Ошибки в связи с прерывания TLS сервисного модуля NGFW для квитирования ошибки сбоя или проверки достоверности сертификата

Содержание

Введение

Этот документ описывает, как устранить неполадки конкретной проблемы с доступом к основанным на HTTPS веб-сайтам через Cisco Межсетевой экран Следующего поколения (NGFW) сервисный модуль с включенной расшифровкой.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Процедуры квитирования Уровня защищенных сокетов (SSL)
- Сертификаты SSL

Используемые компоненты

Сведения в этом документе основываются на Cisco сервисный модуль NGFW с Cisco Главный Менеджер безопасности (PRSM) Версия 9.2.1.2 (52).

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были

запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

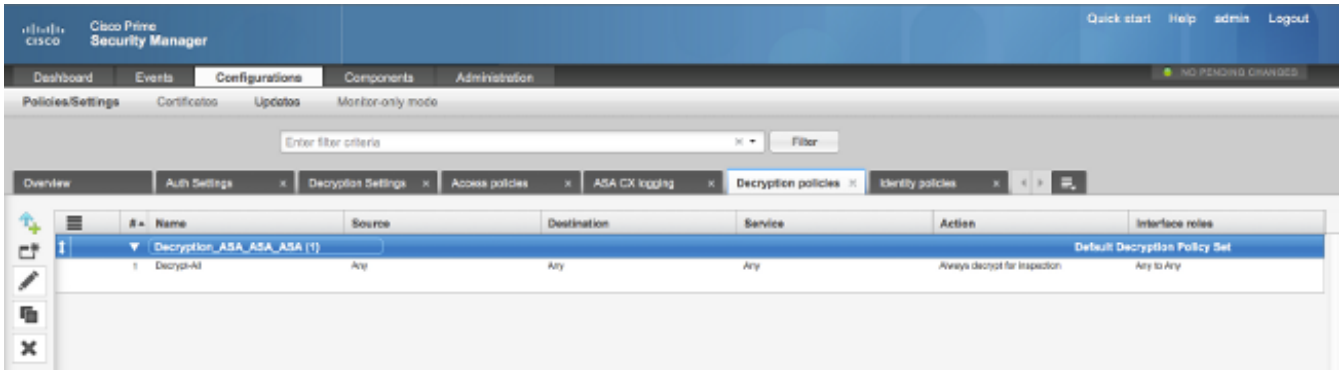
Общие сведения

Расшифровка является функцией, которая позволяет сервисному модулю NGFW дешифровать зашифрованные SSL потоки (и осмотреть диалог, который иначе зашифрован), и принудите политику по трафику. Для настройки этой функции администраторы должны настроить сертификат расшифровки на модуле NGFW, который представлен доступу клиента основанные на HTTPS веб-сайты вместо сертификата исходного сервера.

Для расшифровки для работы модуль NGFW должен доверять представленному серверу сертификату. Этот документ объясняет сценарии, когда подтверждение связи SSL отказывает между сервисным модулем NGFW и сервером, который заставляет определенные основанные на HTTPS веб-сайты отказывать, когда вы пытаетесь достигнуть их.

В целях этого документа эта политика определена на сервисном модуле NGFW с PRSM:

- **Политики идентификации**: нет никаких определенных политик идентификации.
- **Политика расшифровки**: **Дешифрование - Вся** политика использует эту конфигурацию:

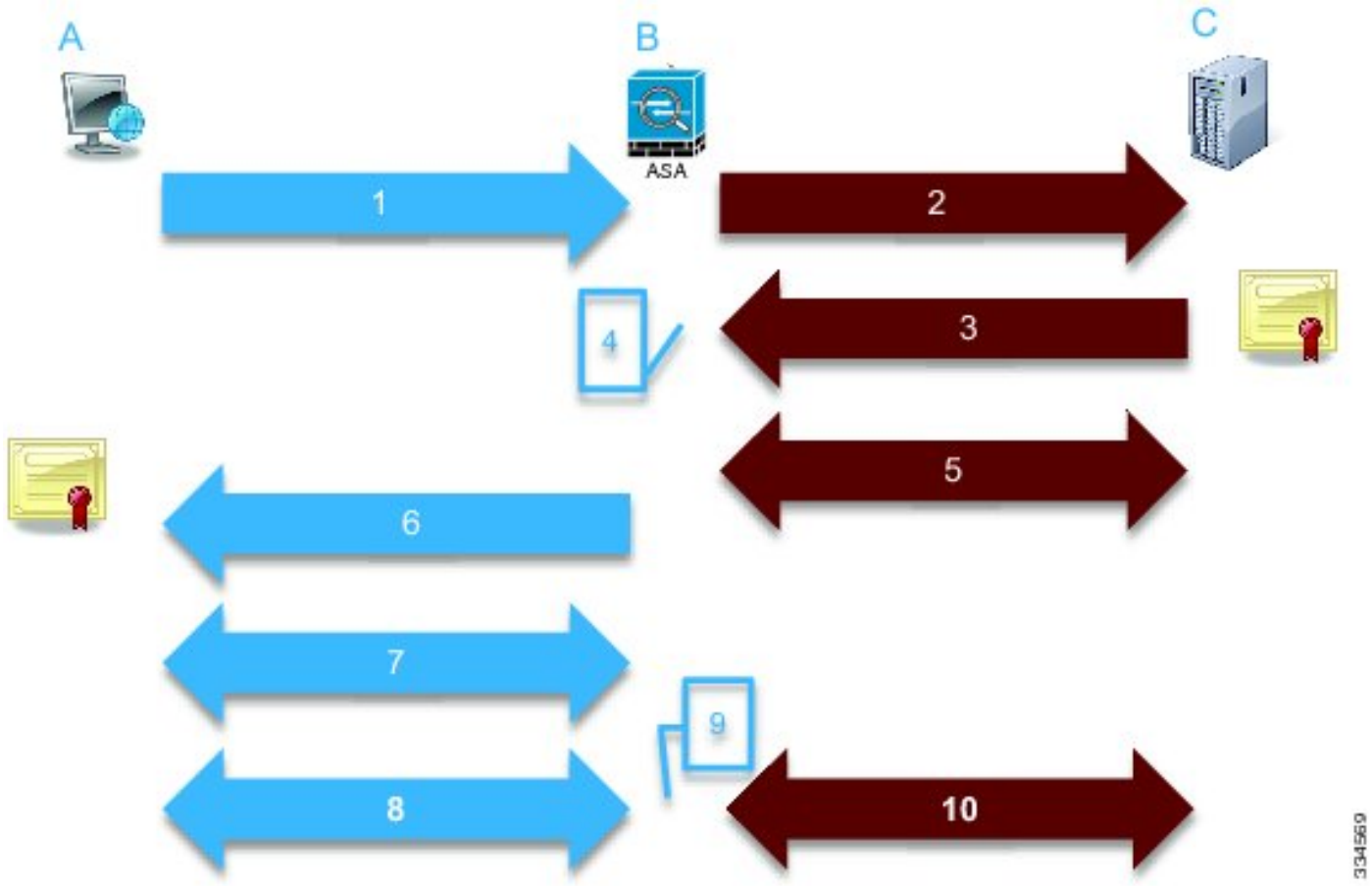


- **Политика доступа**: нет никакой определенной политики доступа.
- **Параметры настройки расшифровки**: Этот документ предполагает, что **сертификат Расшифровки** настроен на сервисном модуле NGFW и что клиенты доверяют ему.

Когда политика расшифровки определена на сервисном модуле NGFW и настроена, как ранее описано, сервисный модуль NGFW пытается перехватить весь зашифрованный поток данных SSL через модуль и дешифровать.

> **Примечание:** Пошаговое пояснение этого процесса доступно в Дешифрованном разделе Трафика Руководства пользователя для CX ASA и Cisco Главный Менеджер безопасности 9.2.

Этот образ изображает последовательность событий:



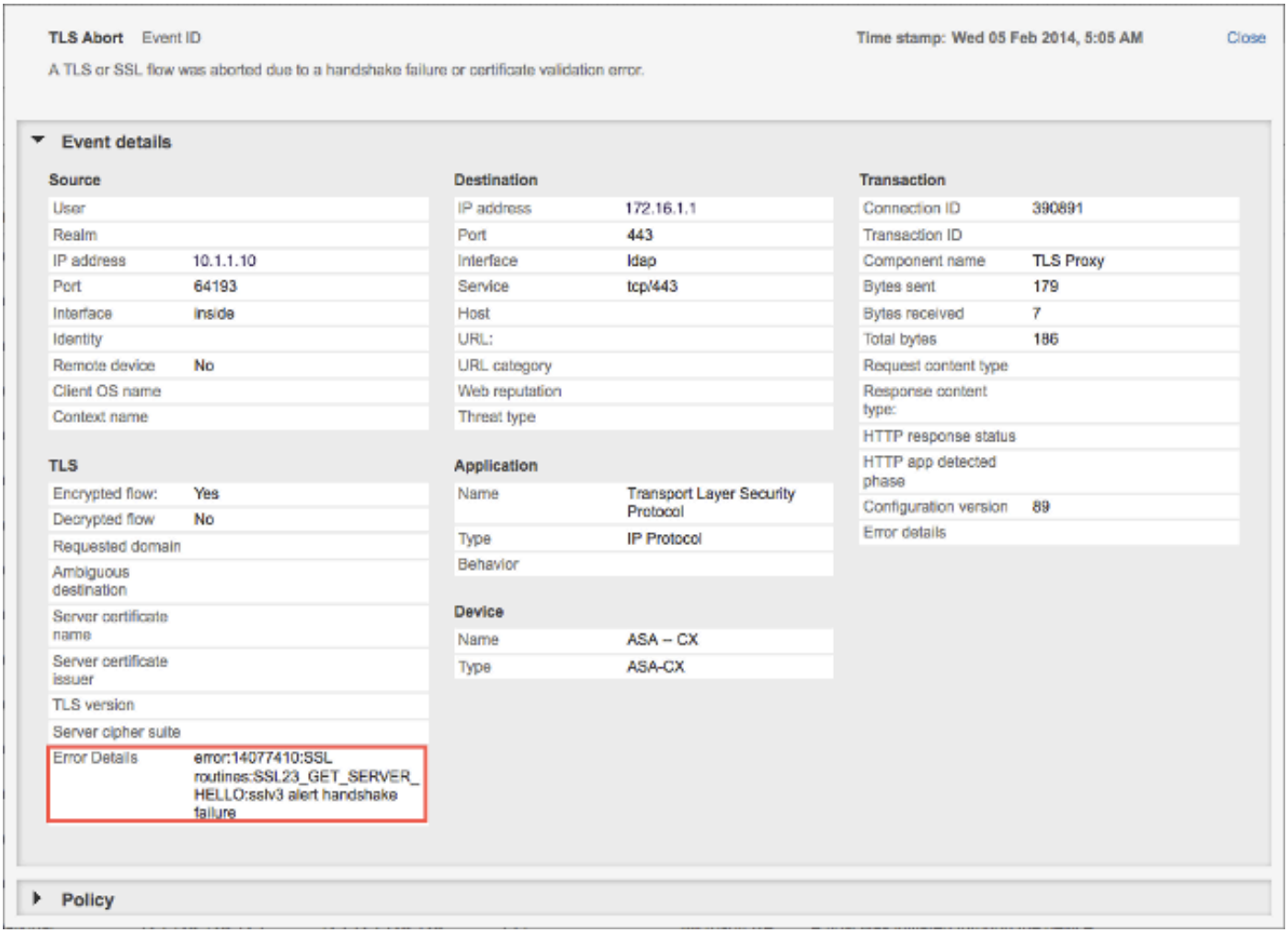
В этом образе **A** является клиентом, **B** является сервисным модулем NGFW, и **C** является сервером HTTPS. Для примеров, предоставленных в этом документе, основанный на HTTPS сервер является Cisco Adaptive Security Device Manager (ASDM) на устройстве адаптивной защиты Cisco (ASA).

Существует два важных фактора об этом процессе, который необходимо рассмотреть:

- В действии второе процесса сервер должен принять один из наборов шифров SSL, которые представлены сервисным модулем NGFW.
- В четвертом шаге процесса сервисный модуль NGFW должен доверять сертификату, который представлен сервером.

Проблема

Если сервер не может принять ни один из шифров SSL, которые представлены сервисным модулем NFGW, вы получаете сообщение об ошибках, подобное этому:



Важно принять во внимание (выделенную) информацию о Деталях ошибки, который показывает:

```
error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure
```

При просмотре **/var/log/cisco/tls_proxy.log** файла в архиве диагностики модуля эти сообщения об ошибках появляются:

```
2014-02-05 05:21:42,189 INFO  TLS_Proxy   - SSL alert message received from
 server (0x228 = "fatal : handshake failure") in Session: x2fd1f6

2014-02-05 05:21:42,189 ERROR TLS_Proxy - TLS problem (error:14077410:
 SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure) while
 connecting to server for Session: x2fd1f6
```

