Fehlerbehebung beim Zugriff auf private Ressourcen mithilfe der Kerberos-Authentifizierung

Inhalt

Einleitung

In diesem Dokument wird das Verhalten von Kerberos bei Verwendung in Verbindung mit Secure Access Zero Trust Network Access (ZTNA) beschrieben.

Voraussetzungen

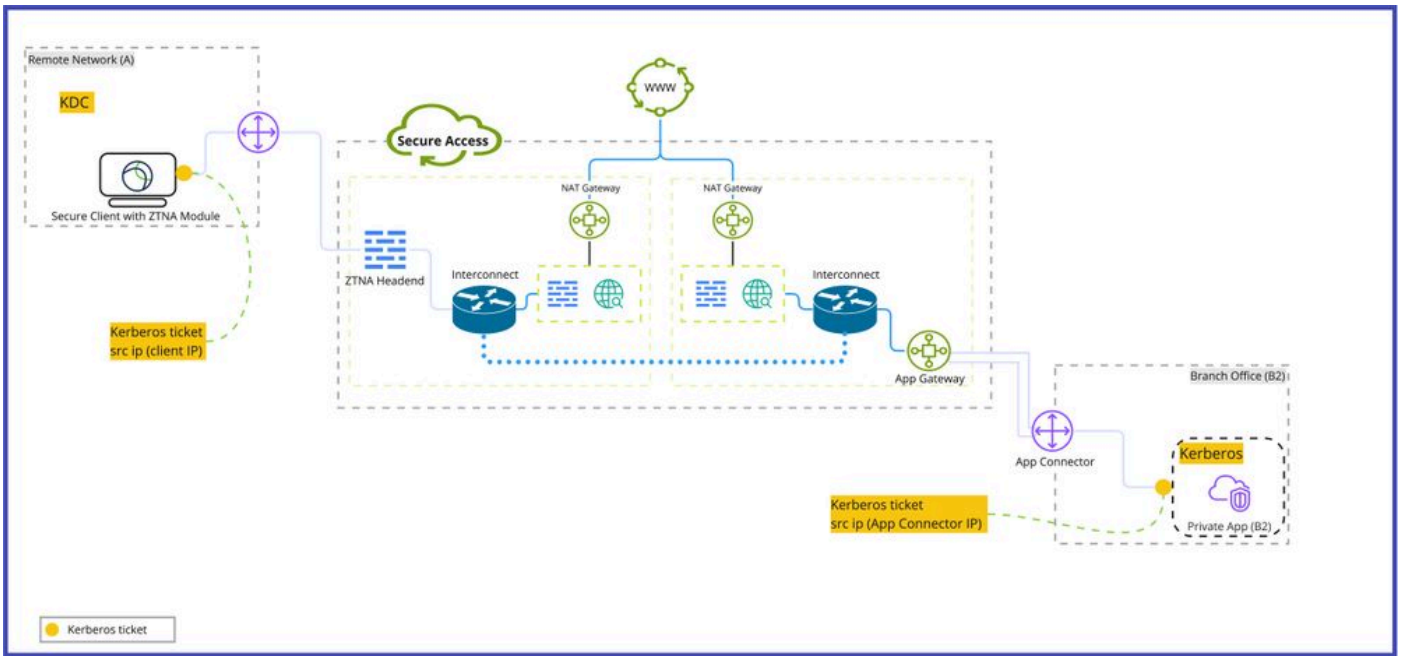
Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sicherer Zugriff
- Cisco Secure Client
- Internet Protocol Security (IPSEC)-Tunnel
- Remote Access Virtual Private Network (RAVPN)
- ZTNA (Zero Trust Network Access)

Hintergrundinformationen

Secure Access wird verwendet, um den Zugriff auf private Anwendungen über mehrere Szenarien hinweg zu ermöglichen, einschließlich ZTNA (Zero Trust Access Module) auf einem sicheren Client, IPSEC-Tunnel oder Remote Access VPN. Während private Anwendungen ihren eigenen Authentifizierungsmechanismus bereitstellen, gibt es eine Beschränkung für die Server, die Kerberos als Authentifizierungsmechanismus nutzen.



