AnyConnect оптимальное руководство устранения неполадок выбора шлюза

Содержание

Введение

Этот документ описывает, как решить проблемы с Оптимальным выбором шлюза (OGS). OGS является функцией, которая может быть использована для определения, какой шлюз имеет самый низкий Round Trip Time (RTT) и подключение к тому шлюзу. Можно использовать функцию OGS для уменьшения задержки для интернет-трафика без вмешательства пользователя. С OGS защищенный мобильный клиент Cisco AnyConnect Secure Mobility (AnyConnect) определяет и выбирает, какой защищенный шлюз является лучшим для соединения или повторного соединения. OGS берется за первое соединение или после повторного соединения спустя по крайней мере четыре часа после предыдущего разъединения. Дополнительные сведения могут быть найдены в руководстве Администратора.

> **Совет:** OGS работает лучше всего с последним клиентом AnyConnect и версией программного обеспечения 9.1 (3) ASA * или позже.

Как делает OGS, работают?

Простой **запрос проверки доступности (ping request)** Протокола ICMP не работает, потому что много устройств адаптивной защиты Cisco (ASA), межсетевые экраны настроены для блокирования пакетов ICMP для предотвращения обнаружения. Вместо этого клиент отправляет три запроса HTTP/443 к каждому головному узлу, который появляется в **слиянии**

всех профилей. Эти Проверки HTTP упоминаются как эхо-запросы OGS в журналах, но, как объяснено ранее, они не эхо-запросы ICMP. Чтобы гарантировать, что (ре) соединение не занимает слишком много времени, OGS выбирает предыдущий шлюз по умолчанию, если это не получает результатов эхо-запроса OGS в течение семи секунд. (Ищите **результаты эхо-запроса OGS** в журнале.)

> **Примечание:** AnyConnect должен передать запрос HTTP к 443, потому что сам ответ важен, не успешный ответ. К сожалению, исправление для обработки прокси отправляет все запросы как HTTPS. Посмотрите идентификатор ошибки Cisco CSCtg38672 - OGS должен пропинговать с запросами HTTP.

> **Примечание:** Если нет никаких головных узлов в кэше, AnyConnect сначала передает один запрос HTTP, чтобы определить, существует ли аутентификация прокси-сервера, и если это может обработать запрос. Это только после этого исходного запроса, что это начинает эхо-запросы OGS для зондирования сервера.

- OGS определяет расположение пользователя на основе информации о сети, такой как суффикс Системы доменных имен (DNS) и IP-адрес сервера DNS. Результаты RTT, наряду с этим местоположением, сохранены в кэше OGS.

- Записи местоположения OGS кэшируются в течение 14 дней. Идентификатор ошибки Cisco CSCtk66531 был подан для установки этих настраиваемых настроек.

- OGS не выполнен снова от этого местоположения до спустя 14 дней после того, как будет сначала кэшироваться запись местоположения. В это время это использует кэшированную запись и RTT, определенные для того местоположения. Это означает, что, когда AnyConnect запускается снова, он не выполняет OGS снова; вместо этого, это использует оптимальный заказ шлюза в кэше для того местоположения. В журналах Диагностического средства создания отчетов AnyConnect (DART) замечено это сообщение:

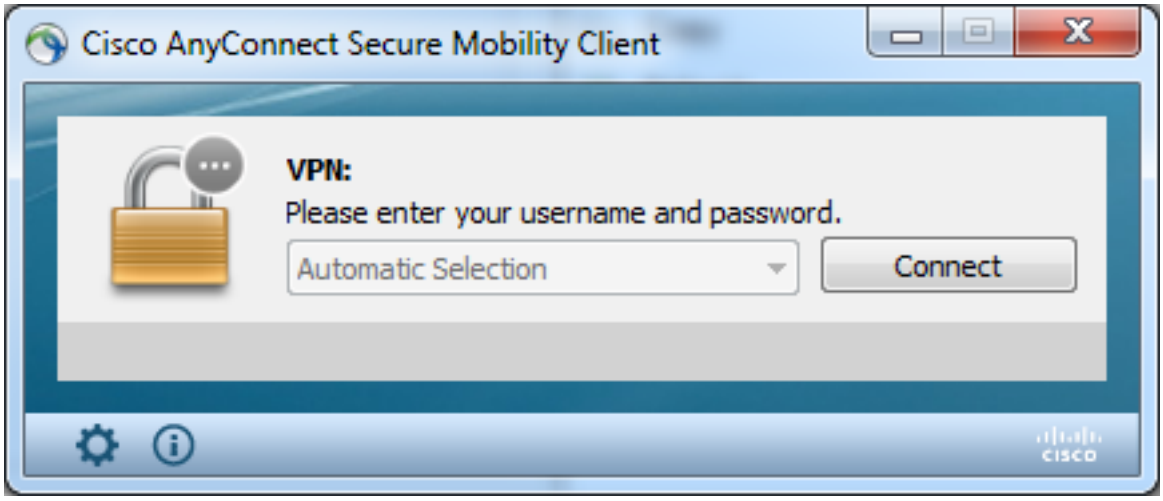
```
*****************************************
Date : 10/04/2013
Time : 14:00:44
Type : Information
Source : acvpnui

Description : Function: ClientIfcBase::startAHS
File: .\ClientIfcBase.cpp
Line: 2785
OGS was already performed, previous selection will be used.

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

- RTT определен с обменом TCP к порту Уровня защищенных сокетов (SSL) шлюза, с которым пользователь попытается соединиться, как задано записью хоста в профиле AnyConnect.

> **Примечание:** В отличие от эхо-запроса HTTP, который делает простой пост HTTP и затем отображает RTT и результат, вычисления OGS немного более сложны. AnyConnect передает три зонда за каждым сервером и вычисляет задержку между SYN HTTP, который это отсылает и FIN/ACK для каждого из этих зондов. Это тогда

использует самую низкую из дельт, чтобы сравнить серверы и сделать его выбор. Так, даже при том, что эхо-запросы HTTP являются довольно хорошей индикацией, которого сервера выберет AnyConnect, они не могли бы обязательно соответствовать. Существуют дополнительные сведения об этом в остатке документа.
- В настоящее время OGS только осуществляет проверки, если пользователь выходит из приостанавливания, и порог был превышен. Если ASA пользователь связан со сбоями или становится недоступным, OGS не соединяется с другим ASA. OGS связывается только с основными серверами в профиле для определения оптимального.

- Как только клиентский профиль OGS загружен, когда пользователь перезапустит клиента AnyConnect, опция для выбора других профилей отобразится серым как показано здесь:



Даже если пользовательская машина будет иметь множественные другие профили, то они не будут в состоянии выбрать любого из них, пока OGS не будет disbaled.

Кэш OGS

Как только вычисление закончено, результаты сохранены в **preferences_global** файле. Были проблемы с этими данными, не сохраненными в файле прежде.

См. идентификатор ошибки Cisco CSCtj84626 для получения дополнительной информации.

Определение местоположения

Кэширование OGS работает на комбинацию Домена DNS и IP-адресов сервера отдельных DN. Это работает следующим образом:

- Местоположение A имеет Домен DNS **locationa.com** и два IP-адреса сервера DNS - **ip1** и **ip2**. Каждая комбинация домена/IP создает ключ кэша, который указывает к записи в кэше OGS. Пример: **locationa.com|ip1-> ogscache1locationa.com|ip2-> ogscache1**
- Если AnyConnect тогда соединяется с физически другой сетью, то же наращивание комбинаций домена/IP создано и проверено против кэшируемого списка. Если существуют какие-либо соответствия вообще, что значение кэша OGS используется, и клиент, как все еще полагают, в **местоположении A**.

Сценарии отказов

Вот некоторые пользователи сценариев отказов, мог бы встретиться:

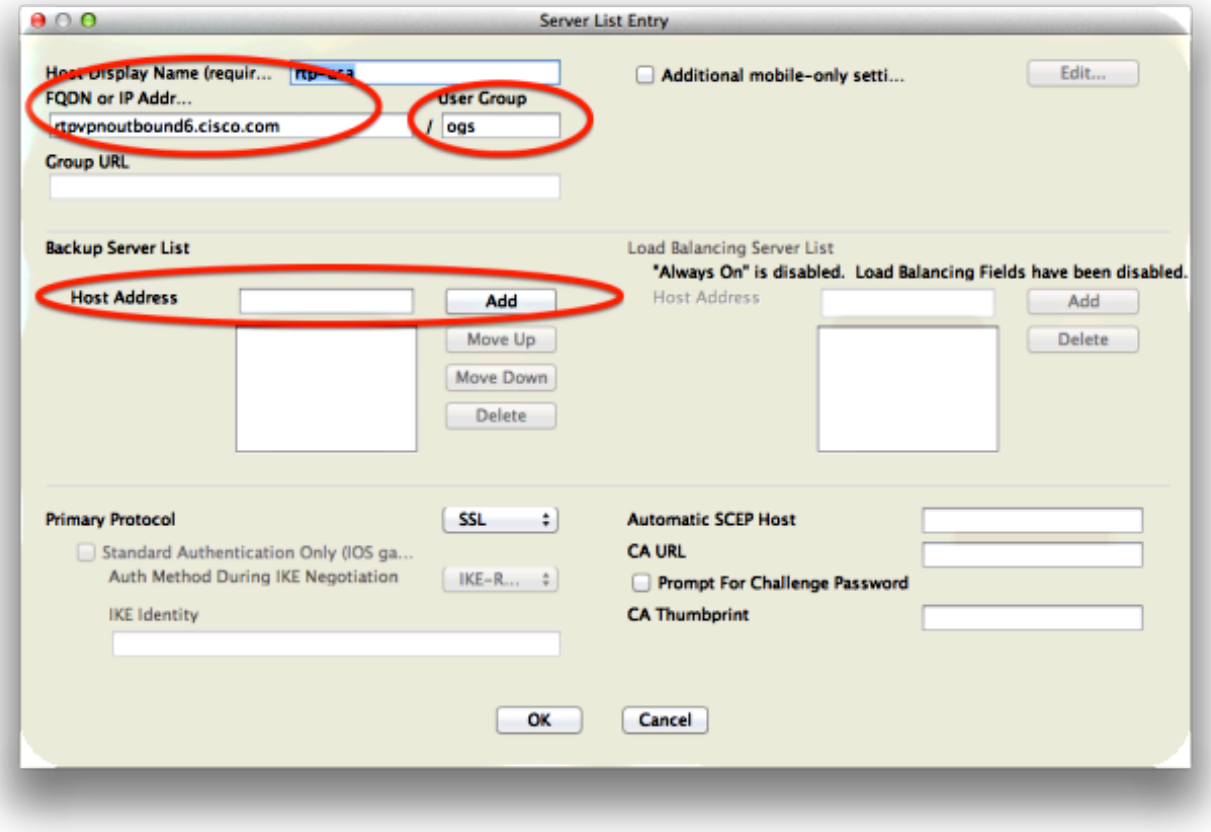
Когда Потеряно Подключение к шлюзу

Когда OGS используется, если подключение к шлюзу, с которым связаны пользователи, потеряно, затем подключения AnyConnect к серверам в **сервере резервного копирования listandnot** к следующему хосту OGS. Заказ операций следующие:

1. OGS связывается только с основными серверами для определения оптимального.

2. После того, как определенный, алгоритм соединения:
   Попытайтесь соединиться с оптимальным сервером.Если это отказывает, попробуйте список сервера резервного копирования оптимального сервера.Если это отказывает, попробуйте каждый сервер, который остается в списке выбора OGS, упорядоченном его результатами выбора.

   Примечание: Когда администратор настраивает список сервера резервного копирования, текущий редактор профиля только позволяет администратору вводить Полное доменное имя (FQDN) для сервера резервного копирования, но не user-group, как возможно для основного сервера:



   Идентификатор ошибки Cisco CSCud84778 был подан для исправления этого, но завершенный URL должен быть введен в поле адреса узла для сервера резервного копирования, и это должно работать: **https://*<ip address>* / usergroup**.

Резюме после приостанавливания

Когда машина была помещена в сон, для OGS для погони за резюме AnyConnect, должно быть, установили соединение. OGS после резюме только выполнен после того, как тест сетевой среды происходит, который предназначается, чтобы подтвердить, что сетевое подключение доступно. Этот тест включает подтест подключения DNS.

Однако, если отбрасывания сервера DNS тип запросы с IP-адресом в поле запроса, в противоположность ответу с "названием, не найденным" (больше общего падежа, с которым всегда встречаются во время тестов), то идентификатор ошибки Cisco CSCti20768 "запрос DNS типа A для IP-адреса, должны быть PTR, чтобы избежать, чтобы применился таймаут".

Размер окна задержанного ACK TCP выбирает Incorrect Gateway

Когда версии ASA ранее, чем Версия 9.1 (3) используются, перехваты на клиентском показе персистентная задержка подтверждения связи SSL. То, что замечено, - то, что клиент передает его ClientHello, тогда ASA передает свой ServerHello. Это обычно придерживается сообщением Сертификата (дополнительный Запрос сертификата) и сообщением ServerHelloDone. Аномалия является двукратной:

1. ASA сразу не передает сообщение Сертификата после ServerHello. Размер окна клиента составляет 64,860 байтов, которого является более чем достаточно для удержания всего ответа от ASA.

2. Клиент не делает ACK ServerHello сразу, таким образом, ASA повторно передает ServerHello после ~120ms, в этот момент клиентские ACK данные. Затем сообщение Сертификата передается. Это почти, как будто клиент ждет большего количества данных.

Это происходит из-за взаимодействия между slowstart TCP и задержанным ACK TCP. До Версии ASA 9.1 (3) ASA использует размер окна slowstart 1, тогда как Windows - клиент использует значение задержанного ACK 2. Это означает, что ASA только передает один пакет данных, пока это не получает ACK, но это также означает, что клиент не передает ACK, пока это не получает два пакета данных. Таймауты ASA после 120 мс и повторно передают ServerHello, после которого клиентские ACK продолжаются данные и соединение. Это поведение было изменено идентификатором ошибки Cisco CSCug98113 так, чтобы ASA использовал размер окна медленного пуска 2 по умолчанию вместо 1.

Это может повлиять на вычисление OGS когда:

- Другие шлюзы выполняют другие версии ASA.
- У клиентов есть другие размеры окна задержанного ACK.

В таких ситуациях задержка, представленная задержанным ACK, могла быть достаточной, чтобы заставить клиента выбирать неправильный ASA. Если это значение отличается между клиентом и ASA, могли бы все еще быть проблемы. В таких ситуациях обходной путь должен отрегулировать Задержанный размер окна Подтверждений.

Windows

1. Запустите **редактор реестра**.

2. Определите GUID интерфейса, на котором вы хотите отключить задержанный ACK. Чтобы сделать это, перейдите к:
   HKEY_LOCAL_MACHINE> ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ> Microsoft> WindowsNT> CurrentVersion> NetworkCards> (номер).
   Посмотрите на каждый номер, перечисленный под NetworkCards. На правой стороне Описание должно перечислить Интерфейс (например, Intel(R) Wireless WiFi Link 5100AGN), и ServiceName должен перечислить соответствующий GUID.

3. Найдите и затем нажмите этот подключ реестра: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces \<Интерфейсный GUID>**
4. В меню Edit, точке к Новому, и затем нажимают **DWORD Value**.
5. Назовите новое значение **TcpAckFrequency** и назначьте его значение **1**.
6. Редактор реестра выхода.
7. Перезапустите Windows для этого изменения для вступления в силу.

   Примечание: Идентификатор ошибки Cisco CSCum19065 был подан для создания параметров настройки TCP конфигурируемыми на ASA.

Пример типичного пользователя

