Настройте статический хост репутации файла или альтернативный облачный пул сервера репутации файла на ESA

Содержание

Введение

Этот документ описывает, как настроить Cisco Email Security Appliance (ESA), чтобы передать и использовать статический хост или альтернативный облачный пул сервера репутации для Репутации Файла в использовании Усовершенствованной вредоносной защиты (AMP).

Общие сведения

Запрос Репутации Файла является первым из двух уровней для AMP на ESA. Репутация файла перехватывает отпечаток пальца каждого файла, поскольку это пересекает ESA и передает его к основанной на облачных вычислениях разведывательной агентуре AMP для вердикта репутации. Учитывая эти результаты, администраторы ESA могут автоматически заблокировать злонамеренные файлы и применить определенную политику администратора. Облачный сервис Репутации Файла размещен на Веб-сервисах Amazon (AWS). При выполнении запросов DNS против имени (имен) хоста, описанного в этом документе вы будете видеть перечисленный ".amazonaws.com".

Второй уровень AMP на ESA является Анализом Файла. Это не покрыто этим документом.

Связь SSL для трафика Репутации Файла использует порт 32137 по умолчанию. Во время конфигурации сервиса порт 443 мог бы использоваться в качестве альтернативы. Консультируйтесь с Руководством пользователя ESA, "Фильтрация Репутации файла и Анализ Файла" разделяют для завершенных подробных данных. ESA и Администраторы сети могли бы хотеть проверить подключение к пулу для IP-адреса (IP-адресов), местоположения IP, и также связи порта (32137 по сравнению с 443) , прежде чем они продолжат конфигурацию.

АМЕРИКИ по умолчанию (Наследство) облачный пул сервера репутации (облако-sa.amp.sourcefire.com)

Как только Репутация Файла лицензируется, включается и настраивается на ESA, по умолчанию она будет установлена для этого облачного пула сервера репутации:

- АМЕРИКИ (Наследство) (облако-sa.amp.sourcefire.com)

Имя хоста "облако-sa.amp.sourcefire.com" является записью Установленного имени DNS (CNAME). CNAME является типом записи ресурса в DNS, используемом, чтобы указать, что доменное имя является псевдонимом для другого домена, который является "каноническим" доменом. Связанные имена хоста в пуле, связанном к этому CNAME, могли бы быть подобны:

- 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)

Существует два дополнительных выбора серверов репутации файла, которые могут быть выбраны:

- АМЕРИКИ (облако-sa.amp. cisco . com)
- ЕВРОПА (облако-sa.eu.amp. cisco . com)

Оба из этих серверов покрыты "Статическими именами хоста сервера Репутации Файла (.cisco.com)" раздел этого документа.

Вы могли бы проверить хосты, которые привязаны к АМЕРИКАМ cloud-sa-amp.sourcefire.com CNAME от вашей сети в любое время, когда вы работаете, это **роет** или запрос **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
```

> **Примечание:** Эти хосты не статичны, и рекомендуется НЕ ограничить трафик Репутации Файла ESA, основанный только этими хостами. Результаты вашего запроса могли бы варьироваться, поскольку хосты в пуле изменятся без предупреждения.

Можно проверить географическое месторасположение IP от этого программного средства третьей стороны:

- 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

Статические имена хоста сервера Репутации Файла (.cisco.com)

Cisco начала предоставлять основанные имена хоста ".cisco.com" для сервиса Репутации Файла для AMP в 2016. Существуют статические имена хоста и IP-адреса, доступные для Репутации Файла от этого:

- облако-sa.amp. cisco . com (Северная Америка - USA)
- облако-sa.eu.amp. cisco . com (Европа – Ирландская Республика)
- облако-sa.apjc.amp. cisco . com (Азиатско - тихоокеанское побережье – Япония)

Вы могли бы проверить хосты и привязали IP-адреса от вашей сети, и выполните запрос **nslookup** или **рыть**:

Северная Америка (US):

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

Европа (Ирландская Республика):

```
$ 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
```

Азиатско - тихоокеанское побережье (Япония):

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

Можно проверить географическое месторасположение IP от этого программного средства третьей стороны:

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

В это время нет никаких планов списать ".sourcefire.com" имена хоста.

Альтернативный ЕВРОПЕЙСКИЙ облачный пул сервера репутации (облако-sa.eu.amp.sourcefire.com)

Поскольку Европейский Союз (EU) базировал клиентов, которые обязаны передавать определенный трафик к находящемуся в EU только серверы и ЦОД, администраторы могут настроить ESA для обращения или к статическому хосту EU или к облачному пулу сервера репутации EU:

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

Как имя хоста по умолчанию "облако-sa.amp.sourcefire.com", имя хоста "облако-sa.eu.amp.sourcefire.com" является также CNAME. Связанные имена хоста в пуле, связанном к этому CNAME, могли бы быть подобны:

- 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)

Вы могли бы проверить хосты, которые привязаны к облачному-sa.eu.amp.sourcefire.com CNAME EUROPEAN от вашей сети и выполняют запрос **nslookup** или **рыть**::

