Veelgestelde vragen over AnyConnect beantwoorden - tunnels, DPD's en inactiviteitstimer

Inhoud

Inleiding

Dit document beschrijft Cisco AnyConnect Secure Mobility Client-tunnels, het gedrag bij opnieuw verbinden, DPD-detectie (Dead Peer Detection) en de inactiviteitstimer.

Achtergrondinformatie

Tunneltypes

Er zijn twee methoden gebruikt om een AnyConnect-sessie aan te sluiten:

- Via de portal (clientloos)
- Via de standalone toepassing

Op basis van de manier waarop u verbinding maakt, maakt u drie verschillende tunnels (sessies) op de Cisco adaptieve security applicatie (ASA), elk met een specifiek doel:

1. Clientless of Parent-Tunnel: Dit is de hoofdsessie die in de onderhandeling wordt gemaakt om het sessieteken in te stellen dat nodig is voor het geval er opnieuw verbinding moet worden gemaakt vanwege problemen met netwerkconnectiviteit of winterslaap. Op basis van het verbindingsmechanisme vermeldt de ASA de sessie als Clientless (Weblaunch via de portal) of Parent (Standalone AnyConnect).

   Opmerking: de AnyConnect-ouder vertegenwoordigt de sessie wanneer de client geen actieve verbinding heeft. In feite werkt het vergelijkbaar met een cookie, in die zin dat het een databasevermelding op de ASA is die toewijst aan de verbinding van een bepaalde client. Als de client slaapt/overwintert, worden de tunnels (IPsec/Internet Key Exchange (IKE)/ Transport Layer Security (TLS)/Datagram Transport Layer Security (DTLS) protocollen) afgebroken, maar de ouder blijft totdat de inactiviteitstimer of de maximale verbindingstijd van kracht wordt. Hierdoor kan de gebruiker opnieuw verbinding maken zonder opnieuw te verifiëren.

2. Secure Sockets Layer (SSL)-Tunnel: de SSL-verbinding wordt als eerste tot stand gebracht en er worden gegevens via deze verbinding doorgegeven terwijl wordt geprobeerd een DTLS-verbinding tot stand te brengen. Zodra de DTLS-verbinding tot stand is gebracht, verstuurt de client de pakketten via de DTLS-verbinding in plaats van via de SSL-verbinding. Besturingspakketten gaan daarentegen altijd over de SSL-verbinding.

3. DTLS-Tunnel: Wanneer de DTLS-Tunnel volledig tot stand is gebracht, worden alle gegevens naar de DTLS-tunnel verplaatst en wordt de SSL-Tunnel alleen gebruikt voor incidenteel verkeer van controlekanalen. Als er iets gebeurt met User Datagram Protocol (UDP), wordt de DTLS-Tunnel afgebroken en gaan alle gegevens opnieuw door de SSL-Tunnel.

Voorbeelduitvoer van ASA

Hier is voorbeelduitvoer van de twee verbindingsmethoden.

AnyConnect verbonden via webstart:

```
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 verbonden via de standalone toepassing:

```
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's en inactiviteitstimers

Wanneer wordt een sessie beschouwd als een inactieve sessie?

De sessie wordt alleen als Inactief beschouwd (en de timer begint toe te nemen) als de SSL-Tunnel niet meer bestaat in de sessie. Elke sessie is dus tijdgestempeld met de SSL-Tunnel drop-tijd.

```
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
```

Wanneer laat de ASA de SSL-Tunnel vallen?

Er zijn twee manieren waarop een SSL-Tunnel kan worden losgekoppeld:

1. **DPD** - DPDs worden door de client gebruikt om een storing in de communicatie tussen de AnyConnect-client en de ASA-head-end te detecteren. DPDs worden ook gebruikt om middelen op ASA te zuiveren. Dit zorgt ervoor dat de head-end geen verbindingen in de database houdt als het eindpunt niet reageert op de DPD pings. Als ASA een DPD naar het eindpunt verzendt en deze reageert, wordt er geen actie ondernomen. Als het eindpunt niet responsief is, scheurt de ASA na het maximale aantal heruitzendingen (dit hangt af van het gebruik van IKEv1 of IKEv2) de tunnel in de sessiedatabank en verplaatst de sessie naar de modus "Wachten om te hervatten". Wat dit betekent is dat DPD van de head-end is begonnen, en de head-end niet meer communiceert met de client. In dergelijke situaties houdt de ASA de Parent-Tunnel omhoog om de gebruiker in staat te stellen om netwerken te zwerven, naar slaap te gaan en de sessie te herstellen. Deze sessies tellen tegen actief verbonden sessies en worden onder deze voorwaarden gewist:
   Uitgangstimer voor gebruikerDe client hervat de oorspronkelijke sessie en logt de sessie correct af
   Om DPD's te configureren gebruikt u de **anyconnect dpd-interval** opdracht onder de WebVPN-

