Часто задаваемые вопросы AnyConnect: туннелирует, повторно подключите поведение и таймер неактивности

Содержание

Введение
Общие сведения
Типы туннелей
Пример выходных данных от ASA
DPD и таймеры неактивности
Когда сеанс считают Неактивным сеансом?
Когда ASA отбрасывает Туннель SSL?
Если DPD уже включены, почему должны быть включены Пакеты Keepalive?
Поведение клиента AnyConnect в случае повторно соединяется
Фактический процесс
Поведение клиента AnyConnect в случае системы приостанавливает
Вопросы и ответы
Q1. DPD Anyconnect имеет интервал, но никакие повторные попытки - сколько пакетов он должен отсутствовать, прежде чем он отметит удаленный конец как мертвый?
Q2. DPD обрабатывает другой для AnyConnect с IKEv2?
Q3. Есть ли другая цель для Родительского Туннеля AnyConnect?
Q4. Можно ли фильтровать и выйти ли из системы просто неактивные сеансы?
Q5. Когда туннельный Idle-Timeout DTLS или TLS истекает, что происходит с Родительским Туннелем?
Q6. Какой смысл того, чтобы поддержать сеанс, как только таймеры DPD разъединили сеанс и почему ASA не освобождает IP-адрес?
Q7. Если ASA переключается при отказе от Активного до Резерва, каково поведение?
Q8. Почему там два других таймаута, время простоя и разъединенный таймаут, если они - оба то же значение?
Q9. Когда клиентский компьютер приостановлен, что происходит?
Q10. Когда повторно подключение происходит, Виртуальный адаптер AnyConnect машет или делает изменение таблицы маршрутизации вообще?
Q11. ? Автоматический Повторно соединяются? предоставить Устойчивость сеансов связи? Если так, есть ли какие-либо дополнительные функции, добавленные в Клиенте AnyConnect?
Q12. Эта функция работает на все варианты Microsoft Windows (Vista, 32-разрядный и 64-разрядный, XP). Как насчет Macintosh? Это работает на OS X 10.4?
Q13. Там какие-либо ограничения к функции с точки зрения подключения (Соединены проводом, Wi-fi, 3G и так далее)? Это поддерживает переход от одного режима до другого (от Wi-Fi до 3G, 3G к проводному, и так далее)?
Q14. Как аутентифицируется операция резюме?

Q15. Авторизация LDAP также выполнена на, повторно соединяются или только аутентификация?
Q16. Предварительный вход в систему и/или hostscan работают на резюме?
Q17. Относительно Распределения нагрузки (LB) VPN и резюме соединения, клиент соединится назад непосредственно с членом кластера, с которым это было связано прежде?
Дополнительные сведения

Введение

Этот документ описывает подробно некоторые важные моменты о защищенном мобильном клиенте Cisco AnyConnect Secure Mobility (AnyConnect) туннели, повторно подключить поведение и Dead Peer Detection (DPD) и таймер неактивности.

Общие сведения

Типы туннелей

Существует два метода, используемые для соединения сеанса AnyConnect:

- Через (безклиентый) портал
- С помощью автономного приложения

На основе пути вы соединяетесь, вы создаете три других туннеля (сеансы) на ASA, каждом с определенной целью:

1. **Безклиентый или Родительский Туннель:** Это - основной сеанс, который создан на согласовании для устанавливания маркера сеанса, который необходим в случае, если повторно подключение необходимо из-за невозможности сетевого подключения или спящего режима. На основе механизма подключения устройство адаптивной защиты Cisco (ASA) перечисляет сеанс как Безклиентый (Weblaunch через Портал) или Родитель (Автономный AnyConnect).

