Configure Static File Reputation Host or an Alternate File Reputation Cloud Server Pool on ESA

Contents

Introduction

This document describes how to configure a Cisco Email Security Appliance (ESA) to communicate and use a static host or an alternative reputation cloud server pool for File Reputation with the use of Advanced Malware Protection (AMP).

Background Information

A File Reputation query is the first of two layers for AMP on the ESA. File Reputation captures a fingerprint of each file as it traverses the ESA and sends it to AMP's cloud-based intelligence network for a reputation verdict. Given these results, ESA administrators can automatically block malicious files and apply administrator-defined policies. The File Reputation cloud service is hosted on Amazon Web Services (AWS). When you perform DNS queries against the hostname(s) described in this document, you will see ".amazonaws.com" listed.

The second layer of AMP on the ESA is File Analysis. That is not covered in this document.

SSL communication for File Reputation traffic uses port 32137 by default. At the time of the configuration of the service, port 443 might be used as an alternative. Consult the ESA User Guide, "File Reputation Filtering and File Analysis" section for complete details. ESA and Network administrators might wish to verify connectivity to the pool for IP address(es), IP location, and also

port communication (32137 vs. 443) before they proceed with the configuration.

Default AMERICAS(Legacy) reputation cloud server pool (cloud-sa.amp.sourcefire.com)

Once File Reputation is licensed, enabled, and configured on an ESA, by default it will be set for this reputation cloud server pool:

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

The hostname "cloud-sa.amp.sourcefire.com" is a DNS Canonical Name record (CNAME). A CNAME is a type of resource record in DNS used to specify that a domain name is an alias for another domain, which is the "canonical" domain. Associated hostnames in the pool tied to this CNAME might be similar to:

- 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)

There are two additional file reputation servers choices that may be selected:

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

Both of these servers are covered in the "Static File Reputation server hostnames (.cisco.com)" section of this document.

You might verify the hosts that are associated to the AMERICAS cloud-sa-amp.sourcefire.com CNAME from your network at anytime when you run this **dig** or **nslookup** query:

```
$ 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
```

> **Note**: These hosts are NOT static and it is recommended to NOT restrict ESA File Reputation traffic based to only these hosts. The results of your query might vary, as the hosts in the pool will change without notice.

You can verify the IP geographical location from this 3rd party tool:

- 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

Static File Reputation server hostnames (.cisco.com)

Cisco began to provide ".cisco.com" based hostnames for the File Reputation service for AMP in 2016. There are static hostnames and IP addresses available for File Reputation from this:

- cloud-sa.amp.cisco.com (North America - USA)
- cloud-sa.eu.amp.cisco.com (Europe – Republic of Ireland)
- cloud-sa.apjc.amp.cisco.com (Asia Pacific – Japan)

You might verify the hosts and associated IP addresses from your network and run a **dig** or **nslookup** query:

North America (US):

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

Europe (Republic of Ireland):

```
$ 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
```

Asia Pacific (Japan):

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

You can verify the IP geographical location from this 3rd party tool:

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

At this time, there are no plans to decommission the ".sourcefire.com" hostnames.

Alternative EUROPE reputation cloud server pool (cloud-sa.eu.amp.sourcefire.com)

For European Union (EU) based customers that are required to send specific traffic to EU-based only servers and data centers, administrators can configure the ESA to point to either the EU static host or to the EU reputation cloud server pool:

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

Like the default hostname "cloud-sa.amp.sourcefire.com", the hostname "cloud-sa.eu.amp.sourcefire.com" is also a CNAME. Associated hostnames in the pool tied to this CNAME might be similar to:

- 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)

You might verify the hosts that are associated to the EUROPEAN cloud-sa.eu.amp.sourcefire.com CNAME from your network and run a **dig** or **nslookup** query::

```
$ 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
```

> **Note**: These hosts are NOT static and it is recommended to NOT restrict ESA File Reputation traffic based to only these hosts. The results of your query might vary, as the hosts in the pool will change without notice.

