AnyConnect の最適なゲートウェイの選択のトラブルシューティング ガイド

目次

概要

このドキュメントでは、最適なゲートウェイの選択（OGS）を使用して問題をトラブルシューティングする方法について説明します。 OGS は、ラウンド トリップ時間（RTT）が最小のゲートウェイを特定してそのゲートウェイに接続するための機能です。 OGS 機能を使用すれば、ユーザの介在なしでインターネット トラフィックの遅延を最小限に抑えることができます。 Cisco AnyConnect セキュア モビリティ クライアント（AnyConnect）は、OGS を使用して、接続または再接続に最適なセキュア ゲートウェイを特定して選択します。 OGS は、初回接続時または、直前の接続解除から 4 時間以上経過した後の再接続時に開始されます。 詳細については、『管理者のガイド』を参照してください。

> **ヒント**： OGS は、最新の AnyConnect クライアントと ASA ソフトウェア バージョン 9.1(3)? 以降と最もうまく連動します。

OGS の機能

簡単なインターネット制御メッセージ プロトコル（ICMP） **ping要求は** ICMPパケットをブロックするようにディスカバリを防ぐために多くの Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェア（ASA）ファイアウォールが設定されるのではたらきません。 代わりに、クライアントは、すべてのプロファイルの **merge** に表示されるヘッドエンドごとに 3 つずつの HTTP/443 要求を送信します。 これらの HTTP プローブはログ内の OGS ping と呼ばれていますが、前述したように、ICMP ping ではありません。 （再）接続の時間を短縮するために、OGS

は OGS ping の結果が 7 秒以内に戻ってこなかった場合に、デフォルトで前回のゲートウェイを選択します（ログで **OGS ping results** を探してください）。

> **注:** AnyConnect は、正常な応答ではなく、応答自体が重要なため、HTTP 要求を 443 に送信する必要があります。 残念ながら、プロキシ処理に対する修正では、すべての要求が HTTPS として送信されます。 「Cisco Bug ID CSCtg38672 - OGS は HTTP 要求を使って ping する必要がある」を参照してください。

> **注:** キャッシュ内にヘッドエンドが存在しない場合は、AnyConnect が最初に、認証プロキシが存在するかどうかとそれが要求を処理できるかどうかを確認するための 1 つの HTTP 要求を送信します。 サーバをプローブするために OGS ping を開始するのはこの初期要求の後だけです。

