Dépannage des problèmes courants de VPN client sécurisé Cisco

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Processus de dépannage
- Collecte d'informations pour le dépannage
  - Client - Statistiques et DART
  - Tête de réseau — ASA
  - Tête de réseau — FTD
  - Problèmes d'installation et de carte virtuelle
  - Déconnexion ou incapacité à établir la connexion initiale
  - Problèmes de passage du trafic
  - Problèmes de panne AnyConnect
  - Fragmentation / Problèmes de passage du trafic
  - Désinstaller automatiquement
  - Problème au moment d'indiquer le nom de domaine complet de la grappe
  - Configuration de la liste de serveurs de sauvegarde
- Client sécurisé Cisco : Problème de base de données de pilotes corrompu
  - Réparation
  - Échec de la réparation
  - Analyser la base de données
- Messages d'erreur
  - Erreur : Unable to Update the Session Management Database
  - Solution 1
  - Solution 2
  - Erreur : "Échec de l'enregistrement du module" pendant l'installation de Cisco Secure Client
  - Solution
  - Erreur : "Une erreur a été reçue de la passerelle sécurisée en réponse à la demande de négociation VPN. Please contact your network administrator »
  - Solution
  - Erreur : AnyConnect non activé sur le serveur VPN lors de la tentative de connexion 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 la demande de connexion ou de reconnexion au RPV de l'agent.

Solution

Erreur : « Une erreur s'est produite au niveau du pilote du client RPV »

Solution

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

Solution

Erreur : « Ouverture de session refusée. Mécanisme de connexion non autorisé. Communiquez avec votre administrateur. »

Solution

Erreur : « Progiciel AnyConnect non disponible ou corrompu. Contact your system administrator »

Solution

Erreur : « Impossible de localiser le progiciel AnyConnect sur la passerelle sécurisée. »

Solution

Erreur : « L'accès à distance au RPV sécurisé n'est pas pris en charge. »

Solution

Erreur : « Le certificat de serveur reçu ou sa chaîne n'est pas conforme aux normes FIPS. A VPN connection will not be established »

Solution

Erreur : « Échec de la validation du certificat »

Solution

Erreur : « Le service d'agent RPV a détecté un problème et doit fermer. We are sorry for the inconvenience »

Solution

Erreur : « Ce programme d'installation n'a pas pu être ouvert. Verify that the package exists »

Solution

Erreur : « Erreur lors de l'application des transformations. Verify that the specified transform paths are valid. »

Solution

Erreur : « La reconnexion au RPV a entraîné une modification des paramètres de configuration. Les paramètres du RPV sont en cours de réinitialisation. Il sera peut-être nécessaire de restaurer les applications qui utilisent le réseau privé. »

Solution

Erreur du client sécurisé Cisco lors de la connexion

Solution

Erreur : Impossible d'activer AnyConnect Essentials tant que toutes ces sessions ne sont pas fermées.

Solution

Erreur : Quelques utilisateurs obtiennent un message indiquant que la connexion a échoué, alors que d'autres sont en mesure de se connecter par l'intermédiaire du RPV d'AnyConnect.

Solution

Erreur : Le certificat que vous consultez ne correspond pas au nom du site que vous tentez d'afficher.

Solution

Le profil AnyConnect n'est pas dupliqué sur le serveur de secours après une panne.

Solution

Message d'erreur : TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER

Solution

Message d'erreur : « Échec de la tentative de connexion en raison d'une entrée hôte non valide. »

Solution

Erreur : « Veillez à ce que vos certificats de serveur puissent passer en mode strict si vous configurez un RPV permanent. »

Solution

Erreur : « An internal error occurred in the Microsoft Windows HTTP Services » (une erreur interne s'est produite dans les services HTTP de Microsoft Windows)

Solution

Erreur : « The SSL transport received a Secure Channel Failure. May be a result of a unsupported crypto configuration on the Secure Gateway. »

Solution

Informations connexes

Introduction

Ce document décrit les problèmes de Cisco Secure Client avec les défaillances et déconnexions d'applications sous Windows, macOS et Linux.

Conditions préalables

Exigences

Avant d'utiliser ce document, assurez-vous d'avoir :

- Cisco Secure Client 5.x sur le terminal (ou la version prise en charge par votre tête de réseau).
- Possibilité de collecter un bundle DART ou des journaux client.
- Accès administratif à la tête de réseau VPN (ASA ou FTD).

Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Client : Cisco Secure Client 5.x (module VPN AnyConnect).
- Tête de réseau Cisco ASA 9.x ou Cisco Secure Firewall Threat Defense (FTD) avec VPN d'accès à distance.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Consultez la section Dépannage de Cisco Secure Client du guide de l'administrateur du produit.

Processus de dépannage

Ce document détaille les problèmes VPN du client sécurisé Cisco (y compris AnyConnect), y compris les pannes d'application, les déconnexions inattendues et les erreurs courantes sur les configurations de tête de réseau Windows, macOS, Linux et Cisco ASA/FTD.

- Applications qui ne fonctionnent pas via le tunnel VPN.
- Les clients se connectent/se déconnectent de manière inattendue.
- Messages d'erreur courants apparaissant sur le client ou la tête de réseau.

Cette section couvre le client VPN sous Windows, macOS et Linux, y compris la configuration de tête de réseau sur Cisco ASA et l'accès à distance Cisco Secure Firewall Threat Defense (FTD). VPN.



Conseil : Avant de procéder au dépannage, collectez un bundle Cisco Secure Client DART. Vous pouvez analyser les sorties DART à l'aide de la tâche BDB de l'analyseur DART.

Passez en revue ces sections pour aborder les problèmes courants et trouver des solutions :

- Collecte d'informations pour le dépannage
- Problèmes d'installation et de carte virtuelle
- Déconnexion ou incapacité à établir la connexion initiale
- Problèmes de passage du trafic
- Problèmes de panne AnyConnect
- Fragmentation / Problèmes de passage du trafic
- Désinstaller automatiquement
- Problème au moment d’indiquer le nom de domaine complet de la grappe
- Configuration de la liste de serveurs de sauvegarde

Collecte d'informations pour le dépannage

Collectez les données client et de tête de réseau avant de modifier la configuration. Le TAC demande généralement un bundle DART.

Client - Statistiques et DART

1. Exporter les statistiques de connexion
   - Fenêtres: Icône d'engrenage > Fenêtre avancée > Statistiques > VPN AnyConnect > Statistiques d'exportation
   - macOS : Icône Statistiques > Exporter les statistiques
   - Linux: Détails sur l'interface utilisateur graphique du client
2. Exécuter DART
   - Windows/Linux : Icône Engrenage > Fenêtre Avancée > Diagnostics
   - macOS : Menu Application > Générer un rapport de diagnostic

   Connectez l'offre groupée à votre dossier TAC ou utilisez Upload to TAC avec le numéro SR et le jeton.
3. Problèmes de navigateur intégré : Fenêtre Avancée > Général > Navigateur Web > Effacer les données.

Tête de réseau — ASA

- show running-config
- show vpn-sessiondb detail anyconnect filter name <username>
- Exemple de débogage :

```
configure terminal
logging enable
logging timestamp
logging class auth console debugging
logging class webvpn console debugging
logging class ssl console debugging
logging class anyconnect console debugging
```

Reproduisez l'échec, capturez le résultat, puis no logging enable.

Tête de réseau — FTD

À partir de FMC/CDO, exportez les paramètres de stratégie et de profil de connexion VPN d'accès à distance. Collecter les journaux de connexion/VPN SSL FTD pour la fenêtre d'échec.

Problèmes d'installation et de carte virtuelle

Si l'installation ou la configuration de la carte virtuelle échoue, collectez :

1. Journaux d'installation de Windows :

```
%SystemRoot%\Inf\setupapi.dev.log
%SystemRoot%\Inf\setupapi.setup.log
```

2. Journal d'installation MSI : %LOCALAPPDATA%\Temp\ ou %SystemRoot%\Temp\ — nom du fichier cisco-secure-client-win-*-install-*.log (le plus récent pour votre version).
3. MSI détaillé (si nécessaire) :

```
msiexec /i cisco-secure-client-win-<version>-predeploy-k9.msi /lvx %TEMP%\ac-install.log
```

4. Informations système : msinfo32 /nfo %TEMP%\msinfo.nfo et systeminfo > %TEMP%\sysinfo.txt

Pour les erreurs de base de données de pilotes, consultez Cisco Secure Client : Problème de base de données de pilotes corrompus et erreur de la section du guide de l'administrateur VPN Client Driver Encounters (après une mise à jour de Microsoft Windows).

Déconnexion ou incapacité à établir la connexion initiale

Si vous rencontrez des problèmes de connexion avec le client sécurisé Cisco, collectez les données par Collecter les informations pour le dépannage avant de modifier la configuration.

- Configuration de tête de réseau : show running-config ou export policy from FMC/CDO for FTD.
- Journaux client : Collectez un bundle DART (voir Collecte d'informations). Ne vous fiez pas aux exportations de l'Observateur d'événements hérité .evt.
- Débogage ASA (si nécessaire) : Activez logging class auth, webvpn, ssl et anyconnect lors du débogage ; reproduire la défaillance ; capturer le résultat de la console ; alors no logging enable.

Si l'utilisateur ne peut pas se connecter, le problème peut être lié au protocole RDP (Remote Desktop Protocol) ou à la commutation rapide d'utilisateurs. L'utilisateur peut voir : Les paramètres de profil AnyConnect nécessitent un seul utilisateur local, mais plusieurs utilisateurs locaux sont actuellement connectés à votre ordinateur. Impossible d'établir une connexion VPN.

Déconnectez la ou les sessions RDP et désactivez la commutation rapide des utilisateurs. Plusieurs utilisateurs locaux simultanés ne sont pas pris en charge sur le même ordinateur pour l'établissement du VPN.

Remarque : Assurez-vous que le port 443 (et UDP 443 pour DTLS) n'est pas bloqué afin que le client puisse atteindre la tête de réseau.

Lorsqu'un utilisateur ne peut pas se connecter, le problème peut être causé par une incompatibilité entre la version du client sécurisé Cisco et le logiciel de tête de réseau. L'utilisateur peut recevoir : Le programme d'installation n'a pas pu démarrer le client VPN Cisco, l'accès sans client n'est pas disponible. Mettez à niveau le client vers une version prise en charge par votre déploiement VPN d'accès à distance ASA ou FTD.

Lorsque vous vous connectez pour la première fois à Cisco Secure Client, le script de connexion peut présenter des problèmes. Si vous vous déconnectez et vous reconnectez, le script de connexion s'exécute souvent comme prévu. Ce comportement peut être attendu en fonction du profil et de la synchronisation du script.

Lorsque vous vous connectez, vous pouvez recevoir : User not authorized for AnyConnect Client access, contact your administrator (l'utilisateur ne possède pas d'accès client à AnyConnect. Communiquez avec votre administrateur). Cela se produit souvent lorsque l'image du client sécurisé est manquante sur la tête de réseau. Téléchargez l'image client correcte et référencez-la dans la configuration VPN RA / WebVPN.

Le DART peut afficher TUNNELPROTOCOLDPDMGR_ERROR_NO_DPD_RESPONSE lorsque le canal DTLS est arrêté en raison d'une défaillance de détection d'homologue mort (DPD). Régler les keepalives sur ASA :

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

Désactivez DTLS uniquement en tant que test temporaire (ASDM : Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles, décochez la case Enable DTLS, ou FMC equivalent). Préférez fixer la synchronisation DPD et autoriser UDP 443.

Problèmes de passage du trafic

Lorsque des problèmes sont détectés lors du transfert du trafic vers le réseau privé avec une session Cisco Secure Client via l'ASA, procédez comme suit :

1. Obtenez le résultat de show vpn-sessiondb detail anyconnect filter name <username> à partir de la console ASA. Si la sortie affiche Filter Name : XXXXX, rassemblez show access-

list XXXXX. Vérifiez que la liste d’accès ne bloque pas le trafic prévu.

2. Exporter les statistiques de connexion : Cisco Secure Client > Gear > Advanced Window > Statistics > AnyConnect VPN > Export Stats.

3. Vérifiez la configuration ASA pour les instructions nat. Si la traduction d'adresses de réseau (NAT) est activée, exemptez le trafic qui retourne au client. Exemple d'exemption NAT pour un pool AnyConnect :

```
access-list in_nat0_out extended permit ip any 10.136.246.0 255.255.255.0
ip local pool IPPool1 10.136.246.1-10.136.246.254 mask 255.252.0.0
nat (inside) 0 access-list in_nat0_out
```

4. Déterminez si la passerelle par défaut tunnellisée doit être activée. Exemple :

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

   Si le client doit atteindre des ressources qui ne figurent pas dans la table de routage de la passerelle VPN, le mot clé tunneled achemine ce trafic à travers le tunnel VPN.

5. Vérifiez si la stratégie d'inspection abandonne le trafic d'application. Vous pouvez exempter un protocole sous le cadre de stratégie modulaire. Exemple pour skinny :

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

Problèmes de panne AnyConnect

Effectuez les étapes suivantes pour recueillir des données :

1. Collectez le DART immédiatement après le crash.
2. Remarque Entrées du rapport d'erreurs Windows pour vpnagent.exe / acvpnui.exe.
3. Journaux client : %LOCALAPPDATA%\Cisco\Cisco Secure Client\Logs (vérifiez le chemin de votre version).

Fragmentation / Problèmes de passage du trafic

Certaines applications, telles que Microsoft Outlook, ne fonctionnent pas lorsque le tunnel transmet un trafic plus faible, comme les petites requêtes ping. Cela peut indiquer une fragmentation sur le chemin. Les routeurs grand public sont souvent médiocres en termes de fragmentation et de réassemblage.

Essayez un ensemble évolutif de requêtes ping : ping -l 500, ping -l 1000, ping -l 1500, ping -l 2000.

Configurez une stratégie de groupe dédiée pour les utilisateurs affectés et définissez une MTU inférieure :

```
group-policy <name> attributes
 webvpn
  anyconnect mtu 1200
```

Désinstaller automatiquement

Problème

Cisco Secure Client se désinstalle après la fin de la connexion, même si l'option keep installed apparaît sélectionnée dans ASDM/FMC.

Solution

```
group-policy <name> attributes
 webvpn
  anyconnect keep-installer installed
```

Problème au moment d’indiquer le nom de domaine complet de la grappe

Problème : Le client AnyConnect indique le nom d’hôte plutôt que le nom de domaine complet de la grappe.

Lorsque vous disposez d'un cluster d'équilibrage de charge pour le VPN SSL et que le client se

connecte, la demande peut être redirigée vers un noeud de cluster et la connexion réussit. Lors d'une tentative de connexion ultérieure, le nom de domaine complet du cluster n'apparaît pas dans Se connecter à ; le nom d'hôte du dernier noeud peut apparaître à la place.

Solution

Le client met en cache le dernier nom d'hôte réussi. Effacez les entrées mises en cache ou définissez le nom de domaine complet du cluster dans la liste des serveurs de profils. Vérifiez sur Cisco Secure Client 5.x. Consultez l'ID de bogue Cisco CSCsz39019 pour les notes spécifiques à la plate-forme.

Configuration de la liste de serveurs de sauvegarde

Une liste de serveurs de sauvegarde est configurée lorsque le serveur principal est inaccessible. Définissez-le dans le volet Backup Server du profil client. Procédez comme suit :

1. Modifiez le profil à l'aide de l'Éditeur de profil à partir de votre package Client sécurisé de tête de réseau ou conformément au Guide de configuration du profil Client sécurisé 5.1. Attribuez le profil dans ASDM ou FMC.

2. Créez ou modifiez le profil XML :
    1. Accédez à l'onglet de la liste de serveurs.
    2. Cliquez sur Ajouter.
    3. Saisissez le nom d'hôte du serveur principal.
    4. Ajoutez des serveurs de sauvegarde dans la liste des serveurs de sauvegarde, puis cliquez sur Add.
3. Attribuez le profil à la connexion sur l'ASA :
    1. Dans ASDM : Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles.
    2. Sélectionnez votre profil et cliquez sur Edit (modifier).
    3. Cliquez sur Manage (gérer) dans la section des politiques de groupe par défaut.
    4. Sélectionnez votre politique de groupe, puis cliquez sur Edit(modifier).
    5. Sélectionnez Advanced, puis SSL VPN Client.
    6. Cliquez sur New, nommez le profil et attribuez le fichier XML.
4. Connectez le client pour télécharger le profil.

Client sécurisé Cisco : Problème de base de données de pilotes corrompu

Cette entrée du fichier SetupAPI.log suggère que le système de catalogue est endommagé :

La liste de classe de signature du pilote W239 "C:\WINDOWS\INF\certclas.inf" était manquante ou non valide. Erreur 0xfffffde5 : Erreur inconnue., en supposant que toutes les classes de périphériques sont soumises à la stratégie de signature du pilote. Vous pouvez également recevoir : Error(3/17): Unable to start VA, setup shared queue, or VA gave up shared queue (erreur(3/17) : impossible de démarrer l'adaptateur virtuel ou de configurer la file d'attente partagée; l'adaptateur virtuel a abandonné la file d'attente partagée).

Et vous pouvez recevoir ce journal sur le client : "The VPN client driver has encountered an error" (une erreur s'est produite au niveau du pilote du client RPV).

Réparation

Ce problème est lié à l'ID de bogue Cisco CSCsm54689. Désactivez le service de routage et d'accès distant (RRAS) avant de démarrer le client sécurisé Cisco. Si le problème persiste :

1. Ouvrez une invite de commandes en tant qu'Administrateur sous Windows.
2. Exécutez net stop CryptSvc.
3. Exécutez la commande :

```
esentutl /p%systemroot%\System32\catroot2\
{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
```

4. Lorsque vous y êtes invité, cliquez sur OK pour tenter la réparation.
5. Quittez l'invite de commandes.
6. Redémarrez.

Échec de la réparation

Si la réparation échoue :

1. Ouvrez une invite de commandes en tant qu'Administrateur sous Windows.
2. Exécutez net stop CryptSvc.
3. Renommez %WINDIR%\system32\catroot2 en catroot2_old.
4. Quittez l'invite de commandes.

5. Redémarrez.

Analyser la base de données

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

1. Ouvrez une invite de commandes en tant qu'Administrateur sous Windows.
2. Exécutez la commande :

```
esentutl /g%systemroot%\System32\catroot2\
{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
```

Référez-vous à Intégrité de base de données du catalogue système pour plus d'informations.

Messages d'erreur

Erreur : Unable to Update the Session Management Database

Cette erreur peut apparaître lors de l'authentification VPN SSL basée sur navigateur ou du portail Web. Le client ou le portail affiche Impossible de mettre à jour la base de données de gestion de session. L'ASA peut consigner %ASA-3-211001: Erreur d'allocation de mémoire. L’appareil de sécurité adaptatif n’a pas pu allouer de mémoire système RAM.

Solution 1

Associé au bogue Cisco ayant l'ID CSCsm51093. Rechargez l'ASA ou mettez à niveau vers une version fixe selon le bogue. Sur FTD, vérifiez la mémoire de la plate-forme et les limites de session VPN RA.

Solution 2

Mémoire de tête de réseau libre :

1. Désactivez la détection des menaces si cette option est activée.
2. Désactiver la compression AnyConnect : anyconnect compression none dans la section webvpn group-policy.
3. Rechargez l'ASA.
4. Sur les plates-formes ASA plus anciennes avec 256 Mo de RAM, passez à 512 Mo si le manque de mémoire persiste.

Erreur : "Échec de l'enregistrement du module" pendant l'installation de Cisco Secure Client

Lors de l'installation sous Windows, le programme d'installation signale qu'un module (par exemple vpnapi.dll) n'a pas pu s'enregistrer et effectue une restauration.

Solution

- Supprimez temporairement les cartes réseau virtuelles VMware en conflit ; réinstaller le client sécurisé ; ajoutez à nouveau VMware.
- Ajoutez le nom de domaine complet de tête de réseau aux sites de confiance si vous utilisez le déploiement Web.
- À partir de C:\Program Files\Cisco\Cisco Secure Client\, exécutez elevé : regsvr32 vpnapi.dll (et vpncommon.dll, vpncommoncrypt.dll le cas échéant).
- Collectez le journal détaillé MSI (voir la section Installation) et le DART si l'installation échoue toujours.
- En dernier recours, réparez Windows ou redéployez à partir d'une désinstallation propre du client sécurisé.

Erreur : "Une erreur a été reçue de la passerelle sécurisée en réponse à la demande de négociation VPN. Please contact your network administrator »

Lorsque des clients se connectent avec Cisco Secure Client, la passerelle renvoie une erreur telle que "Classe d'adresse illégale", "Hôte ou réseau est 0", ou "Autre erreur".

Solution

Le pool d'adresses IP locales ASA ou FTD est épuisé ou mal configuré. Développez le pool d'adresses VPN et utilisez un masque approprié (par exemple /24 au lieu d'un pool /32 uniquement). Voir l'ID de bogue Cisco CSCsl82188.

Erreur : AnyConnect non activé sur le serveur VPN lors de la tentative de connexion

anyconnect à ASA

Le client signale qu'AnyConnect / Secure Client n'est pas activé sur le serveur VPN.

Solution

Activez le VPN d'accès à distance et déployez une image de client sécurisé sur la tête de réseau. Sur ASA : Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles. Sur FTD : Configurez le VPN RA et l'image client dans FMC. Utilisez un guide VPN d'accès à distance, et non une configuration WebVPN sans client uniquement.

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 %ASA-6-722036: Group < client-group > User < xxxx > IP < x.x.x.x> Transmitting large packet 1220 (threshold 1206) message apparaît dans les journaux ASA.

Solution

Un paquet volumineux a été envoyé au client (MTU ou données non compressibles). Désactivez la compression pour la stratégie de groupe :

```
group-policy <name> attributes
 webvpn
  anyconnect compression none
```

Erreur : La passerelle sécurisée a rejeté la demande de connexion ou de reconnexion au RPV de l’agent.

Par exemple, aucune adresse attribuée, Hôte ou réseau 0, ou Aucune licence dans le message de la passerelle.

Solution

Vérifiez que la tête de réseau dispose d'un pool local IP configuré et que l'adresse de stratégie de

groupe est attribuée après rechargement ou basculement :

```
show running-config | include pool
ip local pool SSLPOOL 192.168.30.2 192.168.30.254
 anyconnect address-pool SSLPOOL
```

Pour No License, installez ou activez la licence de mobilité Secure Client requise sur la tête de réseau.

Erreur : « Une erreur s'est produite au niveau du pilote du client RPV »

En général, la défaillance de la carte virtuelle, un conflit RRAS ou un problème de pilote post-Windows Update.

Solution

1. Désactivez le service de routage et d'accès distant (RRAS) avant de démarrer le client sécurisé.
2. Complétez le client sécurisé Cisco : Base de données de pilotes endommagée Émettez des étapes si la setupapi affiche des erreurs de catalogue.
3. Après Windows Update, utilisez Repair VPN Client Driver Error dans le Guide d'administration de Secure Client 5.1.
4. Collectez le DART et contactez le TAC si nécessaire. Voir l'ID de bogue Cisco CSCsm54689.

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

Le client sécurisé Cisco ne parvient pas à se connecter avec Impossible de traiter la réponse de <gateway>.

Solution

- Désactivez et réactivez le VPN d'accès à distance / WebVPN sur l'interface concernée.
- Déplacez temporairement le VPN SSL vers un autre port (par exemple 444), puis restaurez 443.

Voir Configuration du client VPN SSL sur ASA. Collectez le DART si l'erreur persiste.

Erreur : « Ouverture de session refusée. Mécanisme de connexion non autorisé. Communiquez avec votre administrateur. »

Cisco Secure Client affiche Login Denied (Connexion refusée), mécanisme de connexion non autorisé, contactez votre administrateur.

Solution

Vérifiez le profil de connexion et l'authentification sur la tête de réseau (ASA ou FTD). Assurez-vous que la méthode d'authentification du client (RADIUS, SAML, certificat, etc.) correspond au profil. Vérifiez la stratégie de groupe et l'affectation de groupe de tunnels.

Erreur : « Progiciel AnyConnect non disponible ou corrompu. Contact your system administrator »

Cette erreur peut apparaître lors du lancement de Cisco Secure Client à partir d'un client Macintosh.

Solution

1. Téléchargez le package macOS Secure Client vers la mémoire flash de la tête de réseau.
2. Faites-le référence dans la configuration WebVPN :

```
webvpn
 anyconnect image disk0:/cisco-secure-client-macos-<version>-predeploy-k9.pkg 2
```

Erreur : « Impossible de localiser le progiciel AnyConnect sur la passerelle sécurisée. »

Sous Linux (ou d'autres plates-formes), le client ne peut pas télécharger le package à partir de la tête de réseau.

<#root>

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

Solution

Vérifiez que le système d'exploitation client est pris en charge et que l'image correcte est configurée sur la tête de réseau :

```
webvpn
 anyconnect image disk0:/cisco-secure-client-win-<version>-predeploy-k9.pkg 1
 anyconnect image disk0:/cisco-secure-client-macos-<version>-predeploy-k9.pkg 2
```

Consultez Package AnyConnect indisponible ou endommagé pour les étapes associées.

Erreur : « L'accès à distance au RPV sécurisé n'est pas pris en charge. »

Les utilisateurs voient que le VPN sécurisé via le bureau à distance n'est pas pris en charge.

Solution

Passez à une version Cisco Secure Client 5.x prise en charge. Voir ID de bogue Cisco CSCsu22088 et ID de bogue Cisco CSCso42825.

Erreur : « Le certificat de serveur reçu ou sa chaîne n'est pas conforme aux normes FIPS. A VPN connection will not be established »

Le client signale que le certificat ou la chaîne du serveur n'est pas conforme à FIPS.

Solution

Si FIPS est requis sur le terminal, utilisez les certificats conformes FIPS sur la tête de réseau. Si cela n'est pas nécessaire, modifiez le fichier C:\ProgramData\Cisco\Cisco Secure Client\AnyConnectLocalPolicy.xml et définissez <FipsMode>false</FipsMode>, puis redémarrez (droits d'administration requis).

Erreur : « Échec de la validation du certificat »

Les utilisateurs ne peuvent pas lancer le client sécurisé Cisco et recevoir un échec de validation de certificat.

Solution

Pour l'authentification de certificat, importez le certificat client, configurez le profil pour l'authentification de certificat et sur ASA enable :

```
ssl certificate-authentication interface outside port 443
```

Assurez-vous que le certificat du serveur correspond au nom de domaine complet dans la liste des serveurs de profils.

Erreur : « Le service d'agent RPV a détecté un problème et doit fermer. We are sorry for the inconvenience »

Le service vpnagent.exe échoue lors de l'installation, de la mise à niveau ou de la connexion.

Solution

1. Redémarrez Cisco Secure Client - AnyConnect VPN Agent dans les services Windows.
2. Réparer ou réinstaller à partir du déploiement Web de tête de réseau.
3. Collectez le DART si le service échoue plusieurs fois. Pour les conflits Citrix, consultez l'ID de bogue Cisco CSCsq49102.

Erreur : « Ce programme d'installation n'a pas pu être ouvert. Verify that the package exists »

Échec du déploiement Web avec une erreur Windows Installer indiquant que le package n'a pas pu être ouvert.

Solution

1. Vérifiez que le MSI a été téléchargé complètement ; réessayez à partir du portail de tête de réseau.
2. Désactiver temporairement l'antivirus agressif sur le dossier de téléchargement ; collecter le journal MSI détaillé.
3. Vérifiez que le service Windows Installer est en cours d'exécution.
4. Si le problème persiste, collectez les journaux DART/MSI et ouvrez un dossier TAC.

Erreur : « Erreur lors de l’application des transformations. Verify that the specified transform paths are valid. »

Le téléchargement automatique à partir de la tête de réseau échoue, parfois en raison d'une transformation MST corrompue.

Solution

1. Supprimez la transformation MST personnalisée de la définition d'installation personnalisée AnyConnect de tête de réseau.
2. Rechargez l'image du client sécurisé correcte sur la tête de réseau.
3. Dans ASDM : Network (Client) Access > AnyConnect Custom > Installs — Supprime les entrées en double ; conservez l'image active sous les paramètres du client.

Erreur : « La reconnexion au RPV a entraîné une modification des paramètres de configuration. Les paramètres du RPV sont en cours de réinitialisation. Il sera peut-être nécessaire de restaurer les applications qui utilisent le réseau privé. »

Ce message peut s'afficher après la reconnexion lorsque les paramètres Push de tête de réseau changent.

Solution

```
group-policy <Name> attributes
 webvpn
  anyconnect mtu 1200
```

Erreur du client sécurisé Cisco lors de la connexion

Problème : La connexion VPN n'est pas autorisée via un proxy local. Vous pouvez modifier ce paramètre via les paramètres de profil AnyConnect.

Solution

```
<ProxySettings>IgnoreProxy</ProxySettings>
<AllowLocalProxyConnections>false</AllowLocalProxyConnections>
```

Erreur : Impossible d’activer AnyConnect Essentials tant que toutes ces sessions ne sont pas fermées.

ASDM affiche les sessions VPN SSL sans client en cours lors de l'activation d'AnyConnect Essentials.

Solution

AnyConnect Essentials ne peut pas être exécuté simultanément avec la licence VPN SSL partagée premium. Terminez les sessions VPN SSL sans client avant d'activer Essentials. Essentials n'inclut pas le VPN SSL sans client.

Erreur : Quelques utilisateurs obtiennent un message indiquant que la connexion a échoué, alors que d’autres sont en mesure de se connecter par l’intermédiaire du RPV d’AnyConnect.

Certains utilisateurs reçoivent Échec de connexion tandis que d'autres peuvent se connecter.

Solution

Assurez-vous que la pré-authentification (ou l'équivalent) n'est pas définie correctement pour les utilisateurs concernés. Comparez la stratégie de groupe et le mappage de profil de connexion.

Erreur : Le certificat que vous consultez ne correspond pas au nom du site que vous tentez d’afficher.

Lors de la mise à jour du profil sous Windows, la validation du certificat échoue par rapport à l'URL de connexion.

Solution

```
<ServerList>
 <HostEntry>
    <HostName>vpn1.example.com</HostName>
 </HostEntry>
</ServerList>
```

Remarque : Supprimez les entrées <HostAddress> qui utilisent l'adresse IP publique si le certificat est FQDN-only.

Le profil AnyConnect n’est pas dupliqué sur le serveur de secours après une panne.

Après le basculement de l'ASA, les fichiers associés au profil du client sécurisé sont manquants sur l'unité en veille.

Solution

Voir l'ID de bogue Cisco CSCtn7162. Solution : copiez manuellement les fichiers de profil dans la zone de secours. Vérifiez la synchronisation de la configuration de basculement avec état pour les profils VPN RA.

Message d'erreur : TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER

Le client sécurisé Cisco ne parvient pas à se connecter avec Impossible d'établir une connexion. Le journal des événements affiche TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER.

Solution

Cela se produit avec une très grande liste de split-tunnel (environ 180-200 entrées) plus d'autres attributs de stratégie de groupe (par exemple, dns-server).

1. Réduisez les entrées de la liste split-tunnel.
2. Désactiver temporairement DTLS :

```
group-policy groupName attributes
 webvpn
  anyconnect ssl dtls none
```

Voir l'ID de bogue Cisco CSCtc4170.

Message d'erreur : « Échec de la tentative de connexion en raison d’une entrée hôte non valide. »

La tentative de connexion a échoué en raison d'une entrée hôte non valide pendant l'authentification du certificat.

Solution

- Utilisez un nom d'hôte valide (FQDN) dans la liste des serveurs de profils.
- Utiliser le client sécurisé Cisco 5.x pris en charge.
- Supprimez la stratégie Cisco Secure Desktop (CSD) désapprouvée si elle est toujours présente.

Voir l'ID de bogue Cisco CSCti7316.

Erreur : « Veillez à ce que vos certificats de serveur puissent passer en mode strict si vous configurez un RPV permanent. »

Lorsque l'option Always-On est activée, le client peut signaler que les certificats du serveur doivent passer en mode strict.

Solution

Always-On nécessite un certificat de tête de réseau valide correspondant à l'URL de connexion. Le mode de certificat strict dans la stratégie locale provoque un échec si le certificat n'est pas approuvé ou ne correspond pas.

Reportez-vous à la section Certified by an Unknown Authority du Secure Client 5.1 Administrator Guide.

Erreur : « An internal error occurred in the Microsoft Windows HTTP Services » (une erreur interne s’est produite dans les services HTTP de Microsoft Windows)

DART peut afficher les échecs HttpSendRequest et Une erreur interne s'est produite dans les services HTTP Microsoft Windows avec des erreurs CTransportWinHttp.

Solution

Cela peut être dû à un état Winsock endommagé. À partir d'une invite de commandes avec élévation de privilèges : netsh winsock reset

Redémarrez Windows et consultez les conseils de Microsoft sur la réinitialisation de Winsock.

Erreur : « The SSL transport received a Secure Channel Failure. May be a result of a unsupported crypto configuration on the Secure Gateway. »

Le DART du client sécurisé Cisco peut afficher les erreurs CTransportWinHttp et CTransPORT_ERROR_SECURE_CHANNEL_FAILURE lorsque la négociation TLS ou de chiffrement échoue entre le client et la tête de réseau.

Solution

1. Sur la tête de réseau, utilisez TLS 1.2+ et les suites de chiffrement modernes uniquement. N'activez pas DES, 3DES ou RC4.
2. Exemple ASA :

```
ssl cipher tlsv1.2 custom "AES256-GCM-SHA384:AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-R
```

3. Vérifiez la validité du certificat du serveur et la correspondance du nom de domaine complet.
4. Mettez à niveau le client et la tête de réseau vers les versions prises en charge.
5. Sous Windows, conservez Schannel à TLS 1.2+; n'affaiblissez pas le cryptage client pour les têtes de réseau obsolètes.

Informations connexes

- Dépannage de Cisco Secure Client (Guide de l'administrateur 5.1)
- Guide de dépannage du client VPN AnyConnect - Problèmes courants externes
- FAQ sur Cisco Secure Client/AnyConnect

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.