Résolution des problèmes d'accès aux ressources privées avec authentification Kerberos

Table des matières

Introduction

Ce document décrit le comportement de Kerberos lorsqu'il est utilisé avec Secure Access Zero Trust Network Access (ZTNA).

Conditions préalables

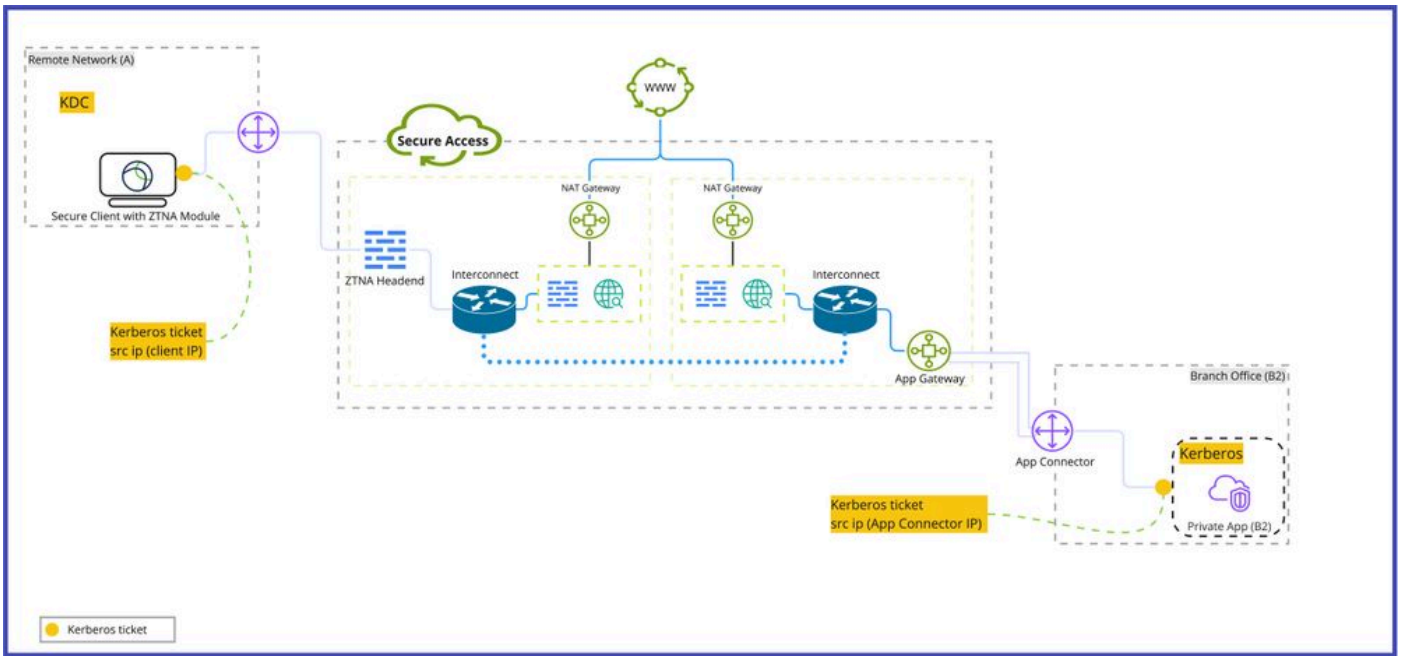
Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès sécurisé
- Client sécurisé Cisco
- Tunnels IPSEC (Internet Protocol Security)
- Réseau privé virtuel d'accès à distance (RAVPN)
- ZTNA (Zero Trust Network Access)

Informations générales

L'accès sécurisé est utilisé pour fournir un accès à des applications privées via plusieurs scénarios, y compris le ZTNA (Zero Trust Access Module) sur le client sécurisé, ou le tunnel IPSEC ou le VPN d'accès à distance. Alors que les applications privées fournissent leur propre mécanisme d'authentification, il existe une limitation sur les serveurs qui s'appuient sur Kerberos comme mécanisme d'authentification.



