Guida alla risoluzione dei problemi di selezione del gateway ottimale di AnyConnect

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi a Optimal Gateway Selection (OGS). OGS è una funzione che può essere utilizzata per determinare il gateway con il Round Trip Time (RTT) più basso e connettersi a tale gateway. È possibile utilizzare la funzione OGS per ridurre al minimo la latenza per il traffico Internet senza l'intervento dell'utente. Con OGS, Cisco AnyConnect Secure Mobility Client (AnyConnect) identifica e seleziona il gateway sicuro migliore per la connessione o la riconnessione. Il sistema OGS inizia al momento della prima connessione o al momento della riconnessione almeno quattro ore dopo la disconnessione precedente. Ulteriori informazioni sono disponibili nella Guida dell'amministratore.

> **Suggerimento**: Il software OGS funziona al meglio con l'ultimo client AnyConnect e il software ASA versione 9.1(3)* o successive.

Come funziona OGS?

Una richiesta **ping** ICMP (Internet Control Message Protocol) non funziona perché molti firewall Cisco Adaptive Security Appliance (ASA) sono configurati per bloccare i pacchetti ICMP e impedire il rilevamento. Al contrario, il client invia tre richieste HTTP/443 a ciascun headend che viene visualizzato in una **unione** di tutti i profili. Queste sonde HTTP vengono chiamate ping OGS nei log, ma, come spiegato in precedenza, non sono ping ICMP. Per evitare che una (ri)connessione richieda troppo tempo, il servizio GOS seleziona il gateway precedente per

impostazione predefinita se non riceve alcun risultato del ping GOS entro sette secondi. Cercare **i risultati del ping OGS** nel registro.

> **Nota:** AnyConnect deve inviare una richiesta HTTP a 443, in quanto la risposta stessa è importante, non è una risposta corretta. La correzione per la gestione del proxy invia tutte le richieste come HTTPS. Vedere l'ID bug Cisco CSCtg38672 - Il servizio OGS deve eseguire il ping con le richieste HTTP.

> **Nota:** Se la cache non contiene headend, AnyConnect invia una richiesta HTTP per determinare se esiste un proxy di autenticazione e se è in grado di gestirla. È solo dopo questa richiesta iniziale che viene avviato il ping OGS per eseguire il probe del server.

- OGS determina la posizione dell'utente in base alle informazioni di rete, ad esempio il suffisso DNS (Domain Name System) e l'indirizzo IP del server DNS. I risultati RTT, insieme a questo percorso, vengono memorizzati nella cache OGS.

- Le voci di percorso OGS vengono memorizzate nella cache per 14 giorni. Per rendere queste impostazioni configurabili dall'utente, non è stato possibile usare l'ID bug Cisco CSCtk6531.

- Il comando OGS non viene eseguito nuovamente da questo percorso fino a 14 giorni dopo la prima memorizzazione nella cache della voce relativa al percorso. Durante questo periodo, utilizza la voce memorizzata nella cache e gli RTT determinati per tale posizione. Ciò significa che, quando AnyConnect viene riavviato, non viene più eseguito il log degli accessi; utilizza invece l'ordine gateway ottimale nella cache per la posizione. Nei log dello strumento di diagnostica per la creazione di rapporti di AnyConnect (DART) viene visualizzato questo messaggio:

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

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

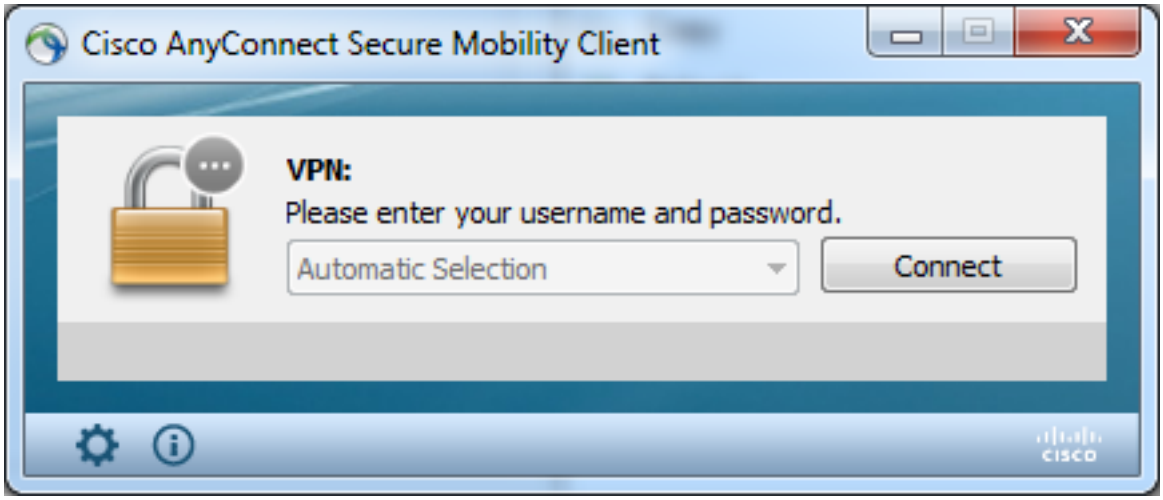
- Il valore RTT viene determinato con uno scambio TCP con la porta SSL (Secure Sockets Layer) del gateway a cui l'utente tenterà di connettersi, come specificato dalla voce host nel profilo AnyConnect.

