使用Kerberos身份验证访问私有资源时排除故障

目录

简介

本文档介绍与安全访问零信任网络访问(ZTNA)配合使用时Kerberos的行为。

先决条件

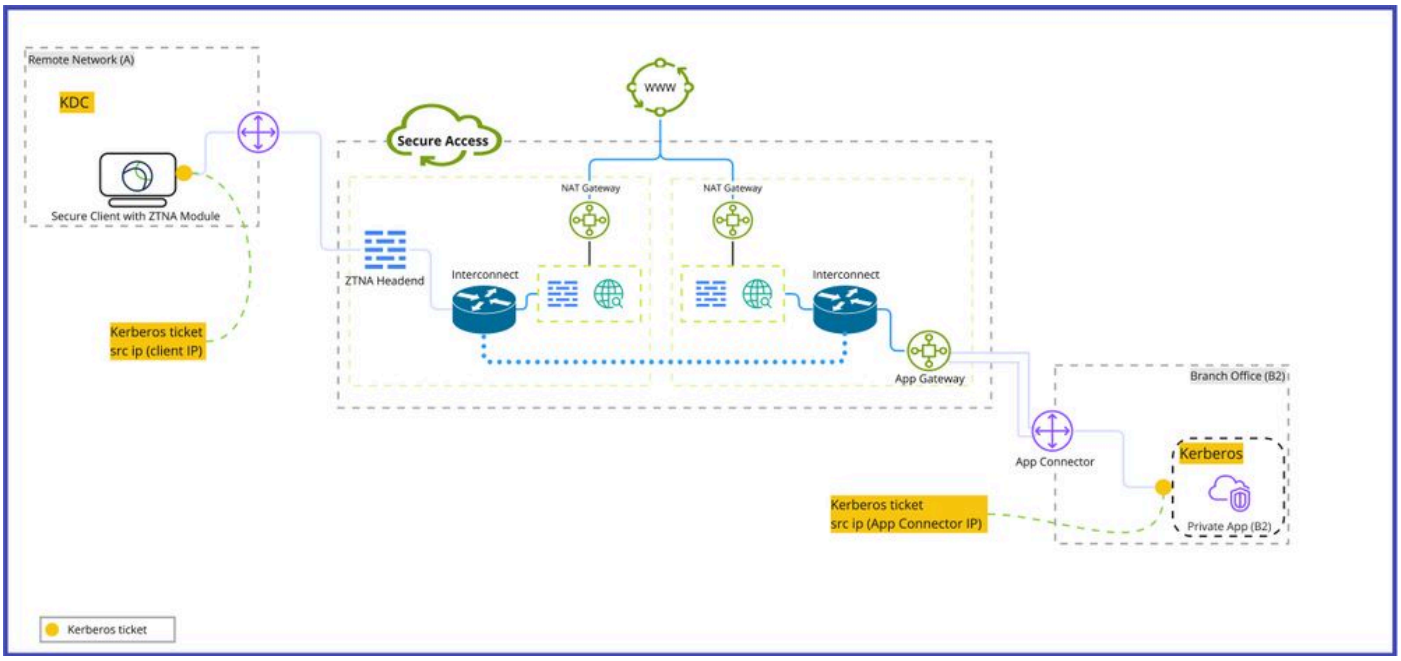
要求

Cisco 建议您了解以下主题：

- 安全访问
- 思科安全客户端
- Internet协议安全(IPSEC)隧道
- 远程访问虚拟专用网络(RAVPN)
- 零信任网络访问(ZTNA)

背景信息

安全访问用于通过多种方案提供对专用应用的访问，包括安全客户端上的零信任访问模块(ZTNA)、IPSEC隧道或远程访问VPN。虽然私有应用程序提供自己的身份验证机制，但是依赖Kerberos作为身份验证机制的服务器存在限制。



