Comportement du protocole Cisco Secure Access RAVPN avec configuration double TLS/DTLS et IPsec(IKEv2)

Table des matières

Problème

Lorsque les protocoles TLS/DTLS et IPsec(IKEv2) sont activés dans Cisco Secure Access RAVPN avec le protocole principal défini sur IPsec(IKEv2), des échecs de connexion se produisent lors de la tentative d'établissement de la connectivité VPN à partir de réseaux où le trafic IPsec (ports UDP 500/4500) est bloqué. Le client sécurisé utilise par défaut l'option IPsec dans la liste déroulante de l'interface utilisateur du client et ne bascule pas automatiquement vers TLS/DTLS lorsque la connectivité IPsec échoue, ce qui entraîne des erreurs de connexion et l'incapacité d'établir la connectivité RAVPN à partir d'environnements réseau restreints.

Environnement

- Cisco Secure Access RAVPN avec configuration à deux protocoles
- Les protocoles TLS/DTLS et IPsec(IKEv2) sont tous deux activés
- Paramètre du protocole principal configuré en IPsec(IKEv2)
- Client sécurisé avec liste déroulante de sélection de protocole contenant des options IPsec et TLS distinctes
- Environnement réseau bloquant le trafic IPsec sur les ports UDP 500 et 4500

Résolution

Le comportement observé est attendu et par conception. Cisco Secure Access RAVPN n'effectue pas de basculement automatique de protocole d'IPsec (IKEv2) vers TLS/DTLS lorsque les deux protocoles sont activés et que le protocole principal rencontre des problèmes de connectivité.

Sélection manuelle du protocole requise

Lors de la connexion à partir de réseaux qui bloquent le trafic IPsec, les utilisateurs doivent sélectionner manuellement le protocole approprié dans le client sécurisé :

Étape 1: Ouvrez l'application Secure Client

Étape 2: Recherchez le menu déroulant de sélection du protocole dans l’interface client

Étape 3: Modifier manuellement la sélection de l'option IPsec à l'option TLS

Étape 4: Lancez la connexion VPN à l'aide du protocole TLS/DTLS

Clarification du comportement du protocole

Le paramètre de protocole principal dans Cisco Secure Access RAVPN détermine le protocole par défaut présenté dans le client sécurisé, mais n'active pas la fonctionnalité de basculement automatique. Lorsque les protocoles TLS/DTLS et IPsec (IKEv2) sont activés :

- Le client sécurisé affiche des options de protocole distinctes dans le menu déroulant
- Le client utilise par défaut le paramètre de protocole principal (IPsec dans ce cas)
- Aucune commutation automatique ne se produit entre les protocoles en fonction des conditions de connectivité réseau
- Les utilisateurs doivent sélectionner manuellement le protocole approprié en fonction de leur environnement réseau

Motif

Cisco Secure Access RAVPN est conçu sans fonctionnalité de basculement de protocole automatique. Lorsque les protocoles TLS/DTLS et IPsec(IKEv2) sont tous deux activés, le système requiert la sélection manuelle du protocole via l'interface Secure Client. Le paramètre de protocole principal détermine uniquement la sélection par défaut dans le menu déroulant du client et n'implémente pas la logique de commutation automatique lorsque des problèmes de connectivité sont rencontrés avec le protocole principal.

Autres informations utiles

- Documentation sur Cisco Secure Access
- 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.