ESA에서 고정 파일 평판 호스트 또는 대체 파일 평판 클라우드 서버 풀 구성

목차

소개

이 문서에서는 AMP(Advanced Malware Protection)를 사용하여 고정 호스트 또는 파일 평판용 대체 평판 클라우드 서버 풀을 통신하고 사용하도록 Cisco ESA(Email Security Appliance)를 구성하는 방법에 대해 설명합니다.

배경 정보

File Reputation(파일 평판) 쿼리는 ESA에서 AMP를 위한 2개의 레이어 중 첫 번째입니다. File Reputation(파일 평판)은 ESA를 통과하는 각 파일의 핑거프린트를 캡처하여 평판 판정을 위해 AMP의 클라우드 기반 인텔리전스 네트워크에 전송합니다.이러한 결과를 바탕으로 ESA 관리자는 악성 파일을 자동으로 차단하고 관리자가 정의한 정책을 적용할 수 있습니다. File Reputation 클라우드 서비스는 Amazon Web Services(AWS)에서 호스팅됩니다. 이 문서에 설명된 호스트 이름에 대해 DNS 쿼리를 수행하면 ".amazonaws.com"이 나열됩니다.

ESA의 두 번째 AMP 레이어는 파일 분석입니다. 이 문서에서는 다루지 않습니다.

파일 평판 트래픽에 대한 SSL 통신에서는 기본적으로 포트 32137을 사용합니다.서비스 컨피그레이션 시 포트 443을 대안으로 사용할 수 있습니다.자세한 내용은 ESA 사용 설명서, "파일 평판 필터링 및 파일 분석" 섹션을 참조하십시오.ESA 및 네트워크 관리자는 구성을 진행하기 전에 IP 주소, IP 위치, 포트 통신(32137 대 443)에 대한 풀 연결을 확인할 수 있습니다.

기본 AMERICAS(레거시) 평판 클라우드 서버 풀(cloud-sa.amp.sourcefire.com)

파일 평판이 ESA에서 라이센스, 활성화 및 구성되면 기본적으로 이 평판 클라우드 서버 풀에 대해 설정됩니다.

- AMERICAS(레거시)(cloud-sa.amp.sourcefire.com)

호스트 이름 "cloud-sa.amp.sourcefire.com"은 DNS CNAME(Canonical Name Record)입니다. CNAME은 도메인 이름이 다른 도메인의 별칭임을 지정하는 데 사용되는 DNS의 리소스 레코드 유형이며, 이는 "canonical" 도메인입니다.이 CNAME에 연결된 풀의 연결된 호스트 이름은 다음과 같을 수 있습니다.

- ec2-107-22-180-78.compute-1.amazonaws.com(107.22.180.78)
- ec2-54-225-142-100.compute-1.amazonaws.com(54.225.142.100)
- ec2-23-21-208-4.compute-1.amazonaws.com(23.21.208.4)
- ec2-54-83-195-228.compute-1.amazonaws.com(54.83.195.228)

두 가지 파일 평판 서버 선택 사항이 추가로 있습니다.

- 미주(cloud-sa.amp.cisco.com)
- 유럽(cloud-sa.eu.amp.cisco.com)

이 두 서버 모두 이 문서의 "정적 파일 평판 서버 호스트 이름(.cisco.com)" 섹션에서 다룹니다.

이 **검색** 또는 nslookup 쿼리를 실행할 때 언제든지 네트워크에서 AMERICAS cloud-sa-amp.sourcefire.com CNAME과 연결된 호스트를 확인할 수 있습니다.

```
$ dig cloud-sa.amp.sourcefire.com +short
cloud-sa-589592150.us-east-1.elb.amazonaws.com.
107.22.180.78
54.225.208.214
23.21.208.4
54.83.195.228

$ nslookup cloud-sa.amp.sourcefire.com
Server: 208.67.222.222
Address: 208.67.222.222#53

Non-authoritative answer:
cloud-sa.amp.sourcefire.com canonical name = cloud-sa-589592150.us-east-1.elb.amazonaws.com.
Name: cloud-sa-589592150.us-east-1.elb.amazonaws.com
Address: 54.225.208.214
Name: cloud-sa-589592150.us-east-1.elb.amazonaws.com
Address: 54.83.195.228
Name: cloud-sa-589592150.us-east-1.elb.amazonaws.com
Address: 107.22.180.78
Name: cloud-sa-589592150.us-east-1.elb.amazonaws.com
Address: 23.21.208.4
```

