Le client Cisco AnyConnect Secure Mobility pour plates-formes mobiles

Le client Cisco AnyConnect® Secure Mobility pour plates-formes mobiles permet de mettre facilement en place une connectivité réseau chiffrée et fiable sur les smartphones et les tablettes, ainsi qu'un accès permanent au réseau de l'entreprise pour les employés en déplacement.

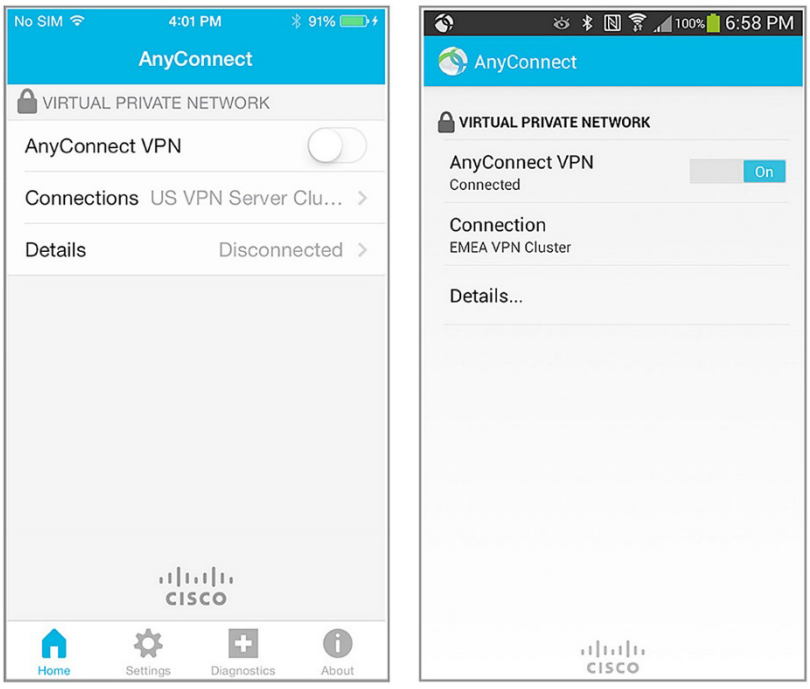
Présentation du produit

Vous pouvez désormais protéger les smartphones et les tablettes de vos employés à l'aide du client Cisco AnyConnect Secure Mobility pour plates-formes mobiles, disponible sur Apple iOS, Android, Windows Phone 8.1, BlackBerry 10.3.2 et versions ultérieures, certains appareils Amazon Kindle et Fire Phone, et sur Google Chrome OS (préversion).

Que vos employés se connectent à leur messagerie professionnelle, à une session de bureau virtuel ou aux applications de l'entreprise, le client AnyConnect fournit une interface conviviale pour l'accès aux informations stratégiques. Le client utilise les protocoles DTLS, IPsec IKEv2 et TLS (HTTP sur TLS/SSL) pour permettre aux applications essentielles à l'activité (par exemple, les applications sensibles à la latence telles que la VoIP) d'accéder aux ressources de l'entreprise à l'aide d'une connexion chiffrée. AnyConnect 4.x prend en charge les fonctions VPN par application pour iOS 8.3 et les versions ultérieures.

La figure 1 montre un exemple d'interface AnyConnect sur les appareils Apple iOS et Android.

Figure 1. Interface des appareils Apple iOS et Android



Caractéristiques et bénéfices

Le tableau 1 décrit les fonctionnalités et les bénéfices du client AnyConnect Secure Mobility pour plates-formes mobiles. Les fonctionnalités disponibles dépendent de la plate-forme. Consultez les notes de version et la documentation relatives à chaque plate-forme pour connaître les fonctionnalités prises en charge par les différents systèmes d'exploitation.

Tableau 1. Caractéristiques et bénéfices

Caractéristique	Bénéfice
Accès aux logiciels et compatibilité	**Disponible sur les boutiques d'applications** • **App Store d'Apple :** pour Apple iOS 6.0 et les versions ultérieures • **Google Play :** pour Android 4.0 et les versions ultérieures Notez que plusieurs images AnyConnect sont disponibles, et qu'il est donc primordial de choisir l'image qui convient à votre appareil. Consultez les notes de version d'Android pour connaître les conditions requises. • **Windows Store :** pour Windows Phone 8.1 (mise à jour 1) et les versions ultérieures • **BlackBerry World** : pour BlackBerry 10.3.2 et les versions ultérieures • **Google Chrome OS** : pour Chrome OS 43 et les versions ultérieures (préversion) • **App-shop Amazon :** pour certains appareils Kindle et Fire Phone
Accès réseau optimisé	• Adopte automatiquement la méthode de tunnellisation la plus efficace en fonction des contraintes du réseau • Utilise le protocole DTLS dans le but de fournir une connexion optimisée pour l'accès TCP aux applications et le trafic sensible à la latence, comme le trafic VoIP • Utilise le protocole TLS (HTTP sur TLS/SSL) pour garantir la connectivité réseau dans les environnements verrouillés • Le protocole IPsec IKEv2 offre une connexion optimisée pour le trafic sensible à la latence lorsque les politiques de sécurité requièrent l'utilisation d'IPsec (cela nécessite un appliance de sécurité adaptative 8.4 ou une version ultérieure) • Compatible avec l'équilibrage de charge VPN ASA
Adapté aux terminaux mobiles	• Reprise transparente après la modification de l'adresse IP, la perte de la connectivité ou la mise en veille de l'appareil
Économie de la batterie	• Compatible avec la mise en veille des appareils
Chiffrement	• Prise en charge de mécanismes de chiffrement forts, notamment AES-256 et 3DES-168. (Le dispositif de passerelle de sécurité doit être associé à une licence de chiffrement renforcé.) • Chiffrement de nouvelle génération, notamment des algorithmes NSA Suite B, ESPv3 avec IKEv2, des clés RSA 4096 bits, Diffie-Hellman (groupe 24) et SHA2 (SHA-256 et SHA-384) améliorées. Disponible uniquement pour les connexions IPsec IKEv2. Une licence AnyConnect Apex est requise.
Options d'authentification	• RADIUS • RADIUS avec échéance de mot de passe (MSCHAPv2) vers NT LAN Manager (NTLM) • Prise en charge d'un mot de passe RADIUS à usage unique (OTP) (attributs de message d'état et de réponse) • RSA SecurID • Active Directory ou Kerberos • Certificat numérique (compatible avec le protocole SCEP intégré à AnyConnect pour le déploiement des informations d'identification) • Prise en charge du protocole LDAP générique • Protocole LDAP avec échéance et vieillissement du mot de passe • Certificat combiné et authentification multifacteur par nom d'utilisateur et mot de passe (double authentification)
Expérience homogène pour l'utilisateur	• Le mode client « full-tunnel » prend en charge l'accès à distance des utilisateurs qui ont besoin d'une expérience uniforme, similaire à celle proposée avec un accès LAN
Gestion et contrôle centralisés des politiques	• Les politiques peuvent être préconfigurées ou configurées localement, puis automatiquement mises à jour à partir de la passerelle de sécurité VPN • Le gestionnaire d'URI d'AnyConnect facilite les déploiements par le biais d'URL intégrées aux pages web ou aux applications • Les certificats peuvent être affichés et contrôlés localement

Caractéristique	Bénéfice
Connectivité réseau IP avancée	• Politique d'accès réseau « split-tunneling » ou « all-tunneling » gérée par l'administrateur • Politique VPN par application pour iOS 8.3 et les versions ultérieures (nécessite Cisco ASA 5500-X avec OS 9.3.2 ou versions ultérieures, et une licence AnyConnect Plus ou Apex) • Politique de contrôle d'accès **Mécanismes d'affectation d'adresses IP :** • Statique • Pool interne • DHCP (Dynamic Host Configuration Protocol) • RADIUS/LDAP
Localisation	**Outre l'anglais, les langues suivantes sont proposées :** • Français canadien (fr-ca) • Tchèque (cs-cz) • Allemand (de-de) • Japonais (ja-jp) • Coréen (ko-kr) • Espagnol (Amérique latine) (es-co) • Polonais (pl-pl) • Chinois simplifié (zh-cn)
Diagnostics	• Des statistiques et des informations de journalisation sont disponibles sur le terminal. • Les journaux peuvent s'afficher sur l'appareil. • Les journaux peuvent être facilement envoyés à Cisco ou à un administrateur en vue de leur analyse.

Compatibilité entre les plates-formes

Le client AnyConnect Secure Mobility est compatible avec tous les modèles de pare-feu de nouvelle génération Cisco ASA 5500-X et de pare-feu d'entreprise Cisco 5500 qui exécutent ASA 8.0(4) ou une version ultérieure. Il est conseillé d'utiliser les versions actuelles du logiciel ASA.

Certaines fonctionnalités nécessitent des versions d'ASA ou des modèles ASA 5500-X ultérieurs.

Cisco prend en charge l'accès VPN d'AnyConnect avec Cisco IOS® 15.1(2)T ou une version ultérieure en tant que passerelle ultrasécurisée ; les fonctionnalités étant toutefois limitées. Pour en savoir plus, reportez-vous à la section Fonctionnalités non prises en charge sur le VPN SSL de Cisco IOS. Reportez-vous à http://www.cisco.com/go/fn pour plus d'informations sur la prise en charge des fonctionnalités de Cisco IOS.

D'autres informations sur les compatibilités sont disponibles à la page http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html.

Informations relatives aux options de licences et aux commandes

Le Guide d'aide à la commande d'AnyConnect comprend des informations sur les licences et les commandes pour AnyConnect, le VPN SSL sans client et l'utilisation d'un VPN tiers avec accès à distance via le protocole IKEv2. Des licences AnyConnect Plus ou Apex sont requises pour une prise en charge complète de la plate-forme et de ses fonctionnalités. Les clients disposant déjà de licences Essentials, Premium ou Mobile sont autorisés à utiliser les versions iOS et Android (à l'exception des fonctions de VPN par application) jusqu'au 30 avril 2016. Toutes les autres plates-formes mobiles nécessitent des licences Plus ou Apex. Les connexions VPN AnyConnect aux têtes de réseau non Cisco ne sont pas autorisées. Pour plus d'informations, reportez-vous au Guide d'aide à la commande à l'adresse http://www.cisco.com/c/dam/en/us/products/security/anyconnect-og.pdf.

Cisco Capital

Un financement pour vous aider à atteindre vos objectifs

L'offre de financement Cisco Capital peut vous aider à acquérir la technologie dont vous avez besoin pour atteindre vos objectifs et rester compétitif. Nous pouvons vous aider à réduire vos CapEx, à accélérer votre croissance et à optimiser votre investissement et votre ROI. L'offre de financement Cisco Capital permet une certaine flexibilité pour l'achat de matériel, de logiciels, de services et d'équipements tiers complémentaires. Vous n'avez qu'une échéance mensuelle à honorer. L'offre de financement Cisco Capital est disponible dans plus de 100 pays. En savoir plus.

Informations complémentaires

- Page dédiée à Cisco AnyConnect : http://www.cisco.com/go/anyconnect.
- Documentation relative à Cisco AnyConnect : http://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html.
- Pare-feu de nouvelle génération Cisco ASA 5500-X : http://www.cisco.com/go/asa.
- Contrat de licence Cisco AnyConnect et politique de confidentialité : http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/license/end_user/AnyConnect-SEULA-v4-x.html.

Remerciements

Ce produit comprend un logiciel développé par OpenSSL Project en vue de son utilisation dans OpenSSL Toolkit.

Ce produit comprend un logiciel cryptographique dont l'auteur est Eric Young.

Ce produit comprend un logiciel dont l'auteur est Tim Hudson.

Ce produit comprend la bibliothèque HTTP de libcurl : Copyright 1996-2006, dont l'auteur est Daniel Stenberg.

Siège social aux États-Unis
Cisco Systems, Inc.
San José. CA

Siège social en Asie-Pacifique
Cisco Systems (États-Unis) Pte. Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam.
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et de fax sont répertoriés sur le site web de Cisco, à l'adresse : www.cisco.com/go/offices.

Imprimé aux États-Unis C78-527494-09 10/15