- OGS は、ドメイン ネーム システム（DNS）のサフィックスや DNS サーバの IP アドレスなどのネットワーク情報に基づいて、ユーザ ロケーションを特定します。 RTT の結果は、このロケーションと一緒に、OGS キャッシュに保存されます。
- OGS ロケーション エントリは 14 日間キャッシュされます。 Cisco バグ ID CSCtk66531 はこれらの設定をユーザ側で設定できるようにするためにファイルされました。
- ロケーション エントリが初めてキャッシュされてから 14 日後まで OGS がこのロケーションから再度実行されることはありません。 その間は、キャッシュされたエントリとそのロケーションに対して決定された RTT が使用されます。 これは、AnyConnect が再開したときは、OGS を再度実行しないことを意味します。 代わりに、キャッシュ内のそのロケーションに最適なゲートウェイ順序が使用されます。 Diagnostic AnyConnect Reporting Tool（DART）ログに、次のメッセージが表示されます。

```
*******************************************
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.

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

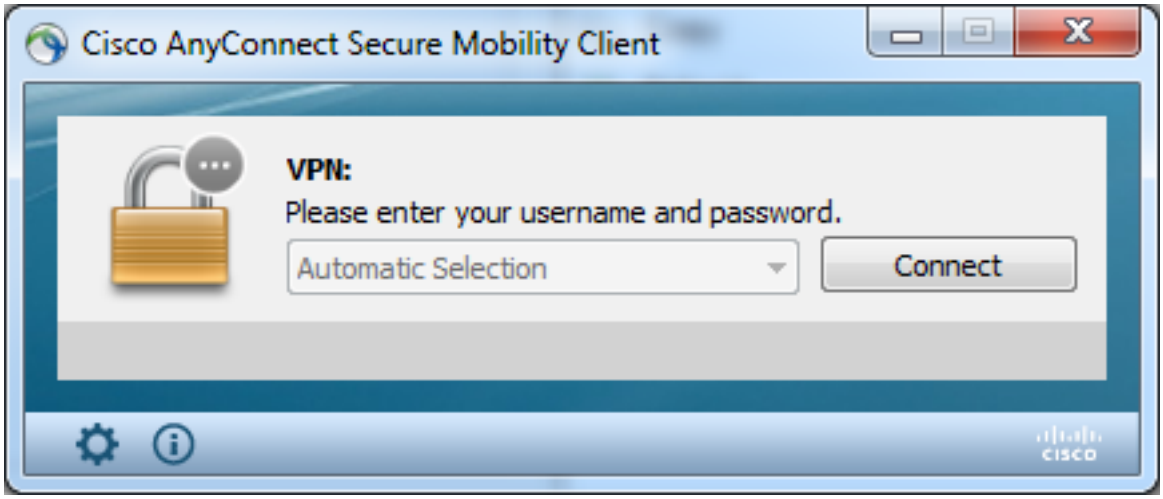
- RTT は、ユーザが AnyConnect プロファイル内のホスト エントリで指定された接続を試みるゲートウェイのセキュア ソケット レイヤ（SSL）ポートに対する TCP 交換を使って決定されます。

> **注:** 単純な HTTP ポストを実行してから、RTT と結果を表示する HTTP ping と違って、OGS の計算はもう少し複雑です。 AnyConnect は、サーバごとに 3 つずつのプローブを送信し、送信した HTTP SYN 間の遅延とそれらのプローブごとの FIN/ACK を計算します。 その後で、最も少ない差分を使ってサーバを比較して、選択を実行します。 そのため、HTTP ping が、AnyConnect が選択するサーバの適切な指針になる場合でも、必ずしも一致しないことがあります。 この詳細については後述します。

- 現時点で、OGS は、ユーザが一時停止から復帰したかどうかとしきい値が超過したかどうか

のチェックだけを実行します。 ユーザが接続している ASA がクラッシュまたは使用不能になっている場合は、OGS が別の ASA に接続しません。 OGS は、プロファイル内のプライマリ サーバとだけ連絡を取って、最適なものを決定します。

- OGS クライアント プロファイルがダウンロードされれば、ユーザが AnyConnect クライアントを再起動する場合、他のプロファイルを選択するオプションはここに示されているように選択不可能になります:



ユーザ マシンに倍数が他のプロファイルあってもそれらは OGS が disbaled までのそれら選択できません。

OGS キャッシュ

計算が終了すると、結果が **preferences_global** ファイルに保存されます。 このデータがファイルに保存されないという問題が発生したことがあります。

詳細については、Cisco Bug ID CSCtj84626 を参照してください。

ロケーション判別

OGS キャッシングは、DNS ドメインと個別の DNS サーバ IP アドレスの組み合わせに対して機能します。 その動作を以下に示します。

- ロケーション A には、**locationa.com** という DNS ドメインと、**ip1** と **ip2** という 2 つの DNS サーバ IP アドレスが割り当てられています。 ドメイン/IP の組み合わせごとに OGS キャッシュ エントリを指しているキャッシュ キーが作成されます。 次に、例を示します。 **locationa.com|ip1 -> ogscache1locationa.com|ip2 -> ogscache1**
- その後で、AnyConnect が物理的に異なるネットワークに接続すると、ドメイン/IP の組み合わせの同じ集合が作成され、キャッシュ リストに照らしてチェックされます。 完全に一致するものが見つかると、その OGS キャッシュ値が使用され、クライアントは**ロケーション A** に存在すると見なされます。

障害シナリオ

ここで、発生する可能性のある障害シナリオを示します。

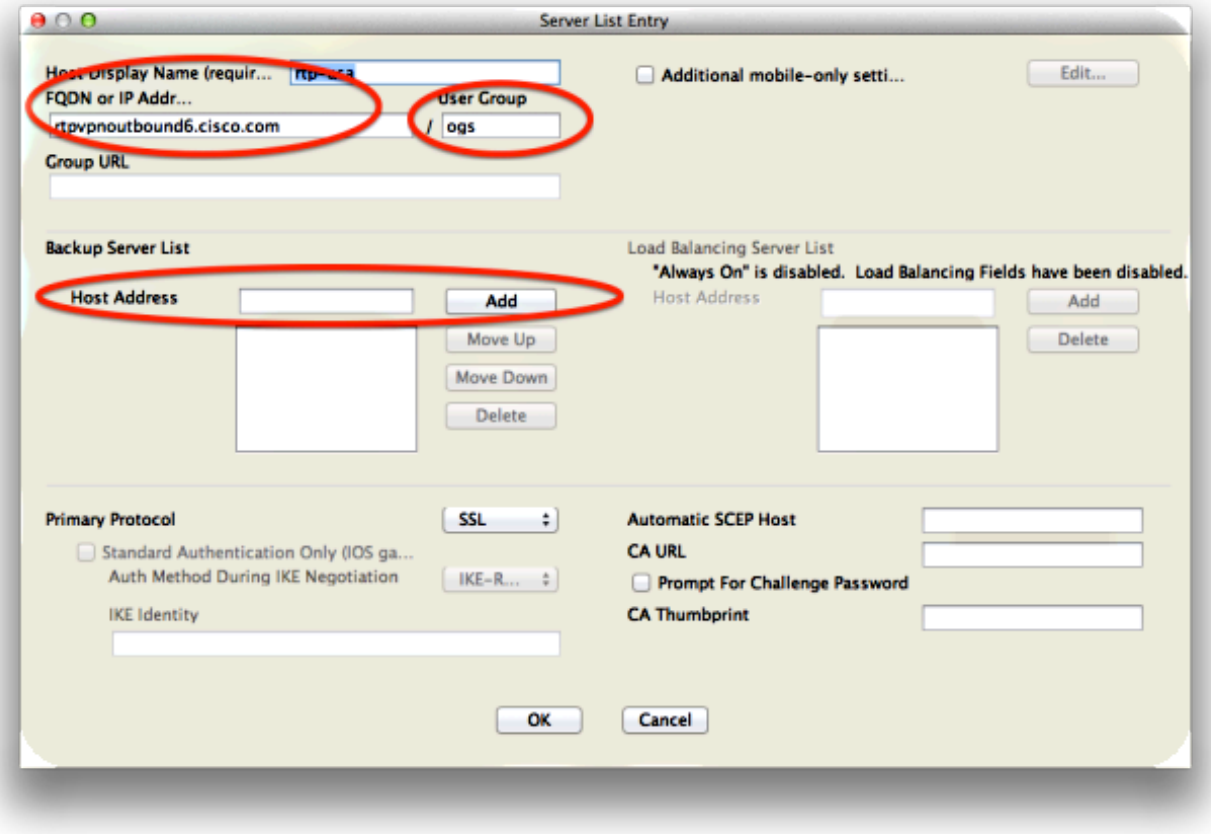
ゲートウェイへの接続が失われた場合

OGS が使用されるとき、ユーザが接続されるゲートウェイへの接続が失われる場合、AnyConnect は次の OGS ホストに**バックアップサーバ listandnot** のサーバに接続します。 動作順序は次のとおりです。

1. OGS は、プライマリ サーバとだけ連絡を取って、最適なものを決定します。

2. 決定後の接続アルゴリズムは次のとおりです。
   最適なサーバへの接続を試行する。それが失敗した場合は、最適なサーバのバックアップ サーバ リストを試す。それが失敗した場合は、選択結果の順に、OGS 選択リストに残っているサーバを試す。

   注: 管理者がバックアップ サーバ リストを設定するときに、最新のプロファイル エディタを使用すれば、バックアップ サーバの完全修飾ドメイン名（FQDN）を入力することはできますが、プライマリ サーバのようにユーザ グループを入力することはできません。



[これを修正するために Cisco Bug ID CSCud84778 が提起されていますが、バックアップ サーバのホスト アドレス フィールドに完全な URL を入力しなければ機能しません。]
https://*<ip-address>/usergroup*.

一時停止後の再開

OGS が再開後に動作するためには、マシンがスリープ状態になった時点で、AnyConnect が接続を確立している必要があります。 再開後の OGS は、ネットワーク接続が使用可能であることを確認するためのネットワーク環境テストの実施後にのみ実行されます。 このテストには DNS 接続サブテストが含まれます。