kenmerken in de instellingen voor groepsbeleid. Standaard is DPD ingeschakeld en ingesteld op 30 seconden voor zowel de ASA (gateway) als de client.

Waarschuwing: let op dat Cisco bug-id CSC66926 - DPD de DTLS-tunnel niet kan beëindigen na een verloren clientverbinding.

2. **Inactiviteitstimer** - De tweede manier waarop de SSL-Tunnel wordt losgekoppeld, is wanneer de Inactiviteitstimer voor deze tunnel vervalt. Vergeet echter niet dat niet alleen de SSL-Tunnel moet worden uitgeschakeld, maar ook de DTLS-tunnel. Tenzij de DTLS-sessietijden zijn verlopen, blijft de SSL-Tunnel behouden in de database.

Waarom moet Keepalives worden ingeschakeld als DPD's al zijn ingeschakeld?

Zoals eerder uitgelegd, doodt de DPD de AnyConnect-sessie zelf niet. Het doodt alleen de tunnel binnen die sessie zodat de klant de tunnel opnieuw kan opzetten. Als de client de tunnel niet opnieuw kan opzetten, blijft de sessie doorgaan totdat de inactiviteitstimer op de ASA verloopt. Aangezien DPD's standaard zijn ingeschakeld, kunnen clients vaak worden losgekoppeld vanwege stromen die in één richting sluiten met netwerkadresomzetting (NAT), firewall en proxyapparaten. Het inschakelen van keepalives met lage intervallen, zoals 20 seconden, helpt dit te voorkomen.

Keepalives zijn ingeschakeld onder de WebVPN-kenmerken van een bepaald groepsbeleid met de **anyconnect ssl keepalive** uit. Standaard worden de timers ingesteld op 20 seconden.

AnyConnect-clientgedrag bij opnieuw verbinden

AnyConnect probeert opnieuw verbinding te maken als de verbinding wordt onderbroken. Dit kan niet automatisch worden geconfigureerd. Zolang de VPN-sessie op de ASA nog geldig is en AnyConnect de fysieke verbinding kan herstellen, wordt de VPN-sessie hervat.

De functie voor opnieuw verbinden gaat door tot de time-out van de sessie of de time-out van de verbinding wordt verbroken, wat in feite de tijdelijke onderbreking is, verloopt (of 30 minuten als er geen time-outs zijn geconfigureerd). Wanneer deze verlopen, kan de client niet verder gaan omdat de VPN-sessies al zijn gedropt op de ASA. De client gaat verder zolang hij denkt dat de ASA nog steeds de VPN-sessie heeft.

AnyConnect maakt opnieuw verbinding, ongeacht de manier waarop de netwerkinterface verandert. Het maakt niet uit of het IP-adres van de netwerkinterfacekaart (NIC) verandert, of of als connectiviteit switches van één NIC naar een andere NIC (draadloos naar bekabeld of vice versa).

Wanneer u het proces voor het opnieuw verbinden van AnyConnect overweegt, zijn er drie sessieniveaus die u moet onthouden. Bovendien is het gedrag van elk van deze sessies losjes gekoppeld, in die zin dat elk van deze sessies opnieuw kan worden ingesteld zonder een afhankelijkheid van de sessieelementen van de vorige laag:

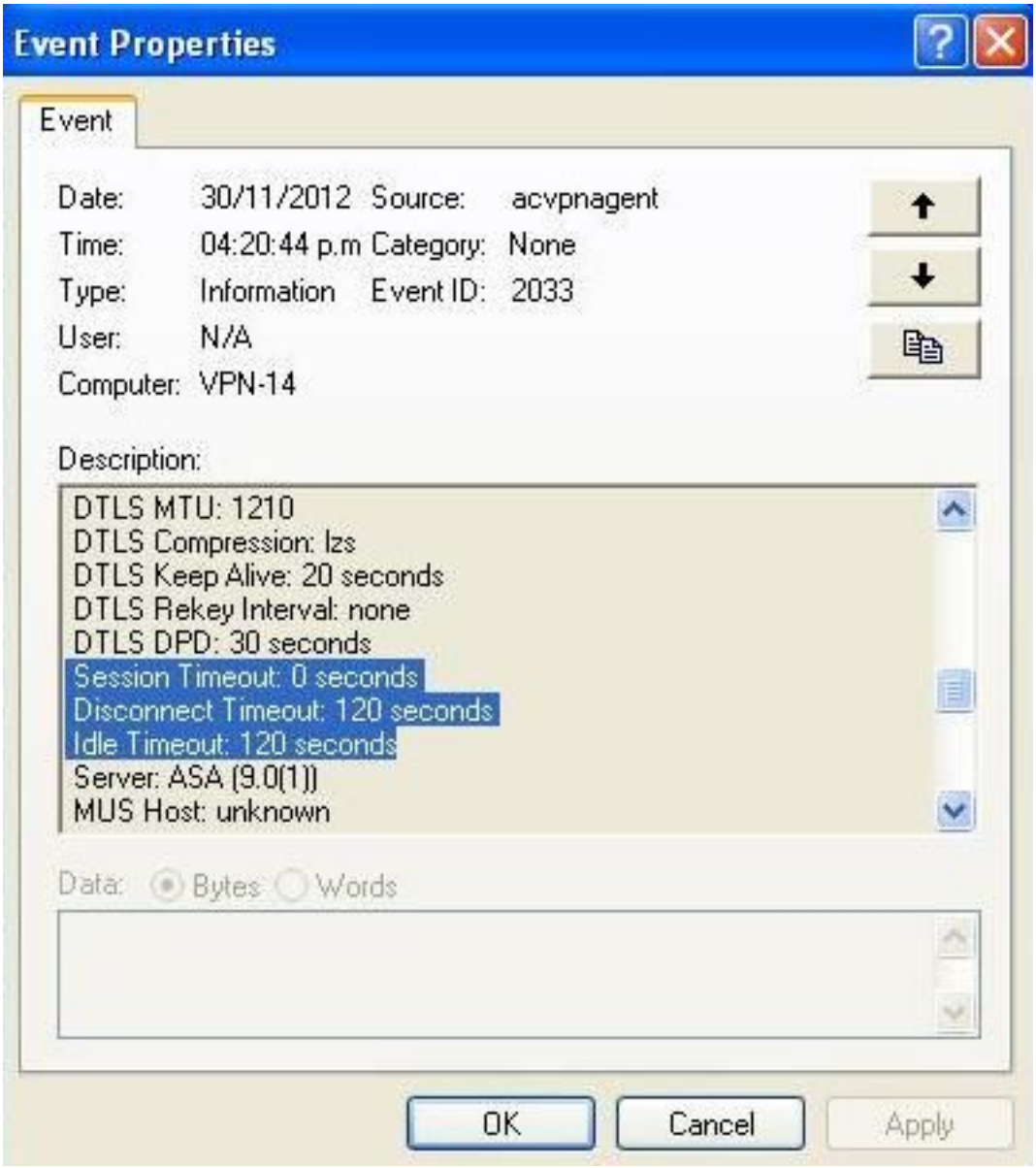
1. TCP- of UDP-verbindingen [OSI Layer 3]
2. TLS, DTLS of IPSec (IKE+ESP) [OSI Layer 4] - TLS-hervatting wordt niet ondersteund.
3. VPN [OSI Layer 7] - Het VPN-sessietoken wordt gebruikt als een verificatietoken om de VPN-sessie via een beveiligd kanaal opnieuw op te starten wanneer er sprake is van een

onderbreking. Het is een bedrijfseigen mechanisme dat conceptueel zeer vergelijkbaar is met hoe een Kerberos-token of een clientcertificaat wordt gebruikt voor verificatie. Het token is uniek en cryptografisch gegenereerd door de head-end, die de sessie-ID plus een cryptografisch gegenereerde willekeurige payload bevat. Het wordt doorgegeven aan de klant als deel van de eerste VPN-vestiging nadat een veilig kanaal naar de head-end is opgezet. Het blijft geldig voor de levensduur van de sessie op de head-end, en het wordt opgeslagen in het clientgeheugen, wat een geprivilegieerd proces is.
Tip: deze ASA releases en bevatten later een sterker cryptografisch sessietoken: 9.1(3) en 8.4(7.1)

