回答AnyConnect常見問題 — 隧道、DPD和非活動狀態計時器

目錄

簡介

本檔案介紹Cisco AnyConnect安全行動化使用者端通道、重新連線行為和失效對等體檢測(DPD)以及非活動計時器。

背景資訊

通道型別

有兩種方法用於連線AnyConnect會話：

- 通過門戶（無客戶端）
- 通過獨立應用程式

根據連線方式，您可以在思科自適應安全裝置(ASA)上建立三個不同的隧道（會話），每個隧道都有特定的用途：

1. 無客戶端或父隧道：這是為了設定會話令牌而在因網路連線問題或休眠而需要重新連線時建立的主要會話。根據連線機制，ASA將會話列為無客戶端（通過門戶進行Web啟動）或父級（獨立AnyConnect）。

   註:AnyConnect-Parent表示客戶端未主動連線時的會話。實際上，它的工作方式與cookie類似，因為它是ASA上的資料庫條目，該條目對映到來自特定客戶端的連線。如果客戶端休眠/休眠，則隧道(IPsec/Internet金鑰交換(IKE)/傳輸層安全(TLS)/資料包傳輸層安全(DTLS)協定)會關閉，但父交換機將一直保留，直到空閒計時器或最大連線時間生效。這樣使用者無需重新身份驗證即可重新連線。

2. 安全套接字層(SSL) — 隧道：首先建立SSL連線，資料通過此連線傳遞，同時它嘗試建立DTLS連線。建立DTLS連線後，客戶端將通過DTLS連線而不是通過SSL連線傳送資料包。另一方面，控制資料包始終通過SSL連線。

3. DTLS隧道：當DTLS隧道完全建立時，所有資料都將移動到DTLS隧道，而SSL隧道僅用於偶爾的控制通道流量。如果使用者資料包協定(UDP)出現問題，則DTLS隧道關閉，所有資料再次通過SSL隧道。

ASA輸出示例

以下是兩種連線方法的輸出示例。

通過Web啟動連線的AnyConnect:

```
ASA5520-C(config)# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1435
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Protocol : Clientless SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : Clientless: (1)RC4 SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : Clientless: (1)SHA1 SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 335765 Bytes Rx : 31508
Pkts Tx : 214 Pkts Rx : 18
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 22:13:37 UTC Fri Nov 30 2012
```

```
Duration : 0h:00m:34s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

Clientless Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

Clientless:
Tunnel ID : 1435.1
Public IP : 172.16.250.17
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : Web Browser
Client Ver : Mozilla/5.0 (Windows NT 5.1; rv:16.0) Gecko/20100101 Firefox/16.0
Bytes Tx : 329671 Bytes Rx : 31508

SSL-Tunnel:
Tunnel ID : 1435.2
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 1241
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.01065
Bytes Tx : 6094 Bytes Rx : 0
Pkts Tx : 4 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 1435.3
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 Compression : LZS
UDP Src Port : 1250 UDP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : DTLS VPN Client
Client Ver : Mozilla/5.0 (Windows NT 5.1; rv:16.0) Gecko/20100101 Firefox/16.0
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

通過獨立應用程式連線的AnyConnect:

```
ASA5520-C(config)# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1436
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 12244 Bytes Rx : 777
Pkts Tx : 8 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
```

```
Login Time : 22:15:24 UTC Fri Nov 30 2012
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 1436.1
Public IP : 172.16.250.17
Encryption : none Hashing : none
TCP Src Port : 1269 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : AnyConnect
Client Ver : 3.1.01065
Bytes Tx : 6122 Bytes Rx : 777
Pkts Tx : 4 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 1436.2
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 1272
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.01065
Bytes Tx : 6122 Bytes Rx : 0
Pkts Tx : 4 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 1436.3
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 Compression : LZS
UDP Src Port : 1280 UDP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : DTLS VPN Client
Client Ver : 3.1.01065
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

