

Guide de dépannage d'AnyConnect VPN Client - Problèmes courants

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Processus de dépannage](#)

[Problèmes d'installation et d'adaptateur virtuel](#)

[Déconnexion ou incapacité d'établir la connexion initiale](#)

[Problèmes avec le trafic de passage](#)

[Problèmes de pannes d'AnyConnect](#)

[Fragmentation/problèmes avec le trafic de passage](#)

[Désinstallez automatiquement](#)

[Question remplissant FQDN de batterie](#)

[Configuration de sauvegarde de liste de serveur](#)

[AnyConnect : Problème de pilote altérée de la base de données](#)

[Réparation](#)

[Réparation défectueuse](#)

[Analysez la base de données](#)

[Messages d'erreur](#)

[Erreur : Incapable de mettre à jour la base de données de gestion de session](#)

[Solution 1](#)

[Solution 2](#)

[Erreur : "« Échec de l'enregistrement du module c:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll »](#)

[Solution](#)

[Erreur : "« Une erreur a été reçue de la passerelle sécurisée en réponse à la demande de négociation VPN. Veuillez contacter votre administrateur réseau »](#)

[Solution](#)

[Erreur : La session n'a pas pu être établie. limite de session de 2 atteinte .](#)

[Solution 1](#)

[Solution 2](#)

[Erreur : AnyConnect non activé sur le serveur VPN tout en essayant de connecter AnyConnect à ASA](#)

[Solution](#)

[Erreur : - %ASA-6-722036 : Groupe client-groupe Utilisateur xxxx IP x.x.x.x Transmission d'un grand paquet 1220 \(seuil 1206\)](#)

[Solution](#)

[Erreur : La passerelle sécurisée a rejeté le vpn de l'agent connectent ou rebranchent la demande.](#)

[Solution](#)

[Erreur : « Incapable de mettre à jour la base de données de Gestion de session »](#)

Solution

Erreur : « Le gestionnaire de client vpn a rencontré une erreur »

Solution

Erreur : « Incapable de traiter la réponse de xxx.xxx.xxx.xxx »

Solution

Erreur : La « procédure de connexion a refusé, mécanisme non autorisé de connexion, contactez votre administrateur »

Solution

Erreur : « Module d'Anyconnect indisponible ou corrompu. Contactez votre administrateur système »

Solution

Erreur : « Le module d'AnyConnect sur la passerelle sécurisée ne pourrait pas se trouvent »

Solution

Erreur : « le VPN sécurisé par l'intermédiaire du bureau distant n'est pas pris en charge »

Solution

Erreur : « Le certificat de serveur reçu ou sa chaîne n'est pas conforme aux PAP. Une connexion VPN ne sera pas établie »

Solution

Erreur : « Panne de validation de certificat »

Solution

Erreur : « Le service d'agent VPN a rencontré un problème et doit se fermer. Nous sommes désolés pour les désagréments »

Solution

Erreur : « Ce module d'installation n'a pas pu être ouvert. Vérifiez que le module existe »

Solution

Erreur : La « application des erreurs transforme. Vérifiez que spécifiés transforment des chemins sont valides. »

Solution

Erreur : « Le gestionnaire de client vpn a rencontré une erreur »

Solution

Erreur : « Un VPN rebranchent eu comme conséquence le paramètre de configuration différent. La configuration de réseau VPN est réinitialisée. Des applications utilisant le réseau privé peuvent devoir être restaurées. »

Solution

Erreur d'AnyConnect tout en ouvrant une session

Solution

Le paramètre de proxy IE n'est pas restauré après que débranchement d'AnyConnect sur le Windows 7

Solution

Erreur : L'AnyConnect Essentials ne peut pas être activé jusqu'à ce que toutes ces sessions soient fermées.

Solution

Erreur : L'onglet Connection sur l'option Internet de l'Internet Explorer masque après avoir obtenu connecté au client d'AnyConnect.

Solution

Erreur : Peu d'utilisateurs obtenant le message d'erreur d'échec de connexion quand d'autres peuvent se connecter avec succès par AnyConnect VPN

Solution

Erreur : Le certificat que vous visualisez ne s'assortit pas avec le nom du site vous essayez de visualiser.

Solution

Ne peut pas lancer AnyConnect de la chambre forte CSD d'un ordinateur de Windows 7

Solution

Le profil d'AnyConnect n'obtient pas répliqué vers le standby après Basculement

Solution

Crash de client d'AnyConnect si l'Internet Explorer va off-line

Solution

Message d'erreur : TLSPROTOCOL ERROR INSUFFICIENT BUFFER

Solution

Message d'erreur : La « tentative de connexion a en raison défectueux de l'entrée de hôte non valide »

Solution

Erreur : « Assurez que vos Certificats de serveur peuvent passer le mode strict si vous configurez le VPN illimité »

Solution

Erreur : « Une erreur interne s'est produite aux services HTTP de Microsoft Windows »

Solution

Erreur : « Le transport SSL a reçu une panne de la Manche de sécuriser. Peut être un résultat d'une crypto configuration non vérifiée sur la passerelle sécurisée. »

Solution

Informations connexes

Introduction

Ce document décrit un scénario de dépannage qui s'applique aux applications qui ne fonctionnent pas par le Cisco AnyConnect VPN Client.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur une appliance de sécurité adaptable Cisco (ASA) cette version 8.x de passages.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Processus de dépannage

Ce scénario typique de dépannage s'applique aux applications qui ne fonctionnent pas par le Cisco AnyConnect VPN Client pour des utilisateurs avec les ordinateurs Microsoft Windows. Ces sections traitent et fournissent des solutions aux problèmes :

- [Problèmes d'installation et d'adaptateur virtuel](#)
- [Déconnexion ou incapacité d'établir la connexion initiale](#)
- [Problèmes avec le trafic de passage](#)
- [Problèmes de pannes d'AnyConnect](#)
- [Fragmentation/problèmes avec le trafic de passage](#)

Problèmes d'installation et d'adaptateur virtuel

Procédez comme suit :

1. Obtenez le fichier journal de périphériques :

Windows XP / Windows 2000 :

```
\Windows\setupapi.log
```

Windows Vista :

Note: Les dossiers masqués doivent être rendus visibles afin de voir ces fichiers.

```
\Windows\Inf\setupapi.app.log  
\Windows\Inf\setupapi.dev.log
```

Si vous voyez des erreurs dans le fichier journal setupapi, vous pouvez définir les commentaires sur 0x2000FFFF comme décrit dans cet [article de la base de connaissances Windows](#). Notez l'article vous indique que pour le placer à 0xFFFF, mais si vous ajoutez la valeur d'ordre élevé de 0x2, elle rend se connecter plus rapide.

2. Obtenez le fichier journal d'installateur MSI :

S'il s'agit d'une installation de déploiement Web initiale, ce journal est situé dans le répertoire temp de l'utilisateur.