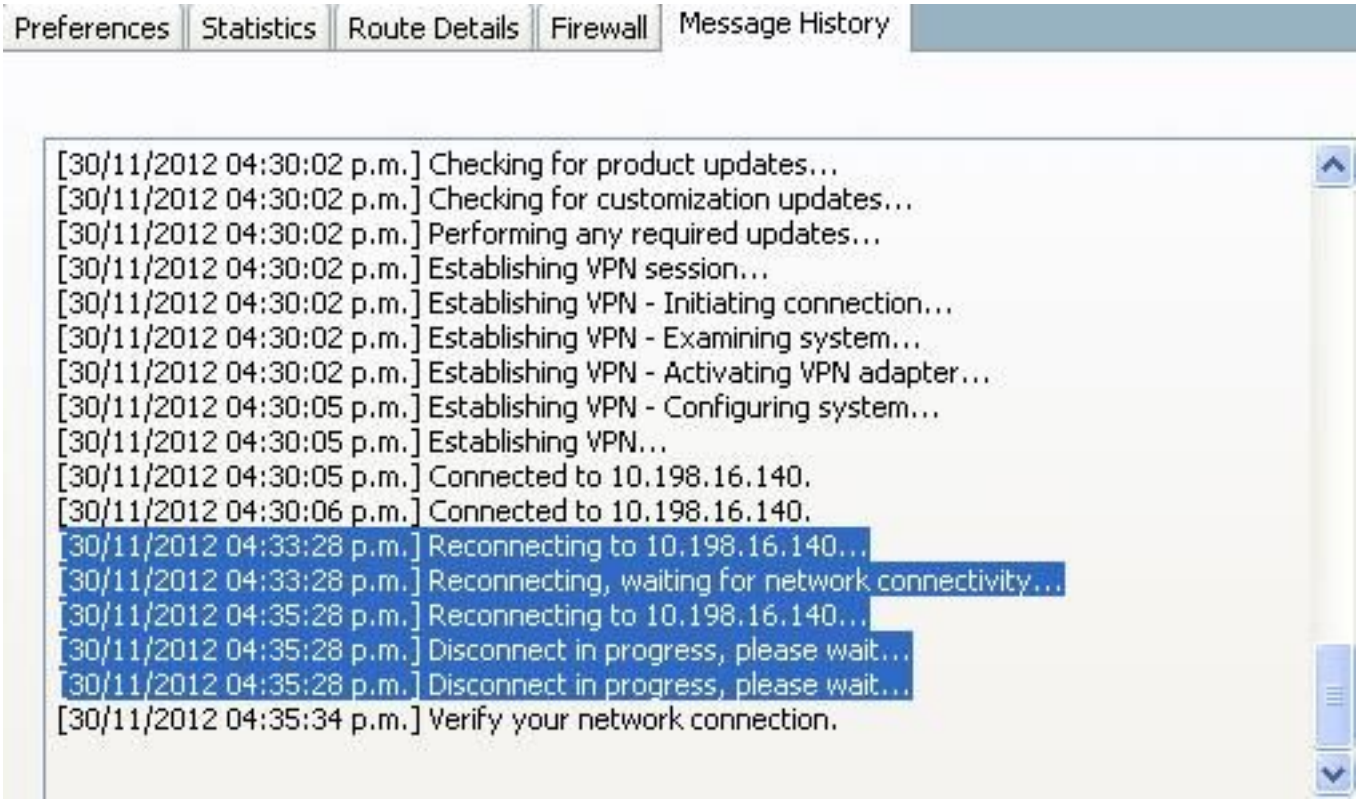
Het eigenlijke proces

Een Time-outtimer voor verbinding verbreken wordt gestart zodra de netwerkverbinding is verstoord. De AnyConnect-client blijft proberen opnieuw verbinding te maken zolang deze timer niet verloopt. De Time-out bij verbroken verbinding is ingesteld op de laagste instelling van de **inactiviteitstimer voor** groepsbeleid of de **maximale verbindingstijd**.

