Client VPN - Forum aux questions

Contenu

Introduction

Ce document répond à des questions fréquemment posées au sujet du Client VPN Cisco.

Remarque : Voici les conventions d'attribution de noms des différents clients VPN :

- Versions de Cisco Secure VPN Client 1.0 à 1.1a uniquement
- Versions 2.x du Client VPN 3000 de Cisco uniquement
- Client VPN Cisco 3.x et versions ultérieures uniquement

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco.](#)

Télécharger le logiciel du client VPN

Q. Où puis-je télécharger le logiciel Cisco VPN Client ?

A. Vous devez vous connecter et posséder un contrat de service valide pour accéder au logiciel Client VPN Cisco. Le logiciel Cisco VPN Client peut être téléchargé à partir de la page [Download Software](#) de Cisco (clients [enregistrés](#) uniquement). **Si vous n'avez pas de contrat de service valide associé à votre profil Cisco.com, vous ne pouvez pas ouvrir de session ni télécharger le logiciel du client VPN.**

Pour obtenir un contrat de service valide, vous pouvez :

- Contactez votre équipe de compte Cisco si vous avez un contrat d'achat direct.
- [Contactez un partenaire ou un revendeur Cisco afin d'acheter un contrat de service.](#)
- Utilisez le [gestionnaire de profil (clients](#) enregistrés seulement) afin de mettre à jour votre

profil Cisco.com et de demander l'association à un accord de service.

Q. La zone de téléchargement du client VPN Cisco semble vide. Pourquoi ?

A. Quand vous atteignez la zone de client VPN du centre logiciel (clients inscrits seulement), veillez à sélectionner la zone de téléchargements pour le système d'exploitation voulu au milieu de la page.

Q. Comment puis-je désactiver la fonctionnalité de pare-feu dynamique lors de l'installation du client VPN Cisco ?

A. Pour les versions du client VPN antérieures à 5.0 :

Reportez-vous à la section Modifications de la documentation des Notes de publication relatives au client VPN Version 4.7 pour en savoir plus sur les deux rubriques « Utilisation de MSI pour installer le client VPN Windows sans pare-feu avec état » et « Utilisation d'InstallShield pour installer le client VPN Windows sans pare-feu avec état ».

Pour les versions du client VPN postérieures à 5.0 :

Àpartir de la version 5.0.3.0560 du client VPN Cisco, un indicateur d'installation MSI a été ajouté pour éviter l'installation de la guilde dans les fichiers de pare-feu :

```
msiexec.exe /i vpnclient_setup.msi DONTINSTALLFIREWALL=1
```

Référez-vous à Ignorer l'installation des fichiers de pare-feu lorsque le pare-feu dynamique n'est pas requis pour plus d'informations à ce sujet.

Q. Comment désinstaller ou mettre à niveau le client VPN Cisco ?

A. Référez-vous à Suppression d'une version de client VPN installée avec MSI Installer pour plus d'informations sur la désinstallation manuelle (InstallShield), puis mettez à niveau la version 3.5 et ultérieure du client VPN Cisco pour Windows 2000 et Windows XP.

Le logiciel Cisco VPN Client pour Windows 2000 et Windows XP peut télécharger automatiquement les mises à jour et les nouvelles versions en toute sécurité via un tunnel à partir d'un concentrateur VPN 3000 ou d'un autre serveur VPN pouvant fournir des notifications. La condition préalable minimale pour cela est que le client VPN pour Windows 4.6 ou version ultérieure doit être installé sur les PC des utilisateurs distants pour qu'ils puissent utiliser la fonctionnalité de mise à jour automatique.

Avec cette fonctionnalité, les utilisateurs n'ont pas besoin de désinstaller une ancienne version du logiciel, de redémarrer, d'installer la nouvelle version, puis de redémarrer une nouvelle fois. Au lieu de cela, un administrateur met des mises à jour et des profils à disposition sur un serveur Web et, quand un utilisateur distant démarre le client VPN, le logiciel détecte qu'un téléchargement est disponible et l'obtient automatiquement. Pour plus d'informations, reportez-vous à Gestion des mises à jour automatiques et Fonctionnement de la mise à jour automatique.

Pour plus d'informations sur le mode de configuration de la mise à jour du client sur un dispositif de sécurité adaptatif dédié de la gamme Cisco ASA 5500 à l'aide d'ASDM, reportez-vous à Configuration de la mise à jour du logiciel du client à l'aide d'ASDM.

Q. Je veux personnaliser les clients VPN pour Vista. Je me rends compte, avec la nouvelle version du client VPN pour Vista, qu'il n'existe aucun fichier comme oem.mst. Comment pouvons-nous personnaliser les nouvelles versions du client VPN (5.x) ou à quel emplacement puis-je trouver ce fichier ?

A. Le fichier MST n'est plus fourni avec le client VPN, mais vous pouvez le télécharger à partir de la page Download Software (enregistré uniquement) :

Nom de fichier : Lisez-moi et MST pour installation sur la version internationale de Windows.

Système d'exploitation

Q. Est-ce que Cisco fournit un client VPN pour Windows Vista ?

A. La nouvelle version de Cisco VPN Client 5.0.07 prend en charge Windows Vista sur x86 (32 bits) et x64. Pour plus d'informations, reportez-vous aux Notes de publication relatives à 5.0.07.0240.

Remarque : Cisco VPN Client n'est pris en charge que sur l'installation propre de Windows Vista, ce qui signifie qu'une mise à niveau de tout système d'exploitation Windows vers Windows Vista n'est pas prise en charge avec le logiciel client VPN. Vous devez procéder à une nouvelle installation de Windows Vista, puis installer le logiciel du client VPN Vista.

Remarque : Si vous n'avez pas de contrat de service valide associé à votre profil Cisco.com, vous ne pouvez pas vous connecter et télécharger le logiciel VPN Client. Pour plus d'informations, reportez-vous à Télécharger le logiciel du client VPN.