Flux de paquets Kerberos

Problème : Échec de l'accès aux ressources privées avec l'authentification Kerberos

L'initiation d'une demande d'authentification à partir d'un périphérique client derrière le module ZTNA vers une application privée derrière App Connector entraînerait la modification de l'adresse IP source sur le chemin du réseau d'accès sécurisé. Ce qui entraîne un échec d'authentification lors de l'utilisation du ticket Kerberos initié par le Centre de distribution Kerberos (KDC) des clients.

Solution

L'adresse IP source du client fait partie des tickets Kerberos octroyés par le Centre de distribution Kerberos (KDC). En général, lorsque des tickets Kerberos traversent un réseau, il est nécessaire que l'adresse IP source reste inchangée, sinon le serveur de destination avec lequel nous nous authentifions n'honore pas le ticket par rapport à l'adresse IP source d'où il provient.

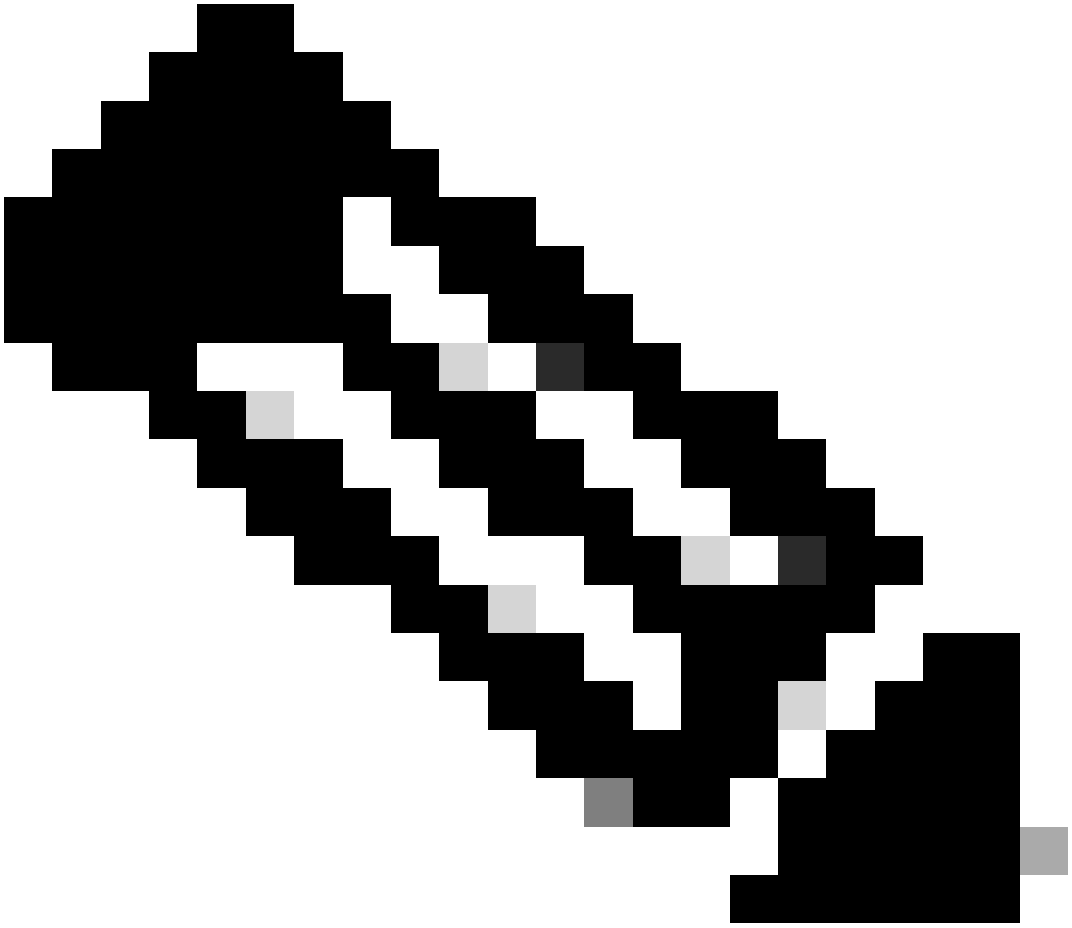
Pour résoudre ce problème, utilisez l'une des options suivantes :