   Примечание: Когда клиент активно не связан, Родитель AnyConnect представляет сеанс. Эффективно, это работает подобное cookie, в котором это - запись базы данных на ASA, который сопоставляет с соединением от конкретного клиента. Если клиент завершает работу или спит, туннели (Ipsec/протокол IKE / Transport Layer Security (TLS) / протоколы Протокола защиты транспортного уровня для дейтаграмм (DTLS)) разъединены, но Родитель остается, пока счетчик простоя или максимальное время соединения не вступает в силу. Это позволяет пользователю воссоединяться без переаутентификации.

2. **Уровень защищенных сокетов (SSL) - Туннель:** подключение SSL установлено сначала, и данные переданы по этому соединению, в то время как это пытается установить соединение DTLS. Как только соединение DTLS установлено, клиент передает пакеты через соединение DTLS вместо через подключение SSL. Управляющие пакеты, с другой стороны, всегда доставляются через соединение SSL.

3. **DTLS-туннель:** Когда DTLS-туннель полностью установлен, все данные перемещаются в DTLS-туннель, и Туннель SSL только используется для случайного трафика управляющего канал. Если что-то происходит с Протоколом UDP, DTLS-туннель разъединен, и все данные проходят через Туннель SSL снова.

Пример выходных данных от ASA

Вот пример выходных данных от этих двух способов подключения.

AnyConnect, Связанный через Веб-запуск:

```
ASA5520-C(config)# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1435
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Protocol : Clientless SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : Clientless: (1)RC4 SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : Clientless: (1)SHA1 SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 335765 Bytes Rx : 31508
Pkts Tx : 214 Pkts Rx : 18
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 22:13:37 UTC Fri Nov 30 2012
Duration : 0h:00m:34s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

Clientless Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

Clientless:
Tunnel ID : 1435.1
Public IP : 172.16.250.17
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : Web Browser
Client Ver : Mozilla/5.0 (Windows NT 5.1; rv:16.0) Gecko/20100101 Firefox/16.0
Bytes Tx : 329671 Bytes Rx : 31508

SSL-Tunnel:
Tunnel ID : 1435.2
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 1241
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.01065
Bytes Tx : 6094 Bytes Rx : 0
Pkts Tx : 4 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

DTLS-Tunnel:
Tunnel ID : 1435.3
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 Compression : LZS
UDP Src Port : 1250 UDP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : DTLS VPN Client
Client Ver : Mozilla/5.0 (Windows NT 5.1; rv:16.0) Gecko/20100101 Firefox/16.0
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

AnyConnect, Связанный с помощью Автономного приложения:

```
ASA5520-C(config)# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1436
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 12244 Bytes Rx : 777
Pkts Tx : 8 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 22:15:24 UTC Fri Nov 30 2012
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 1436.1
Public IP : 172.16.250.17
Encryption : none Hashing : none
TCP Src Port : 1269 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : AnyConnect
Client Ver : 3.1.01065
Bytes Tx : 6122 Bytes Rx : 777
Pkts Tx : 4 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 1436.2
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 1272
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.01065
Bytes Tx : 6122 Bytes Rx : 0
Pkts Tx : 4 Pkts Rx : 0
```

```
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 1436.3
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 Compression : LZS
UDP Src Port : 1280 UDP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : DTLS VPN Client
Client Ver : 3.1.01065
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

DPD и таймеры неактивности

Когда сеанс считают Неактивным сеансом?