DPD和非活動計時器

會話何時被視為非活動會話？

只有當會話中不再存在SSL隧道時，該會話才被視為非活動狀態（並且計時器開始增加）。因此，每個作業階段都使用SSL通道捨棄時間進行時間戳。

```
ASA5520-C# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed
```

```
Username : walter Index : 1336
Public IP : 172.16.250.17
Protocol : AnyConnect-Parent <- Here just the AnyConnect-Parent is active
but not SSL-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none
Hashing : AnyConnect-Parent: (1)none
Bytes Tx : 12917 Bytes Rx : 1187
Pkts Tx : 14 Pkts Rx : 7
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 17:42:56 UTC Sat Nov 17 2012
Duration : 0h:09m:14s
Inactivity : 0h:01m:06s <- So the session is considered Inactive
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

ASA何時丟棄SSL隧道？

有兩種方法可以斷開SSL隧道：

1. **DPD** — 客戶端使用DPD來檢測AnyConnect客戶端和ASA頭端之間的通訊故障。DPD也用於清除ASA上的資源。這可確保如果端點對DPD ping無響應，則頭端不會在資料庫中保持連線。如果ASA向終端傳送DPD並響應，則不執行任何操作。如果端點沒有響應，在最大重傳次數之後（這取決於是否使用IKEv1或IKEv2），ASA將斷開會話資料庫中的隧道，並將會話移至「等待恢復」模式。這意味著頭端的DPD已經啟動，並且頭端不再與客戶端通訊。在這種情況下，ASA保持父隧道處於開啟狀態，以便允許使用者漫遊網路、進入睡眠狀態並恢復會話。這些作業階段對主動連線的作業階段計數，會在以下情況下清除：
   使用者空閒超時客戶端恢復原始會話並正確註銷
   要配置DPD，請使用 **anyconnect dpd-interval** 命令，在group-policy設定中的WebVPN屬性下執行。預設情況下，ASA（網關）和客戶端的DPD均處於啟用狀態並設定為30秒。

   注意：請注意Cisco錯誤ID CSCts66926 - DPD在失去客戶端連線後無法終止DTLS隧道。

2. **Idle-Timeout** - SSL隧道斷開連線的第二種方式是此隧道的空閒超時過期時。但是，請記住，必須空閒的不僅是SSL隧道，還有DTLS隧道。除非DTLS會話超時，否則SSL隧道將保留在資料庫中。

如果已啟用DPD，為什麼需要啟用Keepalive?

如前所述，DPD不會終止AnyConnect會話本身。它只是終止該會話內的隧道，以便客戶端可以重新建立隧道。如果客戶端無法重新建立隧道，會話將一直保持到ASA上的空閒計時器超時。由於預設情況下啟用DPD，客戶端經常會因為使用網路地址轉換(NAT)、防火牆和代理裝置在一個方向上關閉流而斷開連線。以較低的時間間隔（例如20秒）啟用keepalive有助於防止這種情況。

Keepalive在特定group-policy的WebVPN屬性下啟用 **anyconnect ssl keepalive** 指令。預設情況下，計時器設定為20秒。

重新連線時的AnyConnect客戶端行為