Случай наиболее популярного способа использования - когда пользователь дома выполняет OGS первоначально, это делает запись параметров настройки DNS и результатов эхо-запроса OGS в кэше (настройки по умолчанию к 14-дневному таймауту). Когда пользователь возвращается домой следующим вечером, OGS обнаруживает те же параметры настройки DNS, находит его в кэше и пропускает эхо - тест (ping test) OGS. Позже, когда пользователь переходит к отелю или ресторану, который предлагает интернет-сервис, OGS обнаруживает другие параметры настройки DNS, выполняет эхо - тесты (ping test) OGS, выбирает лучший шлюз и делает запись результатов в кэше.

Обработка идентична, когда она возобновляется от приостановленного или была в спящем режиме состояние, если OGS и параметры настройки резюме AnyConnect обеспечивают ее.

Устранение неполадок OGS

Шаг 1. Очистите кэш OGS для принуждения переоценки

Чтобы очистить кэш OGS и переоценить RTT для доступных шлюзов, просто удалите Глобальный Привилегированный файл AnyConnect из ПК. Местоположение файла варьируется на основе Операционной системы (OS):

- Windows Vista и Windows 7
  ```
  C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\preferences_global.xml
  Note: in older client versions it used to be stored in C:\ProgramData\Cisco\Cisco
  AnyConnect VPN Client
  ```
- Windows XP
  ```
  C:\Documents and Settings\AllUsers\Application Data\Cisco\Cisco AnyConnect VPN
  Client\preferences_global.xml
  ```
- Mac OS X
  ```
  /opt/cisco/anyconnect/.anyconnect_global
  Note: with older versions of the client it used to be /opt/cisco/vpn..
  ```
- Linux
  ```
  /opt/cisco/anyconnect/.anyconnect_global
  Note: with older versions of the client it used to be /opt/cisco/vpn..
  ```

Шаг 2. Перехватите зонды сервера во время попытки подключения

1. Запустите Wireshark на тестовой машине.

2. Запустите попытку подключения на AnyConnect.

3. Остановите перехват Wireshark, как только соединение завершено. **Совет:** Так как перехват только используется для тестирования OGS, лучше останавливать перехват, как только AnyConnect выбирает шлюз. Лучше не проходить завершенную попытку подключения, потому что это может объединить захват пакета в облако.

Шаг 3. Проверьте шлюз, выбранный OGS

Для проверки, почему OGS выбрал определенный шлюз, выполните эти шаги:

1. Инициируйте новое соединение.

2. Выполните AnyConnect DART:
   AnyConnect запуска, и нажимает **Advanced**.Нажмите **Diagnostics**.**Нажмите кнопку Next.Нажмите кнопку Next.**
3. Исследуйте результаты DART, найденные в недавно созданном файле **DartBundle_XXXX_XXXX.zip** на рабочем столе.
   Перейдите к **защищенному мобильному клиенту Cisco AnyConnect Secure Mobility> AnyConnect.txt**.

   Обратите внимание на время, которое зонды OGS запустили для индивидуального сервера с этого журнала DART:

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

Date : 10/04/2013
Time : 14:21:27
Type : Information
Source : acvpnui

Description : Function: CHeadendSelection::CSelectionThread::Run
File: .\AHS\HeadendSelection.cpp
Line: 928
OGS starting thread named gw2.cisco.com

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

   Обычно они должны быть около того же времени, но в случае, если перехваты являются большими, штамп времени помогает сужать, какими пакетами являются Проверки HTTP и которые попытки фактического соединения.

   Как только AnyConnect передает три зонда к серверу, это сообщение генерируется с результатами для каждого из зондов:

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

Date : 10/04/2013
Time : 14:31:37
Type : Information
Source : acvpnui
```

```
Description : Function: CHeadendSelection::CSelectionThread::logThreadPingResults
File: .\AHS\HeadendSelection.cpp
Line: 1137
OGS ping results for gw2.cisco.com: (219 218 132 )

**************************************** Важно обратить внимание на эти три значения, потому что они должны совпасть с результатами перехвата.
```

