

AnyConnect FAQ：通道，重新连接行为和不活动计时器

目录

[简介](#)

[背景信息](#)

[通道的类型](#)

[从ASA的输出示例:](#)

[DPDs和不活动计时器](#)

[会话什么时候认为一非激活会话？](#)

[ASA什么时候丢弃SSL通道？](#)

[如果DPDs已经启用，Keepalive为什么需要启用？](#)

[AnyConnect客户端行为在的情况下重新连接](#)

[实际过程](#)

[AnyConnect在系统挂起的情况下客户端行为](#)

[常见问题](#)

[Q1. Anyconnect DPD没有一个间隔，但是重试次数-必须未命中多少数据包，在指示远程终端如停止前？](#)

[Q2. 为与IKEv2的AnyConnect DPD处理是否是不同的？](#)

[Q3. 有没有AnyConnect帕伦特通道的另一个目的？](#)

[Q4. 过滤和能否注销非激活会话？](#)

[Q5. 当DTL或TLS通道Idle-timeout到期时，什么发生在帕伦特通道？](#)

[Q6. 什么是保持会话点DPD计时器为什么一次断开了会话和ASA不释放IP地址？](#)

[Q7. 如果ASA从激活故障切换到待机，什么是行为？](#)

[Q8. 为什么有两不同的超时、空闲超时和断开超时，如果他们两个同一个值？](#)

[Q9. 当客户端机器是中止，什么发生？](#)

[Q10. 发生重新连接时，AnyConnect 虚拟适配器 是否会抖动或者路由表是否会更改？](#)

[Q11. ？自动重新连接？提供会话持续性？如果那样，有没有在AnyConnect客户端添加的任何额外功能？](#)

[Q12. 此功能在所有变形运作Microsoft Windows \(64位的Vista 32位&，XP\)。麦金塔怎么样？它是否工作在OS x 10.4 ？](#)

[Q13. 有没有任何限制对功能根据连接\(有线，wi-fi，3G等等\)？它是否支持从一个模式的转换到另一个\(从wi-fi到3G，3G对有线的，等等\)？](#)

[Q14. 恢复操作如何验证？](#)

[Q15. LDAP授权也被执行重新连接或仅验证？](#)

[Q16. PRE洛金是否和hostscan运行在恢复？](#)

[Q17. 关于VPN负载均衡\(LB\)和连接恢复，客户端是否将连接连接对以前的上一步直接地到集群成员？](#)

[相关信息](#)

简介

本文详细描述关于Cisco AnyConnect安全移动客户端(AnyConnect)通道的一些重点、重新连接行为和对端死机检测(DPD)和不活动计时器。

背景信息

通道的类型

有两个使用的方法为了联络AnyConnect会话：

- 通过门户(无客户端)
- 通过独立应用程序

基于在途中您连接，您创建三个不同的通道(会话)在ASA，每一个与一个特定目的：

1. **无客户端或帕伦特通道**：这是在协商创建为了设置会话标记是必要的主要会话，万一重新连接需要归结于网络连通性问题或冬眠。凭连接机制，思科可适应安全工具(ASA)列出会话作为无客户端(Weblaunch通过门户)或帕伦特(独立AnyConnect)。

注意：当客户端积极地没有连接时，AnyConnect帕伦特代表会话。有效地，它工作类似于Cookie，因为它是在该的ASA的数据库条目映射对从特定的客户端的连接。如果客户端关闭了或睡眠，通道(IPsec/Internet Key Exchange (IKE)/传输层安全(TLS) /Datagram传输层安全(DTL)协议)被切断，但是帕伦特保持直到空闲计时器或最大数量连接时间生效。这允许用户重新连接，无需重新鉴别。

2. **安全套接字协议层(SSL) -通道**：SSL连接首先被建立，并且数据在此连接通过，当尝试建立DTL连接时。一旦DTL连接被建立，客户端通过DTL连接发送数据包而不是通过SSL连接。另一方面，控制数据包始终通过SSL连接进行传输。

3. **DTL通道**：当DTL通道充分地设立时，所有数据移动向DTL通道，并且SSL通道只使用偶尔的控制通道流量。如果某事发生在用户数据报协议(UDP)，DTL通道被切断，并且所有数据再穿过SSL通道。

从ASA的输出示例:

这是从两个连接方法的输出示例:

AnyConnect通过Web启动连接：

```
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

AnyConnect通过独立应用程序连接 :

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

DPDs和不活动计时器

会话什么时候认为非激活会话？

只有当SSL通道不再存在会话在会话上，认为非激活(和计时器开始增加)。因此，每会话用SSL通道

滴下时间标记时间。

```
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什么时候丢弃SSL通道？

有两种方式SSL通道可以被断开：

1. **DPD** -客户端用于DPDs为了检测通信的一失败AnyConnect客户端和ASA首端之间。DPDs也用于为了整理在ASA的资源。这保证首端在数据库不保持连接，如果终端是无响应对DPD ping。如果ASA发送DPD对终端，并且响应，行动没有采取。如果终端不是响应能力的，ASA切断在会话数据库的通道，并且搬入会话恢复”模式的“等待。此的什么含义是从首端的DPD开始，并且首端与客户端不再联络。在这些情况下，ASA停滞帕伦特通道为了允许用户漫游网络，去睡和恢复会话。和清除积极地连接的会话的在这些条件下这些会话计数：用户Idle-timeout客户端恢复原始会话并且适当地注销
为了配置DPDs，请使用[anyconnect DPD间隔](#)命令在WebVPN属性下在组政策设置。默认情况下，DPD启用并且设置为ASA (网关)和客户端的30秒。

警告：注意Cisco Bug ID [CSCts66926](#) - DPD不能终止DTL在丢失的客户端连接以后建立隧道。

2. **Idle-timeout** -第二个方式SSL通道被断开是，当此通道的Idle-timeout到期时。然而，请记住它是必须断开不仅的SSL通道，但是DTL建立隧道。除非DTL会话时间，SSL通道在数据库保留。

如果DPDs已经启用，Keepalive为什么需要启用？

如解释以前，DPD不杀害AnyConnect会话。它仅仅杀害在该会话内的通道，以便客户端能重建通道。如果客户端不能重建通道，会话依然是，直到空闲计时器在ASA超时。默认情况下因为DPDs启用，客户也许经常断开由于关闭在一个方向的流用网络地址转换(NAT)、防火墙和代理设备。启用在低间隔的Keepalive，例如20秒，帮助防止此。

Keepalive启用在一特定的组政策的WebVPN属性下用[anyconnect ssl保活命令](#)。默认情况下，计时器设置为20秒。

AnyConnect客户端行为在的情况下重新连接

如果连接中断，AnyConnect 将尝试重新连接。这不可配置，自动地。只要ASA的VPN会话有效，并且，如果AnyConnect能重建物理连接，VPN会话将恢复。

重新连接功能继续直到会话超时或断开超时，实际上是空闲超时，到期(或30分钟，如果超时没有配置)。一旦这些超时，您不应该继续，因为ASA丢弃了VPN会话。客户端将继续，只要它认为ASA仍然有VPN会话。

AnyConnect将重新连接，无论网络接口更改。不重要，如果网络接口卡(NIC)的IP地址更改，或者，如果从一个NIC的连接交换机到另一个NIC (对有线的或反之亦然的无线)。

当您考虑AnyConnect的时重新连接进程，有您必须记住的三个级别会话。另外，这些会话中的每一的重新连接行为是松散接合的，任何一个可以重新建立，不用在上一个层的会话元素的一从属关系：

