# Statische File Reputation Host of een alternatieve Cloud Server-uploadtoken instellen op ESA

## Inhoud



## Inleiding

Dit document beschrijft hoe u een Cisco e-mail security applicatie (ESA) kunt configureren om een statische host of een alternatieve reputatieswolk server pool te communiceren en te gebruiken voor File Reputation met behulp van Advanced Malware Protection (AMP).

## Achtergrondinformatie

Een File Reputation query is de eerste van twee lagen voor AMP op het ESA. File Reputation vangt een vingerafdruk van elk bestand op terwijl het het ESA overgaat en stuurt het naar het cloudgebaseerd inlichtingennetwerk van AMP voor een reputatieoordeel. Gezien deze resultaten kunnen ESA beheerders automatisch kwaadaardige bestanden blokkeren en beheerder-gedefinieerd beleid toepassen.  De cloudservice voor bestandsrevaluatie wordt georganiseerd op Amazon Web Services (AWS). Wanneer u DNS-vragen uitvoert tegen de hostname(en) die in dit document is beschreven, ziet u de lijst ".amazonaws.com".

De tweede laag AMP op het ESA is File Analysis.  Dat wordt in dit document niet behandeld.

SSL-communicatie voor verkeer met File Reputation gebruikt standaard poort 32137. Ten tijde van de configuratie van de dienst kan haven 443 als alternatief worden gebruikt. Raadpleeg de sectie ESR-gebruikershandleiding, "File Reputation Filtering and File Analysis" voor volledige

informatie. De ESA en de Netwerkbeheerders zouden de connectiviteit met de pool kunnen verifiëren voor IP-adres(en), IP-locatie en ook poortcommunicatie (32137 vs. 443) voordat ze verdergaan met de configuratie.

## Standaard AMERIKAS (Legacy) reputatieswolkenpool (cloud-sa.amp.sourcefire.com)

Nadat File Reputation is toegestaan, ingeschakeld en ingesteld op een ESA, wordt deze standaard ingesteld voor deze reputatieswolkenserver pool:

- AMERIKAS (Legacy) (cloud-sa.amp.sourcefire.com)

De hostname "cloud-sa.amp.sourcefire.com" is een DNS Canonical Name record (CNAME). Een CNAME is een type resource record in DNS dat wordt gebruikt om aan te geven dat een domeinnaam een alias is voor een ander domein, het "canonical"-domein. De geassocieerde hostnamen in de pool die aan deze CNAME is gekoppeld, kunnen gelijk zijn aan:

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

Er zijn twee extra opties voor de bestands reputatie die kunnen worden geselecteerd:

- AMERIKAS (cloud-sa.amp.cisco.com)
- EUROPA (cloud-sa.eu.am)

Beide servers vallen onder het gedeelte "Static File Reputation server hostname (.cisco.com)" van dit document.

U kunt op elk moment wanneer u deze query voor het **graven** of **nslookup-**vraag uitvoert de hosts verifiëren die zijn gekoppeld aan de CNAME van AMERICAS-cloud-sa-amp.sourcefire.com:

```
$ 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
```

> Opmerking: Deze hosts zijn NIET statisch en het wordt aanbevolen het ESR-verkeer niet te beperken op basis van alleen deze hosts. De resultaten van uw query kunnen variëren,

omdat de hosts in de pool zonder kennisgeving zullen veranderen.

U kunt de IP-geografische locatie vanuit dit gereedschap van derden controleren:

- 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

## Statische bestands discodernamen (.cisco.com)

Cisco begon in 2016 op ".cisco.com" gebaseerde hostname voor de service File Reputation voor AMP te bieden. Er zijn statische hostname en IP-adressen beschikbaar voor File Reputation uit deze pagina:

- cloud-sa.amp.cisco.com (Noord-Amerika - VS)
- cloud-sa.eu.amp.cisco.com (Europa - Republiek Ierland)
- cloud-sa.apjc.amp.cisco.com (Azië Pacific - Japan)

U kunt de hosts en bijbehorende IP-adressen van uw netwerk controleren en een vraag **over** het **opzoeken van een** site uitvoeren:

Noord-Amerika (VS):

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

Europa (Republiek Ierland):

```
$ 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
```

Zuidoost-Azië (Japan):

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

U kunt de IP-geografische locatie vanuit dit gereedschap van derden controleren:

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

Op dat moment zijn er geen plannen om de hostname ".sourcefire.com" uit te schakelen.

