Risoluzione dei problemi relativi all'accesso non riuscito alle risorse private tramite l'autenticazione Kerberos

Sommario

Introduzione

In questo documento viene descritto il comportamento di Kerberos quando viene utilizzato con Secure Access Zero Trust Network Access (ZTNA).

Prerequisiti

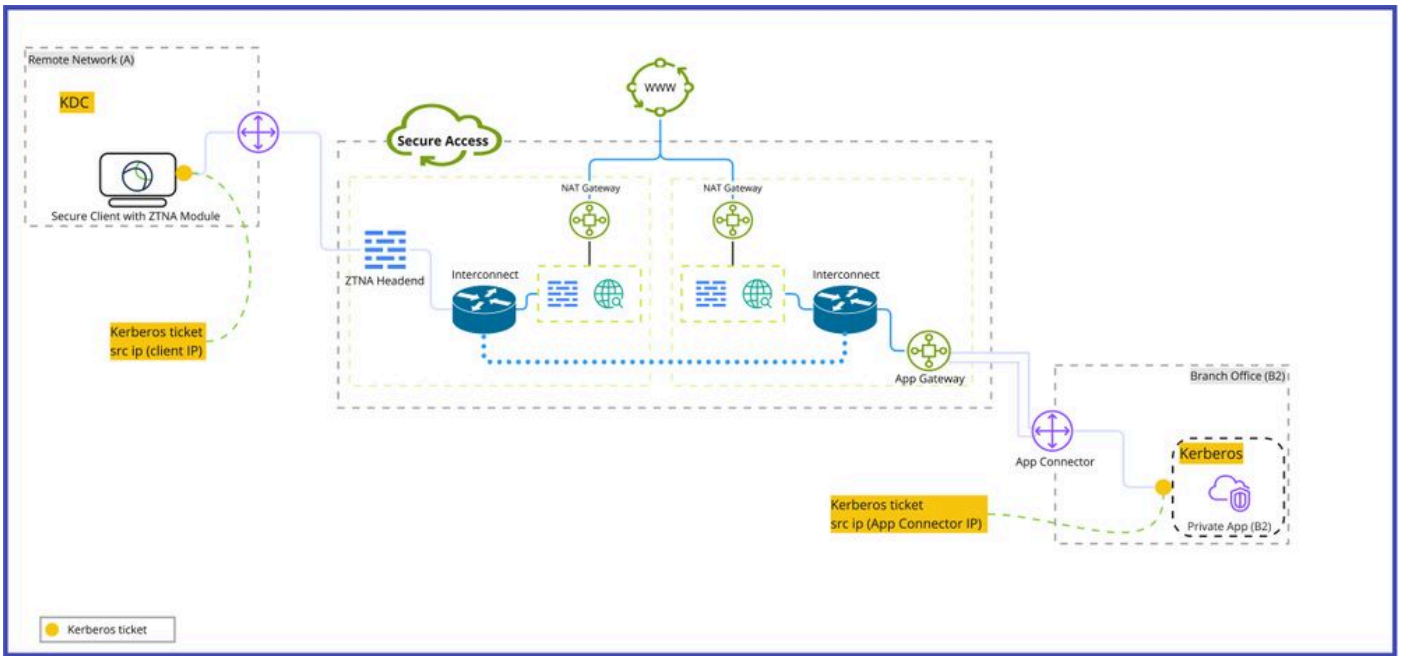
Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso sicuro
- Cisco Secure Client
- Tunnel Internet Protocol Security (IPSEC)
- RAVPN (Virtual Private Network) di accesso remoto
- Accesso di rete senza trust (ZTNA)

Premesse

Secure Access viene utilizzato per fornire l'accesso alle applicazioni private attraverso più scenari, tra cui Zero Trust Access Module (ZTNA) su Secure Client, Tunnel IPSEC o VPN ad accesso remoto. Mentre le applicazioni private forniscono il proprio meccanismo di autenticazione, esiste una limitazione per i server che si basano su Kerberos come meccanismo di autenticazione.