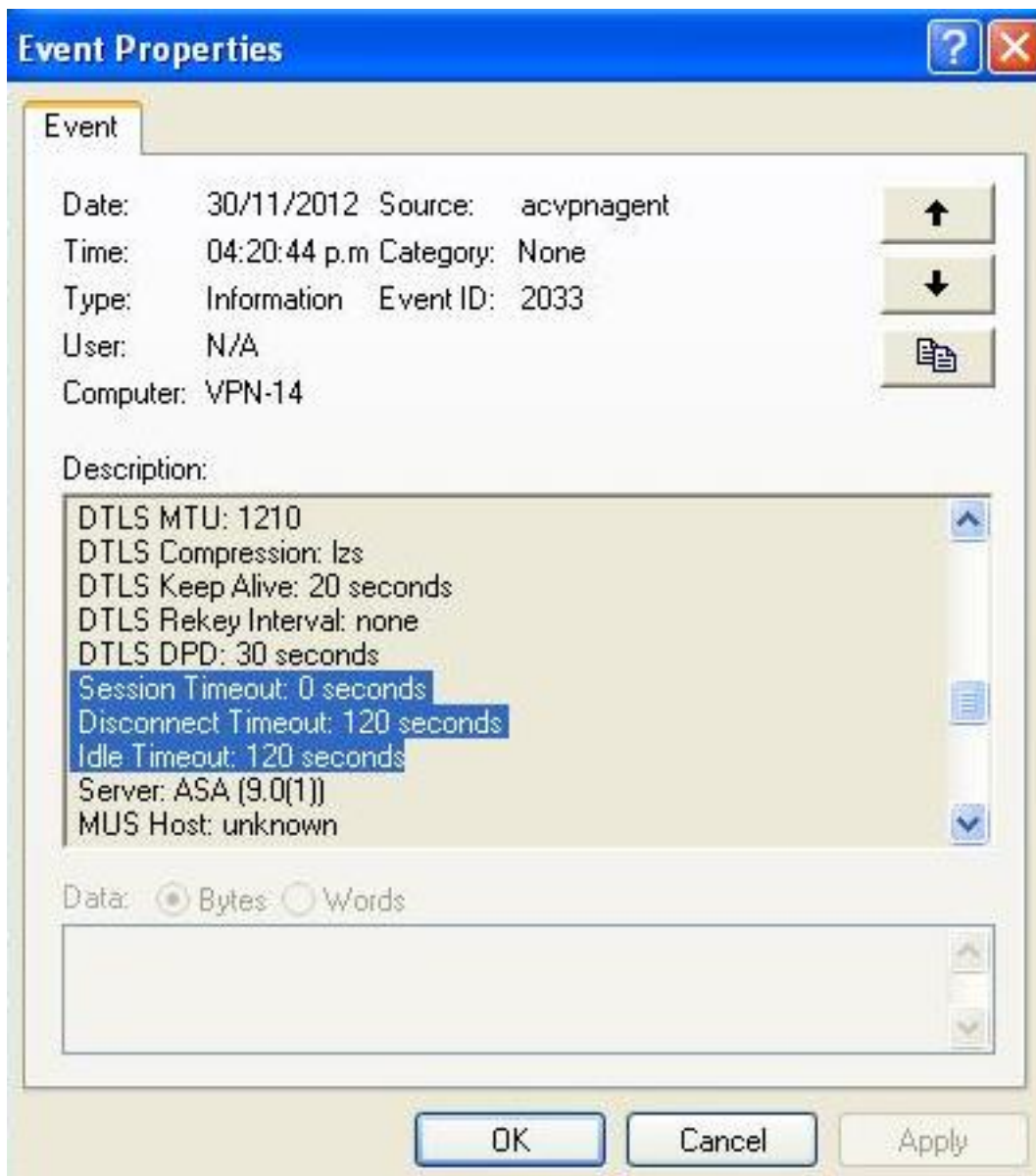
1. TCP或UDP重新连接[OSI层3]
2. TLS、DTL或者IPSec (IKE+ESP) [- TLS恢复不支持OSI层4]。
3. VPN [OSI层7] -，当有中断，VPN会话标记用于，因为验证标记为了重建在一条安全信道的VPN会话。它是非常类似的，概念上的所有权机制，对Kerberos标记或客户端证书如何使用验证。标记是唯一和密码生成由首端，包含会话ID加上一密码生成的随机的有效负载。在对首端的一条安全信道设立后，它通过给客户端作为初始VPN建立一部分。它保持有效为会话的寿命首端的，并且在客户端内存存储，是特权进程。

提示： 这些ASA版本和以后包含一更加强的加密会话标记：9.1(3)和8.4(7.1)

实际过程

当打乱，断开超时计时器开始网络连接。只要此计时器不超时，AnyConnect客户端继续设法重新连接。断开超时设置为组策略Idle-timeout或最大连接时间最低的设置。

