Configurar o host estático da reputação do arquivo ou um pool do server da nuvem da reputação do arquivo alternativo no ESA

Índice

Introdução

Este documento descreve como configurar Cisco envia por correio eletrónico a ferramenta de segurança (ESA) para comunicar e usar um host estático ou um pool alternativo do server da nuvem da reputação para a reputação do arquivo com o uso da proteção avançada do malware (AMP).

Informações de Apoio

Uma pergunta da reputação do arquivo é a primeira de duas camadas para o AMP no ESA. Arquive a reputação captura uma impressão digital de cada arquivo como atravessa o ESA e o envia à rede nuvem-baseada da inteligência do AMP para uma sentença da reputação. Dado estes resultados, os administradores ESA podem automaticamente obstruir arquivos maliciosos e aplicar políticas administrador-definidas. O serviço da nuvem da reputação do arquivo é hospedado nos serviços de Web das Amazonas (AW). Quando você executa perguntas DNS contra os hostname descritos neste documento, você verá que ".amazonaws.com" alistou.

A segunda camada de AMP no ESA é análise do arquivo. Isso não é coberto neste documento.

Uma comunicação SSL para o tráfego da reputação do arquivo usa a porta 32137 à revelia. Na altura da configuração do serviço, a porta 443 pôde ser usada como uma alternativa. Consulte o Guia do Usuário ESA, “arquive a reputação que filtra e arquive seção da análise” para detalhes completos. O ESA e os administradores de rede puderam desejar verificar a Conectividade ao pool para o endereço IP de Um ou Mais Servidores Cisco ICM NT, lugar IP, e igualmente movem uma comunicação (32137 contra 443) antes que continuem com a configuração.

Pool do server da nuvem da reputação de AMERICAS(Legacy) do padrão (cloud-sa.amp.sourcefire.com)

A reputação do arquivo é licenciada uma vez, permitido, e configurado em um ESA, será ajustada à revelia para este pool do server da nuvem da reputação:

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

O hostname “cloud-sa.amp.sourcefire.com” é um registro do nome canônico DNS (CNAME). Um CNAME é um tipo de registro de recurso no DNS usado para especificar que um Domain Name é um pseudônimo para um outro domínio, que seja o domínio “canônico”. O hostnamesin associado o pool amarrado a este CNAME pôde ser similar 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)

Há duas escolhas adicionais dos server da reputação do arquivo que podem ser selecionadas:

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

Both of these server são cobertos “na seção dos nomes de host estáticos do server da reputação do arquivo (.cisco.com)” deste documento.

Você pôde verificar os anfitriões que estão associados aos AMERICAS cloud-sa-amp.sourcefire.com CNAME de sua rede a qualquer hora quando você executa esta pergunta da **escavação** ou do **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: Estes anfitriões não são estáticos e recomenda-se não restringir o tráfego da reputação do arquivo ESA baseado somente a estes anfitriões. Os resultados de sua pergunta puderam variar, como os anfitriões no pool mudarão sem aviso prévio.

Você pode verificar a localização geográfica IP desta ferramenta da 3ª parte:

- 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

Nomes de host estáticos do server da reputação do arquivo (.cisco.com)

Cisco começou a fornecer nomes de host baseados “.cisco.com” para o serviço da reputação do arquivo para o AMP em 2016. Há nomes de host estáticos e uns endereços IP de Um ou Mais Servidores Cisco ICM NT disponíveis para a reputação do arquivo deste:

- cloud-sa.amp.cisco.com (America do Norte - USA)
- cloud-sa.eu.amp.cisco.com (Europa – A República da Irlanda)
- cloud-sa.apjc.amp.cisco.com (Ásia-Pacífico – Japão)

Você pôde verificar os anfitriões e os endereços IP de Um ou Mais Servidores Cisco ICM NT associados de sua rede e executar uma pergunta da **escavação** ou do **nslookup**:

America do Norte (E.U.):

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

Europa (a República da 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
```

Ásia-Pacífico (Japão):

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

Você pode verificar a localização geográfica IP desta ferramenta da 3ª parte:

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

Neste tempo, não há nenhum plano para desarmar os nomes de host “.sourcefire.com”.

Pool alternativo do server da nuvem da reputação de EUROPA (cloud-sa.eu.amp.sourcefire.com)

Para European Union (EU) os clientes baseados que são exigidos enviar o tráfego específico somente aos server e aos centros de dados com base nos EU, os administradores podem configurar o ESA para apontar ao host estático EU ou ao pool do server da nuvem da reputação EU:

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

Como o hostname de padrão “cloud-sa.amp.sourcefire.com”, o hostname “cloud-sa.eu.am p.sourcefire.com” é igualmente um CNAME. Os nomes de host associados no pool amarrado a este CNAME puderam ser similares 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)

Você pôde verificar os anfitriões que são associados a cloud-sa.eu.amp.sourcefire.com EUROPEU CNAME de sua rede e executam uma pergunta da **escavação** ou do **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: Estes anfitriões não são estáticos e recomenda-se não restringir o tráfego da reputação do arquivo ESA baseado somente a estes anfitriões. Os resultados de sua pergunta puderam variar, como os anfitriões no pool mudarão sem aviso prévio.

Você pode verificar a localização geográfica IP desta ferramenta da 3ª parte:

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

Configurar o host estático da reputação do arquivo ou um pool do server da nuvem da reputação do arquivo alternativo no ESA

A reputação do arquivo pode ser configurada do GUI ou do CLI no ESA. As etapas de configuração alistadas neste documento demonstrarão a configuração de CLI. Contudo, as mesmas etapas e informação podem ser aplicadas através do GUI (os **Serviços de segurança > a reputação e a análise do arquivo > editam configurações globais… > avançou ajustes para a reputação do arquivo**).

AsyncOS 10.x e mais novo

Os novos recursos de AsyncOS 10.x permitem que o ESA seja configurado para usar uma nuvem privada da reputação (os Em-locais arquivam o server da reputação) ou o server nuvem-baseado da reputação do arquivo. Com esta mudança, a configuração AMP já não alerta para o hostname com “entra a etapa no pool do server da nuvem da reputação”. Você deve escolher setup o server adicional da reputação do arquivo como uma nuvem privada da reputação e fornecer a chave pública para esse hostname.

Para 10.0.x e mais novo, quando você configura um server da reputação da alternativa AMP, você pôde ser exigido incorporar uma chave pública associada a esse hostname.

Todos os server da reputação AMP usam a mesma chave pública:

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

Este exemplo ajudá-lo-á a setup o server alternativo da reputação do arquivo a 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]>
```