> **Nota**: a differenza di HTTP-ping, che esegue un semplice post HTTP e quindi visualizza RTT e il risultato, i calcoli OGS sono leggermente più complicati. AnyConnect invia tre sonde per ciascun server e calcola il ritardo tra l'SYN HTTP inviato e l'FIN/ACK per ciascuna di queste sonde. Utilizza quindi il delta più basso per confrontare i server ed effettuare la selezione. Pertanto, anche se i ping HTTP sono un'indicazione abbastanza buona di quale server AnyConnect sceglierà, potrebbero non corrispondere necessariamente. Ulteriori informazioni

al riguardo sono disponibili nel resto del documento.

- Attualmente, OGS esegue i controlli solo se l'utente esce da una sospensione e la soglia è stata superata. Il protocollo OGS non si connette a un'appliance ASA diversa se l'appliance ASA a cui è connesso l'utente si blocca o non è più disponibile. OGS contatta solo i server principali nel profilo per determinare quello ottimale.

- Dopo aver scaricato il profilo del client OGS, quando l'utente riavvia il client AnyConnect, l'opzione per la selezione di altri profili non sarà disponibile, come mostrato di seguito:



Anche se il computer dell'utente dispone di più profili, non sarà in grado di selezionarne nessuno finché non viene disabilitato OGS.

Cache OGS

Al termine del calcolo, i risultati vengono memorizzati nel file **preferences_global**. Si sono verificati problemi con i dati non memorizzati nel file in precedenza.

Per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCtj84626.

Determinazione ubicazione

La memorizzazione nella cache OGS funziona su una combinazione di dominio DNS e indirizzi IP dei singoli server DNS. Funziona come segue:

- La posizione A ha un dominio DNS di **location.com** e due indirizzi IP server DNS - **ip1** e **ip2**. Ogni combinazione dominio/IP crea una chiave cache che punta a una voce della cache OGS. Ad esempio: **locationa.com|ip1 -> cache1locationa.com|ip2 -> cache1**
- Se AnyConnect si connette a una rete fisicamente diversa, viene creata la stessa serie di combinazioni di dominio/IP e viene confrontata con l'elenco delle connessioni memorizzate nella cache. Se vengono rilevate corrispondenze, viene utilizzato il valore della cache OGS e il client viene ancora considerato nella **posizione A**.

Scenari di errore

Di seguito sono riportati alcuni possibili scenari di errore:

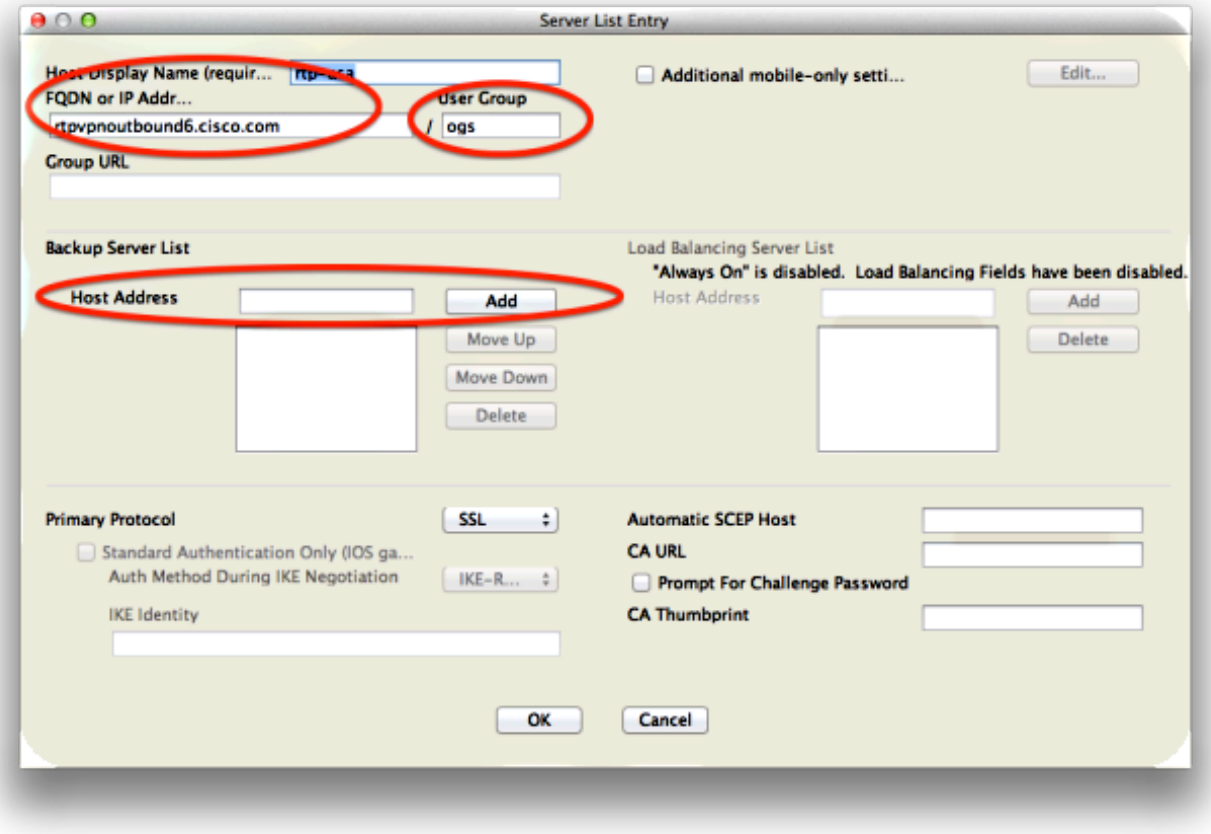
Quando la connettività al gateway viene interrotta