Сеанс считают Неактивным (и таймер начинает увеличиваться), только, когда Туннель SSL больше не существует на сеансе. Так, к каждому сеансу добавляют метку времени со временем отбрасывания Туннеля SSL.

```
ASA5520-C# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1336
Public IP : 172.16.250.17
Protocol : AnyConnect-Parent <- Here just the AnyConnect-Parent is active
but not SSL-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none
Hashing : AnyConnect-Parent: (1)none
Bytes Tx : 12917 Bytes Rx : 1187
Pkts Tx : 14 Pkts Rx : 7
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 17:42:56 UTC Sat Nov 17 2012
Duration : 0h:09m:14s
Inactivity : 0h:01m:06s <- So the session is considered Inactive
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

Когда ASA отбрасывает Туннель SSL?

Существует два способа, которыми может быть разъединен Туннель SSL:

1. **DPD** - DPD используются клиентом для обнаружения сбоя в связи между клиентом AnyConnect и головным узлом ASA. DPD также используются для очистки ресурсов на ASA. Это гарантирует, что головной узел не поддерживает соединения в базе данных, если оконечная точка является небыстро реагирующей к эхо-запросам DPD. Если ASA передает DPD к оконечной точке, и это отвечает, никакие меры не приняты. Если оконечная точка не является быстро реагирующей, ASA разъединяет туннель в базе

данных сеанса и перемещает сеанс в "Ожидание для Возобновления" режима. То, что это означает, - то, что DPD от головного узла запустился, и головной узел больше не связывается с клиентом. В таких ситуациях ASA держит Родительский Туннель, чтобы позволить пользователю перемещаться сети, засыпать и восстанавливать сеанс. Эти сеансы говорят против активно связанных сеансов и очищены при этих условиях: User Idle TimeoutКлиент возобновляет исходный сеанс и выходит из системы должным образом
Для настройки DPD используйте anyconnect команду dpd-interval под атрибутами WebVPN в параметрах настройки групповой политики. По умолчанию DPD включен и установлен в 30 секунд и для ASA (шлюз) и для клиента.

Внимание. : Знайте об идентификаторе ошибки Cisco CSCts66926 - DPD не в состоянии завершать туннель DTLS после потерянного клиентского соединения.

2. **Idle-Timeout** - Второй способ, которым разъединен Туннель SSL, состоит в том, когда истекает Idle-Timeout для этого туннеля. Однако помните, что это не только Туннель SSL, который должен бездельничать, но и туннель DTLS также. Пока времена сеанса DTLS, Туннель SSL не сохранен в базе данных.

Если DPD уже включены, почему должны быть включены Пакеты Keepalive?

Как объяснено ранее, DPD не уничтожает сам сеанс AnyConnect. Это просто уничтожает туннель в том сеансе так, чтобы клиент мог восстановить туннель. Если клиент не может восстановить туннель, сеанс остается, пока счетчик простоя не истекает на ASA. Так как DPD включены по умолчанию, клиенты могли бы часто разъединяться из-за закрытия потоков в одном направлении с Технологией NAT, Устройствами с функциями межсетевого экрана и Промежуточными устройствами. Разрешение пакетов Keepalive в низких интервалах, таких как 20 секунд, помогает предотвращать это.

Пакеты Keepalive включены под атрибутами WebVPN определенной групповой политики с anyconnect ssl команду keepalive . По умолчанию таймеры установлены в 20 секунд.

Поведение клиента AnyConnect в случае повторно соединяется

AnyConnect попытается восстановить разорванное соединение. Это не конфигурируемо, автоматически. Пока сеанс VPN на ASA все еще допустим и если AnyConnect может восстановить физическое соединение, сеанс VPN будет возобновлен.

Повторно подключить функция продолжается до превышения времени ожидания сеанса или таймаута разъединения, который является фактически временем простоя, истекает (или 30 минут, если никакие таймауты не настроены). Как только они истекают, вы не должны продолжать, потому что ASA отбросит сеанс VPN. Клиент продолжит, пока это думает, что ASA все еще имеет сеанс VPN.

AnyConnect повторно соединится независимо от того, как изменяется сетевой интерфейс. Не имеет значения, если IP-адрес изменений сетевой интерфейсной платы (NIC), или если подключение переключается от одного NIC до другого NIC (радио к проводному или