De waarde van deze timer wordt in het gebeurtenisvenster gezien voor de AnyConnect-sessie tijdens de onderhandeling:



In dit voorbeeld wordt de sessie na twee minuten (120 seconden) verbroken. Dit kan worden gecontroleerd in de Berichtgeschiedenis van AnyConnect:



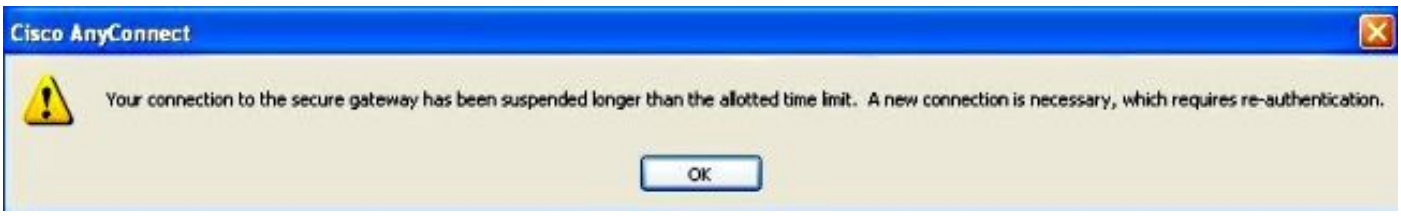
Tip: om de ASA te laten reageren op een client die probeert opnieuw verbinding te maken, moet de Parent-Tunnel sessie nog steeds bestaan in de ASA database. In het geval van failover, moeten DPDs ook worden toegelaten voor het reconnect gedrag om te werken.

Zoals in de vorige berichten wordt weergegeven, is de verbinding opnieuw verbroken. Als het opnieuw verbinden echter lukt, is hier wat er gebeurt:

1. De ouder-tunnel blijft hetzelfde; dit wordt niet opnieuw onderhandeld omdat deze tunnel het sessieteken onderhoudt dat nodig is voor de sessie om opnieuw verbinding te kunnen maken.
2. Er worden nieuwe SSL- en DTLS-sessies gegenereerd en er worden verschillende bronpoorten gebruikt bij het opnieuw verbinden.
3. Alle waarden voor de inactiviteitstimer worden hersteld.
4. De time-out voor inactiviteit wordt hersteld.

Waarschuwing: houd rekening met Cisco bug-id CSC3110. De VPN-sessiedatabase werkt het openbare IP-adres in de ASA-sessiedatabase niet bij wanneer AnyConnect opnieuw wordt verbonden.

In deze situatie, waar de pogingen om opnieuw verbinding te maken mislukken, ontmoet u dit bericht:



Opmerking: dit verzoek om versterking is ingediend om dit te verfijnen: Cisco bug-id

CSC52873 - ASA heeft geen configureerbare time-out voor AnyConnect.

AnyConnect-clientgedrag bij systeemopschorting

Er is een zwervende functie waarmee AnyConnect opnieuw verbinding kan maken na een PC-slaapstand. De client blijft proberen tot de tijdelijke onderbrekingen van de inactiviteitssessie verlopen en de client de tunnel niet onmiddellijk afbreekt wanneer het systeem overschakelt naar de slaapstand. Voor gebruikers die deze functie niet willen, stelt u de sessietime-out in op een lage waarde om te voorkomen dat de slaapstand/hervatting opnieuw wordt verbonden.

> **Opmerking**: na de oplossing van Cisco bug-id CSCso17627 (versie 2.3(11)+) is er een bedieningsknop geïntroduceerd om deze herverbinding op cv-functie uit te schakelen.

Het gedrag Auto-Reconconnect voor AnyConnect kan worden geregeld via het AnyConnect XML-profiel met deze instelling:

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

Met deze wijziging probeert AnyConnect opnieuw verbinding te maken wanneer de computer uit de slaapstand wordt gehaald. De voorkeursinstellingen voor AutoReconconnectBehavior zijn standaard ingesteld op DisconnectOnSuspend. Dit gedrag verschilt van dat van AnyConnect Client release 2.2. Als u opnieuw verbinding wilt maken nadat de procedure is hervat, moet de netwerkbeheerder de voorkeursinstellingen Herstel van de verbinding in het profiel instellen of de voorkeuren voor AutoReconconnect en AutoReconconnectBehavior in het profiel instelbaar maken, zodat gebruikers de voorkeursinstellingen kunnen instellen.

Veelgestelde vragen

V1. AnyConnect DPD heeft een interval maar probeert niet opnieuw - hoeveel pakketten moet het missen voordat het markeert het afgelegen einde als dood?

