AnyConnect Optimal Gateway Selection 트러블슈팅 가이드

목차

[소개](#)
[OGS는 어떻게 작동합니까?](#)
[OGS 캐시](#)
[위치 결정](#)
[실패 시나리오](#)
[게이트웨이에 대한 연결이 끊어진 경우](#)
[일시 중단 후 다시 시작](#)
[TCP Delayed-ACK 창 크기가 잘못된 게이트웨이를 선택합니다.](#)
[일반적인 사용자 예](#)
[OGS 문제 해결](#)
[1단계. 재평가를 강제로 수행하려면 OGS 캐시를 지웁니다.](#)
[2단계. 연결 시도 중에 서버 프로브를 캡처합니다.](#)
[3단계. OGS에서 선택한 게이트웨이를 확인합니다.](#)
[4단계. AnyConnect에서 실행되는 OGS 계산 검증](#)
[분석](#)
[질문과 대답](#)

소개

이 문서에서는 OGS(Optimal Gateway Selection)의 문제를 해결하는 방법에 대해 설명합니다 .OGS는 RTT(Round Trip Time)가 가장 낮은 게이트웨이를 확인하고 해당 게이트웨이에 연결하는 데 사용할 수 있는 기능입니다.사용자 개입 없이 인터넷 트래픽의 레이턴시를 최소화하기 위해 OGS 기능을 사용할 수 있습니다.OGS를 통해 Cisco AnyConnect Secure Mobility Client(AnyConnect)는 연결 또는 재연결에 가장 적합한 보안 게이트웨이를 식별하고 선택합니다 .OGS는 첫 번째 연결 시 또는 이전 연결 해제 후 최소 4시간 후에 재연결 시 시작됩니다.자세한 내용은 관리자 가이드에서 확인할 수 있습니다.

> **팁**:OGS는 최신 AnyConnect 클라이언트 및 ASA 소프트웨어 버전 9.1(3)* 이상에서 가장 잘 작동합니다.

OGS는 어떻게 작동합니까?

많은 Cisco ASA(Adaptive Security Appliance) 방화벽이 검색을 방지하기 위해 ICMP 패킷을 차단하도록 구성되어 있으므로 단순 ICMP(Internet Control Message Protocol) **ping** 요청이 작동하지 않습니다.대신 클라이언트는 모든 프로파일의 **병합**에 나타나는 각 헤드엔드에 3개의 HTTP/443 요청을 보냅니다.이러한 HTTP 프로브는 로그에서 OGS ping이라고 하지만 앞에서 설명한 것처럼 ICMP ping은 아닙니다.(re) 연결이 너무 오래 걸리지 않도록 하기 위해 OGS는 7초 이내에 OGS ping 결과를 수신하지 않을 경우 기본적으로 이전 게이트웨이를 선택합니다.(로그**에서 OGS ping 결과**를 찾습니다.)

참고: AnyConnect는 HTTP 요청을 443으로 보내야 합니다. 응답 자체도 중요하지만 응답이 성공적이지 않기 때문입니다.죄송합니다. 프록시 처리를 위한 수정 사항은 모든 요청을 HTTPS로 전송합니다.Cisco 버그 ID CSCtg38672 - OGS가 HTTP 요청을 사용하여 ping해야 합니다.

참고:캐시에 헤드엔드가 없는 경우 AnyConnect는 인증 프록시가 있는지, 요청을 처리할 수 있는지 확인하기 위해 먼저 하나의 HTTP 요청을 보냅니다.이 초기 요청 이후에만 서버를 검색하기 위해 OGS ping을 시작합니다.

- OGS는 DNS(Domain Name System) 접미사 및 DNS 서버 IP 주소와 같은 네트워크 정보를 기반으로 사용자 위치를 결정합니다.RTT 결과는 이 위치와 함께 OGS 캐시에 저장됩니다.

- OGS 위치 항목은 14일 동안 캐시됩니다.Cisco 버그 ID CSCtk66531이 이 설정을 사용자가 구성할 수 있도록 실패했습니다.

