Foire aux questions d'AnyConnect : Les tunnels, rebranchent le comportement, et le temporisateur d'inactivité

Contenu

Introduction

Ce document décrit en détail quelques points importants au sujet des tunnels de Client à mobilité sécurisé Cisco AnyConnect (AnyConnect), le comportement de rebranchement et Dead Peer Detection (DPD), et le temporisateur d'inactivité.

Informations générales

Types de tunnels

Il y a deux méthodes utilisées afin de connecter une session d'AnyConnect :

- Par l'intermédiaire du portail (sans client)
- Par l'intermédiaire de l'application autonome

Basé sur le chemin vous vous connectez, vous créez trois tunnels différents (sessions) sur l'ASA, chacun avec un but spécifique :

1. **Sans client ou Parent-tunnel :** C'est la session principale qui est créée dans la négociation afin d'installer le jeton de session qui est nécessaire au cas où un rebranchement serait dû nécessaire aux questions ou à l'hibernation de connexion réseau. Basé sur le mécanisme de connexion, l'appliance de sécurité adaptable Cisco (ASA) répertorie la session en tant que sans client (Weblaunch par l'intermédiaire du portail) ou parent (AnyConnect autonome).

   Remarque: L'AnyConnect-parent représente la session quand le client n'est pas activement connecté. En fait, cela fonctionne semblable à un Témoin, parce que c'est une entrée de base de données sur l'ASA cette trace à la connexion d'un client particulier. Si le client s'arrêtait ou des sommeils, les tunnels (IPsec/Échange de clés Internet (IKE)/protocoles Transport Layer Security de Transport Layer Security (TLS) /Datagram (DTLS)) sont démolis, mais les restes de parent jusqu'au temps de connexion de veille de temporisateur ou de maximum les prend effet. Ceci permet à l'utilisateur pour rebrancher sans authentifier à nouveau.

2. **Secure Sockets Layer (SSL) - Tunnel :** La connexion SSL est établie d'abord, et des données sont passées au-dessus de cette connexion tandis qu'elles tentent d'établir une connexion DTLS. Une fois que la connexion DTLS est établie, le client envoie les paquets par l'intermédiaire de la connexion DTLS au lieu de par l'intermédiaire de la connexion SSL. D'autre part, les paquets de contrôle passent toujours par la connexion SSL.

3. **DTLS-tunnel :** Quand le DTLS-tunnel est entièrement établi, toutes les données se déplacent

au DTLS-tunnel, et le SSL-tunnel est seulement utilisé pour le trafic occasionnel de canal de contrôle. Si quelque chose arrive au Protocole UDP (User Datagram Protocol), le DTLS-tunnel est démoli et toutes les données traversent le SSL-tunnel de nouveau.

Sortie témoin d'ASA

Voici la sortie témoin des deux méthodes de connexion.

AnyConnect s'est connecté par l'intermédiaire du Web-lancement :

```
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 s'est connecté par l'intermédiaire de l'application autonome :

```
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 et temporisateurs d'inactivité

Quand est-ce qu'une session est considérée une session inactive ?

La session est considérée inactive (et le temporisateur commence à augmenter) seulement quand le SSL-tunnel n'existe plus en session. Ainsi, chaque session est horodatée avec du temps de baisse de SSL-tunnel.

```
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
```

Quand l'ASA relâche-t-elle le SSL-tunnel ?

Il y a deux manières qu'un SSL-tunnel peut être déconnecté :

1. **DPD** - DPDs sont utilisés par le client afin de détecter une panne dans les transmissions entre le client d'AnyConnect et la tête de réseau ASA. DPDs sont également utilisés afin de nettoyer des ressources sur l'ASA. Ceci s'assure que la tête de réseau ne maintient pas des connexions dans la base de données si le point final est nonsensible aux pings DPD. Si l'ASA envoie un DPD au point final et elle répond, aucune mesure n'est prise. Si le point final n'est pas sensible, l'ASA démolit le tunnel dans la base de données de session, et entre la session dans « attendre pour reprendre » le mode. Ce que ce le moyen est que DPD de la tête de réseau a commencé, et la tête de réseau ne communique plus avec le client. Dans de telles situations, l'ASA tient le Parent-tunnel afin de permettre à l'utilisateur pour errer des

réseaux, pour aller dormir, et pour récupérer la session. Ces sessions comptent contre des sessions actif-connectées et sont effacées dans ces conditions :
User Idle TimeoutLe client reprend la session initiale et se déconnecte correctement
Afin de configurer DPDs, utilisez la commande de dpd-intervalle d'anyconnect sous les attributs de webvpn dans les configurations de stratégie de groupe. Par défaut, le DPD est activé et placé à 30 secondes pour l'ASA (passerelle) et le client.

