Probleemoplossing bij toegang tot privé-bronnen met Kerberos-verificatie

Inhoud

Inleiding

Voorwaarden

Vereisten

Achtergrondinformatie

Probleem: geen toegang tot privé-bronnen met Kerberos-verificatie

Oplossing

Gerelateerde informatie

Inleiding

Dit document beschrijft het gedrag van Kerberos wanneer het samen met Secure Access Zero Trust Network Access (ZTNA) wordt gebruikt.

Voorwaarden

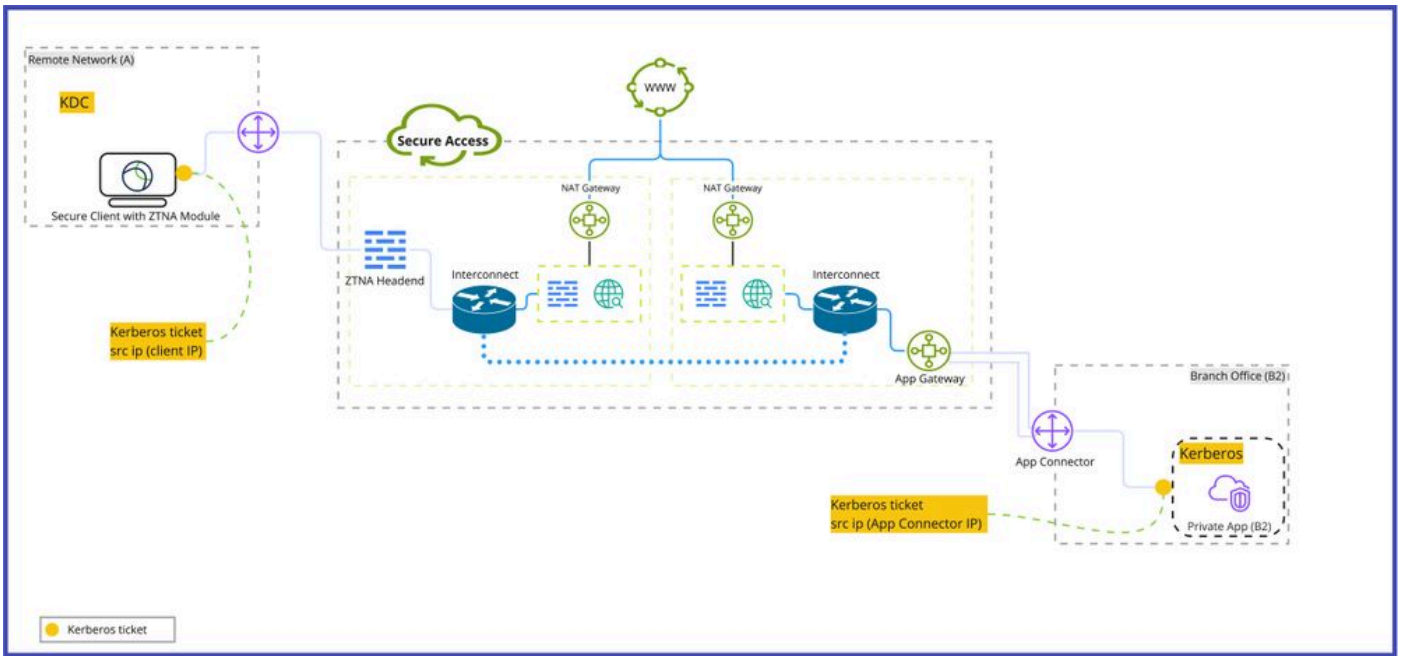
Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Beveiligde toegang
- Cisco Secure-client
- IPSEC-tunnels (Internet Protocol Security)
- Remote Access Virtual Private Network (RAVPN)
- Nul Trust Network Access (ZTNA)

Achtergrondinformatie

Secure Access wordt gebruikt bij het bieden van toegang tot privé-toepassingen via meerdere scenario's, waaronder Zero Trust Access Module (ZTNA) op Secure Client, of IPSEC-tunnel of externe toegang tot VPN. Terwijl particuliere applicaties hun eigen authenticatiemechanisme bieden, is er een beperking op de servers die vertrouwen op Kerberos als een authenticatiemechanisme.