Flusso di pacchetti Kerberos

Problema: impossibile accedere alle risorse private utilizzando l'autenticazione Kerberos

L'avvio di una richiesta di autenticazione da un dispositivo client dietro il modulo ZTNA a un'applicazione privata dietro App Connector, causerebbe la modifica dell'indirizzo IP di origine lungo il percorso della rete di accesso sicuro. Il che determina un errore di autenticazione quando si utilizza il ticket Kerberos avviato dal centro distribuzione Kerberos (KDC) client.

Soluzione

L'indirizzo IP di origine del client fa parte dei ticket Kerberos concessi dal centro di distribuzione Kerberos (KDC). In generale, quando i ticket Kerberos attraversano una rete, è necessario che l'indirizzo IP di origine rimanga invariato. In caso contrario, il server di destinazione con cui viene eseguita l'autenticazione non rispetta il ticket se confrontato con l'indirizzo IP di origine da cui viene inviato.

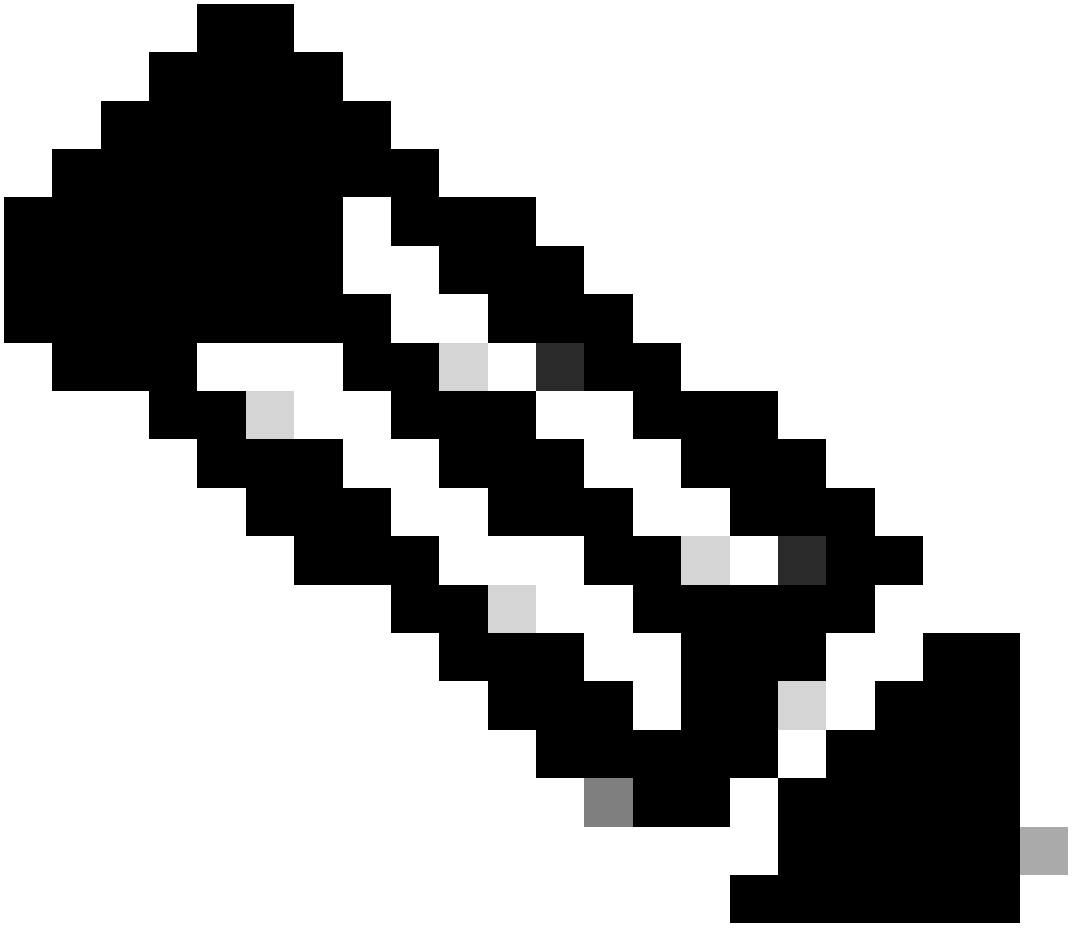
Per risolvere il problema, utilizzare una delle seguenti opzioni:

Opzione 1:

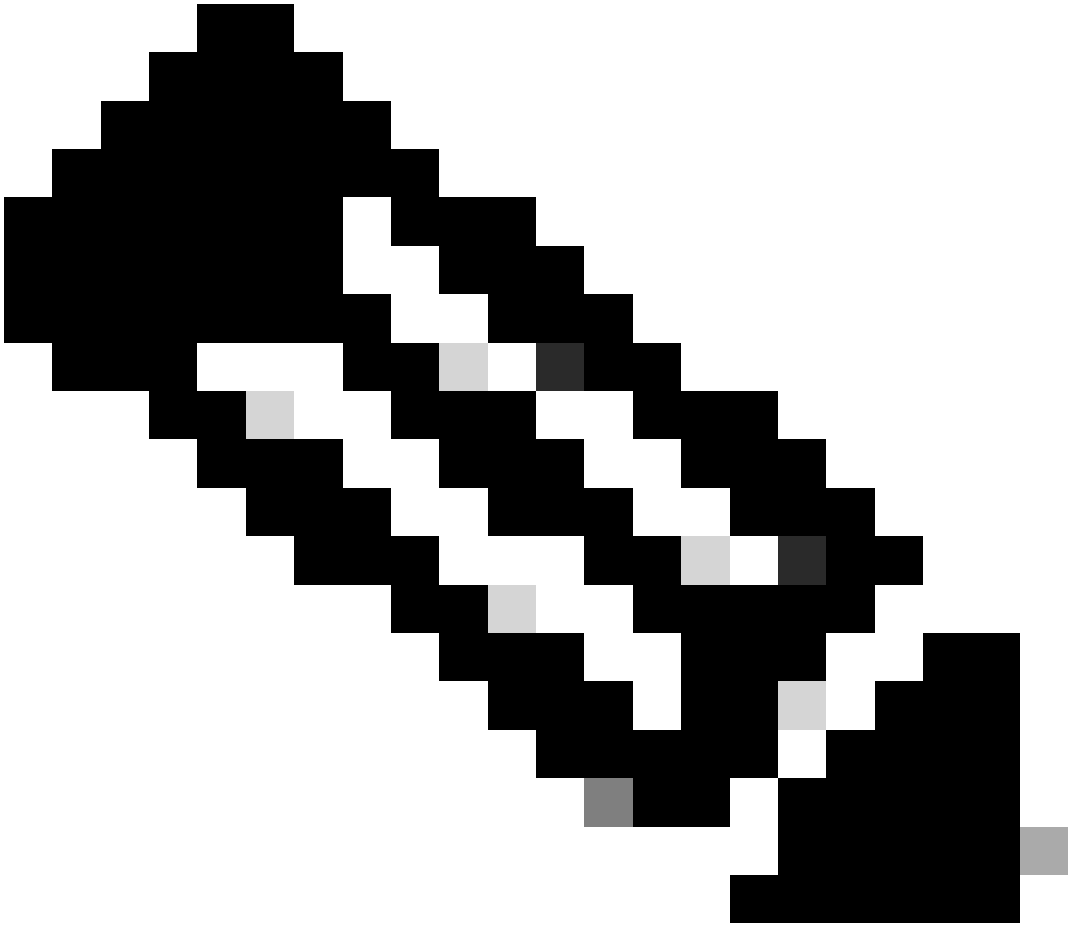
Disabilitare l'opzione per includere l'indirizzo IP di origine nel ticket Kerberos client.

Opzione 2:

Usare la VPN ad accesso sicuro con risorse private dietro il tunnel IPSEC anziché applicazioni private dietro App Connector.



Nota: questo comportamento influisce solo sulle applicazioni private distribuite dietro App Connector e il traffico viene originato dal client con modulo ZTNA senza VPN.



Nota: la ricerca delle attività di accesso sicuro mostra l'azione consentita per la transazione, in quanto il blocco si sta verificando sul lato dell'applicazione privata e non su Secure Access.

Informazioni correlate

- Guida per l'utente di Secure Access
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).