A. Vanuit het perspectief van de klant trachten DPD's alleen een tunnel af te breken tijdens de fase van de tunnelbouw. Als de client drie nieuwe pogingen (verstuurt vier pakketten) tegenkomt tijdens de fase van de tunneloprichting en geen reactie van de primaire VPN-server ontvangt, valt het terug op het gebruik van een van de back-upservers als er een is geconfigureerd. Echter, zodra de tunnel is opgezet, hebben gemiste DPD's geen invloed op de tunnel vanuit het perspectief van de klanten. De werkelijke impact van DPD's is op de VPN-server zoals uitgelegd in de sectie DPD's en Inactivity Timers.

V2. Is de DPD-verwerking anders voor AnyConnect met IKEv2?

A. Ja, IKEv2 heeft een vast aantal herhalingen - zes herhalingen/zeven pakketten.

V3. Is er een ander doel voor de AnyConnect Parent-Tunnel?

A. Naast een mapping op de ASA, wordt de oudertunnel gebruikt om AnyConnect-beeldupgrades

van de ASA naar de client te duwen, omdat de client tijdens het upgradeproces geen actieve verbinding heeft.

V4. Kan je alleen inactieve sessies filteren en afloggen?

A. U kunt inactieve sessies filteren met de **show vpn-sessiondb om het even welke verbinding filter inactieve** opdracht. Er is echter geen opdracht om alleen inactieve sessies uit te loggen. In plaats daarvan moet u specifieke sessies afmelden of alle sessies per gebruiker (index - naam), protocol of tunnelgroep afmelden. Er is een uitbreidingsaanvraag ingediend, Cisco bug-id CSC5707 , om de optie toe te voegen om alleen de inactieve sessies af te loggen.

V5. Wat gebeurt er met de parent-Tunnel wanneer de inactiviteitstimer voor DTLS- of TLS-tunnels verloopt?

A. De timer "Inactief naar links" van de AnyConnect-oudersessie wordt opnieuw ingesteld nadat de SSL-tunnel of de DTLS-tunnel is afgebroken. Hierdoor kan de "idle-timeout" dienst doen als een "disconnected" timeout. Dit wordt effectief de toegestane tijd voor de client om opnieuw verbinding te maken. Als de client niet opnieuw verbinding maakt binnen de timer, wordt de ouder-tunnel beëindigd.

V6. Waarom de sessie houden zodra de DPD timers de sessie hebben losgekoppeld en waarom geeft ASA het IP-adres niet vrij?

A. Het hoofd heeft geen kennis van de staat van de cliënt. In dit geval wacht de ASA op de client om hopelijk opnieuw verbinding te maken tot de sessietijden verlopen op de inactieve timer. DPD doodt een AnyConnect-sessie niet; het doodt alleen de tunnel (binnen die sessie), zodat de client de tunnel opnieuw kan openen. Als de client geen tunnel opnieuw maakt, blijft de sessie doorgaan tot de inactieve timer is verlopen.

Als de zorg over sessies is die worden opgebruikt, stelt u gelijktijdig inloggen in op een lage waarde zoals een. Met deze instelling, gebruikers die een sessie hebben in de sessiedatabank hebben hun eerdere sessie verwijderd wanneer ze opnieuw inloggen.

V7. Wat is het gedrag als de ASA omvalt van Active naar Standby?

A. Aanvankelijk, wanneer de sessie wordt ingesteld, worden de drie tunnels (Parent, SSL en DTLS) gerepliceerd naar de Standby-eenheid; zodra de ASA mislukt, worden de DTLS- en TLS-sessies opnieuw ingesteld, aangezien ze niet worden gesynchroniseerd naar de standby-eenheid, maar alle gegevensstromen door de tunnels moeten zonder onderbreking werken nadat de AnyConnect-sessie is hersteld.

SSL/DTLS-sessies zijn niet stateful, zodat de SSL-status en het volgnummer niet worden behouden en vrij kunnen taxeren. Dus, die sessies moeten vanaf nul worden hersteld, wat gebeurt met de oudersessie en het sessietoken.

> **Tip**: In het geval van een failover-gebeurtenis worden SSL VPN-clientsessies niet naar het stand-by apparaat overgedragen als keepalives zijn uitgeschakeld.

V8 Waarom zijn er twee verschillende timeouts, de idle timeout en de disconnected

timeout, als ze beide dezelfde waarde hebben?