Attention : Rendez-vous compte de l'ID de bogue Cisco CSCts66926 - DPD ne termine pas le tunnel DTLS après la connexion client perdue.

2. **Inactif-délai d'attente** - La deuxième manière que le SSL-tunnel est déconnecté est quand l'Inactif-délai d'attente pour ce tunnel expire. Cependant, souvenez-vous que c'est non seulement le SSL-tunnel qui doit tourner au ralenti, mais les DTLS percent un tunnel aussi bien. À moins que la session DTLS chronomètre, le SSL-tunnel est retenu dans la base de données.

Pourquoi le Keepalives doit-il être activé si DPDs sont déjà activés ?

Comme expliqué précédemment, le DPD ne détruit pas la session d'AnyConnect elle-même. Il détruit simplement le tunnel dans cette session de sorte que le client puisse rétablir le tunnel. Si le client ne peut pas rétablir le tunnel, la session demeure jusqu'à ce que le temporisateur de veille expire sur l'ASA. Puisque DPDs sont activés par défaut, les clients pourraient souvent obtenir en raison déconnecté des écoulements se fermant dans une direction avec des périphériques de Traduction d'adresses de réseau (NAT), de Pare-feu et de proxy. L'activation du Keepalives à bas intervalles, tels que 20 secondes, aide à empêcher ceci.

Le Keepalives est activé sous les attributs de webvpn d'une stratégie de groupe particulière avec la commande de keepalive SSL d'anyconnect. Par défaut, les temporisateurs sont placés à 20 secondes.

Le comportement de client d'AnyConnect en cas de rebranche

AnyConnect essaye de se reconnecter si la connexion est perturbée. Ce n'est pas configurable, automatiquement. Tant que la session VPN sur l'ASA est encore valide et si AnyConnect peut rétablir la connexion physique, la session VPN sera reprise.

La caractéristique de rebranchement continue jusqu'au délai d'attente de session ou le délai d'attente de débranchement, qui est réellement le délai d'attente de veille, expire (ou 30 minutes si aucun délai d'attente n'est configuré). Une fois que ceux-ci expirent, vous ne devriez pas continuer parce que l'ASA aura relâché la session VPN. Le client continuera tant que il pense que l'ASA a toujours la session VPN.

AnyConnect rebranchera n'importe comment l'interface réseau change. Il n'importe pas si l'adresse IP des modifications du network interface card (NIC), ou si la Connectivité commute d'un NIC à un autre NIC (radio à de câble ou vice versa).

Quand vous considérez le procédé de rebranchement pour AnyConnect, il y a trois niveaux des sessions que vous devez se souvenir. Supplémentaire, le comportement de rebranchement de chacune de ces sessions est légèrement connecté, du fait l'un d'entre eux peut être rétabli sans

