Configurazione di un host statico per la reputazione dei file o di un pool di server cloud alternativo per la reputazione dei file su ESA

Sommario

Introduzione
Premesse
Pool di server cloud reputazione America (legacy) predefinito (cloud-sa.amp.sourcefire.com)
Nomi host del server Static File Reputation (.cisco.com)
Pool di server cloud reputazione Europa alternativa (cloud-sa.eu.amp.sourcefire.com)
Configurazione di un host statico per la reputazione dei file o di un pool di server cloud alternativo per la reputazione dei file su ESA
AsyncOS 10.x e versioni successive
AsyncOS 9.7.x e versioni precedenti
Server di reputazione dei file on-premises (FireAMP Private Cloud)
Verifica
Risoluzione dei problemi
Usa Telnet per verificare la connettività
Input della chiave pubblica
Verifica registri AMP
Ulteriori errori e avvisi
Informazioni correlate

Introduzione

In questo documento viene descritto come configurare Cisco Email Security Appliance (ESA) per comunicare e utilizzare un host statico o un pool di server cloud con reputazione alternativa per la reputazione dei file con l'uso di Advanced Malware Protection (AMP).

Premesse

Una query sulla reputazione dei file è il primo dei due livelli per AMP sull'ESA. La reputazione dei file acquisisce un'impronta digitale di ogni file mentre attraversa l'ESA e la invia alla rete di intelligence basata su cloud di AMP per un verdetto sulla reputazione. Dati questi risultati, gli amministratori ESA possono bloccare automaticamente i file dannosi e applicare policy definite dagli amministratori. Il servizio cloud File Reputation è ospitato in Amazon Web Services (AWS). Quando si eseguono query DNS sui nomi host descritti in questo documento, viene visualizzato l'elenco ".amazonaws.com".

Il secondo livello dell'AMP sull'ESA è l'analisi dei file. Questo aspetto non è trattato nel presente documento.

Per impostazione predefinita, la comunicazione SSL per il traffico File Reputation utilizza la porta

32137. Al momento della configurazione del servizio, la porta 443 potrebbe essere utilizzata come alternativa. Per ulteriori informazioni, consultare la Guida dell'utente ESA, sezione "Filtro della reputazione e analisi dei file". Gli amministratori ESA e di rete potrebbero voler verificare la connettività al pool per gli indirizzi IP, la posizione IP e la comunicazione delle porte (32137 rispetto a 443) prima di procedere con la configurazione.

Pool di server cloud reputazione America (legacy) predefinito (cloud-sa.amp.sourcefire.com)

Dopo aver concesso in licenza, abilitato e configurato la reputazione del file su un ESA, per impostazione predefinita verrà impostata per questo pool di server cloud di reputazione:

- AMERICHE (legacy) (cloud-sa.amp.sourcefire.com)

Il nome host "cloud-sa.amp.sourcefire.com" è un record CNAME (Canonical Name) DNS. Un CNAME è un tipo di record di risorse nel DNS utilizzato per specificare che un nome di dominio è un alias per un altro dominio, che è il dominio "canonico". I nomi host associati nel pool associato a questo CNAME potrebbero essere simili a:

- 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)

Èpossibile selezionare altri due server di reputazione file:

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

Entrambi i server sono descritti nella sezione "Nomi host del server Static File Reputation (.cisco.com)" di questo documento.

Èpossibile verificare gli host associati a AMERICHE cloud-sa-amp.sourcefire.com CNAME dalla rete in qualsiasi momento quando si esegue questa query **dig** o **nslookup**:

```
$ 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
```

Nota: Questi host NON sono statici e si consiglia di NON limitare il traffico ESA File Reputation (Reputazione file ESA) solo a questi host. I risultati della query potrebbero variare, poiché gli host nel pool cambiano senza preavviso.

Èpossibile verificare la posizione geografica IP da questo strumento di terze parti:

- 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

Nomi host del server Static File Reputation (.cisco.com)

Cisco ha iniziato a fornire i nomi host basati su ".cisco.com" per il servizio File Reputation per AMP nel 2016. Sono disponibili nomi host statici e indirizzi IP per il servizio File Reputation dal seguente indirizzo:

- cloud-sa.amp.cisco.com (Nord America - Stati Uniti)
- cloud-sa.eu.amp.cisco.com (Europa - Repubblica d'Irlanda)
- cloud-sa.apjc.amp.cisco.com (Asia-Pacifico - Giappone)

Èpossibile verificare gli host e gli indirizzi IP associati dalla rete ed eseguire una query **dig** o **nslookup**:

Nord America (USA):

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

Europa (Repubblica d'Irlanda):

```
$ 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-Pacifico (Giappone):

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

Èpossibile verificare la posizione geografica IP da questo strumento di terze parti:

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

Per il momento non è prevista la rimozione dei nomi host ".sourcefire.com".

Pool di server cloud reputazione Europa alternativa (cloud-

sa.eu.amp.sourcefire.com)

Per i clienti con sede nell'Unione Europea (UE) che devono inviare traffico specifico ai server e ai centri dati solo con sede nell'UE, gli amministratori possono configurare l'ESA in modo che punti all'host statico UE o al pool di server cloud con reputazione UE:

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

Come il nome host predefinito "cloud-sa.amp.sourcefire.com", anche il nome host "cloud-sa.eu.amp.sourcefire.com" è un CNAME. I nomi host associati nel pool associato a questo CNAME potrebbero essere simili a:

- 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)

Èpossibile verificare gli host associati al EUROPEAN cloud-sa.eu.amp.sourcefire.com CNAME dalla rete ed eseguire una query **dig** o **nslookup**::