```
$ 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
```

> **Примечание:** Эти хосты не статичны, и рекомендуется НЕ ограничить трафик Репутации Файла ESA, основанный только этими хостами. Результаты вашего запроса могли бы варьироваться, поскольку хосты в пуле изменятся без предупреждения.

Можно проверить географическое месторасположение IP от этого программного средства третьей стороны:

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

Настройте статический хост репутации файла или

альтернативный облачный пул сервера репутации файла на ESA

Репутация файла может быть настроена или от GUI или от CLI на ESA. Действия настройки, перечисленные в этом документе , продемонстрируют конфигурацию интерфейса командой строки. Однако те же шаги и информация могут быть применены через GUI (**Сервисы безопасности>, Репутация Файла и Анализ> Редактируют Глобальные параметры...> Расширенные настройки для Репутации Файла**).

AsyncOS 10.x и более новый

Новые характеристики AsyncOS 10.x позволяют ESA быть настроенным для использования частного облака репутации (Собственный Сервер Репутации Файла) или основанный на облачных вычислениях сервер репутации файла. С этим изменением конфигурация AMP больше не вызывает для имени хоста с , "Вводят облачный шаг" пула сервера репутации. Необходимо принять решение установить дополнительный сервер репутации файла как частное облако репутации и предоставить открытый ключ для того имени хоста.

Для 10.0.x и более новый при настройке альтернативного сервера репутации AMP вы могли бы быть обязаны вводить открытый ключ, привязанный к тому имени хоста.

Все серверы репутации AMP используют тот же открытый ключ:

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

Данный пример поможет вам устанавливать альтернативный сервер репутации файла для объединения в облако:

```
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]>
```

Передайте любые изменения конфигурации.

AsyncOS 9.7.x и ранее

Данный пример на AsyncOS 9.7.2-065 для Безопасности электронной почты поможет вам альтернативный облачный пул сервера репутации объединяться-в-облако-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]>
```

Передайте любые изменения конфигурации.

Собственный сервер репутации файла (закрытое облако FireAMP)

Использование собственного сервера репутации файла, также известного как Закрытое облако FireAMP, было начато, который запускается с AsyncOS 10.x для Безопасности электронной почты.

При развертывании AMP Cisco Действительное устройство Закрытого облака в сети можно теперь сделать запрос репутации файла прикреплений сообщения, не передавая им к общему облаку репутации. Для настройки устройства для использования собственного сервера репутации файла посмотрите “Фильтрацию Репутации файла и Аналитическую главу” Файла в Руководстве пользователя ESA или онлайновой справке.

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Чтобы видеть, что трафик Репутации Файла проходит к настроенному статическому хосту или облачному пулу сервера репутации, выполните захват пакета от ESA с указанным фильтром для получения трафика порта 32137 или порта 443.

Для данного примера используйте облачный-sa.eu.amp.sourcefire.com облачный пул сервера и связь SSL с использованием порта 443...

Это зарегистрировано к ESA в журналах 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]>
```

Выполнение трассировки пакетов ESA перехватило этот диалог:

```
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]>
```

Вы видите, что трафик связывается по порту 443. От нашего ESA (my11esa.local), это связывается с именем хоста ec2-176-34-122-245.eu-west-1.compute.amazonaws.com. Это имя хоста связано к IP-адресу 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]>
```

IP-адрес 176.34.122.245 является участником пула CNAME для облака-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]>
```

Для данного примера связь была направлена и принята настроенным облачным пулом сервера репутации, облаком-sa.eu.amp.sourcefire.com.

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

Используйте Telnet для тестирования подключения

Для проверки подключения уровня порта к облаку Репутации Файла используйте имя хоста для настроенного облачного пула сервера репутации и тест с **telnet** к порту 32137 или порту 443, согласно конфигурации.

```
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.
```

Подключение Verfiy в EU, успешный по порту 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.
```

Подключение Verfiy в EU, который не в состоянии соединиться по порту 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
```

Можно протестировать telnet к прямому IP или именам хоста позади CNAME для облачного пула сервера репутации с тем же методом тестирования telnet с использованием порта 32137 или порта 443. Если вы не в состоянии к успешно telnet к имени хоста и порту, вы, возможно, должны были бы проверить сетевое подключение и параметры межсетевого экрана, внешние к ESA.

Проверка успеха telnet к собственному серверу репутации файла будет сделана тем же процессом как показано.

Ввод открытого ключа

При вводе открытый ключ в ESA рабочий AsyncOS 10.x и более новый, гарантируете, что были успешны во вставке или загрузке открытого ключа. Любые ошибки в открытом ключе будут отображены к выходным данным конфигурации:

```
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
```

При получении ошибки повторите конфигурацию. Для повторяющихся ошибок свяжитесь с Поддержкой Cisco.

Журналы AMP анализа

Когда вы просматриваете вход в систему AMP ESA, гарантируете , что видите, "что репутация файла сделала запрос от Облака", заданного во время запроса репутации файла:

```
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
```

Если вы видите это, запрос вытянул ответ от локального кэша ESA a НЕ от настроенного облачного пула сервера репутации:

```
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
```

Дополнительные ошибки и предупреждения

Администратор ESA мог бы получить это предупреждение. Если это получено, перешаг через конфигурацию и процесс проверки.

```
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
```

Дополнительные сведения

- Адреса нужного сервера для надлежащих операций AMP
- Cisco Systems – техническая поддержка и документация