Häufig gestellte Fragen zu AnyConnect beantworten - Tunnel, DPDs und Inaktivitäts-Timer

Inhalt

Einleitung

In diesem Dokument werden die Cisco AnyConnect Secure Mobility Client-Tunnel, das Wiederherstellungsverhalten, die Dead Peer Detection (DPD) und der Inaktivitäts-Timer beschrieben.

Hintergrundinformationen

Tunneltypen

Es gibt zwei Methoden, um eine AnyConnect-Sitzung zu verbinden:

- Über das Portal (ohne Client)
- Über die Standalone-Anwendung

Je nach Verbindungsart erstellen Sie auf der Cisco Adaptive Security Appliance (ASA) drei verschiedene Tunnel (Sitzungen) mit jeweils einem spezifischen Zweck:

1. Clientless oder Parent-Tunnel: Dies ist die Hauptsitzung, die in der Aushandlung erstellt wird, um das Sitzungstoken einzurichten, das erforderlich ist, wenn eine erneute Verbindung aufgrund von Netzwerkverbindungsproblemen oder Ruhezustand erforderlich ist. Je nach Verbindungsmechanismus listet die ASA die Sitzung als Clientless (Weblaunch über das Portal) oder Parent (Standalone AnyConnect) auf.

   Hinweis: Der AnyConnect-Parent stellt die Sitzung dar, wenn der Client nicht aktiv verbunden ist. Im Grunde funktioniert dies ähnlich wie ein Cookie, da es sich um einen Datenbankeintrag auf der ASA handelt, der der Verbindung von einem bestimmten Client aus zugeordnet wird. Wenn der Client in den Energiesparmodus/Ruhezustand wechselt, werden die Tunnel (Protokolle: IPsec/Internet Key Exchange (IKE)/Transport Layer Security (TLS)/Datagram Transport Layer Security (DTLS)) abgebaut. Der Parent bleibt jedoch bestehen, bis der Leerlauf-Timer oder die maximale Verbindungszeit greift. Dadurch kann der Benutzer die Verbindung wiederherstellen, ohne sich erneut zu authentifizieren.

2. Secure Sockets Layer (SSL)-Tunnel: Die SSL-Verbindung wird zuerst hergestellt, und die Daten werden über diese Verbindung weitergeleitet, während versucht wird, eine DTLS-Verbindung herzustellen. Sobald die DTLS-Verbindung hergestellt ist, sendet der Client die Pakete über die DTLS-Verbindung statt über die SSL-Verbindung. Kontrollpakete werden dagegen immer über die SSL-Verbindung gesendet.

3. DTLS-Tunnel: Wenn der DTLS-Tunnel vollständig eingerichtet ist, werden alle Daten in den DTLS-Tunnel übertragen, und der SSL-Tunnel wird nur gelegentlich für Kontrollkanalverkehr verwendet. Wenn bei UDP (User Datagram Protocol) ein Problem auftritt, wird der DTLS-Tunnel abgebaut, und alle Daten fließen wieder durch den SSL-Tunnel.

Beispielausgabe aus der ASA

Hier sehen Sie eine Beispielausgabe der beiden Verbindungsmethoden.

AnyConnect mit Verbindung per Weblaunch:

```
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 mit Verbindung über die Standalone-Anwendung:

```
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 und Inaktivitäts-Timer

Wann gilt eine Sitzung als inaktive Sitzung?

Die Sitzung gilt nur dann als inaktiv, wenn der SSL-Tunnel in der Sitzung nicht mehr vorhanden ist. Erst dann beginnt der Timer zu laufen. Daher wird jeder Sitzung ein Zeitstempel zugewiesen, aus dem hervorgeht, wann der SSL-Tunnel verworfen wurde.

```
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
```

Wann wird der SSL-Tunnel von der ASA verworfen?

Es gibt zwei Möglichkeiten, wie ein SSL-Tunnel getrennt werden kann:

1. **DPD:** DPDs werden vom Client verwendet, um einen Kommunikationsfehler zwischen dem AnyConnect-Client und dem ASA-Head-End zu erkennen. Über DPDs werden auch Ressourcen auf der ASA bereinigt. Dadurch wird sichergestellt, dass das Head-End keine Verbindungen in der Datenbank beibehält, wenn der Endpunkt nicht auf die DPD-Pings reagiert. Wenn die ASA eine DPD an den Endpunkt sendet und dieser antwortet, wird keine Aktion durchgeführt. Wenn der Endpunkt nicht reagiert, bricht die ASA nach der maximalen Anzahl an erneuten Übertragungen (es hängt davon ab, ob IKEv1 oder IKEv2 verwendet wird) den Tunnel in der Sitzungsdatenbank ab und verschiebt die Sitzung in den Modus "Warten auf Wiederaufnahme". Dies bedeutet, dass DPD vom Head-End gestartet wurde und das Head-End nicht mehr mit dem Client kommuniziert. In diesen Situationen erhält die ASA den Parent-Tunnel aufrecht, damit der Benutzer das Netzwerk-Roaming nutzen, in den Ruhezustand wechseln und die Sitzung wiederherstellen kann. Diese Sitzungen zählen zu