如果連線中斷，AnyConnect會嘗試重新連線。這是不可自動配置的。只要ASA上的VPN會話仍然有效，並且AnyConnect可以重新建立物理連線，VPN會話就會恢復。

重新連線功能會一直持續，直到會話超時或斷開連線超時（實際上是空閒超時）過期（如果沒有配置超時，則為30分鐘）。一旦這些會話過期，客戶端便無法繼續，因為ASA上已經丟棄了VPN會話。只要客戶端認為ASA仍具有VPN會話，它就會繼續。

無論網路介面如何變更，AnyConnect都會重新連線。無論網路介面卡(NIC)的IP位址是否變更，也不管連線是否從一個NIC交換到另一個NIC（無線交換到有線交換）。

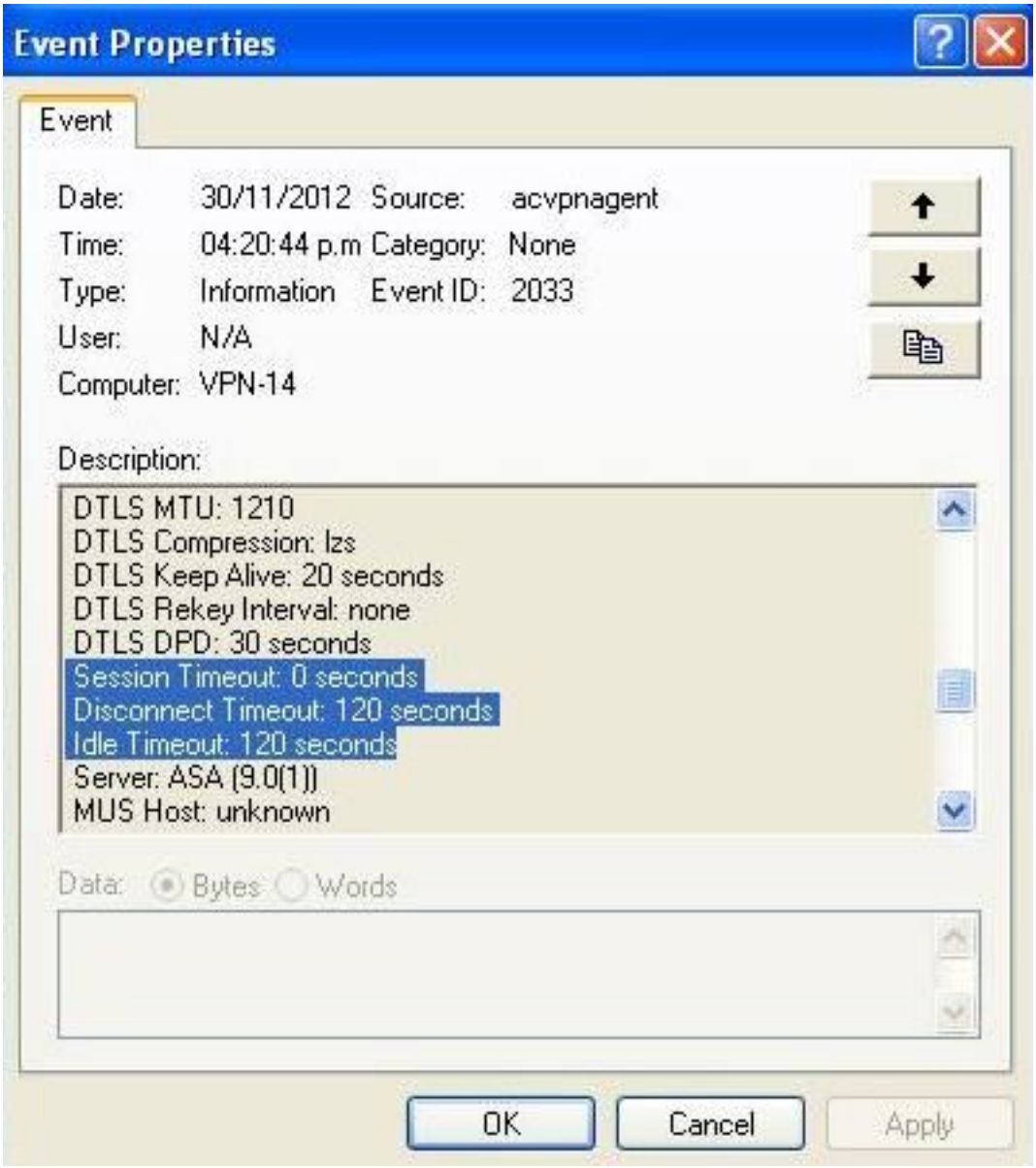
考慮AnyConnect的重新連線過程時，必須記住三個級別的會話。此外，這些會話中每個會話的重新連線行為是松耦合的，因為它們中的任何會話都可以重新建立，而無需依賴於上一層的會話元素：

1. TCP或UDP重新連線[OSI第3層]
2. TLS、DTLS或IPSec(IKE+ESP)[OSI第4層] — 不支援TLS恢復。
3. VPN [OSI第7層] - VPN會話令牌用作身份驗證令牌，以便在發生中斷時通過安全通道重新建立VPN會話。 這是一種專有機制，在概念上與Kerberos令牌或客戶端證書用於身份驗證的方式非常相似。 令牌是唯一的，由頭端加密生成，包含會話ID加上加密生成的隨機負載。在建立到頭端的安全通道之後，它作為初始VPN建立的一部分被傳遞給客戶端。它在頭端會話的生存期內保持有效，並儲存在客戶端記憶體中，這是一個特權進程。
   提示：這些ASA版本及更高版本包含更強的加密會話令牌：9.1(3)和8.4(7.1)

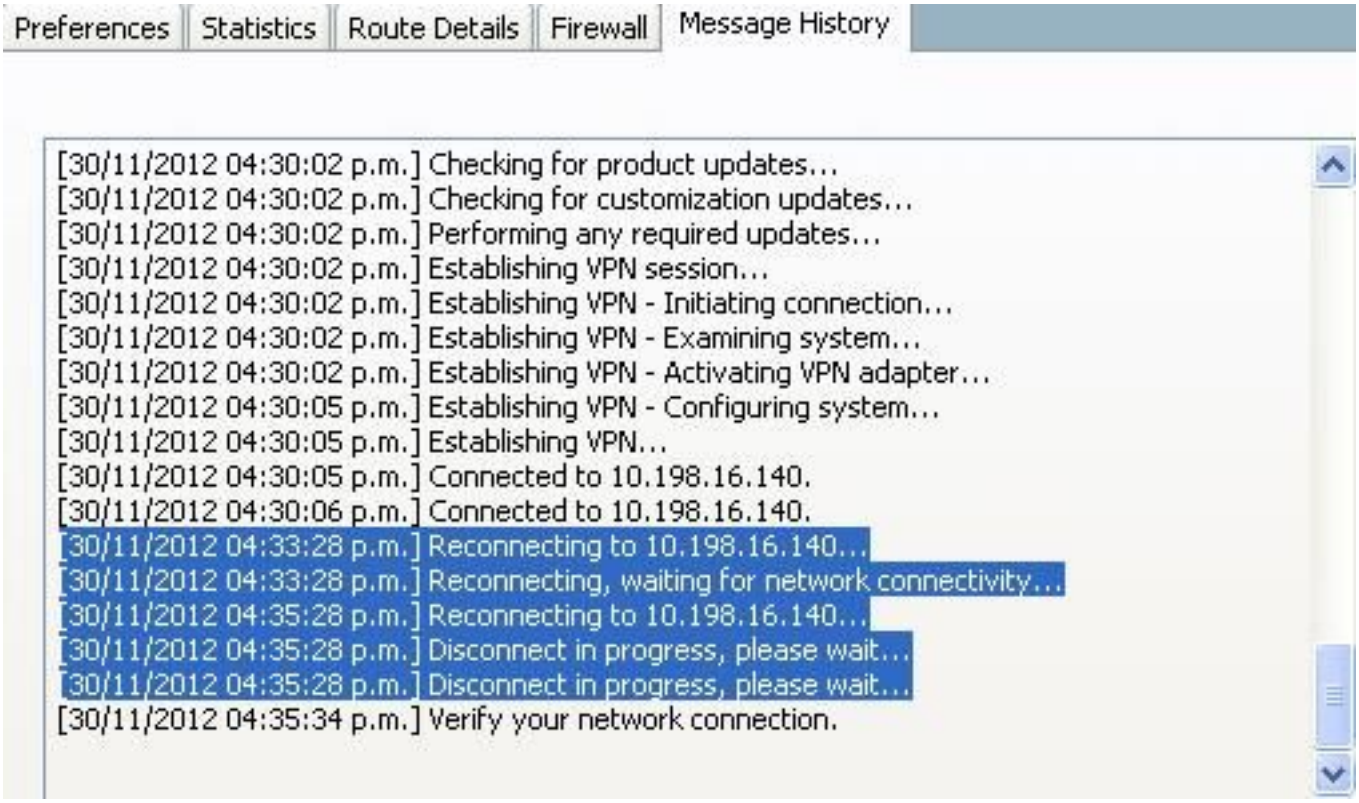
實際流程

一旦網路連線中斷，即會啟動斷開連線超時計時器。只要此計時器沒有過期，AnyConnect客戶端就會繼續嘗試重新連線。「斷開連線超時」設定為組策略**Idle-Timeout**或**Maximum Connect Time**中的**最小設定。**