Windows XP / Windows 2000 :

`\Documents and Settings\\Local Settings\Temp\`

Windows Vista :

`\Users\\AppData\Local\Temp\`

Si c'est une mise à niveau automatique, ce journal est situé dans le répertoire temp du système :

`\Windows\Temp`

Le nom de fichier se présente dans ce format : **anyconnect-win-x.x.xxxx-k9-install-yyyyyyyyyyyyyy.log**. Obtenez le fichier le plus récent pour la version du client que vous voulez installer. x.xxxx change selon la version, comme 2.0.0343, et yyyyyyyyyyyyyy est la date et l'heure de l'installation.

3. Obtenez le fichier d'information système de PC :

Depuis une zone d'invite de commande/DOS, tapez ceci :

Windows XP / Windows 2000 :

```
winmsd /nfo c:\msinfo.nfo
```

Windows Vista :

```
msinfo32 /nfo c:\msinfo.nfo
```

Note: Après que vous tapiez dans cette demande, attendez. Cela peut prendre entre deux et cinq minutes pour terminer le fichier.

Obtenez un vidage de fichier systeminfo depuis une invite de commande :

Windows XP et Windows Vista :

```
systeminfo c:\sysinfo.txt
```

Référez-vous à [AnyConnect : Question de base de données de pilote altérée](#) afin de déboguer le problème du pilote.

Déconnexion ou incapacité d'établir la connexion initiale

Si vous rencontrez des problèmes de connexion avec le client AnyConnect, comme des déconnexions ou l'incapacité d'établir une connexion initiale, obtenez ces fichiers :

- Le fichier de configuration d'ASA afin de déterminer si quelque chose dans la configuration entraîne la panne de connexion :

Depuis la console de l'ASA, tapez `write net X.X.X.X: ASA-Config.txt` où X.X.X.X est l'adresse de l'IP d'un serveur TFTP sur le réseau.

OU

Depuis la console de l'ASA, tapez `show running-config`. Laissez la configuration se terminer à l'écran, puis coupez et collez dans un éditeur de texte, puis enregistrez.

- Les journaux d'événements ASA :

Afin d'activer ou d'ouvrir une session l'ASA pour l'authentification, le webvpn, le Secure Sockets Layer (SSL), et des événements du client de VPN SSL (SVC), émettent ces commandes CLI :

```
config terminal
logging enable
logging timestamp
logging class auth console debugging
logging class webvpn console debugging
logging class ssl console debugging
logging class svc console debugging
```

Lancez une session d'AnyConnect et assurez-vous que la panne peut être reproduite. Saisissez la sortie de journalisation de la console dans un éditeur de texte, puis enregistrez.

Afin de désactiver la journalisation, émettez `no logging enable`.

- Le journal de Cisco AnyConnect VPN Client de l'observateur d'événements Windows du PC client :

Choisissez **Start > Run**.

Entrez :

```
config terminal
logging enable
logging timestamp
logging class auth console debugging
logging class webvpn console debugging
logging class ssl console debugging
logging class svc console debugging
```

Cliquez avec le bouton droit de la souris sur le journal **Cisco AnyConnect VPN Client**, puis sélectionnez **Save Log File as AnyConnect.evt**.

Note: Enregistrez-le toujours sous le **format de fichier .evt**.

Si l'utilisateur ne peut pas se connecter à l'AnyConnect VPN Client, la question pourrait être liée à une commutation établie de session ou de client rapide de Remote Desktop Protocol (la RDP) activée sur le PC client. L'utilisateur peut voir que les paramètres de profil AnyConnect imposent un seul utilisateur local, mais des utilisateurs locaux multiples sont actuellement connectés à votre ordinateur. Message d'erreur Aucune connexion VPN ne sera établie sur le PC client. Afin de résoudre ce problème, déconnectez n'importe quelle session RDP établie et désactivez la commutation rapide d'utilisateur. Ce comportement est contrôlé par l'attribut d'[application de connexion de Windows](#) dans le profil de client, toutefois actuellement il n'y a aucune configuration qui permet réellement à un utilisateur pour établir une connexion VPN tandis que des plusieurs utilisateurs sont ouverts une session simultanément sur le même ordinateur. La demande d'amélioration [CSCsx15061](#) a été classée d'adresser cette caractéristique.

Note: Assurez-vous que le port 443 n'est pas bloqué ainsi le client d'AnyConnect peut se connecter à l'ASA.

Quand un utilisateur ne peut pas connecter le client VPN d'AnyConnect à l'ASA, le problème peut être causé par une incompatibilité entre la version du client d'AnyConnect et la version d'image du logiciel ASA. Dans ce cas, l'utilisateur reçoit ce message d'erreur : *L'installateur ne pouvait pas commencer le Client VPN Cisco, accès sans client n'est pas disponible.*

Afin de résoudre ce problème, mettez à niveau la version du client d'AnyConnect pour être compatible avec l'image du logiciel ASA. Afin de vérifier la compatibilité, référez-vous à la section sur les [appliances de sécurité et logiciels pris en charge](#) des [notes de publication relatives au client AnyConnect](#).

Quand un utilisateur ne peut pas se connecter au client VPN d'AnyConnect depuis le PC, le problème peut être causé par le logiciel antivirus installé sur le PC.

Note: AnyConnect doit être installé sur l'ordinateur avant que vous installiez n'importe quel tiers logiciel de Pare-feu/antivirus (poids du commerce). Si AnyConnect est installé après n'importe quels tiers Pare-feu/logiciel antivirus, alors AnyConnect ne se connecte pas. Afin de résoudre ce problème, désactivez toutes les configurations du firewall/AV personnel. Puis, apportez un petit changement sur l'adaptateur et l'essai virtuels d'AnyConnect pour rebrancher AnyConnect. Le pour en savoir plus, se rapportent aux id [CSCsj91840](#) et

[CSCti16453](#) de bogue Cisco.

Quand vous vous connectez pour la première fois à AnyConnect, le script de connexion ne fonctionne pas. Si vous vous déconnectez et vous reconnectez, le script de connexion fonctionne très bien. C'est le comportement prévu.

Quand vous connectez l'AnyConnect VPN Client à l'ASA, vous pourriez recevoir cette erreur :
L'utilisateur non autorisé pour l'accès client d'AnyConnect, contactez votre administrateur.

Cette erreur est vue quand l'image d'AnyConnect manque de l'ASA. Une fois que l'image est chargée à l'ASA, AnyConnect peut ne se connecter sans aucune question à l'ASA.

Cette erreur peut être résolue en désactivant le Transport Layer Security de datagramme (DTLS). Allez à la **configuration > à l'Accès à distance VPN > réseau (client) Access > des profils de connexion d'AnyConnect** et décochez la case de l'**enable DTLS**. Ceci désactive DTLS.