ただし、DNS サーバが、"name not found" で返信する（より一般的なケース、必ずテスト中に発生する）のとは対照的に、クエリー フィールドに IP アドレスが含まれているタイプ A 要求をド

ロップした場合は、Cisco bug ID CSCti20768「タイムアウトを回避するためには、IP アドレスに対するタイプ A の DNS クエリーを PTR にする必要がある」が適用されます。

TCP 遅延 ACK ウィンドウ サイズでの間違ったゲートウェイの選択

ASA バージョンがバージョン 9.1(3)より先に使用されるとき、クライアントのキャプチャは SSL ハンドシェイクで耐久性がある遅延を示します。 注目すべきは、クライアントがその ClientHello を送信してから、ASA がその ServerHello を送信することです。 通常は、その後に証明書メッセージ（オプションの Certificate Request）と ServerHelloDone メッセージが続きます。 異常はやり取りが 2 重になっていることです。

1. ASA は ServerHello の直後に証明書メッセージを送信しません。 クライアント ウィンドウ サイズは 64,860 バイトで、ASA からの応答全体を保持するのに十分な大きさです。

2. クライアントは ServerHello をすぐに ACK しないため、ASA は 120 ms 以内に ServerHello を再送信し、その時点でクライアントがデータを ACK します。 その後で、証明書メッセージが送信されます。 これは、クライアントが追加のデータを待っているようなものです。

この現象は、TCP slow-start と TCP delayed-ACK の間のやり取りが原因で発生します。 ASA バージョン 9.1(3) 以前は、ASA が 1 の slow-start ウィンドウ サイズを使用するのに対して、Windows クライアントは 2 の delayed-ACK 値を使用します。 これは、ASA は ACK を受信するまで 1 つのデータ パケットしか送信しないことを意味しますが、クライアントは 2 つのデータ パケットを受信するまで ACK を送信しないことも意味します。 ASA は、120 ms 後にタイムアウトして ServerHello を再送信してから、クライアントがデータを ACK して接続を継続します。 この動作は、Cisco Bug ID CSCug98113 によって変更されたため、ASA はデフォルトで、1 ではなく 2 の slow start ウィンドウ サイズを使用します。

これは、次の場合に OGS の計算に影響を与える可能性があります。

- 複数のゲートウェイが複数の ASA バージョンを実行している場合。
- クライアントの delayed-ACK ウィンドウ サイズが異なる場合。

このような場合は、delayed-ACK によってもたらされた遅延によって、クライアントが間違った ASA を選択する可能性があります。 この値がクライアントと ASA で異なる場合も、問題が発生する可能性があります。 このような場合の回避策は、Delayed Acknowledgements ウィンドウ サイズを調整することです。

Windows

1. **レジストリ エディタを起動します。**

2. delayed-ACK を無効にするインターフェイスの GUID を特定します。 これを実行するには、**[HKEY_LOCAL_MACHINE] > [SOFTWARE] > [Microsoft] > [WindowsNT] > [CurrentVersion] > [NetworkCards] > [(数字)] に移動します。**
NetworkCards の下に表示された数字を確認します。 右側で、[Description] にインターフェイス（Intel(R) Wireless WiFi Link 5100AGN など）が、[ServiceName] に対応する GUID が一覧表示されるはずです。

3. 次のレジストリ サブキーを探してクリックします。
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\<Interface GUID>

4. [Edit] メニューで、[New] をポイントしてから、[DWORD Value] をクリックします。

5. 新しい値に **TcpAckFrequency** という名前を付け、それに **1** の値を割り当てます。

6. Registry Editor を終了します。

7. この変更を有効にするために、Windows を再起動します。

   注: Cisco バグ ID CSCum19065 は ASA で TCP チューニング パラメータを設定可能にするためにファイルされました。

標準的な使用例

最も一般的な使用例を紹介します。あるユーザが自宅で OGS を初めて実行したときに、OGS が DNS 設定と OGS ping 結果をキャッシュ（デフォルトで 14 日間のタイムアウトに設定されている）に記録します。 そのユーザが翌日の夕方に帰宅すると、OGS は同じ DNS 設定を検索して、それをキャッシュ内で発見し、OGS ping テストをスキップします。 後日、そのユーザがインターネット サービスを提供しているホテルまたはレストランに行くと、OGS は別の DNS 設定を検出して OGS ping テストを実行し、最適なゲートウェイを選択して、その結果をキャッシュに記録します。

OGS と AnyConnect の再開設定で許可されていれば、中断状態または休止状態から再開される処理は同じです。

OGS のトラブルシューティング

ステップ 1. 再評価を実施するための OGS キャッシュのクリア

OGS キャッシュをクリアして使用可能なゲートウェイの RTT を再評価するには、PC から Global AnyConnect Preferences ファイルを削除するだけです。 ファイルの場所はオペレーティング システム（OS）によって異なります。

- Windows Vista と 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..
```

