Клиент AnyConnect воссоединяется каждую минуту который причины разрушение в трафике

Содержание

Введение

Этот документ обсуждает определенный сценарий, где клиент AnyConnect мог бы воссоединиться с Устройством адаптивной защиты (ASA) точно через одну минуту. Пользователи не могли бы быть в состоянии получить трафик по туннелю Transport Layer Security (TLS), пока не повторно соединяется AnyConnect. Это зависит от нескольких других факторов, которые обсуждены в этом документе.

Компоненты, на которые влияют,

- Выпуск 9.0 ASA или выпуск 9.1
- Релиз клиента AnyConnect 3.0 или выпуск 3.1

Признаки

В данном примере показывают клиента AnyConnect, поскольку он повторно соединяется с ASA.

Этот системный журнал замечен на ASA:

```
%ASA-6-722036: Group <ac_users_group> User <vpn> IP <10.1.75.111>
Transmitting large packet 1418 (threshold 1347).
```

Описание проблемы

Эти журналы Диагностики и средства создания отчетов (DART) замечены с этой проблемой:

```
****************************************

Date        : 11/16/2013
Time        : 01:28:50
Type        : Warning
Source      : acvpnagent

Description : Reconfigure reason code 16:
New MTU configuration.

****************************************

Date        : 11/16/2013
Time        : 01:28:50
Type        : Information
Source      : acvpnagent

Description : The entire VPN connection is being reconfigured.

****************************************

Date        : 11/16/2013
Time        : 01:28:51
Type        : Information
Source      : acvpnui

Description : Message type information sent to the user:
Reconnecting to 10.1.1.2...

****************************************

Date        : 11/16/2013
Time        : 01:28:51
Type        : Warning
Source      : acvpnagent

Description : A new MTU needs to be applied to the VPN network interface.
Disabling and re-enabling the Virtual Adapter. Applications utilizing the
private network may need to be restarted.


****************************************
```

Причины

Причиной этой проблемы является сбой для построения туннеля Протокола защиты транспортного уровня для дейтаграмм (DTLS). Это могло быть из-за двух причин:

- DTLS заблокирован где-нибудь в пути
- Использование ня по умолчанию порт DTLS

DTLS Заблокирован Где-нибудь в Пути

С Выпуска 9.x ASA и Выпуска 3.x AnyConnect, оптимизация была представлена в форме отдельных Максимальных Модулей Перехода (MTU), о которых выполняют согласование относительно TLS/DTLS между клиентом/ASA. Ранее, клиент получил MTU приближенной оценки, который покрыл и TLS/DTLS и был, очевидно, менее, чем оптимален. Теперь, ASA вычисляет служебную информацию при инкапсуляции и для TLS/DTLS и получает значения MTU соответственно.

Целый DTLS включен, клиент применяет MTU DTLS (в этом случае 1418) на адаптере VPN (который включен, прежде чем туннель DTLS установлен и необходим для осуществления маршрутов/фильтров), для обеспечения оптимальной производительности. Если туннель DTLS не может быть установлен, или он отброшен в некоторый момент, клиентские переключения при отказе к TLS и отрегулировал MTU на виртуальном адаптере (VA) к значению MTU TLS (это требует, чтобы сеансовый уровень повторно соединился).

Разрешение

Для устранения этого видимого перехода DTLS> TLS, администратор может настроить группу отдельного туннеля для TLS, только обращаются для пользователей, которые испытывают затруднения из-за установления туннеля DTLS (такой как из-за ограничений межсетевого экрана).