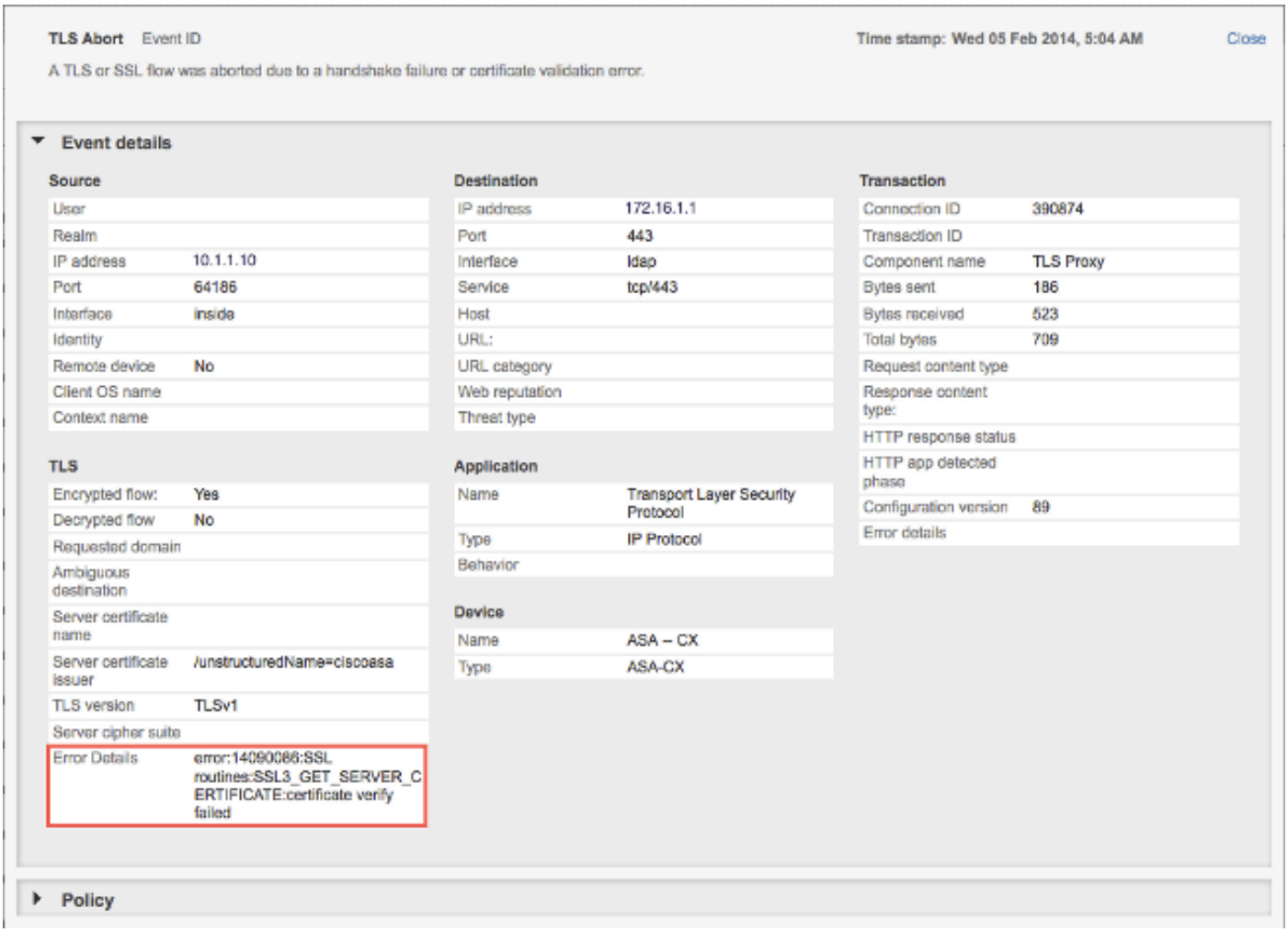
Решение

Одна возможная причина для этой проблемы - то, что Стандарт тройного шифрования данных / Расширенный стандарт шифрования (3DES/AES) лицензия (часто называемый K9) не установлен на модуле. Можно загрузить лицензию K9 на модуль бесплатно и загрузить его через PRSM.

Если проблема сохраняется после того, как вы устанавливаете лицензию 3DES/AES, то получаете захваты пакета для подтверждения связи SSL между сервисным модулем NGFW и сервером, и связываетесь с администратором сервера для включения соответствующего шифра (шифров) SSL на сервере.

Проблема

Если сервисный модуль NGFW не доверяет сертификату, который представлен сервером, то вы получаете сообщение об ошибках, подобное этому:



TLS Abort Event ID — Time stamp: Wed 05 Feb 2014, 5:04 AM — Close

A TLS or SSL flow was aborted due to a handshake failure or certificate validation error.