Les fichiers de dartbundle affichent ce message d'erreur quand l'utilisateur obtient déconnecté :
TUNNELPROTOCOLDPDMGR_ERROR_NO_DPD_RESPONSE : La passerelle sécurisée n'a pas répondu aux paquets de Dead Peer Detection. Cette erreur signifie que le canal DTLS était dû déchiré à la panne de Dead Peer Detection (DPD). Cette erreur est résolue si vous tordez le Keepalives DPD et émettez ces commandes :

```
webvpn
svc keepalive 30
svc dpd-interval client 80
svc dpd-interval gateway 80
```

Le **svc keepalive** et les commandes de **svc dpd-interval** sont remplacés par la **keepalive d'anyconnect** et les commandes de **dpd-intervalle d'anyconnect** respectivement dans la version 8.4(1) et ultérieures ASA comme affiché ici :

```
webvpn
anyconnect ssl keepalive 15
anyconnect dpd-interval client 5
anyconnect dpd-interval gateway 5
```

[Problèmes avec le trafic de passage](#)

Quand des problèmes sont détectés avec passer le trafic au réseau privé avec une session d'AnyConnect par l'ASA, terminez-vous ces étapes de donnée-collecte :

1. Obtenez la sortie de la commande **show vpn-sessiondb detail svc filter name <username>** ASA depuis la console. Si la sortie montre Filter Name: XXXXX, recueillez la sortie pour **show access-list XXXXX**. Vérifiez que access-list XXXXX ne bloque pas le flux de trafic voulu.
2. Exportez les statistiques AnyConnect à partir d'AnyConnect VPN Client > Statistics > Details > Export (AnyConnect-ExportedStats.txt).
3. Vérifiez les instructions **nat** dans le fichier de configuration ASA. Si le Traduction d'adresses de réseau (NAT) est activé, ceux-ci doivent exempter les données qui reviennent au client en raison de NAT. Par exemple, pour que NAT exempte (nat 0) les adresses IP du pool

AnyConnect, utilisez ceci sur le CLI :

```
webvpn
anyconnect ssl keepalive 15
anyconnect dpd-interval client 5
anyconnect dpd-interval gateway 5
```

4. Déterminez si la passerelle par défaut par tunnel doit être activée pour la configuration. La passerelle par défaut traditionnelle est celle du dernier recours pour le trafic non déchiffré.

Exemple :

```
!--- Route outside 0 0 is an incorrect statement.

route outside 0 0 10.145.50.1
route inside 0 0 10.0.4.2 tunneled
```

Par exemple, si le client VPN doit accéder à une ressource qui n'est pas dans la table de routage de la passerelle VPN, le paquet est routé par la passerelle par défaut standard. La passerelle VPN n'a pas besoin de la table de routage interne complète afin de résoudre ceci. Le mot clé **tunneled** peut être utilisé dans ce cas.

5. Vérifiez si le trafic d'AnyConnect est abandonné par la stratégie d'inspection de l'ASA. Vous pourriez exempter l'application spécifique qui est utilisée par le client d'AnyConnect si vous implémentez le cadre de stratégie modulaire de Cisco ASA. Par exemple, vous pourriez exempter le protocole maigre avec ces commandes.

```
ASA(config)# policy-map global_policy
ASA(config-pmap)# class inspection_default
ASA(config-pmap-c)# no inspect skinny
```

Problèmes de pannes d'AnyConnect

Terminez-vous ces étapes de donnée-collecte :

1. Assurez-vous que l'utilitaire Microsoft Dr Watson est activé. Pour ce faire, choisissez Start > Run, puis exécutez **Drwtsn32.exe**. Configurez ceci et cliquez sur **OK** :

```
ASA(config)# policy-map global_policy
ASA(config-pmap)# class inspection_default
ASA(config-pmap-c)# no inspect skinny
```

Quand la panne se produit, récupérez les fichiers .log et .dmp depuis **C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson**. Si ces fichiers semblent être en

service, alors utilisez ntbackup.exe.

2. Obtenez le journal de Cisco AnyConnect VPN Client de l'observateur d'événements Windows du PC client :

Choisissez **Start > Run**.

Entrez :

```
eventvwr.msc /s
```

Cliquez avec le bouton droit de la souris sur le journal Cisco AnyConnect VPN Client, puis sélectionnez Save Log File as AnyConnect.evt.

Note: Enregistrez-le toujours sous le **format de fichier .evt**.

[Fragmentation/problèmes avec le trafic de passage](#)

Quelques applications, telles que Microsoft Outlook, ne fonctionnent pas. Cependant, le tunnel peut transmettre tout autre trafic comme de petits messages Ping.

Ceci peut fournir des indices quant à un problème de fragmentation dans le réseau. Les Routeurs du consommateur sont particulièrement pauvres à la fragmentation de paquets et au réassemblage.

Essayez un ensemble d'évolution de pings afin de déterminer s'il échoue à une certaine taille. Par exemple, ping -l 500, ping -l 1000, ping -l 1500, ping -l 2000.

Il est recommandé que vous configurez un groupe spécial pour les utilisateurs qui éprouvent la fragmentation, et placez l'unité maximum de transition de SVC (MTU) pour ce groupe à 1200. Ceci vous permet de corriger les utilisateurs qui rencontrent ce problème, sans affecter la base d'utilisateurs plus large.

Problème

Blocage des connexions TCP une fois établies avec AnyConnect.

Solution

Afin de vérifier si votre utilisateur a un problème de fragmentation, réglez le mtu pour les clients d'AnyConnect sur l'ASA.

```
eventvwr.msc /s
```

[Désinstallez automatiquement](#)

Problème

Le client VPN d'AnyConnect se désinstalle une fois que la connexion se termine. Les journaux du client montrent que l'option **keep installed** est désactivée.

Solution

AnyConnect se désinstalle en dépit du fait que l'option **keep installed** est sélectionnée sur ASDM (Adaptive Security Device Manager). Afin de résoudre ce problème, configurez la commande **svc keep-installer installed** sous group-policy.

Question remplissant FQDN de batterie

Problème : Le client d'AnyConnect pré-est rempli avec l'adresse Internet au lieu du nom de domaine complet de batterie (FQDN).

Quand vous avez une installation de batterie d'Équilibrage de charge pour le VPN SSL et les tentatives de client de se connecter à la batterie, la demande est réorientée au noeud ASA et le client ouvre une session avec succès. Après une certaine heure, quand les essais de client à connecter à la batterie de nouveau, le FQDN de batterie n'est pas vu dans le **connecter aux entrées**. Au lieu de cela, l'entrée du noeud ASA à laquelle le client a été réorienté est vue.

Solution

Ceci se produit parce que le client d'AnyConnect retient le nom d'hôte auquel il s'est pour la dernière fois connecté. On observe ce comportement et une bogue a été classée. Pour les détails complets au sujet de la bogue, référez-vous à l'ID de bogue Cisco [CSCsz39019](#). Le workaround suggéré est d'améliorer le Cisco AnyConnect à la version 2.5.

Configuration de sauvegarde de liste de serveur

Une liste de sauvegarde de serveur est configurée au cas où le serveur principal sélectionné par l'utilisateur ne serait pas accessible. Ceci est défini dans le volet **de sauvegarde de serveur** dans le profil d'AnyConnect. Procédez comme suit :

1. Téléchargez l'[éditeur de profil d'AnyConnect](#) (clients [enregistrés](#) seulement). Le nom du fichier est **AnyConnectProfileEditor2_4_1.jar**.
2. Créez un fichier XML avec l'éditeur de profil d'AnyConnect.

Allez à l'onglet de liste de serveur.

Cliquez sur **Add**.

Tapez le serveur principal sur le champ d'**adresse Internet**.