> **참고:**이러한 호스트는 정적이지 않으며 이러한 호스트만 기준으로 ESA 파일 평판 트래픽을 제한하지 않는 것이 좋습니다.풀의 호스트가 예고 없이 변경되므로 쿼리 결과는 달라질 수 있습니다.

이 타사 툴에서 IP 지리적 위치를 확인할 수 있습니다.

- http://geoiplookup.net/ip/107.22.180.78
- http://geoiplookup.net/ip/54.225.208.214
- http://geoiplookup.net/ip/23.21.208.4
- http://geoiplookup.net/ip/54.83.195.228

정적 파일 평판 서버 호스트 이름(.cisco.com)

Cisco는 2016년부터 AMP용 파일 평판 서비스에 대해 ".cisco.com" 기반 호스트 이름을 제공하기 시작했습니다. 이 기능에서는 파일 평판에 사용할 수 있는 정적 호스트 이름 및 IP 주소가 있습니다.

- cloud-sa.amp.cisco.com(북미 - 미국)
- cloud-sa.eu.amp.cisco.com(유럽 - 아일랜드 공화국)
- cloud-sa.apjc.amp.cisco.com(아시아 태평양 - 일본)

네트워크에서 호스트 및 관련 IP 주소를 확인하고 **dig** 또는 nslookup 쿼리를 실행할 수 있습니다.

북미(미국):

```
$ dig cloud-sa.amp.cisco.com +short
52.21.117.50
```

유럽(아일랜드):

```
$ nslookup cloud-sa.eu.amp.cisco.com
Server: 208.67.222.222
Address: 208.67.222.222#53

Non-authoritative answer:
Name: cloud-sa.eu.amp.cisco.com
Address: 52.30.124.82
```

아시아 태평양(일본):

```
 $ dig cloud-sa.apjc.amp.cisco.com +short
52.69.39.127
```

이 타사 툴에서 IP 지리적 위치를 확인할 수 있습니다.

- http://geoiplookup.net/ip/52.21.117.50
- http://geoiplookup.net/ip/52.30.124.82
- http://geoiplookup.net/ip/52.69.39.127

현재 ".sourcefire.com" 호스트 이름을 해제할 계획이 없습니다.

대체 유럽 평판 클라우드 서버 풀(cloud-sa.eu.amp.sourcefire.com)

EU 기반 전용 서버 및 데이터 센터로 특정 트래픽을 전송해야 하는 EU(European Union) 기반 고객의 경우, 관리자는 EU 고정 호스트 또는 EU 평판 클라우드 서버 풀을 가리키도록 ESA를 구성할 수 있습니다.

- cloud-sa-eu.amp.cisco.com
- cloud-sa.eu.am.sourcefire.com

기본 호스트 이름 "cloud-sa.amp.sourcefire.com"과 마찬가지로 호스트 이름 "cloud-sa.eu.amp.sourcefire.com"도 CNAME입니다. 이 CNAME에 연결된 풀의 연결된 호스트 이름은 다음과 같을 수 있습니다.

- ec2-54-217-245-97.eu-west-1.compute.amazon.com(54.217.245.97)
- ec2-54-247-186-153.eu-west-1.compute.amazon.com(54.247.186.153)
- ec2-176-34-122-245.eu-west-1.compute.amazon.com(176.34.122.245)