ステップ 2. 接続試行中のサーバ プローブのキャプチャ

1. テスト マシン上で Wireshark を開始します。

2. AnyConnect に対する接続試行を開始します。

3. 接続が完了したら Wireshark キャプチャを停止します。 **ヒント**： キャプチャは OGS のテストにしか使用されないため、AnyConnect がゲートウェイを選択したらすぐにキャプチャを停止することをお勧めします。 パケット キャプチャに悪影響を及ぼす可能性があるため、接続の試みは途中で切り上げることをお勧めします。

ステップ 3. OGS によって選択されたゲートウェイの確認

OGS が特定のゲートウェイを選択した理由を確認するには、次の手順を実行します。

1. 新しい接続を開始します。

2. AnyConnect DART を実行します。
   AnyConnect を起動して、[Advanced] をクリックします。[Diagnostics] をクリックします。[Next] をクリックします。[Next] をクリックします。
3. デスクトップに新しく作成された **DartBundle_XXXX_XXXX.zip ファイル**内の DART 結果を確認します。
   [Cisco AnyConnect Secure Mobility Client] > AnyConnect.txt に移動します。

   この DART ログから、特定のサーバに対して開始された OGS プローブの時刻をメモします。

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

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

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

   通常それらは同じ時間のまわりにあるはずですキャプチャが大きければ、パケットが HTTP プローブであるどれ実際の接続の試みはであるタイムスタンプは狭くなるのを助け。