此計時器的值顯示在協商中AnyConnect會話的事件檢視器中：



在本例中，會話在兩分鐘（120秒）後斷開，可以在AnyConnect的消息歷史記錄中檢查該會話：



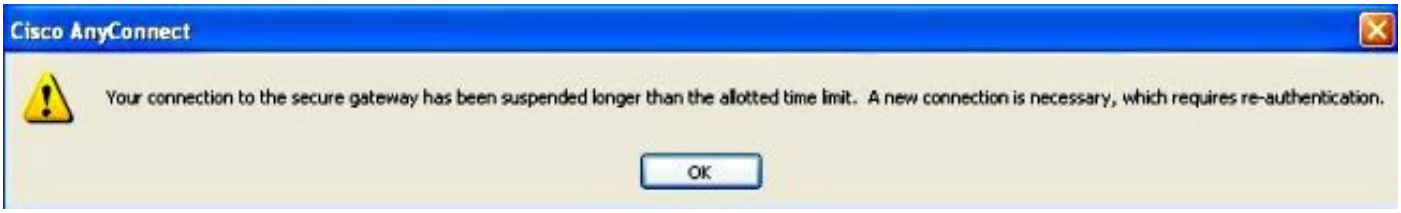
提示：要使ASA響應嘗試重新連線的客戶端，父隧道會話必須仍存在於ASA資料庫中。在故障切換情況下，還需要啟用DPD，以便重新連線行為能夠正常工作。

從前面的消息可見，重新連線失敗。但是，如果重新連線成功，則會發生以下情況：

1. 父通道保持不變；不會重新協商，因為此通道會維護作業階段重新連線所需的作業階段權杖。
2. 將生成新的SSL和DTLS會話，並在重新連線中使用不同的源埠。
3. 所有Idle-Timeout值都將恢復。
4. 不活動超時已恢復。

注意：請注意Cisco錯誤ID CSCtg33110。當AnyConnect重新連線時，VPN會話資料庫不會更新ASA會話資料庫中的公共IP地址。

在嘗試重新連線失敗的情況下，您會遇到以下消息：



註：為了使其更精確，已提交此增強請求：思科錯誤ID CSCsl52873 - ASA對AnyConnect沒有可配置的斷開連線超時。

系統掛起情況下的AnyConnect客戶端行為

漫遊功能允許AnyConnect在PC睡眠後重新連線。客戶端會繼續嘗試，直到空閒或會話超時過期，並且當系統進入休眠/待機狀態時，客戶端不會立即斷開隧道。對於不需要此功能的使用者，請將

會話超時設定為較小的值，以防止睡眠/恢復重新連線。

> **註**：修復思科錯誤ID CSCso17627(版本2.3(111)+)後，引入了控制旋鈕以在恢復功能時禁用此重新連線。

使用以下設定，可以通過AnyConnect XML配置檔案控制AnyConnect的自動重新連線行為：