네트워크에서 EUROPEAN cloud-sa.eu.amp.sourcefire.com CNAME에 연결된 호스트를 확인하고 **dig 또는 nslookup** 쿼리를 실행할 수 있습니다.

```
$ dig cloud-sa.eu.amp.sourcefire.com +short
cloud-sa-162723281.eu-west-1.elb.amazonaws.com.
54.217.245.97
54.247.186.153
176.34.122.245

$ nslookup cloud-sa.eu.amp.sourcefire.com
Server: 208.67.222.222
Address: 208.67.222.222#53

Non-authoritative answer:
cloud-sa.eu.amp.sourcefire.com canonical name = cloud-sa-162723281.eu-west-1.elb.amazonaws.com.
Name: cloud-sa-162723281.eu-west-1.elb.amazonaws.com
Address: 54.247.182.97
Name: cloud-sa-162723281.eu-west-1.elb.amazonaws.com
Address: 176.34.122.245
Name: cloud-sa-162723281.eu-west-1.elb.amazonaws.com
Address: 54.247.186.153
```

> **참고:**이러한 호스트는 정적 호스트가 아니며 이러한 호스트에만 기반하여 ESA 파일 평판 트래픽을 제한하지 않는 것이 좋습니다.풀의 호스트가 예고 없이 변경되므로 쿼리 결과는 달라질 수 있습니다.

이 타사 툴에서 IP 지리적 위치를 확인할 수 있습니다.

- http://geoiplookup.net/ip/176.34.122.245
- http://geoiplookup.net/ip/54.247.186.153
- http://geoiplookup.net/ip/54.217.245.97

ESA에서 고정 파일 평판 호스트 또는 대체 파일 평판 클라우드 서버 풀 구성

파일 평판은 ESA의 GUI 또는 CLI에서 구성할 수 있습니다.이 문서에 나열된 구성 단계는 CLI 컨피그레이션을 보여줍니다.그러나 GUI를 통해 동일한 단계 및 정보를 적용할 수 있습니다(**Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석) > Edit Global Settings(전역 설정 편집)... > Advanced Settings for File Reputation(파일 평판 고급 설정)**.

AsyncOS 10.x 이상

AsyncOS 10.x의 새로운 기능을 통해 프라이빗 평판 클라우드(온프레미스 파일 평판 서버) 또는 클라우드 기반 파일 평판 서버를 사용하도록 ESA를 구성할 수 있습니다.이 변경을 통해 AMP 컨피그레이션에서는 더 이상 "Enter reputation cloud server pool(평판 클라우드 서버 풀 입력)" 단계를 사용하여 호스트 이름을 묻는 메시지가 표시되지 않습니다.추가 파일 평판 서버를 프라이빗 평판 클라우드로 설정하고 해당 호스트 이름에 대한 공개 키를 제공하도록 선택해야 합니다.

10.0.x 이상의 경우 대체 AMP 평판 서버를 구성할 때 해당 호스트 이름과 연결된 공개 키를 입력해야 할 수도 있습니다.

모든 AMP 평판 서버는 동일한 공개 키를 사용합니다.

```
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEchIap1VqPuGibM2n3wjfhqQZdzC9
WI1Z7QZ2Q7VesLe+A53TxYujeo7fCDKJEQKrPjU6kI36PSZusObr9Cur/g==
-----END PUBLIC KEY-----
```

이 예에서는 cloud-sa.eu.amp.sourcefirce.com으로 대체 파일 평판 서버를 설정하는 데 도움이 됩니다.

```
my11esa.local > ampconfig

NOTICE: This configuration command has not yet been configured for the current cluster mode
(Machine 122.local).

What would you like to do?
1. Switch modes to edit at mode "Cluster Test_cluster".
2. Start a new, empty configuration at the current mode (Machine 122.local).
3. Copy settings from another cluster mode to the current mode (Machine 122.local).
[1]>

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable
Other potentially malicious file types
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
- CLUSTERSET - Set how advanced malware protection is configured in a cluster.
- CLUSTERSHOW - Display how advanced malware protection is configured in a cluster.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[2]>

Enter AMP reputation server hostname or IP address?
[]> cloud-sa.eu.amp.sourcefire.com

Do you want to input new public key? [N]> y

Paste the public key followed by a . on a new line
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEchIap1VqPuGibM2n3wjfhqQZdzC9
WI1Z7QZ2Q7VesLe+A53TxYujeo7fCDKJEQKrPjU6kI36PSZusObr9Cur/g==
-----END PUBLIC KEY-----
.
Enter cloud domain?
[a.immunet.com]>
```

```
Do you want use the recommended reputation threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [Y]>

Please make sure you have added the Amp onprem reputation server CA certificate in certconfig-
>CERTAUTHOROTIES->CUSTOM
Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private analysis cloud
[1]>
```

컨피그레이션 변경 사항을 커밋합니다.

