FAQ sur AnyConnect - Tunnels, DPD et minuteurs d'inactivité

Table des matières

Introduction

Ce document décrit les tunnels du client Cisco AnyConnect Secure Mobility, le comportement de reconnexion et la détection d'homologues morts (DPD), ainsi que le minuteur d'inactivité.

Informations générales

Types de tunnels

Deux méthodes sont utilisées pour connecter une session AnyConnect :

- Via le portail (sans client)
- Via l'application autonome

En fonction de la façon dont vous vous connectez, vous créez trois tunnels (sessions) différents sur le dispositif de sécurité adaptatif Cisco (ASA), chacun ayant un objectif spécifique :

1. Clientless ou Parent-Tunnel : il s'agit de la session principale qui est créée dans la négociation afin de configurer le jeton de session qui est nécessaire dans le cas où une reconnexion est nécessaire en raison de problèmes de connectivité réseau ou de mise en veille prolongée. En fonction du mécanisme de connexion, l'ASA répertorie la session comme étant sans client (lancement Web via le portail) ou parent (AnyConnect autonome).

   Remarque : AnyConnect-Parent représente la session lorsque le client n'est pas connecté activement. En effet, il fonctionne de la même manière qu'un cookie, en ce sens qu'il s'agit d'une entrée de base de données sur l'ASA qui correspond à la connexion d'un client particulier. Si le client est en veille/veille prolongée, les tunnels (protocoles IPsec/IKE (Internet Key Exchange)/TLS (Transport Layer Security)/DTLS (Datagram Transport Layer Security)) sont désactivés, mais le parent reste inactif jusqu'à ce que le minuteur d'inactivité ou le temps de connexion maximal prenne effet. Cela permet à l'utilisateur de se reconnecter sans réauthentifier.

2. Secure Sockets Layer (SSL)-Tunnel : la connexion SSL est établie en premier, et les données sont transmises sur cette connexion pendant qu'elle tente d'établir une connexion DTLS. Une fois la connexion DTLS établie, le client envoie les paquets via la connexion DTLS plutôt que via la connexion SSL. D’autre part, les paquets de contrôle passent toujours par la connexion SSL.

3. DTLS-Tunnel : lorsque le tunnel DTLS est entièrement établi, toutes les données sont transférées vers le tunnel DTLS et le tunnel SSL n'est utilisé que pour le trafic occasionnel du canal de contrôle. Si quelque chose arrive au protocole UDP (User Datagram Protocol), le tunnel DTLS est désactivé et toutes les données passent à nouveau par le tunnel SSL.

Exemple de résultats d'ASA

Voici un exemple de sortie des deux méthodes de connexion.

AnyConnect connecté via le lancement Web :

```
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 connecté via 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
```

DPD et minuteurs d'inactivité

Quand une session est-elle considérée comme inactive ?

La session est considérée comme inactive (et le compteur commence à augmenter) uniquement lorsque le tunnel SSL n'existe plus dans la session. Ainsi, chaque session est horodatée avec l'heure d'abandon du tunnel SSL.

```
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 supprime-t-il le tunnel SSL ?

Un tunnel SSL peut être déconnecté de deux façons :

1. **DPD** : les DPD sont utilisés par le client afin de détecter une défaillance dans les communications entre le client AnyConnect et la tête de réseau ASA. Les DPD sont également utilisés afin de nettoyer les ressources sur l'ASA. Cela garantit que la tête de réseau ne conserve pas les connexions dans la base de données si le point d'extrémité ne répond pas aux requêtes ping DPD. Si l'ASA envoie un DPD au point d'extrémité et qu'il répond, aucune action n'est entreprise. Si le point d'extrémité ne répond pas, après le nombre maximal de retransmissions (cela dépend si IKEv1 ou IKEv2 est utilisé), l'ASA détruit le tunnel dans la base de données de session et fait passer la session en mode « Waiting to Resume ». Cela signifie que la DPD de la tête de réseau a commencé et que cette dernière ne communique plus avec le client. Dans de telles situations, l'ASA maintient le tunnel parent actif afin de permettre à l'utilisateur d'explorer les réseaux, de se mettre en veille et de récupérer la session. Ces sessions comptent parmi les sessions connectées activement et sont effacées dans les conditions suivantes :
   Délai d'inactivité utilisateurLe client reprend la session d'origine et se déconnecte correctement
   Afin de configurer les DPD, utilisez la **anyconnect dpd-interval** sous les attributs WebVPN dans les paramètres de stratégie de groupe. Par défaut, le DPD est activé et défini sur 30 secondes pour l'ASA (passerelle) et le client.

Attention : soyez conscient du bogue Cisco ayant l'ID CSCts6926 - DPD ne parvient pas à terminer le tunnel DTLS après la perte de la connexion du client.

2. **Idle-Timeout** - La deuxième façon dont le tunnel SSL est déconnecté est quand le délai d'inactivité pour ce tunnel expire. Cependant, n'oubliez pas que ce n'est pas seulement le tunnel SSL qui doit être inactif, mais aussi le tunnel DTLS. Sauf si la session DTLS expire, le tunnel SSL est conservé dans la base de données.

Pourquoi les messages Keepalive doivent-ils être activés si les fichiers DPD sont déjà activés ?

Comme expliqué précédemment, le DPD ne ferme pas la session AnyConnect elle-même. Il tue simplement le tunnel dans cette session afin que le client puisse rétablir le tunnel. Si le client ne peut pas rétablir le tunnel, la session reste active jusqu'à ce que le minuteur d'inactivité expire sur l'ASA. Comme les DPD sont activés par défaut, les clients peuvent souvent être déconnectés en raison de flux se fermant dans une direction avec des périphériques NAT (Network Address Translation), pare-feu et proxy. L'activation de keepalives à de faibles intervalles, par exemple 20 secondes, permet d'éviter cela.

Les Keepalive sont activés sous les attributs WebVPN d'une stratégie de groupe particulière avec le **anyconnect ssl keepalive** erasecat4000_flash:. Par défaut, les minuteurs sont définis sur 20 secondes.

Comportement du client AnyConnect en cas de reconnexions

AnyConnect tente de se reconnecter si la connexion est interrompue. Ce paramètre n'est pas configurable automatiquement. Tant que la session VPN sur l'ASA est toujours valide et si AnyConnect peut rétablir la connexion physique, la session VPN est reprise.

La fonction de reconnexion se poursuit jusqu'à l'expiration du délai d'expiration de la session ou du délai de déconnexion, qui correspond en fait au délai d'inactivité (ou 30 minutes si aucun délai d'expiration n'est configuré). Une fois que ceux-ci expirent, le client ne peut pas continuer car les sessions VPN ont déjà été abandonnées sur l'ASA. Le client continue tant qu'il pense que l'ASA a toujours la session VPN.

AnyConnect se reconnecte quel que soit le changement d'interface réseau. Peu importe si l'adresse IP de la carte réseau change ou si la connectivité passe d'une carte réseau à une autre (sans fil à câblé ou vice versa).

Lorsque vous envisagez le processus de reconnexion pour AnyConnect, vous devez vous souvenir de trois niveaux de sessions. En outre, le comportement de reconnexion de chacune de ces sessions est faiblement couplé, en ce que l'une quelconque d'entre elles peut être rétablie sans dépendre des éléments de session de la couche précédente :

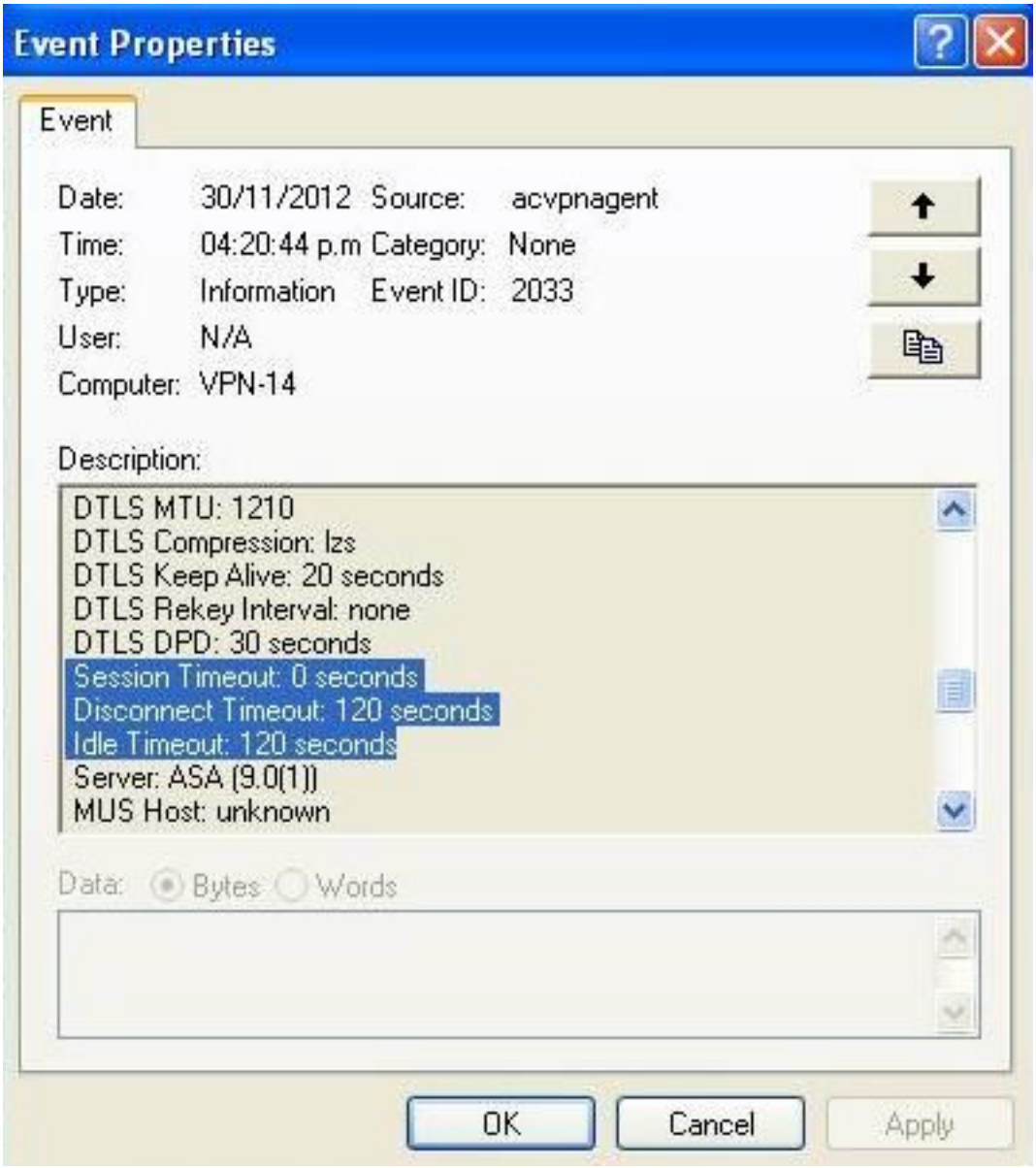
1. Reconnexion TCP ou UDP [couche 3 OSI]
2. TLS, DTLS ou IPSec(IKE+ESP) [couche 4 du modèle OSI] : la reprise TLS n'est pas prise en charge.
3. VPN [couche OSI 7] - Le jeton de session VPN est utilisé comme jeton d'authentification afin de rétablir la session VPN sur un canal sécurisé en cas d'interruption. Il s'agit d'un

mécanisme propriétaire très similaire, conceptuellement, à la façon dont un jeton Kerberos ou un certificat client est utilisé pour l'authentification. Le jeton est unique et généré cryptographiquement par la tête de réseau, qui contient l'ID de session plus une charge utile aléatoire générée cryptographiquement. Il est transmis au client dans le cadre de l'établissement VPN initial après l'établissement d'un canal sécurisé vers la tête de réseau. Il reste valide pendant toute la durée de vie de la session sur la tête de réseau et est stocké dans la mémoire du client, qui est un processus privilégié.
Conseil : ces versions ASA et les versions ultérieures contiennent un jeton de session cryptographique plus puissant : 9.1(3) et 8.4(7.1)

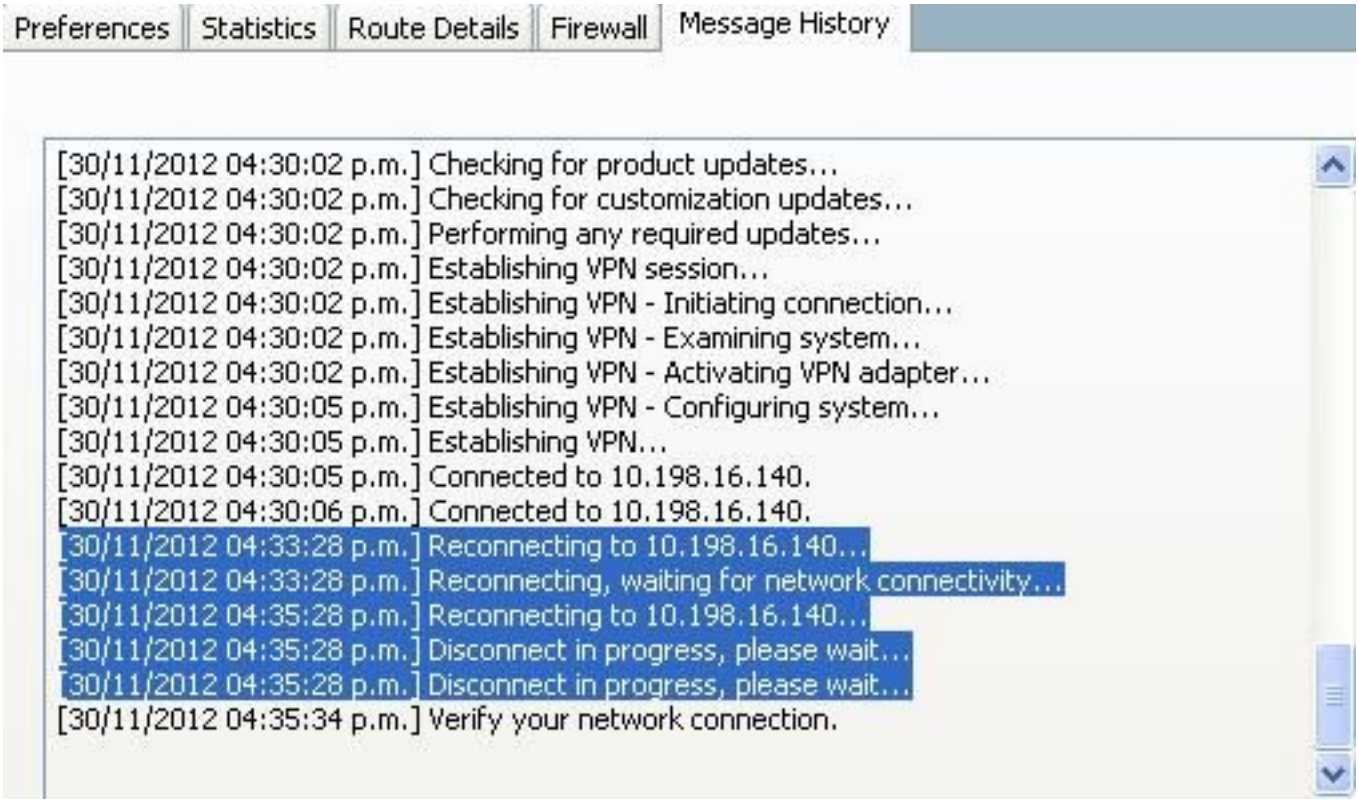
Le processus réel

Un temporisateur de déconnexion est démarré dès que la connexion réseau est interrompue. Le client AnyConnect continue à essayer de se reconnecter tant que ce minuteur n'expire pas. Le délai de déconnexion est défini sur le paramètre le plus bas, soit **Idle-Timeout** de la stratégie de groupe ou **Maximum Connect Time**.

La valeur de ce minuteur apparaît dans l'Observateur d'événements pour la session AnyConnect de la négociation :



Dans cet exemple, la session se déconnecte au bout de deux minutes (120 secondes), ce qui peut être vérifié dans l'historique des messages d'AnyConnect :



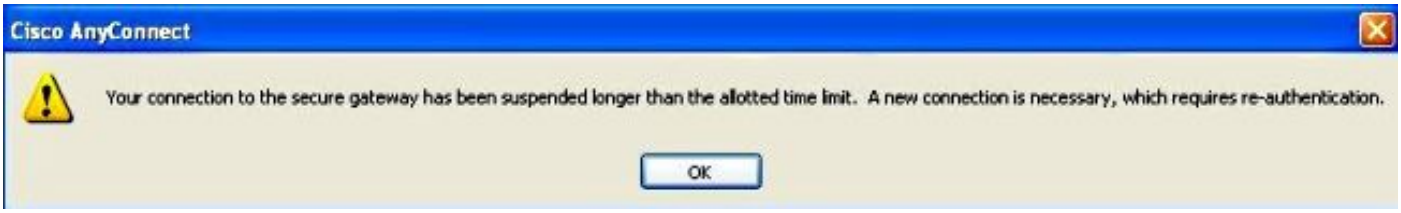
Conseil : pour que l'ASA réponde à un client qui tente de se reconnecter, la session Parent-Tunnel doit toujours exister dans la base de données ASA. En cas de basculement, les DPD doivent également être activés pour que le comportement de reconnexion fonctionne.

Comme le montrent les messages précédents, la reconnexion a échoué. Cependant, si la reconnexion réussit, voici ce qui se passe :

1. Le Parent-Tunnel reste le même ; il n'est pas renégocié car ce tunnel conserve le jeton de session requis pour la session afin de se reconnecter.
2. De nouvelles sessions SSL et DTLS sont générées et différents ports sources sont utilisés lors de la reconnexion.
3. Toutes les valeurs Idle-Timeout sont restaurées.
4. Le délai d'inactivité est restauré.

Attention : prenez connaissance du bogue Cisco ayant l'ID CSCtg3110. La base de données de session VPN ne met pas à jour l'adresse IP publique dans la base de données de session ASA lorsque AnyConnect se reconnecte.

Dans cette situation où les tentatives de reconnexion échouent, vous rencontrez le message suivant :



Remarque : cette demande d'amélioration a été déposée afin de rendre ceci plus granulaire : ID de bogue Cisco CSCsl52873 - ASA n'a pas de délai d'attente de déconnexion

configurable pour AnyConnect.

Comportement du client AnyConnect en cas de suspension du système

Une fonction d'itinérance permet à AnyConnect de se reconnecter après la mise en veille d'un PC. Le client continue d'essayer jusqu'à ce que les délais d'inactivité ou de session expirent et qu'il ne désactive pas immédiatement le tunnel lorsque le système passe en mode veille prolongée/veille. Pour les utilisateurs qui ne veulent pas de cette fonctionnalité, définissez le délai d'expiration de la session sur une valeur faible afin d'empêcher les reconnexions de mise en veille/reprise.

> **Remarque** : après la correction du bogue Cisco ayant l'ID CSCso17627 (Version 2.3(111)+), un bouton de contrôle a été introduit afin de désactiver cette fonction de reconnexion lors de la reprise.

Le comportement de reconnexion automatique pour AnyConnect peut être contrôlé via le profil XML AnyConnect avec ce paramètre :

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

Avec cette modification, AnyConnect tente de se reconnecter lorsque l'ordinateur est remis en veille. La préférence AutoReconnectBehavior prend par défaut la valeur DisconnectOnSuspend. Ce comportement de routage est différent de celui d'AnyConnect client version 2,2. Pour la reconnexion après la reprise, l'administrateur réseau doit soit définir ReconnectAfterResume dans le profil, soit rendre les préférences ReconnexionAutomatique et ComportementReconnexionAutomatique contrôlables par l'utilisateur dans le profil pour permettre aux utilisateurs de le définir.

Forum aux questions

T1. Anyconnect DPD a un intervalle mais aucune nouvelle tentative - combien de paquets doit-il manquer avant de marquer l'extrémité distante comme étant morte ?

A. Du point de vue du client, les DPD ne détruisent un tunnel que pendant l'étape d'établissement du tunnel. Si le client rencontre trois nouvelles tentatives (envoie quatre paquets) au cours de la phase d'établissement du tunnel et ne reçoit pas de réponse du serveur VPN principal, il revient à utiliser l'un des serveurs de secours s'il est configuré. Cependant, une fois le tunnel établi, les DPD manqués n'ont aucun impact sur le tunnel du point de vue des clients. L'impact réel des DPD est sur le serveur VPN comme expliqué dans la section DPD et Minuteurs d'inactivité.

T2. Le traitement DPD est-il différent pour AnyConnect avec IKEv2 ?

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

T3. Le tunnel parent AnyConnect a-t-il une autre fonction ?

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

T4. Pouvez-vous filtrer et fermer uniquement les sessions inactives ?

R. Vous pouvez filtrer les sessions inactives à l'aide de la commande **show vpn-sessiondb anyconnect filter inactive**. Cependant, il n'y a pas de commande pour fermer uniquement les sessions inactives. Au lieu de cela, vous devez fermer des sessions spécifiques ou toutes les sessions par utilisateur (index - nom), protocole ou groupe de tunnels. Une demande d'amélioration, ID de bogue Cisco CSCuh5707 , a été déposée afin d'ajouter l'option pour se déconnecter uniquement des sessions inactives.

Q5. Qu'arrive-t-il au tunnel parent lorsque le délai d'inactivité des tunnels DTLS ou TLS expire ?

R. Le minuteur « Idle TO Left » de la session AnyConnect-Parent est réinitialisé après l'arrêt du tunnel SSL ou du tunnel DTLS. Cela permet au « idle-timeout » d'agir comme un « déconnecté » du délai. Cela devient effectivement le temps autorisé pour le client à se reconnecter. Si le client ne se reconnecte pas dans le temporisateur, le tunnel parent est terminé.

Q6. Pourquoi conserver la session une fois que les minuteurs DPD ont déconnecté la session et pourquoi l'ASA ne libère-t-il pas l'adresse IP ?

R. La tête de réseau ne connaît pas l'état du client. Dans ce cas, l'ASA attend que le client se reconnecte jusqu'à ce que la session expire au moment de l'inactivité. DPD ne tue pas une session AnyConnect ; il tue simplement le tunnel (au sein de cette session) afin que le client puisse rétablir le tunnel. Si le client ne rétablit pas de tunnel, la session reste active jusqu'à l'expiration du minuteur d'inactivité.

Si le problème concerne les sessions qui sont utilisées, définissez les connexions simultanées sur une valeur faible, par exemple 1. Avec ce paramètre, les utilisateurs qui ont une session dans la base de données de session voient leur session précédente supprimée lorsqu'ils se reconnectent.

Q7. Quel est le comportement si l'ASA bascule d'Active vers Standby ?

R. Au départ, lorsque la session est établie, les trois tunnels (Parent, SSL et DTLS) sont répliqués vers l'unité en veille ; une fois que l'ASA bascule, les sessions DTLS et TLS sont rétablies car elles ne sont pas synchronisées avec l'unité en veille, mais tout flux de données à travers les tunnels doit fonctionner sans interruption après le rétablissement de la session AnyConnect.

Les sessions SSL/DTLS n'ayant pas d'état, l'état et le numéro d'ordre SSL ne sont pas conservés et peuvent être très contraignants. Par conséquent, ces sessions doivent être rétablies à partir de zéro, ce qui est fait avec la session Parent et le jeton de session.

> **Conseil** : en cas de basculement, les sessions client VPN SSL ne sont pas transférées vers le périphérique de secours si les keepalives sont désactivés.

Q8. Pourquoi y a-t-il deux temporisations différentes, la temporisation d'inactivité et

la temporisation de déconnexion, si elles ont toutes les deux la même valeur ?

A. Lorsque les protocoles ont été développés, deux délais d'attente différents ont été prévus pour :

- Délai d'inactivité : le délai d'inactivité est défini lorsqu'aucune donnée n'est transmise via une connexion.
- Déconnexion du délai d'attente - Le délai d'attente déconnecté est pour lorsque 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 jamais été implémenté sur l'ASA. Au lieu de cela, l'ASA envoie au client la valeur de délai d'inactivité pour les délais d'inactivité et de déconnexion.

Le client n'utilise pas le délai d'inactivité, car l'ASA gère le délai d'inactivité. Le client utilise la valeur du délai d'attente déconnecté, qui est la même que la valeur du délai d'attente inactif, afin de savoir quand abandonner les tentatives de reconnexion puisque l'ASA a abandonné la session.

Alors qu'il n'est pas connecté activement au client, l'ASA expire la session via le délai d'inactivité. La principale raison de ne pas mettre en oeuvre le délai d'attente déconnecté sur l'ASA était d'éviter l'ajout d'un autre temporisateur pour chaque session VPN et l'augmentation de la surcharge sur l'ASA (bien que le même temporisateur puisse être utilisé dans les deux instances, juste avec des valeurs de délai d'attente différentes, puisque les deux cas sont mutuellement exclusifs).

La seule valeur ajoutée avec le délai d'attente déconnecté est de permettre à un administrateur de spécifier un délai d'attente différent lorsque le client n'est pas connecté de manière active par rapport à inactif. Comme indiqué précédemment, l'ID de bogue Cisco CSCsl52873 a été enregistré pour cela.

Q9. Que se passe-t-il lorsque la machine client est suspendue ?

R. Par défaut, AnyConnect tente de rétablir une connexion VPN lorsque vous perdez la connectivité. Il ne tente pas de rétablir une connexion VPN après la reprise d'un système par défaut. Référez-vous à Comportement du client AnyConnect en cas de suspension du système pour plus de détails.

Q10. Lors d'une reconnexion, l'adaptateur virtuel AnyConnect est-il instable ou la table de routage est-elle modifiée ?

A. Une reconnexion au niveau du tunnel n'effectue aucune des deux opérations. Il s'agit d'une reconnexion sur SSL ou DTLS uniquement. Ils passent environ 30 secondes avant d'abandonner. Si DTLS échoue, il est simplement abandonné. Si SSL échoue, il provoque une reconnexion au niveau de la session. Une reconnexion au niveau de la session refait complètement le routage. Si l'adresse du client attribuée lors de la reconnexion, ou tout autre paramètre de configuration ayant un impact sur l'adaptateur virtuel, n'a pas été modifié, l'adaptateur virtuel n'est pas désactivé. Bien qu'il soit peu probable que les paramètres de configuration reçus de l'ASA soient modifiés, il est possible qu'une modification de l'interface physique utilisée pour la connexion VPN (par exemple, si vous vous déconnectez et passez d'une connexion filaire à une connexion Wi-Fi) entraîne une valeur d'unité de transmission maximale (MTU) différente pour la connexion VPN. La valeur MTU a un impact sur la valeur VA, et une modification de cette valeur entraîne la désactivation de la valeur VA, puis sa réactivation.

Q11. La « reconnexion automatique » assure-t-elle la persistance de session ? Dans l'affirmative, y a-t-il des fonctionnalités supplémentaires ajoutées au client AnyConnect ?

A. AnyConnect n'offre pas de « magie » supplémentaire pour prendre en charge la persistance des sessions pour les applications. Mais la connectivité VPN est restaurée automatiquement peu de temps après la reprise de la connectivité réseau à la passerelle sécurisée, à condition que les délais d'inactivité et de session configurés sur l'ASA n'aient pas expiré. Et contrairement au client IPsec, la reconnexion automatique aboutit à la même adresse IP de client. Tandis qu'AnyConnect tente de se reconnecter, l'adaptateur virtuel AnyConnect reste activé et à l'état connecté, de sorte que l'adresse IP du client reste présente et activée sur le PC client tout le temps, ce qui donne une persistance de l'adresse IP du client. Cependant, les applications PC clientes perçoivent toujours la perte de connectivité à leurs serveurs sur le réseau d'entreprise si la restauration de la connectivité VPN prend trop de temps.

Q12. Cette fonctionnalité fonctionne sur toutes les variantes de Microsoft Windows (Vista 32 bits et 64 bits, XP). Et le Macintosh ? Fonctionne-t-il sur OS X 10.4 ?

A. Cette fonctionnalité fonctionne sur Mac et Linux. Il y a eu des problèmes avec Mac et Linux, mais des améliorations récentes ont été apportées, en particulier pour Mac. Linux nécessite toujours une prise en charge supplémentaire (ID de bogue Cisco CSCsr16670, ID de bogue Cisco CSCsm69213), mais la fonctionnalité de base est également présente. En ce qui concerne Linux, AnyConnect ne reconnaît pas qu'une interruption/reprise (veille/réveil) s'est produite. Cela a essentiellement deux impacts :

- Le paramètre de profil/préférence AutoReconnectBehavior ne peut pas être pris en charge sur Linux sans la prise en charge de la suspension/reprise, de sorte qu'une reconnexion se produit toujours après la suspension/reprise.
- Sous Microsoft Windows et Macintosh, les reconnexions sont immédiatement effectuées au niveau de la session après la reprise, ce qui permet un passage plus rapide à une autre interface physique. Sous Linux, comme AnyConnect ne connaît pas du tout l'interruption/la reprise, les reconnexions ont lieu d'abord au niveau du tunnel (SSL et DTLS), ce qui peut signifier que les reconnexions prennent un peu plus de temps. Mais les reconnexions se produisent toujours sous Linux.

Q13. Y a-t-il des limites à la fonctionnalité en termes de connectivité (filaire, wi-fi, 3G, etc.) ? Prend-il en charge la transition d'un mode à un autre (du Wi-Fi à la 3G, de la 3G au câblé, etc.) ?

A. AnyConnect n'est pas lié à une interface physique particulière pendant toute la durée de vie de la connexion VPN. Si l'interface physique utilisée pour la connexion VPN est perdue ou si les tentatives de reconnexion dépassent un certain seuil d'échec, AnyConnect n'utilise plus cette interface et tente d'atteindre la passerelle sécurisée avec toutes les interfaces disponibles jusqu'à l'expiration des minuteurs d'inactivité ou de session. Notez qu'une modification de l'interface physique peut entraîner une valeur MTU différente pour l'appliance virtuelle, ce qui entraîne la désactivation et la réactivation de l'appliance virtuelle, mais toujours avec la même adresse IP client.

En cas d'interruption du réseau (interface désactivée, réseaux modifiés, interfaces modifiées), AnyConnect tente de se reconnecter ; aucune nouvelle authentification n'est nécessaire lors de la

reconnexion. Ceci s'applique même à un commutateur d'interfaces physiques :

Exemple :

```
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. Comment l'opération de reprise est-elle authentifiée ?

A. Dans un CV, vous soumettez à nouveau le jeton authentifié qui reste pendant la durée de vie de la session, puis la session est rétablie.

Q15. L'autorisation LDAP est-elle également effectuée lors de la reconnexion ou uniquement lors de l'authentification ?

A. Cette opération n'est effectuée que lors de la connexion initiale.

Q16. La pré-connexion et/ou l'analyse des hôtes s'exécute-t-elle lors de la reprise ?

A. Non, ils s'exécutent uniquement sur la connexion initiale. Quelque chose comme cela serait prévu pour la future fonction d'évaluation périodique de la posture.

Q17. En ce qui concerne l'équilibrage de charge (LB) VPN et la reprise de la connexion, le client se reconnecte-t-il directement au membre du cluster auquel il était connecté auparavant ?

R : Oui, c'est correct puisque vous ne rétablissez pas le nom d'hôte via DNS pour le rétablissement d'une session en cours.

Informations connexes

- **Référence DPD ASA : ID de bogue Cisco CSCsr63074 - DPD non envoyé lorsque l'homologue est mort et tunnel non inactif sur s2s avec 7.2.4**
- **Technical Support & Documentation - Cisco Systems**

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.