值此计时器在事件查看器被看到为协商的AnyConnect会话：



在本例中，会话应该在两分钟(120秒)之后断开，可以被登记AnyConnect的消息历史记录：

```
[30/11/2012 04:30:02 p.m.] Checking for product updates...
[30/11/2012 04:30:02 p.m.] Checking for customization updates...
[30/11/2012 04:30:02 p.m.] Performing any required updates...
[30/11/2012 04:30:02 p.m.] Establishing VPN session...
[30/11/2012 04:30:02 p.m.] Establishing VPN - Initiating connection...
[30/11/2012 04:30:02 p.m.] Establishing VPN - Examining system...
[30/11/2012 04:30:02 p.m.] Establishing VPN - Activating VPN adapter...
[30/11/2012 04:30:05 p.m.] Establishing VPN - Configuring system...
[30/11/2012 04:30:05 p.m.] Establishing VPN...
[30/11/2012 04:30:05 p.m.] Connected to 10.198.16.140.
[30/11/2012 04:30:06 p.m.] Connected to 10.198.16.140.
[30/11/2012 04:33:28 p.m.] Reconnecting to 10.198.16.140...
[30/11/2012 04:33:28 p.m.] Reconnecting, waiting for network connectivity...
[30/11/2012 04:35:28 p.m.] Reconnecting to 10.198.16.140...
[30/11/2012 04:35:28 p.m.] Disconnect in progress, please wait...
[30/11/2012 04:35:28 p.m.] Disconnect in progress, please wait...
[30/11/2012 04:35:34 p.m.] Verify your network connection.
```

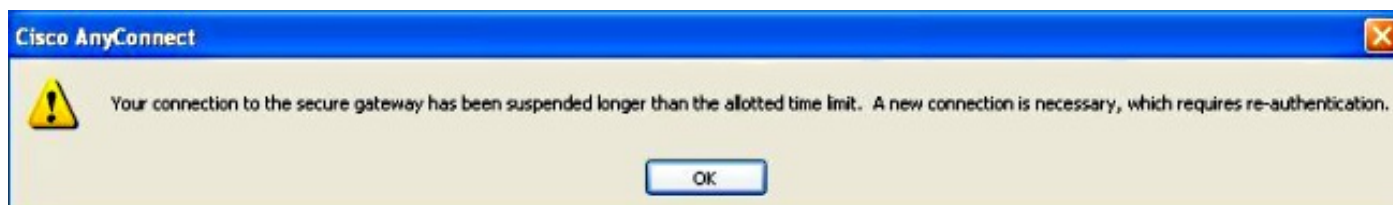
提示：为了使ASA响应对尝试重新连接的客户端，帕伦特通道会话在ASA数据库应该仍然存在。在故障切换情形下，DPDs也需要启用为了重新连接行为能工作。

象从上一个消息可视，失败的重新连接。然而，如果重新连接是成功的，这是发生了什么：

1. 帕伦特通道依然是同样;这没有重新协商，因为为会话要求为了重新连接的此通道维护会话标记。
2. 新的SSL和DTL会话生成，并且不同的源端口用于重新连接。
3. 所有空闲超时值恢复。
4. 休眠超时恢复。

警告：注意Cisco Bug ID [CSCtg33110](#)。当AnyConnect重新连接时，VPN会话数据库不更新在ASA会话数据库的公网IP地址。

在这种情况下尝试重新连接失败，您遇到此消息的地方：



注意：提出此增强请求为了做此更加粒状：[Cisco Bug ID CSCsl52873](#) - ASA没有AnyConnect的一可配置断开超时。

AnyConnect在系统挂起的情况下客户端行为

有允许AnyConnect重新连接，在PC睡眠后的漫游功能。客户端继续尝试直到空闲或会话超时到期，并且客户端不立即切断通道，当系统进入休眠/待机时。对于不想要此功能的客户，请设置会话超时为低值为了防止睡眠/恢复重新连接。

注意：在修正Cisco Bug ID [CSCso17627](#) (版本2.3(111)+)后，控制旋钮介绍为了禁用此请重新连接在恢复功能。

AnyConnect的自动重新连接行为可以通过AnyConnect XML配置文件被控制与此设置：

```
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
```

使用此更改，当计算机带来从睡眠的上一步AnyConnect将设法重新连接。对

DisconnectOnSuspend的AutoReconnectBehavior首选默认。此行为是与那AnyConnect客户端版本不同2.2。对于请在恢复以后重新连接，网络管理员必须在配置文件的任一集合