den aktiv verbundenen Sitzungen und werden unter folgenden Bedingungen gelöscht: Zeitüberschreitung wegen BenutzerinaktivitätDer Client nimmt die ursprüngliche Sitzung wieder auf und führt eine ordnungsgemäße Abmeldung durch.
Um DPDs zu konfigurieren, verwenden Sie die **anyconnect dpd-interval** unter den WebVPN-Attributen in den Gruppenrichtlinieneinstellungen. Standardmäßig ist DPD aktiviert und für die ASA (Gateway) und den Client auf jeweils 30 Sekunden festgelegt.

Achtung: Beachten Sie die Cisco Bug-ID CSCts66926 - DPD terminiert den DTLS-Tunnel nach dem Verlust der Client-Verbindung nicht.

2. **Leerlaufzeitüberschreitung:** Die zweite Möglichkeit zur Trennung des SSL-Tunnels ist das Ablaufen der Leerlaufzeitüberschreitung für diesen Tunnel. Beachten Sie jedoch, dass nicht nur der SSL-Tunnel inaktiv sein muss, sondern auch der DTLS-Tunnel. Sofern die DTLS-Sitzung nicht abläuft, wird der SSL-Tunnel in der Datenbank beibehalten.

Warum müssen Keep-Alives aktiviert werden, wenn DPDs bereits aktiviert sind?

Wie bereits erläutert, beendet DPD die AnyConnect-Sitzung an sich nicht. Es trennt lediglich den Tunnel innerhalb dieser Sitzung, damit der Client den Tunnel erneut herstellen kann. Wenn der Client den Tunnel nicht erneut herstellen kann, bleibt die Sitzung bestehen, bis der Leerlauf-Timer auf der ASA abläuft. Da DPDs standardmäßig aktiviert sind, kann die Verbindung zu Clients aufgrund von Datenflüssen, die sich mit Network Address Translation (NAT), Firewall- und Proxy-Geräten in eine Richtung schließen, oft getrennt werden. Sie können dies verhindern, indem Sie Keep-Alives in kurzen Intervallen (z. B. 20 Sekunden) aktivieren.

Keepalives werden unter den WebVPN-Attributen einer bestimmten Gruppenrichtlinie mit dem **anyconnect ssl keepalive** aus. Standardmäßig sind die Timer auf 20 Sekunden eingestellt.

AnyConnect-Client-Verhalten im Falle einer Wiederverbindung

AnyConnect versucht, die Verbindung wiederherzustellen, wenn die Verbindung unterbrochen wird. Dies ist nicht konfigurierbar, sondern erfolgt automatisch. Solange die VPN-Sitzung auf der ASA gültig ist und AnyConnect die physische Verbindung wiederherstellen kann, wird die VPN-Sitzung wieder aufgenommen.

Die Funktion für die Wiederverbindung wird fortgesetzt, bis die Sitzungszeitüberschreitung oder die Trennungszeitüberschreitung (eigentlich die Leerlaufzeitüberschreitung) abläuft (oder 30 Minuten lang, wenn keine Zeitüberschreitungen konfiguriert sind). Sobald diese ablaufen, kann der Client nicht mehr fortfahren, da die VPN-Sitzungen auf der ASA bereits abgebrochen wurden. Der Client setzt den Vorgang fort, solange er glaubt, dass die ASA noch über eine VPN-Sitzung verfügt.

AnyConnect stellt unabhängig von den Änderungen an der Netzwerkschnittstelle erneut eine Verbindung her. Es spielt keine Rolle, ob sich die IP-Adresse der Netzwerkschnittstellenkarte (Network Interface Card, NIC) ändert oder ob die Verbindung von einer NIC zu einer anderen NIC (Wireless zu kabelgebunden oder umgekehrt) wechselt.

Für den Wiederverbindungsprozess bei AnyConnect sind drei Sitzungsebenen wichtig. Das Wiederverbindungsverhalten der einzelnen Sitzungen ist lose gekoppelt, sodass jede Sitzung ohne Abhängigkeit von den Sitzungselementen der vorherigen Ebene wiederhergestellt werden

