Konfigurieren eines statischen Dateireputations-Hosts oder eines alternativen Dateireputations-Cloud-Serverpools auf der ESA

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie eine Cisco E-Mail Security Appliance (ESA) für die Kommunikation und Verwendung eines statischen Hosts oder eines alternativen Reputations-Cloud-Serverpools für die Dateireputation mithilfe von AMP (Advanced Malware Protection) konfiguriert wird.

Hintergrundinformationen

Eine Dateireputations-Abfrage ist die erste von zwei Ebenen für AMP auf der ESA. Die Dateireputation erfasst einen Fingerabdruck jeder Datei, die die ESA passiert, und sendet diesen an das Cloud-basierte Informationsnetzwerk von AMP, um die Reputation zu überprüfen. Aufgrund dieser Ergebnisse können ESA-Administratoren schädliche Dateien automatisch blockieren und vom Administrator definierte Richtlinien anwenden. Der Dateireputations-Cloud-Service wird auf Amazon Web Services (AWS) gehostet. Wenn Sie DNS-Abfragen für die in diesem Dokument beschriebenen Hostnamen durchführen, wird ".amazonaws.com" aufgelistet.

Die zweite Ebene von AMP auf der ESA ist File Analysis (Dateianalyse). Das wird in diesem Dokument nicht behandelt.

SSL-Kommunikation für Dateireputations-Datenverkehr verwendet standardmäßig Port 32137. Zum Zeitpunkt der Servicekonfiguration kann alternativ Port 443 verwendet werden. Ausführliche Informationen finden Sie im ESA-Benutzerhandbuch "Dateireputations-Filterung und Dateianalyse". ESA- und Netzwerkadministratoren möchten möglicherweise die Verbindung zum Pool für IP-Adressen, IP-Standorte und auch die Port-Kommunikation (32137 vs. 443) überprüfen, bevor sie mit der Konfiguration fortfahren.

Default AMERICAS(Legacy) Reputations-Cloud-Server-Pool (cloud-sa.amp.sourcefire.com)

Sobald die Dateireputation lizenziert, aktiviert und auf einer ESA konfiguriert ist, wird sie standardmäßig für diesen Reputations-Cloud-Server-Pool festgelegt:

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

Der Hostname "cloud-sa.amp.sourcefire.com" ist ein DNS Canonical Name Record (CNAME). Ein CNAME ist ein Ressourcentyp in DNS, der verwendet wird, um anzugeben, dass ein Domänenname ein Alias für eine andere Domäne ist, d. h. die "kanonische" Domäne. Zugeordnete Hostnamen im Pool, die mit diesem CNAME verknüpft sind, können ähnlich sein wie:

- 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)

Es stehen zwei weitere Dateireputations-Server zur Auswahl:

- AMERICAS (cloud-sa.amp.cisco.com)
- EUROPA (cloud-sa.eu.amp.cisco.com)

Beide Server werden im Abschnitt "Hostnamen von Servern für statische Dateireputation (.cisco.com)" in diesem Dokument behandelt.

Sie können die Hosts, die mit dem CNAME von AMERICAS cloud-sa-amp.sourcefire.com verknüpft sind, jederzeit in Ihrem Netzwerk überprüfen, wenn Sie diese Abfrage oder **nslookup** ausführen:

```
$ 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
```

> **Hinweis**: Diese Hosts sind NICHT statisch, und es wird empfohlen, den Reputationsverkehr der ESA-Datei NICHT auf diese Hosts zu beschränken. Die Ergebnisse Ihrer Abfrage können variieren, da sich die Hosts im Pool ohne Vorankündigung ändern.

Sie können den geografischen IP-Standort über dieses Drittanbieter-Tool überprüfen:

- 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

Hostnamen von Servern für statische Dateireputation (.cisco.com)

Cisco hat 2016 damit begonnen, ".cisco.com"-basierte Hostnamen für den Dateireputations-Service für AMP bereitzustellen. Die folgenden statischen Hostnamen und IP-Adressen sind für die Dateireputation verfügbar:

- cloud-sa.amp.cisco.com (Nordamerika - USA)
- cloud-sa.eu.amp.cisco.com (Europa - Republik Irland)
- cloud-sa.apjc.amp.cisco.com (Asien-Pazifik-Raum - Japan)

Sie können die Hosts und die zugeordneten IP-Adressen im Netzwerk überprüfen und eine graf- oder **nslookup-**Abfrage ausführen:

Nordamerika (USA):

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

Europa (Republik Irland):

```
$ 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
```

Asien-Pazifik-Raum (Japan):

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

Sie können den geografischen IP-Standort über dieses Drittanbieter-Tool überprüfen:

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

Derzeit sind keine Stilllegungen der Hostnamen ".sourcefire.com" geplant.