Event details

Source	
User	
Realm	
IP address	10.1.1.10
Port	64186
Interface	inside
Identity	
Remote device	No
Client OS name	
Context name	

Destination	
IP address	172.16.1.1
Port	443
Interface	idap
Service	tcp/443
Host	
URL:	
URL category	
Web reputation	
Threat type	

Transaction	
Connection ID	390874
Transaction ID	
Component name	TLS Proxy
Bytes sent	186
Bytes received	523
Total bytes	709
Request content type	
Response content type:	
HTTP response status	
HTTP app detected phase	
Configuration version	89
Error details	

TLS	
Encrypted flow:	Yes
Decrypted flow	No
Requested domain	
Ambiguous destination	
Server certificate name	
Server certificate issuer	/unstructuredName=ciscoasa
TLS version	TLSv1
Server cipher suite	
Error Details	error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed

Application	
Name	Transport Layer Security Protocol
Type	IP Protocol
Behavior	

Device	
Name	ASA – CX
Type	ASA-CX

Policy

Важно принять во внимание (выделенную) информацию о Деталях ошибки, который показывает:

```
error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
```

При просмотре **/var/log/cisco/tls_proxy.log** файла в архиве диагностики модуля эти сообщения об ошибках появляются:

```
2014-02-05 05:22:11,505 INFO  TLS_Proxy - Certificate verification failure:
 self signed certificate (code 18, depth 0)

2014-02-05 05:22:11,505 INFO TLS_Proxy - Subject: /unstructuredName=ciscoasa

2014-02-05 05:22:11,505 INFO TLS_Proxy - Issuer: /unstructuredName=ciscoasa

2014-02-05 05:22:11,505 INFO TLS_Proxy - SSL alert message received from
 server (0x230 = "fatal : unknown CA") in Session: x148a696e

2014-02-05 05:22:11,505 ERROR TLS_Proxy - TLS problem (error:14090086:
 SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed) while
 connecting to server for Session: x148a696e
```

Решение

Если модуль неспособен доверять сертификату SSL сервера, необходимо импортировать серверный сертификат в модуль с PRSM, чтобы гарантировать, что процесс подтверждения связи SSL успешен.

Выполните эти шаги для импорта серверного сертификата:

1. Обойдите сервисный модуль NGFW при доступе к серверу для загрузки сертификата через браузер. Один способ обойти модуль состоит в том, чтобы создать политику расшифровки, которая не дешифрует трафик к тому индивидуальному серверу. Это видео показывает вам, как создать политику:

   Это шаги, которые показывают в видео:

   Для доступа к PRSM на CX перейдите к **https://<IP_ADDRESS_OF_PRSM>**. Данный пример использует **https://10.106.44.101**.

   Перейдите к **Конфигурациям> Политика/Параметры настройки> Политика расшифровки** в PRSM.

   Нажмите значок, который расположен около верхнего левого угла экрана, и выберите **Add выше опции policy** для добавления политики к вершине списка.

   Назовите политику, оставьте Источник как **Любого** и создайте объект **Группы организации сети CX**.
   Примечание: Не забудьте включать IP-адрес основанного на HTTPS сервера. В данном примере используется IP-адрес **172.16.1.1**.Выберите **Do not decrypt for the Action**.

   Сохраните политику и передайте изменения.
2. Загрузите серверный сертификат через браузер и загрузите его к сервисному модулю NGFW через PRSM, как показано в этом видео:

   Это шаги, которые показывают в видео:

   Как только ранее упомянутая политика определена, используйте браузер для навигации к основанному на HTTPS серверу, который открывается через сервисный модуль NGFW.
   Примечание: В данном примере Версия 26.0 Mozilla Firefox используется для навигации к серверу (ASDM на ASA) с URL **https://172.16.1.1**.Примите предупреждение системы безопасности, если вы раскрываетесь, и добавьте Исключение безопасности.

   Нажмите маленький значок формы блокировки, расположенный налево от строки адреса. Местоположение этого значка варьируется на основе браузера, который используется и версия.

   Нажмите кнопку **View Certificate** и затем кнопку **Export** под вкладкой Details после выбора серверного сертификата.

Сохраните сертификат на своей персональной машине в местоположении по Вашему выбору.

Войдите в PRSM и перейдите к **Конфигурациям> Сертификаты**.

Нажмите **я хочу...> Сертификат импорта** и выбрал ранее загруженный серверный сертификат (из Шага 4).

Сохраните и передайте изменения. Однажды завершенный, сервисный модуль NGFW должен доверять сертификату, который представлен сервером.

3. Удалите политику, которая была добавлена в Шаге 1. Сервисный модуль NGFW теперь в состоянии завершить квитирование успешно с сервером.

Дополнительные сведения

- Руководство пользователя для CX ASA и Cisco Главный Менеджер безопасности 9.2
- Cisco Systems – техническая поддержка и документация