   AnyConnect が 3 つのプローブをサーバに送信すると、プローブごとの結果と一緒に次のメッセージが生成されます。

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

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 )

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

この 3 つの値に注目することが重要です。これは、この値がキャプチャ結果と一致する必要があるからです。

"*** OGS Selection Results***" を含むメッセージを探して、評価された RTT と、最新の接続の試みがキャッシュされた RTT なのか、新しい計算結果なのかを確認します。

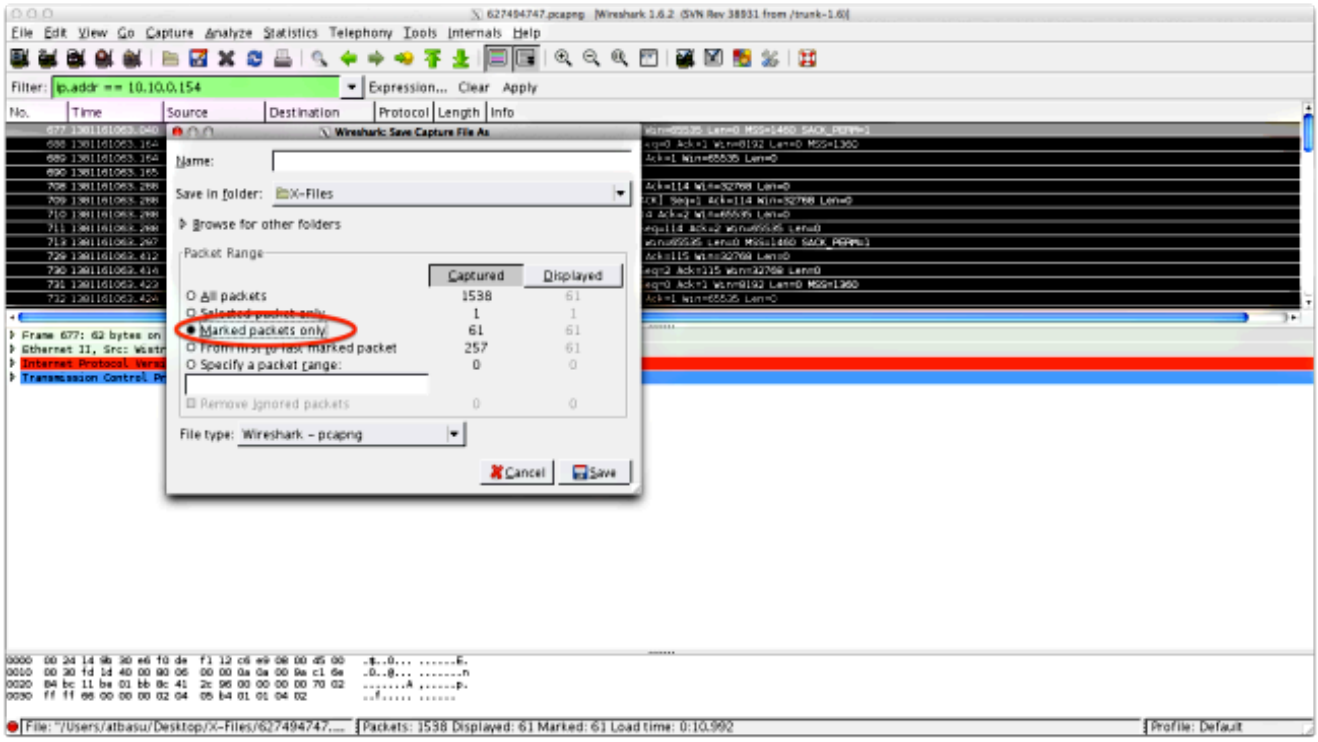
次に例を示します。

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

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.

