修復AnyConnect重新連線導致的流量中斷

目錄

簡介

本文檔介紹當AnyConnect客戶端在一分鐘內重新連線到自適應安全裝置(ASA)時會發生什麼情況。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

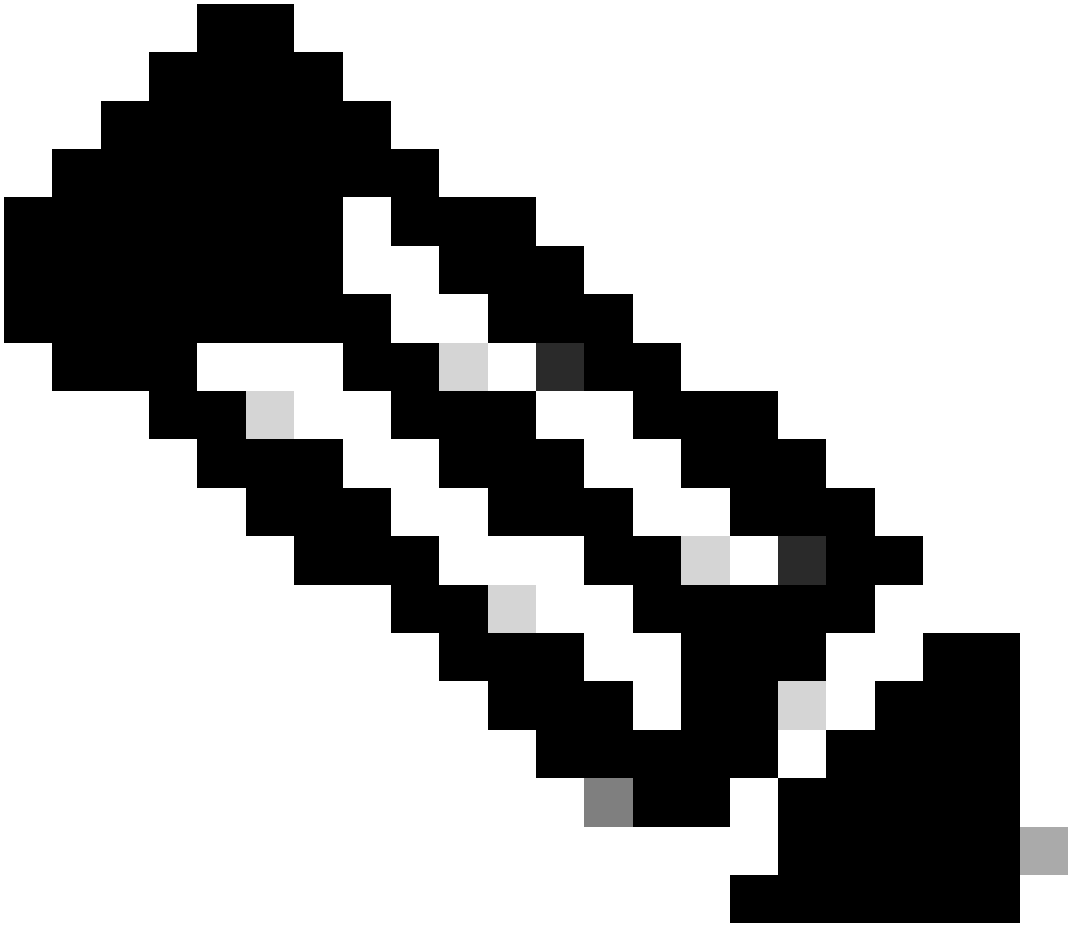
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