Kerberos数据包流

问题：使用Kerberos身份验证访问私有资源失败

从ZTNA模块后的客户端设备向App Connector后的专用应用发起身份验证请求将导致源IP地址沿安全访问网络的路径发生更改。这会导致在使用客户端Kerberos分发中心(KDC)发起的Kerberos票证时身份验证失败。

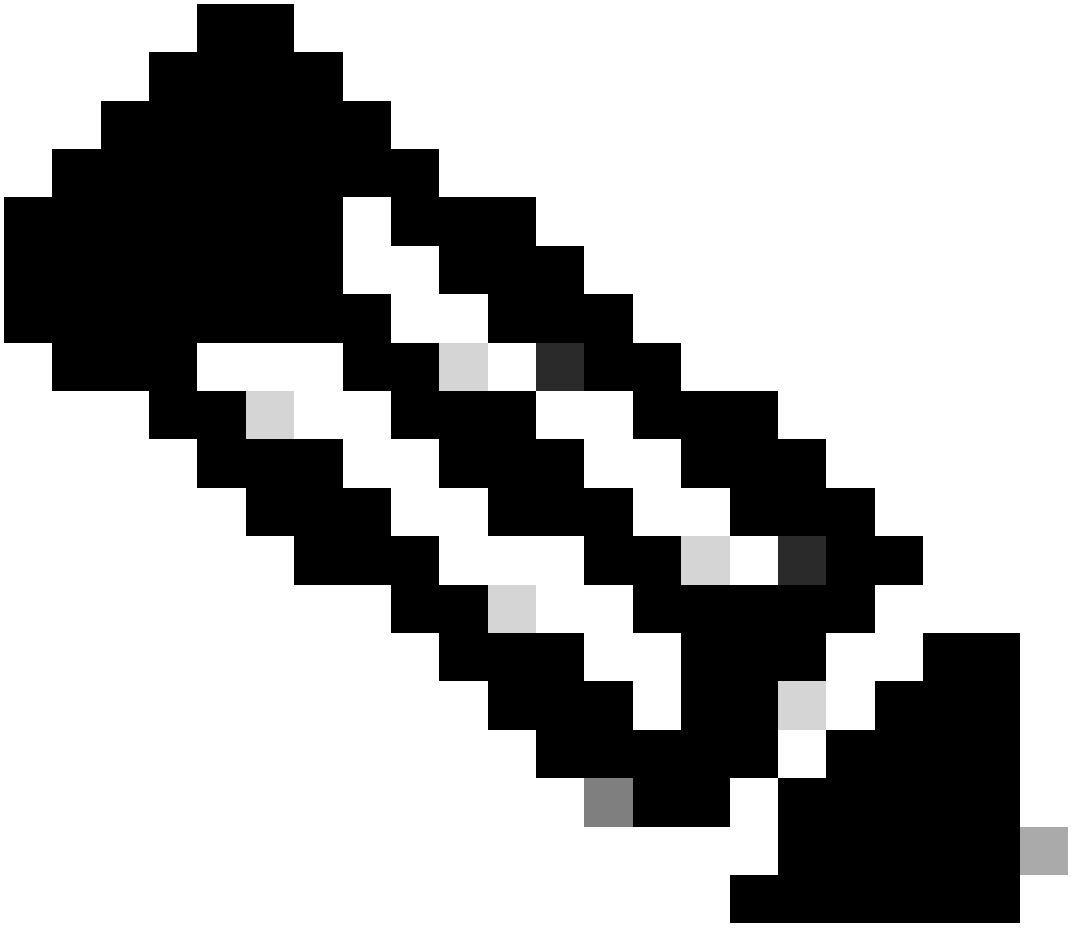
解决方案

客户端源IP地址是从Kerberos分发中心(KDC)授予的Kerberos票证的一部分。通常，当Kerberos票证遍历网络时，要求源IP地址保持不变，否则与发送票证的源IP相比，我们正在与其进行身份验证的目标服务器不会兑现票证。

