回答AnyConnect常见问题 — 隧道、DPD和非活动计时器

目录

简介
背景信息
隧道类型
ASA的输出示例
DPD和非活动计时器
会话何时被视为非活动会话？
ASA何时丢弃SSL隧道？
如果已启用DPD，为什么需要启用Keepalive?
重新连接时的AnyConnect客户端行为
实际流程
系统挂起时AnyConnect客户端的行为
常见问题
问题1.Anyconnect DPD有间隔但没有重试 — 必须将多少数据包丢失，然后才会将远程终端标记为停机？
问题2.使用IKEv2的AnyConnect的DPD处理是否不同？
问题3.AnyConnect父隧道是否有其他用途？
问题4.您能否只过滤和注销非活动会话？
问题5.当DTLS或TLS隧道Idle-Timeout到期时，父隧道会发生什么情况？
问题6.为什么在DPD计时器断开会话后保留会话，为什么ASA不释放IP地址？
问题7.如果ASA从主用状态故障切换到备用状态，会出现什么情况？
问题8.如果空闲超时和断开连接超时值相同，为什么会有两种不同的超时？
问题9.当客户端计算机挂起时，会发生什么情况？
问题10. 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？
问题11. “自动重新连接”是否提供会话持久性？如果是，AnyConnect客户端中是否添加了任何其他功能？
问题12. 此功能适用于Microsoft Windows的所有变体（Vista 32位和64位，XP）。Macintosh怎么样？它在OS X 10.4上运行吗？
问题13. 在连接方面（有线、wi-fi、3G等）该功能是否存在任何限制？它是否支持从一种模式到另一种模式（从Wi-Fi到3G，从3G到有线等）的过渡？
问题14. 如何验证恢复操作？
问题15. LDAP授权是否也在重新连接时执行，还是仅执行身份验证？
问题16. 在恢复时是否运行登录前和/或hostscan?
问题17. 关于VPN负载均衡(LB)和连接恢复，客户端是否直接连接回之前连接的集群成员？
相关信息

简介

本文档介绍Cisco AnyConnect安全移动客户端隧道、重新连接行为和失效对等项检测(DPD)以及非活动计时器。

背景信息

隧道类型

连接AnyConnect会话有两种方法：

- 通过门户（无客户端）
- 通过独立应用程序

根据连接方式，您可在思科自适应安全设备(ASA)上创建三个不同的隧道（会话），每个隧道都有特定的用途：

1. 无客户端或父隧道：这是协商中创建的主要会话，目的是设置会话令牌，以便在因网络连接问题或休眠而需要重新连接时进行必要的会话令牌。根据连接机制，ASA将会话列为无客户端（通过门户进行网络启动）或父级（独立AnyConnect）。

   注意：AnyConnect-Parent表示客户端未主动连接的会话。实际上，它的工作方式与cookie类似，因为它是ASA上的一个数据库条目，映射到来自特定客户端的连接。如果客户端休眠/休眠，隧道(IPsec/Internet密钥交换(IKE)/传输层安全(TLS)/数据报传输层安全(DTLS)协议)将关闭，但父交换机将保持到空闲计时器或最大连接时间生效为止。这样用户无需重新身份验证即可重新连接。

2. 安全套接字层(SSL) — 隧道：首先建立SSL连接，数据通过此连接传递，同时它尝试建立DTLS连接。建立DTLS连接后，客户端将通过DTLS连接而不是通过SSL连接发送数据包。另一方面，控制数据包始终通过 SSL 连接进行传输。

3. DTLS-Tunnel：当DTLS-Tunnel完全建立时，所有数据都移动到DTLS-tunnel，并且SSL-Tunnel仅用于偶尔的控制信道流量。如果用户数据报协议(UDP)发生问题，DTLS隧道将关闭，所有数据将再次通过SSL隧道。

ASA的输出示例

以下是两种连接方法的输出示例。

通过Web启动连接的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
```

通过独立应用程序连接的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和非活动计时器

会话何时被视为非活动会话？

仅当会话中不再存在SSL隧道时，会话才被视为非活动状态（并且计时器开始增加）。因此，每个会话都带有SSL隧道丢弃时间的时间戳。