Kerberos-Paketfluss

Problem: Fehler beim Zugriff auf private Ressourcen mithilfe der Kerberos-Authentifizierung

Das Auslösen einer Authentifizierungsanforderung von einem Client-Gerät hinter dem ZTNA-Modul an eine private Anwendung hinter App Connector würde dazu führen, dass sich die Quell-IP-Adresse entlang des Pfads des Secure Access-Netzwerks ändert. Dies führt zu einem Authentifizierungsfehler bei Verwendung des vom Clients Kerberos Distribution Center (KDC) initiierten Kerberos-Tickets.

Lösung

Die Client-Quell-IP-Adresse ist Teil der Kerberos-Tickets, die vom Kerberos Distribution Center (KDC) gewährt werden. Im Allgemeinen muss die Quell-IP-Adresse beim Durchlaufen eines Kerberos-Tickets durch ein Netzwerk unverändert bleiben. Andernfalls akzeptiert der Zielserver, mit dem wir uns authentifizieren, das Ticket nicht, wenn er mit der Quell-IP verglichen wird, von der es gesendet wurde.

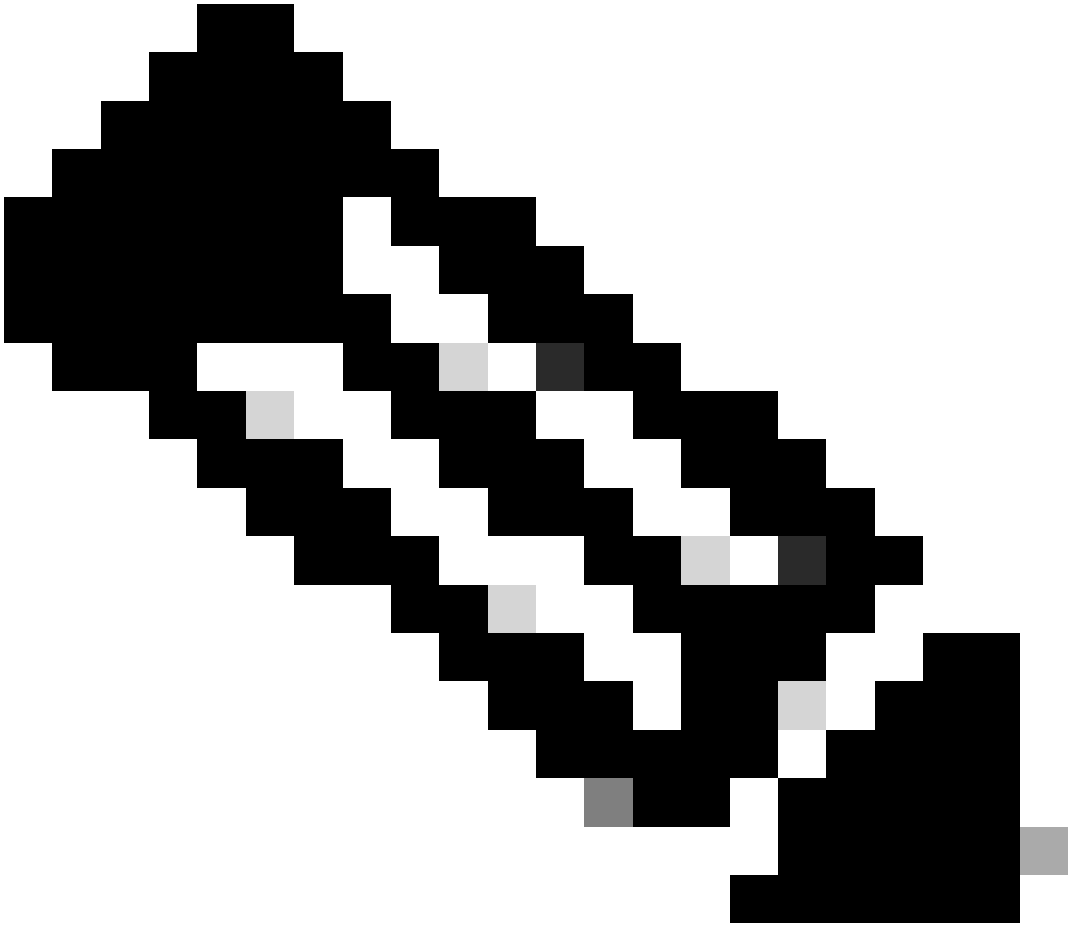
Verwenden Sie eine der folgenden Optionen, um dieses Problem zu beheben:

Option 1:

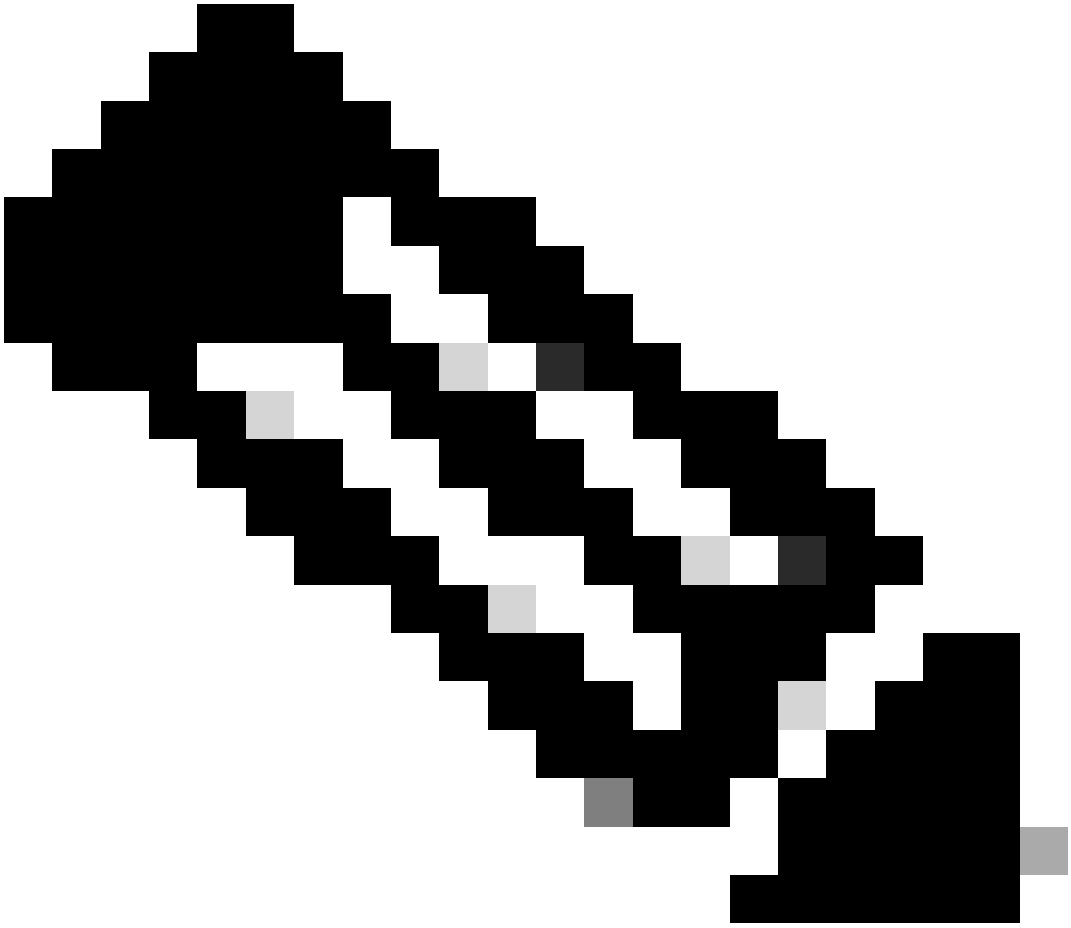
Deaktivieren Sie die Option, die Quell-IP-Adresse in das Client Kerberos-Ticket aufzunehmen.

Option 2:

Verwenden Sie Secure Access VPN mit privaten Ressourcen hinter dem IPSEC-Tunnel anstelle von privaten Anwendungen hinter App Connector.



Hinweis: Dieses Verhalten beeinträchtigt nur private Anwendungen, die hinter App Connector bereitgestellt werden, und der Datenverkehr stammt vom Client mit ZTNA-Modul ohne VPN.



Hinweis: Die Aktivitätssuche für sicheren Zugriff zeigt die zulässige Aktion für die Transaktion an, da die Sperre auf der Seite für private Anwendungen und nicht auf der Seite für sicheren Zugriff stattfindet.

Zugehörige Informationen

- Benutzerhandbuch zu Secure Access
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.