You can verify the IP geographical location from this 3rd party tool:

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

Configure Static File Reputation Host or an Alternate File Reputation Cloud Server Pool on ESA

File Reputation can be configured from either the GUI or CLI on the ESA. The configuration steps listed in this document will demonstrate the CLI configuration. However, the same steps and information can be applied via the GUI (**Security Services > File Reputation and Analysis > Edit Global Settings... > Advanced Settings for File Reputation**).

AsyncOS 10.x and Newer

New features of AsyncOS 10.x allow the ESA to be configured to use a private reputation cloud (On-Premises File Reputation Server) or cloud-based file reputation server. With this change, AMP configuration no longer prompts for the hostname with the "Enter reputation cloud server pool" step. You must choose to setup the additional file reputation server as a private reputation

cloud and provide the public key for that hostname.

For 10.0.x and newer, when you configure an alternative AMP reputation server, you might be required to enter a public key associated to that hostname.

All of the AMP reputation servers use the same public key:

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

This example will help you set up the alternative file reputation server to 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]>
```

Commit any configuration changes.

AsyncOS 9.7.x and earlier

This example on AsyncOS 9.7.2-065 for Email Security will help you up the alternative reputation cloud server pool to cloud-sa.eu.amp.sourcefirce.com:

```
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]>
```

Commit any configuration changes.

On-Premises File Reputation Server (FireAMP Private Cloud)

Use of an on-premises file reputation server, also known as a FireAMP Private Cloud, was introduced that starts with AsyncOS 10.x for Email Security.

If you have deployed a Cisco AMP Virtual Private Cloud appliance on your network, you can now query the file reputation of message attachments without sending them to the public reputation cloud. To configure your appliance to use an on-premises file reputation server, see the “File Reputation Filtering and File Analysis” chapter in the ESA User Guide or online help.

Verify

Use this section in order to confirm that your configuration works properly.

In order to see File Reputation traffic passing to the configured static host or reputation cloud server pool, perform a packet capture from the ESA with specified filter to capture port 32137 or port 443 traffic.

For this example, use the cloud-sa.eu.amp.sourcefire.com cloud server pool and SSL communication with the use of port 443...

This is logged to the ESA in the AMP logs:

```
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
```

The ESA packet trace running captured this conversation:

```
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

You see that the traffic communicates over port 443. From our ESA (my11esa.local), it communicates to the hostname ec2-176-34-122-245.eu-west-1.compute.amazonaws.com. This hostname is tied to the IP address 176.34.122.245:

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

The IP address of 176.34.122.245 is a pool member of the CNAME for 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
```

For this example, communication was directed and accepted by the configured reputation cloud server pool, cloud-sa.eu.amp.sourcefire.com.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Use Telnet to Test Connectivity

In order to verify port level connectivity to the File Reputation cloud, use the hostname for the configured reputation cloud server pool, and test with **telnet** to port 32137, or port 443, as configured.

```
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.
```

Verfiy connectivity to EU, successful over 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.
```

Verfiy connectivity to EU, not able to connect over port 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
```

You can test telnet to the direct IP or hostnames behind the CNAME for the reputation cloud server pool with the same telnet test method, with the use of port 32137 or port 443. If you are not able to successfully telnet to the hostname and port, you might need to check network connectivity and firewall settings external to the ESA.

Verification of telnet sucess to an on-premise file reputation server will be done by the same process as shown.

Input of the Public Key

When you enter the public key on an ESA running AsyncOS 10.x and newer, assure that you were successful in pasting or loading the public key. Any errors in the public key will be displayed to the configuration output:

```
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
```

If you receive an error, retry the configuration. For persistent errors, contact Cisco Support.

Review AMP logs

When you view the AMP log on the ESA, ensure that you see "file reputation query from Cloud" specified at the time of file reputation 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
```

If you see this, the query pulled the response from local ESA cache and NOT from the configured reputation cloud 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
```

Additional Errors and Alerts

An ESA administrator might receive this notice. If this is received, re-step through the configuration and verification process.

```
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
```

Related Information

- **Required Server Addresses for Proper AMP Operations**
- **Technical Support & Documentation - Cisco Systems**