Comprometa todas as alterações de configuração.

AsyncOS 9.7.x e mais cedo

Este exemplo em AsyncOS 9.7.2-065 para a Segurança do email ajudá-lo-á acima do pool alternativo do server da nuvem da reputação a 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]>
```

Comprometa todas as alterações de configuração.

Server da reputação do arquivo dos Em-locais (nuvem privada de FireAMP)

O uso do em-locais arquiva o server da reputação, igualmente conhecido como uma nuvem privada de FireAMP, foi introduzido que comece com AsyncOS 10.x para a Segurança do email.

Se você distribuiu um dispositivo privado virtual da nuvem de Cisco AMP em sua rede, você pode agora perguntar a reputação do arquivo de acessórios da mensagem sem enviá-los à nuvem pública da reputação. Para configurar seu dispositivo para usar os em-locais arquivam o server da reputação, consideram do “reputação arquivo filtrar e arquivam o capítulo da análise” no Guia do Usuário ou na ajuda online ESA.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A fim ver o tráfego da reputação do arquivo passar ao pool do server do host estático configurado ou da nuvem da reputação, execute uma captura de pacote de informação do ESA com o filtro especificado para capturar o tráfego da porta 32137 ou da porta 443.

Para este exemplo, use o pool do server da nuvem de cloud-sa.eu.amp.sourcefire.com e uma comunicação SSL com o uso da porta 443…

Isto é registrado ao ESA nos logs 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]>
```

O corredor do rastreamento de pacotes ESA capturou esta conversação:

```
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]>
```

Você vê que o tráfego se comunica sobre a porta 443. De nosso ESA (my11esa.local), comunica-se ao hostname ec2-176-34-122-245.eu-west-1.compute.amazonaws.com. Este hostname é amarrado ao endereço 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]>
```

O endereço IP de Um ou Mais Servidores Cisco ICM NT de 176.34.122.245 é um membro do pool do CNAME para 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]>
```

Para este exemplo, uma comunicação foi dirigida e aceitada pelo pool configurado do server da nuvem da reputação, cloud-sa.eu.amp.sourcefire.com.

Troubleshooting

Esta seção fornece informações que você pode usar na solução de problemas de sua configuração.

Use o telnet para testar a Conectividade

A fim verificar a Conectividade nivelada da porta à nuvem da reputação do arquivo, use o hostname para o pool configurado do server da nuvem da reputação, e teste-o com o **telnet à** porta 32137, ou a porta 443, como configurado.

```
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.
```

Conectividade de Verfiy ao EU, porta excedente bem sucedida 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.
```

Conectividade de Verfiy ao EU, não capaz de conectar sobre a 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
```

Você pode testar o telnet ao IP direto ou os nomes de host atrás do CNAME para o pool do server da nuvem da reputação com o mesmo método do teste do telnet, com o uso da porta 32137 ou da porta 443. Se você não é com sucesso telnet capaz ao hostname e move, você pôde precisar de verificar a conectividade de rede e as configurações de firewall externos ao ESA.

A verificação do sucesso do telnet a um server da reputação do arquivo dos em-locais será feita pelo mesmo processo como mostrado.

Entrada da chave pública

Quando você incorpora a chave pública em um ESA que executa AsyncOS 10.x e mais novo, assegure que você era bem sucedido em colar ou em carregar a chave pública. Todos os erros na chave pública serão indicados às saídas de configuração:

```
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
```

Se você recebe um erro, experimente de novo a configuração. Para erros persistentes, contacte o apoio de Cisco.

Reveja logs AMP

Quando você vê o fazer logon AMP o ESA, assegure-se de que você ver do “a pergunta da reputação arquivo da nuvem” especificada na altura da pergunta da reputação do arquivo:

```
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
```

Se você vê este, a pergunta puxou a resposta do esconderijo local ESA e NÃO do pool configurado do server da nuvem da reputação:

```
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
```

Erros e alertas adicionais

Um administrador ESA pôde receber esta observação. Se isto é recebido, re-etapa com a configuração e o processo de verificação.

```
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
```

Informações Relacionadas

- Endereços do servidor obrigatório para operações apropriadas AMP
- Suporte Técnico e Documentação - Cisco Systems