Answer AnyConnect FAQ - Tunnels, DPDs, and Inactivity Timer

Contents

Introduction

This document describes Cisco AnyConnect Secure Mobility Client tunnels, the reconnect behavior and Dead Peer Detection (DPD), and inactivity timer.

Background Information

Types of Tunnels

There are two methods used in order to connect an AnyConnect session:

- Via the Portal (Clientless)
- Via the Standalone Application

Based on the way you connect, you create three different tunnels (sessions) on the Cisco Adaptive Security Appliance (ASA), each one with a specific purpose:

1. Clientless or Parent-Tunnel: This is the main session that is created in the negotiation in order to set up the session token that is necessary in case a reconnect is needed due to network connectivity issues or hibernation. Based on the connection mechanism, the ASA lists the session as Clientless (Weblaunch via the Portal) or Parent (Standalone AnyConnect).

   Note: The AnyConnect-Parent represents the session when the client is not actively connected. Effectively, it works similar to a cookie, in that it is a database entry on the ASA that maps to the connection from a particular client. If the client sleeps/hibernates, the tunnels (IPsec/Internet Key Exchange (IKE)/ Transport Layer Security (TLS)/Datagram Transport Layer Security (DTLS) protocols) are torn down, but the Parent remains until the idle timer or maximum connect time takes effect. This allows the user to reconnect without reauthenticating.

2. Secure Sockets Layer (SSL)-Tunnel: The SSL connection is established first, and data is passed over this connection while it attempts to establish a DTLS connection. Once the DTLS connection is established, the client sends the packets via the DTLS connection instead of via the SSL connection. Control packets, on the other hand, always go over the SSL connection.

3. DTLS-Tunnel: When the DTLS-Tunnel is fully established, all data moves to the DTLS-tunnel, and the SSL-Tunnel is only used for occasional control channel traffic. If something happens to User Datagram Protocol (UDP), the DTLS-Tunnel is torn down and all data passes through the SSL-Tunnel again.

Sample Output from ASA

Here is sample output from the two connection methods.

AnyConnect Connected via Web-launch:

```
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 Connected via the Standalone Application:

```
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 and Inactivity Timers

When is a session considered an Inactive Session?

The session is considered Inactive (and the timer begins to increase) only when the SSL-Tunnel does not exist anymore in the session. So, each session is time-stamped with the SSL-Tunnel drop time.

```
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
```

When does the ASA drop the SSL-Tunnel?

There are two ways that an SSL-Tunnel can be disconnected:

1. **DPD** - DPDs are used by the client in order to detect a failure in communications between the AnyConnect client and the ASA head-end. DPDs are also used in order to clean up resources on the ASA. This ensures that the head-end does not keep connections in the database if the endpoint is nonresponsive to the DPD pings. If the ASA sends a DPD to the endpoint and it responds, no action is taken. If the endpoint is not responsive, after the maximum number of retransmission (it depends if IKEv1 or IKEv2 is used) the ASA tears down the tunnel in the session database, and moves the session into a "Waiting to Resume" mode. What this means is that DPD from the head-end has started, and the head-end no longer communicates with the client. In such situations, the ASA holds the Parent-Tunnel up in order to allow the user to roam networks, go to sleep, and recover the session. These sessions count against actively-connected sessions and are cleared under these conditions: User Idle-TimeoutClient resumes the original session and logs out properly
   In order to configure DPDs, use the **anyconnect dpd-interval** command under the WebVPN attributes in the group-policy settings. By default, the DPD is enabled and set to 30 seconds for both the ASA (gateway) and the client.

   Caution: Be aware of Cisco bug ID CSCts66926 - DPD fails to terminate DTLS tunnel after lost client connection.

2. **Idle-Timeout** - The second way that the SSL-Tunnel is disconnected is when the Idle-Timeout for this tunnel expires. However, remember that it is not only the SSL-Tunnel that must idle out, but the DTLS tunnel as well. Unless the DTLS session times out, the SSL-Tunnel is retained in the database.

Why do Keepalives need to be enabled if DPDs are already enabled?

As explained previously, the DPD does not kill the AnyConnect session itself. It merely kills the tunnel within that session so that the client can reestablish the tunnel. If the client cannot reestablish the tunnel, the session remains until the idle timer expires on the ASA. Since DPDs are enabled by default, clients can often get disconnected due to flows closing in one direction with Network Address Translation (NAT), Firewall and Proxy devices. Enabling keepalives at low intervals, such as 20 seconds, helps to prevent this.