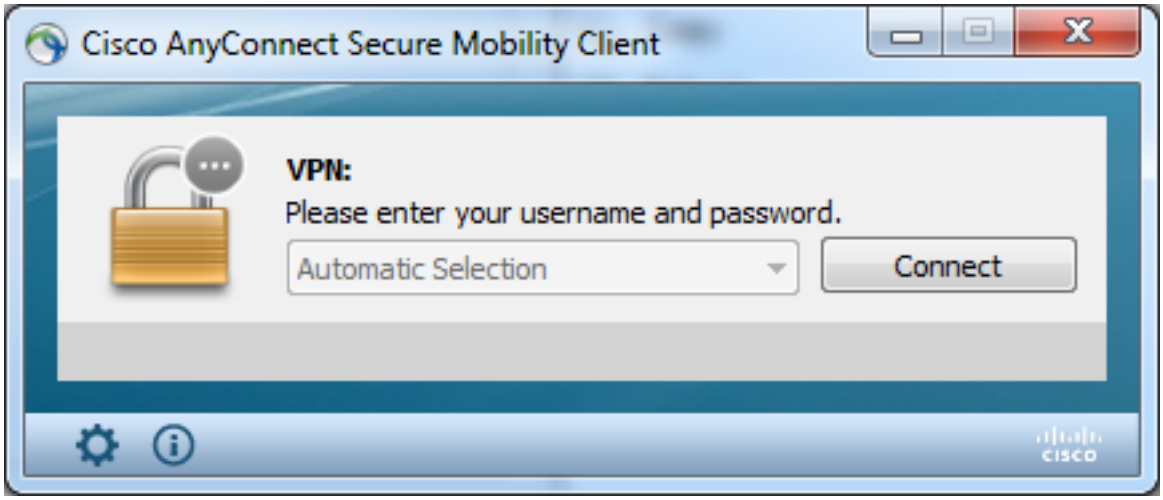
- OGS는 위치 항목이 처음 캐시된 후 14일이 경과할 때까지 이 위치에서 다시 실행되지 않습니다.이 시간 동안 캐시된 항목과 해당 위치에 대해 결정된 RTT를 사용합니다.즉, AnyConnect가 다시 시작되면 OGS가 다시 수행되지 않습니다.대신 캐시에 있는 최적의 게이트웨이 순서를 해당 위치에 사용합니다.진단 DART(AnyConnect Reporting Tool) 로그에서 다음 메시지가 표시됩니다.

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

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

- RTT는 사용자가 AnyConnect 프로파일의 호스트 항목에 지정된 대로 연결을 시도할 게이트웨이의 SSL(Secure Sockets Layer) 포트에 대한 TCP 교환을 통해 결정됩니다.

  참고: 간단한 HTTP 게시물을 수행한 다음 RTT와 결과를 표시하는 HTTP-ping과 달리 OGS 계산은 약간 더 복잡합니다.AnyConnect는 각 서버에 대해 3개의 프로브를 전송하고, 전송하는 HTTP SYN과 각 프로브에 대한 FIN/ACK 간의 지연을 계산합니다.그런 다음 가장 낮은 델타 값을 사용하여 서버를 비교하고 선택합니다.따라서 HTTP-ping은 AnyConnect에서 어떤 서버를 선택할지 잘 나타내지만 반드시 집계되지는 않을 수도 있습니다.이에 대한 자세한 내용은 문서의 나머지 부분에 나와 있습니다.
- 현재 OGS는 사용자가 일시 중단에서 나오고 임계값이 초과된 경우에만 검사를 실행합니다.사용자가 ASA에 연결되어 있는 경우 OGS가 다른 ASA에 연결되지 않거나 사용할 수 없게 되면 OGS는 연결되지 않습니다.OGS는 최적의 서버를 확인하기 위해 프로파일의 기본 서버에만 연결합니다.

- OGS 클라이언트 프로파일이 다운로드되면 사용자가 AnyConnect 클라이언트를 다시 시작하면 다음과 같이 다른 프로파일을 선택하는 옵션이 회색으로 비활성화됩니다.



사용자 시스템에 다른 프로파일이 여러 개 있는 경우에도 OGS가 비활성화될 때까지 해당 프로파일을 선택할 수 없습니다.

OGS 캐시

계산이 완료되면 결과가 preferences_**global** 파일에 저장됩니다.이 데이터가 이전에 파일에 저장되지 않는 데 문제가 있습니다.

자세한 내용은 Cisco 버그 ID CSCtj84626을 참조하십시오.

위치 결정

OGS 캐싱은 DNS 도메인과 개별 DNS 서버 IP 주소의 조합에서 작동합니다.다음과 같이 작동합니다.

- 위치 A에는 **locationa.com**의 DNS 도메인이 있으며 두 개의 DNS 서버 IP 주소(**ip1** 및 **ip2)가 있습니다**. 각 도메인/IP 조합은 OGS 캐시 항목을 가리키는 캐시 키를 생성합니다.예: **locationa.com|ip1 -> ogscache1locationa.com|ip2 -> ogscache1**
- AnyConnect가 물리적으로 다른 네트워크에 연결되면 캐시된 목록에 대해 동일한 도메인/IP 조합 확대가 생성되고 확인됩니다.일치하는 항목이 있으면 해당 OGS 캐시 값이 사용되며 클라이언트는 여전히 **A 위치**에 있는 것으로 간주됩니다.

실패 시나리오

다음과 같은 몇 가지 오류 시나리오를 사용자에게 제공합니다.

