# Correggi le interruzioni del flusso di traffico causate dalle riconnessioni AnyConnect

## Sommario



## Introduzione

In questo documento viene descritto cosa succede quando un client AnyConnect si riconnette all'appliance ASA (Adaptive Security Appliance) in un minuto esatto.

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

### Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

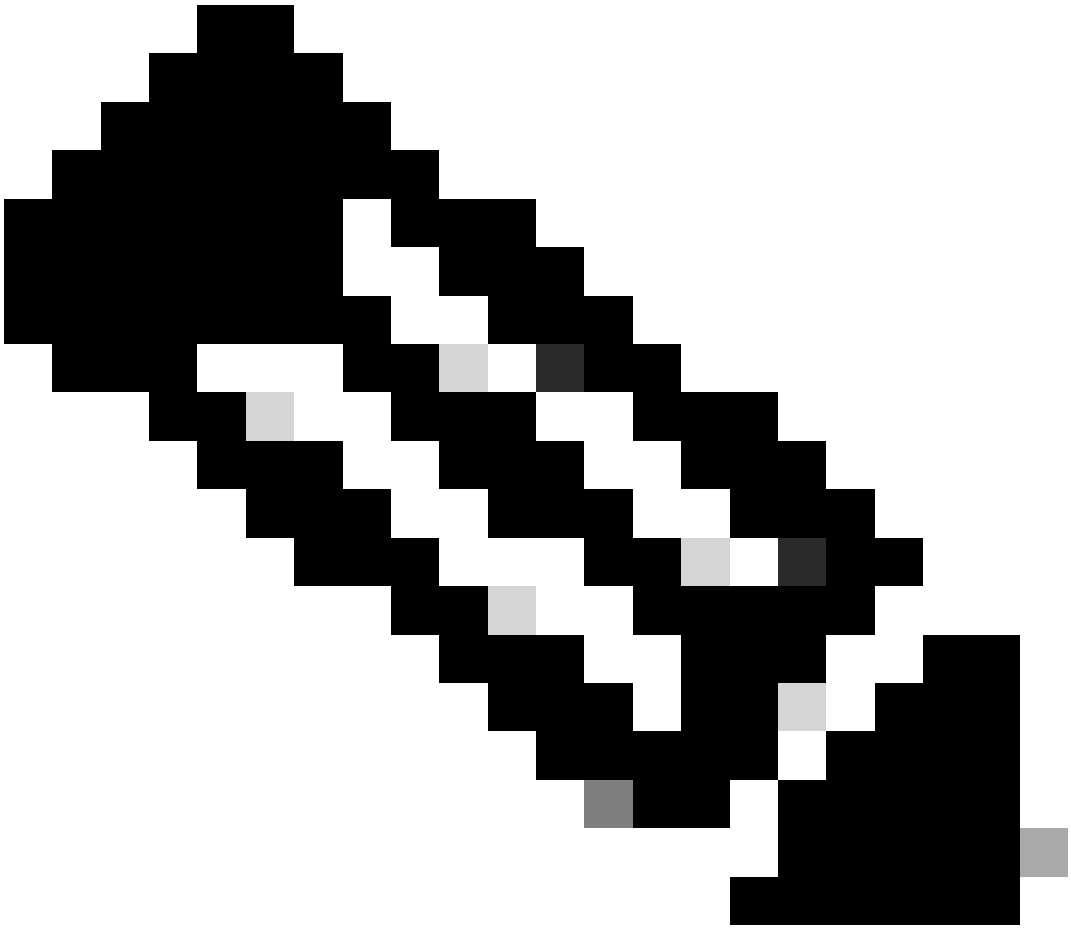
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

### Prodotti correlati

Questi prodotti sono stati interessati dal problema:

- ASA release 9.17
- AnyConnect Client release 4.10

## Premesse

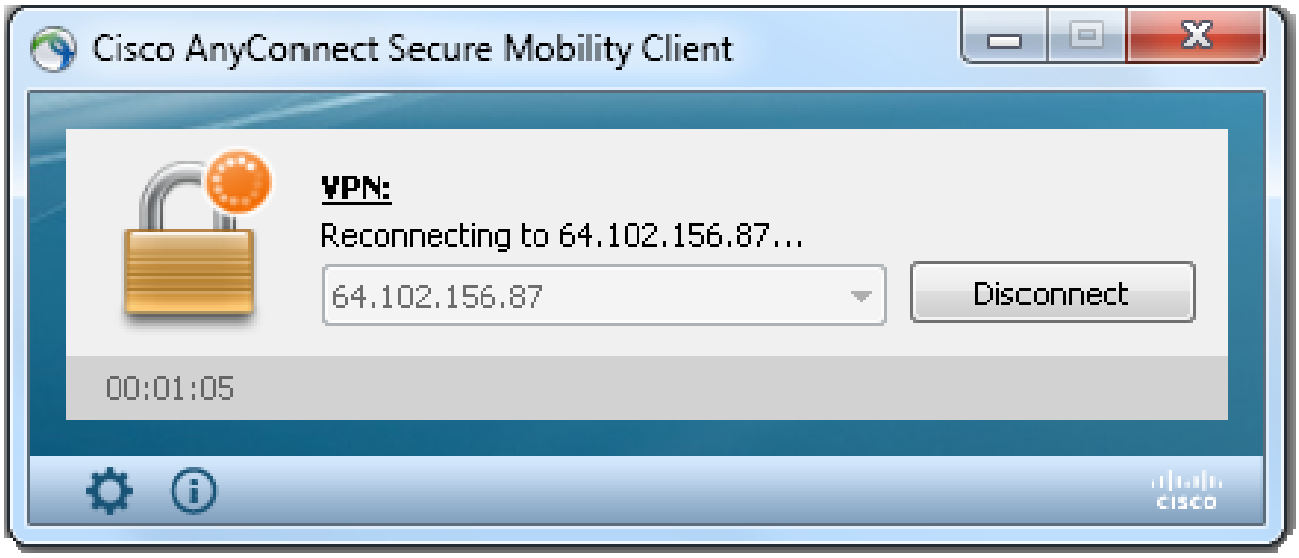


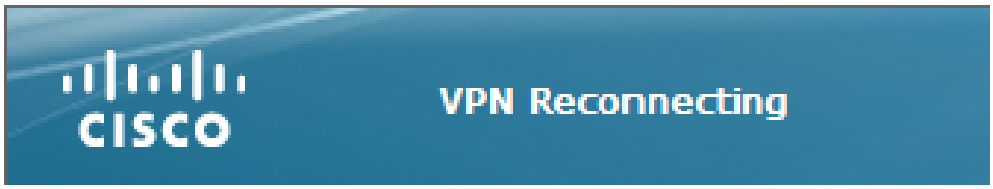
> Nota: AnyConnect è stato rinominato in Cisco Secure Client. Non è stato cambiato nulla, è cambiato solo il nome e il processo di installazione è lo stesso.

Se il client AnyConnect si riconnette all'appliance ASA (Adaptive Security Appliance) esattamente in un minuto, gli utenti non possono ricevere traffico sul tunnel Transport Layer Security (TLS) finché AnyConnect non si riconnette. Ciò dipende da alcuni altri fattori discussi nel presente documento.

## Sintomi

Nell'esempio, viene mostrato come il client AnyConnect si riconnette all'appliance ASA.




Questo syslog viene visualizzato sull'appliance ASA:

```
%ASA-6-722036: Group <ac_users_group> User <vpn> IP <10.1.75.111>
Transmitting large packet 1418 (threshold 1347).
```

# Descrizione del problema

I seguenti registri diagnostici e Reporting strumenti (DART) presentano il seguente problema:

<#root>

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

Date : 11/16/2022
Time : 01:28:50
Type : Warning
Source : acvpnagent

Description : Reconfigure reason code 16:

**New MTU configuration.**

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

Date        : 11/16/2022
Time        : 01:28:50
Type        : Information
```

```
Source      : acvpnagent

Description : The entire VPN connection is being reconfigured.

****************************************

Date        : 11/16/2022
Time        : 01:28:51
Type        : Information
Source      : acvpnui

Description : Message type information sent to the user:
Reconnecting to 10.1.1.2...

****************************************

Date        : 11/16/2022
Time        : 01:28:51
Type        : Warning
Source      : acvpnagent

Description : A new MTU needs to be applied to the VPN network interface.
Disabling and re-enabling the Virtual Adapter. Applications utilizing the
private network may need to be restarted.

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

Cause

La causa di questo problema è la mancata compilazione di un tunnel DTLS (Datagram Transport Layer Security). Ciò può essere dovuto a due motivi:

- DTLS è bloccato in un punto del percorso.
- Uso di una porta DTLS non predefinita.

DTLS bloccato in un punto qualsiasi del percorso

A partire dalla versione ASA 9.x e dalla versione AnyConnect 4.x, è stata introdotta un'ottimizzazione sotto forma di MTU (Maximum Transition Units) distinte negoziate per TLS/DTLS tra il client/ASA. In precedenza, il client ha ricavato una stima approssimativa dell'MTU che copriva sia TLS che DTLS ed era ovviamente meno che ottimale. A questo punto, l'ASA calcola il sovraccarico di incapsulamento per entrambi i protocolli TLS/DTLS e deriva i valori MTU di conseguenza.

Finché il DTLS è abilitato, il client applica l'MTU DTLS (in questo caso 1418) sulla scheda VPN (abilitata prima che il tunnel DTLS sia stabilito e necessaria per l'applicazione di route/filtri), per garantire prestazioni ottimali. Se non è possibile stabilire il tunnel DTLS o viene scartato a un certo punto, il client esegue il failover su TLS e regola l'MTU sulla scheda virtuale (VA) sul valore MTU TLS (è necessaria una riconnessione a livello di sessione).