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

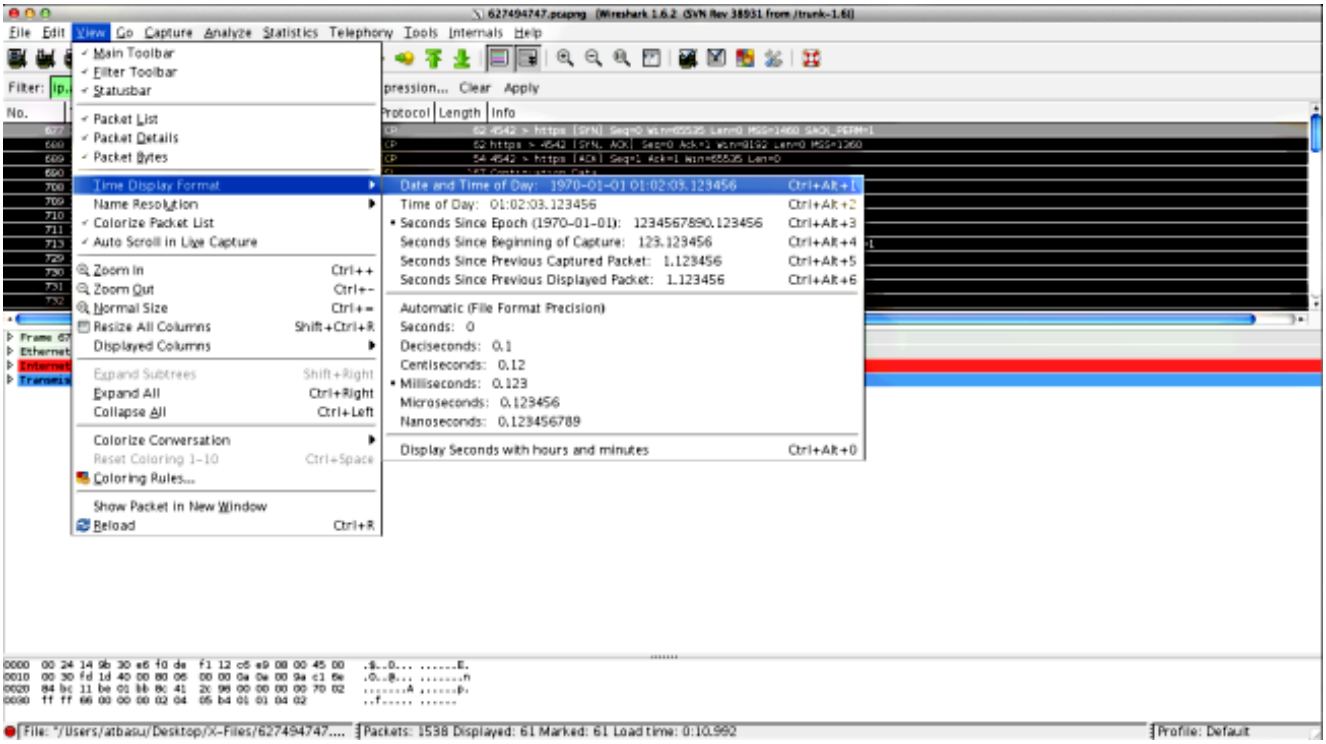
ステップ 4. AnyConnect によって実行された OGS 計算の検証

RTT の計算に使用された TCP/SSL プローブのキャプチャを検査します。 HTTPS 要求が 1 回の TCP 接続を占有する時間を確認します。 プローブ要求ごとに別々の TCP 接続を使用する必要があります。 これを実現するには、Wireshark 内のキャプチャを開いて、サーバごとに次の手順を繰り返します。

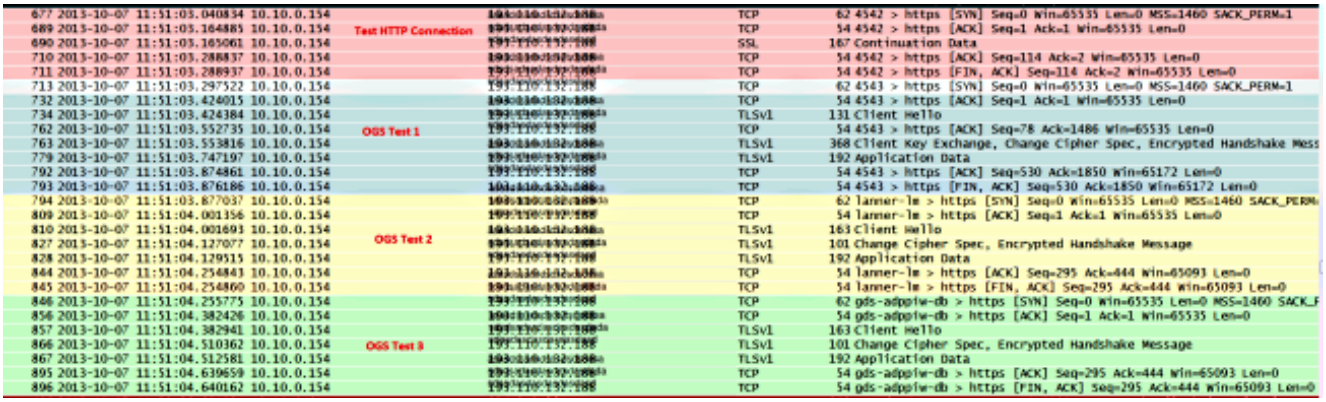
1. **ip.addr フィルタ**を使用して、各サーバに送信されたパケットを個別のキャプチャに分離します。 これを実現するには、[Edit] に移動して、[MarkAll Displayed Packets] を選択します。 **その後で**、[File] > [Save As] に移動して、[Markedpackets only] オプションを選択し、[Save] をクリックします。