게이트웨이에 대한 연결이 끊어진 경우

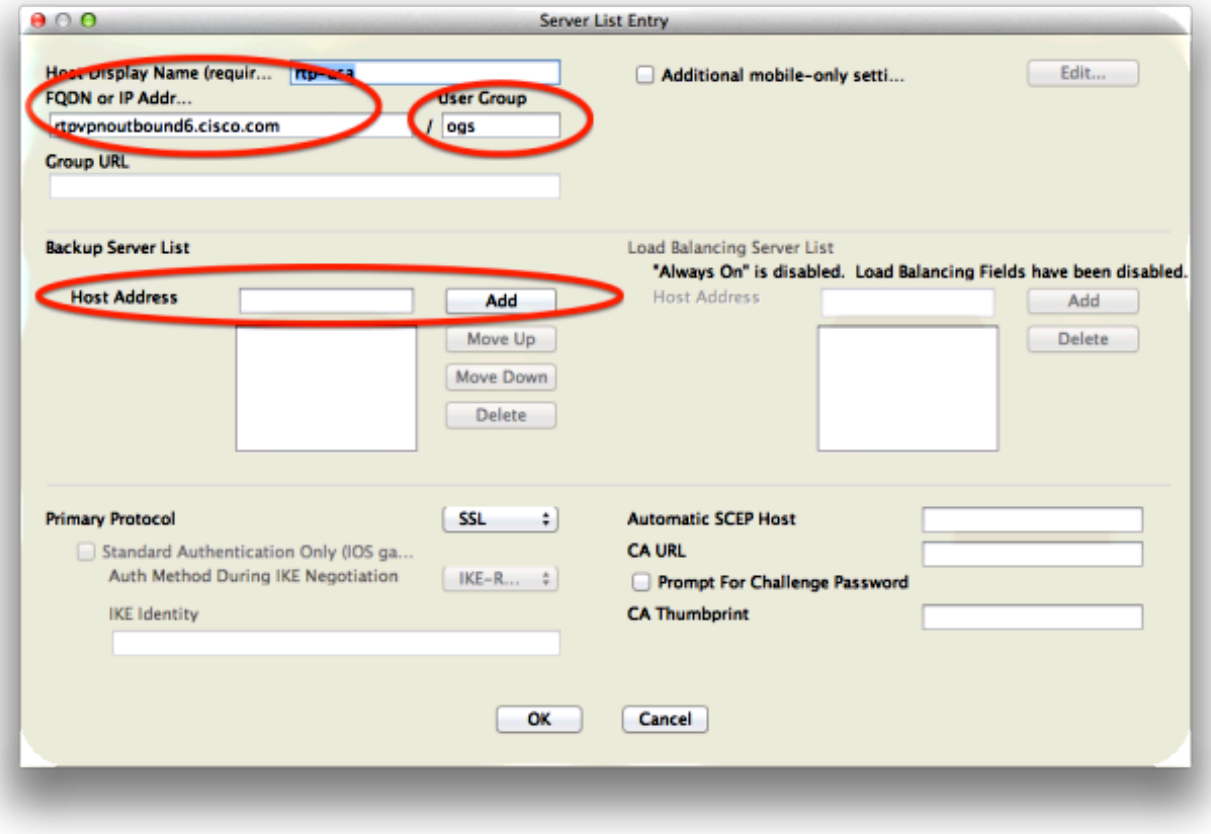
OGS를 사용할 때 사용자가 연결된 게이트웨이에 대한 연결이 끊기면 AnyConnect가 의 서버에 연결됩니다. **백업 서버 목록및아님** 다음 OGS 호스트에 연결합니다.운영 순서는 다음과 같습니다.

1. OGS는 기본 서버에만 연결하여 최적의 서버를 결정합니다.

2. 연결 알고리즘이 확인되면 다음과 같습니다.
   최적의 서버에 연결을 시도합니다.오류가 발생하면 최적의 서버 백업 서버 목록을 시도합니다

.오류가 발생하면 OGS 선택 목록에 남아 있는 각 서버를 선택 결과에 따라 정렬하여 시도합니다.

참고:관리자가 백업 서버 목록을 구성할 때, 현재 프로파일 편집기는 관리자가 백업 서버에 대한 FQDN(Fully Qualified Domain Name)만 입력할 수 있지만 주 서버에 대해서는 사용자 그룹을 입력할 수 없습니다.



Cisco 버그 ID CSCud84778을 수정하기 위해 이 오류가 발생했지만 전체 URL은 백업 서버의 호스트 주소 필드에 입력해야 하며 다음 작업을 수행해야 합니다.**https://*<ip-address>*/usergroup**.

일시 중단 후 다시 시작

OGS를 이력서 후에 실행하려면 시스템이 절전 모드로 전환될 때 AnyConnect에 연결이 설정되어 있어야 합니다.다시 시작 후 OGS는 네트워크 환경 테스트가 발생한 후에만 수행되며, 이는 네트워크 연결이 사용 가능한지 확인하는 것입니다.이 테스트에는 DNS 연결 하위 테스트가 포함되어 있습니다.

그러나 DNS 서버가 "name not found"(일반적으로 테스트 중에 항상 발생)로 회신하는 대신 쿼리 필드에 IP 주소가 있는 A 유형의 요청을 삭제하는 경우, Cisco 버그 ID CSCti20768 "IP 주소에 대한 A 유형의 DNS 쿼리는 시간 초과를 방지하려면 PTR이어야 합니다."가 적용됩니다.

TCP Delayed-ACK 창 크기가 잘못된 게이트웨이를 선택합니다.

버전 9.1(3) 이전의 ASA 버전을 사용하는 경우, 클라이언트의 캡처는 SSL 핸드셰이크의 지속적인 지연을 표시합니다.클라이언트가 ClientHello를 전송한 다음 ASA가 ServerHello를 전송한다는 점에 주목됩니다.일반적으로 인증서 메시지(선택적 인증서 요청) 및 ServerHelloDone 메시지가 그 뒤에 옵니다.이상 징조는 2배입니다.

