Kerberos認証を使用したプライベートリソースへのアクセス障害のトラブルシューティング

内容

はじめに

このドキュメントでは、Secure Access Zero Trust Network Access(ZTNA)とともに使用される場合のKerberosの動作について説明します。

前提条件

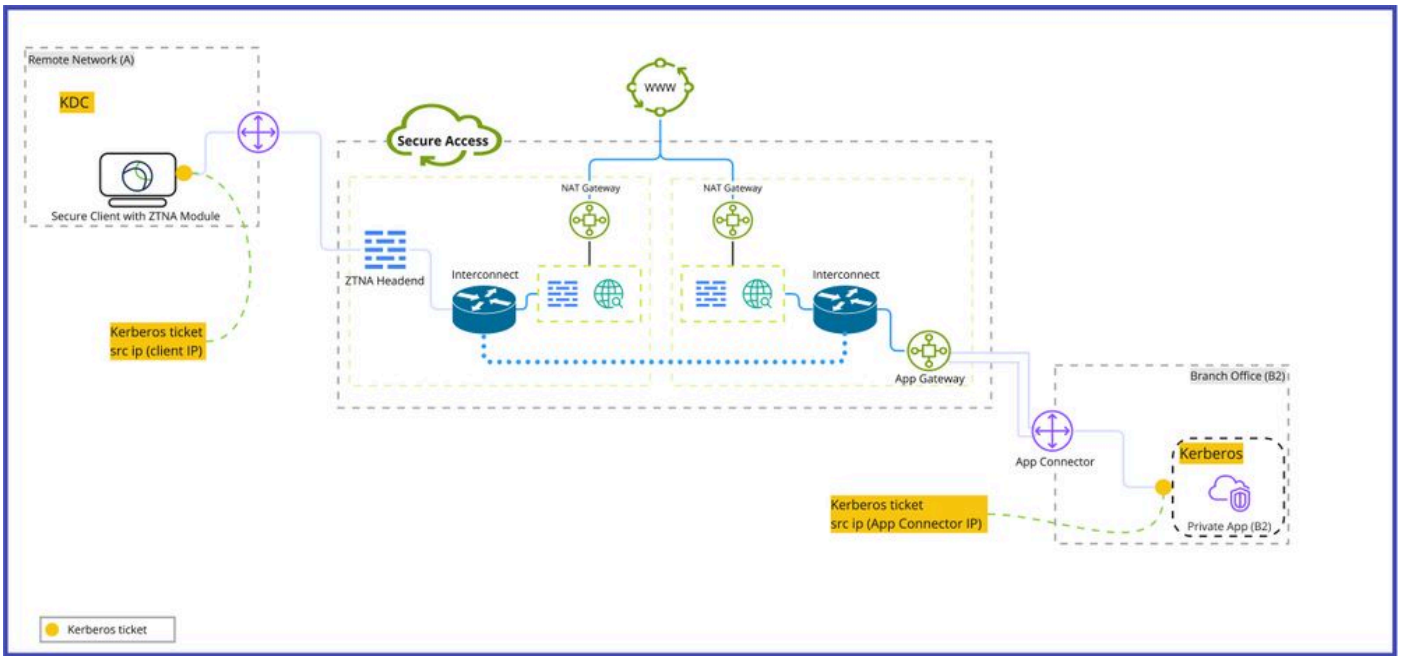
要件

次の項目に関する知識があることが推奨されます。

- セキュアなアクセス
- Cisco Secure Client
- インターネットプロトコルセキュリティ(IPSEC)トンネル
- リモートアクセス仮想プライベートネットワーク(RAVPN)
- ゼロトラストネットワークアクセス(ZTNA)

背景説明

セキュアアクセスは、セキュアクライアント上のZero Trust Access Module(ZTNA)、IPSECトンネル、リモートアクセスVPNなど、複数のシナリオを通じてプライベートアプリケーションへのアクセスを提供する際に使用されます。プライベートアプリケーションは独自の認証メカニズムを提供しますが、認証メカニズムとしてKerberosに依存するサーバには制限があります。