Alternative EUROPE Reputations-Cloud-Server-Pool (cloud-sa.eu.amp.sourcefire.com)

Für Kunden mit Sitz in der Europäischen Union (EU), die spezifischen Datenverkehr an nur in der EU ansässige Server und Rechenzentren senden müssen, können Administratoren die ESA so konfigurieren, dass sie entweder auf den statischen Host in der EU oder auf den Reputations-Cloud-Server-Pool in der EU verweist:

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

Wie der Standard-Hostname "cloud-sa.amp.sourcefire.com" ist auch der Hostname "cloud-sa.eu.amp.sourcefire.com" ein CNAME. Zugeordnete Hostnamen im Pool, die mit diesem CNAME verknüpft sind, sind möglicherweise ähnlich wie:

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

Sie können die Hosts überprüfen, die dem EUROPEAN cloud-sa.eu.amp.sourcefire.com-CNAME in Ihrem Netzwerk zugeordnet sind, und eine **graf-** oder **nslookup-**Abfrage ausführen::

```
$ 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
```

> **Hinweis**: Diese Hosts sind NICHT statisch, und es wird empfohlen, den Reputationsverkehr der ESA-Datei NICHT auf diese Hosts zu beschränken. Die Ergebnisse Ihrer Abfrage können variieren, da sich die Hosts im Pool ohne Vorankündigung ändern.

Sie können den geografischen IP-Standort über dieses Drittanbieter-Tool überprüfen:

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

Konfigurieren eines statischen Dateireputations-Hosts oder eines alternativen Dateireputations-Cloud-Serverpools auf der ESA

Die Dateireputation kann entweder über die GUI oder die CLI der ESA konfiguriert werden. Die in diesem Dokument aufgeführten Konfigurationsschritte veranschaulichen die CLI-Konfiguration. Die gleichen Schritte und Informationen können jedoch auch über die GUI (**Sicherheitsdienste > Dateireputation und Analyse > Globale Einstellungen bearbeiten..) angewendet werden. > Erweiterte Einstellungen für Dateireputation**).

AsyncOS 10.x und höher

Neue Funktionen von AsyncOS 10.x ermöglichen die Konfiguration der ESA für die Verwendung einer Private Reputations-Cloud (On-Premises File Reputation Server) oder eines Cloud-basierten Dateireputations-Servers. Mit dieser Änderung wird in der AMP-Konfiguration nicht mehr der Hostname mit dem Schritt "Enter reputation cloud server pool" (Reputations-Cloud-Serverpool eingeben) angezeigt. Sie müssen den zusätzlichen Dateireputations-Server als Private Reputations-Cloud einrichten und den öffentlichen Schlüssel für diesen Hostnamen angeben.

Wenn Sie für 10.0.x und höher einen alternativen AMP-Reputationsserver konfigurieren, müssen Sie möglicherweise einen öffentlichen Schlüssel für diesen Hostnamen eingeben.

Alle AMP-Reputationsserver verwenden denselben öffentlichen Schlüssel:

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

Dieses Beispiel hilft Ihnen bei der Einrichtung eines alternativen Dateireputations-Servers auf cloud-sa.eu.amp.sourcefirce.com:

```
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]>
```

Bestätigen Sie alle Konfigurationsänderungen.

AsyncOS 9.7.x und frühere Version

Dieses Beispiel auf AsyncOS 9.7.2-065 für E-Mail Security hilft Ihnen, den alternativen Reputations-Cloud-Serverpool auf cloud-sa.eu.amp.sourcefirce.com aufzurufen:

```
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]>
```

Bestätigen Sie alle Konfigurationsänderungen.

Dateireputations-Server am Standort (FireAMP Private Cloud)

Die Verwendung eines standortbasierten Dateireputations-Servers, auch bekannt als FireAMP Private Cloud, wurde eingeführt, der mit AsyncOS 10.x für Email Security beginnt.

