

Adresses de destination d'accès sécurisé pour la configuration du routage partagé

Table des matières

Problème

Lors du déploiement de Cisco Secure Access (CSA) avec Cisco Secure Client (CSC) sur des terminaux Windows dans une architecture réseau Hub-Spoke, les entreprises ont très probablement besoin de configurer le routage partagé pour permettre au trafic du site Spoke de se connecter directement à CSA sur le circuit Internet Spoke local au lieu de se reconnecter via le concentrateur. Cette configuration nécessite la connaissance de toutes les adresses de destination Cisco utilisées lors de l'établissement du tunnel CSA afin que les exceptions de routage (routage de séparation/séparation) puissent être définies sur les périphériques réseau tels que les pare-feu Fortigate.

L'exigence spécifique est d'identifier toutes les informations de destination (adresses IP ou URL) pour les points d'extrémité CSA utilisés par CSC lors de l'établissement de tunnels TLS/DTLS, permettant une configuration correcte des politiques de routage qui contournent le tunnel VPN Hub-Spoke pour le trafic CSA.

Environnement

- Déploiement de Cisco Secure Access (CSA)
- Cisco Secure Client (CSC) sur les terminaux Windows
- Topologie de réseau Hub-Spoke avec pare-feu Fortigate
- Connectivité du tunnel TLS/DTLS vers CSA

Résolution

Pour configurer le routage partagé pour les connexions Cisco Secure Access, les informations de destination décrites dans les sections suivantes doivent être configurées sur le périphérique Fortigate pour permettre une connectivité directe aux points d'extrémité CSA.

Domaine et ports de destination CSA

Domaine principal

`*.vpn.sse.cisco.com`

Ports et protocoles requis

- TCP/UDP 443 : Utilisé pour l'établissement de tunnel TLS/DTLS
- UDP 500/4500 : Utilisé pour l'établissement du tunnel IPsec
- TCP 80 : Utilisé pour les contrôles de révocation de certificat VPN

Fortigate Configuration Approach

Configurez les politiques de routage sur le périphérique Fortigate pour diriger le trafic destiné au domaine CSA (`*.vpn.sse.cisco.com`) et aux ports spécifiés via le circuit Internet Spoke local plutôt que via le tunnel VPN Hub-Spoke. Cela active le flux de trafic décrit dans les extraits de code suivants.

Flux de trafic souhaité

Spoke Site → CSA Tunnel Connection → CSA-mediated Internet Communication

Plutôt que le flux de trafic via le site concentrateur

Spoke Site → Hub Site → CSA Tunnel Connection → CSA-mediated Internet Communication

Considérations importantes

Les destinations de connexion CSA sont déterminées dynamiquement pendant l'exécution, ce qui signifie que des adresses IP spécifiques ne peuvent pas être prédéterminées pour la configuration du routage statique. L'approche basée sur le domaine qui utilise *.vpn.sse.cisco.com constitue la méthode la plus fiable pour configurer les politiques de routage partagé.

Référez-vous à la documentation officielle de Cisco Secure Access pour connaître les exigences les plus récentes en matière de destination et de port, car elles sont très probablement mises à jour avec les nouvelles versions logicielles.

Motif

Dans les topologies de réseau Hub-Spoke, l'ensemble du trafic Internet provenant des sites Spoke est généralement acheminé par défaut via le site Hub. Lors de la mise en oeuvre de CSA avec CSC, ce comportement de routage par défaut entraîne l'épinglage du trafic du tunnel CSA à travers le site du concentrateur avant d'atteindre les points d'extrémité CSA, ce qui peut entraîner une latence et une inefficacité de la bande passante. La nature dynamique de la sélection des terminaux CSA nécessite des politiques de routage basées sur le domaine plutôt que des règles statiques basées sur IP pour garantir une fonctionnalité de routage partagé appropriée.

Autres informations utiles

- [Documentation Cisco Secure Access - Conditions requises pour la connexion](#)
- [Documentation Cisco Secure Access - Configuration du réseau](#)

- [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.