Kerberosパケットフロー

問題：Kerberos認証を使用したプライベートリソースへのアクセスの失敗

ZTNAモジュールの背後にあるクライアントデバイスからApp Connectorの背後にあるプライベートアプリケーションに認証要求を開始すると、送信元IPアドレスがSecure Accessネットワークのパスに沿って変更されます。これにより、クライアントのKerberos配布センター(KDC)によって開始されたKerberosチケットを使用する場合に、認証エラーが発生します。

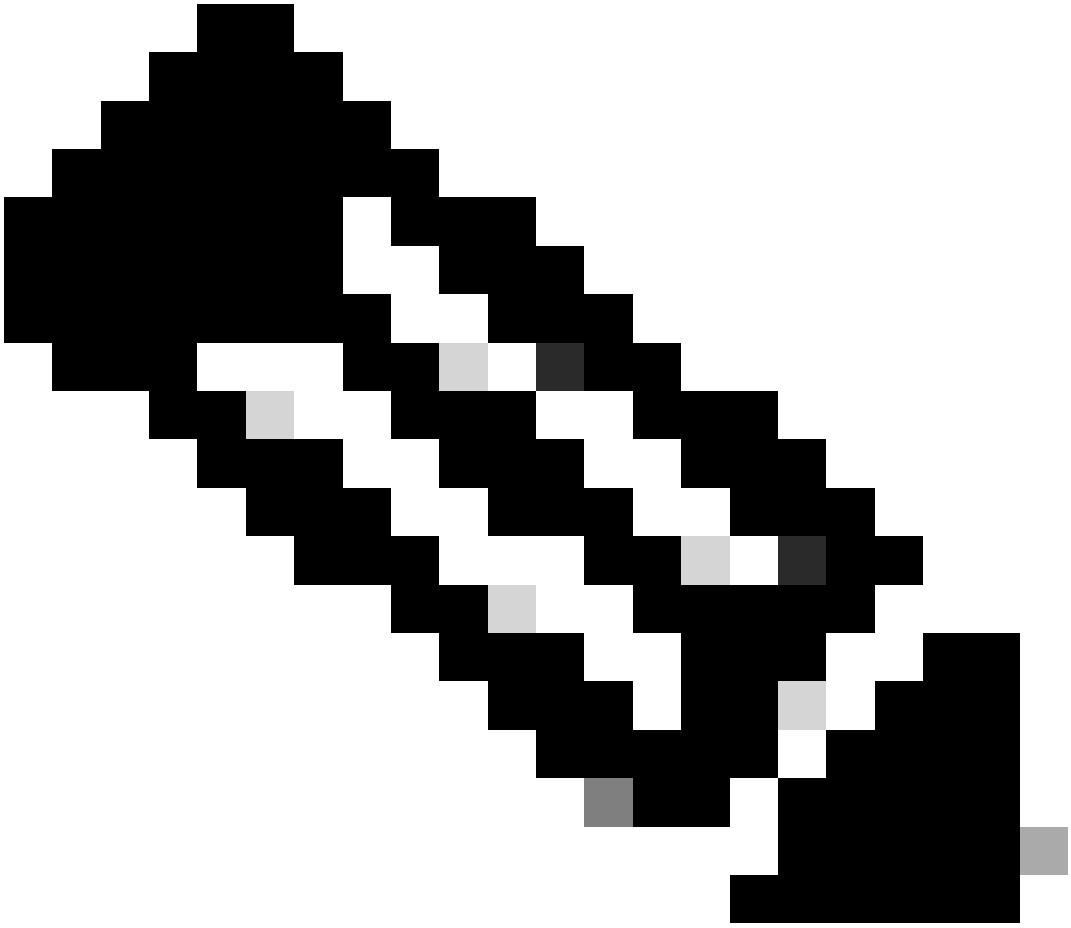
解決方法

クライアントの送信元IPアドレスは、Kerberos配布センター(KDC)から付与されたKerberosチケットの一部です。一般に、Kerberosチケットがネットワークを通過する場合、送信元IPアドレスは変更されないままにしておく必要があります。そうしない場合、認証に使用する宛先サーバでは、送信元IPと比較してチケットが承認されません。