```
      <AutoReconnect UserControllable="true">true
<AutoReconnectBehavior>ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
```

通過此更改，AnyConnect會在電腦從睡眠狀態恢復時嘗試重新連線。 AutoReconnectBehavior首選項預設為DisconnectOnSuspend。此行為不同於AnyConnect客戶端版本2.2。若要在恢復後重新連線，網路管理員必須在配置檔案中設定ReconnectAfterResume，或者讓使用者可以在配置檔案中控制AutoReconnect和AutoReconnectBehavior首選項，以便使用者對其進行設定。

常見問題

問題1.Anyconnect DPD有間隔但沒有重試 — 它必須將多少資料包丟失，然後才會將遠端終端標籤為宕機？

A. 從客戶端的角度來看，DPD僅在隧道建立階段拆除隧道。如果客戶端在隧道建立階段遇到三次重試（傳送四個資料包），並且沒有收到來自主VPN伺服器的響應，則如果配置了一個備用伺服器，它會回退到使用其中一個。但是，隧道建立後，從客戶端的角度來看，丟失的DPD對隧道沒有任何影響。DPDs的實際影響在VPN伺服器上，如DPDs and Inactivity Timers一節所述。

問題2.使用IKEv2的AnyConnect的DPD處理是否不同？

答：是，IKEv2的重試次數是固定的，每次重試六次/七個資料包。

問題3.AnyConnect父隧道是否有其他用途？

A. 除了是ASA上的對映外，父隧道還用於將AnyConnect映像升級從ASA推送到客戶端，因為客戶端在升級過程中未主動連線。

問題4.您是否可以僅過濾和註銷非活動會話？

答：您可以使用**show vpn**-sessiondb anyconnect filter inactive**命令過濾非活動會**話。但是，沒有命令可以只註銷非活動會話。相反，您需要註銷特定會話，或註銷每個使用者（索引 — 名稱）、協定或隧道組的所有會話。增強功能請求Cisco錯誤ID CSCuh55707已存檔，以便新增僅註銷非活動會話的選項。

問題5.當DTLS或TLS隧道Idle-Timeout過期時，父隧道會發生什麼情況？

A.在SSL隧道或DTLS隧道關閉後，AnyConnect父會話的「空閒至左側」計時器將重置。這允許「空閒超時」充當「斷開連線」超時。這實際上成為客戶端重新連線的允許時間。如果使用者端沒有在計時器內重新連線，則父通道會終止。

問題6.在DPD計時器斷開會話後，為什麼還要保留會話？為什麼ASA不釋放IP地址？

A.頭端對客戶的狀態一無所知。在這種情況下，ASA會等待客戶端重新連線，直到會話在空閒計時器超時為止。DPD不會終止AnyConnect會話；它只會終止隧道（在該會話中），以便客戶端可以重新建立隧道。如果使用者端沒有重新建立通道，作業階段會一直保留，直到閒置計時器到期。

如果關注的是已使用的會話，請將同時登入設定為較小的值，如1。使用此設定，會話資料庫中具有會話的使用者在再次登入時將刪除其以前的會話。

問題7.如果ASA從活動狀態故障切換到備用狀態，該行為是什麼？

A.最初，建立會話時，將三個隧道（父隧道、SSL隧道和DTLS隧道）複製到備用裝置；當ASA進行故障轉移後，DTLS和TLS會話會重新建立，因為它們沒有同步到備用裝置，但是在AnyConnect會話重新建立後，通過隧道的所有資料流都必須正常運作。

SSL/DTLS會話不是有狀態的，因此SSL狀態和序列號不會維護，並且可能非常繁重。因此，需要重新建立這些作業階段，這可通過父作業階段和作業階段權杖來完成。

> **提示**：在出現故障切換事件時，如果禁用keepalive，則SSL VPN客戶端會話不會轉移到備用裝置。

問題8.如果空閒超時和斷開連線超時值相同，為什麼它們有兩個不同的超時值？

A. 在開發協定時，會提供兩種不同的超時：

- 空閒超時 — 當沒有資料通過連線時，將啟用空閒超時。
- 斷開連線超時 — 當您由於連線已丟失且無法重新建立而放棄VPN會話時，將發生斷開連線超時。

ASA上從未實現斷開連線的超時。相反，ASA會將空閒和斷開連線超時的空閒超時值傳送到客戶端。

客戶端不使用空閒超時，因為ASA處理空閒超時。客戶端使用斷開連線的超時值（與空閒超時值相同），以便瞭解由於ASA已丟棄會話而何時放棄重新連線嘗試。

ASA未主動連線到客戶端，但會通過空閒超時使會話超時。在ASA上不實施斷開連線超時的主要原因是避免為每個VPN會話新增另一個計時器以及ASA上的額外開銷（儘管這兩種情況下可以使用相同的計時器，但使用不同的超時值即可，因為兩種情況是互斥的）。

通過斷開連線超時新增的唯一值是允許管理員為客戶端未主動連線與空閒時指定不同的超時。如前所述，已針對此問題提交了思科錯誤ID CSCsl52873。

問題9.客戶端電腦掛起時會發生什麼情況？

