Richieste DNS eccessive sulla porta 53 durante le sessioni VPN AnyConnect

Sommario

Problema

Dopo aver implementato la VPN ad accesso remoto (RA-VPN), gli utenti che si connettono tramite Cisco AnyConnect generano dozzine di richieste DNS sulla porta 53 al server DNS secondario. Questo comportamento viene osservato in Monitoraggio attività per tutti gli utenti connessi al tunnel VPN e determina numerose richieste consentite che inondano il tunnel. Questa attività DNS eccessiva non si verifica quando gli utenti si connettono tramite ZTA (Zero Trust Access), indicando che il problema è correlato in modo specifico al metodo di connessione VPN di AnyConnect.

Ambiente

- Famiglia di prodotti: Accesso sicuro
- Implementazione: Distribuzione VPN di Accesso remoto
- Ambiente di confronto: ZTA (Zero Trust Access): comportamento di flooding DNS diverso

Risoluzione

L'analisi delle richieste DNS eccessive richiede la raccolta e l'analisi dei registri per identificare la causa principale del comportamento di flooding DNS. La raccolta di log include la raccolta dell'acquisizione dei pacchetti che include il PID per ogni pacchetto per determinare quale applicazione su un endpoint sta generando il traffico e l'output di Process Monitor.

Causa

L'analisi ha mostrato che è prevista questa quantità di traffico DNS.

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).