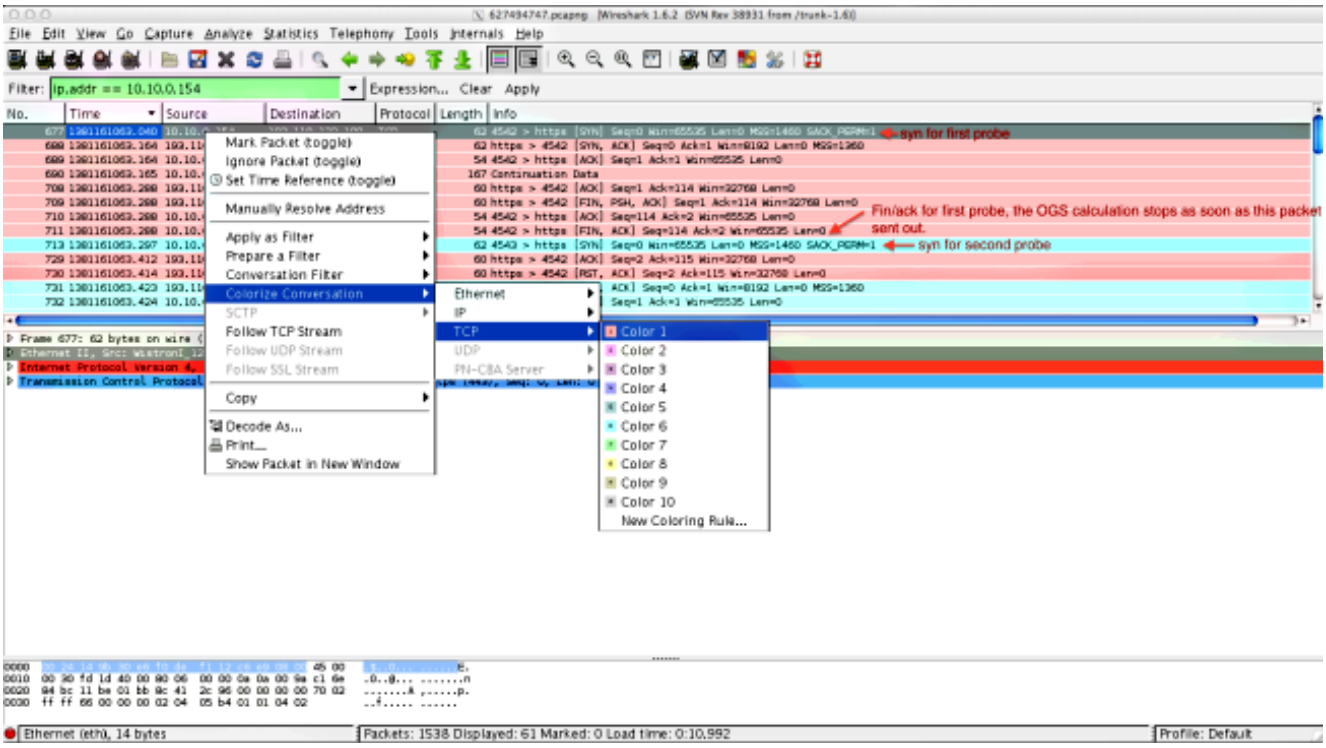
2. この新しいキャプチャで、[View] > [Time Display Format] > [Date and Time of Day] に移動します。



3. OGS プローブがステップ 3.3.2 で特定された DART ログに基づいて送信されたときに、送信されたこのキャプチャ内の最初の HTTP SYN パケットを特定します。 最初のサーバでは、最初の HTTP 要求がサーバ プローブではないことを覚えておくことが重要です。 最初の要求をサーバ プローブと誤解することによって、OGS の報告とは全く異なる値に辿り着くことがよくあります。 ここで、この問題を具体的に示します。