```
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何时丢弃SSL隧道？

可以通过两种方式断开SSL隧道：

1. **DPD** — 客户端使用DPD来检测AnyConnect客户端和ASA头端之间的通信故障。DPD也用于清除ASA上的资源。这可以确保在终端对DPD ping无响应时，前端不会在数据库中保留连接。如果ASA向终端发送DPD并响应，则不执行任何操作。如果终端无响应，在最大重传次数后（取决于是否使用IKEv1或IKEv2），ASA将断开会话数据库中的隧道，并将会话移动到“等待恢复”模式。这意味着头端的DPD已经启动，并且头端不再与客户端通信。在这种情况下，ASA会保持父隧道打开，以便允许用户漫游网络、进入睡眠状态并恢复会话。这些会话将计入主动连接的会话，并在以下情况下清除：
   用户空闲超时客户端恢复原始会话并正确注销
   要配置DPD，请使用 **anyconnect dpd-interval** 命令。默认情况下，ASA（网关）和客户端的DPD均处于启用状态并设置为30秒。

   注意：请注意Cisco Bug ID CSCts66926 - DPD在丢失客户端连接后无法终止DTLS隧道。

2. **Idle-Timeout** - SSL隧道的第二种断开方式是此隧道的Idle-Timeout超时。但是，请记住，必须空闲的不仅是SSL隧道，还有DTLS隧道。除非DTLS会话超时，否则SSL隧道将保留在数据库中。

如果已启用DPD，为什么需要启用Keepalive?

如前所述，DPD不会终止AnyConnect会话本身。它只是终止该会话中的隧道，以便客户端可以重新建立隧道。如果客户端无法重新建立隧道，会话将一直保持到ASA上的空闲计时器超时。由于默认情况下启用DPD，客户端经常会因使用网络地址转换(NAT)、防火墙和代理设备在一个方向上关闭流而断开连接。以较低的时间间隔（例如20秒）启用keepalive有助于防止这种情况。

Keepalive在特定group-policy的WebVPN属性下启用 **anyconnect ssl keepalive** 命令。默认情况下，计时器设置为20秒。

重新连接时的AnyConnect客户端行为

如果连接中断，AnyConnect会尝试重新连接。这是不可自动配置的。只要ASA上的VPN会话仍然有效，并且如果AnyConnect可以重新建立物理连接，VPN会话就会恢复。

重新连接功能会一直持续到会话超时或断开超时（实际上是空闲超时）到期（如果未配置超时，则为30分钟）。一旦这些会话过期，客户端便无法继续，因为VPN会话已经在ASA上被丢弃。只要客户端认为ASA仍有VPN会话，它就会继续。

无论网络接口如何变化，AnyConnect都会重新连接。网络接口卡(NIC)的IP地址是否更改，或者连接是否从一个NIC切换到另一个NIC（从无线切换到有线或反之亦然），都无关紧要。