Keepalives are enabled under the WebVPN attributes of a particular group-policy with the **anyconnect ssl keepalive** command. By default, the timers are set to 20 seconds.

AnyConnect Client Behavior in Case of Reconnects

AnyConnect attempts to reconnect if the connection is disrupted. This is not configurable, automatically. As long as the VPN session on the ASA is still valid and if AnyConnect can re-establish the physical connection, the VPN session is resumed.

The reconnect feature continues until the session timeout or the disconnect timeout, which is actually the idle timeout, expires (or 30 minutes if no timeouts are configured). Once these expire, the client cannot continue because the VPN sessions have already been dropped on the ASA. The client continues as long as it thinks the ASA still has the VPN session.

AnyConnect reconnects no matter how the network interface changes. It does not matter if the IP address of the Network Interface Card (NIC) changes, or if connectivity switches from one NIC to another NIC (wireless to wired or vice versa).

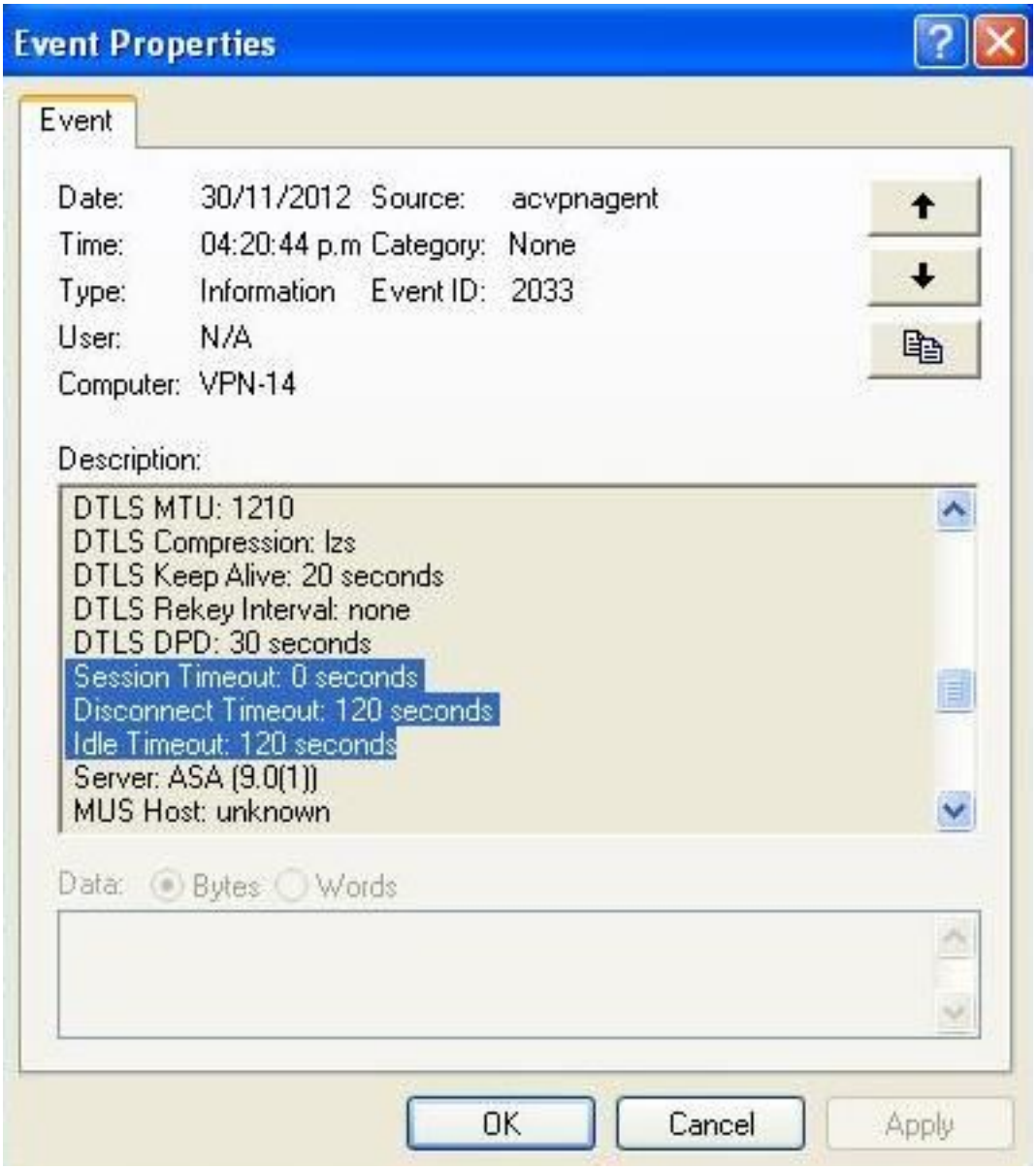
When you consider the reconnect process for AnyConnect, there are three levels of sessions that you must remember. Additionally, the reconnect behavior of each of these sessions is loosely coupled, in that any of them can be re-established without a dependency on the session elements of the previous layer:

1. TCP or UDP reconnects [OSI Layer 3]
2. TLS, DTLS, or IPSec(IKE+ESP) [OSI Layer 4] - TLS resumption is not supported.
3. VPN [OSI layer 7] - The VPN session token is used as an authentication token in order to reestablish the VPN session over a secured channel when there is a disruption. It is a proprietary mechanism that is very similar, conceptually, to how a Kerberos token or a client certificate is used for authentication. The token is unique and cryptographically generated by the head-end, which contains the session ID plus a cryptographically generated random payload. It is passed to the client as part of the initial VPN establishment after a secure channel to the head-end is established. It remains valid for the lifetime of the session on the head-end, and it is stored in the client memory, which is a privileged process.
   Tip: These ASA releases and later contain a stronger cryptographic session token: 9.1(3) and 8.4(7.1)

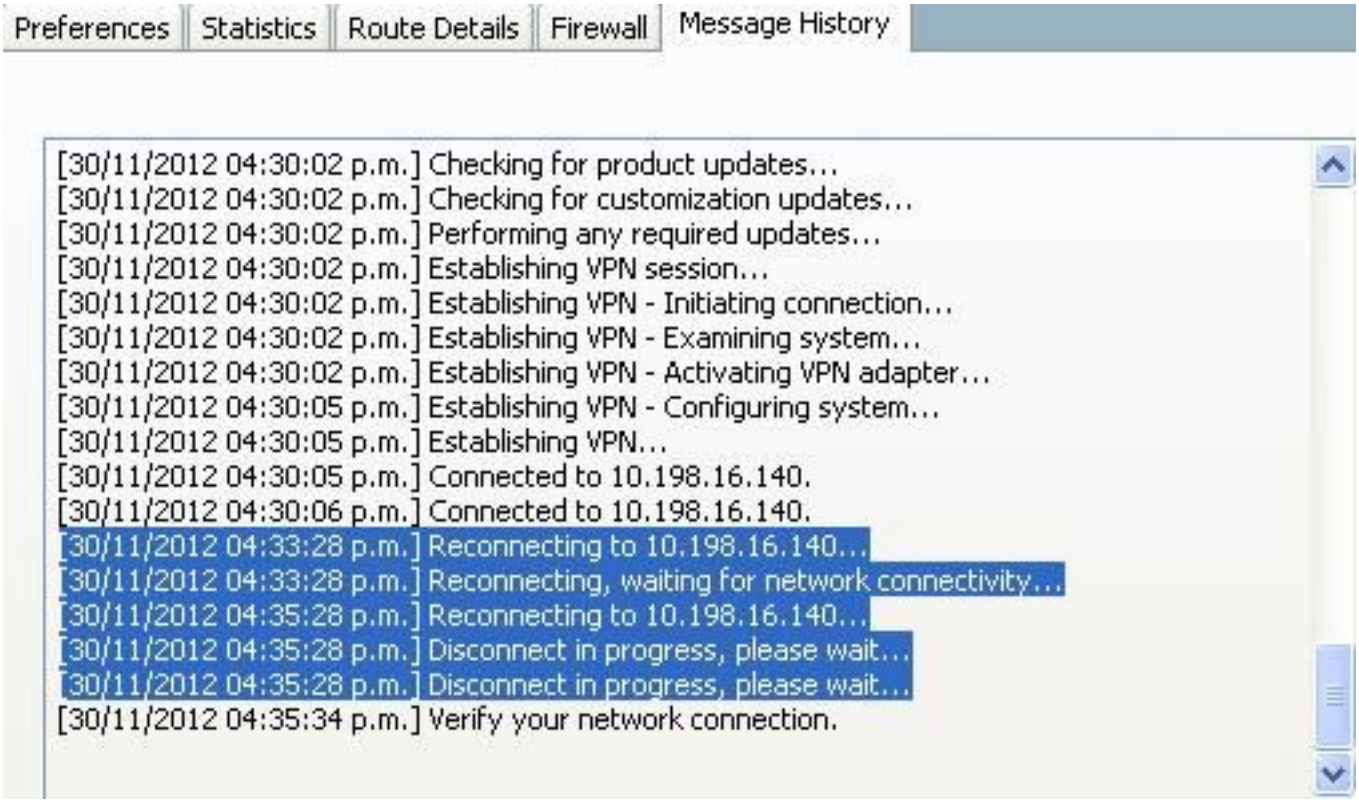
The Actual Process

A Disconnect Timeout timer is started as soon as the network connection is disrupted. The AnyConnect client continues to try to reconnect as long as this timer does not expire. The Disconnect Timeout is set to the lowest setting of either the Group Policy **Idle-Timeout** or the **Maximum Connect Time**.

The value of this timer is seen in the Event Viewer for the AnyConnect session in the negotiation:



In this example, the session disconnects after two minutes (120 seconds), which can be checked in the Message History of the AnyConnect:



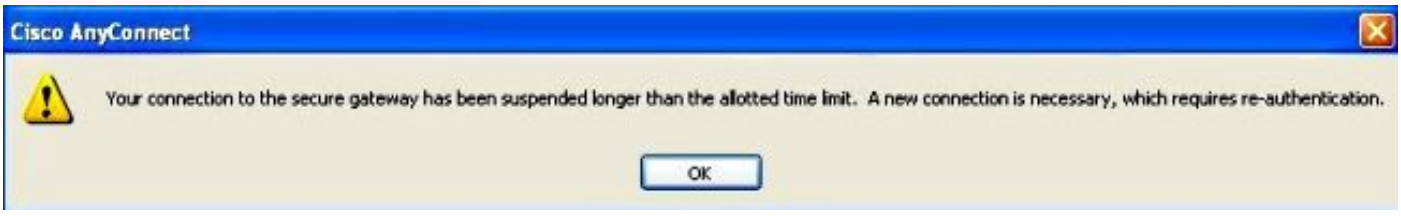
Tip: For the ASA to respond to a client that attempts to reconnect, the Parent-Tunnel session must still exist in the ASA database. In the event of failover, DPDs also need to be enabled for the reconnect behavior to work.

As is visible from the previous messages, the reconnect failed. However, if the reconnect is successful, here is what happens:

1. The Parent-Tunnel remains the same; this is not renegotiated because this tunnel maintains the session token that is required for the session in order to reconnect.