наоборот).

Когда вы рассматриваете повторно подключить процесс для AnyConnect, существует три уровня сеансов, которые необходимо помнить. Кроме того, повторно подключить поведение каждого из этих сеансов слабо связано в этом, любой из них может быть восстановлен без зависимости от элементов сеанса предыдущего уровня:

1. TCP или UDP повторно подключают [OSI уровень 3]
2. TLS, DTLS или IPSec (IKE+ESP) [OSI уровень 4] - возобновление TLS не поддерживается.
3. Когда существует разрушение, VPN [OSI уровень 7] - маркер сеанса VPN используется в качестве маркера аутентификации для восстановления сеанса VPN по безопасному каналу. Это - собственный механизм, который подобен, концептуально, к тому, как маркер Kerberos или сертификат клиента используются для аутентификации. Маркер уникален и криптографически генерируемый головным узлом, который содержит идентификатор сеанса плюс криптографически генерируемое случайное информационное наполнение. Это передают клиенту как часть начального установления VPN после того, как будет установлен безопасный канал к головному узлу. Это остается допустимым для срока действия сеанса на головном узле, и это сохранено в клиентской памяти, которая является привилегированным процессом. **Совет:** Эти версии ASA и позже содержат более сильный криптографический маркер сеанса: 9.1 (3) и 8.4 (7.1)

Фактический процесс

Таймер Таймаута Разъединения запущен, как только разрушено сетевое подключение. Клиент AnyConnect продолжает пытаться воссоединиться, пока не истекает этот таймер. Таймаут Разъединения установлен в самую низкую установку или **Idle-Timeout** Групповой политики или **Максимальное Время соединения**.

Значение этого таймера замечено в конечном счете Средство просмотра для сеанса AnyConnect на согласовании:

В данном примере сеанс должен разъединить после двух минут (120 секунд), который может быть проверен в сообщении История AnyConnect:

> **Совет:** Для ASA для ответа на клиента, который пытается воссоединиться Родительский Туннельный сеанс должен все еще существовать в базе данных ASA. В случае аварийного переключения DPD также должны быть включены для повторно подключить поведения работать.

Как видимо из предыдущих сообщений, повторно подключение отказавшего. Однако, если повторно подключение успешно, вот то, что происходит:

1. Родительский Туннель остается тем же; это не пересмотрено, потому что этот туннель поддерживает маркер сеанса, который требуется для сеанса для повторного подключения.
2. Новый SSL и сеансы DTLS генерируются, и порты другого источника используются в повторно подключении.

3. Все значения Idle-Timeout восстановлены.
4. Время ожидания при бездействии восстановлено.

Внимание. : Знайте об идентификаторе ошибки Cisco CSCtg33110. Когда AnyConnect повторно соединяется, база данных сеанса VPN не обновляет Открытый IP - адрес в базе данных сеанса ASA.

В этой ситуации, где попытки повторно подключить сбой, вы встречаетесь с этим сообщением:

Примечание: Этот запрос на расширение был подан для создания этого более гранулированным: Идентификатор ошибки Cisco CSCsl52873 - ASA не имеет конфигурируемого разъединенного таймаута для AnyConnect.

Поведение клиента AnyConnect в случае системы приостанавливает

Существует бродящая функция, которая позволяет AnyConnect повторно соединяться после сна ПК. Клиент продолжает пробовать, пока простаивающее или превышение времени ожидания сеанса не истекают, и клиент сразу не разъединяет туннель, когда система входит, в спящем режиме/резерв. Для клиентов, которые не хотят эту функцию, установите превышение времени ожидания сеанса в низкое значение для предотвращения сна/резюме, повторно соединяется.

Примечание: После исправления идентификатора ошибки Cisco CSCso17627 (Версия 2.3 (111) +), ручка управления была представлена для отключения, это повторно соединяется на функции резюме.

Автоповторно подключить поведение для AnyConnect может управляться через профиль XML AnyConnect с этой установкой:

```
      <AutoReconnect UserControllable="true">true
<AutoReconnectBehavior>ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
```

Когда компьютер будет возвращен изо сна, с этим изменением AnyConnect попытается повторно соединиться. Привилегированные настройки по умолчанию AutoReconnectBehavior к DisconnectOnSuspend. Это поведение отличается от того из Релиза клиента AnyConnect 2.2. Для повторно соединяются после резюме администратор сети должен или установить ReconnectAfterResume в профиле или сделать привилегированного пользователя AutoReconnect и AutoReconnectBehavior управляемым в профиле, чтобы позволить пользователям устанавливать его.

Вопросы и ответы

Q1. DPD Anyconnect имеет интервал, но никакие повторные попытки - сколько

пакетов он должен отсутствовать, прежде чем он отметит удаленный конец как мертвый?

O. Это должно пропустить три пакета повторных попыток/четырех.

Q2. DPD обрабатывает другой для AnyConnect с IKEv2?

O. Да, IKEv2 имеет фиксированный номер повторных попыток - шесть пакетов повторных попыток/семи.

Q3. Есть ли другая цель для Родительского Туннеля AnyConnect?

O. В дополнение к тому, чтобы быть сопоставлением на ASA родительский туннель используется для продвижения обновлений образа AnyConnect от ASA до клиента, потому что клиент активно не связан во время процесса обновления.

Q4. Можно ли фильтровать и выйти ли из системы просто неактивные сеансы?

O. Можно фильтровать неактивные сеансы с **покажите vpn-sessiondb anyconnect, фильтруют неактивную** команду. Однако нет никакой команды, чтобы выйти из системы просто неактивные сеансы. Вместо этого необходимо выйти из системы определенные сеансы или выход все сеансы на пользователя (индекс - название), протокол или туннельная группа. Запрос на расширение, идентификатор ошибки Cisco CSCuh55707, был подан для добавления опции, чтобы выйти из системы просто неактивные сеансы.

Q5. Когда туннельный Idle-Timeout DTLS или TLS истекает, что происходит с Родительским Туннелем?

O. "Простаивающий к Левому" таймеру Родительского AnyConnect сеанса перезагружен, или после разъединены Туннель SSL или после DTLS-туннель. Это позволяет "idle-timeout" действовать как "разъединенный" таймаут. Это эффективно становится допустимым временем для клиента для повторного подключения. Если клиент не воссоединится в таймере, то Родительский Туннель будет завершен.

Q6. Какой смысл того, чтобы поддержать сеанс, как только таймеры DPD разъединили сеанс и почему ASA не освобождает IP-адрес?

O. Головной узел не знает о состоянии клиента. В этом случае ASA ждет клиента для обнадеживающего повторного подключения до времен сеанса на счетчик простоя. DPD не уничтожает сеанс AnyConnect; это просто уничтожает туннель (в том сеансе) так, чтобы клиент мог восстановить туннель. Если клиент не восстанавливает туннель, сеанс остается, пока не истекает счетчик простоя.

Если беспокойство об израсходованных сеансах, одновременные входы в систему набора к низкому значению такой как один. С этой установкой пользователям, у которых есть сеанс в

базе данных сеанса, удалили их предшествующий сеанс, когда они входят снова.

Q7. Если ASA переключается при отказе от Активного до Резерва, каково поведение?

O. Первоначально, когда сеанс установлен, три туннеля (Родитель, SSL и DTLS) реплицированы в Резервный модуль; как только ASA переключается при отказе, DTLS и сеансы TLS восстановлены, поскольку они не синхронизируются к резервному модулю, но любые потоки данных через туннели должны работать без разрушения после того, как восстановлен сеанс AnyConnect.

Сеансы SSL/DTLS не с отслеживанием состояния, таким образом, состояние SSL и порядковый номер не поддержаны и могут быть довольно налоговыми. Таким образом те сеансы должны быть восстановлены с нуля, который сделан с Родительским сеансом и маркером сеанса.

> **Совет:** Если пакеты Keepalive отключены, в случае события аварийного переключения сеансы VPN-клиента SSL (SVC) не перенесены на резервное устройство.