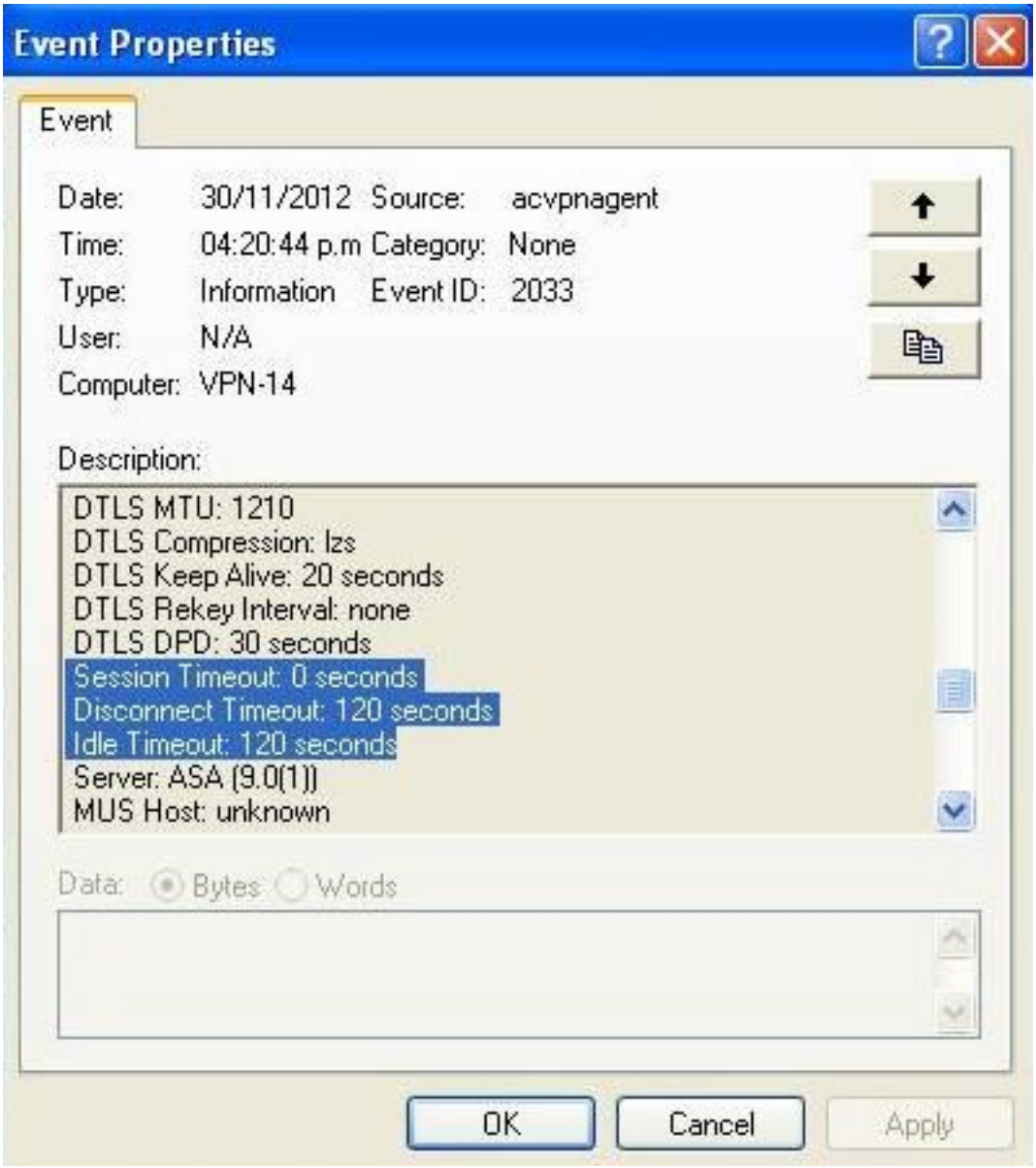
考虑AnyConnect的重新连接过程时，必须记住三个级别的会话。此外，每个会话的重新连接行为是松散耦合的，因为任何会话都可以重新建立，而不依赖于上一层的会话元素：

1. TCP或UDP重新连接[OSI第3层]
2. TLS、DTLS或IPSec(IKE+ESP)[OSI第4层] — 不支持TLS恢复。
3. VPN [OSI第7层] - VPN会话令牌用作身份验证令牌，以便在出现中断时通过安全通道重新建立VPN会话。 它是一种专有机制，概念上与Kerberos令牌或客户端证书用于身份验证的方式非常相似。 令牌是唯一的，由头端加密生成，包含会话ID以及加密生成的随机负载。在建立到头端的安全通道后，它作为初始VPN建立的一部分被传递到客户端。它在头端会话的生存期内保持有效，并存储在客户端内存中，这是一个特权进程。
   提示：这些ASA版本及更高版本包含更强大的加密会话令牌：9.1(3)和8.4(7.1)