AsyncOS 9.7.x 이하

AsyncOS 9.7.2-065 for Email Security의 다음 예에서는 cloud-sa.eu.amp.sourcefire.com의 대체 평판 클라우드 서버 풀을 시작하는 데 도움이 됩니다.

```
my97esa.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable
Other potentially malicious file types
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Enter cloud domain?
[a.immunet.com]>

Enter reputation cloud server pool?
[cloud-sa.amp.sourcefire.com]> cloud-sa.eu.amp.sourcefire.com

Do you want use the recommended reputation threshold from cloud service? [Y]>

Choose a file analysis server:
```

```
1. AMERICAS (https://panacea.threatgrid.com)
2. Private Cloud
[1]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [Y]>

Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>
```

컨피그레이션 변경 사항을 커밋합니다.

온프레미스 파일 평판 서버(FireAMP Private Cloud)

AsyncOS 10.x for Email Security에서 시작되는 온프레미스 파일 평판 서버(FireAMP Private Cloud라고도 함)를 사용했습니다.

네트워크에 Cisco AMP Virtual Private Cloud 어플라이언스를 구축한 경우, 이제 메시지 첨부 파일을 퍼블릭 평판 클라우드로 전송하지 않고 파일 평판을 쿼리할 수 있습니다.온프레미스 파일 평판 서버를 사용하도록 어플라이언스를 구성하려면 ESA 사용 설명서 또는 온라인 도움말의 "파일 평판 필터링 및 파일 분석" 장을 참조하십시오.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

구성된 고정 호스트 또는 평판 클라우드 서버 풀로 전달되는 File Reputation 트래픽을 보려면 지정된 필터를 사용하여 ESA에서 패킷 캡처를 수행하여 포트 32137 또는 포트 443 트래픽을 캡처합니다.

이 예에서는 cloud-sa.eu.amp.sourcefire.com 클라우드 서버 풀 및 포트 443 사용을 위한 SSL 통신을 사용합니다.

이는 AMP 로그에서 ESA에 기록됩니다.

```
Sun Mar 26 21:17:45 2017 Info: File reputation query initiating. File Name =
'contract_604418.doc', MID = 463, File Size = 139816 bytes, File Type = application/msword
Sun Mar 26 21:17:46 2017 Info: Response received for file reputation query from Cloud. File Name
= 'contract_604418.doc', MID = 463, Disposition = MALICIOUS, Malware = W32.8A78D308C9-95.SBX.TG,
Reputation Score = 99, sha256 =
8a78d308c96ff5c7158ea1d6ca25f3546fae8515d305cd699eab2d2ef3c08745, upload_action = 2
```