```
$ 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
```

> **Nota:** Questi host NON sono statici e si consiglia di NON limitare il traffico ESA File Reputation basato solo su questi host. I risultati della query potrebbero variare, poiché gli host nel pool cambiano senza preavviso.

Èpossibile verificare la posizione geografica IP da questo strumento di terze parti:

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

Configurazione di un host statico per la reputazione dei file o di un pool di server cloud alternativo per la reputazione dei file su ESA

La reputazione dei file può essere configurata dalla GUI o dalla CLI sull'ESA. I passaggi di configurazione elencati in questo documento mostrano la configurazione CLI. Tuttavia, gli stessi passaggi e le stesse informazioni possono essere applicati attraverso la GUI (**Security Services > File Reputation and Analysis > Edit Global Settings... > Advanced Settings for File Reputation**).

AsyncOS 10.x e versioni successive

Le nuove funzionalità di AsyncOS 10.x consentono di configurare l'ESA in modo che utilizzi un cloud di reputazione privata (On-Premises File Reputation Server) o un file reputation server basato su cloud. Con questa modifica, la configurazione AMP non richiede più il nome host con il passaggio "Immettere il pool di server cloud di reputazione". È necessario scegliere di configurare il server della reputazione del file aggiuntivo come cloud della reputazione privata e fornire la chiave pubblica per tale nome host.

Per la versione 10.0.x e successive, quando si configura un server di reputazione AMP alternativo, potrebbe essere necessario immettere una chiave pubblica associata a tale nome host.

Tutti i server della reputazione AMP utilizzano la stessa chiave pubblica:

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

In questo esempio viene illustrato come configurare il server alternativo per la reputazione dei file su 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]>
```

Eseguire il commit delle modifiche alla configurazione.

AsyncOS 9.7.x e versioni precedenti

Questo esempio relativo ad AsyncOS 9.7.2-065 for Email Security consente di configurare il pool di server cloud con reputazione alternativa su 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]>
```

Eseguire il commit delle modifiche alla configurazione.

Server di reputazione dei file on-premises (FireAMP Private Cloud)

Èstato introdotto l'uso di un server di reputazione dei file locale, noto anche come FireAMP Private Cloud, che inizia con AsyncOS 10.x for Email Security.

Se nella rete è stata distribuita un'appliance Cisco AMP Virtual Private Cloud, è ora possibile eseguire query sulla reputazione dei file degli allegati senza inviarli al cloud della reputazione pubblica. Per configurare l'appliance in modo che utilizzi un server di reputazione file locale, consultare il capitolo relativo al filtro della reputazione e all'analisi dei file nella Guida per l'utente ESA o nella Guida in linea.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Per vedere il traffico File Reputation passare all'host statico configurato o al pool di server cloud di reputazione, eseguire un'acquisizione di pacchetti dall'ESA con il filtro specificato per acquisire il traffico della porta 32137 o 443.

Per questo esempio, utilizzare il pool di server cloud cloud-sa.eu.amp.sourcefire.com e la comunicazione SSL con l'utilizzo della porta 443...

L'operazione viene registrata sull'ESA nei registri AMP:

```
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
```

La traccia del pacchetto ESA in esecuzione ha acquisito questa conversazione:

```
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
```

Vedete che il traffico comunica sulla porta 443. Dalla nostra ESA (my11esa.local), comunica con il hostname ec2-176-34-122-245.eu-west-1.compute.amazonaws.com. Il nome host è associato all'indirizzo IP 176.34.122.245:

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

L'indirizzo IP 176.34.122.245 è un membro del pool CNAME per 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
```

Per questo esempio, la comunicazione è stata indirizzata e accettata dal pool di server cloud di reputazione configurato, cloud-sa.eu.amp.sourcefire.com.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Usa Telnet per verificare la connettività

Per verificare la connettività a livello di porta nel cloud File Reputation, utilizzare il nome host per il pool di server cloud di reputazione configurato e verificare con **telnet** la porta 32137 o la porta 443 configurata.

```
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.
```

Verificare la connettività all'UE, superando il porto 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.
```

Verificare la connettività all'UE, impossibile collegarsi tramite la porta 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
```

Èpossibile testare telnet su IP diretto o nomi host dietro CNAME per il pool di server cloud di reputazione con lo stesso metodo di test telnet, utilizzando la porta 32137 o la porta 443. Se non si riesce a eseguire correttamente il telnet su nome host e porta, potrebbe essere necessario controllare la connettività di rete e le impostazioni del firewall esterne all'ESA.

La verifica della riuscita di telnet su un file server on-premise reputazione verrà effettuata con lo stesso processo mostrato.

Input della chiave pubblica

Quando si immette la chiave pubblica su un'ESA con AsyncOS 10.x e versioni successive, accertarsi di aver incollato o caricato correttamente la chiave pubblica. Eventuali errori nella chiave pubblica verranno visualizzati nell'output di configurazione:

```
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
```

Se viene visualizzato un errore, ripetere la configurazione. Per gli errori persistenti, contattare il supporto Cisco.

Verifica registri AMP

Quando si visualizza il log AMP sull'ESA, assicurarsi di vedere "query reputazione file dal cloud"

specificato al momento della query reputazione file:

```
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
```

In questo caso, la query ha estratto la risposta dalla cache ESA locale e NON dal pool di server cloud della reputazione configurata:

```
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
```

Ulteriori errori e avvisi

Un amministratore ESA potrebbe ricevere tale notifica. In caso affermativo, eseguire nuovamente la procedura di configurazione e verifica.

```
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
```

Informazioni correlate

- Indirizzi server necessari per il corretto funzionamento dell'AMP
- Documentazione e supporto tecnico – Cisco Systems