Configurez l'hôte statique de réputation de fichier ou un groupe de serveur de nuage de réputation de fichier index sur l'ESA

Contenu

Introduction

Ce document décrit comment configurer une appliance de sécurité du courrier électronique de Cisco (ESA) pour communiquer et utiliser un hôte statique ou un groupe alternatif de serveur de nuage de réputation pour la réputation de fichier avec l'utilisation de la protection avancée de malware (AMP).

Informations générales

Une requête de réputation de fichier est la première de deux couches pour l'AMP sur l'ESA. Classez la réputation capture une empreinte digital de chaque fichier comme elle traverse l'ESA et l'envoie au réseau basé sur nuage de l'intelligence de l'Ampère pour un verdict de réputation. Donné ces résultats, les administrateurs ESA peuvent automatiquement bloquer les fichiers malveillants et appliquer des stratégies administrateur-définies. Le service en nuage de réputation de fichier est hébergé sur les services Web d'Amazone (AWS). Quand vous exécutez des requêtes DNS contre les noms d'hôte décrits dans ce document, vous verrez que « .amazonaws.com » l'a répertorié.

La deuxième couche d'AMP sur l'ESA est analyse de fichier. Cela n'est pas couvert dans ce document.

La transmission SSL pour le trafic de réputation de fichier utilise le port 32137 par défaut. Au moment de la configuration du service, le port 443 pourrait être utilisé comme alternative. Consultez le guide utilisateur ESA, « classez la réputation filtrant et section classez analyse » pour les détails complets. L'ESA et les administrateurs réseau pourraient souhaiter vérifier la Connectivité au groupe pour l'adresse IP, emplacement IP, et mettent en communication également la transmission (32137 contre 443) avant qu'ils poursuivent la configuration.

Groupe par défaut de serveur de nuage de réputation d'AMERICAS(Legacy) (cloud-sa.amp.sourcefire.com)

La réputation de fichier est autorisée, activée, et une fois configurée sur un ESA, par défaut qu'il sera placé pour ce groupe de serveur de nuage de réputation :

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

L'adresse Internet « cloud-sa.amp.sourcefire.com » est un enregistrement canonique de nom de DN (CNAME). Un CNAME est un type d'enregistrement de ressource dans des DN utilisés pour spécifier qu'un nom de domaine est un pseudonyme pour un autre domaine, qui est le domaine « canonique ». Le hostnamesin associé le groupe attaché à ce CNAME pourrait être semblable à :

- 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)

Il y a deux choix supplémentaires de serveurs de réputation de fichier qui peuvent être sélectionnés :

- L'AMÉRIQUES (cloud-sa.amp.cisco.com)
- L'EUROPE (cloud-sa.eu.am p.cisco.com)

Chacun des deux serveurs sont couverts dans la section « de fichier de réputation des adresses Internet statiques de serveur (.cisco.com) » de ce document.

Vous pourriez vérifier les hôtes qui sont associés en AMÉRIQUES cloud-sa-amp.sourcefire.com CNAME de votre réseau à tout moment quand vous exécutez cette requête de **fouille** ou de **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
```

> **Note**: Ces hôtes ne sont pas statiques et il est recommandé pour ne pas limiter le trafic de réputation de fichier ESA basé seulement à ces hôtes. Les résultats de votre requête pourraient varier, comme les hôtes dans le groupe modification sans préavis.

Vous pouvez vérifier la situation géographique IP de cet outil de tiers :

- 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

Adresses Internet statiques de serveur de réputation de fichier (.cisco.com)

Cisco a commencé à fournir les adresses Internet basées « .cisco.com » pour le service de réputation de fichier pour l'AMP en 2016. Il y a les adresses Internet statiques et les adresses IP disponibles pour la réputation de fichier de ceci :

- cloud-sa.amp.cisco.com (Amérique du Nord - L'USA)
- cloud-sa.eu.amp.cisco.com (l'Europe – La république d'Irlande)
- cloud-sa.apjc.amp.cisco.com (Asia Pacific – Le Japon)

Vous pourriez vérifier les hôtes et les adresses IP associées de votre réseau et exécuter une requête de **fouille** ou de **nslookup** :

L'Amérique du Nord (US) :

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

L'Europe (république d'Irlande) :

