Configurer les options et les fonctionnalités VPN pour un accès sécurisé en Chine

Table des matières

Problème

Les entreprises qui analysent les capacités VPN pour les déploiements Cisco Secure Access en Chine doivent clarifier la prise en charge du cryptage et les contraintes opérationnelles. Plus précisément, il y a des questions sur la prise en charge officielle du VPN IPsec (IKEv1/IKEv2) sur les périphériques Cisco Secure Firewall déployés en Chine continentale, sur la raison pour laquelle la tunnellisation GRE semble être l'option couramment recommandée, et sur les conditions préalables ou alternatives existantes pour une communication sécurisée. En outre, il est nécessaire de comprendre la prise en charge des tunnels GRE lors de la migration de pare-feu de point de contrôle virtuel dans AWS China vers une plate-forme FTD pour établir la connectivité avec AWS Transit Gateway.

Environnement

- Cisco Secure Access Chine (solution de périphérie de service de sécurité fournie dans le cloud)
- Déploiements de Cisco Secure Firewall en Chine continentale
- Scénarios de migration de plate-forme FTD
- Connectivité requise pour AWS China Transit Gateway
- Environnements de pare-feu de point de contrôle virtuel prenant en charge GRE uniquement

Résolution

Cisco Secure Access China offre des fonctionnalités VPN complètes avec prise en charge de

protocoles spécifiques et options de configuration :

Prise en charge VPN IPsec

Cisco Secure Access China prend en charge le VPN IPsec en utilisant uniquement le protocole IKEv2. IKEv1 n'est pas pris en charge dans ce modèle de déploiement. Les paramètres IPsec pris en charge et les options de configuration sont documentés dans la documentation officielle de Cisco Secure Access China.

Principales caractéristiques de la prise en charge IPsec :

- Protocole IKEv2 pris en charge exclusivement.
- Aucun micrologiciel spécial ni aucune image de chiffrement n'est requis.
- Solution SSE (Security Service Edge) fournie dans le cloud.
- Configuration de paramètre IPsec standard disponible.

Options de haute disponibilité

Pour une fiabilité accrue, les groupes de tunnels réseau Cisco Secure Access China prennent en charge les configurations de concentrateurs principal et secondaire avec des fonctionnalités de haute disponibilité.

Motif

Aucune cause spécifique n'a été identifiée.

Autres informations utiles

- Paramètres IPsec de Cisco Secure Access Chine

- Configuration GRE de Cisco Secure Access en Chine
- Documentation des paramètres IPsec pris en charge
- Groupes de tunnels réseau Haute disponibilité
- Guide d'utilisation du déploiement VPN
- 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.