相關產品

以下產品受此問題影響：

- ASA版本9.17
- AnyConnect客戶端版本4.10

背景資訊

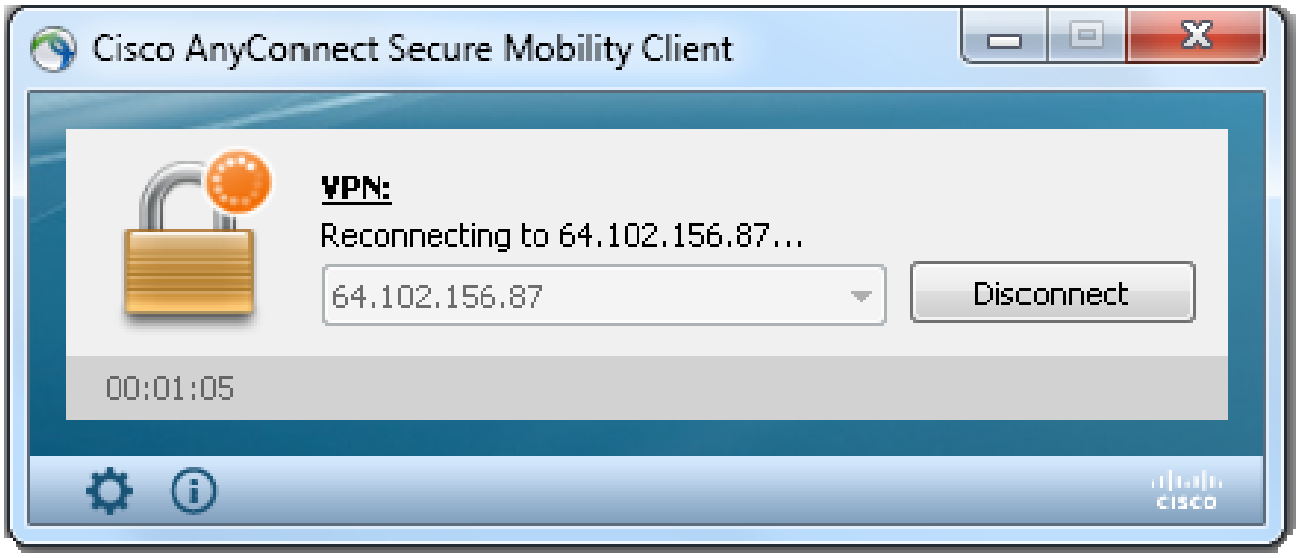


注意：AnyConnect已重新命名為Cisco Secure Client。沒有更改其他內容，僅更改名稱，並且安裝程式相同。

如果AnyConnect客戶端在一分鐘內重新連線到自適應安全裝置(ASA)，則在AnyConnect重新連線之前，使用者無法通過傳輸層安全(TLS)隧道接收流量。這取決於本文檔中討論的幾個其他因素。

症狀

在本示例中，AnyConnect客戶端在重新連線到ASA時顯示。



在ASA上看到此系統日誌：

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

問題描述

以下診斷和Reporting工具(DART)日誌顯示在此問題中：

<#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.

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

原因

此問題的原因是無法建立資料包傳輸層安全性(DTLS)通道。這可能有兩個原因：

- DTLS在路徑中的某處被阻止。
- 使用非預設DTLS埠。

DTLS在路徑中的某處被阻止

從ASA版本9.x和AnyConnect版本4.x開始，以客戶端/ASA之間為TLS/DTLS協商的不同最大過渡單元(MTU)的形式引入最佳化。以前，客戶端會得出一個涵蓋TLS/DTLS的粗略估計MTU，並且明顯低於最優估計MTU。現在，ASA會計算兩個TLS/DTLS的封裝開銷並相應地派生MTU值。

只要啟用DTLS，客戶端就會在VPN介面卡上應用DTLS MTU（在本例中為1418）（該介面卡在建立DTLS隧道之前啟用，並且是實施路由/過濾器所必需的），以確保最佳效能。如果DTLS通道無法建立，或是在某個時候遭到捨棄，使用者端會容錯移轉至TLS，並將虛擬介面卡(VA)上的MTU調整為TLS MTU值（這需要重新連線階段作業）。

解析

為了消除DTLS > TLS的這一可見轉換，管理員可以為建立DTLS隧道時遇到困難（例如由於防火牆

限制）的使用者配置一個單獨的TLS專用訪問隧道組。

1. 最佳選項是將AnyConnect MTU值設定為低於TLS MTU，然後進行協商。

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

這使TLS和DTLS MTU值相等。在這種情況下，看不到重新連線。

2. 第二個選項是允許分段。

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

使用分段時，大型資料包（其大小超過MTU值）可以分段並透過TLS隧道傳送。

3. 第三個選項是將「最大區段大小(MSS)」設定為1460，如下所示：

```
sysopt conn tcpmss 1460
```

在這種情況下，TLS MTU可以是1427 (RC4/SHA1)，大於DTLS MTU 1418 (AES/SHA1/LZS)。這解決了從ASA到AnyConnect客戶端的TCP問題（多虧了MSS），但從ASA到AnyConnect客戶端的大量UDP流量可能會遇到此問題，因為AnyConnect客戶端MTU 1418較低，可能會被AnyConnect客戶端丟棄。如果sysopt conn tcpmss被修改，可能會影響其他功能，例如LAN到LAN (L2L) IPSec VPN隧道。

重新連線工作流程

假設已配置以下密碼：

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

這種情況下會發生以下一系列事件：

- AnyConnect使用AES256-SHA256作為SSL加密來建立父隧道和TLS資料隧道。

- 路徑中阻止了DTLS，因此無法建立DTLS隧道。
- ASA向AnyConnect通告引數，其中包括TLS和DTLS MTU值，這兩個值是兩個獨立的值。
- 預設情況下，DTLS MTU為1418。
- TLS MTU是根據sysopt conn tcpmss值計算的（預設值為1380）。以下是TLS MTU的派生（如debug webvpn anyconnect輸出所示）：

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

- AnyConnect會啟動VPN介面卡並向其分配DTLS MTU，以預期可以透過DTLS進行連線。
- AnyConnect客戶端現已連線，使用者將訪問特定網站。
- 瀏覽器傳送TCP SYN，並在其中設定MSS = 1418-40 = 1378。
- ASA內部的HTTP伺服器傳送大小為1418的資料包。
- ASA不能將它們放入隧道中，也不能將其分段，因為它們已設定不分段(DF)位。
- ASA列印和丟棄資料包時顯示mp-svc-no-fragment-ASP丟棄原因。

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

- 同時，ASA會向傳送方傳送ICMP Destination Unreachable， Fragment Needed：

```
%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
```

- 如果允許網際網路控制訊息通訊協定(ICMP)，則傳送者會重新傳輸捨棄的封包，所有專案都會開始運作。如果ICMP被阻止，則流量在ASA上被黑洞。
- 在多次重新傳輸之後，它瞭解無法建立DTLS隧道，需要重新為VPN介面卡分配新的MTU值。
- 重新連線的目的是分配新的MTU。

有關重新連線行為和計時器的詳細資訊，請參閱AnyConnect常見問題解答：隧道、重新連線行為和非活動計時器

相關資訊

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。