A. Toen de protocollen werden ontwikkeld, waren er twee verschillende uitloopdatums voorzien:

- Inactiviteitstimer - De inactiviteitstimer wordt gebruikt als er geen gegevens via een verbinding worden doorgegeven.
- Niet-verbonden timeout - De niet-verbonden timeout is wanneer u de VPN-sessie opgeeft omdat de verbinding verloren is gegaan en niet opnieuw ingesteld kan worden.

De niet-verbonden time-out is nooit op de ASA geïmplementeerd. In plaats daarvan, verzendt ASA de nutteloze onderbrekingswaarde voor zowel de nutteloze als losgemaakte onderbrekingen naar de cliënt.

De client maakt geen gebruik van de time-out bij inactiviteit, omdat de ASA de time-out bij inactiviteit verwerkt. De client gebruikt de waarde van de afgebroken time-out, die gelijk is aan de waarde van de ongeactiveerde time-out, om te weten wanneer de pogingen tot herverbinding moeten worden opgegeven sinds de ASA de sessie heeft laten vallen.

Terwijl het niet actief verbonden is met de client, verlaat de ASA de sessie via de time-out bij inactiviteit. De belangrijkste reden om de niet-verbonden time-out op de ASA niet te implementeren was om de toevoeging van een andere timer voor elke VPN-sessie en de toename van de overheadkosten op de ASA te voorkomen (hoewel dezelfde timer in beide gevallen kan worden gebruikt, alleen met verschillende time-outwaarden, omdat de twee gevallen elkaar uitsluiten).

De enige toegevoegde waarde met de niet-verbonden time-out is dat een beheerder een andere time-out kan opgeven voor wanneer de client niet actief verbonden is ten opzichte van idle. Zoals eerder vermeld is hiervoor Cisco bug-id CSC52873 gedeponeerd.

V9. Wat gebeurt er als de client-machine is stilgezet?

A. Standaard probeert AnyConnect een VPN-verbinding opnieuw tot stand te brengen wanneer u de verbinding verliest. Het probeert niet om een VPN verbinding opnieuw tot stand te brengen nadat een systeem standaard is hervat. Raadpleeg AnyConnect-clientgedrag in het geval van systeemopschorting voor meer informatie.

V10. Wanneer er opnieuw verbinding wordt gemaakt, knippert de AnyConnect virtuele adapter of verandert de routeringstabel überhaupt?

A. Een tunnel-vlakke herverbinding doet ook niet. Dit is een herverbinding via SSL of DTLS. Deze gaan ongeveer 30 seconden voordat ze opgeven. Als DTLS mislukt, wordt deze zojuist verwijderd. Als SSL faalt, veroorzaakt het opnieuw verbinden op sessieniveau. Een sessie-niveau opnieuw verbinden volledig opnieuw de routing. Als het clientadres dat is toegewezen aan de herverbinding, of andere configuratieparameters die invloed hebben op de virtuele adapter (VA), niet zijn gewijzigd, wordt de VA niet uitgeschakeld. Hoewel het onwaarschijnlijk is dat de configuratieparameters die van de ASA zijn ontvangen, zullen veranderen, is het mogelijk dat een wijziging in de fysieke interface die wordt gebruikt voor de VPN-verbinding (bijvoorbeeld als u ontkoppelt en overschakelt van bekabeld naar WiFi) kan resulteren in een andere waarde voor de Maximum Transmission Unit (MTU) voor de VPN-verbinding. De waarde MTU beïnvloedt de VA, en een verandering in het veroorzaakt dat de VA wordt onbruikbaar gemaakt en dan re-toegelaten.

V11. Biedt "Automatisch opnieuw verbinden" sessiepersistentie? Zo ja, is er extra functionaliteit toegevoegd aan de AnyConnect-client?

A. AnyConnect biedt geen extra "magie" om sessiepersistentie voor toepassingen mogelijk te maken. Maar de connectiviteit van VPN wordt automatisch hersteld kort nadat de netwerkconnectiviteit aan de veilige gateway hervat, op voorwaarde dat de nutteloze en zittingsonderbrekingen die op ASA worden gevormd niet zijn verlopen. En anders dan bij de IPsec-client resulteert de automatische herverbinding in hetzelfde IP-adres van de client. AnyConnect probeert opnieuw verbinding te maken, maar de AnyConnect virtuele adapter blijft ingeschakeld en blijft in de verbonden staat, zodat het IP-adres van de client de hele tijd aanwezig en ingeschakeld blijft op de client-pc, waardoor het IP-adres van de client blijft behouden. De client-pc-toepassingen merken echter nog steeds het verlies van connectiviteit met hun servers op het ondernemingsnetwerk op als het te lang duurt voordat de VPN-connectiviteit is hersteld.