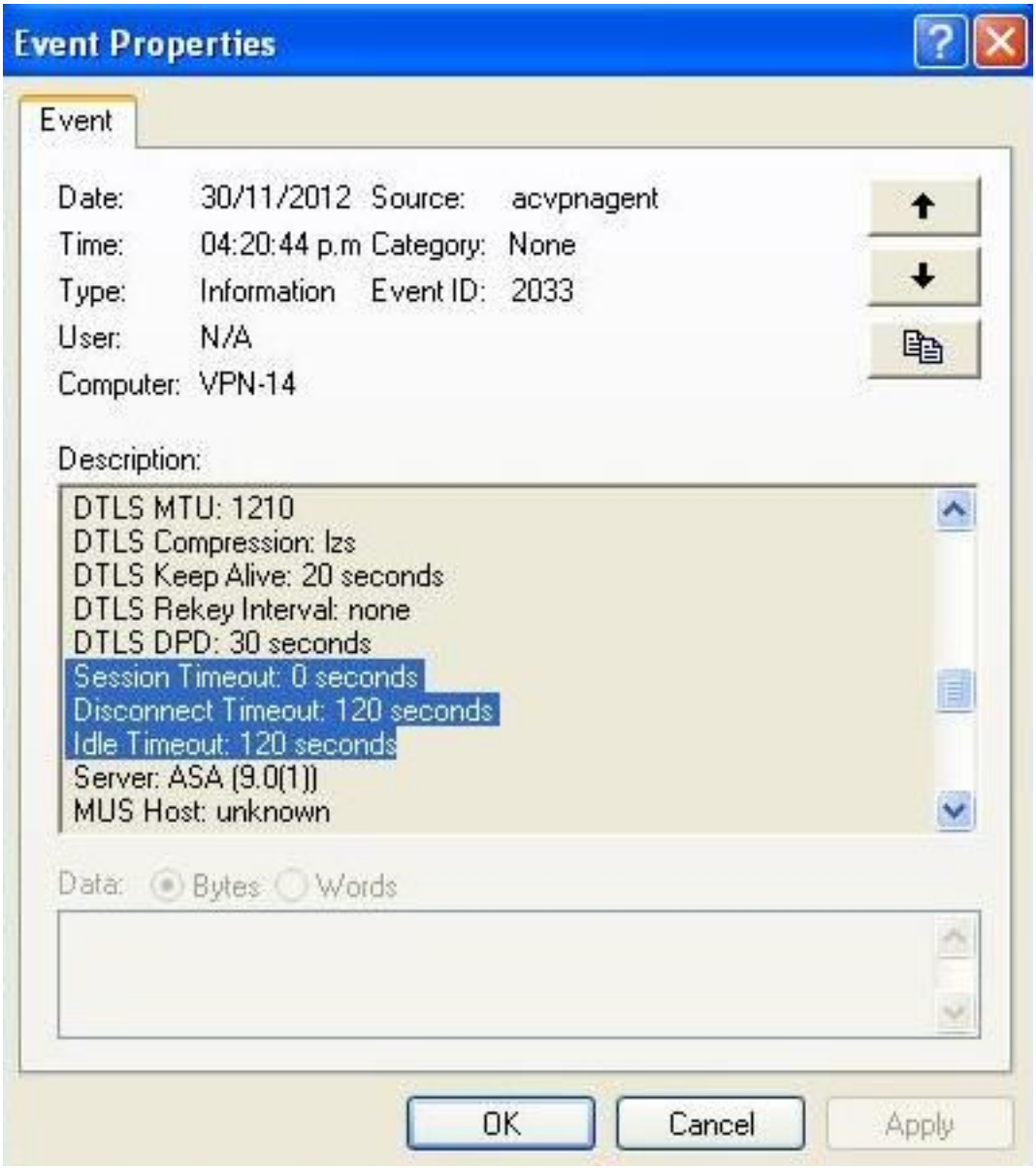
kann:

1. TCP- oder UDP-Wiederverbindung [OSI-Schicht 3]
2. TLS, DTLS oder IPsec (IKE+ESP) [OSI-Schicht 4]: TLS-Fortsetzung wird nicht unterstützt.
3. VPN [OSI-Schicht 7]: Das VPN-Sitzungstoken wird als Authentifizierungstoken verwendet, um die VPN-Sitzung bei einer Unterbrechung über einen geschützten Kanal wiederherzustellen. Es handelt sich um einen proprietären Mechanismus, der konzeptionell der Verwendung eines Kerberos-Tokens oder eines Client-Zertifikats für die Authentifizierung ähnelt. Das Token ist eindeutig und wird kryptografisch vom Head-End generiert, das die Sitzungs-ID und eine kryptografisch generierte zufällige Nutzlast enthält. Es wird im Rahmen der anfänglichen VPN-Einrichtung an den Client weitergegeben, nachdem ein sicherer Kanal zum Head-End eingerichtet wurde. Es bleibt während der gesamten Dauer der Sitzung auf dem Head-End gültig und wird im Arbeitsspeicher des Clients gespeichert. Dies ist ein Prozess mit höheren Berechtigungen.
   Tipp: Diese und neuere ASA-Versionen enthalten ein kryptografisches Sitzungstoken mit höherer Stabilität: 9.1(3) und 8.4(7.1)