1. ASA는 ServerHello 후에 인증서 메시지를 즉시 전송하지 않습니다.클라이언트 윈도우 크기는

64,860바이트로, ASA의 전체 응답을 저장하기에 충분합니다.

2. 클라이언트가 ServerHello를 즉시 ACK하지 않으므로 ASA는 ~120ms 후 ServerHello를 재전송하며, 여기서 클라이언트 ACK는 데이터를 재전송합니다.그러면 인증서 메시지가 전송됩니다.클라이언트가 더 많은 데이터를 기다리는 것과 같습니다.

이는 TCP slow-start와 TCP delayed-ACK 간의 상호 작용 때문에 발생합니다.ASA 버전 9.1(3) 이전 버전에서는 ASA가 느린 시작 창 크기 1을 사용하는 반면 Windows 클라이언트는 delayed-ACK 값 2를 사용합니다. 즉, ASA는 ACK를 가져올 때까지 데이터 패킷을 하나만 전송하지만, 클라이언트가 두 개의 데이터 패킷을 받을 때까지 ACK를 전송하지 않음을 의미합니다.ASA는 120ms 후 시간이 초과되어 ServerHello를 재전송합니다. 그러면 클라이언트는 데이터를 ACK로 전송하고 연결이 계속됩니다. 이 동작은 Cisco 버그 ID CSCug98113에 의해 변경되어 ASA가 기본적으로 1이 아닌 2의 느린 시작 창 크기를 사용합니다.

다음과 같은 경우 OGS 계산에 영향을 줄 수 있습니다.

- 게이트웨이가 서로 다른 ASA 버전을 실행합니다.
- 클라이언트의 지연 ACK 창 크기가 다릅니다.

이러한 경우 delayed-ACK에서 도입된 지연으로 인해 클라이언트가 잘못된 ASA를 선택하게 할 수 있습니다. 클라이언트와 ASA 간에 이 값이 다르면 여전히 문제가 발생할 수 있습니다.이러한 경우 해결 방법은 지연된 확인 응답 창 크기를 조정하는 것입니다.

윈도우

1. **레지스트리 편집기를 시작합니다.**

2. delayed-ACK를 비활성화할 인터페이스의 GUID를 식별합니다.이렇게 하려면 대상: **HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > WindowsNT > CurrentVersion > NetworkCards > (number).**
NetworkCards 아래에 나열된 각 번호를 확인합니다.오른쪽의 설명에 인터페이스(예: 인텔(R) 무선 WiFi 링크 5100AGN)가 나열되고 서비스 이름에 해당 GUID가 나열되어야 합니다.

3. 다음 레지스트리 하위 키를 찾아 클릭합니다.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\<인터페이스 GUID>

4. 편집 메뉴에서 새로 만들기를 가리킨 다음 **DWORD 값**을 클릭합니다.

5. 새 값의 이름을 **TcpAckFrequency**로 지정하고 값을 **1**로 지정합니다.

6. 레지스트리 편집기를 끝냅니다.

7. 변경 내용을 적용하려면 Windows를 다시 시작하십시오.

참고: Cisco 버그 ID CSCum19065가 ASA에서 TCP 튜닝 매개변수를 구성할 수 있도록 실패했습니다.

일반적인 사용자 예

가장 일반적인 활용 사례는 홈에서 사용자가 처음으로 OGS를 실행할 때 DNS 설정을 기록하고 OGS ping을 수행하면 캐시에 저장됩니다(기본값은 14일 시간 제한). 사용자가 다음날 저녁에 집으로 돌아오면 OGS는 동일한 DNS 설정을 탐지하고 캐시에서 이를 찾은 다음 OGS ping 테스트를 건너뜁니다.나중에 사용자가 인터넷 서비스를 제공하는 호텔 또는 레스토랑으로 이동하면 OGS는 다른 DNS 설정을 탐지하고 OGS ping 테스트를 실행하고 최상의 게이트웨이를 선택하며 결과를 캐시

에 기록합니다.

OGS 및 AnyConnect 재개 설정이 허용하는 경우 일시 중단 또는 최대 절전 모드 상태에서 다시 시작할 때 처리가 동일합니다.

OGS 문제 해결

1단계. 재평가를 강제로 수행하려면 OGS 캐시를 지웁니다.

OGS 캐시를 지우고 사용 가능한 게이트웨이에 대한 RTT를 재평가하려면 PC에서 Global AnyConnect Preferences 파일을 삭제하기만 하면 됩니다.파일 위치는 운영 체제(OS)에 따라 달라집니다.