ReconnectAfterResume或做AutoReconnect和AutoReconnectBehavior首选用户可控制在配置文件允许用户设置它。

常见问题

Q1. Anyconnect DPD没有间隔，但是重试次数-必须未命中多少数据包，在指示远程终端如停止前？

A.它必须未命中三重试次数/四数据包。

Q2. 为与IKEv2的AnyConnect DPD处理是否是不同的？

A.是，IKEv2有重试次数固定数量的-六重试次数/七数据包。

Q3. 有没有AnyConnect帕伦特通道的另一个目的？

A.除是之外，因为客户端没有在升级进程中，积极地连接在ASA的一映射，parent通道用于为了推

送从ASA的AnyConnect镜像升级对客户端。

Q4. 过滤和能否注销非激活会话？

A. 您能过滤非激活会话用显示vpn-sessiondb anyconnect过滤器非激活命令。然而，no命令注销非激活会话。反而，您需要注销特定会话或注销所有会话每用户(索引名)，协议或者隧道群。Cisco Bug ID CSCuh55707，提出增强请求为了添加选项注销非激活会话。

Q5. 当DTL或TLS通道Idle-timeout到期时，什么发生在帕伦特通道？

A. 在SSL通道或DTL通道被切断后，对AnyConnect帕伦特会话的左侧”计时器的“空闲重置。这允许“idle-timeout”作为“断开了”超时。这有效变为客户端的允许的时候重新连接。如果客户端不在计时器内重新连接，则帕伦特通道将终止。

Q6. 什么是保持会话点DPD计时器为什么一次断开了会话和ASA不释放IP地址？

A. 首端不了解客户端状态。在这种情况下，ASA等待客户端有希望地重新连接直到会话时间在空闲计时器。DPD不杀害一AnyConnect会话;它仅仅杀害通道(在该会话内)，以便客户端能重建通道。如果客户端不重建一个通道，会话依然是，直到空闲计时器超时。

如果注意事项是关于会话用完，设置同时登录为一低值例如一个。使用此设置，有一会话在会话数据库让他们的前期会话删除的用户，当他们再登陆。

Q7. 如果ASA从激活故障切换到待机，什么是行为？

A. 最初，当会话建立时，三个通道(帕伦特、SSL和DTL)复制到备用装置;一旦ASA故障切换，DTL和TLS会话被重建，因为他们没有被同步到备用装置，但是所有数据流经通道应该工作，不用中断，在AnyConnect会话被重建后。

SSL/DTLS会话没有状态的，因此SSL状态和序号没有维护并且能相当纳税。因此，那些会话需要从头被重建，执行与帕伦特会话和会话标记。

提示：在故障切换事件情形下，如果Keepalive禁用，SSL VPN客户端会话没有转入到暂挂设备。

Q8. 为什么有两不同的超时、空闲超时和断开超时，如果他们是两个同一个值？

A. 当协议开发，两不同的超时提供了为：

- 空闲超时-空闲超时为，当数据没有在连接时通过。
- 断开超时-断开超时为，当您放弃VPN会话时，因为连接丢失并且不可能重新建立。

断开超时在ASA未曾实现。反而，ASA发送空闲和断开超时的空闲超时值给客户端。

因为ASA处理空闲超时，客户端不使用空闲超时。客户端什么时候使用断开超时值，是相同的象空闲超时值，为了知道放弃重新连接尝试，因为ASA丢弃了会话。

当不积极地连接对客户端，ASA通过空闲超时超时会话。主要原因不实现ASA的断开超时是避免另一个计时器的新增内容每VPN会话和增加的在ASA的开销(虽然同一个计时器可能用于两个实例，用不同的超时值，因为两个案件互相排斥)。

当客户端积极地没有连接与空闲时，仅增值与断开超时是允许管理员指定一不同的超时为。如注释前，Cisco Bug ID [CSCsl52873](#)为此被归档了。

Q9. 当客户端机器是中止，什么发生？

A.默认情况下，当您丢失连接时，AnyConnect尝试重建VPN连接。默认情况下后，在系统恢复它不尝试重建VPN连接。[在系统挂起的情况下](#)参考的[AnyConnect客户端行为](#)关于详细信息。