## Alternatieve Europese reputatieswolkenserver-pool (cloud-sa.eu.amp.sourcefire.com)

Voor klanten in de Europese Unie (EU) die specifieke verkeersstromen naar uitsluitend in de EU gevestigde servers en datacentra moeten doorsturen, kunnen beheerders het ESA configureren om te verwijzen naar de statische EU-gastheer of naar de reputatie van de EU-cloudserver:

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

Net als de standaard hostname "cloud-sa.amp.sourcefire.com" is de hostname "cloud-sa.eu.amp.sourcefire.com" ook een CNAME. De geassocieerde hostnamen in de pool die aan deze CNAME is gekoppeld, kunnen vergelijkbaar zijn met:

- eg2-54-217-245-97.eu-west-1.computer.amazonaws.com (54.217.245.97)
- eg2-54-247-186-153.eu-west-1.computer.amazonaws.com (54.247.186.153)
- eg2-176-34-122-245.eu-west-1.computer.amazonaws.com (176.34.122.245)

U kunt de hosts controleren die zijn gekoppeld aan de EUROPEAN cloud-sa.eu.amp.sourcefire.com-naam van uw netwerk en een **dig** of **nslookup-**query uitvoeren::

```
$ 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
```

> Opmerking: Deze hosts zijn NIET statisch en het wordt aanbevolen het reactieverkeer van ESR-bestanden niet te beperken op basis van alleen deze hosts. De resultaten van uw query kunnen variëren, omdat de hosts in de pool zonder kennisgeving zullen veranderen.

U kunt de IP-geografische locatie vanuit dit gereedschap van derden controleren:

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

## Statische File Reputation Host of een alternatieve Cloud Server-uploadtoken instellen op ESA

File Reputation kan worden ingesteld vanuit de GUI of de CLI in het ESR. De configuratiestappen in dit document zullen de CLI-configuratie aantonen. Dezelfde stappen en informatie kunnen echter ook worden toegepast via de GUI (**Security Services > File Reputation and Analysis > Global Settings.. > Advanced Settings voor File Reputation**).

## AsyncOS 10.x en nieuwer

Dankzij de nieuwe functies van AsyncOS 10.x kan het ESA worden ingesteld om een privéreputatieswolk (On-Premises File Reputation Server) of een op de cloud gebaseerde bestands reputatieserver te gebruiken. Met deze verandering leidt AMP configuratie niet langer tot de hostname met de "Voer reputatie cloud pool" stap in. U moet ervoor kiezen de extra server voor de bestands reputatie op te zetten als een privéreputatieswolk en de openbare sleutel voor die hostname te verstrekken.

Voor 10.0.x en nieuwer, wanneer u een alternatieve AMP reputatieserver vormt, zou u een openbare sleutel verbonden aan die hostname kunnen moeten ingaan.

Alle reputatieservers van AMP gebruiken dezelfde openbare sleutel:

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

Dit voorbeeld zal u helpen om de alternatieve server van de bestands reputatie aan cloud-sa.eu.amp.sourcefirce.com op te zetten:

```
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]>
```

Stel alle configuratiewijzigingen in.

## AsyncOS 9.7.x en eerder

Dit voorbeeld op AsyncOS 9.7.2-065 voor e-mail security zal u helpen om de alternatieve reputatie van de cloudserver aan cloud-sa.eu.amp.sourcefirce.com op te waarderen:

```
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]>
```

Stel alle configuratiewijzigingen in.

