Problemi Di Connettività Client Completa Mediante Accesso Sicuro

Sommario

Problema

Il client completo Omnissa non è in grado di caricare i desktop virtuali quando è connesso tramite Cisco Secure Access. Si verificano errori di connettività durante il tentativo di stabilire connessioni ad ambienti virtuali utilizzando l'applicazione client completa. Tuttavia, l'accesso tramite il client HTML/Web continua a funzionare normalmente, indicando che l'infrastruttura desktop virtuale sottostante è funzionante, ma esiste un problema specifico che influisce sulla piena capacità del client di stabilire connessioni tramite la soluzione Cisco Secure Access.

Ambiente

- Tecnologia: Supporto per la soluzione (SSPT - contratto obbligatorio)
- Sottotecnologia: Cisco Secure Access
- Famiglia di prodotti: SECACS
- Versione del software: Tutte le versioni interessate
- Applicazione client: Client completo Omnissa
- Ambiente desktop virtuale: Desktop virtuali Omnissa
- Infrastruttura di rete: Tunnel IPsec e FTD (Firepower Threat Defense)

Risoluzione

La risoluzione implica l'implementazione di modifiche specifiche alla configurazione della rete per

abilitare il routing corretto per il client completo Omnissa tramite Cisco Secure Access. Per risolvere il problema di connettività, sono state effettuate le seguenti operazioni:

- Configurare le impostazioni dello split-tunnel. Aggiungere configurazioni di split-tunnel per consentire al client completo Omnissa di stabilire connessioni dirette agli host di destinazione richiesti. Questa configurazione garantisce che il traffico destinato a client desktop virtuali specifici venga correttamente instradato attraverso i percorsi di rete appropriati.
- Implementare configurazioni di route statiche. Configurare route statiche per i client specifici che devono stabilire connessioni a desktop virtuali. Il requisito chiave è configurare le route non solo verso il server di aggregazione a valle, ma direttamente verso gli host di destinazione che i client desktop virtuali devono raggiungere.
- Cancella tunnel IPsec. Dopo aver implementato le modifiche alla configurazione, cancellare i tunnel IPsec sulla FTD per assicurare che le nuove configurazioni di routing abbiano effetto correttamente.
- Convalida connettività. Eseguire il test della connettività client completa di Omnissa dopo l'implementazione delle modifiche per verificare che sia possibile stabilire connessioni desktop virtuali tramite Cisco Secure Access.

Pianificazione dell'implementazione

Le modifiche alla configurazione devono essere implementate durante un intervento di manutenzione pianificato per ridurre al minimo l'impatto sugli utenti. Dopo l'implementazione, convalidare sia la raggiungibilità che la connettività client completa di Omnissa per garantire la riuscita della risoluzione.

Causa

Il problema di connettività è stato causato da configurazioni di routing insufficienti nell'ambiente Cisco Secure Access. In particolare, la rete era configurata con route solo verso il server di aggregazione a valle, ma mancava delle necessarie configurazioni di split-tunnel e route statiche per i client specifici a cui il client completo Omnissa doveva stabilire le connessioni. Questa interruzione di routing ha impedito al client completo di raggiungere correttamente gli host desktop virtuali, mentre il client HTML/Web poteva ancora funzionare perché utilizzava percorsi di connessione diversi configurati correttamente.

Contenuto correlato

- Supporto tecnico Cisco e download

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).