실행 중인 ESA 패킷 추적으로 이 대화를 캡처했습니다.

```
1060 28.504624 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 74 51391
443 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 WS=64 SACK_PERM=1 TSval=198653388 TSecr=0
1072 28.594265 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 74 443
```

```
51391 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval=142397924
TSecr=198653388 WS=256
1073 28.594289 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=1 Ack=1 Win=16384 Len=0 TSval=198653478 TSecr=142397924
1074 28.595264 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com SSL 502
Client Hello
1085 28.685554 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 66 443
51391 [ACK] Seq=1 Ack=437 Win=30208 Len=0 TSval=142397947 TSecr=198653478
1086 28.687344 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TLSv1 1434
Server Hello
1087 28.687378 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=437 Ack=1369 Win=15040 Len=0 TSval=198653568 TSecr=142397947
1088 28.687381 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 146 [TCP
segment of a reassembled PDU]
1089 28.687400 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=437 Ack=1449 Win=14912 Len=0 TSval=198653568 TSecr=142397947
1090 28.687461 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 1434 [TCP
segment of a reassembled PDU]
1091 28.687475 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=437 Ack=2817 Win=13568 Len=0 TSval=198653568 TSecr=142397947
1092 28.687479 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 1346 [TCP
segment of a reassembled PDU]
1093 28.687491 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=437 Ack=4097 Win=12288 Len=0 TSval=198653568 TSecr=142397947
1094 28.687614 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 [TCP
Window Update] 51391  443 [ACK] Seq=437 Ack=4097 Win=16384 Len=0 TSval=198653568 TSecr=142397947
1096 28.711945 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TLSv1 1120
Certificate
1097 28.711973 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=437 Ack=5151 Win=15360 Len=0 TSval=198653594 TSecr=142397953
1098 28.753074 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TLSv1 392
Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1099 28.855886 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TLSv1 348 New
Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1100 28.855934 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=763 Ack=5433 Win=16128 Len=0 TSval=198653740 TSecr=142397989
1101 28.856555 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TLSv1 252
Application Data, Application Data
1104 28.952344 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TLSv1 252
Application Data, Application Data
1105 28.952419 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=949 Ack=5619 Win=16192 Len=0 TSval=198653837 TSecr=142398013
1106 28.958953 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TLSv1 300
Application Data, Application Data
1107 29.070057 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TLSv1 268
Application Data, Application Data
1108 29.070117 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=1183 Ack=5821 Win=16192 Len=0 TSval=198653951 TSecr=142398043
1279 59.971986 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TLSv1 103
Encrypted Alert
1280 59.972030 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=1183 Ack=5858 Win=16320 Len=0 TSval=198684848 TSecr=142405768
1281 59.972034 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 66 443
51391 [FIN, ACK] Seq=5858 Ack=1183 Win=33280 Len=0 TSval=142405768 TSecr=198653951
1282 59.972044 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=1183 Ack=5859 Win=16320 Len=0 TSval=198684848 TSecr=142405768
1283 59.972392 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TLSv1 103
Encrypted Alert
1284 59.972528 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [FIN, ACK] Seq=1220 Ack=5859 Win=16384 Len=0 TSval=198684848 TSecr=142405768
1285 60.062083 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 66 443
51391 [ACK] Seq=5859 Ack=1221 Win=33280 Len=0 TSval=142405791 TSecr=198684848
```

트래픽은 포트 443을 통해 통신합니다. ESA(my11esa.local)에서 호스트 이름 ec2-176-34-122-

245.eu-west-1.compute.amazon.com으로 통신합니다.이 호스트 이름은 IP 주소 176.34.122.245:

```
$ dig ec2-176-34-122-245.eu-west-1.compute.amazonaws.com +short
176.34.122.245
```

176.34.122.245의 IP 주소는 cloud-sa.eu.amp.sourcefire.com의 CNAME 풀 멤버입니다.

```
$ dig cloud-sa.eu.amp.sourcefire.com +short
cloud-sa-162723281.eu-west-1.elb.amazonaws.com.
54.217.245.200
54.247.186.153
176.34.122.245
```

이 예에서는 구성된 평판 클라우드 서버 풀인 cloud-sa.eu.amp.sourcefire.com에서 통신을 지정하고 수락했습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

텔넷을 사용하여 연결 테스트

File Reputation 클라우드에 대한 포트 레벨 연결을 확인하려면 구성된 평판 클라우드 서버 풀의 호스트 이름을 사용하고 포트 32137 또는 포트 443에 대한 **텔넷**으로 테스트합니다.

```
my97esa.local> telnet cloud-sa.amp.sourcefire.com 443

Trying 23.21.208.4...
Connected to ec2-23-21-208-4.compute-1.amazonaws.com.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

EU에 대한 연결 확인, 포트 443에서 성공:

```
my97esa.local> telnet cloud-sa.eu.amp.sourcefire.com 443

Trying 176.34.113.72...
Connected to ec2-176-34-113-72.eu-west-1.compute.amazonaws.com.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