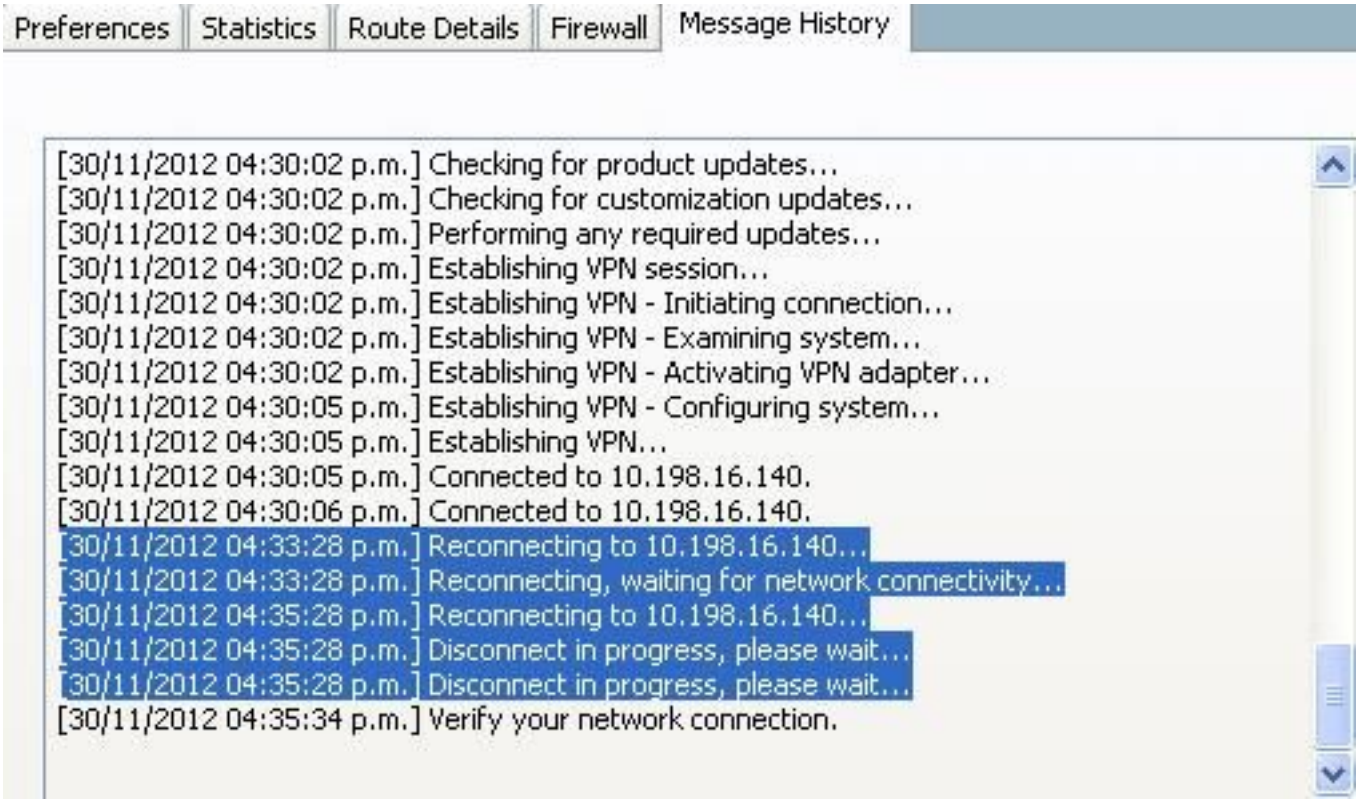
Der tatsächliche Prozess

Bei Unterbrechung der Netzwerkverbindung wird sofort ein Timer für die Trennungszeitüberschreitung gestartet. Der AnyConnect-Client versucht weiterhin, die Verbindung wiederherzustellen, solange dieser Timer nicht abläuft. Die Trennungszeitüberschreitung wird entweder auf die **Leerlaufzeitüberschreitung** aus der Gruppenrichtlinie oder auf die **maximale Verbindungszeit** festgelegt – je nachdem, welcher Wert niedriger ist.

Der Wert dieses Timers wird in der Ereignisanzeige für die AnyConnect-Sitzung in der Aushandlung angezeigt:



In diesem Beispiel wird die Sitzung nach zwei Minuten (120 Sekunden) getrennt. Dies kann im Nachrichtenverlauf des AnyConnect überprüft werden:



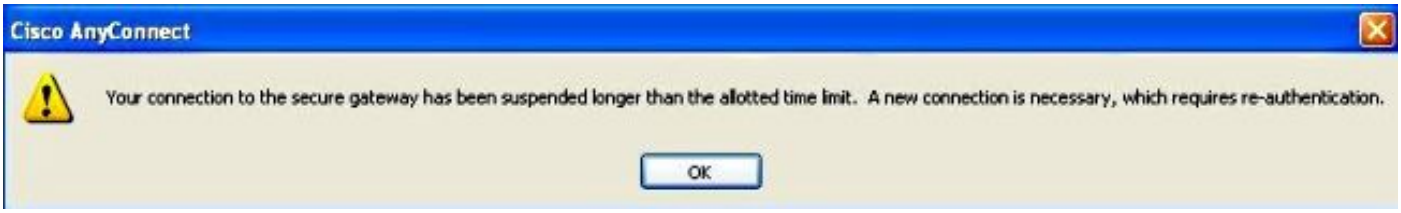
Tipp: Damit die ASA auf einen Client antworten kann, der versucht, die Verbindung wiederherzustellen, muss die Parent-Tunnel-Sitzung weiterhin in der ASA-Datenbank vorhanden sein. Im Falle eines Failovers müssen auch DPDs aktiviert werden, damit das Wiederverbindungsverhalten funktioniert.

