Configuration de la stratégie basée sur la géolocalisation RAVPN pour la version FTD du pare-feu sécurisé

Table des matières

Problème

Environnement

Résolution

Motif

Autres informations utiles

- Problème
- Environnement
- Résolution
- Motif
- Autres informations utiles

Problème

Une stratégie de contrôle d'accès configurée avec des règles de filtrage basées sur la géolocalisation pour les connexions de réseau privé virtuel (VPN SSL) AnyConnect Secure Sockets Layer ne fonctionne pas comme prévu. La stratégie inclut une règle spécifiquement conçue pour autoriser les connexions VPN SSL AnyConnect provenant d'Arabie saoudite uniquement. La fonctionnalité de stratégie de contrôle d'accès basée sur la géolocalisation dont dépendent ces règles pour identifier et filtrer le trafic en fonction du pays d'origine ne fonctionne pas sur la version 7.0.9 actuelle de Cisco Secure Firewall Threat Defense (FTD).

Environnement

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD) version 7.0.9

- Contrôle des applications Firepower avec services de géolocalisation
- Configuration VPN SSL AnyConnect avec règles de contrôle d'accès basées sur la géolocalisation
- Stratégie de contrôle d'accès configurée avec un filtrage spécifique au pays

Résolution

La politique de contrôle d'accès basée sur la géolocalisation pour la fonctionnalité RAVPN nécessite FTD version 7.7 ou ultérieure pour fonctionner correctement. Comme l'environnement actuel exécute FTD version 7.0.9, une mise à niveau est nécessaire pour résoudre ce problème.

- Priorité de mise à niveau FMC : Le FMC doit être mis à niveau en premier et doit exécuter une version supérieure ou égale à la version FTD cible. Assurez-vous que FMC est mis à niveau en conséquence avant de mettre à niveau FTD.
- Sauvegarde de la configuration : Effectuez une sauvegarde complète des configurations FMC et FTD avant de lancer le processus de mise à niveau.
- Fenêtre de maintenance : Planifiez une fenêtre de maintenance car le processus de mise à niveau nécessite le redémarrage du périphérique et peut entraîner une interruption temporaire du trafic.
- Révision des notes de version : Consultez les notes de version de chaque version intermédiaire et de la version cible pour connaître les problèmes connus ou les mises en garde.

Motif

La fonctionnalité de politique de contrôle d'accès basée sur la géolocalisation pour le réseau privé virtuel d'accès à distance (RAVPN) est uniquement prise en charge à partir de la version FTD 7.7 et ultérieure. La version actuelle de FTD 7.0.9 n'inclut pas la prise en charge de cette fonctionnalité, qui empêche les règles de filtrage basées sur la géolocalisation de fonctionner correctement dans la stratégie de contrôle d'accès.

Autres informations utiles

- Configurer des politiques basées sur la géolocalisation pour Secure Firewall Threat Defense
- Téléchargement du logiciel Cisco Secure Firewall Threat Defense - Version 7.7.11
- Guide de planification de la mise à niveau de Cisco Secure Firewall Management Center
- 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.