Solución de problemas de acceso a recursos privados mediante la autenticación Kerberos

Contenido

Introducción

Este documento describe el comportamiento de Kerberos cuando se utiliza junto con Secure Access Zero Trust Network Access (ZTNA).

Prerequisites

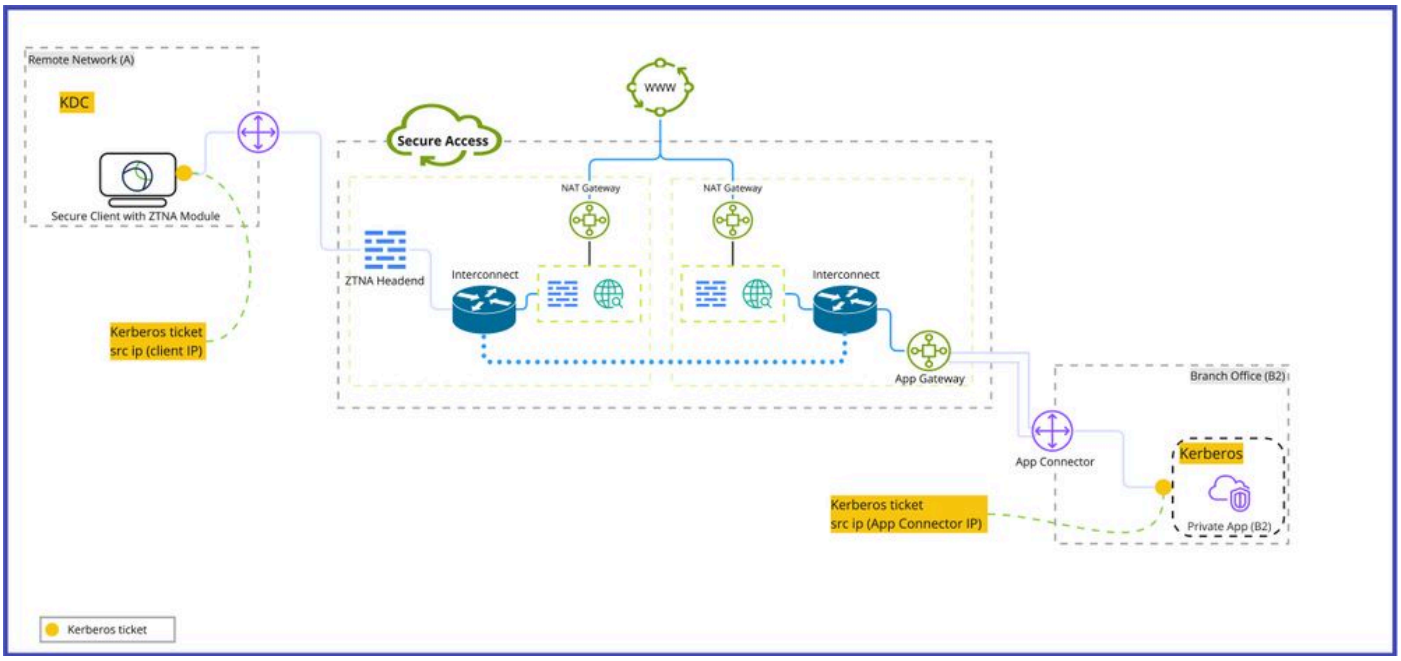
Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso seguro
- Cliente seguro de Cisco
- Túneles de seguridad de protocolo de Internet (IPSEC)
- Red privada virtual de acceso remoto (RAVPN)
- Acceso a la red sin confianza (ZTNA)

Antecedentes

El acceso seguro se utiliza para proporcionar acceso a aplicaciones privadas a través de varios escenarios, incluido el módulo de acceso de confianza cero (ZTNA) en Secure Client, o túnel IPSEC o VPN de acceso remoto. Mientras que las aplicaciones privadas proporcionan su propio mecanismo de autenticación, hay una limitación en los servidores que dependen de Kerberos como mecanismo de autenticación.



flujo de paquetes Kerberos

Problema: Error al obtener acceso a recursos privados mediante la autenticación Kerberos

Iniciar una solicitud de autenticación desde un dispositivo cliente detrás del módulo ZTNA a una aplicación privada detrás de App Connector, haría que la dirección IP de origen cambiara a lo largo de la trayectoria de la red de acceso seguro. Lo que provoca un error de autenticación al utilizar el vale Kerberos iniciado por el Centro de distribución Kerberos (KDC) de clientes.