Quando si usa OGS, se la connettività al gateway a cui gli utenti sono connessi viene interrotta, AnyConnect si connette ai server nel **elenco dei server di backupenon** al successivo host OGS. L'ordine delle operazioni è il seguente:

1. OGS contatta solo i server primari per determinare quello ottimale.

2. Una volta determinato, l'algoritmo di connessione è:
   Tentativo di connessione al server ottimale.Se l'operazione non riesce, provare l'elenco dei server di backup ottimali.In caso di esito negativo, provare a utilizzare ogni server che rimane nell'elenco di selezione OGS, ordinato in base ai risultati della selezione.

   Nota: Quando l'amministratore configura l'elenco dei server di backup, l'editor di profili corrente consente solo all'amministratore di immettere il nome di dominio completo (FQDN) per il server di backup, ma non il gruppo di utenti possibile per il server primario:



   Per risolvere questo problema, consultare l'ID bug Cisco CSCud84778, ma l'URL completo deve essere immesso nel campo dell'indirizzo host del server di backup e deve funzionare: **https://*<indirizzo-ip>*/usergroup**.

Riprendi dopo sospensione

Per consentire l'esecuzione di GOS dopo una ripresa, è necessario che per AnyConnect sia stata stabilita una connessione quando il computer è stato messo in sospensione. Il sistema OGS viene eseguito solo dopo il test dell'ambiente di rete, allo scopo di verificare che la connettività di rete sia disponibile. Questo test include un subtest di connettività DNS.

Tuttavia, se il server DNS rifiuta le richieste di tipo A con un indirizzo IP nel campo della query, in contrapposizione alla risposta con "nome non trovato" (il caso più comune, sempre rilevato durante i test), allora Cisco bug ID CSCti20768 Si applica il criterio "Query DNS di tipo A per

l'indirizzo IP, deve essere PTR per evitare il timeout".

Le dimensioni della finestra TCP Delayed-ACK selezionano un gateway non corretto

Quando si usano versioni ASA precedenti alla versione 9.1(3), le clip sul client mostrano un ritardo persistente nell'handshake SSL. Si noti che il client invia il proprio ClientHello, quindi l'ASA invia il proprio ServerHello. Questo messaggio è in genere seguito da un messaggio di certificato (richiesta di certificato facoltativa) e da un messaggio ServerHelloDone. L'anomalia è duplice:

1. L'appliance ASA non invia immediatamente il messaggio del certificato dopo ServerHello. La dimensione della finestra del client è 64.860 byte, più del necessario per contenere l'intera risposta dell'appliance ASA.

2. Il client non invia immediatamente il pacchetto ServerHello, quindi l'ASA trasmette nuovamente il pacchetto dopo circa 120 ms, dopodiché il client riceve i dati. Quindi viene inviato il messaggio Certificato. È quasi come se il client aspettasse più dati.