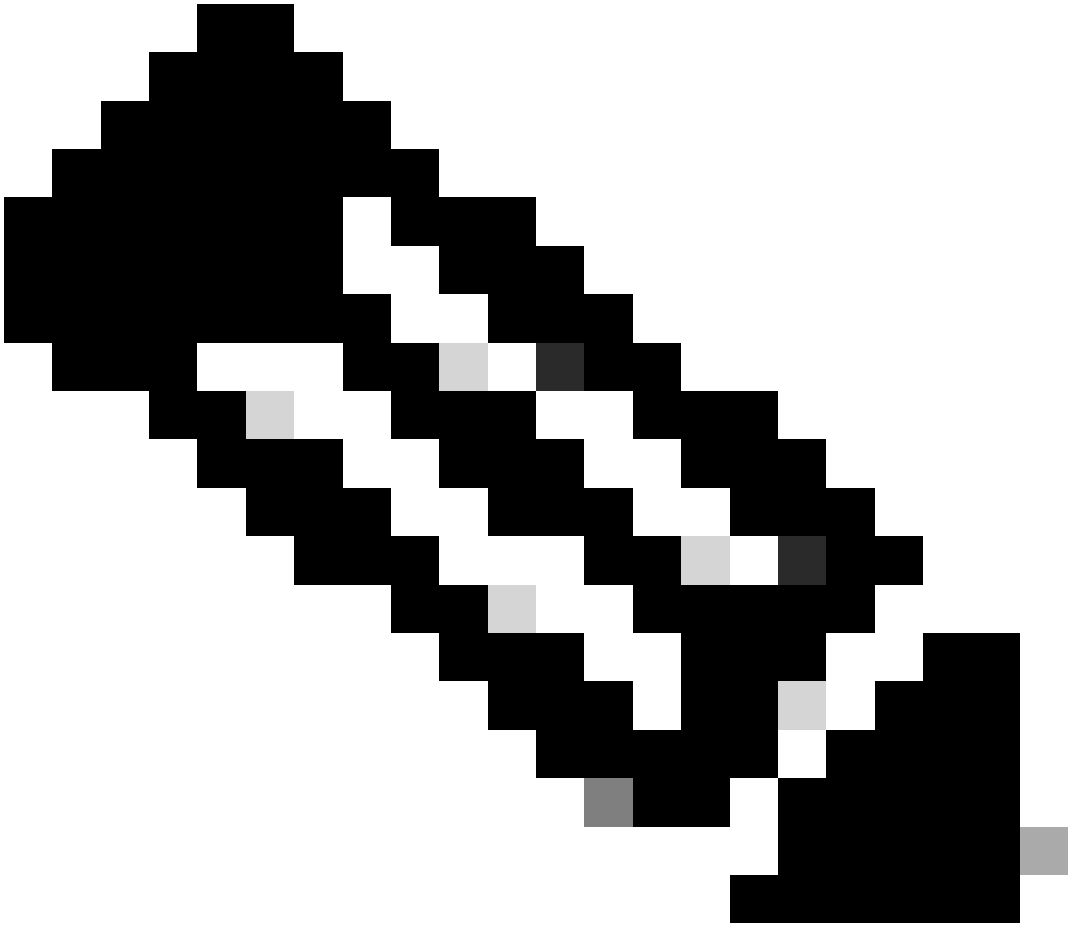
为了解决此问题：

1. 禁用在客户端Kerberos票证中包含源IP地址的选项。

2. 将安全访问VPN与IPSEC隧道后的专用资源配合使用，而不是与App Connector后的专用应用配合使用。



注意：此行为仅影响部署在App Connector之后的专用应用，并且流量来自不带VPN的ZTNA模块的客户端。



注意：安全访问活动搜索显示允许的交易操作，因为阻止发生在专用应用端，而不是安全访问端。

相关信息

- 安全访问用户指南
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。