

Méthodes de distribution de client sécurisé pour RAVPN d'accès sécurisé

Table des matières

Problème

Lors de la configuration de l'accès d'un fournisseur externe au VPN d'accès à distance (RAVPN) dans Cisco Secure Access, les administrateurs ont besoin d'une méthode permettant aux fournisseurs de télécharger le logiciel AnyConnect/Secure Client. Contrairement aux déploiements ASA précédents où l'URL VPN fournissait des téléchargements client directs, les URL de tête de réseau VPN d'accès sécurisé Cisco ne fournissent pas de fonction de téléchargement client. Cette limitation a un impact sur le processus d'intégration pour les fournisseurs externes qui ont besoin de fonctionnalités d'accès à distance.

Les administrateurs s'attendent à ce que les URL de configuration VPN dans Secure Access accordent aux fournisseurs l'accès pour télécharger le client AnyConnect, comme cela était le cas avec les déploiements basés sur ASA où l'URL VPN autoriserait les téléchargements du client avant la connexion.

Environnement

- Cisco Secure Access avec configuration RAVPN
- Besoins d'accès fournisseur externe
- Migration depuis un déploiement VPN basé sur ASA
- Besoins de distribution AnyConnect/Secure Client

Résolution

Cisco Secure Access n'héberge pas les packages Secure Client sur les URL de tête de réseau VPN. La solution utilise la technologie hostscan au lieu de fournir des téléchargements client directs via l'URL VPN. Pour distribuer le logiciel Secure Client à des fournisseurs externes, utilisez l'une des méthodes approuvées suivantes.

Méthode 1 : Distribution du tableau de bord Secure Access

- 1.- Obtenez les packages d'installation directement à partir du tableau de bord Secure Access pour une distribution manuelle.
- 2.- Accédez à End User Connectivity et cliquez sur le bouton Cisco Secure Client pour télécharger les packages d'installation à distribuer aux fournisseurs.

Méthode 2 : Site de téléchargement de logiciels Cisco

Les fournisseurs peuvent télécharger les packages directement s'ils disposent des droits appropriés :

- Le Fournisseur doit disposer d'un compte Cisco avec droit logiciel
- Accédez aux packages via software.cisco.com
- Nécessite une planification de prédéploiement et la configuration du compte Cisco du fournisseur

Méthode 3 : Distribution manuelle

Distribuez le logiciel Secure Client à des fournisseurs externes manuellement ou via d'autres canaux de distribution en dehors de l'URL VPN. Cette méthode offre le meilleur contrôle sur le processus de distribution et ne nécessite pas de comptes Cisco fournisseur.

Motif

Les URL de tête de réseau VPN Cisco Secure Access sont conçues différemment des déploiements basés sur ASA. La solution Secure Access n'héberge pas les packages d'installation du client sur les têtes de réseau et utilise plutôt la technologie hostscan. Cette différence architecturale signifie que les URL VPN ne peuvent pas fournir la même fonctionnalité de téléchargement client que celle qui était disponible avec les déploiements ASA.

Autres informations utiles

- [Assistance technique de Cisco et téléchargements](#)

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.