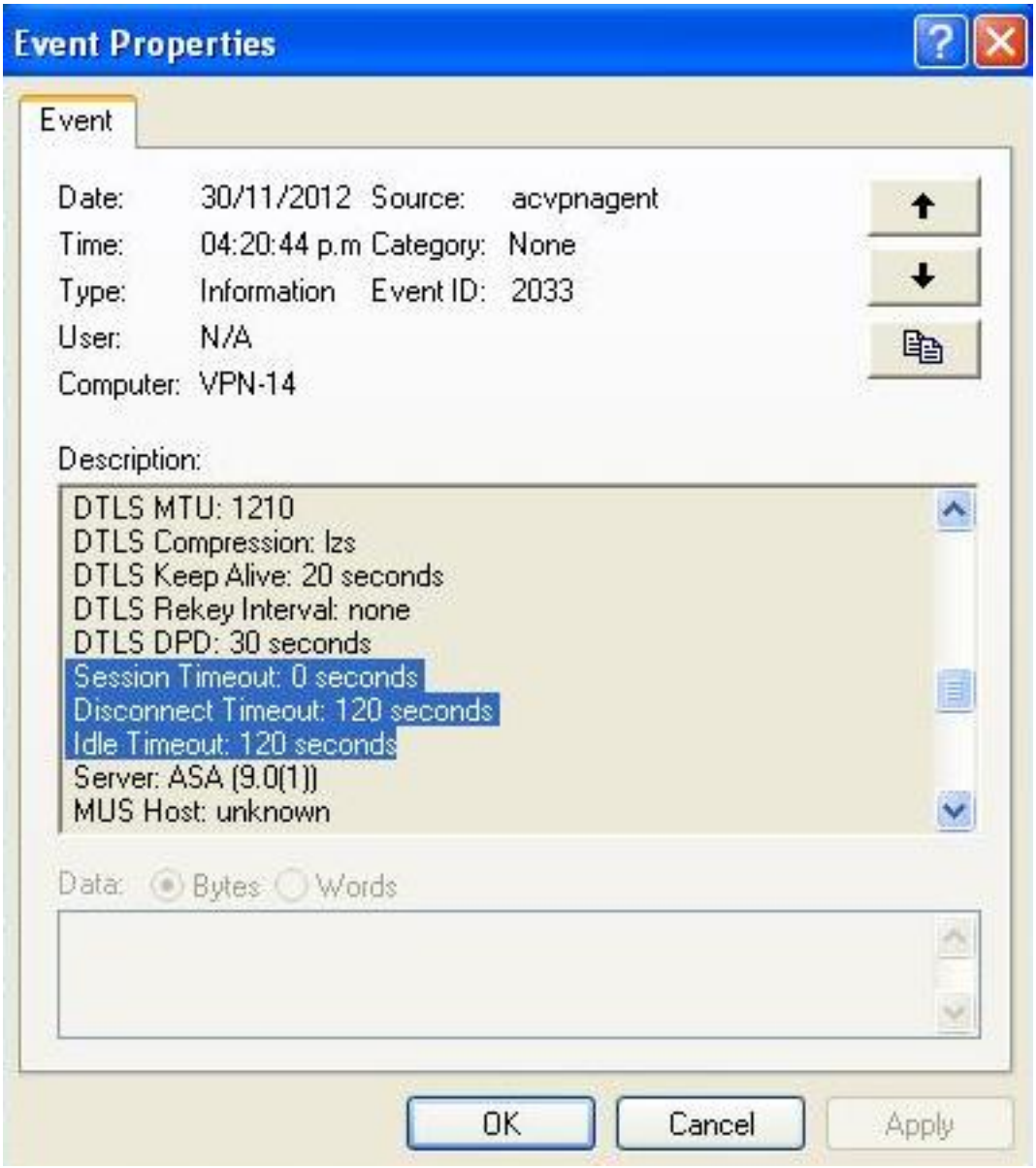
dépendance sur les éléments de session de la couche précédente :

1. Le TCP ou l'UDP rebranche [couche OSI 3]
2. TLS, DTLS, ou IPSec (IKE+ESP) [la couche OSI 4] - reprise de TLS n'est pas prise en charge.
3. VPN [couche OSI 7] - Le jeton de session VPN est utilisé car un jeton d'authentification afin de rétablir la session VPN au-dessus d'un canal sécurisé quand il y a une interruption. C'est un mécanisme de propriété industrielle qui est très semblable, conceptuellement, à la façon dont un jeton de Kerberos ou un certificat client est utilisé pour l'authentification. Le jeton est seul et cryptographiquement généré par la tête de réseau, qui contient l'ID de session plus une charge utile aléatoire cryptographiquement générée. Il est passé au client en tant qu'élément de l'établissement de l'initiale VPN après qu'un canal de sécuriser à la tête de réseau soit établi. Il reste valide pour la vie de la session sur la tête de réseau, et il est enregistré dans la mémoire de client, qui est un processus privilégié.
   Conseil : Ces releases ASA et contiennent plus tard un jeton cryptographique plus fort de session : 9.1(3) et 8.4(7.1)

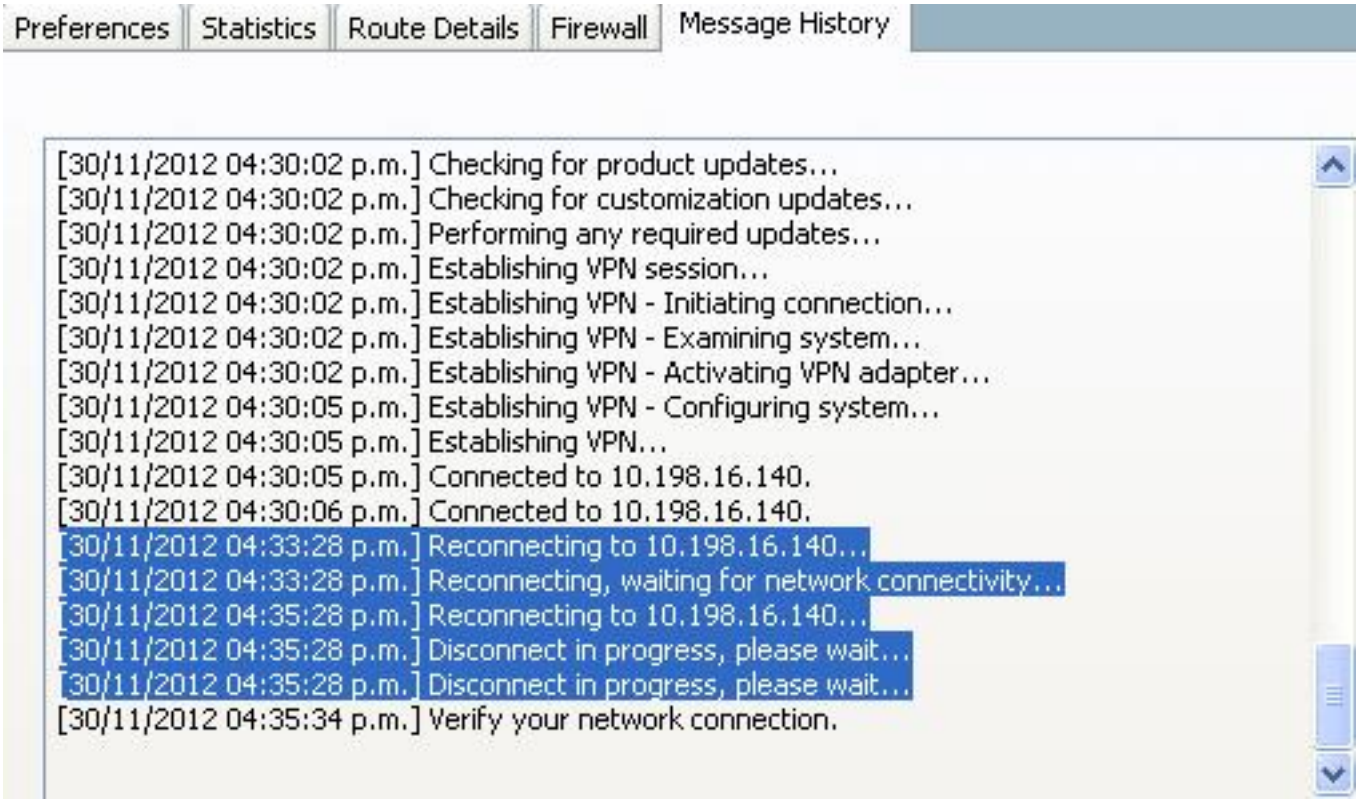
Le processus réel

Un temporisateur de délai d'attente de débranchement est démarré dès que la connexion réseau sera perturbée. Le client d'AnyConnect continue à essayer de rebrancher tant que ce temporisateur n'expire pas. Le délai d'attente de débranchement est placé à la plus basse configuration du l'Inactif-**délai d'attente de** stratégie de groupe ou du **temps de connexion maximum**.

La valeur de ce temporisateur est en cas visualiseur vu pour la session d'AnyConnect dans la négociation :



Dans cet exemple, la session devrait déconnecter après deux minutes (120 secondes), qui peuvent être signées l'historique de message de l'AnyConnect :



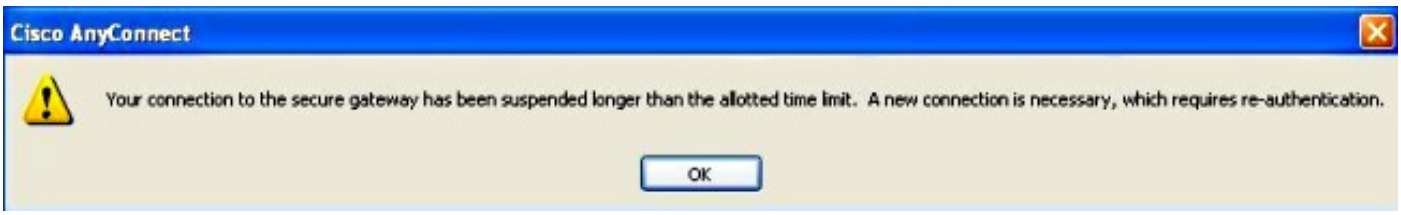
Conseil : Pour que l'ASA réponde à un client qui tente de rebrancher, la session de Parent-tunnel devrait encore exister dans la base de données ASA. En cas du Basculement, DPDs doit également être activé pour que le comportement de rebranchement fonctionne.

De même que visible des messages précédents, le rebranchement a manqué. Cependant, si le rebranchement est réussi, voici ce qui se produit :

1. Le Parent-tunnel reste le même ; ceci n'est pas renégocié parce que ce tunnel met à jour le jeton de session qui est exigé pour la session afin de rebrancher.
2. De nouvelles sessions SSL et DTLS sont générées, et différents ports de source sont utilisés dans le rebranchement.
3. Toutes les valeurs d'Inactif-délai d'attente sont restaurées.
4. La temporisation d'inactivité est restaurée.

Attention : Rendez-vous compte de l'ID de bogue Cisco CSCtg33110. La base de données de session VPN ne met pas à jour l'adresse IP publique dans la base de données de session ASA quand AnyConnect rebranche.

Dans cette situation où les tentatives de rebrancher l'échouer, vous rencontrent ce message :



Remarque: Cette demande d'amélioration a été classée afin de faire ce plus granulaire : ID de bogue Cisco CSCsl52873 - L'ASA n'a pas un délai d'attente déconnecté configurable pour AnyConnect.

Le comportement de client d'AnyConnect en cas de système s'interrompent

Il y a une caractéristique d'itinérance qui permet à AnyConnect pour rebrancher après qu'un sommeil PC. Le client continue à essayer jusqu'à l'inactif ou les délais d'attente de session expirent et le client ne démolit pas immédiatement le tunnel quand le système entre dans hibernent/standby. Pour les clients qui ne veulent pas cette caractéristique, placez le délai d'attente de session à une faible valeur afin d'empêcher le sommeil/reprise rebranche.

> Remarque: Après que la difficulté de l'ID de bogue Cisco CSCso17627 (version 2.3(111)+), un bouton de commande ait été introduite afin de désactiver ceci rebranchez sur la caractéristique de reprise.

Le comportement d'Automatique-rebranchement pour AnyConnect peut être commandé par le profil d'AnyConnect XML avec cette configuration :

```
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
```

Avec cette modification, AnyConnect essayera de rebrancher quand l'ordinateur est rapporté du sommeil. Les par défaut de préférence d'AutoReconnectBehavior à DisconnectOnSuspend. Ce comportement de routage est différent de celui d'AnyConnect client version 2,2. Pour rebranchez après reprise, l'administrateur réseau doit placer ReconnectAfterResume dans le profil ou utilisateur faire d'AutoReconnect et d'AutoReconnectBehavior préférences contrôlable dans le profil pour permettre à des utilisateurs pour le placer.

Forum aux questions

Q1. Anyconnect DPD n'a un intervalle mais aucune relance - combien de paquets doit-il manquer avant qu'il marque l'extrémité distante comme morte ?

R. Il doit manquer trois relances/quatre paquets.

Q2. Le traitement DPD est-il différent pour AnyConnect avec IKEv2 ?

R. Oui, IKEv2 a un nombre fixe de relances - six relances/sept paquets.

Q3. Y a-t-il un autre but pour le Parent-tunnel d'AnyConnect ?

A. En plus d'être un mappage sur l'ASA, le tunnel de parent est utilisé afin de pousser des mises à niveau d'image d'AnyConnect de l'ASA au client, parce que le client n'est pas activement connecté pendant le processus de mise à niveau.

Q4. Pouvez-vous filtrer et fermer une session juste des sessions inactives ?

R. Vous pouvez filtrer des sessions inactives avec la commande **inactive de filtre d'anyconnect de VPN-sessiondb d'exposition**. Cependant, il n'y a aucune commande de fermer une session juste des sessions inactives. Au lieu de cela, vous devez fermer une session des sessions spécifiques ou fermer une session toutes les sessions par utilisateur (nom de l'index), protocole, ou groupe de tunnels. Une demande d'amélioration, l'ID de bogue Cisco CSCuh55707, a été classée afin d'ajouter l'option de fermer une session juste les sessions inactives.

Q5. Qu'arrive au Parent-tunnel quand l'Inactif-délai d'attente des tunnels DTLS ou de TLS expire ?

R. Le « inactif » au temporisateur gauche de la session d'AnyConnect-parent est remis à l'état initial après que le SSL-tunnel ou le DTLS-tunnel soit démoli. Ceci permet au « inactif-délai d'attente » pour agir en tant que « a déconnecté » le délai d'attente. Ceci devient efficacement l'heure permise pour que le client rebranche. Si le client ne rebranche pas dans le temporisateur, alors le Parent-tunnel sera terminé.

Q6. Quel est le point de garder la session une fois que les temporisateurs DPD ont déconnecté la session et pourquoi l'ASA ne libère pas l'adresse IP ?

R. La tête de réseau n'a aucune connaissance de l'état de client. Dans ce cas, les attentes ASA le client à rebrancher si tout va bien jusqu'aux temps de session sur le temporisateur de veille. DPD ne détruit pas une session d'AnyConnect ; il détruit simplement le tunnel (dans cette session) de sorte que le client puisse rétablir le tunnel. Si le client ne rétablit pas un tunnel, la session demeure jusqu'à ce que le temporisateur de veille expire.

Si le souci est au sujet des sessions étant utilisées, placez les simultané-procédures de connexion à une faible valeur telle qu'une. Avec cette configuration, utilisateurs qui ont une session dans la base de données de session avoir leur session antérieure supprimée quand ils ouvrent une session de nouveau.

Q7. Quel est le comportement si l'ASA bascule de l'Active au standby ?

R. Au commencement, quand la session est établie, les trois tunnels (parent, SSL, et DTLS) sont

répliqués vers l'équipement de réserve ; une fois que l'ASA bascule, les DTLS et les sessions de TLS sont rétablis car ils pas synced à l'équipement de réserve, mais n'importe quelles données traversent les tunnels devraient fonctionner sans interruption après que la session d'AnyConnect soit rétablie.

Les sessions SSL/DTLS ne sont pas avec état, ainsi l'état et le numéro de séquence SSL ne sont pas mis à jour et peuvent tout à fait imposer. Ainsi, ces sessions doivent être à partir de zéro rétabli, qui est fait avec la session de parent et le jeton de session.

> **Conseil** : En cas d'un événement de Basculement, des sessions de client de VPN SSL ne sont pas reportées au périphérique de réserve si le Keepalives est désactivé.

Q8. Pourquoi y a-t-il deux délais d'attente différents, le délai d'attente de veille et le délai d'attente déconnecté, s'ils sont tous deux la même valeur ?

R. Quand les protocoles ont été développés, deux délais d'attente différents ont été fournis pour :

- Délai d'attente de veille - Le délai d'attente de veille est pour quand aucune donnée n'est passée au-dessus d'une connexion.
- Délai d'attente déconnecté - Le délai d'attente déconnecté est pour quand vous abandonnez la session VPN parce que la connexion a été perdue et ne peut pas être rétablie.

Le délai d'attente déconnecté n'a été jamais mis en application sur l'ASA. Au lieu de cela, l'ASA envoie la valeur du dépassement de durée de veille pour le les deux l'inactif et des délais d'attente déconnectés au client.

Le client n'utilise pas le délai d'attente de veille, parce que l'ASA manipule le délai d'attente de veille. Le client emploie la valeur du dépassement de durée déconnectée, qui est identique que la valeur du dépassement de durée de veille, afin de savoir quand abandonner rebranchent des tentatives puisque l'ASA aura relâché la session.

Tandis que pas activement connectée au client, l'ASA délai d'attente la session par l'intermédiaire du délai d'attente de veille. La raison principale de ne pas implémenter le délai d'attente déconnecté sur l'ASA était d'éviter l'ajout d'un autre temporisateur pour chaque session VPN et l'augmentation du temps système sur l'ASA (bien que le même temporisateur pourrait être utilisé dans les deux exemples, juste avec différentes valeurs du dépassement de durée, puisque les deux cas sont mutuellement - exclusivité).

Le seul à valeur ajoutée avec le délai d'attente déconnecté est de permettre à un administrateur pour spécifier un délai d'attente différent pour quand le client n'est pas activement connecté contre l'inactif. Comme remarquable plus tôt, l'ID de bogue Cisco CSCsl52873 a été classé pour ceci.

Q9. Que se produit quand la machine cliente est interrompue ?

R. Par défaut, AnyConnect tente de rétablir une connexion VPN quand vous perdez la Connectivité. Il ne tente pas de rétablir une connexion VPN après qu'une reprise de système par défaut. Référez-vous au client d'AnyConnect que le comportement en cas de système s'interrompent pour des détails.

Q10. Quand un rebranchement se produit, l'adaptateur virtuel d'AnyConnect s'agite-t-il ou la table de routage change-elle du tout ?

R. Un niveau du tunnel rebranche ne fera pas non plus. Il s'agit d'une reconnexion sur SSL ou DTLS uniquement. Ceux-ci disparaissent environ 30 secondes avant qu'ils abandonnent. Si DTLS échoue, il est juste relâché. Si le SSL échoue, il entraîne un niveau de la session rebranchent. Un niveau de la session rebranche refera complètement le routage. Si l'adresse du client assignée sur le rebranchement, ou aucun autre paramètre de configuration qui affectent l'adaptateur virtuel (VA), n'ont changé, alors le VA n'est pas désactivé. Tandis qu'il est peu probable pour avoir n'importe quel changement des paramètres de configuration reçus de l'ASA, il est possible qu'un changement de l'interface physique utilisée pour la connexion VPN (par exemple, si vous détachez et allez de câble au WiFi) pourrait avoir comme conséquence une valeur différente de Maximum Transmission Unit (MTU) pour la connexion VPN. La valeur de MTU affecte le VA, et une modification à elle cause le VA d'être désactivé et puis réactivé.

Q11. Fait ? L'automatique rebranchent ? fournissez la Persistance de session ? Si oui, y a-t-il une fonctionnalité supplémentaire ajoutée dans le client d'AnyConnect ?

A. AnyConnect ne fournit aucun « Magic » supplémentaire pour faciliter la Persistance de session pour des applications. Mais la connectivité VPN est restaurée automatiquement peu de temps après que connexion réseau aux reprises sécurisées de passerelle, si les délais d'attente d'inactif et de session configurés sur l'ASA n'ont pas expiré. Et à la différence du client d'IPsec, les automatiques rebranchent des résultats dans la même adresse IP de client. Tandis que les tentatives d'AnyConnect de rebrancher, l'adaptateur virtuel d'AnyConnect demeure activée et dans l'état connecté, ainsi l'adresse IP de client demeure le présent et activé sur le PC client le temps entier, qui donne la persistance d'adresse IP de client. Les applications de PC client, cependant, percevront vraisemblablement toujours la perte de connectivité à leurs serveurs sur le réseau d'entreprise si il prend trop long pour que la connectivité VPN soit restaurée.

Q12. Cette caractéristique travaille à toutes les variantes de Microsoft Windows (vista de 32 bits et 64-bit, XP). Que diriez-vous de Macintosh ? Fonctionne-t-cela sur l'OS X 10.4 ?

R. Cette caractéristique travaille au MAC et au Linux. Il y a eu des questions avec le MAC et le Linux, mais des améliorations récentes ont été apportées, en particulier pour le MAC. Le Linux exige toujours un certain support supplémentaire (CSCsr16670, CSCsm69213), mais la fonctionnalité de base est là aussi bien. Quant au Linux, AnyConnect n'identifiera pas qu'un interrompre/reprise (sommeil/sillage) s'est produit. Ceci a fondamentalement deux incidences :

- Le profil/configuration des préférences d'AutoReconnectBehavior ne peut pas être pris en charge sur le Linux sans s'interrompent/support de reprise, ainsi un rebranchement se produira toujours après qu'interrompiez/reprise.
- Sur Microsoft Windows et Macintosh, rebranche sont immédiatement exécutés au niveau de session après reprise, qui tient compte d'un commutateur plus rapide à une interface physique différente. Sur le Linux, parce qu'AnyConnect est complètement inconscient de l'interrompre/de reprise, rebranche aura lieu d'abord (au SSL et au DTLS) niveau du tunnel et ceci pourrait signifier que rebranche la prise légèrement plus longue. Mais rebranche se produira toujours sur le Linux.

Q13. Y a-t-il des limites à la caractéristique en termes de Connectivité (de câble, Wi-Fi, 3G et ainsi de suite) ? Prend en charge-il la transition d'un mode à l'autre (du WiFi à 3G, à 3G à de câble, et ainsi de suite) ?

A. AnyConnect n'est pas attaché à une interface physique particulière pour la vie de la connexion VPN. Si l'interface physique utilisée pour la connexion VPN est perdue ou si rebranchez les tentatives au-dessus de elle dépassent un certain seuil de panne, alors AnyConnect n'utilisera plus cette interface et la tentative d'atteindre la passerelle sécurisée avec Qu'est ce qu'interfaces sont disponibles jusqu'aux temporisateurs d'inactif ou de session expirent. Notez qu'un changement d'interface physique pourrait avoir comme conséquence une valeur différente de MTU pour le VA, qui fera devoir le VA être désactivé et réactivé, mais toujours avec la même adresse IP de client.

S'il y a n'importe quelle interruption du réseau (interface vers le bas, réseaux changés, interfaces changées), AnyConnect essayera de rebrancher ; aucune ré-authentification n'est nécessaire en fonction pour rebrancher. Ceci applique même à un commutateur des interfaces physiques :

Exemple :

```
ASA5520-C# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1336
Public IP : 172.16.250.17
Protocol : AnyConnect-Parent    <- Here just the AnyConnect-Parent is active
but not SSL-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none
Hashing : AnyConnect-Parent: (1)none
Bytes Tx : 12917 Bytes Rx : 1187
Pkts Tx : 14 Pkts Rx : 7
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 17:42:56 UTC Sat Nov 17 2012
Duration : 0h:09m:14s
Inactivity   : 0h:01m:06s          <- So the session is considered Inactive
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

Q14. Comment l'exécution de reprise est-elle authentifiée ?

R. Dans une reprise, vous resoumettez le jeton authentifié qui demeurera pour la vie de la session, et la session est alors rétablie.

Q15. L'autorisation de LDAP est-elle également exécutée au moment rebranchent-elles ou seulement l'authentification ?

R. Ceci est seulement exécuté dans la connexion initiale.

Q16. La pré-procédure de connexion et/ou le passage hostscan sur reprend-elle ?

R. Non, ceux-ci fonctionnent sur la connexion initiale seulement. N'importe quoi de pareil slated pour la future caractéristique périodique d'estimation de posture.

Q17. En ce qui concerne l'Équilibrage de charge VPN (livre) et la reprise de connexion, le client se connectera-t-il de retour directement au cluster member qu'elle a été connectée à avant ?

A : Oui, c'est correct puisque vous ne faites pas re-résolution l'adresse Internet par l'intermédiaire des DN pour re-estblishment d'une session existante.

Informations connexes

- Référence ASA DPD : ID de bogue Cisco CSCsr63074 - DPD non envoyé quand le pair est mort et tunnel non de veille sur s2s avec 7.2.4
- Support et documentation techniques - Cisco Systems