Wie aus den vorherigen Meldungen hervorgeht, ist der Wiederverbindungsversuch fehlgeschlagen. Wenn die Wiederverbindung jedoch erfolgreich ist, geschieht Folgendes:

1. Der Parent-Tunnel bleibt derselbe; dies wird nicht neu verhandelt, da dieser Tunnel das Sitzungstoken beibehält, das für die Sitzung erforderlich ist, um die Verbindung wiederherzustellen.
2. Neue SSL- und DTLS-Sitzungen werden generiert, und beim Wiederverbinden werden andere Quellports verwendet.
3. Alle Leerlaufzeitüberschreitungswerte werden wiederhergestellt.
4. Die Inaktivitätszeitüberschreitung wird wiederhergestellt.

Vorsicht: Beachten Sie die Cisco Bug-ID CSCtg33110. Von der VPN-Sitzungsdatenbank wird die öffentliche IP-Adresse in der ASA-Sitzungsdatenbank nicht aktualisiert, wenn AnyConnect die Verbindung wiederherstellt.

In dieser Situation, in der die Wiederverbindungsversuche fehlschlagen, wird folgende Meldung angezeigt:



Hinweis: Diese Erweiterungsanfrage wurde eingereicht, um das Ganze noch detaillierter zu gestalten: Cisco Bug-ID CSCsl52873 - ASA hat keinen konfigurierbaren, getrennten Timeout für AnyConnect.

AnyConnect-Client-Verhalten bei Systemaussetzung

Es gibt eine Roaming-Funktion, die es AnyConnect ermöglicht, nach einem Ruhezustand des PC die Verbindung wiederherzustellen. Der Client versucht es weiter, bis die Leerlauf- oder Sitzungszeitüberschreitung abläuft. Der Tunnel wird nicht sofort abgebaut, wenn das System in den Ruhezustand/ins Standby wechselt. Für Benutzer, die diese Funktion nicht benötigen, legen Sie den Wert für das Sitzungs-Timeout auf einen niedrigen Wert fest, um zu verhindern, dass die Verbindung im Standby-Modus wieder aufgenommen wird.

Hinweis: Nach der Behebung des Cisco Bug-ID CSCso17627 (Version 2.3(111)+) wurde ein Kontrollknopf eingeführt, um diese erneute Verbindung bei der Wiederaufnahme zu deaktivieren.

Das automatischen Wiederverbinden bei AnyConnect kann über das AnyConnect-XML-Profil mit dieser Einstellung gesteuert werden:

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

Mit dieser Änderung versucht AnyConnect, die Verbindung wiederherzustellen, sobald der Computer wieder in den Ruhemodus versetzt wird. Die Einstellung unter „AutoReconnectBehavior“ (Automatisches Wiederverbindungsverhalten) lautet standardmäßig „DisconnectOnSuspend“ (Beim Aussetzen trennen). Dieses Verhalten unterscheidet sich von AnyConnect-Client Version 2.2. Für die Wiederverbindung nach dem Fortsetzen muss der Netzwerkadministrator entweder „ReconnectAfterResume“ (Nach Fortsetzen Verbindung wiederherstellen) im Profil festlegen oder die Einstellungen für „AutoReconnect“ (Automatische Wiederverbindung) und „AutoReconnectBehavior“ (Automatisches Wiederverbindungsverhalten) im Profil als steuerbar festlegen, damit Benutzer sie festlegen können.

Häufig gestellte Fragen

Frage 1: AnyConnect DPD hat ein Intervall, aber keine Wiederholungsversuche. Wie viele Pakete muss es verpassen, bevor es das Remote-Ende als inaktiv markiert?

Antwort: Aus Sicht des Kunden reißen DPDs einen Tunnel nur während der Tunneleinrichtung ab. Wenn der Client während der Tunnel-Einrichtungsphase auf drei Wiederholungen (vier Pakete sendet) stößt und keine Antwort vom primären VPN-Server erhält, greift er auf einen der Backup-Server zurück, sofern dieser konfiguriert ist. Sobald der Tunnel jedoch eingerichtet ist, haben verpasste DPDs aus Kundensicht keine Auswirkungen mehr auf den Tunnel. Die tatsächlichen Auswirkungen von DPDs betreffen den VPN-Server, wie im Abschnitt DPDs und Inaktivitäts-Timer erläutert.

