Problemi di controllo del traffico ZTNA basato su client con Secure Client

Sommario

Problema

L'accesso ZTNA (Zero Trust Network Access) basato su client non consente l'accesso alle applicazioni interne quando vi si accede tramite FQDN o indirizzo IP diretto, mentre le stesse applicazioni rimangono raggiungibili tramite connessione VPN.

I sintomi specifici osservati includono:

- Secure Client ZTNA non può raggiungere le applicazioni interne tramite FQDN o IP diretto quando la VPN è disconnessa.
- L'accesso ZTNA basato su browser funziona correttamente per le stesse applicazioni.
- Nessun evento ZTNA viene visualizzato nei log attività quando la VPN è inattiva, a indicare che il traffico client non viene instradato attraverso il percorso ZTNA.
- Le definizioni delle app private sono state verificate in modo da corrispondere alle risorse instradabili VPN con le configurazioni IP/porta/FQDN corrette.
- I criteri ZTNA sono stati confermati per corrispondere alle assegnazioni di utenti e gruppi di test.

Il problema riguarda in modo specifico il meccanismo di controllo o imposizione del traffico ZTNA Secure Client, in quanto la ZTNA basata su browser verifica che la pubblicazione e l'imposizione back-end funzionino correttamente.

Ambiente

- Tecnologia: Accesso sicuro - Accesso di rete senza trust (ZTNA)

- Componenti: ZTNA basata su client, postura, registrazione, accesso alle risorse private
- Secure Client con profili VPN coesistenti
- Applicazioni private accessibili tramite FQDN e indirizzamento IP diretto
- Funzionalità ZTNA basata su browser confermata
- Imposizione dei criteri configurata nella modalità di imposizione Corrispondenza più specifica

Risoluzione

La risoluzione ha comportato la modifica della configurazione del profilo ZTA e la convalida dei criteri. Le procedure descritte nelle sezioni seguenti sono state eseguite per ripristinare la funzionalità ZTNA basata su client.

Passaggio 1: Aggiungi risorse private al profilo ZTA

Risorse private aggiunte alla configurazione del profilo ZTA. Dopo questa modifica, gli eventi bloccati hanno iniziato a comparire nei log delle attività e negli screenshot, indicando che il traffico dei client era ora correttamente instradato attraverso il percorso ZTNA.

Passaggio 2: Verifica e collaudo delle policy

È stata aggiunta una regola temporanea "consenti qualsiasi" per convalidare il flusso di traffico. Mentre questa regola era attiva, l'accesso ZTNA basato su client funzionava correttamente, confermando che il meccanismo di gestione del traffico funzionava ma che l'applicazione delle policy richiedeva una modifica.

Passaggio 3: Miglioramento delle policy

La regola di autorizzazione temporanea-any è stata rimossa e i criteri di accesso specifici sono stati convalidati. L'accessibilità della risorsa privata è stata confermata in base ai criteri di accesso denominati Private Ressources_Cyril utilizzando la modalità di imposizione della corrispondenza

più specifica della piattaforma.

Passaggio 4: Convalida configurazione

L'utente ha confermato che l'accesso ZTNA basato su client ha iniziato a funzionare in modo coerente dopo le modifiche alla configurazione. Il problema è stato risolto senza richiedere ulteriori modifiche ai criteri o al sistema.

Causa

La causa principale è una configurazione incompleta delle risorse private nel profilo ZTA. Senza risorse private appropriate definite nel profilo ZTA, il traffico client non veniva indirizzato attraverso il percorso di imposizione ZTNA, causando il fallback ai meccanismi di routing locali. Questo ha portato il traffico a bypassare completamente le policy ZTNA, che ha spiegato perché nessun evento ZTNA è apparso nei log di attività quando VPN è stato disconnesso.

Il problema era specifico della configurazione del controllo del traffico ZTNA basato su client, mentre lo ZTNA basato su browser ha continuato a funzionare perché usa un meccanismo di gestione del traffico diverso che era configurato 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).