2. New SSL and DTLS sessions are generated, and different source ports are used in the reconnect.
3. All the Idle-Timeout values are restored.
4. The Inactivity Timeout is restored.

Caution: Be aware of Cisco bug ID CSCtg33110. The VPN session database does not update the Public IP address in the ASA session database when AnyConnect reconnects.

In this situation where the attempts to reconnect fail, you encounter this message:



Note: This enhancement request has been filed in order to make this more granular: Cisco bug ID CSCsl52873 - ASA does not have a configurable disconnected timeout for AnyConnect.

AnyConnect Client Behavior in Case of System Suspend

There is a roaming feature that allows AnyConnect to reconnect after a PC sleep. The client continues to try until the idle or session timeouts expire and the client does not immediately tear down the tunnel when the system goes into hibernate/standby. For users who do not want this feature, set the session timeout to a low value in order to prevent sleep/resume reconnects.

> **Note**: After the fix of Cisco bug ID CSCso17627 (Version 2.3(111)+), a control knob was introduced in order to disable this reconnect on resume feature.

The Auto-Reconnect behavior for AnyConnect can be controlled through the AnyConnect XML profile with this setting:

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

With this change, AnyConnect tries to reconnect when the computer is brought back from sleep. The AutoReconnectBehavior preference defaults to DisconnectOnSuspend. This behavior is different from that of AnyConnect Client Release 2.2. For reconnect after resume, the network administrator must either set ReconnectAfterResume in the profile or make the AutoReconnect and AutoReconnectBehavior preferences user controllable in the profile to allow users to set it.

Frequently Asked Questions

Q1. Anyconnect DPD has an interval but no retries - how many packets does it have to miss before it marks the remote end as dead?