Q8. Почему там два других таймаута, время простоя и разъединенный таймаут, если они - оба то же значение?

O. Когда протоколы были разработаны, два других таймаута были обеспечены:

- Время простоя - время простоя для того, когда никакие данные не переданы по соединению.
- Разъединенный таймаут - разъединенный таймаут для того, когда вы бросаете сеанс VPN, потому что соединение было потеряно и не может быть восстановлено.

Разъединенный таймаут никогда не внедрялся на ASA. Вместо этого ASA передает значение времени ожидания простоя за обоими простаивающие и разъединенные таймауты клиенту.

Клиент не использует время простоя, потому что ASA обрабатывает время простоя. Клиент использует разъединенное значение таймаута, которое совпадает со значением времени ожидания простоя для знания, когда сдаться, повторно подключают попытки, так как ASA отбросит сеанс.

В то время как не активно связанный с клиентом, ASA будет таймаут сеанс через время простоя. Основная причина не внедрить разъединенный таймаут на ASA состояла в том, чтобы избежать добавления другого таймера для каждого сеанса VPN и увеличения издержек на ASA (невзирая на то, что тот же таймер мог использоваться в обоих экземплярах, только с другими значениями таймаута, так как эти два случая являются взаимоисключающими).

Единственное значение, добавленное с разъединенным таймаутом, должно позволить администратору задавать другой таймаут для того, когда клиент активно не связан по сравнению с простаивающим. Как обращено внимание ранее, идентификатор ошибки Cisco CSCsl52873 был подан для этого.

Q9. Когда клиентский компьютер приостановлен, что происходит?

O. По умолчанию AnyConnect действительно пытается восстановить VPN-подключение при потере подключения. Это не пытается восстановить VPN-подключение после системного резюме по умолчанию. См. Поведение Клиента AnyConnect в случае Системы Приостанавливают за подробные данные.

Q10. Когда повторно подключение происходит, Виртуальный адаптер AnyConnect машет или делает изменение таблицы маршрутизации вообще?

O. Туннельный уровень повторно соединяется, не сделает также. При этом заново устанавливается только сеанс SSL или DTLS. Они идут приблизительно за 30 секунд до того, как они сдадутся. В случае отказа DTLS соединение попросту разрывается. Если SSL отказывает, он вызывает сеансовый уровень, повторно соединяются. Сеансовый уровень повторно соединяется, полностью восстановит маршрутизацию. Если адрес клиента назначил на повторно подключении, или любые другие параметры конфигурации, которые влияют на Виртуальный адаптер (VA), не изменились, то BA не отключен. В то время как это вряд ли будет иметь любое изменение в параметрах конфигурации, полученных от ASA, возможно, что изменение в физическом интерфейсе, используемом для VPN-подключения (например, если вы расстыковываете и идете от проводного до WiFi), мог бы привести к другому значению Максимального размера передаваемого блока данных (MTU) для VPN-подключения. Значение MTU влияет на BA, и изменение к нему заставляет BA быть отключенным и затем реактивированным.

Q11. ? Автоматический Повторно соединяются? предоставить Устойчивость сеансов связи? Если так, есть ли какие-либо дополнительные функции, добавленные в Клиенте AnyConnect?

O. AnyConnect не предоставляет дополнительного "волшебства" принять устойчивость сеансов связи для приложений. Но возможность VPN - подключения восстановлена автоматически вскоре после сетевого подключения к резюме защищенного шлюза, предоставил времена ожидания простоя и сеанса, настроенные на ASA, не истекли. И в отличие от Клиента IPSEC, автоматические повторно подключают результаты в том же IP-адресе клиента. В то время как AnyConnect пытается повторно соединиться, Виртуальный адаптер AnyConnect остается включенным и в связанном состоянии, таким образом, IP-адрес клиента остается существующим и включенным на клиентском компьютере все время, которое дает устойчивость IP-адреса клиента. Приложения клиентского компьютера, однако, будут, вероятно, все еще чувствовать, что потеря подключения к их серверам на корпоративной сети должна он занимать слишком много времени у возможности VPN - подключения быть восстановленной.