Risoluzione

Per eliminare questa transizione visibile di **DTLS > TLS**, l'amministratore può configurare un gruppo di tunnel separato per l'accesso TLS solo per gli utenti che hanno problemi a stabilire il tunnel DTLS (ad esempio a causa delle restrizioni del firewall).

- L'opzione migliore è impostare il valore MTU di AnyConnect su un valore inferiore all'MTU del TLS, che viene quindi negoziato.

```
group-policy ac_users_group attributes
 webvpn
  anyconnect mtu 1300
```

In questo modo, i valori TLS e DTLS MTU sono uguali. Le riconnessioni non vengono rilevate.

- La seconda opzione prevede la frammentazione.

```
group-policy ac_users_group attributes
 webvpn
  anyconnect ssl df-bit-ignore enable
```

Con la frammentazione, i pacchetti di grandi dimensioni (le cui dimensioni superano il valore MTU) possono essere frammentati e inviati tramite il tunnel TLS.

- La terza opzione consiste nell'impostare il valore MSS (Maximum Segment Size) su 1460, come mostrato di seguito:

```
sysopt conn tcpmss 1460
```

In questo caso, l'MTU TLS può essere 1427 (RC4/SHA1), ossia una dimensione superiore all'MTU DTLS 1418 (AES/SHA1/LZS). In questo modo si risolve il problema con il TCP tra l'ASA e il client AnyConnect (grazie al valore MSS), ma il traffico UDP grande tra l'ASA e il client AnyConnect può esserne danneggiato in quanto può essere scartato dal client AnyConnect a causa della MTU 1418 del client AnyConnect più bassa. Se si modifica il protocollo tcpmss della connessione sysost, la configurazione può influire su altre

funzionalità, ad esempio i tunnel VPN IPSec da LAN a LAN (L2L).

Riconnetti flusso di lavoro

Si supponga che queste cifrature siano configurate:

ssl cipher tlsv1.2 custom AES256-SHA256 AES128-SHA256 DHE-RSA-AES256-SHA256

Questa sequenza di eventi si verifica in questo caso:

- AnyConnect stabilisce un tunnel padre e un tunnel di dati TLS con AES256-SHA256 come crittografia SSL.
- DTLS è bloccato nel percorso e non è possibile stabilire un tunnel DTLS.
- L'appliance ASA comunica i parametri a AnyConnect, che include i valori TLS e DTLS MTU, due valori distinti.
- Per impostazione predefinita, l'MTU DTLS è 1418.
- L'MTU TLS viene calcolata a partire dal valore tcpmss della costante di sistema (il valore predefinito è 1380). Di seguito viene riportata la modalità di derivazione dell'MTU TLS (come mostrato nell'output del comando debug webvpn anyconnect):

1380 - 5 (TLS header) - 8 (CSTP) - 0 (padding) - 20 (HASH) = 1347

- AnyConnect attiva la scheda VPN e le assegna l'MTU DTLS in anticipo, in modo che possa connettersi tramite DTLS.
- Il client AnyConnect è ora connesso e l'utente visita un sito Web specifico.
- Il browser invia TCP SYN e imposta MSS = 1418-40 = 1378.
- Il server HTTP all'interno dell'appliance ASA invia pacchetti di dimensioni 1418.
- L'appliance ASA non può inserirli nel tunnel e non può frammentarli perché il bit "non frammentare" (DF, Do not Fragment) è impostato.
- L'ASA stampa e scarta i pacchetti con il motivo della perdita mp-svc-no-fragment-ASP.

%ASA-6-722036: Group <ac_users_group> User <vpn> IP <10.1.75.111>

Transmitting large packet 1418 (threshold 1347)

- Allo stesso tempo, l'ASA invia la destinazione ICMP "destinazione irraggiungibile" e la frammentazione richiesta al mittente:

```
%ASA-6-602101: PMTU-D packet 1418 bytes greater than effective mtu 1347,
dest_addr=10.10.10.1, src_addr=10.48.66.200, prot=TCP
```

- Se il protocollo ICMP (Internet Control Message Protocol) è consentito, il mittente ritrasmette i pacchetti ignorati e tutto inizia a funzionare. Se l'ICMP è bloccato, il traffico sull'appliance ASA è bloccato.

- Dopo diversi ritrasmissioni, capisce che il tunnel DTLS non può essere stabilito e deve riassegnare un nuovo valore MTU alla scheda VPN.

- Lo scopo della riconnessione è assegnare una nuova MTU.

Per ulteriori informazioni sul comportamento e i timer della riconnessione, vedere le domande frequenti su AnyConnect: tunnel, comportamento di riconnessione e timer di inattività

Informazioni correlate

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).