```
$ 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 (Japon) :

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

Vous pouvez vérifier la situation géographique IP de cet outil de tiers :

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

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

Àce moment, il n'y a aucun plan pour désarmer les adresses Internet « .sourcefire.com ».

Groupe alternatif de serveur de nuage de réputation de l'EUROPE (cloud-sa.eu.amp.sourcefire.com)

Pour les clients basés européens de l'Union (UE) qui sont requis d'envoyer le trafic spécifique seulement aux serveurs et aux centres de traitement des données basés dans l'UE, les administrateurs peuvent configurer l'ESA pour indiquer à l'hôte statique UE ou le groupe de serveur de nuage de réputation UE :

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

Comme l'adresse Internet par défaut « cloud-sa.amp.sourcefire.com », l'adresse Internet « cloud-sa.eu.am p.sourcefire.com » est également un CNAME. Les adresses Internet associées dans le groupe attaché à ce CNAME pourraient être semblables à :

- 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)

Vous pourriez vérifier les hôtes qui sont associés à cloud-sa.eu.amp.sourcefire.com EUROPÉEN CNAME de votre réseau et exécutent une requête de **fouille** ou de **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
```

> **Note**: Ces hôtes ne sont pas statiques et il est recommandé pour ne pas limiter le trafic de réputation de fichier ESA basé seulement à ces hôtes. Les résultats de votre requête pourraient varier, comme les hôtes dans le groupe modification sans préavis.

Vous pouvez vérifier la situation géographique IP de cet outil de tiers :

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

Configurez l'hôte statique de réputation de fichier ou un groupe de serveur de nuage de réputation de fichier index sur l'ESA

La réputation de fichier peut être configurée du GUI ou du CLI sur l'ESA. Les étapes de configuration répertoriées dans ce document expliqueront la configuration CLI. Cependant, les mêmes étapes et informations peuvent être appliquées par l'intermédiaire du GUI (les **Services de sécurité > la réputation et l'analyse de fichier > éditent des paramètres généraux… > paramètres avancés pour la réputation de fichier**).

AsyncOS 10.x et plus nouveau

Les nouvelles caractéristiques d'AsyncOS 10.x permettent l'ESA à configurer pour utiliser un nuage privé de réputation (les Sur-sites classent le serveur de réputation) ou le serveur basé sur nuage de réputation de fichier. Avec cette modification, la configuration d'AMP n'incite plus pour l'adresse Internet avec l'étape « présentent de réputation de nuage de serveur groupe ». Vous devez choisir d'installer le serveur supplémentaire de réputation de fichier comme nuage privé de réputation et de fournir la clé publique pour cette adresse Internet.

Pour 10.0.x et plus nouveau, quand vous configurez un serveur alternatif de réputation d'AMP, vous pourriez être requis d'introduire une clé publique associée à cette adresse Internet.

Tous les serveurs de réputation d'AMP utilisent la même clé publique :

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

Cet exemple vous aidera à installer le serveur alternatif de réputation de fichier à 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]>
```

Commettez toutes les modifications de configuration.