- Windows Vista 및 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..
```

- 리눅스

```
/opt/cisco/anyconnect/.anyconnect_global
Note: with older versions of the client it used to be /opt/cisco/vpn..
```

2단계. 연결 시도 중에 서버 프로브를 캡처합니다.

1. 테스트 시스템에서 Wireshark를 시작합니다.

2. AnyConnect에서 연결 시도를 시작합니다.

3. 연결이 완료되면 Wireshark 캡처를 중지합니다. **팁**:캡처는 OGS를 테스트하는 데만 사용되므로 AnyConnect에서 게이트웨이를 선택하는 즉시 캡처를 중지하는 것이 좋습니다.완전한 연결 시도를 거치지 않는 것이 가장 좋습니다. 이는 패킷 캡처를 클라우드로 만들 수 있기 때문입니다.

3단계. OGS에서 선택한 게이트웨이를 확인합니다.

OGS에서 특정 게이트웨이를 선택한 이유를 확인하려면 다음 단계를 수행하십시오.

1. 새 연결을 시작합니다.

2. AnyConnect DART 실행:
   AnyConnect**를** 시작하고 Advanced(고급)를 **클릭합니다**.Diagnostics(진단)를 **클릭합니다**

.Next(**다음)를 클릭합니다**.Next(**다음)를 클릭합니다**.

3. 데스크톱에서 새로 생성된 DartBundle**_XXXX_XXXX.zip** 파일에서 발견된 DART 결과를 검토합니다.
   Cisco AnyConnect **Secure Mobility Client > AnyConnect.txt로 이동합니다**.

   이 DART 로그에서 특정 서버에 대해 OGS 프로브가 시작된 시간을 확인합니다.

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

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

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

   일반적으로 거의 같은 시간이어야 하지만 캡처가 큰 경우 타임 스탬프는 어떤 패킷이 HTTP 프로브이고 어떤 패킷이 실제 연결 시도인지를 좁히는 데 도움이 됩니다.

   AnyConnect가 서버에 3개의 프로브를 전송하면 각 프로브에 대한 결과와 함께 이 메시지가 생성됩니다.

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

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 )

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

   이러한 세 가지 값은 캡처 결과와 일치해야 하므로 주의하여 보아야 합니다.

   평가된 RTT를 보려면 "*** OGS 선택 결과***"가 포함된 메시지를 찾고, 가장 최근의 연결 시도가 캐시된 RTT 또는 새 계산의 결과인지 확인합니다.

   예를 들면 다음과 같습니다.

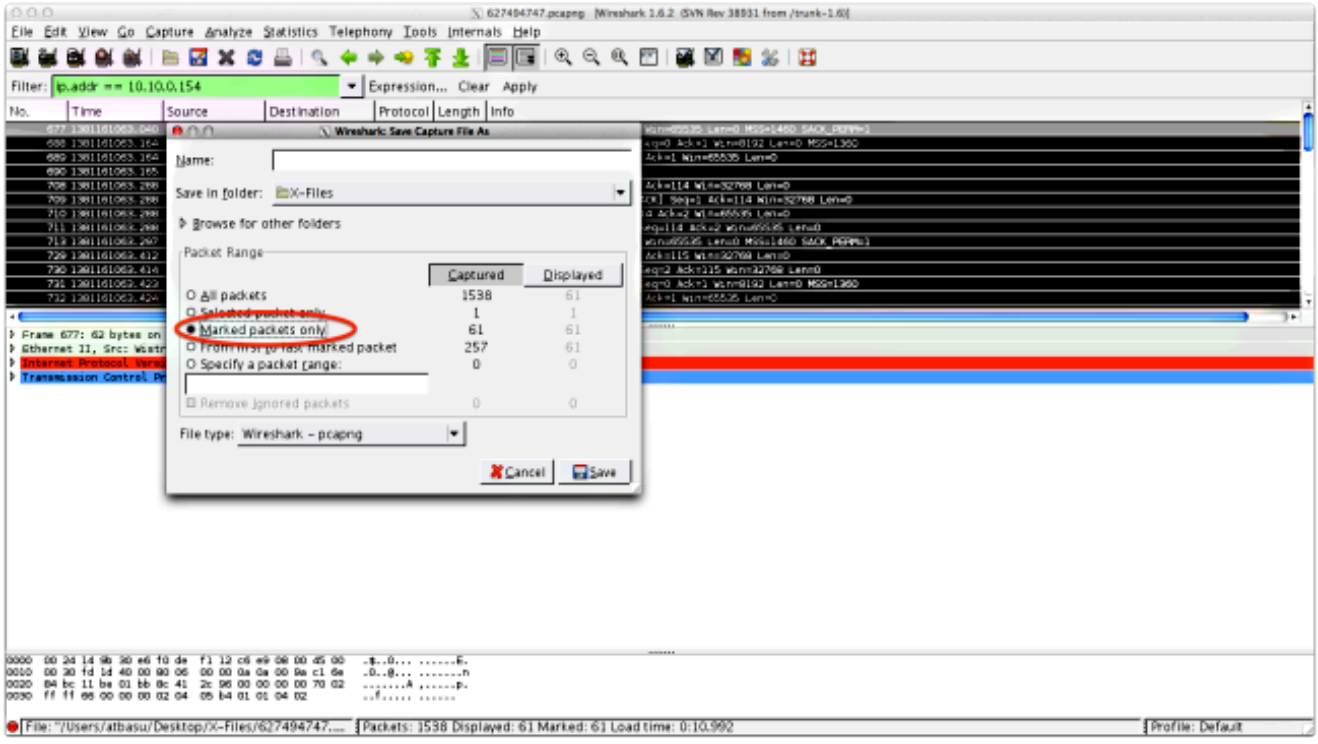
```
****************************************

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.