V12. Deze functie werkt op alle varianten van Microsoft Windows (Vista 32-bit en 64-bit, XP). En de Macintosh dan? Werkt het op OS X 10.4?

A. Deze functie werkt op Mac en Linux. Er zijn problemen geweest met Mac en Linux, maar er zijn recente verbeteringen aangebracht, met name voor de Mac. Linux vereist nog steeds enige extra ondersteuning (Cisco bug-id CSCsr1670, Cisco bug-id CSCsm69213), maar de basisfunctionaliteit is er ook. Met betrekking tot Linux, AnyConnect erkent niet dat een schorsing/hervat (slaap/wake) heeft plaatsgevonden. Dit heeft in wezen twee gevolgen:

- Het AutoReconconnectBehavior-profiel/de voorkeursinstelling kan niet worden ondersteund op Linux zonder de ondersteuning op te schorten/hervatten. Daarom wordt altijd opnieuw verbinding gemaakt nadat de verbinding is onderbroken/hervat.
- Op Microsoft Windows en Macintosh worden de herverbindingen direct na het hervatten uitgevoerd op sessieniveau, waardoor een snellere switch mogelijk is naar een andere fysische interface. Voor Linux, omdat AnyConnect zich volledig niet bewust is van de onderbreking/hervatting, vinden de heraansluitingen plaats op het tunnelniveau eerst (SSL en DTLS) en dit kan betekenen dat de heraansluitingen iets langer duren. Maar de herverbindingen vinden nog steeds plaats op Linux.

V13. Zijn er beperkingen aan de functie in termen van connectiviteit (bekabeld, wi-fi, 3G enzovoort)? Ondersteunt het de overgang van de ene modus naar de andere (van Wi-Fi naar 3G, 3G naar bekabeld, enzovoort)?

A. AnyConnect is niet gekoppeld aan een bepaalde fysieke interface tijdens de levensduur van de VPN-verbinding. Als de fysieke interface die gebruikt wordt voor de VPN-verbinding verloren is of als pogingen om opnieuw verbinding te maken over een bepaalde foutdrempel overschrijden, dan gebruikt AnyConnect die interface niet meer en probeert de beveiligde gateway te bereiken met de interfaces die beschikbaar zijn tot de inactieve of sessietimers verlopen. Merk op dat een verandering in de fysieke interface kan resulteren in een andere MTU-waarde voor de VA, waardoor de VA moet worden uitgeschakeld en opnieuw ingeschakeld, maar nog steeds met hetzelfde IP-adres van de client.

Als er sprake is van een netwerkonderbreking (interface down, gewijzigde netwerken, gewijzigde interfaces) probeert AnyConnect opnieuw verbinding te maken; bij opnieuw verbinding maken is geen opnieuw verificatie nodig. Dit is zelfs van toepassing op een switch van fysieke interfaces:

Voorbeeld:

```
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
```

V14. Hoe wordt de cv-handeling geverifieerd?

A. In een cv dient u de geverifieerde token die overblijft gedurende het leven van de sessie opnieuw in, waarna de sessie opnieuw wordt ingesteld.

V15. Wordt LDAP-autorisatie ook uitgevoerd bij opnieuw verbinden of alleen bij de verificatie?

A. Dit wordt alleen uitgevoerd bij de eerste verbinding.

V16. Werkt pre-login en/of hostscan bij hervatting?

A. Nee, deze worden alleen uitgevoerd via de eerste verbinding. Iets als dit zou worden gepland voor de toekomstige Periodic Posture Assessment functie.

V17. Met betrekking tot VPN-taakverdeling en het hervatten van de verbinding, maakt de client rechtstreeks verbinding met het clusterlid waarmee het eerder verbinding had?

A: Ja, dit is correct aangezien u de hostname niet via DNS opnieuw oplost voor het opnieuw instellen van een huidige sessie.

Gerelateerde informatie

- ASA DPD Referentie: Cisco bug-id CSCsr63074 - DPD niet verzonden wanneer peer dood is & tunnel niet inactief op s2s met 7.2.4
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.