Problèmes de connectivité client complète Omnissa via un accès sécurisé

Table des matières

Problème

Le client complet Omnissa ne peut pas charger de postes de travail virtuels lorsqu'il est connecté via Cisco Secure Access. Les utilisateurs rencontrent des problèmes de connectivité lorsqu'ils tentent d'établir des connexions à des environnements virtuels à l'aide de l'application cliente complète. Cependant, l'accès via le client HTML/Web continue à fonctionner normalement, ce qui indique que l'infrastructure de poste de travail virtuel sous-jacente est fonctionnelle, mais qu'un problème spécifique affecte la capacité complète du client à établir des connexions via la solution Cisco Secure Access.

Environnement

- Technologie : Assistance pour les solutions (SSPT - contrat requis)
- Sous-technologie : Accès sécurisé Cisco
- Gamme de produits : SECACS
- Version du logiciel: Toutes les versions concernées
- Application cliente : Client complet Omnissa
- Environnement de bureau virtuel : Bureaux virtuels Omnissa
- Infrastructure réseau : Tunnels IPsec et FTD (Firepower Threat Defense)

Résolution

La résolution implique la mise en oeuvre de modifications spécifiques de la configuration du réseau pour permettre un routage approprié pour le client complet Omnissa via Cisco Secure Access. Les étapes suivantes ont été suivies pour résoudre le problème de connectivité :

- Configurez les paramètres du tunnel partagé. Ajoutez des configurations de tunnel partagé pour permettre au client Omnissa complet d'établir des connexions directes aux hôtes de destination requis. Cette configuration garantit que le trafic destiné à des clients de bureau virtuel spécifiques est correctement acheminé via les chemins réseau appropriés.
- Implémenter des configurations de route statique. Configurez des routes statiques pour les clients spécifiques qui doivent établir des connexions aux bureaux virtuels. La configuration des routes vers le serveur d'agrégation en aval, mais aussi directement vers les hôtes de destination que les clients de poste de travail virtuel doivent atteindre, est essentielle.
- Effacez les tunnels IPsec. Après avoir implémenté les modifications de configuration, effacez les tunnels IPsec sur le FTD pour vous assurer que les nouvelles configurations de routage prennent effet correctement.
- Validez la connectivité. Testez la connectivité client complète d'Omnissa après avoir implémenté les modifications pour confirmer que les connexions de poste de travail virtuel peuvent être établies avec succès via Cisco Secure Access.

Calendrier De Mise En Oeuvre

Les modifications de configuration doivent être implémentées pendant une fenêtre de maintenance planifiée afin de minimiser l'impact sur les utilisateurs. Une fois la mise en oeuvre terminée, validez l'accessibilité et la connectivité complète du client Omnissa pour garantir la réussite de la résolution.

Motif

Le problème de connectivité est dû à des configurations de routage insuffisantes dans l'environnement Cisco Secure Access. Plus précisément, le réseau était configuré avec des routes uniquement vers le serveur d'agrégation en aval, mais il manquait les configurations de tunnel partagé et de route statique nécessaires pour les clients spécifiques auxquels le client complet Omnissa devait établir des connexions. Cette lacune de routage a empêché le client complet d'atteindre correctement les hôtes de bureau virtuel, alors que le client HTML/Web pouvait encore fonctionner car il utilisait différents chemins de connexion correctement configurés.

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.