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

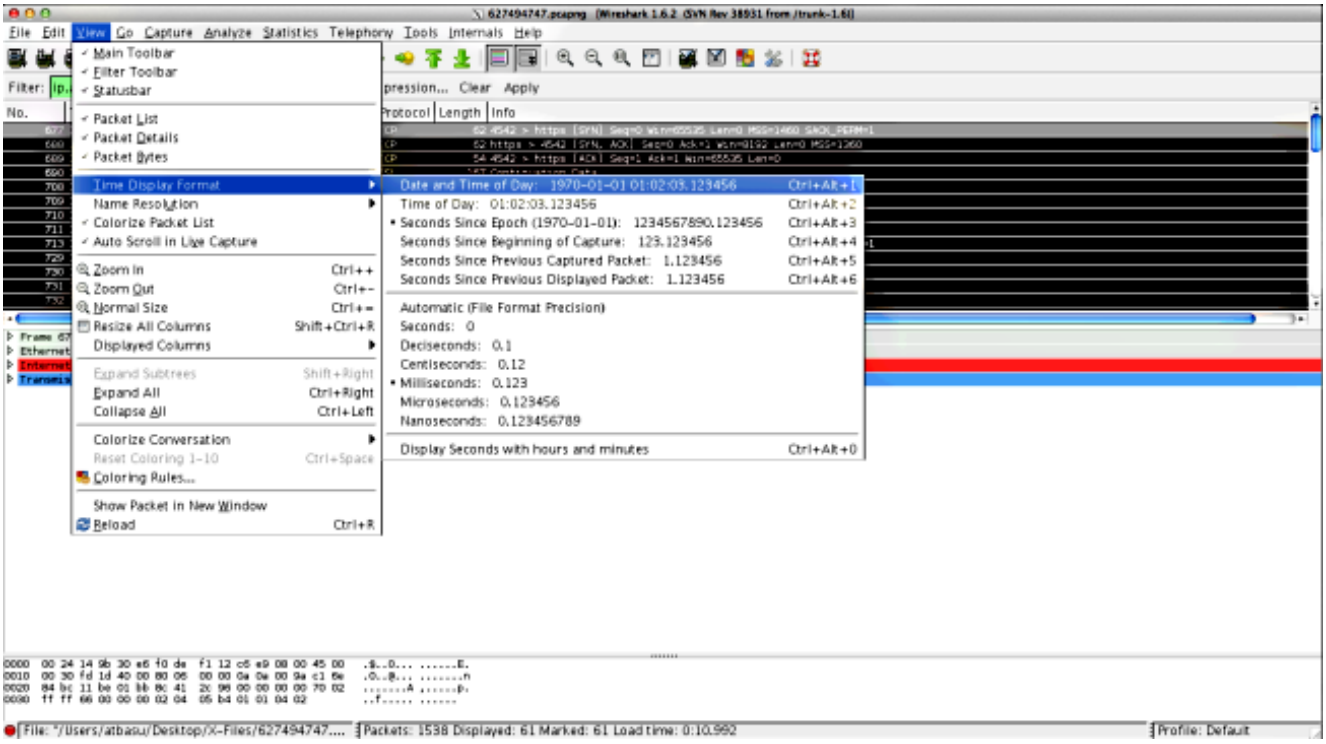
4단계. AnyConnect에서 실행되는 OGS 계산 검증

RTT를 계산하는 데 사용되는 TCP/SSL 프로브에 대해 캡처를 검사합니다.HTTPS 요청이 단일 TCP 연결을 완료하는 기간을 확인합니다.각 프로브 요청에서는 다른 TCP 연결을 사용해야 합니다.이렇게 하려면 Wireshark에서 캡처를 열고 각 서버에 대해 다음 단계를 반복합니다.

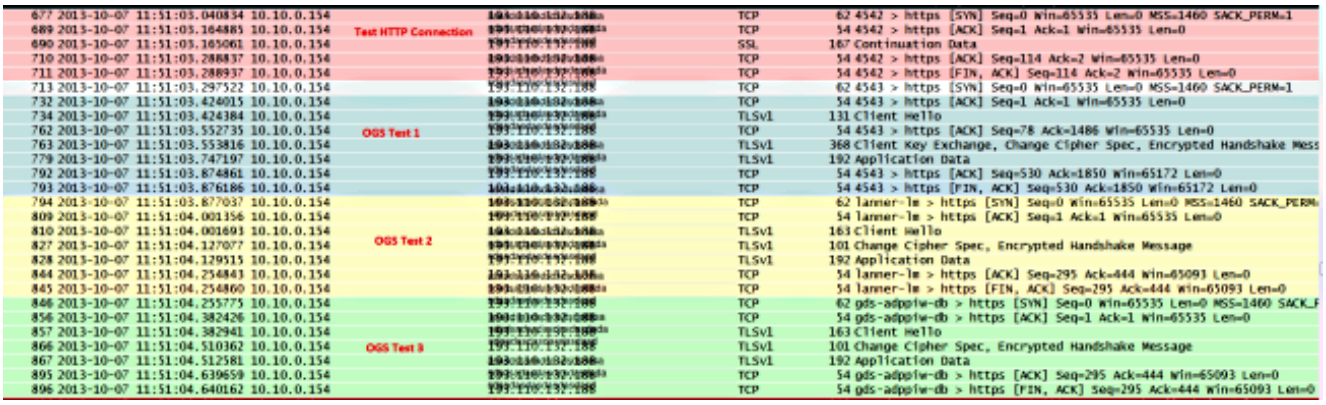
1. 각 서버로 전송된 패킷을 자체 캡처로 격리하려면 **ip.addr** 필터를 사용합니다.이렇게 하려면 Edit(편집)로 이동하여 **Mark All Displayed** Packets(**표시된 모든 패킷 표시**)**를 선택합니다**.그런 다음 File(**파일**) **> Save As(다른 이름으로 저장**)로 이동하고 **Marked packets only** 옵션을 선택하고 **Save(저장)**를 클릭합니다.