Q12. Эта функция работает на все варианты Microsoft Windows (Vista, 32-разрядный и 64-разрядный, XP). Как насчет Macintosh? Это работает на OS X 10.4?

O. Эта функция действительно работает на Mac и Linux. Были проблемы с Mac и Linux, но недавние улучшения были сделаны, особенно для Mac. Linux все еще требует некоторой

дополнительной поддержки (CSCsr16670, CSCsm69213), но базовые функции там также. Относительно Linux AnyConnect не распознает, что приостановить/возобновить (сон/след) произошел. Это в основном имеет два влияния:

- Профиль/настройки AutoReconnectBehavior не может поддерживаться на Linux без, приостанавливают/возобновляют поддержку, таким образом, повторно подключение будет всегда происходить, после приостанавливают/возобновляют.
- На Microsoft Windows и Macintosh, повторно подключение сразу выполнено на сеансовом уровне после резюме, которое обеспечивает более быстрый коммутатор к другому физическому интерфейсу. На Linux, потому что AnyConnect полностью не знает о приостанавливании/возобновлении, повторно подключение будет иметь место на туннельном уровне сначала (SSL и DTLS), и это могло бы означать, что повторно подключение берет немного дольше. Но повторно подключение все еще произойдет на Linux.

Q13. Там какие-либо ограничения к функции с точки зрения подключения (Соединены проводом, Wi-fi, 3G и так далее)? Это поддерживает переход от одного режима до другого (от Wi-Fi до 3G, 3G к проводному, и так далее)?

O. AnyConnect не связан к определенному физическому интерфейсу для жизни VPN-подключения. Если физический интерфейс, используемый для VPN-подключения, потерян или если повторно соединяются, попытки по нему превышают определенное пороговое значение отказа, то AnyConnect больше не будет использовать тот интерфейс и пытаться достигнуть, защищенный шлюз с любыми интерфейсами доступны до простаивающего, или таймеры сеанса истекают. Обратите внимание на то, что изменение в физическом интерфейсе могло привести к другому значению MTU для BA, который заставит BA должным быть быть отключен и реактивирован, но все еще с тем же IP-адресом клиента.

Если будет какой-либо разрыв сети (интерфейс вниз, измененные сети, измененные интерфейсы), то AnyConnect попытается повторно соединиться; никакая повторная проверка подлинности не необходима на, повторно соединяются. Это даже применяется к коммутатору физических интерфейсов:

Пример:

```
1. wireless off, wired on: AC connection established
2. disconnect wired physically, turn wired on: AC re-established connection in
30 seconds
3. connect wired, turn off wireless: AC re-established connection in 30 secs
```

Q14. Как аутентифицируется операция резюме?

O. В резюме вы повторно отправляете аутентифицируемый маркер, который останется для срока действия сеанса, и сеанс тогда восстановлен.

Q15. Авторизация LDAP также выполнена на, повторно соединяются или только аутентификация?

O. Это только выполнено в первоначальном подключении.

Q16. Предварительный вход в систему и/или hostscan работают на резюме?

O. Нет, они работают на первоначальном подключении только. Что-то вроде этого было бы намечено для будущей Периодической функции Оценки Положения.

Q17. Относительно Распределения нагрузки (LB) VPN и резюме соединения, клиент соединится назад непосредственно с членом кластера, с которым это было связано прежде?

O: Да, это корректно, так как вы не повторно решаете имя хоста через DNS для re-estblishment существующего сеанса.

Дополнительные сведения

- Ссылка DPD ASA: CSCsr63074 Идентификатора ошибки Cisco - DPD, не передаваемый, когда узел мертв и туннель, не простаивающий на s2s с 7.2.4
- Cisco Systems – техническая поддержка и документация