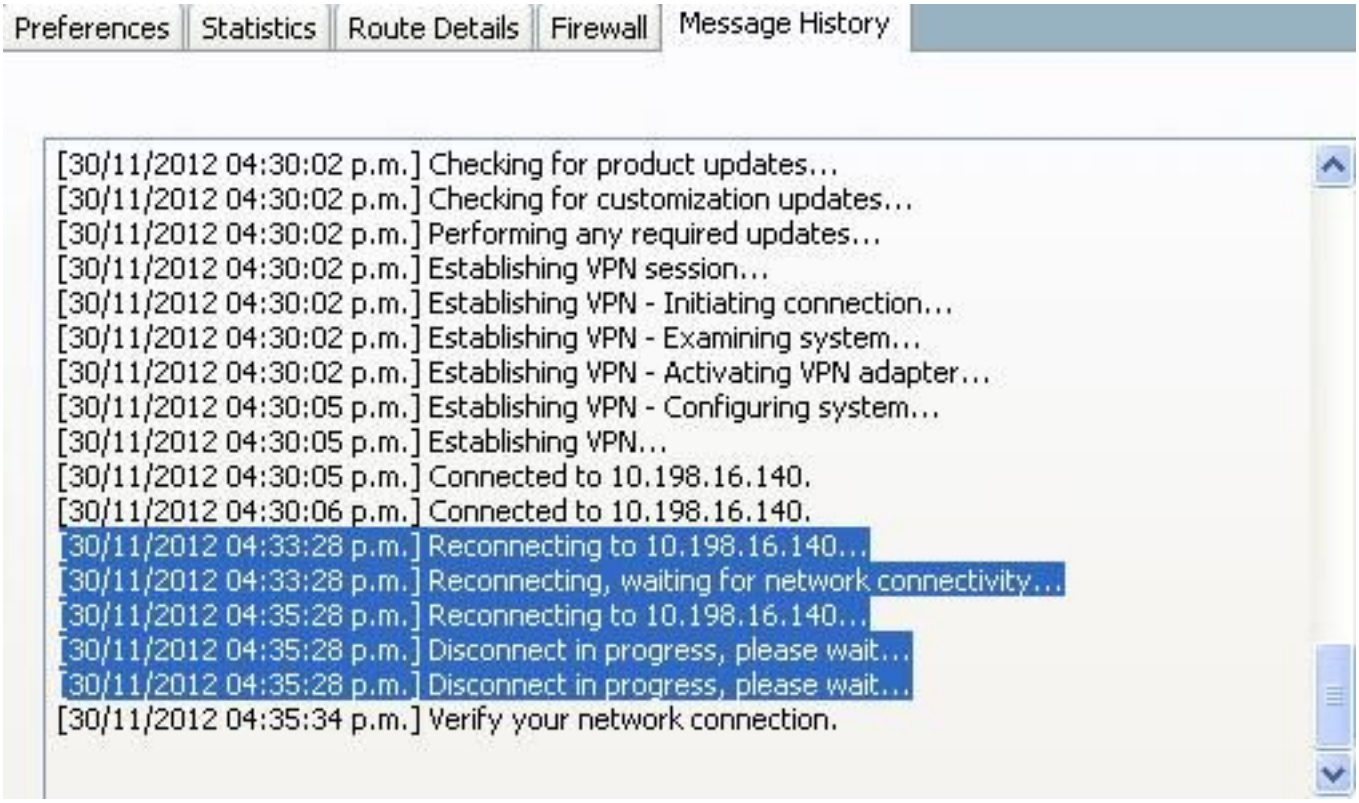
实际流程

一旦网络连接中断，就会启动断开超时计时器。只要此计时器未过期，AnyConnect客户端就会继续尝试重新连接。Disconnect Timeout设置为Group Policy **Idle-Timeout**或**Maximum Connect Time**的**最低**设置。