Ищите сообщение, которое содержит "*** OGS Результаты Выбора ***" для наблюдения оцененного RTT, и если новая попытка подключения была результатом кэшируемого RTT или нового вычисления.

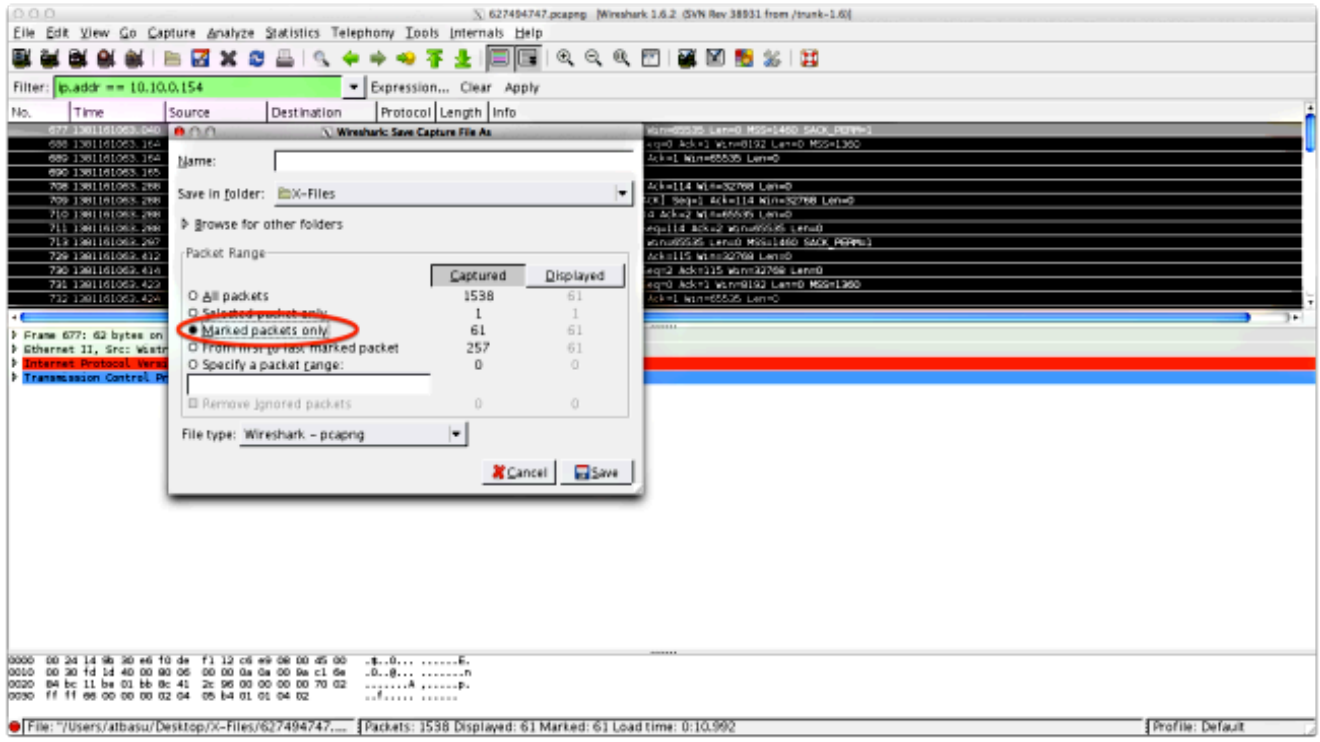
Например: `****************************************`

```
Date       : 10/04/2013
Time       : 12:29:38
Type       : Information
Source     : vpnui

Description : Function: CHeadendSelection::logPingResults
File: .\AHS\HeadendSelection.cpp
Line: 589
*** OGS Selection Results ***
OGS performed for connection attempt. Last server: 'gw2.cisco.com'

Results obtained from OGS cache. No ping tests were performed.

Server Address    RTT (ms)
gw1.cisco.com    302
gw2.cisco.com    132 <========= As seen, 132 was the lowest delay
of the three probes from the previous DART log
gw3.cisco.com    506
gw4.cisco.com    877


Selected 'gw2.cisco.com' as the optimal server.

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

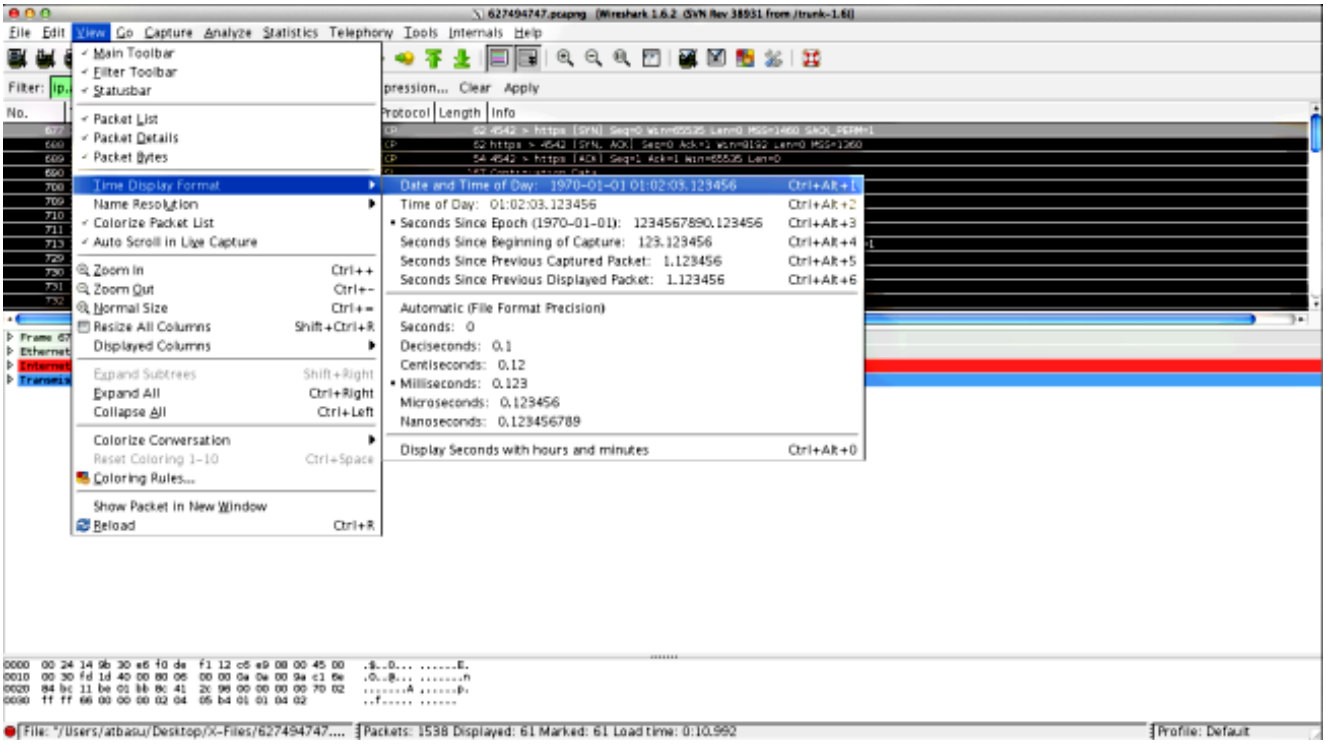
Шаг 4. . Проверьте вычисления OGS, выполненные AnyConnect

