

Considerazioni sul comportamento manuale della connessione VPN TND Secure Client e sul blocco degli URL

Sommario

Problema

Quando si utilizza un profilo VPN con la funzionalità TND (Trusted Network Detection) configurata con l'impostazione Rete attendibile impostata su Disconnetti, gli endpoint presenti nella rete attendibile possono comunque stabilire una connessione VPN quando gli utenti avviano manualmente le connessioni utilizzando Cisco Secure Client.

Questo comportamento si verifica nonostante la configurazione TND sia impostata per disconnettere le sessioni VPN quando l'endpoint viene rilevato in una rete attendibile.

Le preoccupazioni specifiche individuate comprendono:

- Le connessioni VPN manuali da endpoint di rete attendibili non possono essere controllate o bloccate tramite la configurazione TND standard
- Non è sicuro che le impostazioni Cisco Secure Access (CSA) possano bloccare le connessioni VPN manuali da endpoint di rete attendibili
- Domande sulla stabilità dell'URL della connessione al profilo VPN (xxxx.vpn.sse.cisco.com) e se cambia periodicamente, il che potrebbe influire sulle strategie di blocco basate sul firewall

Ambiente

- Implementazione di Cisco Secure Access (CSA)
- Cisco Secure Client con configurazione del profilo VPN

- Funzionalità TND (Trusted Network Detection) abilitata
- Impostazione di rete attendibile TND configurata come Disconnetti
- Endpoint posizionati nella rete attendibile configurata
- Infrastruttura firewall per il controllo dell'accesso alla rete

Risoluzione

Comprensione del comportamento TND con le connessioni VPN manuali

Il comportamento osservato è coerente con la funzionalità Cisco Secure Client documentata. In base alla documentazione di Cisco, il TND non disconnette né impedisce una sessione VPN che un utente avvia manualmente su una rete attendibile. Questo è il comportamento previsto indipendentemente dalle impostazioni di configurazione TND.

I principali aspetti tecnici sono:

- La funzionalità di disconnessione automatica TND si applica solo alle connessioni VPN stabilite automaticamente.
- Le connessioni VPN manuali avviate dagli utenti ignorano il comportamento di disconnessione TND.
- Non esiste alcuna impostazione di configurazione CSA per bloccare le connessioni VPN manuali dagli endpoint di rete attendibili.

Strategia di mitigazione operativa

Il metodo principale per controllare le connessioni VPN manuali dagli endpoint di rete attendibili consiste nei controlli a livello di rete:

Passaggio 1: Implementa blocco URL firewall: Configurare il firewall Rete attendibile per bloccare l'accesso all'URL della connessione al profilo VPN (xxxx.vpn.sse.cisco.com). In questo modo si impedisce agli endpoint nella rete attendibile di raggiungere l'endpoint del servizio VPN.

Passaggio 2: Verifica stabilità URL: L'identificativo URL del profilo VPN (la parte xxxx) è specifico del tenant e non deve essere modificato periodicamente. In questo modo viene fornita una destinazione stabile per le regole di blocco del firewall.

Convalida e test

I test hanno confermato che il blocco dell'URL di connessione del profilo VPN nel firewall Rete attendibile impedisce agli endpoint di stabilire connessioni VPN, anche quando gli utenti tentano connessioni manuali tramite Cisco Secure Client.

Causa

Questo comportamento è stato progettato nell'implementazione TND di Cisco Secure Client. La funzione TND è stata appositamente progettata per gestire le connessioni VPN automatiche in base allo stato di attendibilità della rete, ma non interferisce intenzionalmente con le connessioni VPN manuali avviate dall'utente. Questa progettazione consente agli utenti di ignorare il comportamento automatico quando necessario, fornendo comunque il rilevamento automatico della rete e la gestione della connessione per i casi di utilizzo tipici.

Contenuto correlato

- [Guida per l'amministratore di Cisco Secure Client - Configurazione TND](#)
- [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).