Q10. 发生重新连接时，AnyConnect 虚拟适配器 是否会抖动或者路由表是否会更改？

A. 通道级别重新连接不会执行或者。这是仅发生在 SSL 或 DTLS 上的重新连接。大约30秒，在他们放弃前，这些是。如果DTL发生故障，它丢弃。如果SSL发生故障，导致会话级别重新连接。会话级别重新连接完全将恢复路由。如果在重新连接分配的客户端地址，或者影响虚拟适配器的任何其他配置参数(VA)，未更改，则VA没有禁用。当是不太可能的有在从ASA时接收的配置参数上的所有变化，很可能，在用于VPN连接的物理接口上的一个变化(例如，如果从有线的驶出船坞并且去WiFi)可能导致VPN连接的一个不同的最大传输单元(MTU)值。MTU值影响VA，并且对它的一更改造造成VA禁用然后重新授权给

Q11. ？自动重新连接？提供会话持续性？如果那样，有没有在AnyConnect客户端添加的任何额外功能？

a. AnyConnect不提供任何额外的“魔术”适应应用程序的会话持续性。但是VPN连接自动地恢复，在对安全网关的网络连通性恢复之后，假设在ASA配置的空闲和会话超时未超时。并且不同于IPSec客户端，自动重新连接导致同样客户端IP地址。当AnyConnect尝试重新连接时，AnyConnect虚拟适配器保持已启用和在CONNECTED状态，因此客户端IP地址一直保持现在和已启用在客户端PC，给客户端IP地址持续时间。如果采取太长能将恢复的VPN连接的客户端PC应用程序，然而，可能将察觉失去连接到他们的在企业网络的服务器。

Q12. 此功能在所有变形运作Microsoft Windows (64位的Vista 32位&，XP)。麦金塔怎么样？它是否工作在OS x 10.4 ？

A. 此功能在Mac和Linux运作。有与Mac和Linux的问题，但是最近的改进特别为Mac被做了。Linux仍然要求某其他支持([CSCsr16670](#)，[CSCsm69213](#))，但是基本功能在那里。关于Linux，AnyConnect不会认为挂起/恢复(睡眠/苏醒)发生。这基本上有两影响：

- 不可能Linux支持AutoReconnectBehavior配置文件/首选设定没有挂起/恢复支持，因此重新连接永远将发生，在挂起/恢复后。
- 在Microsoft Windows和麦金塔，重新连接立即执行在会话级在恢复以后，允许一更加快速的交换机对一个不同的物理接口。在Linux，因为AnyConnect对挂起/恢复是完全没有察觉的，重新连接在通道级别(SSL和DTL)首先将发生，并且这也许含义重新连接采取轻微更加长。但是在Linux重新连接将发生。

Q13. 有没有任何限制对功能根据连接(有线，wi-fi，3G等等)？它是否支持从一个模式的转换到另一个(从wi-fi到3G，3G对有线的，等等)？

a. AnyConnect没有附加对一个特定的物理接口为VPN连接的寿命。如果用于VPN连接的物理接口丢失或，如果请重新连接在它的尝试超出一特定的失败阈值，然后AnyConnect不再将使用该接口，并且尝试到达安全网关与任何接口是可用的直到空闲或会话计时器请超时。注意在物理接口上的一个变化可能导致VA的一个不同的MTU值，将造成VA必须禁用和重新启用，但是仍然与同样客户端IP地址。

如果有任何网络中断(接口，已更改网络，下来已更改接口)，AnyConnect将设法重新连接;再验证没有必要重新连接。此均等适用于物理接口交换机：

示例：

```
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
```

Q14. 恢复操作如何验证？

A. 在恢复，您重新提交为会话的寿命将保持的已验证标记，并且会话然后被重建。

Q15. LDAP授权也被执行重新连接或仅验证？

A. 这在初始连接只执行。

Q16. PRE洛金是否和hostscan运行在恢复？

A. 不，在仅初始连接运行的这些。如此物将指定为将来定期状态评估功能。

Q17. 关于VPN负载均衡(LB)和连接恢复，客户端是否将连接连接对以前的上一步直接地到集群成员？

回答: 因为您不再通过再establishment的DNS解决主机名现有的会话，是，这正确。

相关信息

- ASA DPD参考：[Cisco Bug ID CSCsr63074](#) -没发送的DPD，当对等体是停止&通道不空闲在与7.2.4的s2s
- [技术支持和文档 - Cisco Systems](#)