Осмотрите перехват для зондов TCP/SSL, используемых для вычисления RTT. Посмотрите, сколько времени Запрос HTTPS принимает одиночный TCP - подключение. Каждый тестовый запрос должен использовать другой TCP - подключение. Чтобы сделать это, откройте перехват в Wireshark и повторите эти шаги для каждого из серверов:

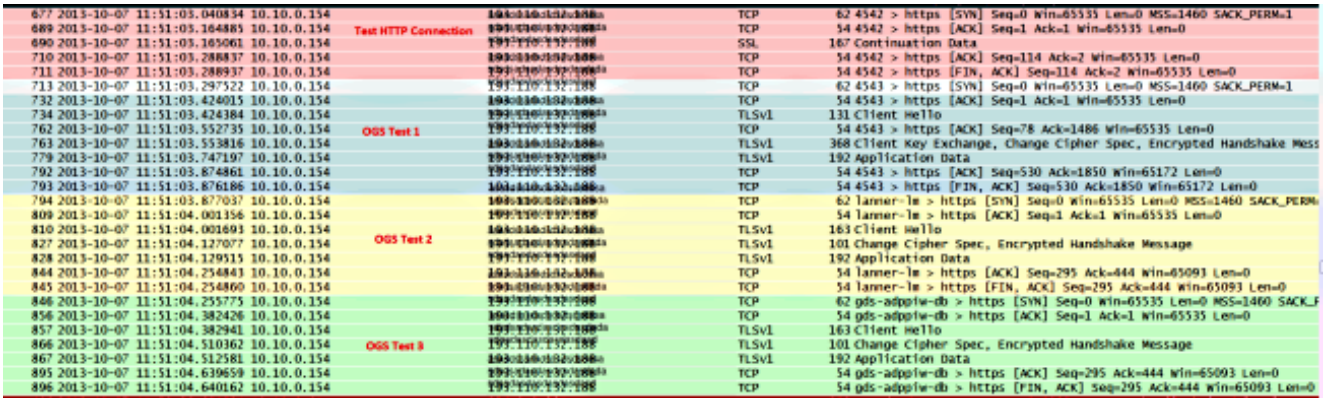
1. Используйте фильтр **ip.addr** для изоляции пакетов, переданных к каждому из серверов в их собственный перехват. Чтобы сделать это, перейдите, чтобы **Отредактировать**, и выбрать **Mark All Displayed Packets**. Затем перейдите, чтобы **File> Save as**, выбрать **Маркированные пакеты только** опция и нажать **Save**:



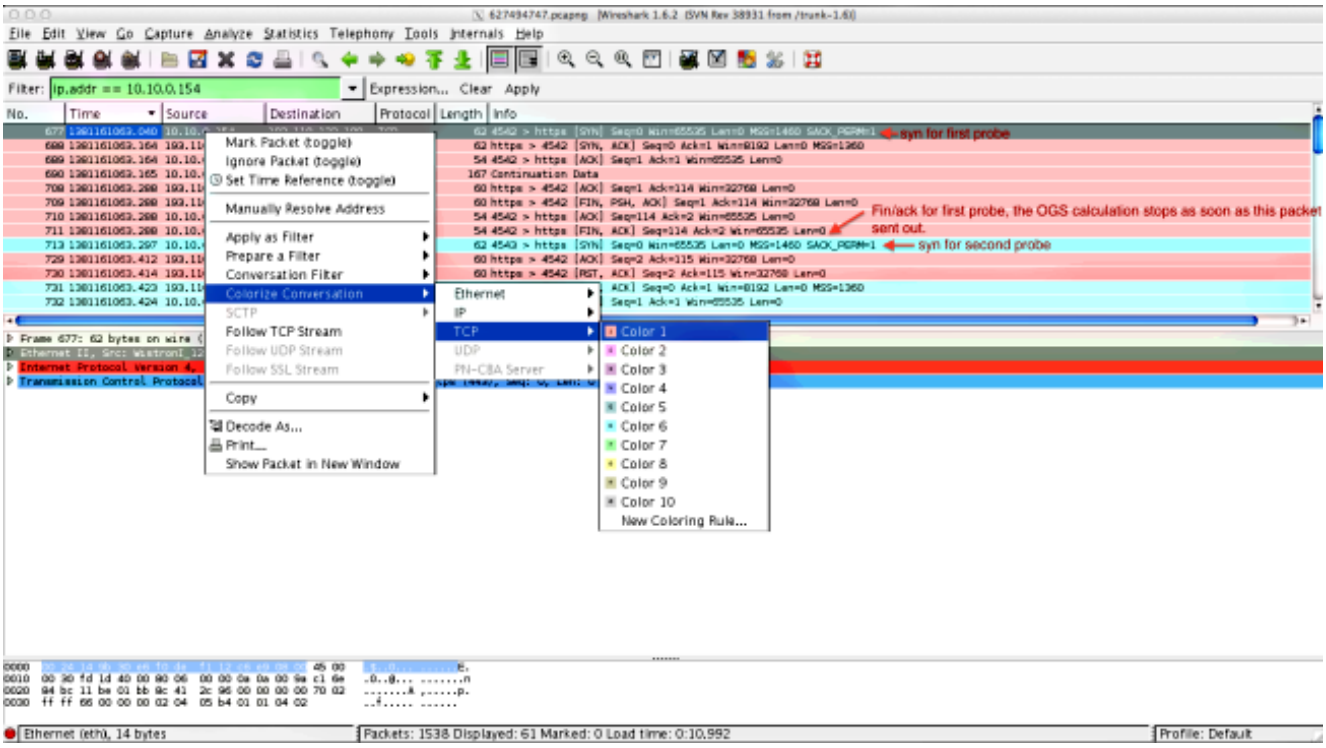
2. В этом новом перехвате перейдите для **Просмотра> Формат отображения времени> Дата и время Дня**:



3. Определите первый SYN - пакет HTTP в этом перехвате, который передавался, когда зонд OGS передавался на основе журналов DART, как определено в Шаге 3.3.2. Важно помнить, что для первого сервера первый запрос HTTP не является зондом сервера. Легко принять первый запрос о зонде сервера, и таким образом поступить в значения, абсолютно отличающиеся от того, о чем сообщает OGS. Эта проблема выделена здесь:

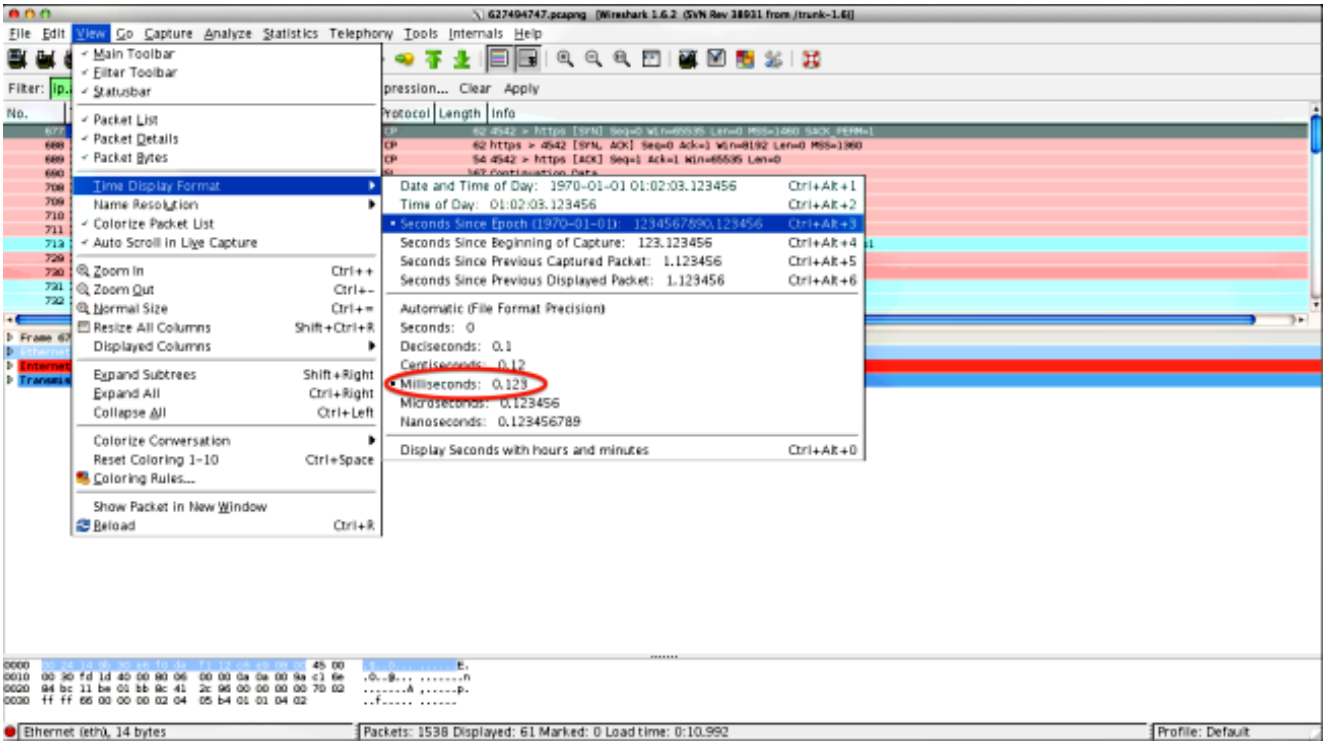


4. Чтобы более легко определить каждый из зондов, щелкните правой кнопкой мыши **SYN HTTP** для первого зонда, и затем выберите **Colorize Conversation** как показано здесь:



Повторите этот процесс для SYN на всех зондах. Как показано в предыдущем образе, первые два зонда изображены в других цветах. Преимущество colorizing диалоги TCP должно легко определить повторные передачи или другие такие причуды на зонд.

5. Для изменения отображения времени перейдите для **Просмотра> Формат отображения времени> Секунды С Эпохи**:



Выберите **Milliseconds**, потому что это - уровень точности это использование OGS.

6. Вычислите разницу во времени между SYN HTTP и FIN/ACK, как показано в схеме Шага 4. Повторите этот процесс для каждого из трех зондов и выдержите сравнение, значения к показанным в DART входит в Шаг 3.3.3.

Анализ

Если после анализа перехватов решительные значения RTT вычислены и по сравнению со значениями, замеченными в журналах DART, и все, как находят, совпадает, но все еще кажется, что неправильный шлюз выбирается, то это происходит из-за одной из двух проблем:

- На головном узле существует проблема. Если это верно, могло бы быть слишком много повторных передач от одного определенного головного узла или любые другие такие причуды, замеченные в зондах. Требуется более близкий анализ обмена.

- Существует проблема с интернет-провайдером (ISP). Если это верно, могла бы быть фрагментация или большие задержки, видевшие один определенный головной узел.

ВОПРОСЫ И ОТВЕТЫ

Вопрос. : OGS работает с распределением нагрузки?

О: Да. OGS только знает о кластерном основном названии и использовании это для оценки самого близкого головного узла.

Вопрос. : OGS работает с параметрами прокси, определенными в браузере?

О: OGS не поддерживает автоматические файлы или автоматического config прокси (PAC)

прокси, но действительно поддерживает жестко закодированный прокси-сервер. Также, операция OGS не происходит. Соответствующее сообщение журнала: "**OGS не будет выполнен, потому что настроено автоматическое обнаружение прокси**".