Ajoutez le serveur de sauvegarde au-dessous de la liste de sauvegarde de serveur sur le champ de **host address**. Puis, cliquez sur **Add**.

3. Une fois que vous avez le fichier XML, vous devez l'assigner à la connexion que vous utilisez sur l'ASA.

Dans l'ASDM, choisissez la **configuration > l'Accès à distance VPN > réseau (client) Access > des profils de connexion d'AnyConnect.**

Sélectionnez votre profil et cliquez sur Edit.

Le clic **gèrent de la** section de stratégie de groupe par défaut.

Sélectionnez votre stratégie de groupe et cliquez sur Edit.

Avancés choisis et cliquent sur alors le **client de VPN SSL.**

Cliquez sur **New**. Puis, vous devez introduire un nom pour le profil et assigner le fichier XML.

4. Connectez le client à la session afin de télécharger le fichier XML.

AnyConnect : Problème de pilote altérée de la base de données

Cette entrée dans le fichier SetupAPI.log suggère que le système de catalogue est altéré :

La liste de classe de signature du pilote W239 " C:\WINDOWS\INF\certclas.inf" était manquante ou non valide. `Erreur 0xfffffde5` : Erreur inconnue. Le système assume que toutes les classes de périphérique sont sujettes à la stratégie de signature du pilote.

Vous pouvez également recevoir ce message d'erreur : `Error(3/17) : Incapable de commencer le VA, l'installation a partagé la file d'attente, ou le VA a abandonné la file d'attente partagée.`

Vous pouvez recevoir ce login le client : « Le gestionnaire de client vpn a rencontré une erreur ».

Réparation

Cette question est due à l'ID de bogue Cisco [CSCsm54689](#). Afin de résoudre ce problème, assurez-vous que le service de routage et d'accès distant est désactivé avant de démarrer AnyConnect. Si ceci ne résout pas le problème, complétez ces étapes :

1. Ouvrez une invite de commande en tant qu'administrateur sur le PC (invite élevée sur Vista).
2. Exécutez `net stop CryptSvc`.
3. Exécutez-vous :

```
eventvwr.msc /s
```

4. Une fois incité, choisissez **CORRECT** afin de tenter la réparation.
5. Quittez l'invite de commande.
6. Réinitialisation.

Réparation défectueuse

Si la réparation échoue, complétez ces étapes :

1. Ouvrez une invite de commande en tant qu'administrateur sur le PC (invite élevée sur Vista).
2. Exécutez net stop CryptSvc.
3. Renommez le répertoire %WINDIR%\system32\catroot2 en catroot2_old.
4. Quittez l'invite de commande.
5. Réinitialisation.

Analysez la base de données

Vous pouvez analyser la base de données à tout moment afin de déterminer si elle est valide.

1. Ouvrez une invite de commande en tant qu'administrateur sur le PC.
2. Exécutez-vous :

```
eventvwr.msc /s
```

Référez-vous à [Intégrité de la base de données de catalogue système](#) pour plus d'informations.

Messages d'erreur

Erreur : [Incapable de mettre à jour la base de données de gestion de session](#)

Tandis que le VPN SSL est connecté par un navigateur web, le message d'erreur Incapable de mettre à jour la base de données de gestion de session. apparaît, et les journaux ASA indiquent %ASA-3-211001 : Erreur d'allocation mémoire. L'appliance de sécurité adaptable n'a pas alloué la mémoire système de RAM.

Solution 1

Cette question est due à l'ID de bogue Cisco [CSCsm51093](#). Afin de résoudre ce problème, rechargez le logiciel ASA ou mettez-le à niveau à la version intermédiaire mentionnée dans le bogue. Référez-vous au pour en savoir plus de l'ID de bogue Cisco [CSCsm51093](#).

Solution 2

Cette question peut également être résolue si vous désactivez la menace-détection sur l'ASA si la menace-détection est utilisée.

Erreur : "« Échec de l'enregistrement du module c:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll »

Quand vous utilisez le client d'AnyConnect sur des ordinateurs portables ou des PC, une erreur se produit pendant l'installer :

`eventvwr.msc /s`

Quand vous rencontrez cette erreur, l'installateur ne peut pas avancer et le client est retiré.

Solution

Voici les solutions de contournement possibles pour résoudre cette erreur :

- Le plus défunt client d'AnyConnect plus n'est officiellement pris en charge avec le Microsoft Windows 2000. C'est un problème de Registre avec l'ordinateur 2000. Reportez-vous à la section relative aux [critères Windows](#) des [notes de publication relatives à AnyConnect](#).
- Supprimez les applications de vmware. Une fois qu'AnyConnect est installé, des applications de vmware peuvent être rajoutées au PC.
- Ajoutez ASA à leurs sites de confiance. Pour plus d'informations, reportez-vous à la section relative à [l'ajout d'un appliance de sécurité à la liste des sites de confiance](#) des notes de publication relatives à AnyConnect.
- Copiez ces fichiers du dossier \ProgramFiles\Cisco\CiscoAnyconnect vers un nouveau dossier et exécutez l'**invite de commande regsvr32 vpnapi.dll** :

```
vpnapi.dllvpncommon.dllvpncommoncrypt.dll
```

- Réimaginez le système d'exploitation sur le laptop/PC.

Le message du journal lié à cette erreur sur le client AnyConnect est semblable à ceci :

`eventvwr.msc /s`

Erreur : "« Une erreur a été reçue de la passerelle sécurisée en réponse à la demande de négociation VPN. Veuillez contacter votre administrateur réseau »

Quand l'essai de clients à connecter au VPN au Cisco AnyConnect VPN Client, cette erreur est reçu.

Ce message a été reçu de la passerelle sécurisée :

« *Illegal address class* » ou « *Host or network is 0* » ou « *Other error* »

Solution

Le problème se pose en raison de l'épuisement de pool IP local ASA. Pendant que la ressource en groupe VPN est épuisée, la chaîne de pool d'IP doit être agrandie.

L'ID de bogue Cisco est [CSCsl82188](#) est classé pour cette question. Cette erreur se produit habituellement quand le groupe local pour l'affectation d'adresses est épuisé, ou si un masque de sous-réseau de 32 bits est utilisé pour le pool d'adresses. Le contournement est de développer le pool d'adresses et d'utiliser un masque de sous-réseau 24-bit pour le groupe.

Erreur : La session n'a pas pu être établie. limite de session de 2 atteinte.

Quand vous essayez de connecter plus de deux clients à l'AnyConnect VPN Client, vous recevez le message d'erreur d'échec de connexion sur le client et un message d'avertissement dans les logs ASA que la session d'états ne pourrait pas être établie. limite de session de 2 atteinte. Je dispose de la licence **AnyConnect essential** sur ASA, qui exécute la version **8.0.4**.

Solution 1

Cette erreur se produit parce que la licence **AnyConnect essential** n'est pas prise en charge par ASA version 8.0.4. Vous devez mettre à niveau ASA vers la version 8.2.2. Ceci résout l'erreur.

Note: Indépendamment du permis utilisé, si la limite de session est atteinte, l'utilisateur recevra le message d'erreur d'échec de connexion.