Frage 2: Gibt es einen Unterschied bei der DPD-Verarbeitung für AnyConnect mit

IKEv2?

Antwort: Ja, IKEv2 hat eine feste Anzahl von Wiederholungen - sechs Wiederholungen/sieben Pakete.

Frage 3: Gibt es einen anderen Zweck für den AnyConnect-Parent-Tunnel?

Antwort: Der Parent-Tunnel ist nicht nur eine Zuordnung auf der ASA, sondern wird auch verwendet, um AnyConnect-Image-Upgrades von der ASA auf den Client zu übertragen, da der Client während des Upgrade-Prozesses nicht aktiv verbunden ist.

Frage 4: Ist es möglich, nur inaktive Sitzungen herauszufiltern und sich nur von diesen abzumelden?

A. Sie können inaktive Sitzungen mit dem Befehl **show vpn-sessiondb anyconnect filter inactive** filtern. Es gibt jedoch keinen Befehl zum Abmelden nur von den inaktiven Sitzungen. Stattdessen müssen Sie entweder die Sitzungen einzeln oder alle Sitzungen pro Benutzer (Index – Name), Protokoll oder Tunnelgruppe abmelden. Verbesserungsvorschlag (Cisco Bug-ID CSCuh55707) wurde eingereicht, um die Option hinzuzufügen, sich nur von den inaktiven Sitzungen abzumelden.

Frage 5: Was passiert mit dem Parent-Tunnel, wenn die Leerlaufzeitüberschreitung des DTLS- oder TLS-Tunnels abläuft?

A. Der Timer "Idle TO Left" der AnyConnect-Parent-Sitzung wird zurückgesetzt, nachdem entweder der SSL-Tunnel oder der DTLS-Tunnel deaktiviert wurde. Dadurch kann die Leerlaufzeitüberschreitung als Trennungszeitüberschreitung fungieren. Dies wird effektiv zur zulässigen Zeit für die Wiederverbindung des Clients. Wenn der Client die Verbindung nicht innerhalb des Timers wiederherstellt, wird der Parent-Tunnel beendet.

Frage 6: Warum sollte die Sitzung beibehalten werden, nachdem die DPD-Timer die Sitzung getrennt haben, und warum gibt die ASA die IP-Adresse nicht frei?

A. Das Headend hat keine Kenntnis vom Zustand des Kunden. In diesem Fall erwartet die ASA, dass der Client die Verbindung wiederherstellt, bis die Sitzung nach dem Leerlauf-Timer abläuft. Die DPD beendet keine AnyConnect-Sitzung, sondern nur den Tunnel (innerhalb dieser Sitzung), sodass der Client den Tunnel wieder herstellen kann. Wenn der Client den Tunnel nicht wiederherstellen kann, bleibt die Sitzung bestehen, bis der Leerlauf-Timer abläuft.

Wenn es um verbrauchte Sitzungen geht, legen Sie für die gleichzeitige Anmeldung einen niedrigen Wert fest (z. B. 1). Mit dieser Einstellung wird die vorherige Sitzung von Benutzern mit einer Sitzung in der Sitzungsdatenbank gelöscht, wenn sie sich erneut anmelden.

Frage 7: Welches Verhalten erfolgt, wenn die ASA von aktiv auf Standby umschaltet?

A. Anfänglich werden die drei Tunnel (Parent, SSL und DTLS) bei Sitzungsaufbau in die Standby-Einheit repliziert. Nach einem Failover der ASA werden die DTLS- und TLS-Sitzungen wieder hergestellt, da sie nicht mit der Standby-Einheit synchronisiert werden. Alle Datenflüsse durch die

Tunnel müssen jedoch nach Wiederherstellung der AnyConnect-Sitzung unterbrechungsfrei funktionieren.

SSL-/DTLS-Sitzungen sind nicht zustandsbehaftet, sodass der SSL-Status und die Sequenznummer nicht verwaltet werden und eine Herausforderung sein können. Daher müssen diese Sitzungen von Grund auf neu eingerichtet werden, was mit der Parent-Sitzung und dem Sitzungstoken erfolgt.

> **Tipp:** Bei einem Failover werden SSL VPN-Client-Sitzungen nicht auf das Standby-Gerät übertragen, wenn Keepalives deaktiviert sind.

Frage 8: Warum gibt es zwei verschiedene Zeitüberschreitungen (Leerlaufzeitüberschreitung und Trennungszeitüberschreitung), wenn beide den gleichen Wert haben?

Antwort: Bei der Entwicklung der Protokolle wurden zwei verschiedene Zeitüberschreitungen bereitgestellt:

- Leerlaufzeitüberschreitung: Die Leerlaufzeitüberschreitung greift, wenn keine Daten über eine Verbindung übertragen werden.
- Trennungszeitüberschreitung: Die Trennungszeitüberschreitung greift, wenn Sie die VPN-Sitzung aufgeben, weil die Verbindung unterbrochen wurde und nicht wiederhergestellt werden kann.