此计时器的值显示在协商中AnyConnect会话的事件查看器中：



在本示例中，会话将在两分钟（120秒）后断开，可以在AnyConnect的消息历史记录中检查该会话：



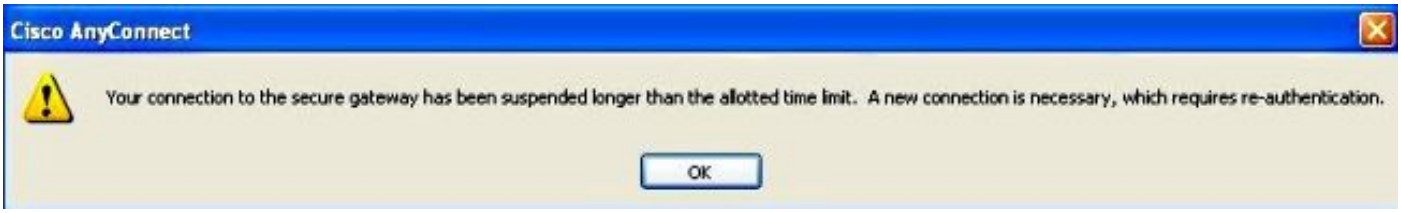
提示：对于ASA要响应尝试重新连接的客户端，父隧道会话必须仍存在于ASA数据库中。在发生故障切换时，还需要启用DPD才能使重新连接行为生效。

从前面的消息中可以看到，重新连接失败。但是，如果重新连接成功，会出现以下情况：

1. 父隧道保持不变；不会重新协商，因为此隧道会维护会话重新连接所需的会话令牌。
2. 将生成新的SSL和DTLS会话，并在重新连接中使用不同的源端口。
3. 所有Idle-Timeout值都将恢复。
4. 非活动超时已恢复。

注意：请注意Cisco Bug ID CSCtg33110。当AnyConnect重新连接时，VPN会话数据库不会更新ASA会话数据库中的公共IP地址。

在尝试重新连接失败的情况下，您会遇到以下消息：



注：此增强请求已存档，以便更精细地处理：Cisco Bug ID CSCsl52873 - ASA没有可配置的AnyConnect断开连接超时。

系统挂起时AnyConnect客户端的行为

有一个漫游功能，允许AnyConnect在PC睡眠后重新连接。客户端继续尝试，直到空闲或会话超时到期，并且当系统进入休眠/待机状态时，客户端不会立即中断隧道。对于不需要此功能的用户，请

将会话超时设置为低值以防止睡眠/恢复重新连接。

> **注意**：在修复了Cisco Bug ID CSCso17627(Version 2.3(111)+)之后，引入了一个控制命令，以便在恢复功能时禁用此重新连接。

使用以下设置，可以通过AnyConnect XML配置文件控制AnyConnect的自动重新连接行为：

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

通过此更改，AnyConnect会在计算机从睡眠状态恢复时尝试重新连接。 AutoReconnectBehavior首选项默认为DisconnectOnSuspend。此行为与AnyConnect客户端版本2.2的行为不同。要在恢复后重新连接，网络管理员必须在配置文件中设置ReconnectAfterResume，或让用户在配置文件中控制AutoReconnect和AutoReconnectBehavior首选项以允许用户对其进行设置。

常见问题

问题1.Anyconnect DPD有间隔但没有重试 — 必须将多少数据包丢失，然后才会将远程终端标记为停机？

A. 从客户端的角度来看，DPD仅在隧道建立阶段中断隧道。如果客户端在隧道建立阶段遇到三次重试（发送四个数据包），并且未收到来自主VPN服务器的响应，则如果配置了一个备用服务器，它会回退到使用其中一台备用服务器。但是，隧道建立后，从客户端的角度来看，错过的DPD对隧道没有任何影响。DPD的实际影响在VPN服务器上，如DPDs and Inactivity Timers部分所述。