Wenn Sie eine Cisco AMP Virtual Private Cloud-Appliance in Ihrem Netzwerk bereitgestellt haben, können Sie jetzt die Dateireputation von Nachrichtenanlagen abfragen, ohne diese an die Public Reputation Cloud zu senden. Informationen zum Konfigurieren der Appliance für die Verwendung eines Dateireputations-Servers vor Ort finden Sie im Kapitel "Dateireputations-Filterung und Dateianalyse" im ESA-Benutzerhandbuch oder in der Online-Hilfe.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Um zu sehen, wie der Dateireputations-Datenverkehr an den konfigurierten statischen Host- oder Reputations-Cloud-Serverpool weitergeleitet wird, führen Sie eine Paketerfassung der ESA mit dem angegebenen Filter durch, um den Datenverkehr an Port 32137 oder Port 443 zu erfassen.

Verwenden Sie für dieses Beispiel den Cloud-Server-Pool cloud-sa.eu.amp.sourcefire.com und die SSL-Kommunikation mit Port 443...

Dies wird bei der ESA in den AMP-Protokollen protokolliert:

```
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
```

Die ESA-Paketverfolgung, die ausgeführt wurde, hat diese Konversation aufgezeichnet:

```
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
```

Sie sehen, dass der Datenverkehr über Port 443 kommuniziert. Von unserer ESA (my11esa.local) wird mit dem Hostnamen ec2-176-34-122-245.eu-west-1.compute.amazonaws.com kommuniziert. Dieser Hostname ist an die IP-Adresse 176.34.122.245 gebunden:

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

Die IP-Adresse von 176.34.122.245 ist Poolmitglied von CNAME für 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
```

In diesem Beispiel wurde die Kommunikation vom konfigurierten Reputations-Cloud-Server-Pool cloud-sa.eu.amp.sourcefire.com geleitet und akzeptiert.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Telnet zum Testen der Verbindung verwenden

Um die Verbindung auf Portebene zur Dateireputations-Cloud zu überprüfen, verwenden Sie den Hostnamen für den konfigurierten Reputations-Cloud-Serverpool und testen Sie mit **telnet** zu Port 32137 oder Port 443, wie konfiguriert.

```
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.
```

Überprüfung der Verbindung zur EU, erfolgreich über Port 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.
```

Konnektivität mit der EU überprüfen, keine Verbindung über Port 32137 möglich:

```
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
```

Sie können Telnet für den Reputations-Cloud-Server-Pool mit derselben Telnet-Testmethode an die direkte IP-Adresse oder an die Hostnamen hinter dem CNAME testen, wobei Port 32137 oder Port 443 verwendet wird. Wenn Sie Telnet nicht erfolgreich zum Hostnamen und Port senden können, müssen Sie möglicherweise die Netzwerkverbindungen und Firewall-Einstellungen außerhalb der ESA überprüfen.

Die Überprüfung des Telnet-Erfolgs auf einen Dateireputations-Server vor Ort erfolgt mit demselben Prozess wie gezeigt.

Eingabe des öffentlichen Schlüssels

Wenn Sie den öffentlichen Schlüssel auf einer ESA, auf der AsyncOS 10.x und höher ausgeführt wird, eingeben, müssen Sie sicherstellen, dass Sie den öffentlichen Schlüssel erfolgreich eingefügt oder geladen haben. Alle Fehler im öffentlichen Schlüssel werden der Konfigurationsausgabe angezeigt:

```
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
```

Wenn Sie einen Fehler erhalten, versuchen Sie es erneut. Bei persistenten Fehlern wenden Sie sich an den Cisco Support.

AMP-Protokolle überprüfen

Wenn Sie das AMP-Protokoll auf der ESA anzeigen, stellen Sie sicher, dass Sie die "Datei-Reputationsabfrage aus der Cloud" sehen, die zum Zeitpunkt der Dateireputationsabfrage angegeben ist:

```
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
```

Wenn Sie dies sehen, wurde die Antwort aus dem lokalen ESA-Cache und NICHT aus dem konfigurierten Reputations-Cloud-Serverpool abgerufen:

```
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
```

Zusätzliche Fehler und Warnungen

Möglicherweise erhält ein ESA-Administrator diese Benachrichtigung. Wenn Sie diese Meldung erhalten, führen Sie den Konfigurations- und Überprüfungsprozess erneut durch.

```
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
```

Zugehörige Informationen

- Erforderliche Serveradressen für einen ordnungsgemäßen AMP-Betrieb
- Technischer Support und Dokumentation - Cisco Systems