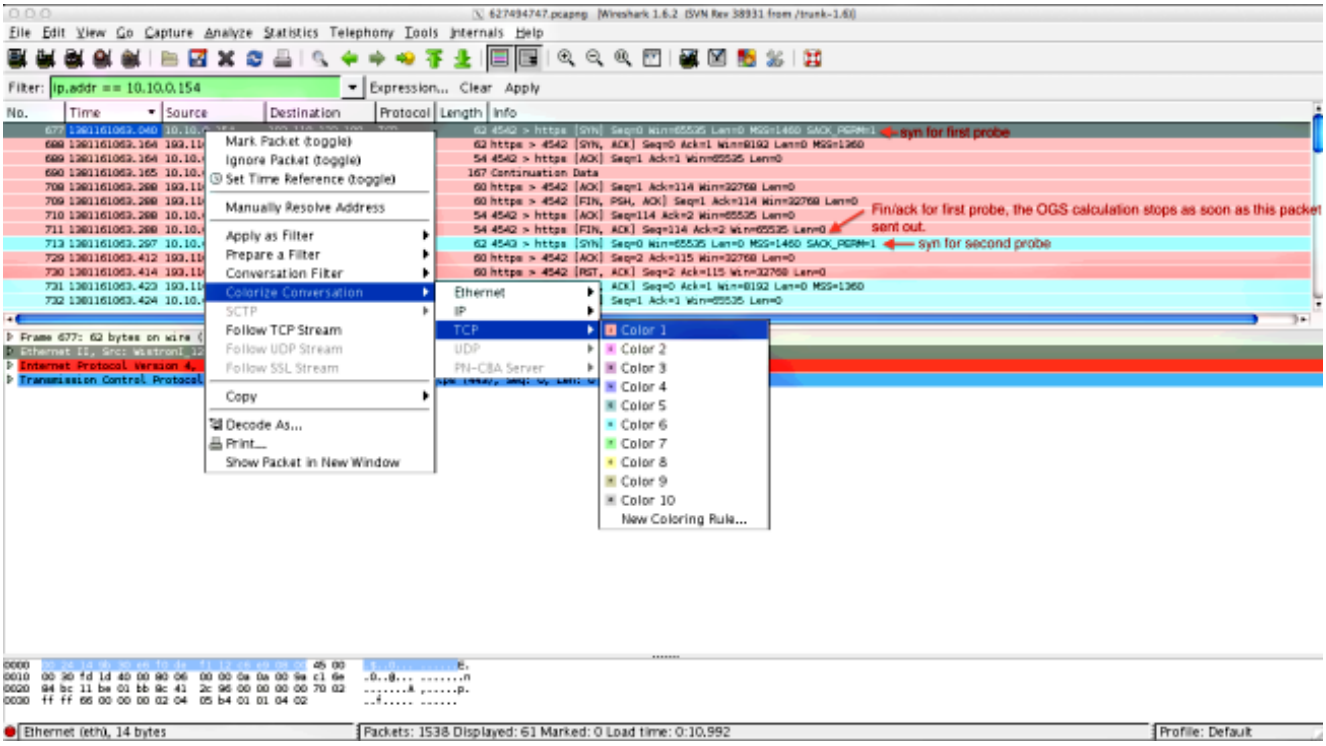
2. 이 새 캡처에서 **보기 > 시간 표시 형식 > 날짜 및 시간**:



3. 3.3.2단계에서 식별된 DART 로그를 기반으로 OGS 프로브가 전송될 때 보낸 이 캡처에서 첫 번째 HTTP SYN 패킷을 식별합니다. 첫 번째 서버의 경우 첫 번째 HTTP 요청이 서버 프로브가 아니라는 점을 기억해야 합니다.서버 프로브에 대한 첫 번째 요청을 잘못 입력하기 쉬우므로 OGS에서 보고하는 것과 완전히 다른 값에 도달합니다.이 문제는 여기에서 강조 표시됩니다.