Die Trennungszeitüberschreitung wurde nie auf der ASA implementiert. Stattdessen sendet die ASA den Wert für die Leerlaufzeitüberschreitung sowohl für die Leerlaufzeitüberschreitung als auch für die Trennungszeitüberschreitung an den Client.

Der Client verwendet die Leerlaufzeitüberschreitung nicht, da diese von der ASA verarbeitet wird. Der Client verwendet den Wert für die getrennte Zeitüberschreitung, der dem Wert für die Leerlaufzeitüberschreitung entspricht, um zu ermitteln, wann die Verbindungsversuche abgebrochen werden müssen, da die ASA die Sitzung abgebrochen hat.

Während die ASA nicht aktiv mit dem Client verbunden ist, wird die Sitzung über die Zeitüberschreitung bei Inaktivität beendet. Die Trennungszeitüberschreitung wurde vor allem deshalb nicht auf der ASA implementiert, um zu verhindern, dass für jede VPN-Sitzung ein weiterer Timer hinzukommt, was den Overhead auf der ASA erhöhen würde. (Es wäre jedoch möglich, denselben Timer mit unterschiedlichen Zeitüberschreitungswerten in beiden Instanzen zu nutzen, weil sich die beiden Fälle gegenseitig ausschließen.)

Der einzige Vorteil der Trennungszeitüberschreitung ist, dass Administratoren für den Fall, dass der Client nicht aktiv verbunden ist oder sich im Leerlauf befindet, eine andere Zeitüberschreitung angeben können. Wie bereits erwähnt, wurde hierfür Cisco Bug-ID CSCsl52873 eingereicht.

Frage 9: Was passiert, wenn der Client-Computer ausgesetzt wird?

A. Standardmäßig versucht AnyConnect, eine VPN-Verbindung wiederherzustellen, wenn die Verbindung unterbrochen wird. Es wird nicht versucht, eine VPN-Verbindung wiederherzustellen, wenn ein System standardmäßig fortgesetzt wurde. Weitere Informationen finden Sie unter AnyConnect-Client-Verhalten bei Systemaussetzung.

Frage 10: Wenn eine Wiederverbindung erfolgt, tritt dann beim virtuellen AnyConnect-Adapter Flapping auf? Ändert sich die Routing-Tabelle?

Antwort: Auch eine erneute Verbindung auf Tunnelebene ist nicht möglich. Es handelt sich um eine Wiederverbindung nur bei SSL oder DTLS. Bis zur Aufgabe dauert es etwa 30 Sekunden. Wenn DTLS fehlschlägt, wird es einfach verworfen. Wenn SSL fehlschlägt, führt dies zu einer Wiederverbindung auf Sitzungsebene. Bei einer erneuten Verbindung auf Sitzungsebene wird das Routing vollständig wiederhergestellt. Wenn sich die beim Wiederverbinden zugewiesene Client-Adresse und andere Konfigurationsparameter, die sich auf den virtuellen Adapter (VA) auswirken, nicht geändert haben, wird der VA nicht deaktiviert. Es ist unwahrscheinlich, dass sich die von der ASA empfangenen Konfigurationsparameter ändern. Es kann jedoch vorkommen, dass eine Änderung der für die VPN-Verbindung verwendeten physischen Schnittstelle (z. B. wenn Sie die Verbindung trennen und von einer kabelgebundenen zu einer Wi-Fi-Verbindung wechseln) zu einem abweichenden MTU-Wert (Maximum Transmission Unit) für die VPN-Verbindung führt. Der MTU-Wert wirkt sich auf den VA aus. Eine Änderung führt dazu, dass der VA deaktiviert und dann wieder aktiviert wird.

Frage 11: Ermöglicht die Funktion zur automatischen Wiederverbindung Sitzungspersistenz? Wenn ja, gibt es zusätzliche Funktionen beim AnyConnect-Client?

Antwort: AnyConnect bietet keine zusätzlichen Möglichkeiten für Sitzungspersistenz bei Anwendungen. Die VPN-Verbindung wird jedoch kurz nach Wiederaufnahme der Netzwerkverbindung zum sicheren Gateway automatisch wiederhergestellt, sofern die in der ASA konfigurierten Leerlauf- und Sitzungszeitüberschreitungen nicht abgelaufen sind. Anders als beim IPsec-Client ergibt sich beim automatischen Wiederverbinden die gleiche Client-IP-Adresse. Während AnyConnect versucht, die Verbindung wiederherzustellen, bleibt der virtuelle AnyConnect-Adapter aktiviert und verbunden, sodass die Client-IP-Adresse durchgehend auf dem Client-PC vorhanden und aktiviert bleibt, wodurch die Persistenz der Client-IP-Adresse gegeben ist. Die Client-PC-Anwendungen nehmen jedoch immer noch den Verlust der Verbindung zu ihren Servern im Unternehmensnetzwerk wahr, wenn es zu lange dauert, bis die VPN-Verbindung wiederhergestellt ist.

