Troubleshoot Failure in Accessing Private Resources Using Kerberos Authentication

Contents

Introduction

This document describes Kerberos behavior when being used along with Secure Access Zero Trust Network Access (ZTNA).

Prerequisites

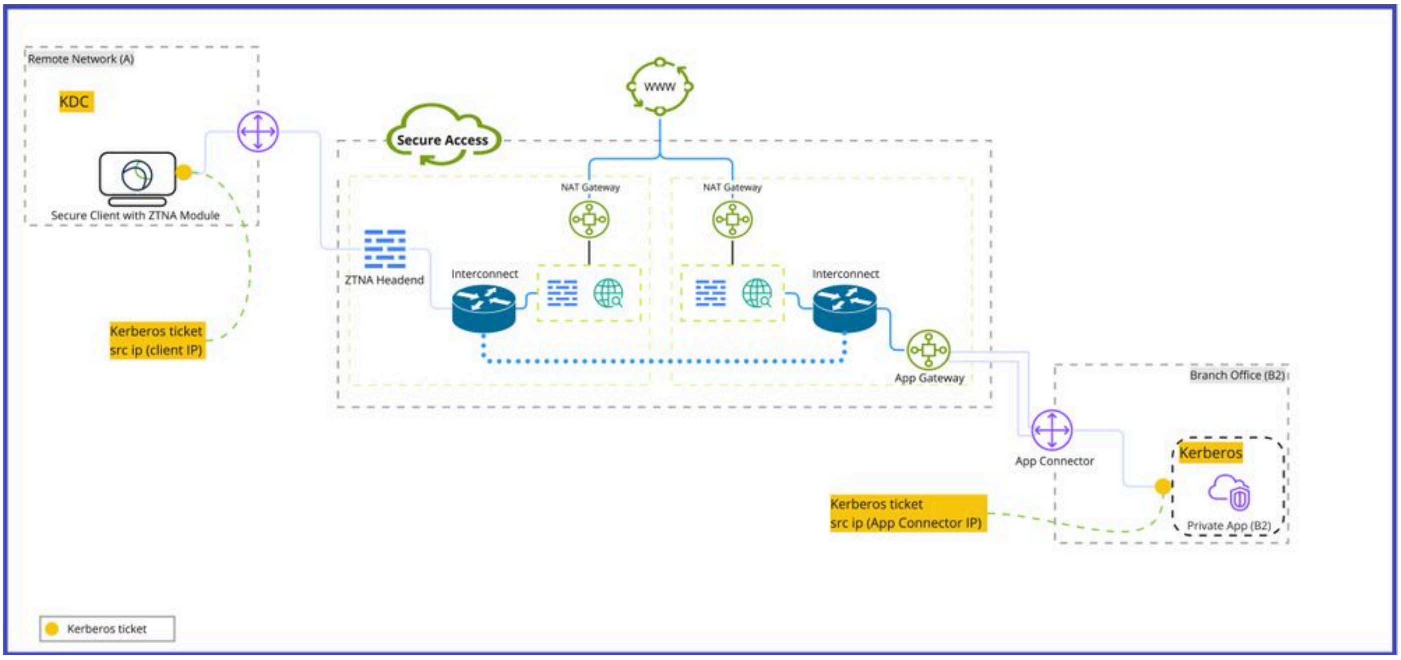
Requirements

Cisco recommends that you have knowledge of these topics:

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

Background Information

Secure Access is used in providing access to private applications through multiple scenarios including Zero Trust Access Module (ZTNA) on Secure Client, or IPSEC Tunnel or Remote Access VPN. While private applications provide their own authentication mechanism there is a limitation on the servers that rely on Kerberos as an authentication mechanism.



Kerberos packet flow

Problem: Failure in Accessing Private Resources Using Kerberos Authentication

Initiating an authentication request from a client device behind ZTNA module to a private application behind App Connector, would cause the source IP address to change along the path of Secure Access network. Which results in Authentication failure when using the kerberos ticket initiated by the Clients Kerberos Distribution Center (KDC).

Solution

Client source IP address is part of the Kerberos tickets granted from Kerberos Distribution Center (KDC). In general when Kerberos tickets traverse through a network it is required that source IP address remain unchanged, otherwise the destination server we are authenticating with, does not not honor the ticket when compared to the source IP its sent from.

To resolve this problem use one of the options:

Option 1:

Disable the option to include the source IP address in Client Kerberos ticket.

Option 2:

Use Secure Access VPN with private resources behind IPSEC tunnel instead of Private applications behind App Connector.

Note: This behavior is only impacting Private Applications deployed behind App Connector and traffic is sourced from Client with ZTNA Module without VPN.

Note: The Secure Access Activity Search shows allowed action for the transaction, as the block is happening on Private Application side not on Secure Access.

Related Information

- **Secure Access User Guide**
- **Technical Support & Documentation - Cisco Systems**