答：預設情況下，AnyConnect會在您失去連線時嘗試重新建立VPN連線。預設情況下，系統恢復後不會嘗試重新建立VPN連線。有關詳細資訊，請參閱系統掛起情況下的AnyConnect客戶端行為。

問題10. 發生重新連線時，AnyConnect虛擬介面卡是否翻動，或者路由表是否完全更改？

A. 隧道級重新連線也不起作用。這只是在SSL或DTLS上重新連線。這些在投降前大約需要30秒。如果DTLS失敗，則直接丟棄。如果SSL失敗，將導致會話級重新連線。會話級重新連線將完全重做路由。如果在重新連線時分配的客戶端地址或影響虛擬介面卡(VA)的任何其他配置引數未更改，則不會禁用VA。雖然從ASA接收的配置引數不太可能有任何更改，但用於VPN連線的物理介面的變化（例如，取消停靠並從有線連線到WiFi）可能會導致VPN連線的不同最大傳輸單位(MTU)值。MTU值會影響VA，如果更改該值，則會禁用VA，然後重新啟用。

問題11. 「自動重新連線」是否提供會話永續性？如果是，AnyConnect客戶端中是否新增了任何其他功能？

A. AnyConnect不提供任何額外的「魔法」來適應應用程式的會話永續性。但是，只要在ASA上配置的空閒和會話超時未過期，VPN連線將在恢復安全網關的網路連線後不久自動恢復。而且與IPsec客戶端不同，自動重新連線會導致同一客戶端IP地址。當AnyConnect嘗試重新連線時，AnyConnect虛擬介面卡保持啟用狀態且處於已連線狀態，因此客戶端IP地址始終在客戶端PC上保持存在並啟用，這樣客戶端IP地址就具有永續性。但是，如果恢復VPN連線的時間過長，客戶端PC應用程式仍會感到與企業網路上的伺服器失去連線。

問題12. 此功能適用於Microsoft Windows的所有變體（Vista 32位和64位，XP）。Macintosh怎麼樣？在OS X 10.4上是否有效？

A. 此功能在Mac和Linux上有效。Mac和Linux也存在一些問題，但最近也有一些改進，特別是Mac。Linux仍需要一些其他支援(思科錯誤ID CSCsr16670、思科錯誤ID CSCsm69213)，但也有基本功能。對於Linux，AnyConnect無法識別已發生掛起/恢復（睡眠/喚醒）。這基本上會產生兩個影響：

- 如果不提供掛起/恢復支援，則Linux上無法支援AutoReconnectBehavior配置檔案/首選項設定，因此掛起/恢復後始終進行重新連線。
- 在Microsoft Windows和Macintosh上，恢復後會立即在會話級別執行重新連線，這樣可以更快地切換到不同的物理介面。在Linux上，由於AnyConnect完全不知道掛起/恢復，因此重新連線先在隧道級別進行（SSL和DTLS），這可能意味著重新連線需要稍長的時間。但是重新連線仍然發生在Linux上。

問題13. 在連線方面（有線、wi-fi、3G等）該功能是否存在任何限制？它是否支援從一種模式到另一種模式（從Wi-Fi到3G、3G到有線等）的轉換？

A. AnyConnect在VPN連線的生命週期內未繫結到特定物理介面。如果用於VPN連線的物理介面丟失，或者如果重新連線嘗試超過某個故障閾值，則AnyConnect不再使用該介面，並嘗試使用任何可用的介面訪問安全網關，直到空閒計時器或會話計時器過期。請注意，物理介面的更改可能導致VA的MTU值不同，這將導致VA必須被禁用並重新啟用，但仍使用相同的客戶端IP地址。

如果出現任何網路中斷（介面關閉、網路更改、介面更改），AnyConnect會嘗試重新連線；重新連線時無需重新身份驗證。這甚至適用於實體介面的交換器：

範例：

```
1. wireless off, wired on: AC connection established
2. disconnect wired physically, turn wired on: AC re-established connection in
30 seconds
3. connect wired, turn off wireless: AC re-established connection in 30 secs
```

問題14. 如何驗證恢復操作？

A. 在簡歷中，您重新提交在會話生存期內保留的已驗證令牌，然後會話重新建立。

問題15. 在重新連線時是否也執行LDAP授權，還是僅執行身份驗證？

A. 這僅在初始連線中執行。

問題16. 恢復時是否運行登入前和/或hostscan?

A. 不，這些操作僅在初始連線上運行。類似內容將安排在未來的定期狀態評估功能中。

問題17. 關於VPN負載平衡(LB)和連線恢復，客戶端是否直接連線回之前連線到的集群成員？

答：是，這是正確的，因為您不會通過DNS重新解析主機名以重新建立當前會話。

相關資訊

- ASA DPD參考：思科錯誤ID CSCsr63074 — 對等體失效時，不傳送DPD；在使用7.2.4的s2上，隧道不空閒
- 技術支援與文件 - Cisco Systems

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）。