Solution 2

Cette erreur peut également se produire si la commande de [session-limit de maximum-anyconnect-premium-ou-essentiel-limite de VPN-sessiondb](#) est utilisée de fixer la limite des sessions VPN permises pour être établi. Si la session-limit est fixée en tant que deux, alors l'utilisateur ne peut pas établir plus de deux sessions quoique le permis installé prenne en charge plus de sessions. Fixez la session-limit au nombre de sessions VPN requises afin d'éviter ce message d'erreur.

Erreur : AnyConnect non activé sur le serveur VPN tout en essayant de connecter AnyConnect à ASA

Vous recevez l'anyconnect non activé sur le message d'erreur de serveur VPN quand vous essayez de connecter AnyConnect à l'ASA.

Solution

Cette erreur est résolue si vous activez AnyConnect sur l'interface extérieure de l'ASA avec l'ASDM. Pour plus d'informations sur la façon d'activer AnyConnect sur l'interface externe, référez-vous à la section relative à l'[activation du protocole client VPN SSL](#).

Erreur : - %ASA-6-722036 : [Groupe client-groupe Utilisateur xxx IP x.x.x.x](#) Transmission d'un grand paquet 1220 (seuil 1206)

Le message d'erreur %ASA-6-722036: Groupe < client-groupe > Utilisateur < xxxx > IP < x.x.x.x > Transmission d'un grand paquet 1220 (seuil 1206), le message d'erreur apparaît dans les journaux de l'ASA. Que signifie ce journal et comment est-ce résolu ?

Solution

Ce message du journal déclare qu'un grand paquet a été envoyé au client. La source du paquet ne reconnaît pas le MTU du client. Ceci peut également être dû à la compression de données incompressibles. La solution de contournement consiste à désactiver la compression SVC avec la commande [svc compression none](#). Ceci résout le problème.

Erreur : La passerelle sécurisée a rejeté le vpn de l'agent connectent ou rebranchent la demande.

Quand vous vous connectez au client d'AnyConnect, cette erreur est reçue : « La passerelle sécurisée a rejeté le vpn de l'agent connectent ou rebranchent la demande. Une nouvelle connexion exige la ré-authentification et doit être commencée manuellement. Veuillez contacter votre administrateur réseau si ce problème persiste. Le message suivant a été reçu de la passerelle sécurisée : aucune adresse attribuée ».

Cette erreur est également reçue quand vous vous connectez au client d'AnyConnect : « La passerelle sécurisée a rejeté la tentative de connexion. Une nouvelle tentative de connexion à la même chose ou un autre sécurisent la passerelle est nécessaire, qui exige la ré-authentification. Le message suivant a été reçu de la passerelle sécurisée : L'hôte ou le réseau est 0 ».

Cette erreur est également reçue quand vous vous connectez au client d'AnyConnect : « La passerelle sécurisée a rejeté le vpn de l'agent connectent ou rebranchent la demande. Une nouvelle connexion exige une ré-authentification et doit être commencée manuellement. Veuillez contacter l'administrateur réseau si le problème persiste. Le message suivant a été reçu de la passerelle sécurisée : Aucun permis ».

Solution

Le routeur manquait la configuration de groupe après recharge. Vous devez ajouter la configuration intéressée de nouveau au routeur.

```
Router#show run | in pool
```

```
ip local pool SSLPOOL 192.168.30.2 192.168.30.254  
svc address-pool SSLPOO
```

« La passerelle sécurisée a rejeté le vpn de l'agent connectent ou rebranchent la demande. Une nouvelle connexion exige une ré-authentification et doit être commencée manuellement. Veuillez contacter l'administrateur réseau si le problème persiste. Le message suivant a été reçu de la passerelle sécurisée : Erreur d'aucun permis la » se produit quand le permis de mobilité d'AnyConnect manque. Une fois que le permis est installé, la question est résolue.

Erreur : « Incapable de mettre à jour la base de données de Gestion de session »

Quand vous essayez d'authentifier dans WebPortal, ce message d'erreur est reçu : « Incapable de mettre à jour la base de données de Gestion de session ».

Solution

Ce problème est lié à l'allocation de mémoire sur l'ASA. Cette question est en grande partie produite quand la version ASA est 8.2.1. Initialement, ceci exige une RAM 512MB pour sa

fonctionnalité complète. Référez-vous à la section de [mémoires réquises](#) dans les notes de mise à jour.

Comme contournement permanent, améliorez la mémoire à 512MB. Vous pouvez commander [« les kits d'adaptation de mémoire »](#).

Comme contournement provisoire, essayez pour libérer la mémoire avec ces étapes :

1. Désactivez la menace-détection.
2. Compactage de SVC de débronnement.
3. Rechargez l'ASA.

Erreur : « Le gestionnaire de client vpn a rencontré une erreur »

C'est un message d'erreur obtenu sur la machine cliente quand vous essayez de vous connecter à AnyConnect.

Solution

Afin de résoudre cette erreur, remplissez cette procédure afin de placer manuellement l'agent d'AnyConnect VPN à interactif :

1. Cliquez avec le bouton droit **mon ordinateur > gèrent > des services et des applications > des services >** et sélectionnez l'agent du Cisco AnyConnect VPN.
2. Cliquez avec le bouton droit **Propriétés**, puis le login, et choisissez **permettre au service pour interagir avec l'appareil de bureau**.

Ceci place la valeur de type DWORD de registre à 110 (le par défaut est 010) pour le HKEY_LOCAL_MACHINE \ SYSTÈME \ CurrentControlSet \ services \ le vpnagent.

Note: Si ce doit être utilisé, alors la préférence serait d'utiliser le **.MST** transformant dans ce cas. C'est parce que si vous placez ceci manuellement avec ces méthodes, il exige que ceci soit placé après chaque installent/processus de mise à niveau. C'est pourquoi il y a un besoin d'identifier l'application qui pose ce problème.

Quand l'acheminement et le Remote Access Service (RRAS) est activé sur le PC Windows, AnyConnect échoue avec le message **le client vpn que le gestionnaire a rencontré une erreur**. Afin de résoudre ce problème, assurez-vous que l'acheminement et le RRAS est désactivé avant de commencer AnyConnect. Référez-vous au [pour en savoir plus de l'ID de bogue Cisco CSCsm54689](#).

Erreur : « Incapable de traiter la réponse de xxx.xxx.xxx.xxx »

Les clients d'AnyConnect ne se connectent pas à Cisco ASA. L'erreur dans la fenêtre d'AnyConnect ne peut pas « **traiter la réponse de xxx.xxx.xxx.xxx** ».

Solution

Afin de résoudre cette erreur, essayez ces contournements :

- Retirez le webvpn de l'ASA et réactivez it.<
- Changez le numéro de port à 444 des 443 existants et réactivez-le sur 443.

Pour plus d'informations sur la façon d'activer le webvpn et changer le port pour le webvpn, référez-vous à cette [solution](#).

Erreur : La « procédure de connexion a refusé, mécanisme non autorisé de connexion, contactez votre administrateur »

Les clients d'AnyConnect ne se connectent pas à Cisco ASA. L'erreur dans la fenêtre d'AnyConnect est « `procédure de connexion refusée, mécanisme non autorisé de connexion, contactez votre administrateur` ».