Solución

La dirección IP de origen del cliente forma parte de los vales Kerberos concedidos desde el Centro de distribución de Kerberos (KDC). En general, cuando los tickets Kerberos atraviesan una red, se requiere que la dirección IP de origen permanezca sin cambios; de lo contrario, el servidor de destino con el que estamos autenticando no respeta el ticket cuando se compara con la IP de origen desde la que se envía.

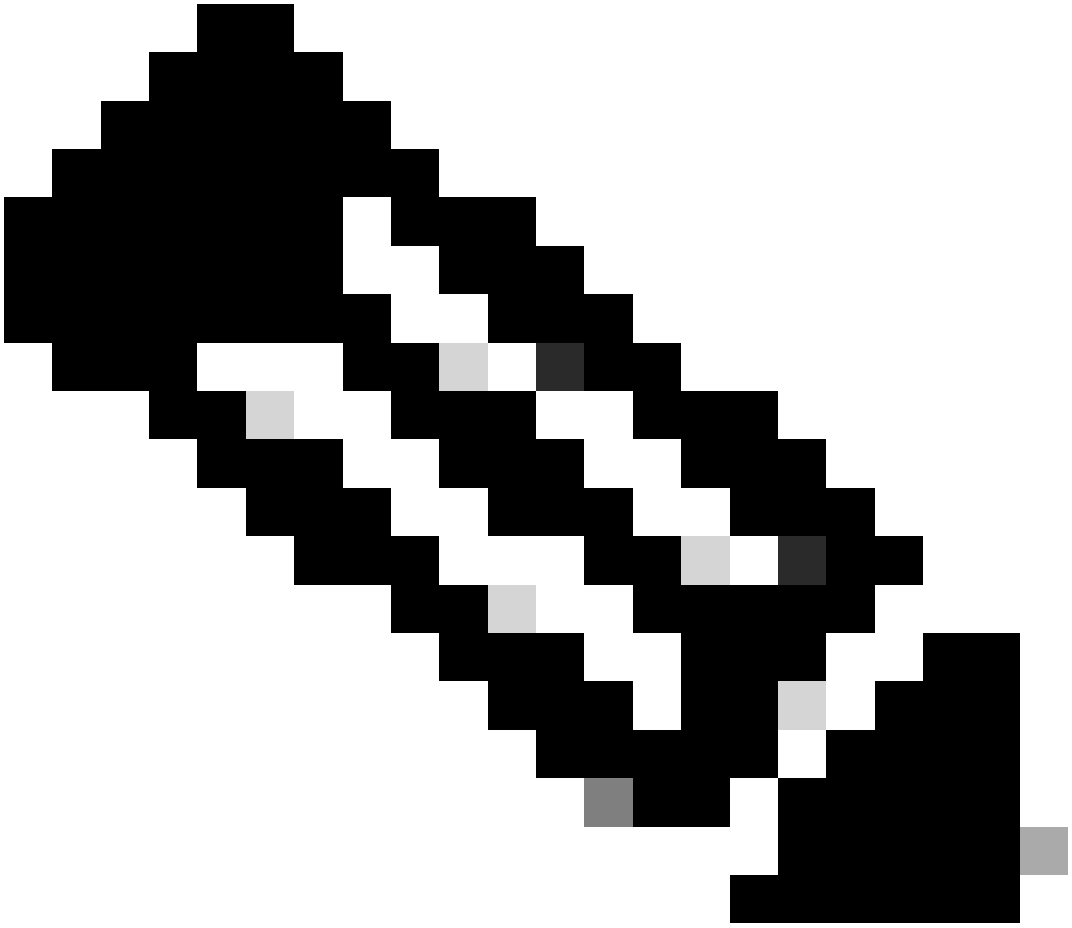
Para resolver este problema, utilice una de las siguientes opciones:

Opción 1:

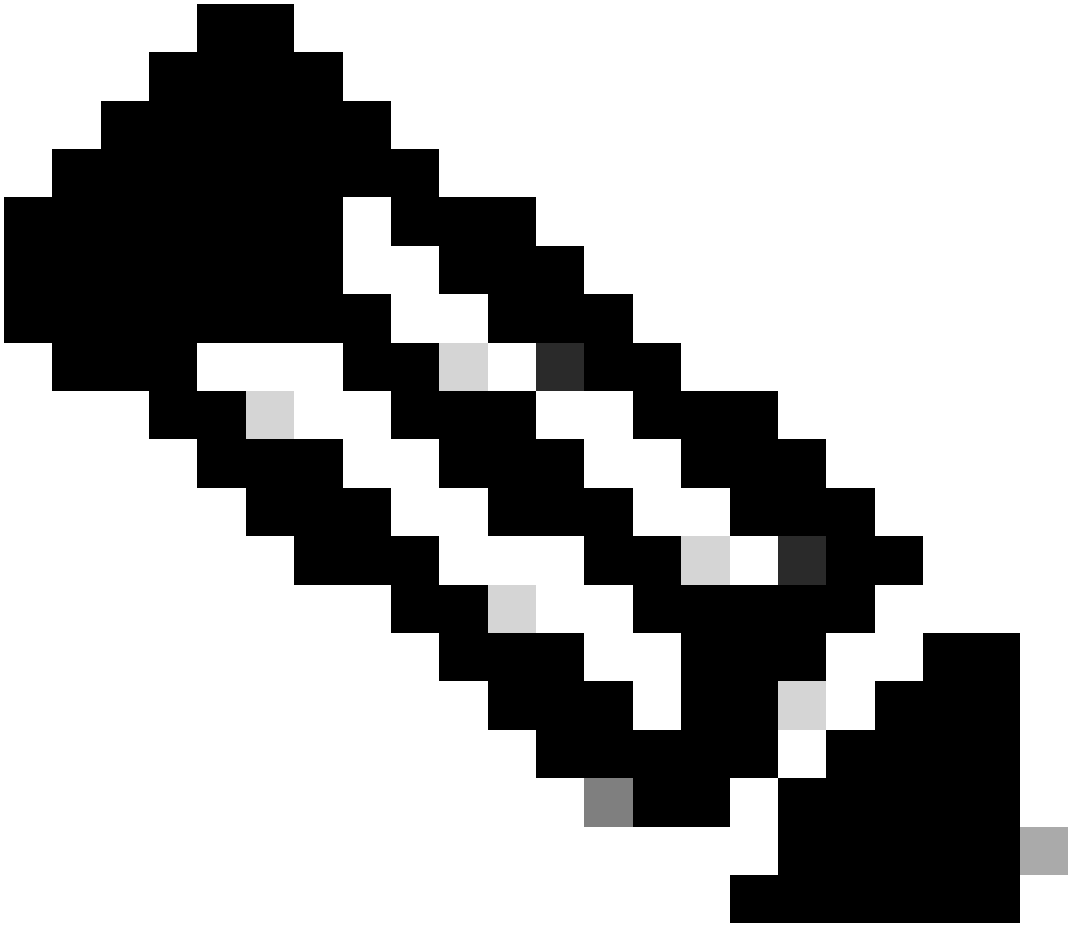
Desactive la opción para incluir la dirección IP de origen en el vale Kerberos de cliente.

Opción 2:

Utilice VPN de acceso seguro con recursos privados detrás del túnel IPSEC en lugar de aplicaciones privadas detrás de App Connector.



Nota: este comportamiento solo afecta a las aplicaciones privadas implementadas detrás de App Connector y el tráfico se origina en el cliente con el módulo ZTNA sin VPN.



Nota: La búsqueda de actividad de acceso seguro muestra la acción permitida para la transacción, ya que el bloqueo se produce en el lado de la aplicación privada y no en el de acceso seguro.

Información Relacionada

- Guía del usuario de Secure Access
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).