问题2.使用IKEv2的AnyConnect的DPD处理是否不同？

A.是,IKEv2具有固定的重试次数 — 六次重试/七个数据包。

问题3.AnyConnect父隧道是否有其他用途？

A. 除了是ASA上的映射外，父隧道还用于将AnyConnect映像升级从ASA推送到客户端，因为客户端在升级过程中未主动连接。

问题4.您能否只过滤和注销非活动会话？

A.您可以使用**show vpn-sessiondb anyconnect filter inactive命令过滤非活动**会话。但是，没有命令可以只注销非活动会话。相反，您需要注销特定会话或注销每个用户(index - name)、协议或隧道组的所有会话。已提交增强请求Cisco Bug ID CSCuh55707，以便添加仅注销非活动会话的选项。

问题5.当DTLS或TLS隧道Idle-Timeout到期时，父隧道会发生什么情况？

A.在SSL隧道或DTLS隧道关闭后，AnyConnect-Parent会话的“Idle to Left”计时器重置。这允许“空闲超时”充当“断开连接”超时。这实际上成为客户端重新连接的允许时间。如果客户端在计时器内未重新连接，则父隧道将终止。

问题6.为什么在DPD计时器断开会话后保留会话，为什么ASA不释放IP地址？

A.头端对客户的状态一无所知。在这种情况下，ASA会等待客户端重新连接，直到会话在空闲计时器超时为止。DPD不会终止AnyConnect会话；它只会终止隧道（在该会话中），以便客户端可以重新建立隧道。如果客户端不重新建立隧道，会话将一直保持到空闲计时器超时。

如果关注的是已使用的会话，请将同时登录设置为较低的值，如1。使用此设置，在会话数据库中拥有会话的用户在再次登录时将删除其之前的会话。

问题7.如果ASA从主用状态故障切换到备用状态，会出现什么情况？

A.最初，建立会话时，三个隧道（父隧道、SSL和DTLS）会复制到备用设备；ASA故障转移后，DTLS和TLS会话会重新建立，因为它们未同步到备用设备，但是在AnyConnect会话重新建立后，通过隧道的所有数据流都必须正常工作，且不会中断。

SSL/DTLS会话没有状态，因此SSL状态和序列号不会被维护，并且可能非常繁重。因此，需要从头重新建立这些会话，这通过父会话和会话令牌完成。

> **提示**：如果禁用keepalive，在发生故障切换事件时，SSL VPN客户端会话不会转移到备用设备。

问题8.如果空闲超时和断开连接超时值相同，为什么会有两种不同的超时？

A. 在开发协议时，会提供两种不同的超时：

- 空闲超时 — 空闲超时用于在连接上未传递数据时使用。
- Disconnected timeout — 由于连接已丢失且无法重新建立，当您放弃VPN会话时，将发生断开超时。

未在ASA上实施断开连接的超时。相反，ASA会将空闲超时和断开超时两者的空闲超时值发送到客户端。

客户端不使用空闲超时，因为ASA处理空闲超时。客户端使用断开连接的超时值（与空闲超时值相同），以便了解由于ASA已丢弃会话，何时放弃重新连接尝试。

当未主动连接到客户端时，ASA会通过空闲超时使会话超时。未在ASA上实施断开超时的主要原因是避免为每个VPN会话添加另一个计时器以及ASA上的开销增加（尽管两个实例中可以使用同一计时器，只不过使用不同的超时值，因为两种情况是互斥的）。

通过断开连接超时添加的唯一值是允许管理员为客户端未主动连接时指定不同的超时时间，而不是为空闲时指定不同的超时时间。如前所述，Cisco Bug ID CSCsl52873已针对此进行了注册。

问题9.当客户端计算机挂起时，会发生什么情况？

答：默认情况下，AnyConnect会在您失去连接时尝试重新建立VPN连接。默认情况下，系统恢复后不会尝试重新建立VPN连接。有关详细信息，请参阅在系统暂停情况下的AnyConnect客户端行为。

问题10. 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. 隧道级重新连接也不起作用。这是仅发生在 SSL 或 DTLS 上的重新连接。这些在它们放弃之前大约需要30秒。如果DTLS失败，则它将被丢弃。如果SSL失败，将导致会话级重新连接。会话级重