# Premises File Reputation Server (FireAMP Private Cloud)

Het gebruik van een server met bestands reputatie, ook bekend als een FireAMP Private Cloud, werd geïntroduceerd die begon met AsyncOS 10.x voor e-mail security.

Als u een Cisco Advanced Malware Protection Virtual Private Cloud Appliance op uw netwerk hebt ingezet, kunt u de bestands reputatie van berichtbijlagen nu vragen zonder ze naar de openbare reputatieswolk te verzenden. Zie het hoofdstuk "Filtering en bestandsanalyse" in de ESR-gebruikershandleiding of online help voor informatie over de configuratie van uw wasmachine met een server die bekend is als u een bestands-reputatie wilt gebruiken.

# Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Om het verkeer van de Bestandsreutatie dat naar de geconfigureerde statische host- of reputatieswolkenpool wordt doorgegeven, voert u een pakketvastlegging uit van het ESA met een gespecificeerd filter om poort 32137 of poort 443-verkeer op te nemen.

Gebruik bijvoorbeeld de cloudserverpool cloud-sa.eu.am en de SSL-communicatie met het gebruik van poort 443...

Dit staat in de logboeken van het AMP aan het ESA gelogd:

```
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
```

Tijdens het ESA pakkettransport dat actief was werd dit gesprek opgenomen:

```
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
```

Het verkeer communiceert via poort 443. Vanuit onze ESA (my11esa.local) communiceert het met de hostname ec2-176-34-122-245.eu-west-1.computer.amazonaws.com. Deze hostname is verbonden met het IP-adres 176.34.122.245:

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

Het IP-adres van 176.34.122.245 is een gezamenlijk lid van de CNAME voor cloud-sa.eu.amp.sourcefire.com:

```
$ 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
```

Bij dit voorbeeld werd communicatie geleid en geaccepteerd door de geconfigureerde reputatieswolk server pool, cloud-sa.eu.amp.sourcefire.com.

# Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

## Gebruik telnet om connectiviteit te testen

Om de connectiviteit van het havenniveau aan de wolk van de Bestandsreputatie te verifiëren, gebruik de hostname voor de gevormde server van de reputatieswolk, en test met **telnet** om 32137, of haven 443, zoals gevormd.

```
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.
```

Veelzeggende verbinding met de EU, succesvol in haven 443:

```
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.
```

Veelzijdige aansluiting op de EU, niet in staat om verbinding te maken via haven 32137:

```
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
```

U kunt telnet aan de directe IP of hostnamen achter de CNAME voor de reputatie cloud server pool testen met dezelfde telnet testmethode, met gebruik van poort 32137 of poort 443. Als u niet met succes op de hostname en poort kunt telen, kunt u netwerkconnectiviteit en firewallinstellingen buiten het ESA moeten controleren.

De verificatie van het telnet is op een server die de reputatie van een bestand aankan, uitgevoerd door hetzelfde proces als getoond.

## Invoer van de openbare sleutel

Wanneer u de openbare toets op een ESA ingaat met AsyncOS 10.x en nieuwer, verzeker u dat u met succes de openbare toets hebt geplakt of geladen. Alle fouten in de openbare toets worden weergegeven in de configuratie-uitgang:

```
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
```

Als u een fout ontvangt, probeer dan de configuratie opnieuw. Neem contact op met Cisco-ondersteuning voor persistente fouten.

## AMP-logboeken bekijken

Wanneer u het AMP-logbestand op het ESA bekijkt, zorg er dan voor dat u "file reputatie query from Cloud" ziet, gespecificeerd op het moment van file reputatie query:

```
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
```

Als u dit ziet, trok de query de respons uit het lokale ESA cache en NIET uit de geconfigureerde reputatieswolk server pool:

```
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
```

# Aanvullende fouten en meldingen

Een ESA-beheerder kan deze kennisgeving ontvangen. Als dit ontvangen is, stap dan door het configuratie- en verificatieproces.

```
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
```

# Gerelateerde informatie

- Vereiste serveradressen voor correcte AMP-bewerkingen
- Technische ondersteuning en documentatie – Cisco Systems