1. Наилучший вариант состоит в том, чтобы заставить значение MTU AnyConnect быть ниже, чем MTU TLS, о котором тогда выполняют согласование.`group-policy ac_users_group attributes`
   `webvpn`
   `anyconnect mtu 1300` Это делает TLS и значения MTU DTLS равными. Повторные соединения не замечены в этом случае.
2. Вторая опция должна позволить фрагментацию. `group-policy ac_users_group attributes`
   `webvpn`
   `anyconnect ssl df-bit-ignore enable`С фрагментацией большие пакеты (чей размер превышает значение MTU) могут быть фрагментированы и переданы через туннель TLS.
3. Третья опция должна установить Maximum Segment Size (MSS) в 1460 следующим образом:`sysopt conn tcpmss 1460` В этом случае MTU TLS будет 1427 (RC4/SHA1), который больше, чем MTU DTLS 1418 (AES/SHA1/LZS). Это должно решить вопрос с TCP от ASA до клиента AnyConnect (благодаря MSS), но большой трафик UDP от ASA до клиента AnyConnect мог бы пострадать от этого, поскольку это будет отброшено клиентом AnyConnect из-за более низкого MTU клиента AnyConnect 1418. Если **sysopt ведет tcpmss**, модифицируется, это могло бы влиять на другие функции, такие как LAN-LAN (L2L) VPN-туннели IPSec.

Использование ня по умолчанию порт DTLS

Другая потенциальная причина для сбоя DTLS включает DTLS на порту ня по умолчанию после того, как WebVPN включают (например, когда **webvpn enable вне** команды введен). Это происходит из-за идентификатора ошибки Cisco CSCuh61321 и было замечено в

Выпуске 9.x, где ASA выдвигает порт ня по умолчанию клиенту, но продолжает слушать порт по умолчанию. Следовательно, DTLS не создан, и AnyConnect повторно соединяется.

```
webvpn
 port 444
 enable outside
 dtls port 444
 anyconnect enable

ciscoasa(config-webvpn)# show asp table socket


Protocol Socket   State     Local Address            Foreign Address
SSL      0001fc08 LISTEN    172.16.11.1:444           0.0.0.0:*

DTLS     00020dc8 LISTEN    172.16.11.1:443          0.0.0.0:*
```

После того, как туннель TLS установлен, клиент пытается установить туннель DTLS к порту 444 как ожидалось:

Заказ команд, которые приводят к проблеме и открытым сокетам таблицы ускоренного пути безопасности (ASP):

1. Запустите с сокетов WebVPN, не включенных.
```
ciscoasa(config)# show run webvpn
webvpn
 anyconnect image disk0:/anyconnect-win-3.1.04066-k9.pkg 1
 anyconnect enable


ciscoasa(config)# show asp table socket
Protocol Socket   State     Local Address            Foreign Address
ciscoasa(config)#
```
2. Порт TLS изменения к 444 и включает WebVPN.
```
ciscoasa(config-webvpn)# show run webvpn
webvpn
 port 444
 enable outside
 anyconnect image disk0:/anyconnect-win-3.1.04066-k9.pkg 1
 anyconnect enable


ciscoasa(config-webvpn)# show asp tabl socket
Protocol Socket   State     Local Address            Foreign Address
SSL      0001fc08 LISTEN    172.16.11.1:444          0.0.0.0:*
DTLS     00020dc8 LISTEN    172.16.11.1:443          0.0.0.0:*
```
3. Измените порт DTLS на 444.
```
ciscoasa(config-webvpn)# dtls port 444
ciscoasa(config-webvpn)#
ciscoasa(config-webvpn)# show run webvpn
webvpn
 port 444
 enable outside
 dtls port 444
 anyconnect image disk0:/anyconnect-win-3.1.04066-k9.pkg 1
 anyconnect enable

ciscoasa(config-webvpn)# show asp table socket


Protocol Socket   State     Local Address           Foreign Address
SSL      0001fc08 LISTEN    172.16.11.1:444          0.0.0.0:*
DTLS     00020dc8 LISTEN    172.16.11.1:443         0.0.0.0:*
```

Примечание: Порт сокета DTLS все еще 443. На этом этапе клиенты AnyConnect

устанавливают DTLS к 444 хотя!

Разрешение

Обходной путь для этой проблемы должен придерживаться заказа:

1. Отключите WebVPN.
2. Введите порт DTLS.
3. Включите WebVPN.