A. From the client perspective, DPDs only tear down a tunnel during the tunnel establishment stage. If the client encounters three retries(sends four packets) during the tunnel establishment stage and does not recieve a response from the primary VPN server, it falls back to using one fo the back up servers if one is configured. However, once the tunnel has been established, missed DPDs do not have any impact on the tunnel from the clients perspective. The real impact of DPDs is on the VPN server as explained in the section DPDs and Inactivity Timers.

Q2. Is the DPD processing different for AnyConnect with IKEv2?

A. Yes, IKEv2 has a fixed number of retries - six retries/seven packets.

Q3. Is there another purpose for the AnyConnect Parent-Tunnel?

A. In addition to being a mapping on the ASA, the parent tunnel is used in order to push AnyConnect image upgrades from the ASA to the client, because the client is not actively connected during the upgrade process.

Q4. Can you filter and log off just inactive sessions?

A. You can filter inactive sessions with the **show vpn-sessiondb anyconnect filter inactive** command. However, there is no command to log off just inactive sessions. Instead, you need to

log off specific sessions or log off all sessions per user (index - name), protocol, or tunnel-group. An enhancement request, Cisco bug ID CSCuh55707 , has been filed in order to add the option to log off just the inactive sessions.

Q5. What happens to the Parent-Tunnel when the DTLS or TLS tunnels Idle-Timeout expires?

A. The "Idle TO Left" timer of the AnyConnect-Parent session is reset after either the SSL-Tunnel or DTLS-Tunnel is torn down. This allows the "idle-timeout" to act as a "disconnected" timeout. This effectively becomes the allowable time for the client to reconnect. If the client does not reconnect within the timer, then the Parent-Tunnel is terminated.

Q6. Why keep the session once the DPD timers have disconnected the session and why does the ASA not release the IP address?

A. The head-end has no knowledge of the client's state. In this case, the ASA waits for the client to hopefully reconnect until the session times out upon the idle timer. DPD does not kill an AnyConnect session; it merely kills the tunnel (within that session) so that the client can reestablish the tunnel. If the client does not reestablish a tunnel, the session remains until the idle timer expires.

If the concern is about sessions that are used up, set simultaneous-logins to a low value such as one. With this setting, users who have a session in the session database have their prior session deleted when they log in again.

Q7. What is the behavior if the ASA fails over from Active to Standby?

A. Initially, when the session is established, the three tunnels (Parent, SSL, and DTLS) are replicated to the Standby Unit; once the ASA fails over, the DTLS and the TLS sessions are reestablished as they are not synced to the standby unit, but any data flows through the tunnels must work without disruption after the AnyConnect session is reestablished.

SSL/DTLS sessions are not stateful, so the SSL state and sequence number are not maintained and can be quite taxing. Thus, those sessions need to be reestablished from scratch, which is done with the Parent session and the session token.

> **Tip**: In the event of a failover event, SSL VPN client sessions are not carried over to the standby device if keepalives are disabled.

Q8. Why are there two different timeouts, the idle timeout and the disconnected timeout, if they are both the same value?

A. When the protocols were developed, two different timeouts were provided for:

- Idle timeout - The idle timeout is for when no data is passed over a connection.
- Disconnected timeout - The disconnected timeout is for when you give up the VPN session because the connection has been lost and cannot be re-established.

The disconnected timeout was never implemented on the ASA. Instead, the ASA sends the idle timeout value for both the idle and disconnected timeouts to the client.

The client does not use the idle timeout, because the ASA handles the idle timeout. The client uses the disconnected timeout value, which is the same as the idle timeout value, in order to know when to give up reconnect attempts since the ASA has dropped the session.

While not actively connected to the client, the ASA times out the session via the idle timeout. The primary reason to not implement the disconnected timeout on the ASA was to avoid the addition of another timer for every VPN session and the increase in overhead on the ASA (although the same timer could be used in both instances, just with different timeout values, since the two cases are mutually exclusive).

The only value added with the disconnected timeout is to allow an administrator to specify a different timeout for when the client is not actively connected versus idle. As noted earlier, Cisco bug ID CSCsl52873 has been filed for this.

Q9. What happens when the client machine is suspended?

A. By default, AnyConnect does attempt to re-establish a VPN connection when you lose connectivity. It does not attempt to re-establish a VPN connection after a system resume by default. Refer to AnyConnect Client Behavior in Case of System Suspend for details.