Questo si verifica a causa dell'interazione tra TCP slow-start e TCP delayed-ACK. Nelle versioni precedenti alla 9.1(3), l'ASA usa una dimensione della finestra con avvio lento pari a 1, mentre il client Windows usa un valore di delay-ACK pari a 2. Ciò significa che l'ASA invia un solo pacchetto di dati finché non riceve un ACK, ma che il client non invia un ACK finché non riceve due pacchetti di dati. Dopo 120 ms, l'ASA scade e trasmette nuovamente il messaggio ServerHello, dopodiché il client riconferma i dati e la connessione continua. Questo comportamento è stato modificato dall'ID bug Cisco CSCug98113 in modo che l'ASA usi per impostazione predefinita una dimensione della finestra con avvio lento di 2 anziché di 1.

Questo può influire sul calcolo di OGS quando:

- Gateway diversi eseguono versioni ASA diverse.
- I client hanno dimensioni della finestra ritardata-ACK diverse.

In queste situazioni, il ritardo introdotto da delayed-ACK potrebbe essere sufficiente per spingere il client a selezionare l'appliance ASA errata. Se questo valore differisce tra il client e l'appliance ASA, potrebbero verificarsi dei problemi. In tali situazioni, per ovviare al problema è possibile modificare le dimensioni della finestra Conferme di avvenuta ricezione.

Windows

1. Avviare l'**Editor del Registro di sistema**.

2. Identificare il GUID dell'interfaccia su cui si desidera disabilitare la funzione ritardata-ACK. A tale scopo, passare alla a:
HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > WindowsNT > CurrentVersion > NetworkCard > (numero).
Esaminare ogni numero elencato in Schede di rete. Sulla destra, la Descrizione deve elencare l'Interfaccia (ad esempio, Intel(R) Wireless WiFi Link 5100AGN) e il NomeServizio deve elencare il GUID corrispondente.

3. Individuare la sottochiave del Registro di sistema seguente e fare clic su di essa:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\<GUID interfaccia>

4. Scegliere Nuovo dal menu Modifica, quindi **Valore DWORD**.

5. Denominare il nuovo valore **TcpAckFrequency** e assegnargli il valore **1**.

6. Uscire dall'Editor del Registro di sistema.

7. Riavviare Windows per rendere effettiva la modifica.

   Nota: Per rendere i parametri di regolazione TCP configurabili sull'appliance ASA, è stato archiviato l'ID bug Cisco CSCum19065.

Esempio di utente tipico

Il caso d'uso più comune si verifica quando un utente a casa esegue OGS la prima volta, registra le impostazioni DNS e i risultati del ping OGS nella cache (per impostazione predefinita, il timeout è di 14 giorni). Quando l'utente torna a casa la sera successiva, OGS rileva le stesse impostazioni DNS, le trova nella cache e ignora il test ping di OGS. In seguito, quando l'utente si reca in un hotel o in un ristorante che offre un servizio Internet, il servizio OGS rileva diverse impostazioni DNS, esegue i test ping di OGS, seleziona il gateway migliore e registra i risultati nella cache.

L'elaborazione è identica quando riprende da uno stato di sospensione o ibernazione, se le impostazioni di ripristino di OGS e AnyConnect lo consentono.

Risoluzione dei problemi di OGS

Passaggio 1. Cancellare la cache OGS per forzare una rivalutazione

Per cancellare la cache OGS e rivalutare l'RTT dei gateway disponibili, è sufficiente eliminare il file delle preferenze AnyConnect globali dal PC. La posizione del file varia in base al sistema operativo:

- Windows Vista e 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..
```

Passaggio 2. Acquisire le sonde del server durante il tentativo di connessione

1. Avviare Wireshark sulla macchina di prova.

2. Avvia un tentativo di connessione su AnyConnect.

3. Interrompere l'acquisizione di Wireshark al termine della connessione. **Suggerimento**: Poiché l'acquisizione viene usata solo per testare il protocollo OGS, è meglio interromperla non appena AnyConnect seleziona un gateway. È consigliabile non passare attraverso un tentativo di connessione completo, perché ciò può cloud l'acquisizione del pacchetto.

Passaggio 3. Verificare il gateway selezionato da OGS

Per verificare il motivo per cui GOS ha selezionato un particolare gateway, procedere come segue:

1. Avviare una nuova connessione.

2. Eseguire AnyConnect DART:
   Avviare **AnyConnect** e fare clic su **Avanzate**.Fare clic su **Diagnostica**.Fare clic su **Next** (Avanti).Fare clic su **Next** (Avanti).
3. Esaminare i risultati DART trovati nel file **DartBundle_XXXX_XXXX.zip** appena creato sul desktop.
   Passare a **Cisco AnyConnect Secure Mobility Client > AnyConnect.txt**.

   Si noti l'ora di avvio delle richieste OGS per un determinato server dal seguente registro 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

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

   Di solito dovrebbero essere all'incirca nello stesso periodo di tempo, ma nel caso in cui le clip siano grandi, l'indicatore orario aiuta a individuare i pacchetti che sono le sonde HTTP e i tentativi di connessione effettivi.