Это поведение не существует в версиях Выпуска 8.4.x, где сокеты DTLS сразу обновлены с настраиваемыми портами после того, как введена конфигурация:

Выпуск 8.4.6 ASA:

```
ciscoasa(config-webvpn)# port 444
ciscoasa(config-webvpn)# enable outside
ciscoasa(config-webvpn)# show asp table socket

Protocol Socket Local Address Foreign Address State
SSL 0000bf2f 172.16.11.1:444 0.0.0.0:* LISTEN
DTLS 0000d5df 172.16.11.1:443 0.0.0.0:* LISTEN

ciscoasa(config-webvpn)# dtls port 444
ciscoasa(config-webvpn)#
ciscoasa(config-webvpn)# show asp table socket

Protocol Socket Local Address Foreign Address State
SSL 0000bf2f 172.16.11.1:444 0.0.0.0:* LISTEN
DTLS 0000eb5f 172.16.11.1:444 0.0.0.0:* LISTEN << changed immediately
```

Повторно подключите поток операций

Предположим, что настроены эти шифры:

```
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1
```

Эта последовательность событий имеет место в этом случае:

- AnyConnect устанавливает родительский туннель и туннель данных TLS с SHA RC4 как шифрование SSL.
- DTLS заблокирован в пути, и туннель DTLS не может быть установлен.
- ASA объявляет о параметрах AnyConnect, который включает TLS и значения MTU DTLS, которые являются двумя отдельными значениями.
- MTU DTLS является 1418 по умолчанию.
- MTU TLS вычислен от **sysopt, ведут** значение **tcpmss** (по умолчанию является 1380). Это - то, как MTU TLS получен (как замечено по **debug webvpn anyconnect** выходные данные):
  `1380 - 5 (TLS header) - 8 (CSTP) - 0 (padding) - 20 (HASH) = 1347`
- AnyConnect переводит адаптер VPN в рабочее состояние и назначает MTU **DTLS** на него в ожидании, что это будет в состоянии соединиться через DTLS.
- Клиент AnyConnect теперь связан, и пользователь переходит к определенному веб-сайту.

- Браузер передает SYN TCP и устанавливает MSS = 1418-40 = 1378 в нем.
- Сервер HTTP на внутренней части ASA передает пакеты размера 1418.
- ASA не может поместить их в туннель и не может фрагментировать их, поскольку им установили бит "Не фрагментировать" (DF).
- Печать ASA`%ASA-6-722036: Group <ac_users_group> User <vpn> IP <10.1.75.111> Transmitting large packet 1418 (threshold 1347)`и пакеты отбрасываний с mp-svc-no-fragment-ASP отбрасывают причину.
- В то же время ASA передает Недостижимому Назначению ICMP, Необходимая Фрагментация к отправителю:

```
    %ASA-6-602101: PMTU-D packet 1418 bytes greater than effective mtu 1347,
dest_addr=10.10.10.1, src_addr=10.48.66.200, prot=TCP
```

- Если Протокол ICMP позволен, то отправитель повторно передает отброшенные пакеты, и все начинает работать. Если ICMP заблокирован, то трафик помещен в черный список на ASA.
- После того, как несколько повторно передают, это понимает, что туннель DTLS не может быть установлен, и этому нужно к reassign новое значение MTU к адаптеру VPN.
- Цель этого повторно соединяется, должен назначить новый MTU.

Для получения дополнительной информации о повторно подключите поведение и таймеры, посмотрите часто задаваемые вопросы AnyConnect: Туннелирует, Повторно подключите Поведение и Таймер неактивности

Предупреждения

Идентификатор ошибки Cisco CSCuh61321 AC 3.1:ASA неправильно обрабатывает альтернативный порт DTLS, причины повторно соединяются

Дополнительные сведения

- Часто задаваемые вопросы AnyConnect: туннелирует, повторно подключите поведение и таймер неактивности
- Cisco Systems – техническая поддержка и документация