Q10. When a reconnect happens, does the AnyConnect Virtual Adapter flap or does the routing table change at all?

A. A tunnel-level reconnect does not do either. This is a reconnect on just SSL or DTLS. These go about 30 seconds before they give up. If DTLS fails, it is just dropped. If SSL fails, it causes a session-level reconnect. A session-level reconnect completely redo the routing. If the client address assigned on the reconnect, or any other configuration parameters that impact the Virtual Adapter (VA), have not changed, then the VA is not disabled. While it is unlikely to have any change in the configuration parameters received from the ASA, it is possible that a change in the physical interface used for the VPN connection (for example, if you undock and go from wired to WiFi) could result in a different Maximum Transmission Unit (MTU) value for the VPN connection. The MTU value impacts the VA, and a change to it causes the VA to be disabled and then re-enabled.

Q11. Does the “Auto Reconnect” provide Session Persistence? If so, is there any extra functionality added in the AnyConnect Client?

A. AnyConnect does not provide any extra "magic" to accommodate session persistence for applications. But VPN connectivity is restored automatically shortly after network connectivity to the secure gateway resumes, provided the idle and session timeouts configured on the ASA have not expired. And unlike the IPsec client, the automatic reconnect results in the same client IP address. While AnyConnect attempts to reconnect, the AnyConnect Virtual Adapter remains enabled and in the connected state, so the client IP address remains present and enabled on the client PC the entire time, which gives client IP address persistence. The client PC applications, however, still perceive the loss of connectivity to their servers on the enterprise network if it takes too long for VPN connectivity to be restored.

Q12. This feature works on all variants of Microsoft Windows (Vista 32-bit & 64-bit, XP). How about the Macintosh? Does it work on OS X 10.4?

A. This feature does work on Mac and Linux. There have been issues with Mac and Linux, but recent improvements have been made, particularly for the Mac. Linux still requires some additional support (Cisco bug ID CSCsr16670, Cisco bug ID CSCsm69213), but the basic functionality is there as well. With regards to Linux, AnyConnect does not recognize that a suspend/resume (sleep/wake) has occurred. This basically has two impacts:

- The AutoReconnectBehavior profile/preference setting cannot be supported on Linux without suspend/resume support, so a reconnect always occurs after suspend/resume.
- On Microsoft Windows and Macintosh, the reconnects are immediately performed at the session level after resume, which allows for a quicker switch to a different physical interface. On Linux, because AnyConnect is completely unaware of the suspend/resume, the reconnects take place at the tunnel-level first (SSL and DTLS) and this can mean the reconnects take slightly longer. But the reconnects still occur on Linux.

Q13. Are there any limitations to the feature in terms of connectivity (Wired, wi-fi, 3G and so on)? Does it support transition from one mode to another (from Wi-Fi to 3G, 3G to wired, and so on)?

A. AnyConnect is not tied to a particular physical interface for the life of the VPN connection. If the physical interface used for the VPN connection is lost or if reconnect attempts over it exceed a certain failure threshold, then AnyConnect no longer uses that interface and attempt to reach the secure gateway with whatever interfaces are available until the idle or session timers expire. Note that a change in physical interface could result in a different MTU value for the VA, which cause the VA to have to be disabled and re-enabled, but still with the same client IP address.

If there is any network disruption (interface down, changed networks, changed interfaces), AnyConnect tries to reconnect; no re-authentication is needed on reconnect. This even applies to a switch of physical interfaces:

Example:

```
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
```

Q14. How is the resume operation authenticated?

A. In a resume, you resubmit the authenticated token that remains for the lifetime of the session, and the session is then re-established.

Q15. Is LDAP authorization also performed upon reconnect or only the authentication?

A. This is only performed in the initial connection.

Q16. Does pre-login and/or hostscan run upon resume?

A. No, these run on the initial connection only. Something like this would be slated for the future Periodic Posture Assessment feature.

Q17. With respect to VPN Load Balancing (LB) and connection resume, does the client connect back directly to the cluster member it was connected to before?

A: Yes, this is correct since you do not re-resolve the hostname via DNS for re-estblishment of a current session.

Related Information

- **ASA DPD Reference: Cisco bug ID CSCsr63074 - DPD not sent when peer is dead & tunnel not idle on s2s with 7.2.4**
- **Technical Support & Documentation - Cisco Systems**