   Una volta che AnyConnect invia tre richieste al server, questo messaggio viene generato con i risultati di ciascuna delle richieste:

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

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 )

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

È importante prestare attenzione a questi tre valori, in quanto devono corrispondere ai risultati dell'acquisizione.

Cercare il messaggio che contiene "**** Risultati selezione OGS***" per visualizzare l'RTT valutato e verificare se il tentativo di connessione più recente è il risultato di un RTT memorizzato nella cache o di un nuovo calcolo.

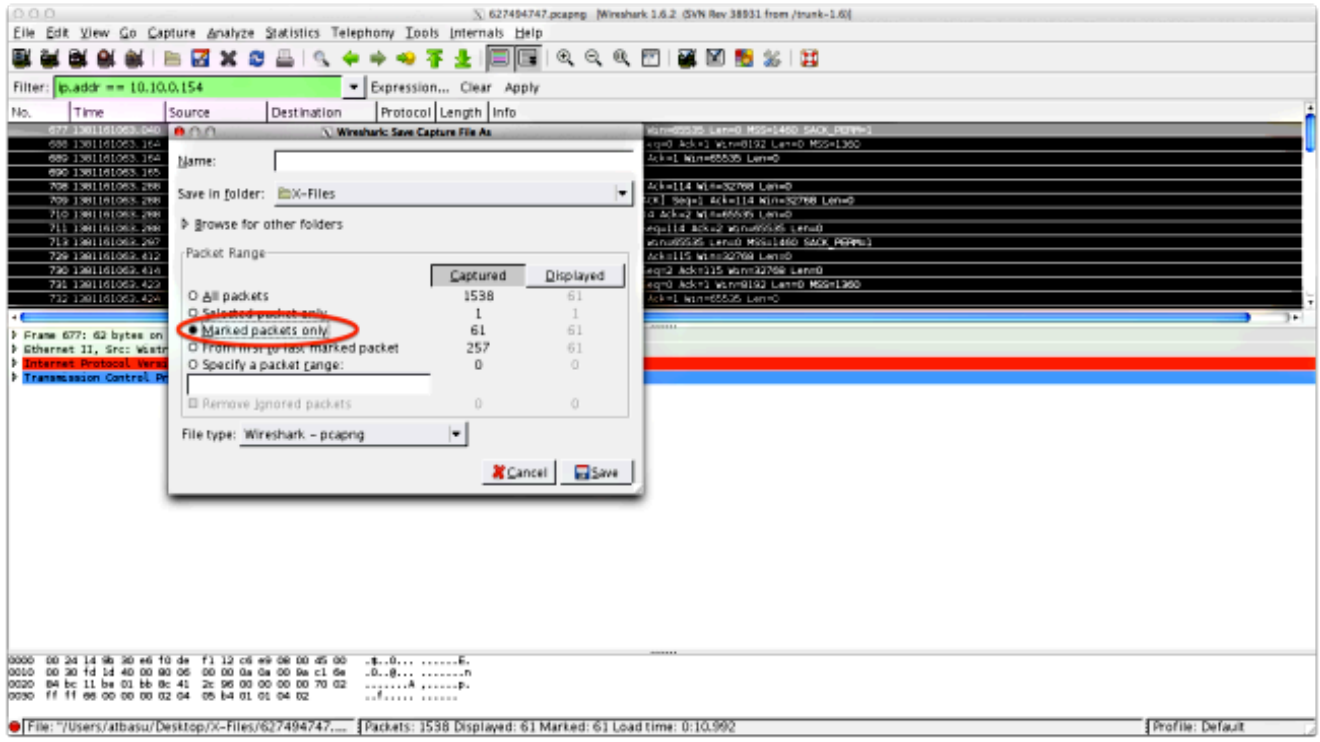
Di seguito è riportato un esempio:

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

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.

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

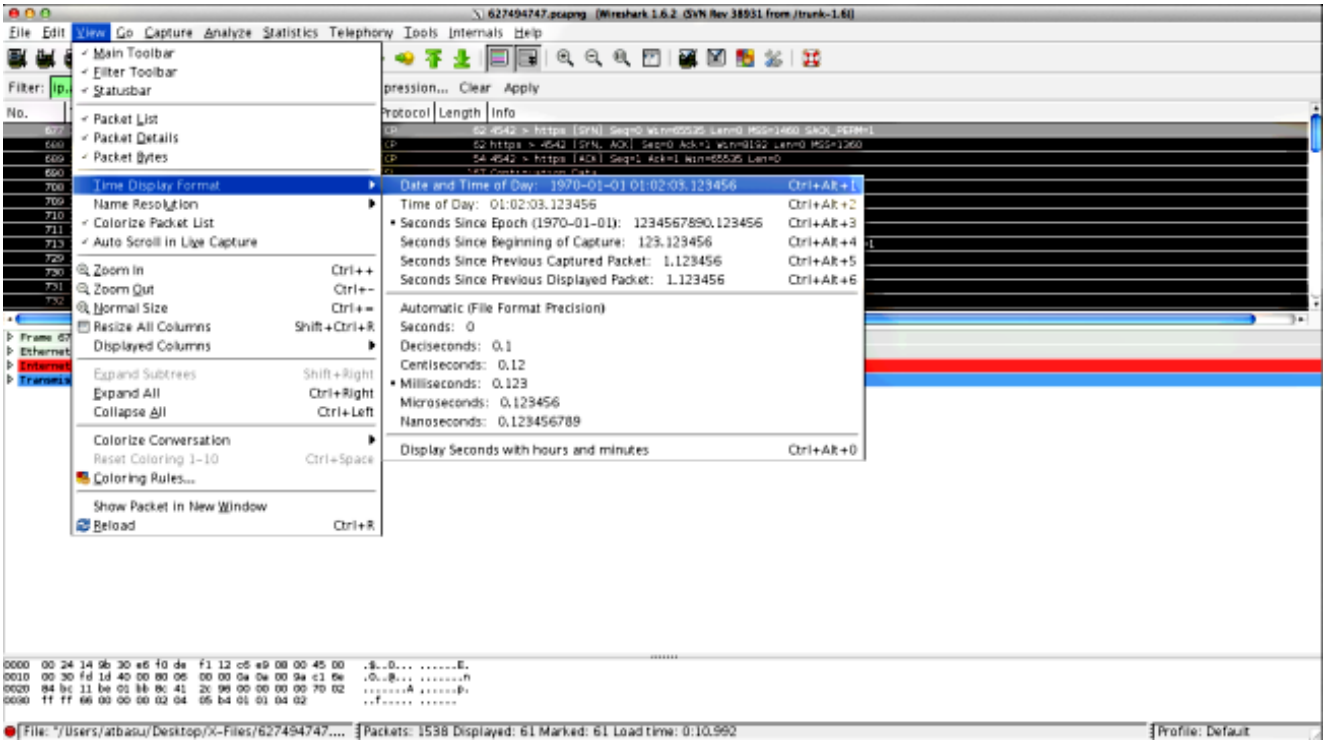
Passaggio 4. Convalida dei calcoli OGS eseguiti da AnyConnect

Controllare l'acquisizione delle sonde TCP/SSL usate per calcolare il valore RTT. Verifica il tempo impiegato dalla richiesta HTTPS su una singola connessione TCP. Ogni richiesta di sonda deve utilizzare una connessione TCP diversa. A tale scopo, aprire l'acquisizione in Wireshark e ripetere i seguenti passaggi per ogni server:

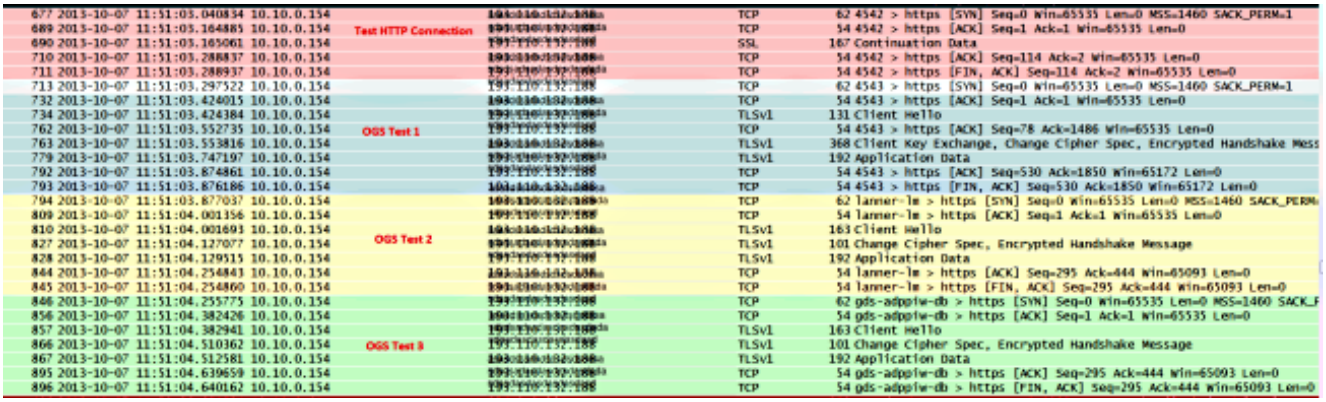