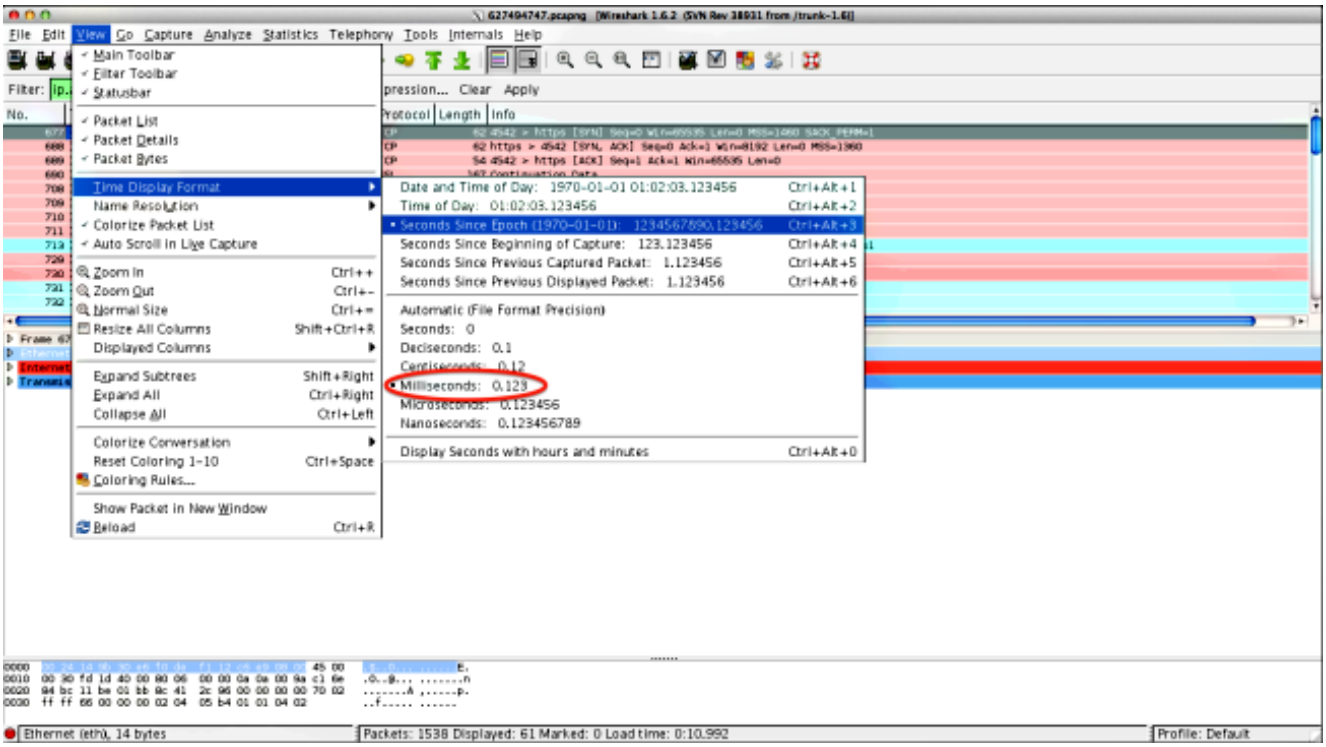


4. 각 프로브를 보다 쉽게 식별하려면 첫 번째 프로브에 대한 **HTTP SYN**을 마우스 오른쪽 단추로 클릭한 다음 아래**와** 같이 **Colorize Conversation**을 선택합니다.



모든 프로브의 SYN에 대해 이 프로세스를 반복합니다.이전 이미지에 표시된 것처럼 처음 두 프로브는 다른 색상으로 표시됩니다.TCP 대화를 색상화하면 프로브당 재전송 또는 기타 그러한 속성을 쉽게 찾아낼 수 있습니다.

5. 시간 표시를 변경하려면 View(보기) **> Time Display Format(시간 표시 형식) > Seconds Since Epoch(Epoch 이후 초)로** 이동합니다.



OGS에서 사용하는 정밀도 레벨이므로 Milliseconds를 선택합니다.

6. 단계 4 다이어그램에 표시된 대로 HTTP SYN과 FIN/ACK 간의 시간 차이를 계산합니다. 3개의 프로브 각각에 대해 이 프로세스를 반복하고 3.3.3단계의 DART 로그에 표시된 값과 비교

합니다.

분석

캡처 분석 후 확인된 RTT 값이 계산되어 DART 로그에 표시된 값과 비교되고 모든 값이 일치된 것으로 확인되었지만, 잘못된 게이트웨이가 선택되고 있는 것처럼 보일 경우 다음 두 가지 문제 중 하나가 원인입니다.

- 헤드엔드에 문제가 있습니다.이 경우, 특정 헤드엔드에서 재전송하거나 프로브에 표시되는 다른 속성이 너무 많을 수 있습니다.자세한 교환 분석이 필요합니다.

- 인터넷 서비스 공급자(ISP)에 문제가 있습니다. 이 경우 특정 헤드엔드에 대해 프래그먼트화 또는 대규모 지연이 발생할 수 있습니다.

질문과 대답

Q: OGS는 로드 밸런싱에서 작동합니까?

A: 예.OGS는 클러스터 마스터 이름만 알고 있으며 가장 가까운 헤드엔드를 판단하기 위해 이를 사용합니다.

Q:OGS는 브라우저에 정의된 프록시 설정을 사용하여 작동합니까?

A:OGS는 자동 프록시 또는 PAC(Proxy Auto Config) 파일을 지원하지 않지만 하드 코딩된 프록시 서버를 지원합니다.따라서 OGS 작업이 발생하지 않습니다. 관련 로그 메시지는 "**자동 프록시 탐지가 구성되어 있으므로 OGS가 수행되지 않습니다**."