Solution

Ce message d'erreur se produit en grande partie en raison des questions de configuration qui sont inexactes ou d'une configuration inachevée. Vérifiez la configuration et assurez-vous qu'elle est au besoin de résoudre le problème.

Erreur : « Module d'Anyconnect indisponible ou corrompu. Contactez votre administrateur système »

Cette erreur se produit quand vous essayez de lancer le logiciel d'AnyConnect d'un client de Macintosh afin de se connecter à une ASA.

Solution

Afin de résoudre ceci, terminez-vous ces étapes :

1. Téléchargez le module de Macintosh AnyConnect à l'éclair de l'ASA. Pour plus d'informations sur ceci, référez-vous à [télécharger l'image d'AnyConnect](#).
2. Modifiez la configuration de webvpn afin de spécifier le module d'AnyConnect qui est utilisé.

```
Router#show run | in pool
```

```
ip local pool SSLPOOL 192.168.30.2 192.168.30.254  
svc address-pool SSLPOO
```

La commande d'image de `svc` est remplacée par la commande d'image d'`anyconnect` dans la version 8.4(1) et ultérieures ASA comme affiché ici :

```
hostname(config)#webvpn
```

```
hostname(config-webvpn)#anyconnect image disk0:/  
anyconnect-win-3.0.0527-k9.pkg 1
```

```
hostname(config-webvpn)#anyconnect image disk0:/  
anyconnect-macosx-i386-3.0.0414-k9.pkg 2
```

Erreur : « Le module d'AnyConnect sur la passerelle sécurisée ne pourrait pas se trouver »

Cette erreur est provoquée par sur la machine Linux de l'utilisateur quand elle essaye de se connecter à l'ASA en lançant AnyConnect. Voici l'erreur complète :

```
"The AnyConnect package on the secure gateway could not be located. You may  
be experiencing network connectivity issues. Please try connecting again."
```

Solution

Afin de résoudre ce message d'erreur, vérifiez si le système d'exploitation (SYSTÈME D'EXPLOITATION) qui est utilisé sur la machine cliente est pris en charge par le client d'AnyConnect. Pour des informations complètes sur le logiciel pris en charge, référez-vous à la section de [configurations système requises](#) dans les [notes de mise à jour en AnyConnect](#).

Si le SYSTÈME D'EXPLOITATION est pris en charge, alors vérifiez si le module d'AnyConnect est spécifié dans la configuration de webvpn ou pas. Voyez la section [indisponible ou corrompue de module d'Anyconnect de](#) ce pour en savoir plus de document.

Erreur : « le VPN sécurisé par l'intermédiaire du bureau distant n'est pas pris en charge »

Les utilisateurs ne peuvent pas exécuter un accès de bureau distant. Le VPN sécurisé par l'intermédiaire du bureau distant n'est pas message d'erreur pris en charge apparaît.

Solution

Cette question est due à ces id de bogue Cisco : [CSCsu22088](#) et [CSCso42825](#). Si vous promouvez l'AnyConnect VPN Client, il peut résoudre le problème. Référez-vous à ces pour en savoir plus de bogues.

Erreur : « Le certificat de serveur reçu ou sa chaîne n'est pas conforme aux PAP. Une connexion VPN ne sera pas établie »

Quand vous tentez au VPN à l'ASA 5505, le le certificat de serveur reçu ou sa chaîne n'est pas conforme aux PAP. Une connexion VPN ne sera pas message d'erreur établi apparaît.

Solution

Afin de résoudre cette erreur, vous devez désactiver les Normes fédérales pour le traitement de l'information (PAP) dans le **fichier de stratégie de gens du pays d'AnyConnect**. Ce fichier peut habituellement être trouvé à l'AnyConnect VPN Client de C:\ProgramData\Cisco\Cisco \

AnyConnectLocalPolicy.xml. Si ce fichier n'est pas trouvé dans ce chemin, alors localisez le fichier à un répertoire différent avec un chemin tel que des utilisateurs \ données des applications \ Cisco AnyConnectVPNClient \ AnyConnectLocalPolicy.xml de C:\Documents and Settings\All. Une fois que vous localisez le fichier de xml, apportez des modifications à ce fichier comme affiché ici :

Changez l'expression :

```
<FipsMode>true</FipsMode>
```

À:

```
<FipsMode>>false</FipsMode>
```

Puis, redémarrez l'ordinateur. Les utilisateurs doivent avoir des autorisations administratives afin de modifier ce fichier.

Erreur : « Panne de validation de certificat »

Les utilisateurs ne peuvent pas lancer AnyConnect et recevoir l'erreur de panne de validation de certificat.

Solution

Les travaux d'authentification de certificat différemment avec AnyConnect ont comparé au client d'IPSec. Pour que l'authentification de certificat fonctionne, vous devez importer le certificat client à votre navigateur et changer le profil de connexion afin d'utiliser l'authentification de certificat. Vous devez également permettre à cette commande sur votre ASA afin de permettre des certificats client SSL à utiliser sur l'interface extérieure :

port extérieur 443 d'interface de certificat-authentification SSL

Pour plus d'informations sur cette commande, référez-vous à l'[authentification de certificat ssl](#).

Erreur : « Le service d'agent VPN a rencontré un problème et doit se fermer. Nous sommes désolés pour les désagréments »

Quand la version 2.4.0202 d'AnyConnect est installée sur un PC de Windows XP, elle arrête à mettre des dossiers à jour de localisation et un message d'erreur prouve que le vpnagent.exe échoue.

Solution

Ce comportement est l'ID de bogue Cisco ouvert une session [CSCsq49102](#). Le contournement suggéré est de désactiver le client de Citrix.

Erreur : « Ce module d'installation n'a pas pu être ouvert. Vérifiez que le module existe »

Quand AnyConnect est téléchargé, ce message d'erreur est reçu :

« Contactez votre administrateur système. L'installateur a manqué avec l'erreur suivante : Ce module d'installation n'a pas pu être ouvert. Vérifiez que le module existe et que vous pouvez l'accéder à, ou contactez le fournisseur d'applications pour vérifier que c'est un module valide d'installer windows. »

Solution

Terminez-vous ces étapes afin de réparer cette question :

1. Enlevez n'importe quel logiciel antivirus.
2. Désactivez le pare-feu Windows.
3. Si ni les aides d'étape 1 ou 2, alors formatez l'ordinateur et puis l'installent.
4. Si le problème persiste toujours, ouvrez une [valise TAC](#).

Erreur : La « application des erreurs transforme. Vérifiez que spécifiés transforment des chemins sont valides. »

Ce message d'erreur est reçu pendant l'automatique-téléchargement d'AnyConnect de l'ASA :

```
"Contact your system administrator. The installer failed with the following error:  
Error applying transforms. Verify that the specified transform paths are valid."
```

C'est le message d'erreur reçu en se connectant à AnyConnect pour le MaOS :

```
"The AnyConnect package on the secure gateway could not be located. You may be  
experiencing network connectivity issues. Please try connecting again."
```

Solution

Terminez-vous un de ces contournements afin de résoudre ce problème :

1. La cause principale de cette erreur pourrait être due à un fichier corrompu de traduction MST (par exemple, importé). Exécutez ces étapes pour réparer ceci :

Retirez la table de traduction MST.

Configurez l'image d'AnyConnect pour le MaOS dans l'ASA.

2. De l'ASDM, suivez le **réseau (client) Access > coutume d'AnyConnect > installe le** chemin et supprime le fichier de package d'AnyConnect. Assurez-vous que le module demeure dans le **réseau (client) Access > a avancé > configuration de VPN SSL > de client**.

Si ni l'un ni l'autre de ces contournements ne résolvent le problème, entrez en contact avec le [support technique de Cisco](#).

Erreur : « Le gestionnaire de client vpn a rencontré une erreur »

Cette erreur est reçue :

The VPN client driver has encountered an error when connecting through Cisco AnyConnect Client.

Solution

Cette question peut être résolue quand vous désinstallez le client d'AnyConnect, et puis enlève le logiciel antivirus. Après ceci, réinstallez le client d'AnyConnect. Si cette résolution ne fonctionne pas, alors reformatez le PC afin de réparer cette question.

Erreur : « Un VPN rebranchent eu comme conséquence le paramètre de configuration différent. La configuration de réseau VPN est réinitialisée. Des applications utilisant le réseau privé peuvent devoir être restaurées. »

Cette erreur est reçue quand vous essayez de lancer AnyConnect :

```
"A VPN reconnect resulted in different configuration setting. The VPN network setting is being re-initialized. Applications utilizing the private network may need to be restarted."
```

Solution

Afin de résoudre cette erreur, utilisez ceci :

```
"A VPN reconnect resulted in different configuration setting. The VPN network setting is being re-initialized. Applications utilizing the private network may need to be restarted."
```

La commande de **mtu de svc** est remplacée par la commande de **mtu d'anyconnect** dans la version 8.4(1) et ultérieures ASA comme affiché ici :

```
hostname(config)#group-policy <Name> attributes
```

```
hostname(config-group-policy)#webvpn
```

```
hostname(config-group-webvpn)#anyconnect mtu 500
```

Erreur d'AnyConnect tout en ouvrant une session

Problème

L'AnyConnect reçoit cette erreur quand il se connecte au client :

```
hostname(config)#group-policy <Name> attributes
```

```
hostname(config-group-policy)#webvpn
```

```
hostname(config-group-webvpn)#anyconnect mtu 500
```

Solution

La question peut être résolue si vous apportez ces modifications au profil d'AnyConnect :

Ajoutez cette ligne au profil d'AnyConnect :

```
hostname(config)#group-policy <Name> attributes
```

```
hostname(config-group-policy)#webvpn
```

```
hostname(config-group-webvpn)#anyconnect mtu 500
```

Le paramètre de proxy IE n'est pas restauré après que débranchement d'AnyConnect sur le Windows 7

Problème

Dans le Windows 7, si le paramètre de proxy IE est configuré pour **automatiquement détectez les configurations** et l'AnyConnect abaisse un nouveau paramètre de proxy, le paramètre de proxy IE n'est pas restauré de nouveau à **automatiquement détectent des configurations** après les utilisateurs finaux la session d'AnyConnect. Ceci entraîne des questions de RÉSEAU LOCAL pour les utilisateurs qui ont besoin de leur paramètre de proxy configuré pour **automatiquement détectent des configurations**.

Solution

Ce comportement est l'ID de bogue Cisco ouvert une session [CSCtj51376](#). Le contournement suggéré est d'améliorer à [AnyConnect 3.0](#).

Erreur : L'AnyConnect Essentials ne peut pas être activé jusqu'à ce que toutes ces sessions soient fermées.

Ce message d'erreur est reçu sur Cisco ASDM quand vous tentez d'activer le permis d'AnyConnect Essentials :

```
There are currently 2 clientless SSL VPN sessions in progress. AnyConnect Essentials can not be enabled until all these sessions are closed.
```

Solution

C'est le comportement normal de l'ASA. L'AnyConnect Essentials est un client séparément autorisé de VPN SSL. Il est entièrement configuré sur l'ASA et fournit à la pleine capacité d'AnyConnect, ces exceptions :

- Aucun Cisco Secure Desktop (CSD) (décapant y compris de HostScan/chambre forte/cache)
- Aucun VPN SSL sans client
- Support facultatif de Windows Mobile

Ce permis ne peut pas être utilisé en même temps que la licence premium partagée de VPN SSL. Quand vous devez utiliser un permis, vous devez désactiver l'autre.

Erreur : L'onglet Connection sur l'option Internet de l'Internet Explorer masque après avoir obtenu connecté au client d'AnyConnect.

L'onglet de **connexion** sur l'**option Internet de l'Internet Explorer** masque après que vous soyez connecté au client d'AnyConnect.

Solution

C'est dû à la caractéristique de [lockdown de msie-proxy](#). Si vous activez cette caractéristique, elle masque l'onglet de connexions dans Microsoft Internet Explorer pour la durée d'une session VPN d'AnyConnect. Si vous désactivez la configuration, elle laisse l'affichage de l'onglet de connexions inchangé.

Erreur : Peu d'utilisateurs obtenant le message d'erreur d'échec de connexion quand d'autres peuvent se connecter avec succès par AnyConnect VPN

Quelques utilisateurs reçoivent le message d'erreur d'échec de connexion quand d'autres peuvent se connecter avec succès par l'AnyConnect VPN.

Solution

Cette question peut être résolue si vous vous assurez que **n'exigez pas la** case à cocher de **pré-authentification** est vérifié les utilisateurs.

Erreur : Le certificat que vous visualisez ne s'assortit pas avec le nom du site vous essayez de visualiser.

Pendant la mise à jour de profil d'AnyConnect, une erreur est affichée que dit que le certificat est non valide. Ceci se produit avec Windows seulement et à la phase de mise à jour de profil. Le message d'erreur est affiché ici :

```
The certificate you are viewing does not match with the name of the site
you are trying to view.
```

Solution

Ceci peut être résolu si vous modifiez la liste de serveur du profil d'AnyConnect afin d'utiliser le FQDN du certificat.

C'est un échantillon du profil XML :

```
The certificate you are viewing does not match with the name of the site
you are trying to view.
```

Note: S'il y a une entrée existante pour l'adresse IP publique du serveur telle que le `<HostAddress>`, alors enlevez-le et retenez seulement le FQDN du serveur (par exemple, `<HostName>` mais pas `< host address >`).

Ne peut pas lancer AnyConnect de la chambre forte CSD d'un ordinateur de Windows 7

Quand l'AnyConnect est lancé de la chambre forte CSD, cela ne fonctionne pas. Ceci est tenté sur

des ordinateurs de Windows 7.

Solution

Actuellement, ce n'est pas possible parce qu'il n'est pas pris en charge.

Le profil d'AnyConnect n'obtient pas répliqué vers le standby après Basculement

Le client d'AnyConnect 3.0 VPN avec le logiciel de version 8.4.1 ASA fonctionne bien. Cependant, après Basculement, il n'y a aucune réplication pour la configuration associée par profil d'AnyConnect.

Solution

Ce problème a été observé et connecté sous l'ID de bogue Cisco [CSCtn71662](#). Le contournement provisoire est de copier manuellement les fichiers sur l'équipement de réserve.

Crash de client d'AnyConnect si l'Internet Explorer va off-line

Quand ceci se produit, le journal d'événements d'AnyConnect contient des entrées semblables à ces derniers :

```
The certificate you are viewing does not match with the name of the site  
you are trying to view.
```

Solution

Ce comportement est observé et connecté sous l'ID de bogue Cisco [CSCtx28970](#). Afin de résoudre ceci, quittez l'application d'AnyConnect et la relancez. Les entrées de connexion réapparaissent après relance.

Message d'erreur : TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER

Le client d'AnyConnect ne se connecte pas et l'incapable d'établir un message d'erreur de connexion est reçu. Dans le journal d'événements d'AnyConnect, l'erreur TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER est trouvée.

Solution

Ceci se produit quand le headend est configuré pour la Segmentation de tunnel avec une liste très grande de tunnel partagé (approximativement 180-200 entrées) et un ou plusieurs autres attributs de client sont configurés dans la stratégie de groupe, telle que le dns-server.

Pour résoudre ce problème, exécutez les étapes suivantes :

1. Réduisez le nombre d'entrées dans la liste de tunnel partagé.
2. Employez cette configuration afin de désactiver DTLS :

The certificate you are viewing does not match with the name of the site you are trying to view.

Le pour en savoir plus, se rapportent à l'ID de bogue Cisco [CSCtc41770](#).

Message d'erreur : La « tentative de connexion a en raison défectueux de l'entrée de hôte non valide »

La tentative de connexion a en raison défectueux du message d'erreur non valide d'entrée de hôte est reçue tandis qu'AnyConnect est authentifié avec l'utilisation d'un certificat.

Solution

Afin de résoudre ce problème, essayez l'un ou l'autre de ces solutions possibles :

- Améliorez l'AnyConnect à la version 3.0.
- Cisco Secure Desktop de déblocage sur votre ordinateur.

Le pour en savoir plus, se rapportent à l'ID de bogue Cisco [CSCti73316](#).

Erreur : « Assurez que vos Certificats de serveur peuvent passer le mode strict si vous configurez le VPN illimité »

Quand vous activez la caractéristique illimitée sur AnyConnect, l'assurer vos Certificats de serveur peut passer le mode strict si vous configurez le message d'erreur illimité VPN est reçu.

Solution

Ce message d'erreur implique que si vous voulez utiliser la caractéristique illimitée, vous avez besoin d'un valide divisez le certificat configuré sur le headend. Sans certificat de serveur valide, cette caractéristique ne fonctionne pas. Le mode strict de CERT est une option que vous placez dans le fichier de stratégie local d'AnyConnect afin d'assurer l'utilisation de connexions à un certificat valide. Si vous activez cette option dans le fichier de stratégie et vous connectez à un certificat factice, la connexion échoue.

Erreur : « Une erreur interne s'est produite aux services HTTP de Microsoft Windows »

Cet outil de génération de rapports diagnostique d'AnyConnect (DART) affiche un essai raté :

Date : 03/25/2014
Time : 09:52:21
Type : Error
Source : acvpnuui

Description : Function: CTransportWinHttp::SendRequest
File: .\CTransportWinHttp.cpp
Line: 1170

Invoked Function: HttpSendRequest

Return Code: 12004 (0x00002EE4)

Description: An internal error occurred in the Microsoft

Windows HTTP Services

Date : 03/25/2014
Time : 09:52:21
Type : Error
Source : acvpnui

Description : Function: ConnectIfc::connect
File: .\ConnectIfc.cpp
Line: 472

Invoked Function: ConnectIfc::sendRequest
Return Code: -30015443 (0xFE36002D)
Description: CTRANSPORT_ERROR_CONN_UNKNOWN

Date : 03/25/2014
Time : 09:52:21
Type : Error
Source : acvpnui

Description : Function: ConnectIfc::TranslateStatusCode
File: .\ConnectIfc.cpp
Line: 2999

Invoked Function: ConnectIfc::TranslateStatusCode
Return Code: -30015443 (0xFE36002D)
Description: CTRANSPORT_ERROR_CONN_UNKNOWN
Connection attempt failed. Please try again.

En outre, référez-vous au visualisateur d'événements ouvre une session l'ordinateur Windows.

Solution

Ceci pourrait être provoqué par en raison d'une connexion corrompue de Winsock. Remettez à l'état initial la connexion de l'invite de commande avec cette commande et redémarrez votre ordinateur de fenêtres :

remise de Winsock de netsh

Référez-vous [le comment déterminer et récupérer de la corruption Winsock2 dans les Windows Server 2003, dans Windows XP, et dans le](#) pour en savoir plus d'article de la base de connaissances de [Windows Vista](#).

Erreur : « Le transport SSL a reçu une panne de la Manche de sécuriser. Peut être un résultat d'une crypto configuration non vérifiée sur la passerelle sécurisée. »

Cet outil de génération de rapports diagnostique d'AnyConnect (DART) affiche un essai raté :

Date : 03/25/2014
Time : 09:52:21
Type : Error
Source : acvpnui

Description : Function: CTransportWinHttp::SendRequest
File: .\CTransportWinHttp.cpp
Line: 1170

Invoked Function: HttpSendRequest

Return Code: 12004 (0x00002EE4)
Description: **An internal error occurred in the Microsoft Windows HTTP Services**

Date : 03/25/2014
Time : 09:52:21
Type : Error
Source : acvpnui

Description : Function: ConnectIfc::connect
File: .\ConnectIfc.cpp
Line: 472

Invoked Function: ConnectIfc::sendRequest
Return Code: -30015443 (0xFE36002D)
Description: CTRANSPORT_ERROR_CONN_UNKNOWN

Date : 03/25/2014
Time : 09:52:21
Type : Error
Source : acvpnui

Description : Function: ConnectIfc::TranslateStatusCode
File: .\ConnectIfc.cpp
Line: 2999

Invoked Function: ConnectIfc::TranslateStatusCode
Return Code: -30015443 (0xFE36002D)
Description: CTRANSPORT_ERROR_CONN_UNKNOWN
Connection attempt failed. Please try again.

Solution

Windows 8.1 ne prend en charge pas le RC4 selon la mise à jour suivante de KO :

<http://support2.microsoft.com/kb/2868725>

Configurez les chiffrements DES/3DES pour le VPN SSL sur l'ASA DES-sha1" du ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 utilisant commande « OU éditez le fichier du registre de Windows sur la machine cliente comme mentionné ci-dessous :

<https://technet.microsoft.com/en-us/library/dn303404.aspx>

Informations connexes

- [Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500](#)
- [Client VPN AnyConnect - Forum Aux Questions](#)
- [Cisco Secure Desktop \(CSD\) - Forum Aux Questions](#)
- [Cisco AnyConnect VPN Client](#)
- [Support et documentation techniques - Cisco Systems](#)