Frage 12: Diese Funktion wird bei allen Varianten von Microsoft Windows (Vista 32-Bit und 64-Bit, XP) unterstützt. Was ist mit Macintosh? Funktioniert dies auch unter OS X 10.4?

Antwort: Diese Funktion wird unter Mac und Linux unterstützt. Es gab Probleme mit Mac und Linux, aber kürzlich wurden Verbesserungen vorgenommen, insbesondere für Mac. Linux benötigt immer noch zusätzliche Unterstützung (Cisco Bug-ID CSCsr16670, Cisco Bug-ID CSCsm69213), aber die grundlegende Funktionalität ist ebenfalls vorhanden. In Bezug auf Linux erkennt AnyConnect nicht, dass ein Suspend/Resume (Sleep/Wake) aufgetreten ist. Dies hat im Wesentlichen zwei Auswirkungen:

- Die Profil-/Voreinstellungseinstellung "AutoReconnectBehavior" kann unter Linux nicht ohne Suspend-/Resume-Unterstützung unterstützt werden. Daher erfolgt eine erneute Verbindung immer nach Suspend/Resume.
- Unter Microsoft Windows und Macintosh erfolgt die Wiederverbindung nach dem Fortsetzen sofort auf Sitzungsebene, was einen schnelleren Wechsel zu einer anderen physischen Schnittstelle ermöglicht. Da AnyConnect unter Linux den Suspend/Resume-Vorgang nicht

erkennt, werden die Verbindungen zuerst auf Tunnelebene (SSL und DTLS) neu hergestellt, was dazu führen kann, dass die erneuten Verbindungen etwas länger dauern. Aber die Verbindungen treten immer noch unter Linux auf.

Frage 13: Gibt es bei der Funktion Einschränkungen hinsichtlich der Konnektivität (Kabel, Wi-Fi, 3G usw.)? Unterstützt sie den Übergang von einem Modus in einen anderen (von Wi-Fi zu 3G, 3G zu kabelgebunden usw.)?

Antwort: AnyConnect ist während der Lebensdauer der VPN-Verbindung nicht an eine bestimmte physische Schnittstelle gebunden. Wenn die für die VPN-Verbindung verwendete physische Schnittstelle verloren geht oder die versuchten Neuverbindungen einen bestimmten Schwellenwert überschreiten, bei dem ein Fehler aufgetreten ist, verwendet AnyConnect diese Schnittstelle nicht mehr und versucht, das sichere Gateway über alle verfügbaren Schnittstellen zu erreichen, bis die Timer für Inaktivität oder Sitzung ablaufen. Beachten Sie, dass eine Änderung an der physischen Schnittstelle zu einem anderen MTU-Wert für die VA führen kann, was dazu führen kann, dass die VA deaktiviert und erneut aktiviert werden muss, jedoch immer noch mit derselben Client-IP-Adresse.

Bei einer Unterbrechung des Netzwerks (ausgefallene Schnittstelle, geänderte Netzwerke, geänderte Schnittstellen) versucht AnyConnect, die Verbindung wiederherzustellen. Bei einer erneuten Verbindung ist keine erneute Authentifizierung erforderlich. Dies gilt sogar bei einem Wechsel der physischen Schnittstellen:

Beispiel:

```
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
```

Frage 14: Wie wird der Fortsetzungsvorgang authentifiziert?

Antwort: In einem Lebenslauf senden Sie das authentifizierte Token, das für die Lebensdauer der Sitzung erhalten bleibt, erneut, und die Sitzung wird dann wiederhergestellt.

Frage 15: Wird die LDAP-Autorisierung auch beim Wiederverbinden oder nur bei der Authentifizierung durchgeführt?

Antwort: Dies erfolgt nur bei der Erstverbindung.

Frage 16: Wird die Voranmeldung und/oder der Host-Scan nach dem Fortsetzen ausgeführt?

Antwort: Nein, diese werden nur bei der Erstverbindung ausgeführt. Etwas in dieser Richtung wäre für die zukünftige Funktion zur regelmäßigen Statusüberprüfung vorgesehen.

Frage 17: Wird der Client beim VPN-Lastenausgleich (VPN Load Balancing, LB) und bei der Wiederherstellung der Verbindung direkt mit dem zuvor verbundenen Clustermitglied verbunden?

A: Ja, dies ist richtig, da Sie den Hostnamen nicht über DNS für die Wiederherstellung einer aktuellen Sitzung erneut auflösen.

Zugehörige Informationen

- **ASA DPD-Referenz: Cisco Bug-ID CSCsr63074 - DPD wird nicht gesendet, wenn der Peer ausgefallen ist und Tunnel nicht im Leerlauf auf s2s mit 7.2.4**
- **Technischer Support und Dokumentation für Cisco Systeme**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.