1. Usare il filtro **ip.addr** per isolare i pacchetti inviati a ciascuno dei server nella relativa acquisizione. A tale scopo, passare a **Modifica** e selezionare **Contrassegna tutti i pacchetti visualizzati**. Passare quindi a **File > Salva con nome**, selezionare l'opzione **Solo pacchetti contrassegnati** e fare clic su **Salva**:



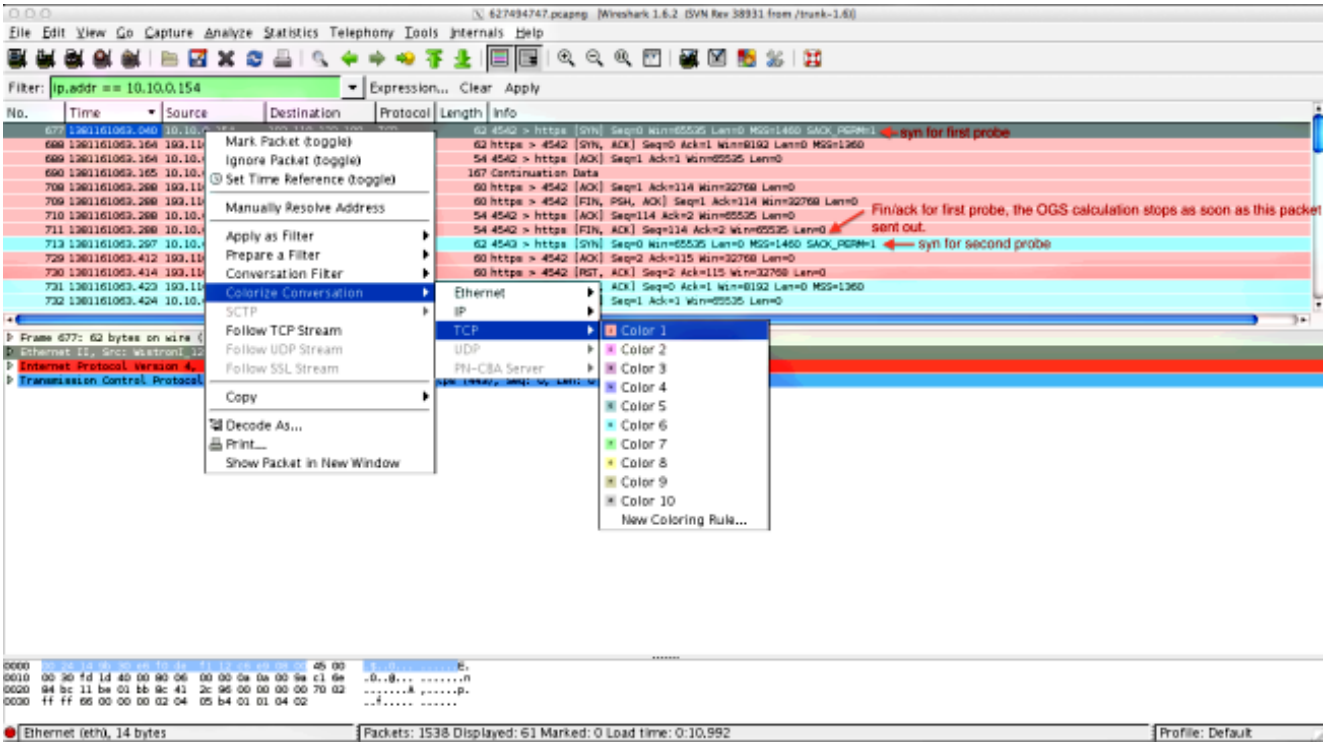
2. In questa nuova acquisizione, passare a **Visualizza > Formato visualizzazione ora > Data e ora del giorno**:



3. Identificare il primo pacchetto SYN HTTP in questa acquisizione inviato quando è stata inviata la sonda OGS in base ai log DART identificati nel passo 3.3.2. È importante ricordare che, per il primo server, la prima richiesta HTTP non è una sonda server. È facile confondere la prima richiesta di una sonda server e quindi ottenere valori completamente diversi da quelli riportati da OGS. Il problema è evidenziato qui:

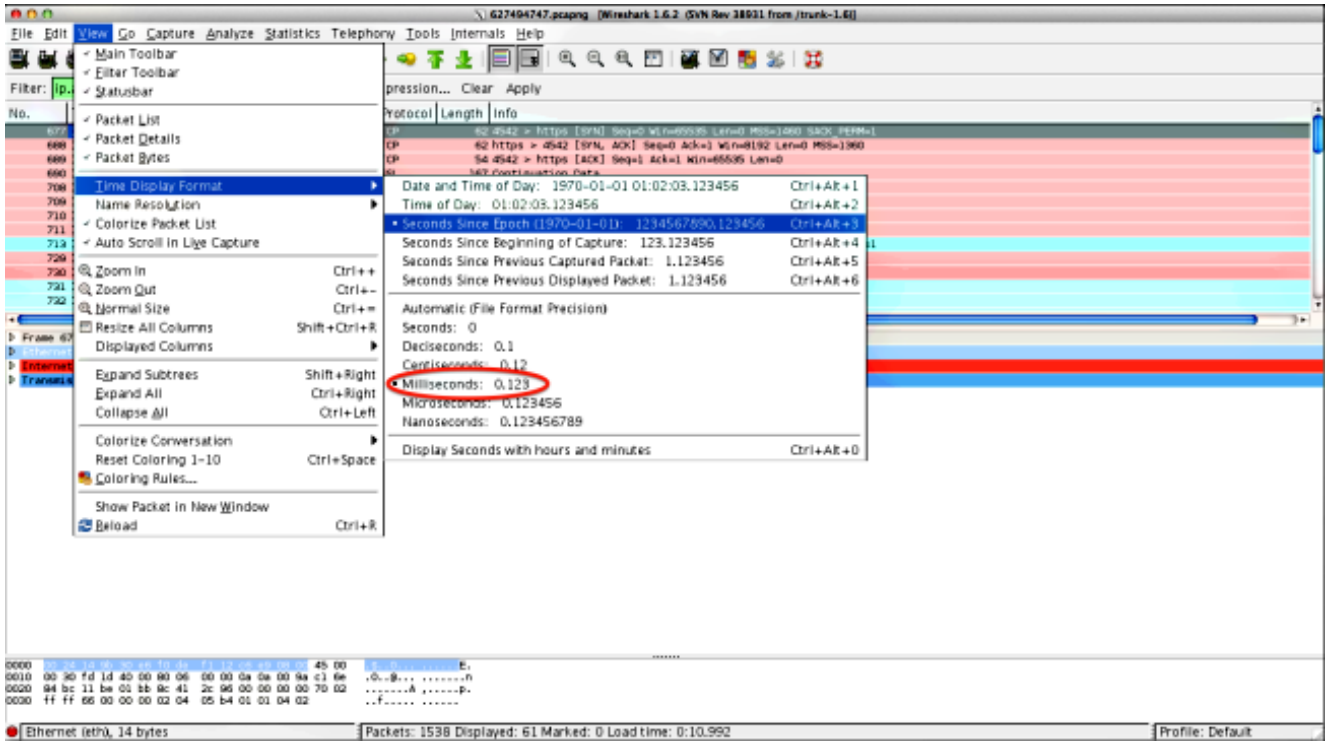


4. Per identificare più facilmente ciascuna sonda, fare clic con il pulsante destro del mouse sulla **SYN HTTP** della prima sonda, quindi selezionare **Colora conversazione** (Colora conversazione), come mostrato di seguito:



Ripetere questa procedura per i SYN su tutte le sonde. Come mostrato nell'immagine precedente, le prime due sonde sono rappresentate in colori diversi. Il vantaggio di colorizzare le conversazioni TCP è di individuare facilmente le ritrasmissioni o altre stranezze per sonda.

5. Per modificare la visualizzazione del tempo, selezionare **Visualizza > Formato visualizzazione tempo > Secondi dall'epoca**:



Selezionare **Millisecondi**, poiché questo è il livello di precisione utilizzato da OGS.