Conseil : Le client VPN Cisco AnyConnect est désormais disponible pour les systèmes d'exploitation Windows, qui incluent Vista 32 et 64 bits. Le client AnyConnect prend en charge SSL et DTLS. Il ne prend pas en charge IPsec pour l'instant. En outre, AnyConnect n'est disponible que pour être utilisé avec un dispositif de sécurité adaptatif Cisco qui exécute la version 8.0(2) ou ultérieure. Le client peut également être utilisé en mode de lancement Web avec des dispositifs IOS exécutant la version 12.4(15)T. VPN 3000 n'est pas pris en charge.

Cisco AnyConnect VPN Client et ASA 8.0 peuvent être obtenus à partir du centre logiciel (clients inscrits seulement) . Pour plus d'informations sur le client AnyConnect, reportez-vous aux Notes de publication relatives à Cisco AnyConnect VPN Client. Pour plus d'informations sur ASA 8.0, reportez-vous aux Notes de publication relatives aux dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500.

Remarque : Si vous n'avez pas de contrat de service valide associé à votre profil Cisco.com, vous ne pouvez pas vous connecter et télécharger le logiciel AnyConnect VPN Client ou ASA. Pour plus d'informations, reportez-vous à Télécharger le logiciel du client VPN.

Q. Comment est-ce que je configure une connexion PPTP à partir d'un PC Microsoft Windows ?

A. La configuration dépend de la version de Microsoft Windows que vous exécutez. Vous devez contacter Microsoft pour obtenir ces informations spécifiques. Voici des instructions de configuration pour certaines des versions communes de Windows :

Windows 95

1. Installez Msdun13.exe.
2. Choisissez **Programs > Accessories > Dial Up Networking**.
3. Créez une connexion nommée « PPTP ».
4. Sélectionnez **VPN Adapter comme périphérique pour la connexion.**
5. Entrez l'adresse IP de l'interface publique du commutateur et cliquez sur **Finish**.
6. Retournez à la connexion que vous venez de créer, cliquez avec le bouton droit, puis choisissez **Properties**.
7. Sous Allowed Network Protocols, au minimum, désactivez **netbeui**.
8. Configurez le paramètre Advanced Options : Laissez les valeurs par défaut pour permettre au commutateur et au client de négocier automatiquement la méthode d'authentification.Activez **Require Encrypted Password pour forcer l'authentification CHAP (Challenge Handshake Authentication Protocol).**Activez **Require Encrypted Password et Require Data Encryption pour forcer l'authentification MS-CHAP.**

Windows 98

1. Exécutez les étapes suivantes afin d'installer la fonctionnalité PPTP : Choisissez **Start > Settings > Control Panel > Add New Hardware** et cliquez sur **Next**.Cliquez sur **Select from List**, choisissez **Network Adapter** et cliquez sur **Next**.Choisissez **Microsoft dans le panneau de gauche et Microsoft VPN Adapter dans le panneau de droite.**
2. Exécutez les étapes suivantes afin de configurer la fonctionnalité PPTP : Choisissez **Start > Programs > Accessories > Communications > Dial Up Networking**.Cliquez sur **Make new connection** et choisissez **Microsoft VPN Adapter pour Select a device.** L'adresse IP du serveur VPN est égale au point de terminaison du tunnel 3000.
3. Exécutez les étapes suivantes afin de modifier le PC pour autoriser également le protocole PAP (Password Authentication Protocol) : **Remarque :** L'authentification par défaut de Windows 98 consiste à utiliser le chiffrement par mot de passe (CHAP ou MS-CHAP).Choisissez **Properties > Server types**.Désactivez **Require encrypted password**. Vous pouvez configurer le chiffrement des données (Microsoft Point-to-Point Encryption [MPPE] ou pas de MPPE) dans cette zone.

Windows 2000

1. **Choisissez Start > Programs > Accessories > Communications > Network and Dialup connections.**
2. Cliquez sur **Make new connection**, puis sur **Next**.
3. Choisissez **Connect to a private network through the Internet and Dial a connection prior (ne sélectionnez pas cette option si vous avez un réseau local) et cliquez sur Next**.
4. Entrez le nom d'hôte ou l'adresse IP du point de terminaison du tunnel (3000).
5. Si vous devez changer le type de mot de passe, choisissez **Properties > Security for the connection > Advanced**. La valeur par défaut est MS-CHAP et MS-CHAP v2 (et non CHAP ou PAP). Vous pouvez configurer le chiffrement des données (MPPE ou pas de MPPE) dans cette zone.

Windows NT

Reportez-vous à [Installation, configuration et utilisation de PPTP avec les serveurs et clients Microsoft.]

Q. Quelles versions de système d'exploitation prennent en charge le Client VPN Cisco ?

A. La prise en charge d'autres systèmes d'exploitation est ajoutée en permanence pour le client VPN. Reportez-vous à la section Configuration requise dans les notes de publication pour la version 5.0.07 du client VPN pour en savoir plus, ou reportez-vous à Matériel Cisco et clients VPN prenant en charge IPsec/PPTP/L2TP.

Remarques :

- Le client VPN inclut la prise en charge des stations de travail double processeur et double cœur pour Windows XP et Windows Vista.
- La version 4.8.00.440 du client VPN Windows était la version finale qui prenait officiellement en charge le système d'exploitation Windows 98.
- La version 4.6.04.0043 du client VPN Windows était la version finale qui prenait officiellement en charge le système d'exploitation Windows NT.
- Le Client VPN Cisco Version 5.0.07 prend en charge Windows Vista et Windows 7 dans les éditions x86 (32 bits) et x64 (64 bits).
- Le Client VPN Cisco prend en charge Windows XP 32 bits uniquement, mais Windows XP 64 bits n'est pas pris en charge.**Remarque :** Windows Vista 32 bits était pris en charge dans toutes les versions 5.x. Le Client VPN Cisco Version 5.0.07 a ajouté la prise en charge 64 bits.

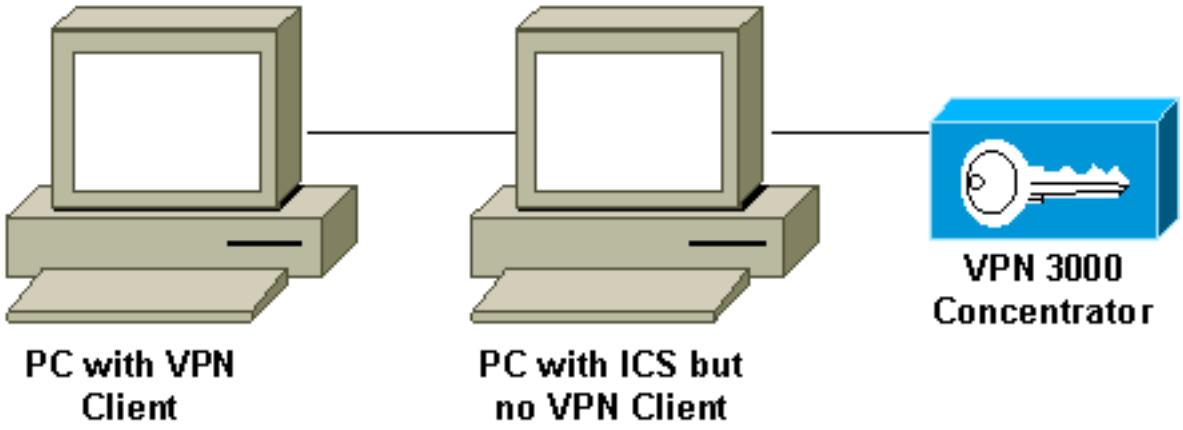
Q. Dois-je être un administrateur sur les ordinateurs Windows NT/2000 afin de charger le client VPN ?

A. Oui, vous devez disposer de privilèges administrateur afin d'installer le client VPN sur Windows NT et Windows 2000, car ces systèmes d'exploitation nécessitent des privilèges administrateur pour la liaison aux pilotes réseau existants ou pour l'installation de nouveaux pilotes réseau. Le logiciel du client VPN est un logiciel réseau. Vous devez disposer de privilèges administrateur pour l'installer.

Q. Le Client VPN Cisco peut-il fonctionner avec le Partage de connexion Internet Microsoft installé sur le même ordinateur ?

A. Non, le Client VPN 3000 de Cisco n'est pas compatible avec le Partage de connexion Internet Microsoft sur le même ordinateur. Vous devez désinstaller le Partage de connexion Internet avant de pouvoir installer le client VPN. Pour plus d'informations, reportez-vous à Désactivation du Partage de connexion Internet lors de la préparation de l'installation ou de la mise à niveau vers le Client VPN Cisco 3.5.x sur Microsoft Windows XP.

Bien que le fait d'avoir le client VPN et le Partage de connexion Internet sur le même PC ne fonctionne pas, cet arrangement fonctionne.



Q. Mon client VPN semble se connecter seulement à certaines adresses. J'exécute Windows XP. Que dois-je faire ?

A. Vérifiez que le pare-feu intégré dans Windows XP est désactivé.

Q. Le Client VPN Cisco est-il compatible avec le pare-feu avec état Windows XP ?

A. Ce problème a été résolu. Pour plus d'informations, consultez le bogue Cisco ayant l'ID CSCdx15865 (clients inscrits seulement) dans la Boîte à outils des bogues.

Q. Lorsque j'installe le client VPN sur Windows XP et Windows 2000, est-ce que l'interface multi-utilisateur est désactivée ?

A. L'installation désactive l'écran d'accueil et le changement rapide d'utilisateur. Pour plus d'informations, consultez le bogue Cisco ayant l'ID CSCdu24073 (clients inscrits seulement) dans la Boîte à outils des bogues.

Q. Comment puis-faire en sorte que le client VPN pour Linux passe à l'arrière-plan après l'exécution ? Si je lance une connexion telle que vpnclient connect foo, la connexion est établie, mais le shell est retourné.

A. Une fois connecté, tapez :

- ^Z
- bg

Q. Quand j'installe le Client VPN Cisco sur Windows XP Édition familiale, la barre des tâches n'est pas visible. Comment annuler cet état ?

A. Choisissez **Control Panel > Network Connections > Remove Network Bridge pour régler ce paramètre.**

Q. Quand j'essaye d'installer le client VPN Linux sur RedHat 8.0, un message d'erreur qui indique que le module ne peut pas être chargé, car il a été compilé avec GCC 2 et le noyau a été compilé avec GCC 3.2 s'affiche. Que dois-je faire ?

A. Cela est dû au fait que la nouvelle version de RedHat comprend une version plus récente du compilateur GCC (3.2+), ce qui provoque l'échec du Client VPN Cisco actuel. Ce problème a été résolu et la fonction est disponible dans le Client VPN Cisco 3.6.2a. Pour plus d'informations, consultez le bogue Cisco ayant l'ID CSCdy49082 (clients inscrits seulement) dans la Boîte à outils des bogues ou téléchargez le logiciel à partir du centre logiciel VPN (clients inscrits seulement) .

Q. Pourquoi le logiciel désactive-t-il le changement rapide d'utilisateur quand j'installe le client VPN 3.1 sur Windows XP ?

A. Microsoft désactive automatiquement le changement rapide d'utilisateur dans Windows XP lorsqu'un fichier GINA.dll est spécifié dans le Registre. Le Client VPN Cisco installe le fichier CSgina.dll pour implémenter la fonctionnalité SBL (Start Before Login). Si vous avez besoin du changement rapide d'utilisateur, désactivez la fonctionnalité SBL. Les utilisateurs inscrits peuvent obtenir d'autres informations dans le bogue Cisco ayant l'ID CSCdu24073 (clients inscrits seulement) dans la Boîte à outils des bogues.

Q. Le client VPN IPsec prend-il en charge la fonctionnalité SBL (Start Before Logon) sous Windows 7 ?

A. La fonctionnalité SBL n'est pas prise en charge sur les clients VPN IPsec sous Windows7. Il est pris en charge par le client VPN AnyConnect.

Messages d'erreur

Q. Quand j'installe le Client VPN Cisco 4.x, je reçois le message d'erreur suivant : **Avertissement 201 : The necessary VPN sub-system is not available. Vous ne pouvez pas vous connecter au serveur VPN distant**

A. Ce problème peut être causé par des packages de pare-feu installés sur votre ordinateur client VPN. Afin d'éviter ce message d'erreur, assurez-vous qu'aucun pare-feu ni logiciel antivirus n'est installé ou en cours d'exécution sur votre PC au moment de l'installation.

Q. J'ai effectué une mise à niveau vers Mac OS X 10.3 (connu sous le nom de « Panther »), mais mon Client VPN Cisco 4.x affiche à présent le message d'erreur suivant : **Connexion VPN sécurisée interrompue localement par le motif client : Impossible de contacter la passerelle de sécurité**

A. Vous devez ajouter UseLegacyIKEPort=0 au profil (fichier .pcf) qui figure dans le répertoire /etc/CiscoSystemsVPNClient/Profiles/ pour que le Client VPN Cisco 4.x fonctionne avec Mac OS X 10.3 (« Panther »).

Q. Lorsque je tente de désinstaller le client VPN, je reçois le message d'erreur suivant : **Message d'erreur : impossible de trouver le fichier de désinstallation...** Que signifie ce message d'erreur et comment puis-je effectuer correctement la désinstallation ?

A. Vérifiez dans le Panneau de configuration réseau que DNE (Deterministic NDIS Extender) n'a pas été installé. Choisissez également **Microsoft > Current Version > Uninstall pour rechercher le fichier de désinstallation.** Supprimez le fichier

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{5624C000-B109-11D4-9DB4-00E0290FCAC5}, puis retentez la désinstallation.

Q. Je ne peux pas installer le client VPN sur Windows 2000 Professionnel. Je reçois le message d'erreur suivant : `Impossible d'installer un fichier de support d'installation.` Défaillance Catastrophique. Que dois-je faire ?

A. Supprimez la clé **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall.** Redémarrez ensuite votre ordinateur, puis réinstallez le client VPN.

Remarque : afin de trouver la clé correcte pour le logiciel Client VPN Cisco sous le chemin HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall\<*clé à déterminer*>, accédez à HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\, puis cliquez sur **Client VPN**. Dans la fenêtre de droite, affichez Uninstall Path (sous la colonne Name). La colonne Data correspondante affiche la valeur de la clé du client VPN. Prenez note de cette clé, accédez à HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall\, sélectionnez la clé identifiée, puis supprimez-la.

Pour plus d'informations, reportez-vous à Dépannage des erreurs d'initialisation et au bogue Cisco ayant l'ID CSCdv15391 (clients inscrits seulement) dans la Boîte à outils des bogues.

Q. Quand j'essaye d'installer le client VPN Linux sur RedHat 8.0, je reçois un message d'erreur qui indique que le module ne peut pas être chargé, car il a été compilé avec GCC 2 et le noyau a été compilé avec GCC 3.2. Que dois-je faire ?

A. Ce problème se pose parce que la nouvelle version de RedHat comprend une version plus récente du compilateur GCC (3.2+), ce qui provoque l'échec du Client VPN Cisco actuel. Ce problème a été résolu et la fonction est disponible dans le Client VPN Cisco 3.6.2a. Pour plus d'informations, consultez le bogue Cisco ayant l'ID CSCdy49082 (clients inscrits seulement) dans la Boîte à outils des bogues ou téléchargez le logiciel à partir du centre logiciel VPN (clients inscrits seulement) .

Q. Je reçois un message d'erreur qui indique qu'un pair ne répond plus lorsque mon client Linux 3.5 essaie d'établir une connexion IPsec à un dispositif PIX ou un concentrateur VPN 3000. Que dois-je faire ?

A. Le symptôme de ce problème est que le client Linux semble essayer de se connecter, mais n'obtient jamais de réponse du périphérique de passerelle.

Le système d'exploitation Linux a un pare-feu intégré (ipchains) qui bloque le port UDP 500, le port UDP 1000 et les paquets ESP (Encapsulating Security Payload). Étant donné que le pare-feu est activé par défaut, vous devez le désactiver ou ouvrir les ports pour la communication IPsec à la fois pour les connexions entrantes et sortantes afin de résoudre le problème.

Q. Je reçois une erreur d'extension de noyau quand j'essaye d'exécuter le Client VPN 5000 5.2.2 de Cisco sur Mac OS X 10.3. Que dois-je faire ?

A. Comme indiqué dans les notes de publication relatives au produit, le Client VPN 5000 de Cisco est pris en charge jusqu'à la version 10.1.x et, par conséquent, n'est pas pris en charge sur la

version 10.3. Il est possible de faire fonctionner le client VPN quand vous réinitialisez les autorisations sur deux des fichiers installés après avoir exécuté le script d'installation. Voici un exemple :

Remarque : Cette configuration *n*'est *pas* prise en charge par Cisco.

```
sudo chown -R root:wheel /System/Library/Extensions/VPN5000.kext
sudo chmod -R go-w /System/Library/Extensions/VPN5000.kext
```

Q. Je ne peux pas installer la nouvelle version du Client VPN Cisco. Lors de l'installation, je reçois l'un des messages d'erreur suivants : « **Error DNEinst execution error while installing DNE, return code -2146500093 » ou « InstallDNE Error: DNEinst execution error while installing DNE, returncode -2147024891.**" This issue occurs when I installed the Deterministic Network Enhancer. Ce problème se pose quand j'ai installé Deterministic Network Enhancer.

A. Installez la dernière mise à niveau de DNE à partir de Deterministic Networks .

Q. J'obtiens les journaux suivants pour le Client VPN Cisco quand j'établis une connexion :

```
208    15:09:08.619  01/17/08  Sev=Debug/7CVPND/0x63400015
Value for ini parameter VAEnableAlt is 1.

209    15:09:08.619  01/17/08  Sev=Warning/2CVPND/0xE3400003
Function RegOpenKey failed with an error code of 0x00000002(WindowsVirtualAdapter:558)

210    15:09:08.619  01/17/08  Sev=Warning/3CVPND/0xE340000C
The Client was unable to enable the Virtual Adapter because it could not open the device.
```

A. Il s'agit d'un message d'erreur assez générique, qui nécessite habituellement une désinstallation manuelle du client. Suivez les instructions de ce lien. Suppression d'une version de client VPN installée avec le programme d'installation MSI.

Une fois que vous effectué la désinstallation, assurez-vous de redémarrer. Réinstallez alors le client. Assurez-vous que vous êtes connecté en tant qu'utilisateur qui a des droits d'administrateur sur l'ordinateur local.

Q. Lorsque je tente de connecter le client VPN Cisco sur un Mac OS, je reçois ce message d'erreur : **Erreur 51 - Impossible de communiquer avec le sous-système VPN.** Comment puis-je résoudre ce problème ?

A. Le problème peut être résolu si vous redémarrez le service après avoir fermé le client VPN de la façon suivante :

Pour arrêter :

```
sudo kextunload -b com.cisco.nke.ipsec
```

Pour démarrer :

`sudo kextload /System/Library/Extensions/CiscoVPN/CiscoVPN`
Vérifiez également que les éléments suivants s'exécutent sur la même machine où le client VPN est installé et désactivez-les.

- Tous les logiciels virtuels (tels que, VMWare Fusions, Parallels, Crossovers).
- Tout logiciel antivirus/pare-feu.
- Compatibilité du client VPN avec le système d'exploitation 64 bits ; reportez-vous aux notes de version du client VPN Cisco.

Q. Je reçois le message d'erreur « Reason 442: failed to enable virtual adapter ». Comment est-ce que je peux résoudre cette erreur ?

A. Le message d'erreur `Reason 442: failed to enable virtual adapter s'affiche une fois que Vista a signalé qu'une adresse IP en double a été détectée.` Les connexions ultérieures échouent avec le même message, mais Vista ne signale pas qu'une adresse IP en double a été détectée. Pour plus d'informations sur la façon de résoudre ce problème, reportez-vous à Une adresse IP en double déclenche l'erreur 442 sur Windows Vista.

Q. Quand j'installe le Client VPN Cisco, le message d'erreur **`Deterministic Network Enhancer Add Plugin Failed s'affiche.`** Comment cette erreur est-elle résolue ?

A. L'installation de l'adaptateur DNE peut résoudre le problème. Il est préférable d'utiliser la version Installshield pour l'installation au lieu de MSI.

Q. J'ai reçu cette erreur : **`Reason 442: échec de l'activation de la carte virtuelle.`** Comment puis-je résoudre ce problème ?

A. Cette erreur apparaît après que Windows 7 et Windows Vista aient signalé une adresse IP en double détectée. Les connexions suivantes échouent avec le même message, mais le système d'exploitation ne signale pas que l'adresse IP dupliquée est détectée. Référez-vous à Dupliquer l'erreur 442 des déclencheurs d'adresse IP sur Windows 7 et Windows Vista pour plus d'informations sur la façon de résoudre ce problème.

Q. Lorsque j'essaie de lancer le client VPN 4.9 pour MAC OS 10.6, je reçois cette erreur : **`Erreur 51 : Impossible de communiquer avec le sous-système vpn.`** Comment résoudre ce problème ?

A. Ce problème se produit parce que la prise en charge 64 bits n'est pas disponible avec le client VPN Cisco pour MAC OS version 4.9. Comme solution de contournement, vous pouvez démarrer en mode noyau 32 bits. Pour plus d'informations, référez-vous à ID de bogue Cisco CSCth11092 (clients enregistrés uniquement) et client VPN Cisco pour les notes de version MAC OSX.

Compatibilité avec des tiers

Q. Est-ce que le client Nortel est compatible avec les concentrateurs VPN 3000 de Cisco ?

A. Non. Le client Nortel ne peut pas se connecter au concentrateur Cisco VPN 3000.

Q. Est-ce que des clients VPN d'autres fabricants, tels que le client VPN Contivity de Nortel, peuvent être installés simultanément avec le Client VPN Cisco ?

A. Non. Il existe des problèmes connus lorsque plusieurs clients VPN sont installés sur le même PC.

Q. Est-ce que les Clients VPN Cisco sont pris en charge avec des concentrateurs VPN tiers ?

A. Les Clients VPN Cisco ne sont pas pris en charge avec des concentrateurs VPN tiers.

Authentification

Q. Comment est-ce que les Clients VPN Cisco versions 1.1 et 3.x stockent-ils en interne les certificats numériques (X.509v3) ?

A. Le Client VPN Cisco 1.1 dispose de son propre magasin de certificats. Le Client VPN Cisco 3.x peut stocker les certificats dans le magasin Microsoft à l'aide de l'interface CAPI (Common-Application Programming Interface) ou dans le magasin de Cisco (RSA Data Security).

Q. Est-ce que je peux avoir les mêmes noms de groupe et d'utilisateur sur le concentrateur VPN ?

A. Non, les noms de groupe et d'utilisateur ne peuvent pas être identiques. Il s'agit d'un problème identifié, trouvé dans les versions de logiciel 2.5.2 et 3.0, et intégré à 3.1.2. Pour plus d'informations, consultez le bogue Cisco ayant l'ID CSCdw29034 (clients inscrits seulement) dans la Boîte à outils des bogues.

Q. Est-ce que les cartes « full-challenge » telles que Defender sont prises en charge sur le Client VPN Cisco pour PIX ?

A. Non, les cartes de ce type ne sont pas prises en charge.

Version de logiciel du client VPN

Q. Qu'est-il arrivé à l'option « Set MTU Utility » qui figurait dans les versions 2.5.2 et antérieures du Client VPN Cisco ?

A. Le Client VPN Cisco règle maintenant la taille de l'unité de transmission maximale (MTU). L'option Set MTU Utility ne constitue plus une étape d'installation requise. L'option Set MTU est utilisée principalement pour le dépannage des problèmes de connectivité. Le chemin d'accès pour sélectionner l'option Set MTU pour un ordinateur Windows est **Start > Programs > Cisco Systems VPN Client > SetMTU**. Pour plus d'informations sur l'option Set MTU et la définition de cette option dans d'autres systèmes d'exploitation, reportez-vous à Modification de la taille de l'unité de transmission maximale via l'option Set MTU.

Q. Quelles sont les langues prises en charge dans les versions de l'interface

utilisateur graphique du Client VPN Cisco postérieures à 4.0 ?

A. Les langues prises en charge dans les versions de l'interface utilisateur graphique du Client VPN Cisco postérieures à 4.0 sont le canadien, le français et le japonais.

Q. Quels pare-feu personnels sont pris en charge avec le Client VPN Cisco ?

A. Pour offrir encore plus de sécurité, le client VPN peut imposer le fonctionnement d'un pare-feu pris en charge ou recevoir une stratégie de pare-feu avec état pour le trafic lié à Internet.

Actuellement, le client VPN 5.0 prend en charge les pare-feu personnels suivants :

- BlackIce Defender
- Cisco Security Agent
- Sygate Personal Firewall
- Sygate Personal Firewall Pro
- Sygate Security Agent
- ZoneAlarm
- ZoneAlarmPro

Depuis la version 3.1, une nouvelle fonctionnalité est ajoutée au concentrateur VPN 3000 qui détecte le logiciel pare-feu personnel que les utilisateurs distants ont installé et empêche les utilisateurs de se connecter en l'absence du logiciel approprié. Choisissez **Configuration > User Management > Groups > Client FW** et cliquez sur l'onglet du groupe pour lequel configurer cette fonctionnalité.

Pour plus d'informations sur l'application de la stratégie de pare-feu sur un ordinateur du Client VPN Cisco, reportez-vous à Scénarios de configuration de pare-feu.

Q. Existe-t-il des problèmes de connectivité lors de l'utilisation du Client VPN Cisco 3.x avec AOL 7.0 ?

A. Le Client VPN Cisco ne fonctionne pas avec AOL 7.0 sans l'utilisation de la transmission tunnel partagée. Pour plus d'informations, consultez le bogue Cisco ayant l'ID CSCdx04842 (clients inscrits seulement) dans la Boîte à outils des bogues.

Configuration du logiciel du client VPN

Q. Pourquoi est-ce que le Client VPN Cisco se déconnecte après 30 minutes ? Est-ce que je peux prolonger cette période ?

A. S'il n'y a aucune activité de communication sur une connexion utilisateur pendant cette période de 30 minutes, le système met fin à la connexion. La valeur du délai d'attente inactif par défaut est de 30 minutes, avec une valeur minimale autorisée de 1 minute et une valeur maximale autorisée de 2 147 483 647 minutes (plus de 4 000 ans).

Choisissez **Configuration > User Management > Groups** et choisissez le nom du groupe approprié pour modifier la valeur du délai d'attente inactif. Choisissez **Modify Group**, cliquez sur l'onglet **HW Client et tapez la valeur voulue dans le champ User Idle Timeout.** Tapez **0afin de désactiver le délai d'attente et d'autoriser une période d'inactivité illimitée.**

Q. Le Client VPN Cisco peut-il être déployé avec tous les paramètres préconfigurés ?

A. Si le fichier vpnclient.ini est fourni avec le logiciel du client VPN lors de la première installation, le client VPN est configuré automatiquement pendant l'installation. Vous pouvez également distribuer les fichiers des profils (un fichier .pcf pour chaque entrée de connexion) en tant que profils de connexion préconfigurés pour la configuration automatique. Pour distribuer des copies préconfigurées du logiciel du client VPN aux utilisateurs pour l'installation, exécutez les étapes suivantes :

1. Copiez les fichiers du logiciel du client VPN du CD-ROM de distribution dans chaque répertoire où vous avez créé un fichier vpnclient.ini (global) et des profils de connexion distincts pour un ensemble d'utilisateurs.**Remarque :** Pour la plate-forme Mac OS X, les fichiers préconfigurés sont placés dans les dossiers Profiles and Resources (Profils et ressources) avant l'installation du client VPN. Le fichier vpnclient.ini est placé dans le répertoire du programme d'installation. Vous devez placer les fichiers vpnclient.ini personnalisés dans le répertoire du programme d'installation du client VPN au même niveau que les dossiers Profiles et Resources. Pour plus d'informations, consultez le chapitre 2 du Guide de l'utilisateur du client VPN pour Mac OS X.
2. Préparez et distribuez le logiciel fourni. Distribution par CD-ROM ou via le réseau. Veillez à ce que le fichier vpnclient.ini et les fichiers des profils soient dans le même répertoire avec tous les fichiers image de CD-ROM. Vous pouvez demander aux utilisateurs de procéder à l'installation à partir de ce répertoire via une connexion réseau ; ou vous pouvez copier tous les fichiers sur un nouveau CD-ROM pour distribution ; ou vous pouvez créer un fichier zip à extraction automatique qui contient tous les fichiers de ce répertoire et demander aux utilisateurs de le télécharger, puis d'installer le logiciel.
3. Fournissez aux utilisateurs toutes les autres instructions et informations de configuration nécessaires. Consultez le chapitre 2 du Guide de l'utilisateur du client VPN pour votre plate-forme.

Q. Il semble que le Client VPN Cisco est en conflit avec ma carte NIC. Comment puis-je résoudre ce problème ?

A. Assurez-vous que vous exécutez les derniers pilotes sur la carte NIC. Cela est toujours recommandé. Si possible, effectuez des tests pour savoir si le problème est spécifique au système d'exploitation, au matériel du PC et à d'autres cartes NIC.

Q. Comment automatiser la connexion du Client VPN Cisco à partir de l'accès réseau à distance ?

A. Choisissez **Options > Properties > Connections** et faites en sorte que le Client VPN Cisco extraie une entrée de l'annuaire téléphonique d'accès réseau à distance afin d'automatiser entièrement l'accès à distance dans la connexion VPN.

Q. Comment configurer le concentrateur VPN 3000 de Cisco pour informer les utilisateurs distants d'une mise à jour du client VPN ?

A. Vous pouvez informer les utilisateurs du client VPN quand il est temps de mettre à jour le

logiciel du client VPN sur leurs systèmes distants. Pour une approche pas à pas, reportez-vous à Notification aux utilisateurs distants d'une mise à jour du client . Assurez-vous de taper les informations de version sous la forme « (Rel) », comme indiqué dans l'étape 7 du processus.

Q. Quelle peut être la cause d'un retard avant l'affichage du Client VPN Cisco, particulièrement lorsque l'option « Start Before Logon » est activée ?

A. Le Client VPN Cisco est en mode *de secours.* Ce mode contribue au retard. En mode de secours, le client VPN fonctionne différemment lorsque l'option « Start Before Logon » est utilisée. Lorsqu'il fonctionne en mode de secours, le client VPN ne vérifie pas si les services Windows nécessaires ont démarré. Par conséquent, la connexion VPN peut échouer si elle est initiée trop rapidement.Désinstallez le client VPN Cisco et supprimez les applications incriminées pour autoriser le démarrage sans être en mode « retour arrière ». Réinstallez ensuite le Client VPN Cisco. Pour plus d'informations sur le mode de secours, reportez-vous à Start Before Logon.

Pour plus d'informations, consultez le bogue Cisco ayant l'ID CSCdt88922 (clients inscrits seulement) et CSCdt55739 (clients inscrits seulement) dans la Boîte à outils des bogues.

Q. Je dois comprendre la différence entre ipsecdialer.exe et vpngui.exe. Pourquoi, alors que vpngui.exe est installé dans STARTUP dans mon ordinateur Windows XP, dois-je quand même démarrer manuellement ipsecdialer afin d'atteindre les ressources de mes sociétés ? Et (indépendamment de la taille) ces programmes semblent déclencher la même action : une connexion VPN au réseau de ma société.

A. ipsecdialer.exe était le mécanisme de lancement initial pour le Client VPN Cisco version 3.x. Quand l'interface utilisateur graphique a été modifiée dans les versions 4.x, un fichier exécutable appelé vpngui.exe a été créé. Le fichier ipsecdialer.exe a été transmis en nom uniquement pour rétrocompatibilité et lance seulement le fichier vpngui.exe. C'est la raison pour laquelle vous pouvez voir la différence dans la taille de fichier.

Ainsi, quand vous passez à une version antérieure (de la version 4.x à la version 3.x) du Client VPN Cisco, vous avez besoin du fichier ipsecdialer.exe pour lancer le fichier vpngui.exe.

Q. Puis-je supprimer en toute sécurité l'icône VPN de démarrage ? Pourquoi est-ce nécessaire ?

A. Le Client VPN Cisco dans le dossier de démarrage prend en charge la fonctionnalité « Start Before Logon ». Si vous n'utilisez pas la fonctionnalité, vous n'en avez pas besoin dans le dossier de démarrage.

Q. Pourquoi est-ce que « user_logon » a été ajouté et non au niveau du raccourci pour ipsecdialer.exe ? Quelle est la fonction de « user_logon » ?

A. La fonctionnalité « Start Before Logon » nécessite « user_logon », mais un lancement normal du Client VPN Cisco par l'utilisateur n'en a pas besoin.

Problèmes NAT/PAT

Q. Je rencontre des problèmes avec seulement un client VPN (pour les versions 3.3 et antérieures) en mesure de se connecter via un périphérique PAT (Port Address Translation). Que puis-je faire pour remédier à ce problème ?

A. Un bogue dans plusieurs implémentations PAT et NAT (Network Address Translation) a eu pour conséquence que des ports inférieurs à 1024 n'ont pas été traduits. Sur le Client VPN Cisco 3.1, même avec la transparence NAT activée, la session ISAKMP (Internet Security Association and Key Management Protocol) utilise UDP 512. Le premier client VPN passe par le périphérique PAT et garde le port source 512 sur l'extérieur. Quand le deuxième client VPN se connecte, le port 512 est déjà en service. La tentative échoue.

Il y a trois solutions de contournement possibles.

- Réparez le périphérique PAT.
- Mettez à niveau les clients VPN vers 3.4 et utilisez l'encapsulation TCP.
- Installez un VPN 3002 qui remplace tous les clients VPN.

Q. Deux ordinateurs portables peuvent-ils être connectés au Client VPN Cisco à partir du même emplacement ?

A. Deux clients peuvent se connecter à la même tête de réseau à partir du même emplacement tant qu'ils ne sont pas tous deux derrière un périphérique qui implémente PAT, par exemple un pare-feu/routeur SOHO. De nombreux périphériques PAT peuvent associer UNE connexion VPN à un client derrière, mais pas deux. Afin de permettre à deux clients VPN de se connecter à partir du même emplacement derrière un périphérique PAT, activez un type d'encapsulation, par exemple NAT-T, IPSec sur UDP ou IPsec sur TCP au niveau de la tête de réseau. Généralement, une encapsulation NAT-T ou autre doit être activée si N'IMPORTE QUEL périphérique NAT se trouve entre le client et la tête de réseau.

Divers

Q. Quand je me connecte au réseau au bureau en utilisant mon ordinateur portable, puis que je ramène le portable à mon domicile, j'ai des problèmes pour me connecter au concentrateur VPN 3000. Quel est le problème ?

A. Il est possible que l'ordinateur portable conserve les informations de routage de la connexion LAN. Pour plus d'informations sur la façon de résoudre ce problème, reportez-vous à Clients VPN avec des problèmes de routage Microsoft.

Q. Comment puis-je savoir si un client VPN est connecté au concentrateur VPN ?

A. Vérifiez la clé de Registre nommée HKLM\Software\Cisco Systems\VPN Client\TunnelEstablished. Si un tunnel est en activité, la valeur est 1. Si aucun tunnel n'est présent, la valeur est 0.

Q. J'ai des problèmes avec la connexion NetMeeting entre un PC derrière un concentrateur VPN et un client VPN, mais la connexion fonctionne lors de l'exécution entre le PC et un client VPN derrière un concentrateur VPN. Comment

est-ce que je peux résoudre ce problème ?

A. Suivez les étapes appropriées mentionnées ici afin de contrôler les paramètres de connexion :

- Sur le lecteur principal du PC, choisissez **Program Files > Cisco Systems > VPN Client > Profiles**. Cliquez avec le bouton droit sur le profil que vous utilisez, puis choisissez **Open With** afin d'ouvrir le profil dans un éditeur de texte (tel que le Notepad). (Lorsque vous choisissez le programme à utiliser, veillez à désactiver la case à cocher qui indique **Always use this program to open these files**.) Recherchez le paramètre de profil pour ForcekeepAlives et remplacez la valeur 0 par **1**, puis enregistrez le profil.ou
- Pour le client VPN, choisissez **Options > Properties > General** et entrez une valeur pour « Peer response timeout », comme illustré dans cet exemple de fenêtre. Vous pouvez spécifier une sensibilité de délai d'attente de 30 secondes à 480 secondes.ou
- Pour le concentrateur VPN, choisissez **Configuration > User Management > Groups > *modify group***. Sur l'onglet IPsec, choisissez l'option pour IKE Keepalives, comme illustré dans cet exemple de fenêtre.

L'intervalle DPD (Dead Peer Detection) varie selon le paramètre de sensibilité. Si aucune réponse n'est reçue, il passe en mode plus agressif et envoie des paquets toutes les cinq secondes jusqu'à ce que le seuil de réponse de pair soit atteint. À ce moment-là, la connexion est arrêtée. Vous pouvez désactiver les connexions actives mais, si votre connexion est réellement coupée, vous devez attendre la fin du délai d'attente. Cisco recommande de définir une valeur de sensibilité très faible pour commencer.

Q. Est-ce que le Client VPN Cisco prend en charge une double authentification ?

A. Non. L'authentification double n'est pas prise en charge sur le client VPN Cisco.

Q. Comment est-ce que je peux configurer le Client VPN Cisco pour une connexion en mode principal et non en mode agressif ?

A. Vous devez employer des signatures numériques (certificats) afin de permettre au Client VPN Cisco de se connecter en mode principal. Il existe 2 méthodes pour effectuer cette opération :

1. Obtenez des certificats d'une Autorité de certification auprès du fournisseur de certificats tiers (par exemple, Verisign ou Entrust) sur le routeur et tous les Clients VPN Cisco. Inscrivez les certificats d'identité du même serveur d'Autorité de certification et utilisez les signatures numériques comme moyen d'authentification entre le Client VPN Cisco et le routeur. Pour plus d'informations sur cette configuration, reportez-vous à Configuration d'IPSec entre les routeurs Cisco IOS et le Client VPN Cisco à l'aide de certificats Entrust.
2. La deuxième option consiste à configurer le routeur comme serveur d'Autorité de certification avec la tête de réseau pour le VPN d'accès à distance. L'installation des certificats (et de tous les autres éléments) est identique à celle décrite dans le lien précédent sauf que le routeur se comportera comme un serveur d'Autorité de certification. Pour plus d'informations, reportez-vous à VPN de LAN à LAN dynamique entre des routeurs Cisco IOS à l'aide de l'Autorité de certification IOS sur l'exemple de configuration Hub.

Q. Comment est-ce que je fais pour que les paramètres requis dans le fichier d'accès client VPN soient en lecture seule ?

A. Ajoutez un point d'exclamation (!) devant chaque paramètre dans le fichier .pcf pour chaque utilisateur afin que le paramètre soit en lecture seule.

Les valeurs pour les paramètres qui commencent par un point d'exclamation (!) ne peuvent pas être modifiées par l'utilisateur dans le client VPN. Les champs pour ces valeurs dans l'interface utilisateur graphique seront grisés (en lecture seule).

Voici un exemple de configuration :

Fichier .pcf d'origine

```
[main]

Description=connection to TechPubs server

Host=10.10.99.30

AuthType=1

GroupName=docusers

GroupPwd=

enc_GroupPwd=158E47893BDCD398BF863675204775622C494B39523E5CB65434D3C85
              1ECF2DCC8BD488857EFA FDE1397A95E01910CABECCE4E040B7A77BF

EnableISPConnect=0

ISPConnectType=0

ISPConnect=

ISPCommand=

Username=alice
```

Fichier .pcf modifié

```
[main]

!Description=connection to TechPubs server

!Host=10.10.99.30

AuthType=1

!GroupName=docusers

GroupPwd=

enc_GroupPwd=158E47893BDCD398BF863675204775622C494B39523E5CB65434D3C
          851ECF2DCC8BD488857EFA FDE1397A95E01910CABECCE4E040B7A77BF

EnableISPConnect=0

ISPConnectType=0

ISPConnect=
```

```
ISPCommand=

!Username=alice
```

Dans cet exemple, l'utilisateur ne peut pas changer les valeurs *Description*, *Host*, *GroupName* ni *Username* .

Q. Est-il possible de limiter/restreindre l'accès des clients VPN en fonction des adresses MAC ?

A. Non. Il n'est pas possible de limiter/restreindre l'accès des clients VPN en fonction des adresses MAC.

Informations connexes

- Page de support pour le Client Cisco VPN 3000
- Cisco VPN Client Support Page
- Solutions de dépannage les plus fréquentes concernant un VPN IPsec LAN à LAN et d'accès à distance
- Support et documentation techniques - Cisco Systems