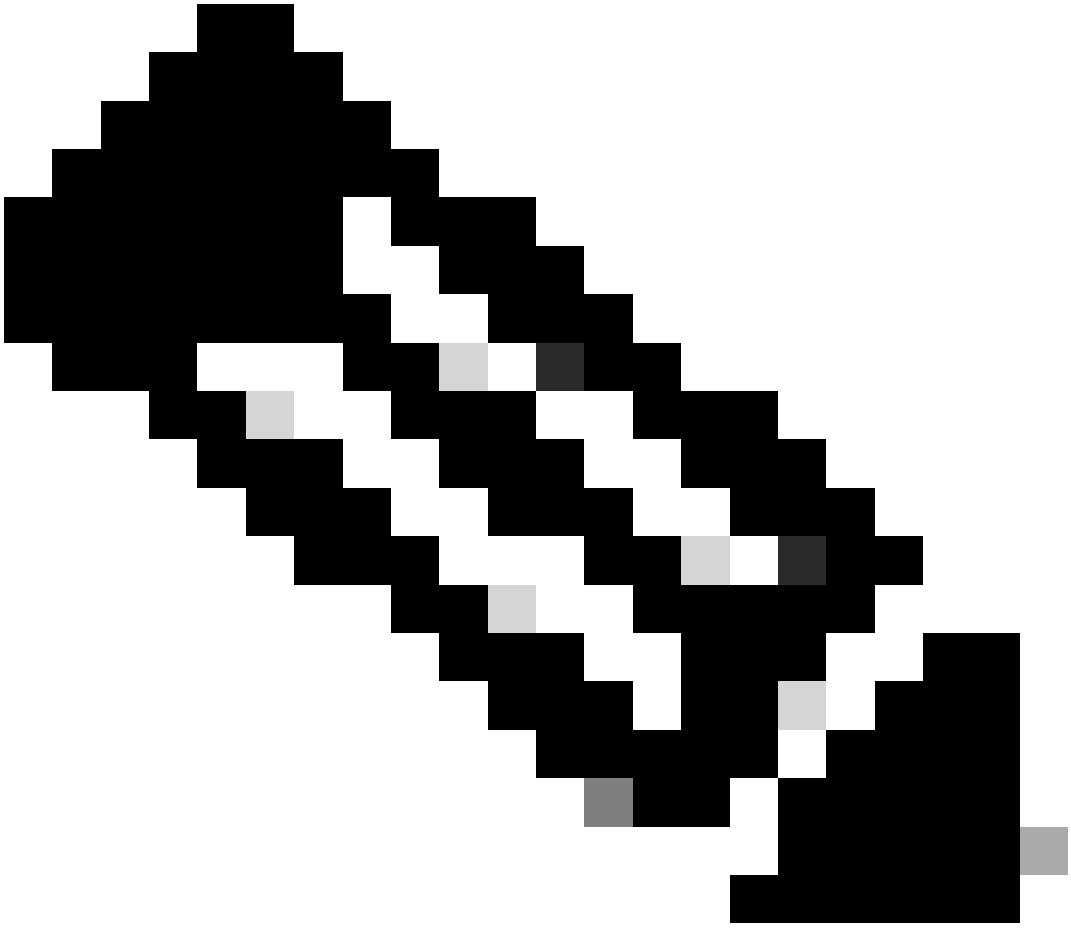
この問題を解決するには、

1. クライアントのKerberosチケットに送信元IPアドレスを含めるオプションを無効にします。

2. App Connectorの背後にあるプライベートアプリケーションの代わりに、IPSECトンネルの背後にあるプライベートリソースを持つセキュアアクセスVPNを使用します。



注：この動作は、App Connectorの背後に導入されたプライベートアプリケーションにのみ影響し、トラフィックの送信元はVPNを使用しないZTNAモジュールを使用するクライアントです。



注意：ブロックはセキュア・アクセスではないプライベート・アプリケーション側で発生しているため、セキュア・アクセス・アクティビティ検索にはトランザクションで許可されたアクションが表示されます。

関連情報

- セキュアアクセスユーザガイド
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。