6. Calcolare la differenza di tempo tra il valore SYN HTTP e il valore FIN/ACK, come mostrato nel diagramma del passo 4. Ripetere questo processo per ciascuna delle tre sonde e confrontare i valori con quelli mostrati nei log DART del passo 3.3.3.

Analisi

Se dopo l'analisi delle acquisizioni i valori RTT determinati vengono calcolati e confrontati con i valori visualizzati nei log DART e viene trovata una corrispondenza per tutti gli elementi, ma sembra che sia stato selezionato il gateway errato, allora ciò è dovuto a uno dei due problemi seguenti:

- Si è verificato un problema nell'headend. In questo caso, potrebbero esserci troppe ritrasmissioni da un headend particolare, o altre stranezze simili rilevate nelle sonde. è necessaria un'analisi più approfondita dello scambio.

- Problema con il provider di servizi Internet (ISP). In questo caso, è possibile che si verifichino frammentazioni o ritardi considerevoli per un headend specifico.

Domande e risposte

D: Il sistema OGS funziona con il bilanciamento del carico?

R: Sì. OGS è a conoscenza solo del nome del master del cluster e lo utilizza per valutare l'headend più vicino.

D: Il software OGS funziona con le impostazioni proxy definite nel browser?

A: OGS non supporta i file proxy automatico o i file PAC (proxy Auto Config), ma supporta un

server proxy hardcoded. Di conseguenza, l'operazione OGS non viene eseguita. Il messaggio di log pertinente è: "**OGS non verrà eseguito perché è configurato il rilevamento automatico proxy**".