AsyncOS 9.7.x et plus tôt

Cet exemple sur AsyncOS 9.7.2-065 pour la sécurité du courrier électronique vous aidera vers le haut du groupe alternatif de serveur de nuage de réputation à 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]>
```

Commettez toutes les modifications de configuration.

Serveur de réputation de fichier de Sur-sites (nuage privé de FireAMP)

On a introduit l'utilisation de l'des sur-sites classent le serveur de réputation, également connu sous le nom de nuage privé de FireAMP, qui commence par AsyncOS 10.x pour la sécurité du courrier électronique.

Si vous avez déployé une appliance privée virtuelle de nuage d'AMP de Cisco sur votre réseau, vous pouvez maintenant questionner la réputation de fichier des connexions de message sans les envoyer au nuage public de réputation. Pour configurer votre appliance pour utiliser les sur-sites classent le serveur de réputation, voient « réputation de fichier filtrer et le chapitre classent analyse » dans le guide utilisateur ESA ou l'aide en ligne.

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Afin de voir le trafic de réputation de fichier passer au groupe statique configuré de serveur d'hôte ou de nuage de réputation, effectuez une capture de paquet de l'ESA avec le filtre spécifié pour capturer le trafic du port 32137 ou du port 443.

Pour cet exemple, utilisez le groupe de serveur de nuage de cloud-sa.eu.amp.sourcefire.com et la transmission SSL avec l'utilisation du port 443…

Ceci est enregistré à l'ESA dans les logs d'AMP :

```
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]>
```

L'exécution de tracé de paquets ESA a capturé cette conversation :

```
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]>
```

Vous voyez que le trafic communique au-dessus du port 443. De notre ESA (my11esa.local), il communique à l'adresse Internet ec2-176-34-122-245.eu-west-1.compute.amazonaws.com. Cette adresse Internet est attachée à l'adresse IP 176.34.122.245 :

```
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]>
```

L'adresse IP de 176.34.122.245 est un membre de groupe du CNAME pour cloud-sa.eu.amp.sourcefire.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]>
```

Pour cet exemple, la transmission a été dirigée et reçue par le groupe configuré de serveur de nuage de réputation, cloud-sa.eu.amp.sourcefire.com.

Dépanner

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Telnet d'utilisation pour tester la Connectivité

Afin de vérifier la Connectivité de niveau de port au nuage de réputation de fichier, utilisez l'adresse Internet pour le groupe configuré de serveur de nuage de réputation, et testez avec le **telnet au** port 32137, ou le port 443, comme configuré.

```
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.
```

Connectivité de Verfiy à l'UE, port fini réussi 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.
```

Connectivité de Verfiy à l'UE, non capable se connecter au-dessus du 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
```

Vous pouvez tester le telnet à l'IP ou aux adresses Internet direct derrière le CNAME pour le serveur de nuage de réputation que le groupe avec le même telnet testent la méthode, avec l'utilisation du port 32137 ou du port 443. Si vous n'êtes pas avec succès telnet capable à l'adresse Internet et port, vous pourriez devoir vérifier la connexion réseau et les paramètres du pare-feu externes à l'ESA.

La vérification du succès de telnet à un serveur de réputation de fichier de sur-site sera faite par le même processus qu'affichée.

Entrée de la clé publique

Quand vous introduisez la clé publique sur un ESA exécutant AsyncOS 10.x et plus nouveau, assurez que vous étiez réussi en collant ou en chargeant la clé publique. Toutes les erreurs dans la clé publique seront affichées à la sortie de configuration :

```
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
```

Si vous recevez une erreur, relancez la configuration. Pour des erreurs persistantes, le contact Cisco les prennent en charge.

Logs d'AMP d'examen

Quand vous visualisez le login d'AMP l'ESA, assurez-vous que vous voyez « la requête de réputation de fichier du nuage » spécifié au moment de la requête de réputation de fichier :

```
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
```

Si vous voyez ceci, la requête a tiré la réponse du cache ESA de gens du pays et PAS du groupe configuré de serveur de nuage de réputation :

```
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
```

Erreurs et alertes supplémentaires

Un administrateur ESA pourrait recevoir cet avis. Si ceci est reçu, re-étape par la configuration et le processus de vérification.


```
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
```


Informations connexes

- Adresses du serveur requises pour des exécutions appropriées d'AMP
- Support et documentation techniques - Cisco Systems