新连接将完全重新执行路由。如果在重新连接时分配的客户端地址或影响虚拟适配器(VA)的任何其他配置参数未更改，则不会禁用VA。虽然从ASA接收的配置参数不会有任何更改，但用于VPN连接的物理接口发生更改（例如，取消停靠并从有线连接到WiFi）可能会导致VPN连接的不同最大传输单位(MTU)值。MTU值会影响VA，更改该值会导致VA被禁用然后重新启用。

问题11. “自动重新连接”是否提供会话持久性？如果是，AnyConnect客户端中是否添加了任何其他功能？

A. AnyConnect不提供任何额外的“魔力”来适应应用的会话持久性。但是，只要在ASA上配置的空闲和会话超时未过期，VPN连接将在恢复与安全网关的网络连接后不久自动恢复。与IPsec客户端不同，自动重新连接会导致同一客户端IP地址。当AnyConnect尝试重新连接时，AnyConnect虚拟适配器保持启用状态，并且处于连接状态，因此客户端IP地址始终在客户端PC上保持存在并启用，这样客户端的IP地址将持续存在。但是，如果恢复VPN连接花费的时间过长，客户端PC应用程序仍会感觉失去与企业网络上服务器的连接。

问题12. 此功能适用于Microsoft Windows的所有变体（Vista 32位和64位，XP）。Macintosh怎么样？它在OS X 10.4上运行吗？

A. 此功能在Mac和Linux上有效。Mac和Linux也存在一些问题，但最近也进行了改进，特别是Mac。Linux仍需要一些附加支持(Cisco Bug ID CSCsr16670、Cisco Bug ID CSCsm69213)，但基本功能也在Linux上。对于Linux，AnyConnect无法识别已发生挂起/恢复（睡眠/唤醒）。这基本上会产生两个影响：

- 如果不提供挂起/恢复支持，则Linux上无法支持AutoReconnectBehavior配置文件/首选项设置，因此，挂起/恢复后始终会发生重新连接。
- 在Microsoft Windows和Macintosh上，恢复后立即在会话级别执行重新连接，这样可以更快地切换到不同的物理接口。在Linux上，由于AnyConnect完全不知道挂起/恢复，因此重新连接先在隧道级别进行（SSL和DTLS），这可能意味着重新连接花费的时间稍长。但重新连接仍发生在Linux上。

问题13. 在连接方面（有线、wi-fi、3G等）该功能是否存在任何限制？它是否支持从一种模式到另一种模式（从Wi-Fi到3G，从3G到有线等）的过渡？

A. AnyConnect在VPN连接的生命周期内未绑定到特定物理接口。如果用于VPN连接的物理接口丢失或者如果重新连接尝试超过特定故障阈值，则AnyConnect不再使用该接口并尝试使用任何可用接口访问安全网关，直到空闲计时器或会话计时器到期。请注意，物理接口的更改可能会导致VA的MTU值不同，这会导致VA被禁用并重新启用，但仍使用相同的客户端IP地址。

如果出现任何网络中断（接口关闭、网络更改、接口更改），AnyConnect会尝试重新连接；重新连接时不需要重新进行身份验证。这甚至适用于物理接口的交换机：

示例：

```
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
```

问题14. 如何验证恢复操作？

A. 在简历中，您将重新提交保留到会话生命周期的已验证令牌，然后会话将重新建立。

问题15. LDAP授权是否也在重新连接时执行，还是仅执行身份验证？

A. 这仅在初始连接中执行。

问题16. 在恢复时是否运行登录前和/或hostscan?

A. 否，这些操作仅在初始连接上运行。类似内容将安排用于未来的定期状况评估功能。

问题17. 关于VPN负载均衡(LB)和连接恢复，客户端是否直接连接回之前连接的集群成员？

答：是，这是正确的，因为您不通过DNS重新解析主机名以重新建立当前会话。

相关信息

- **ASA DPD参考：Cisco Bug ID CSCsr63074 — 当对等体失效时不会发送DPD，在使用7.2.4的s2上隧道不会空闲**
- **技术支持和文档 - Cisco Systems**

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。