Solucione problemas de falha no acesso a recursos privados usando a autenticação Kerberos

Contents

Introdução

Este documento descreve o comportamento do Kerberos ao ser usado junto com o ZTNA (Secure Access Zero Trust Network Access).

Pré-requisitos

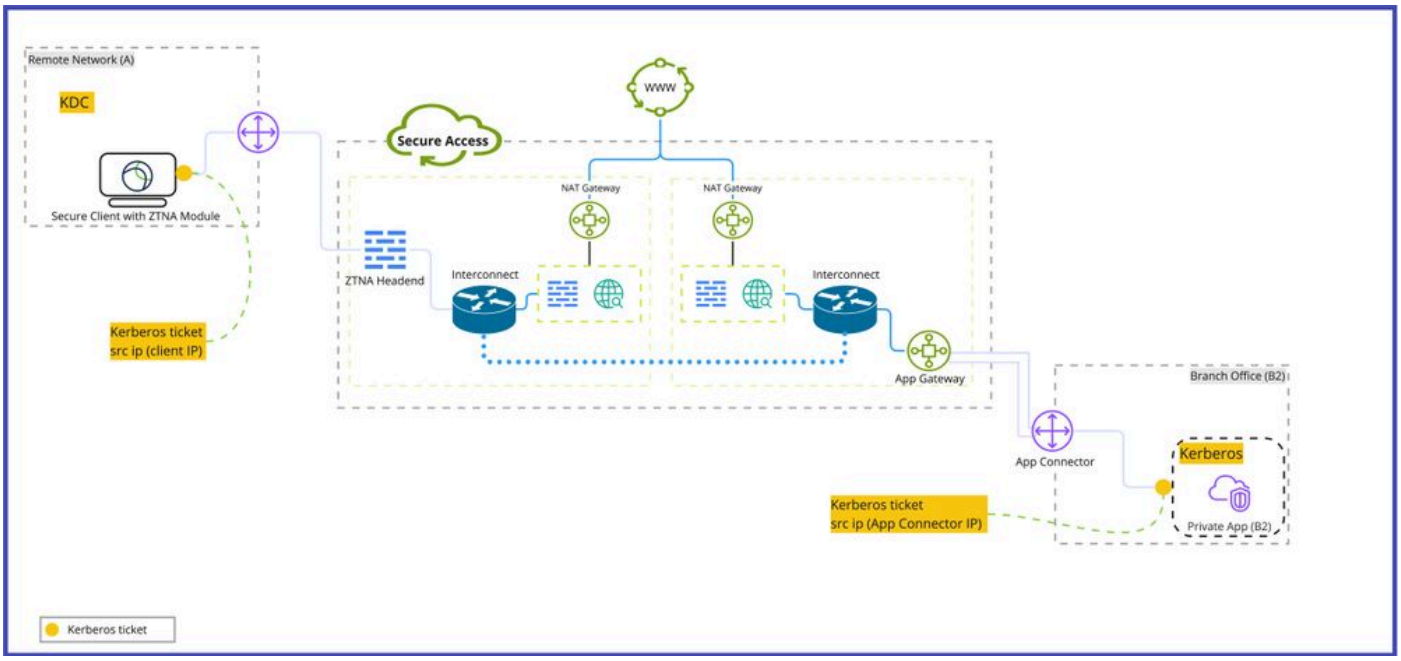
Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso seguro
- Cisco Secure Client
- Túneis de Segurança de Protocolo Internet (IPSEC)
- Rede Virtual Privada de Acesso Remoto (RAVPN)
- Acesso à rede com confiança zero (ZTNA)

Informações de Apoio

O acesso seguro é usado para fornecer acesso a aplicativos privados por meio de vários cenários, incluindo Zero Trust Access Module (ZTNA) no Secure Client, ou IPSEC Tunnel ou Remote Access VPN. Embora os aplicativos privados forneçam seu próprio mecanismo de autenticação, há uma limitação nos servidores que dependem do Kerberos como um mecanismo de autenticação.