EU에 대한 연결 확인, 포트 32137을 통해 연결할 수 없음:

```
my97esa.local> telnet cloud-sa.eu.amp.sourcefire.com 32137

Trying 176.34.113.72...
telnet: connect to address 176.34.113.72: Operation timed out
telnet: Unable to connect to remote host
```

포트 32137 또는 포트 443을 사용하여 동일한 텔넷 테스트 방법으로 평판 클라우드 서버 풀의 CNAME 뒤에 있는 직접 IP 또는 호스트 이름에 대한 텔넷을 테스트할 수 있습니다. 호스트 이름 및 포트에 성공적으로 텔넷할 수 없는 경우 ESA 외부에 있는 네트워크 연결과 방화벽 설정을 확인해

야 할 수 있습니다.

온프레미스 파일 평판 서버에 대한 텔넷 성공 확인은 표시된 것과 동일한 프로세스를 통해 수행됩니다.

공개 키 입력

AsyncOS 10.x 이상을 실행하는 ESA에 공개 키를 입력할 때 공개 키를 붙여넣거나 로드하는 데 성공했는지 확인합니다.공개 키의 오류가 컨피그레이션 출력에 표시됩니다.

```
Do you want to input new public key? [N]> y

Paste the public key followed by a . on a new line
-----BEGIN PUBLIC KEY-----
MEAwEAYHKoZIzj0CAQYFK4EEAAEDLAAEAIHPMkqCH057gxeQK6aUKqmpqk+1AW0u
vxOkpuI+gtfLICRijTx3Vh45
-----END PUBLIC KEY-----
.
Failed to save public key
```

오류가 발생하면 구성을 다시 시도하십시오.지속적인 오류에 대해서는 Cisco 지원에 문의하십시오.

AMP 로그 검토

ESA에서 AMP 로그를 볼 때 파일 평판 쿼리 시 지정된 "클라우드에서 파일 평판 쿼리"가 표시되는지 확인합니다.

```
Sun Mar 26 11:28:13 2017 Info: File reputation query initiating. File Name =
'billing_fax_271934.doc', MID = 458, File Size = 143872 bytes, File Type = application/msword
Sun Mar 26 11:28:14 2017 Info: Response received for file reputation query from Cloud. File Name
= 'billing_fax_271934.doc', MID = 458, Disposition = MALICIOUS, Malware = W32.50944E2888-
100.SBX.TG, Reputation Score = 0, sha256 =
50944e2888b551f41f3de2fc76b4b57cb3cd28e718c9265c43128568916fe70f, upload_action = 2
```

이 메시지가 표시되면 쿼리는 로컬 ESA 캐시에서 응답을 가져온 것이며 구성된 평판 클라우드 서버 풀에서 응답하지 않습니다.

```
Sun Mar 26 11:30:18 2017 Info: File reputation query initiating. File Name =
'billing_fax_271934.doc', MID = 459, File Size = 143872 bytes, File Type = application/msword
Sun Mar 26 11:30:18 2017 Info: Response received for file reputation query from Cache. File Name
= 'billing_fax_271934.doc', MID = 459, Disposition = MALICIOUS, Malware = W32.50944E2888-
100.SBX.TG, Reputation Score = 0, sha256 =
50944e2888b551f41f3de2fc76b4b57cb3cd28e718c9265c43128568916fe70f, upload_action = 2
```

추가 오류 및 경고

ESA 관리자가 이 알림을 받을 수 있습니다.이 메시지가 수신되면 구성 및 확인 프로세스를 다시 수행합니다.

```
The Warning message is:
```

```
amp The previously selected regional server cloud-sa.eu.amp.sourcefire.com is unavailable.
Server cloud-sa.amp.sourcefire.com has been selected as default.

Version: 11.0.0-028
Serial Number: 1111CEE15FF3A9F9A1111-1AAA2CF4A1A1
Timestamp: 26 Mar 2017 11:09:29 -0400
```

관련 정보

- 적절한 AMP 작업을 위한 필수 서버 주소
- 기술 지원 및 문서 – Cisco Systems