Содержание

Введение

Этот документ описывает предупреждение, приписанное Cisco Email Security Appliance (ESA) с Усовершенствованной вредоносной защитой (AMP), включенной на нем, куда сервис не связывается по порту 443 для Уровня защищенных сокетов (SSL).

Корректный "Сервис Репутации Файла в облаке является недостижимой" Ошибкой, Полученной для AMP

AMP был освобожден для использования на ESA в Версии 8.5.5 AsyncOS и позже. С лицензируемым AMP и включил на ESA, администраторы получают это сообщение:

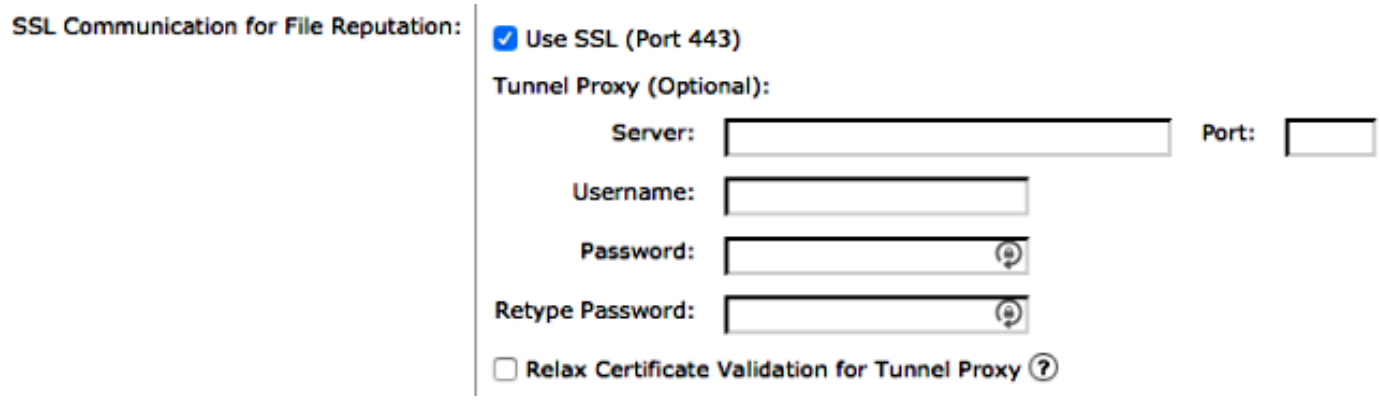
Сервис AMP мог бы быть включен, но вероятно не связывается по порту 443.

Чтобы гарантировать, что AMP передает более чем 443, выполните **ampconfig> усовершенствованный** от CLI и быть уверенными, что **Y** выбран для **вас, хотят включить связь SSL (порт 443) для репутации файла? [Y]>**:

```
> 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


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- 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]>

Do you want use the recommended reputation threshold from cloud service? [Y]>

Enter file analysis server URL?
[https://intel.api.sourcefire.com]>

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]>
```

При использовании GUI нажмите **Security Services> File Reputation и Analysis> Edit Global Settings> (выпадающий) Advanced** и гарантируйте, что флажок **Use SSL** включен как показано здесь:



Передайте любого и все изменения к вашей конфигурации.

Наконец, рассмотрите текущий журнал AMP для наблюдения успешности или неуспешности подключения и сервиса. Можно выполнить это от CLI с **хвостовым усилителем**.

До изменений, внесенных в **ampconfig>, совершенствовался**, вы видели бы это в журналах AMP:

```
> 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


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- 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]>

Do you want use the recommended reputation threshold from cloud service? [Y]>

Enter file analysis server URL?
[https://intel.api.sourcefire.com]>

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]>
```

После того, как изменение делается в **ampconfig> усовершенствованным**, вы видите это в журналах AMP:

```
> 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


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- 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]>

Do you want use the recommended reputation threshold from cloud service? [Y]>

Enter file analysis server URL?
[https://intel.api.sourcefire.com]>

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]>
```

amp_watchdog.txt файл отображается каждые 10 минут в журналах. Этот файл является частью поддержки активности для AMP.

В журналах AMP обычный запрос был бы подобен этому:

```
> 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


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- 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]>

Do you want use the recommended reputation threshold from cloud service? [Y]>

Enter file analysis server URL?
[https://intel.api.sourcefire.com]>

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]>
```

С этой информацией, должна существовать возможность для корреляции Идентификатора сообщения (MID) в почтовых журналах.

Устранение неполадок

Межсетевой экран анализа и настройки сети, чтобы гарантировать, что связь SSL открыта для них:

Порт	Протокол	Входящий/исходящий	Host name	Описание
443	TCP	/*	Согласно конфигурации в Сервисах безопасности> Репутация Файла и Анализ, Усовершенствованный раздел.	Доступ к облачны сервисам для ана файла.
32137	TCP	/*	Согласно конфигурации в Сервисах безопасности> Репутация Файла и Анализ, Усовершенствованный раздел, Усовершенствованный раздел, Облачный параметр Пула Сервера.	Доступ к облачны сервисам для получения репута файла.

Можно протестировать основное подключение от ESA до облачного сервиса более чем 443 через Telnet, чтобы гарантировать, что устройство может успешно достигнуть сервисов AMP.

> **Примечание:** Адреса для Анализа Репутации и Файла Файла настроены на CLI с **ampconfig> усовершенствованный**, или от GUI с **Сервисами безопасности>, Репутация Файла и Анализ> Редактируют Глобальные параметры> Усовершенствованный (выпадающий)**.

Пример Репутации файла:

```
ironport:service 36] telnet cloud-sa.amp.sourcefire.com 443
Trying 184.73.186.190...
Connected to cloud-sa.amp.sourcefire.com.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

Аналитический пример файла:

```
ironport:service 37] telnet intel.api.sourcefire.com 443
Trying 198.148.79.52...
Connected to intel.api.sourcefire.com.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

Дополнительные сведения

- Тест Усовершенствованной вредоносной защиты (AMP) ESA
- Руководства пользователя ESA
- Часто задаваемые вопросы ESA: Что такое Идентификатор сообщения (MID), Инжекционный Идентификатор соединения (ICID) или Идентификатор соединения Доставки (DCID)?
- То, как я ищу и просматриваю почту, входит в систему ESA?