Option 1 :

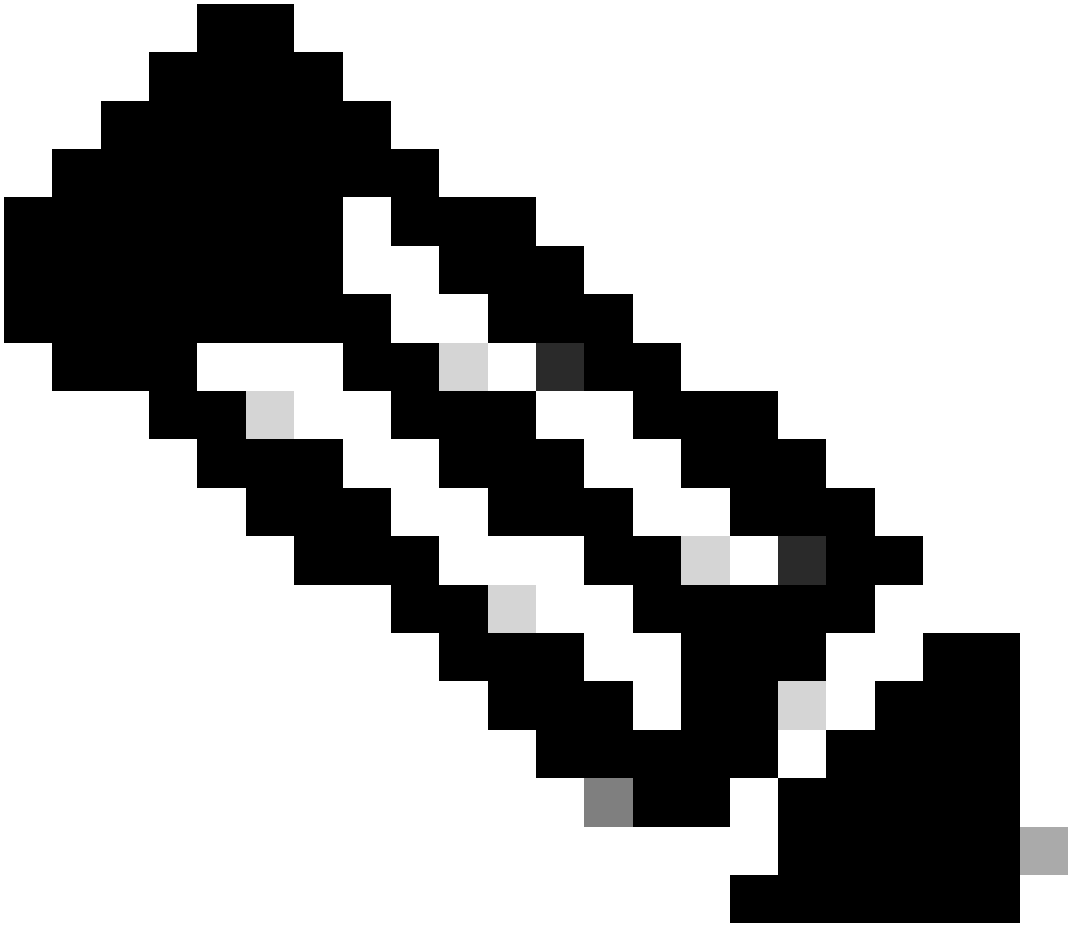
Désactivez l'option pour inclure l'adresse IP source dans le ticket Kerberos client.

Option 2 :

Utilisez un VPN d'accès sécurisé avec des ressources privées derrière le tunnel IPSEC au lieu d'applications privées derrière App Connector.



Remarque : ce comportement n'affecte que les applications privées déployées derrière App Connector et le trafic provient du client avec module ZTNA sans VPN.



Remarque : la recherche d'activité d'accès sécurisé affiche l'action autorisée pour la transaction, car le blocage se produit du côté de l'application privée et non de l'accès sécurisé.

Informations connexes

- Guide de l'utilisateur Secure Access
- Assistance et documentation techniques - Cisco Systems

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.