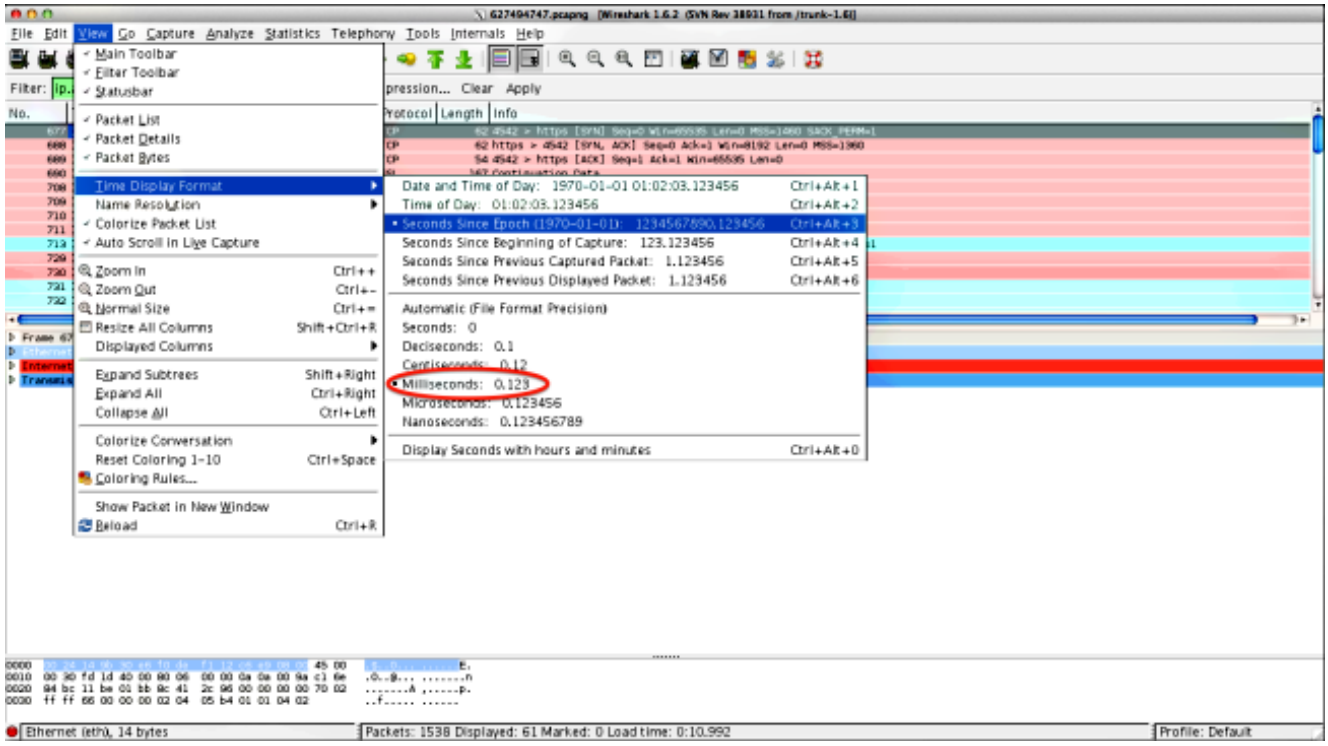


4. より簡単にプローブを識別するには、次のように、最初のプローブの [HTTP SYN] を右クリックしてから、[Colorize Conversation] を選択します。



すべてのプローブの SYN に対してこのプロセスを繰り返します。 前の図に示すように、最初の 2 つのプローブが別々の色で表示されます。 TCP カンバセーションを色分けするメリットは、プローブごとの再送信などの異常な振る舞いを簡単に見分けることができることです。

5. 時間表示を変更するには、[View] > [Time Display Format] > [Seconds Since Epoch] に移動します。



[Milliseconds] を選択します。これは、それが OGS が使用する精度レベルだからです。

6. ステップ 4 の図に示すように、HTTP SYN と FIN/ACK 間の時間差を計算します。3 つのプローブのそれぞれに対してこのプロセスを繰り返し、ステップ 3.3.3 の DART ログに表示された値と比較します。

分析

の分析は投げ矢ログで調べられる値と判別された RTT 値を計算され、比較されるおよびキャプチャ した後すべてが調和するためにあるが間違ったゲートウェイのようにそれでも選択されればようである場合、2 つの問題の 1 つが原因です:

- ヘッドエンドに問題がある場合。 この場合は、特定のヘッドエンドからの再送信が多すぎたり、他にもプローブ内で似たような異常が見られたりします。 より厳密なやり取りの分析が必要です。

- インターネット サービス プロバイダー（ISP）に問題がある場合。 この場合は、特定のヘッドエンドでフラグメンテーションや大きな遅延が見つかることがあります。

Q&A

Q： OGS はロードバランシングと連動しますか。

A： はい。 OGS は、クラスタ マスター名だけを認識して、それを最も近いヘッドエンドの判別に使用します。

Q： OGS はブラウザで定義されたプロキシ設定と連動しますか。

A： OGS は、自動プロキシまたはプロキシ自動設定（PAC）ファイルをサポートしませんが、ハードコードされたプロキシ サーバはサポートします。 そのため、OGS 操作は行われません。 関

連する口グ メッセージは次のとおりです。 「OGS will not be performed because automatic proxy detection is configured.」