Kerberos-pakketstroom

Probleem: geen toegang tot privé-bronnen met Kerberos-verificatie

Het initiëren van een verificatieverzoek van een clientapparaat achter de ZTNA-module naar een privétoepassing achter App Connector, zou ervoor zorgen dat het IP-adres van de bron verandert langs het pad van Secure Access-netwerk. Dat resulteert in verificatiefout bij het gebruik van het kerberos-ticket geïnitieerd door het Clients Kerberos Distribution Center (KDC).

Oplossing

Het IP-adres van de clientbron maakt deel uit van de Kerberos-tickets die zijn verleend door het Kerberos Distribution Center (KDC). In het algemeen wanneer Kerberos-tickets door een netwerk reizen, is het vereist dat het IP-bronadres ongewijzigd blijft, anders de doelserver waarmee we authenticeren, het ticket niet wordt gehonoreerd in vergelijking met het IP-bronadres waarvan het wordt verzonden.

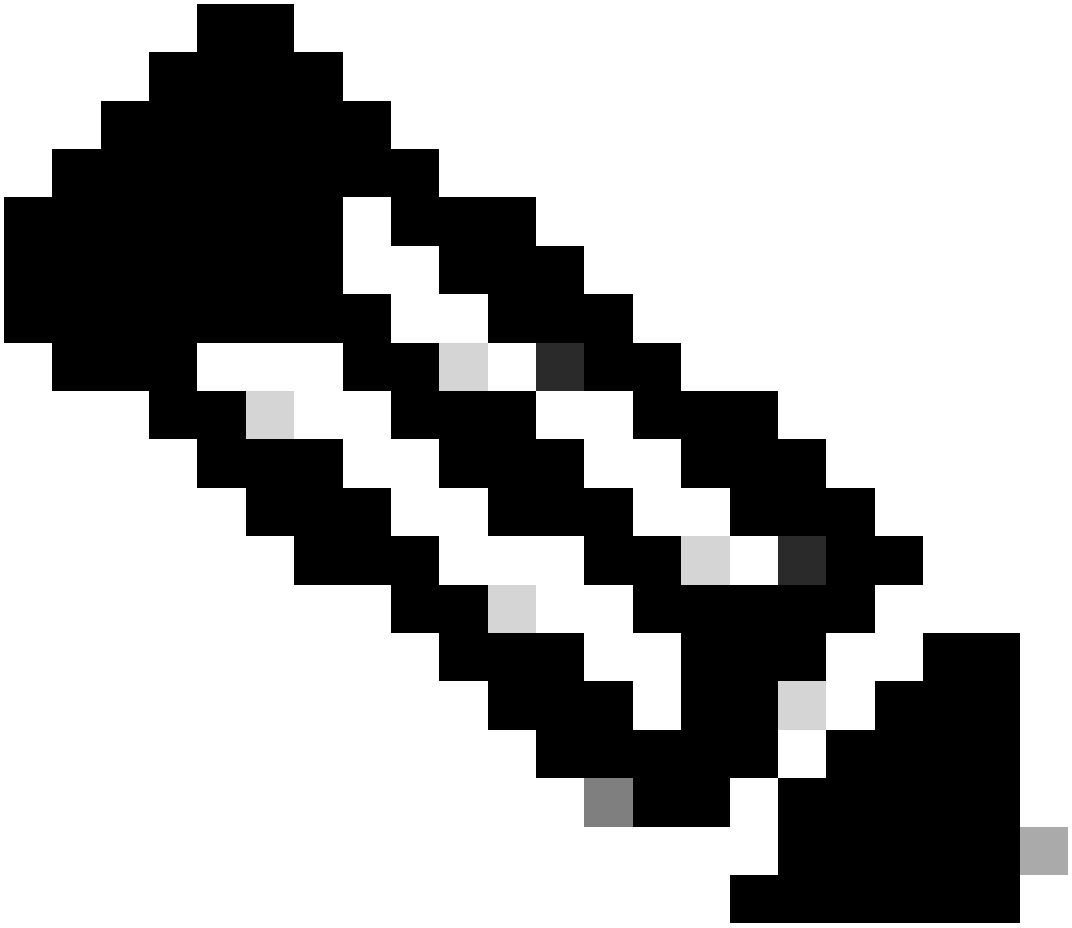
Gebruik een van de volgende opties om dit probleem op te lossen:

Optie 1:

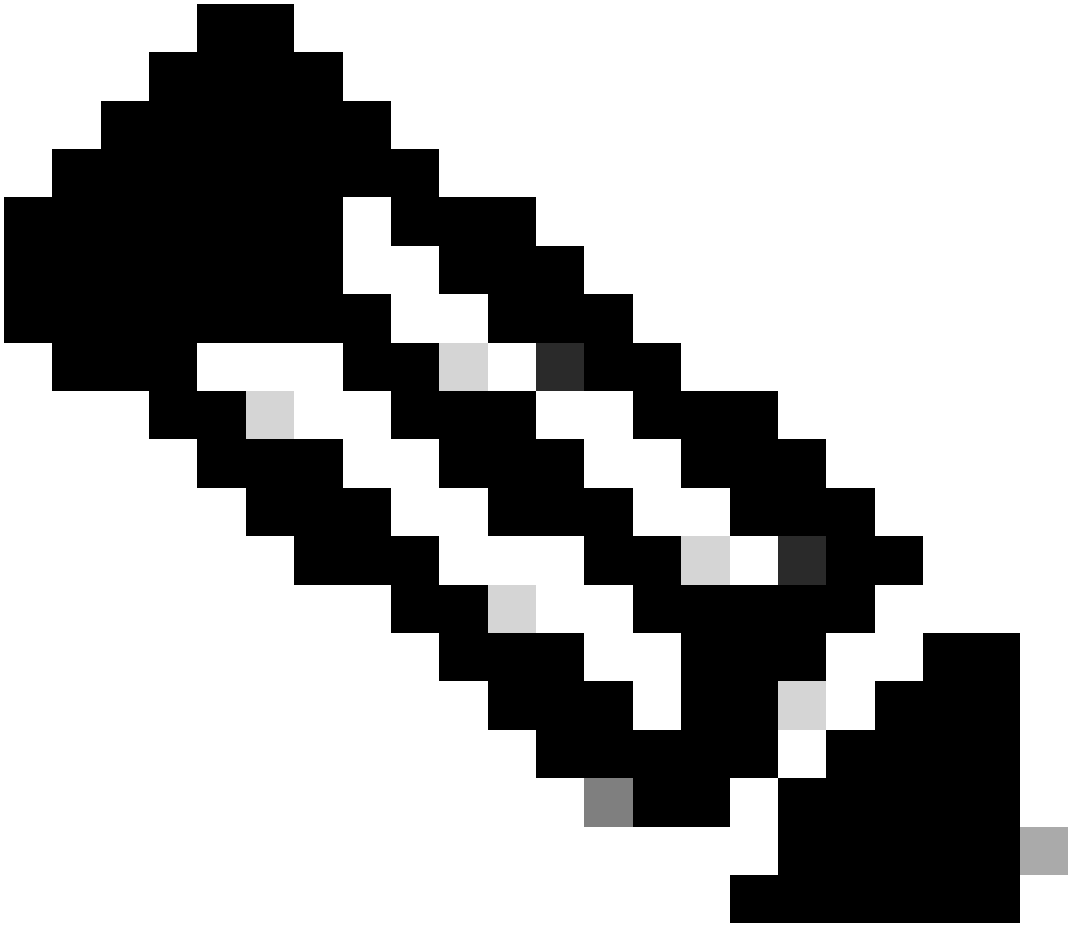
Schakel de optie uit om het IP-adres van de bron op te nemen in het ticket van Client Kerberos.

Optie 2:

Gebruik Secure Access VPN met privé-bronnen achter de IPSEC-tunnel in plaats van Private applicaties achter App Connector.



Opmerking: dit gedrag heeft alleen invloed op Private Toepassingen die worden geïmplementeerd achter App Connector en verkeer is afkomstig van client met ZTNA-module zonder VPN.



Opmerking: Het zoeken naar beveiligde toegangsactiviteiten laat zien dat er actie voor de transactie is toegestaan, aangezien het blok wordt uitgevoerd op Private Application kant en niet op Secure Access.

Gerelateerde informatie

- Gebruikershandleiding voor Secure Access
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.