Fluxo de pacote Kerberos

Problema: falha ao acessar recursos privados usando a autenticação Kerberos

Iniciar uma solicitação de autenticação de um dispositivo cliente por trás do módulo ZTNA para um aplicativo privado por trás do App Connector faria com que o endereço IP de origem mudasse ao longo do caminho da rede de Acesso Seguro. O que resulta em falha de autenticação ao usar o tíquete kerberos iniciado pelo Centro de Distribuição Kerberos de Clientes (KDC).

Solução

O endereço IP de origem do cliente faz parte dos tíquetes Kerberos concedidos pelo Centro de Distribuição Kerberos (KDC). Em geral, quando tíquetes Kerberos atravessam uma rede, é necessário que o endereço IP de origem permaneça inalterado; caso contrário, o servidor de destino com o qual estamos autenticando não honra o tíquete quando comparado ao IP de origem do qual ele foi enviado.

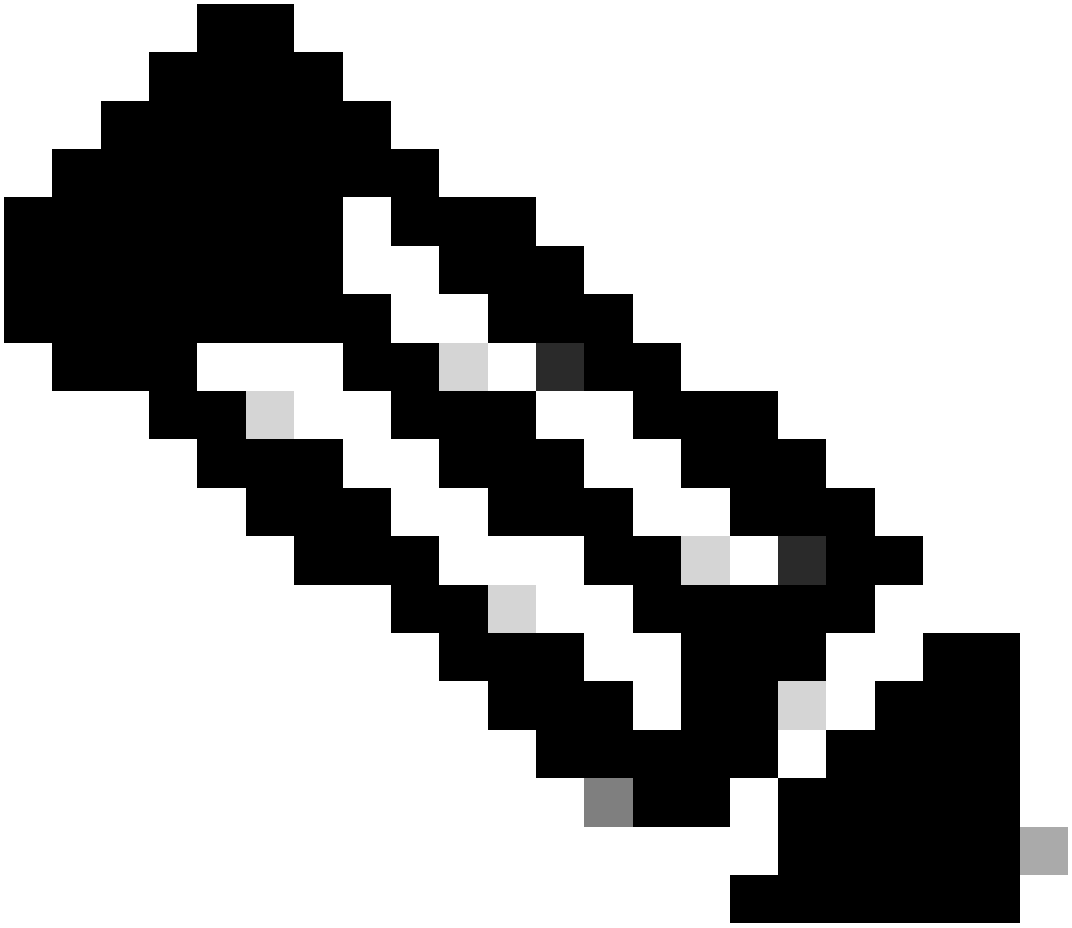
Para resolver esse problema, use uma das opções:

Opção 1:

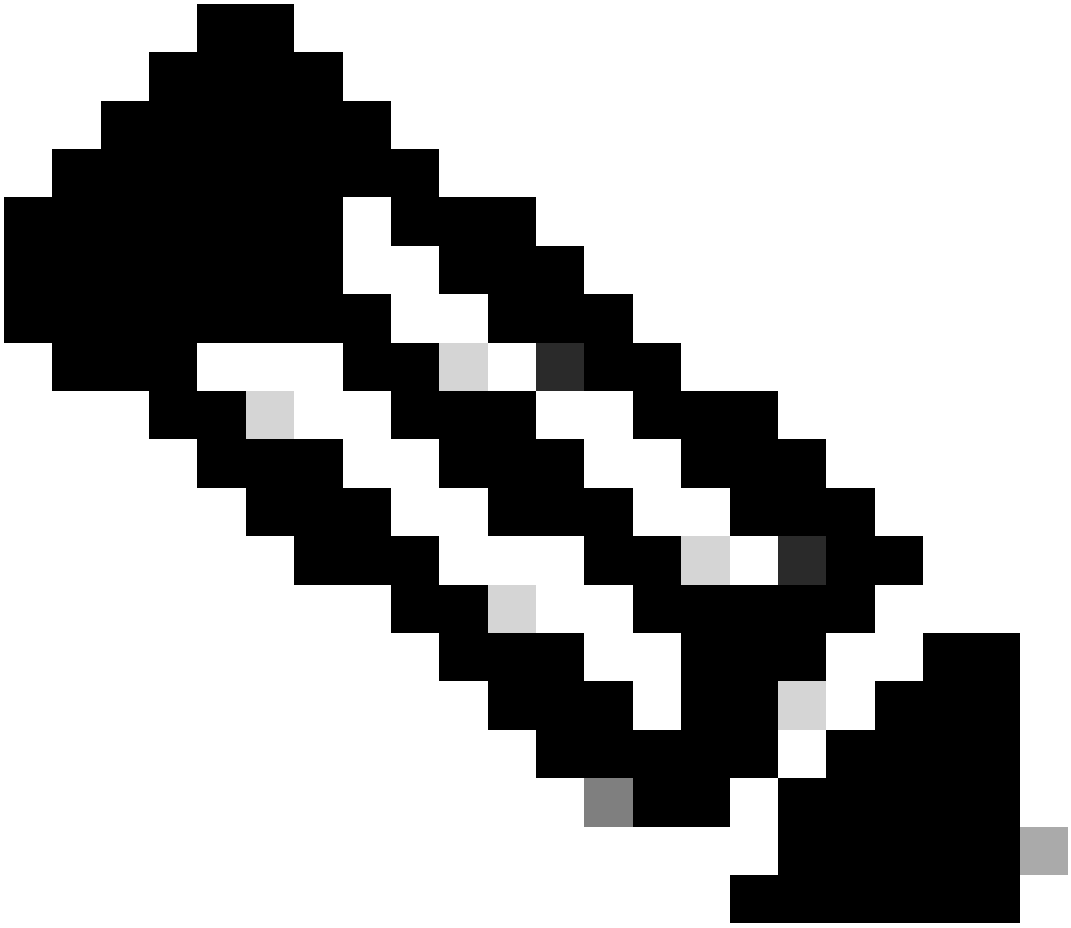
Desative a opção para incluir o endereço IP de origem no tíquete Kerberos do cliente.

Opção 2:

Use a VPN de acesso seguro com recursos privados por trás do túnel IPSEC em vez de aplicativos privados por trás do App Connector.



Observação: esse comportamento está afetando somente aplicativos privados implantados atrás do App Connector e o tráfego é originado do cliente com o ZTNA Module sem VPN.



Observação: A Pesquisa de Atividade de Acesso Seguro mostra a ação permitida para a transação, pois o bloqueio está acontecendo no lado da Aplicação Privada e não no Acesso Seguro.

Informações Relacionadas

- Guia do usuário do Secure Access
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.