anti-Virus 엔진이 Cisco ESA(Email Security Appliance)에서 스캐닝되고 있는지 확인하기 위해 샘플 메시지를 보내는 방법

ESA를 통해 테스트 바이러스 페이로드와 함께 샘플 메시지를 전송하면 Sophos 또는 McAfee 안티바이러스 엔진을 트리거할 수 있습니다. 이 문서에 나열된 단계를 수행하기 전에 수신 또는 발신 메일 정책을 설정하고 안티바이러스 삭제 또는 바이러스 감염 메시지를 격리하도록 메일 정책을 구성해야 합니다. 이 문서에서는 테스트 바이러스를 첨부 파일으로 시뮬레이션하는 EICAR(www.eicar.org)에서 제공하는 ASCII 코드를 사용합니다.

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

> **참고:**EICAR별: *이 테스트 파일은 EICAR에 "EICAR Standard Anti-Virus Test File(EICAR 표준 안티바이러스 테스트 파일)"로 배포하기 위해 제공되었으며 위에 나열된 모든 기준을 충족합니다.바이러스가 아니며 바이러스 코드의 어떤 조각도 포함하지 않기 때문에 그것은 돌아다니는 것이 안전합니다.대부분의 제품은 바이러스와 같이 반응합니다(일반적으로 "EICAR-AV-Test"와 같이 명백한 이름으로 보고함).*

TXT 파일 만들기

위의 ASCII 문자열을 사용하여 .txt 파일을 만들고 파일 본문으로 작성된 문자열을 배치합니다. 이 파일을 샘플 메시지의 첨부 파일로 보낼 수 있습니다.

샘플 메시지 보내기

작업 방법에 따라 ESA를 통해 다양한 방법으로 샘플 메시지를 보낼 수 있습니다. **메일** 또는 Outlook(또는 기타 이메일 애플리케이션)을 사용하는 UNIX CLI를 통한 두 가지 예제 방법이 있습니다.

UNIX CLI

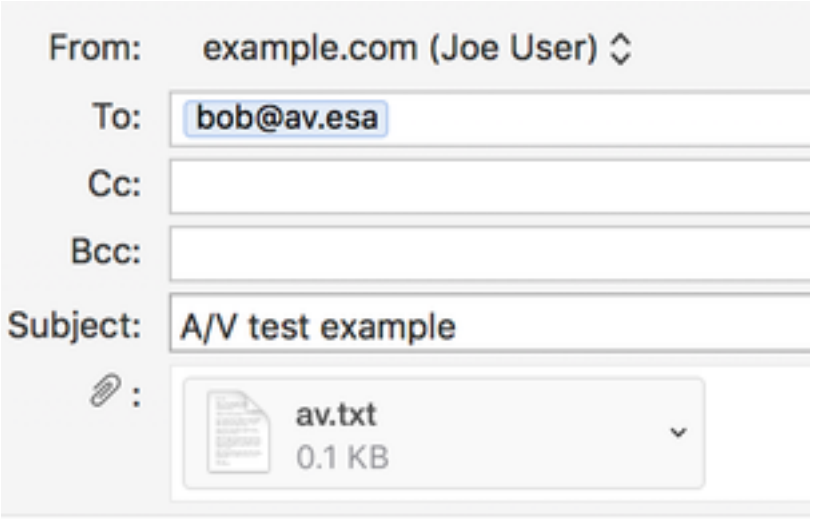
```
joe@unix.local:~$ echo "TEST MESSAGE w/ ATTACHMENT" | mail -s "A/V test example" -A av.txt
bob@av.esa
```

ESA를 통해 메일을 보내거나 릴레이하려면 UNIX 환경을 올바르게 설정해야 합니다.

Outlook

Outlook(또는 다른 이메일 애플리케이션)을 사용하면 다음을 통해 ASCII 코드를 전송할 때 두 가지 선택 사항이 있습니다.1) 생성된 .txt 파일을 사용하여 2) 메일 메시지 본문에 있는 ASCII 문자열의 직접 붙여넣기

.txt 파일을 첨부 파일로 사용:




```
TEST MESSAGE w/ ATTACHMENT
```

메일 메시지 본문에서 ASCII 문자열 사용:

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

ESA를 통해 메일을 보내거나 릴레이하려면 Outlook(또는 기타 이메일 애플리케이션)을 올바르게 설정해야 합니다.

확인

ESA CLI에서 **tail mail_logs** 명령을 사용하여 샘플 메시지를 전송합니다. 메일 로그를 시청하는 동안 메시지가 스캔되어 McAfee에 의해 "VIRAL"로 포착되는 것을 볼 수 있습니다.

```
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
```

Sophos에서 보내고 스캔한 동일한 메시지:

```
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
```

이 Lab ESA에서 'Virus Infected Messages'는 특정 메일 정책의 "Action Applied to Message(메시지에 적용된 작업)"를 격리하도록 구성됩니다. ESA에 대한 작업은 메일 정책에서 안티바이러스로 처리되는 바이러스 감염 메시지에 대해 수행한 작업에 따라 달라질 수 있습니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems