Découvrez le client Cisco AnyConnect Secure Mobility

Objectif

Cet article porte sur les fonctionnalités, les spécifications et les avantages de l'utilisation de Cisco AnyConnect. Pour plus d'informations sur les licences AnyConnect sur les routeurs de la gamme RV340, consultez l'article Licence AnyConnect pour les routeurs de la gamme RV340.

Version du logiciel

4.2.03013 (Notes de version)

Caractéristiques et caractéristiques

Fonctionnalité	Avantages et détails
VPN d'accès à distance	
Prise en charge étendue des systèmes d'exploitation	• Windows 10, 8.1, 8 et 7 • Mac OS X 10.8 et versions ultérieures • Intel Linux (x64) ◦ Consultez la fiche technique AnyConnect Mobile pour obtenir des informations sur la plate-forme mobile.
Accès réseau optimisé : Protocole VPN SSL (TLS et DTLS); IPsec IKEv2	• AnyConnect offre un choix de protocoles VPN, afin que les administrateurs puissent utiliser le protocole le mieux adapté à leurs besoins professionnels. • La prise en charge de la tunnellisation inclut SSL (TLS 1.2 et DTLS) et IPsec IKEv2 de nouvelle génération. • DTLS fournit une connexion optimisée pour le trafic sensible à la latence, tel que le trafic VoIP ou l'accès aux applications basé sur TCP. • TLS 1.2 (HTTP sur TLS ou SSL) permet de garantir la disponibilité de la connectivité réseau via des environnements verrouillés, y compris ceux qui utilisent des serveurs proxy Web. • IPsec IKEv2 fournit une connexion optimisée pour le trafic sensible à la latence lorsque les stratégies de sécurité nécessitent l'utilisation d'IPsec.
Sélection optimale de la passerelle	• Détermine et établit la connectivité au point d'accès réseau optimal, éliminant ainsi le besoin pour les utilisateurs finaux de déterminer l'emplacement le plus proche.
Mobilité	• Conçu pour les utilisateurs mobiles • Peut être configuré de manière à ce que la connexion VPN reste établie lors des modifications d'adresse IP, de la perte de connectivité ou de la mise en veille ou en veille prolongée. • Grâce à la détection de réseau fiable, la connexion VPN peut se déconnecter automatiquement lorsqu'un utilisateur final se trouve au bureau et se connecter lorsqu'un utilisateur se trouve à un emplacement distant.
Chiffrement	• AES-256 et 3DES-168. (Une licence de chiffrement fort doit être

	activée sur le périphérique de la passerelle de sécurité.) • Algorithmes NSA Suite B, ESPv3 avec IKEv2, clés RSA 4096 bits, groupe Diffie-Hellman 24 et SHA2 amélioré (SHA-256 et SHA-384). S'applique uniquement aux connexions IKEv2 IPsec. Une licence AnyConnect Apex est requise.
Large éventail d'options de déploiement et de connexion	**Options de déploiement :** • Prédéploiement, y compris Microsoft Installer • Déploiement automatique de la passerelle de sécurité (droits d'administration requis pour l'installation initiale) par ActiveX (Windows uniquement) et Java **Modes de connexion :** • Icône autonome par système • Initié par le navigateur (lancement Web) • Création d'un portail sans client • CLI initié • API initiée
Large éventail d'options d'authentification	• RADIUS • RADIUS avec expiration du mot de passe (MSCHAPv2) vers NT LAN Manager (NTLM) • Prise en charge du mot de passe à usage unique (OTP) RADIUS (attributs de message d'état et de réponse) • RSA SecurID (intégration SoftID incluse) • Active Directory ou Kerberos • Autorité de certification intégrée • Certificat numérique ou carte à puce (y compris la prise en charge des certificats machine), sélection automatique ou par l'utilisateur • Protocole LDAP (Lightweight Directory Access Protocol) avec expiration et vieillissement des mots de passe • Prise en charge LDAP générique • Authentification multifacteur de certificat et de mot de passe utilisateur combinés (double authentification)
Expérience utilisateur homogène	• Le mode client Full-Tunnel prend en charge les utilisateurs à accès distant qui ont besoin d'une expérience utilisateur cohérente de type LAN. • Plusieurs méthodes de livraison permettent d'assurer une compatibilité étendue d'AnyConnect. • L'utilisateur peut différer les mises à jour poussées. • L'option de retour d'expérience client est disponible.
Contrôle et gestion centralisés des politiques	• Les stratégies peuvent être préconfigurées ou configurées localement et peuvent être mises à jour automatiquement à partir de la passerelle de sécurité VPN. • L'API pour AnyConnect facilite les déploiements via des pages Web ou des applications. • Des avertissements utilisateur et de contrôle sont émis pour les certificats non fiables. • Les certificats peuvent être affichés et gérés localement.
Connectivité réseau IP avancée	• Connectivité publique vers et depuis les réseaux IPv4 et IPv6 • Accès aux ressources réseau IPv4 et IPv6 internes • Politique d'accès au réseau par fractionnement contrôlé par l'administrateur et par fractionnement en canaux • Stratégie de contrôle d'accès • Politique VPN par application pour Google Android (Lollipop) et Samsung KNOX (nouveau dans la version 4.0); nécessite Cisco ASA 5500-X avec OS 9.3 ou ultérieur et licences AnyConnect 4.0)

	Mécanismes d'attribution des adresses IP : • Statique • Pool interne • DHCP (Dynamic Host Configuration Protocol) • RADIUS/LDAP
Conformité robuste des terminaux unifiés (Licence Apex requise)	• L'évaluation et la correction de la position des terminaux sont prises en charge pour les environnements filaires et sans fil (remplacement de l'agent NAC Cisco Identity Services Engine). Nécessite Identity Services Engine 1.3 ou version ultérieure avec licence Identity Services Engine Apex. • Cisco Hostscan cherche à détecter la présence d'un logiciel antivirus, d'un logiciel de pare-feu personnel et de Service Packs Windows sur le système de terminaux avant d'accorder l'accès au réseau. • Les administrateurs ont également la possibilité de définir des contrôles personnalisés en fonction de la présence de processus en cours d'exécution. • L'analyse d'hôte détecte la présence d'un filigrane sur un système distant. Le filigrane peut être utilisé pour identifier les actifs appartenant à l'entreprise et fournir ainsi un accès différencié. La fonctionnalité de vérification des filigranes inclut les valeurs du Registre système, l'existence de fichiers correspondant à une somme de contrôle CRC32 requise, la correspondance de plage d'adresses IP et les certificats émis par ou à une autorité de certification correspondante. Des fonctionnalités supplémentaires sont prises en charge pour les applications non conformes. • Les fonctions varient selon le système d'exploitation. Reportez-vous aux graphiques de prise en charge de l'analyse des hôtes pour obtenir des informations détaillées.
Stratégie de pare-feu client	• Offre une protection supplémentaire pour les configurations de fractionnement en canaux. • Utilisé conjointement avec le client AnyConnect pour autoriser les exceptions d'accès local (par exemple, l'impression, la prise en charge des périphériques raccordés, etc.). • Prend en charge les règles basées sur les ports pour IPv4 et les listes de contrôle d'accès réseau et IP pour IPv6. • Disponible pour les plates-formes Windows et Mac OS X.
Localisation	**Outre l'anglais, les traductions suivantes sont incluses :** • Tchèque (cs-cz) • Allemand (de-de) • Espagnol (es-es) • Français (fr-fr) • Japonais (ja-jp) • Coréen (ko-kr) • Polonais (pl-pl) • Chinois simplifié (zh-cn) • Chinois (Taïwan) (zh-tw) • Néerlandais (nl-nl) • Hongrois (hu-hu) • Italien (it-it) • Portugais (Brésil) (pt-br) • Russe (ru-ru)
Facilité d'administration des clients	• Les administrateurs peuvent distribuer automatiquement les mises à jour de logiciels et de politiques à partir de l'appliance de sécurité

	de tête de réseau, éliminant ainsi l'administration associée aux mises à jour de logiciels clients. • Les administrateurs peuvent déterminer quelles fonctionnalités mettre à disposition pour la configuration de l'utilisateur final. • Les administrateurs peuvent déclencher un script de point de terminaison aux heures de connexion et de déconnexion lorsque les scripts de connexion de domaine ne peuvent pas être utilisés. • Les administrateurs peuvent entièrement personnaliser et localiser les messages visibles de l'utilisateur final.
Éditeur de profil	• Les stratégies AnyConnect peuvent être personnalisées directement à partir de Cisco Adaptive Security Device Manager (ASDM).
Diagnostics	• Des statistiques et des informations de journalisation sont disponibles sur le périphérique. • Les journaux peuvent être affichés sur le périphérique. • Les journaux peuvent être facilement envoyés par e-mail à Cisco ou à un administrateur pour analyse.
Norme fédérale de traitement de l'information (FIPS)	• Compatible FIPS 140-2 niveau 2 (les restrictions de plate-forme, de fonctionnalité et de version s'appliquent)
	Mobilité sécurisée et visibilité du réseau
Intégration de la sécurité Web (Licence Cloud Web Security requise)	:: Utilise Cloud Web Security, le plus grand fournisseur mondial de sécurité Web SaaS (Software-as-a-Service), pour empêcher les programmes malveillants de se connecter aux réseaux de l'entreprise et contrôler et protéger l'utilisation du Web par les employés. • Prend en charge les configurations hébergées dans le cloud et le chargement dynamique. • Offre aux entreprises la flexibilité et le choix en prenant en charge les services cloud en plus des services sur site. • S'intègre à l'appareil de sécurité Web. • Prend En Charge La Détection De Réseau Fiable. • Applique la stratégie de sécurité dans chaque transaction, indépendamment de l'emplacement de l'utilisateur. • Nécessite une connectivité réseau hautement sécurisée permanente avec une politique permettant d'autoriser ou de refuser la connectivité réseau si l'accès devient indisponible. • Détecte les points d'accès et les portails captifs.
Module de visibilité du réseau (Licence Apex requise)	• Détecter les anomalies de comportement potentielles en surveillant l'utilisation des applications. • Permet de prendre des décisions plus éclairées en matière de conception de réseau. • Peut partager des données d'utilisation avec un nombre croissant d'outils d'analyse réseau compatibles IPFIX (Internet Protocol Flow Information Export).
Advanced Malware Protection (AMP) pour Endpoints Enabler (AMP for Endpoints sous licence séparée)	• Simplifie l'activation des services de protection contre les menaces sur les terminaux AnyConnect en distribuant et en activant CiscoAMP for Endpoints. • Étend les services de protection contre les menaces de terminaux aux terminaux distants, augmentant ainsi la couverture des menaces de terminaux. • Offre une protection plus proactive pour garantir une atténuation plus rapide des attaques au niveau du terminal distant.
Prise en charge étendue du	• Windows 10, 8.1, 8 et 7

système d'exploitation	• Mac OS X 10.8 et versions ultérieures
Network Access Manager et 802.1X	
Support multimédia	• Ethernet (IEEE 802.3) • Wi-Fi (IEEE 802.11a/b/g/n)
Authentification réseau	• IEEE 802.1X-2001, 802.1X-2004 et 802.1X-2010 • Permet aux entreprises de déployer un cadre d'authentification 802.1X unique pour accéder aux réseaux filaires et sans fil. • Gère l'identité de l'utilisateur et du périphérique et les protocoles d'accès au réseau requis pour un accès hautement sécurisé. • Optimise l'expérience utilisateur lors de la connexion à un réseau câblé et sans fil unifié Cisco.
Méthodes EAP (Extensible Authentication Protocol)	• Sécurité de la couche transport EAP (TLS) • Protocole PEAP (EAP-Protected Extensible Authentication Protocol) avec les méthodes internes suivantes : - EAP-TLS - EAP-MSCHAPv2 - Carte à jeton générique EAP (GTC) • Authentification EAP-Flexible via Secure Tunneling (FAST) avec les méthodes internes suivantes : - EAP-TLS - EAP-MSCHAPv2 - EAP-GTC • TLS (EAP-Tunneled TLS) avec les méthodes internes suivantes : - PAP (Password Authentication Protocol). - Protocole CHAP (Challenge Handshake Authentication Protocol). - CHAP Microsoft (MSCHAP). - MSCHAPv2 - EAP-MD5 - EAP-MSCHAPv2 • EAP léger (LEAP), Wi-Fi uniquement • EAP-Message Digest 5 (MD5), configuré en mode administratif, Ethernet uniquement • EAP-MSCHAPv2, configuré en mode administratif, Ethernet uniquement • EAP-GTC, configuration administrative, Ethernet uniquement
Méthodes de cryptage sans fil (nécessite la prise en charge de la carte réseau 802.11 correspondante)	• Ouvrir • WEP (Wired Equivalent Privacy) • WEP dynamique • Wi-Fi Protected Access (WPA) Enterprise • WPA2 Enterprise • WPA personnel (WPA-PSK) • WPA2 personnel (WPA2-PSK) • CCKM (nécessite une carte réseau sans fil Cisco CB21AG)
Protocoles de cryptage sans fil	• Mode compteur avec le protocole CCMP (Cipher Block Chaining Message Authentication Code Protocol) à l'aide de l'algorithme AES (Advanced Encryption Standard) • Protocole TKIP (Temporal Key Integrity Protocol) utilisant le chiffrement de flux Rivest Cipher 4 (RC4)
Reprise de session	• Reprise de session RFC2716 (EAP-TLS) utilisant EAP-TLS, EAP-FAST, EAP-PEAP et EAP-TTLS • Reprise de session EAP-FAST sans état • Mise en cache PMK-ID (mise en cache proactive des clés ou mise en cache opportuniste des clés), Windows XP uniquement
Cryptage Ethernet	• Contrôle d'accès au support : IEEE 802.1AE (MACsec)

	• Gestion des clés : Contrat de clé MACsec (MKA) • Définit une infrastructure de sécurité sur un réseau Ethernet câblé pour assurer la confidentialité des données, l'intégrité des données et l'authentification de l'origine des données. • Protège la communication entre les composants fiables du réseau.
Une connexion à la fois	• Autorise une seule connexion au réseau, déconnectant toutes les autres. • Pas de pontage entre les adaptateurs. • Les connexions Ethernet sont automatiquement prioritaires.
Validation de serveur complexe	• Prend en charge “ extrémités avec ” et “ règles de ” de correspondance exacte. • Prise en charge de plus de 30 règles pour les serveurs sans commune nom.
Chaînage EAP (EAP-FASTv2)	• Différencie l'accès en fonction des ressources de l'entreprise et des autres. • Valide les utilisateurs et les périphériques dans une seule transaction EAP.
Application des connexions d'entreprise (ECE)	• Permet de s'assurer que les utilisateurs se connectent uniquement au réseau d'entreprise approprié. • Empêche les utilisateurs de se connecter à un point d'accès tiers pour surfer sur Internet pendant qu'ils se trouvent au bureau. • Empêche les utilisateurs d'établir l'accès au réseau invité. • Élimine les listes noires encombrantes.
Chiffrement de nouvelle génération (Suite B)	• Prend en charge les dernières normes cryptographiques. • Échange de clé Diffie-Hellman de courbe elliptique • Certificats ECDSA (Elliptic Curve Digital Signature Algorithm)
Types d'informations d'identification	• Mots de passe utilisateur interactifs ou mots de passe Windows • Jetons RSA SecurID • Jetons de mot de passe unique (OTP) • Cartes à puce (Axalto, Gemplus, SafeNet iKey, Alladin). • Certificats X.509. • Certificats ECDSA (Elliptic Curve Digital Signature Algorithm).
Prise en charge des bureaux distants	• Authentifie les informations d'identification des utilisateurs distants sur le réseau local lors de l'utilisation du protocole RDP (Remote Desktop Protocol).
Systèmes d'exploitation pris en charge	• Windows 10, 8.1, 8 et 7