VPN d'accès sécurisé - accès impossible à Jabber

Table des matières

Problème

Les utilisateurs du client sécurisé n'ont pas pu accéder aux applications internes et privées telles que Jabber et Epic sur le tunnel VPN d'accès sécurisé lors de l'utilisation d'une stratégie d'accès privé. Les utilisateurs ont rencontré des problèmes de connectivité lorsqu'ils ont tenté d'accéder à ces applications métier critiques via la connexion VPN. Au cours du dépannage, un trafic unidirectionnel a été observé pour les ressources Epic, où le trafic ping et TCP SYN a été vu quittant le tunnel VPN Secure Access, mais des problèmes de validation du trafic de retour ont été identifiés sur le pare-feu Palo Alto. En outre, des problèmes d'accessibilité Jabber ont été documentés lorsque les FQDN CUCM étaient résolus via le DNS interne alors que le routage basé sur IP était configuré pour le routage de trafic, provoquant une non-correspondance dans le flux de trafic.

Environnement

- Cisco Secure Access avec configuration de tunnel VPN
- Client sécurisé pour la connectivité VPN
- Implémentation de la politique d'accès privé
- Cisco Unified Communications Manager (CUCM) pour les services Jabber
- Ressources d'application Epic
- Pare-feu Palo Alto pour la sécurité du réseau
- Résolution DNS interne pour FQDN CUCM

Résolution

La résolution impliquait plusieurs modifications de configuration et étapes de dépannage pour restaurer la connectivité aux applications internes via le tunnel VPN d'accès sécurisé :

Configuration de sous-réseau et modifications de tunnel

Étape 1: Ajouter des sous-réseaux supplémentaires au tunnel VPN

Des sous-réseaux supplémentaires ont été ajoutés à la configuration du tunnel VPN pour les ressources affectées. Après l'implémentation de cette modification, les ressources qui étaient auparavant inaccessibles ont commencé à se charger correctement.

Configuration du pilotage d'adresse IP CUCM

Étape 2: Configurer CUCM IP Steering

Pour résoudre le problème de connectivité Jabber lorsque les FQDN CUCM étaient résolus via le DNS interne alors que le pilotage du trafic était basé sur IP, les adresses IP CUCM ont été dirigées vers le client sécurisé. Cette modification de configuration a aligné la résolution DNS sur le mécanisme de direction du trafic.

Étape 3: Créer une règle de stratégie d'accès

Une règle de stratégie d'accès a été créée pour permettre l'accessibilité aux adresses IP CUCM. Cette règle a restauré la connectivité appropriée à l'infrastructure CUCM, activant la fonctionnalité Jabber sur le tunnel VPN.

Configuration du routage statique

Étape 4: Configuration du routage statique pour le sous-réseau CUCM

Assurez-vous que les adresses IP CUCM et le sous-réseau CUCM global sont inclus dans la table de routage statique du tunnel réseau. Cette configuration garantit un routage correct du trafic entre le pool d'utilisateurs du client sécurisé et l'infrastructure CUCM.

Validation du trafic de retour

Étape 5: Valider le flux de paquets et le trafic de retour

Validez la configuration du flux de paquets pour confirmer que le trafic de retour peut atteindre le pool d'utilisateurs du client sécurisé. Cela inclut l'examen de la configuration du pare-feu Palo Alto pour garantir une validation correcte du chemin de retour pour toutes les ressources internes, en

particulier pour la connectivité Epic où le trafic unidirectionnel a été observé.

Motif

Les problèmes de connectivité ont été causés par de multiples lacunes de configuration dans la mise en oeuvre du VPN d'accès sécurisé :

- Des configurations de sous-réseau manquantes dans le tunnel VPN ont empêché un routage correct vers les ressources d'application internes
- Une non-correspondance entre la résolution DNS (basée sur FQDN) et la configuration de l'orientation du trafic (basée sur IP) pour les services CUCM a causé des échecs de connectivité Jabber
- Règles de stratégie d'accès incomplètes qui n'autorisaient pas le trafic vers les adresses IP CUCM
- Entrées de routage statique manquantes pour les sous-réseaux CUCM dans la configuration du tunnel réseau
- Retourner les problèmes de validation du chemin du trafic sur le pare-feu Palo Alto affectant la communication bidirectionnelle

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.