# Problematiche di configurazione del tunneling ripartito per l'accesso sicuro

## Sommario

## Problema

Durante la configurazione della funzionalità Cisco Secure Access (TIA) per il traffico dello split-tunnel, sono state riscontrate diverse complicazioni durante il processo di configurazione che hanno impedito la corretta installazione:

- Sfide nell'identificazione del traffico: Quando si configura il TIA per il tunneling suddiviso, tutto il traffico VPN deve essere escluso dall'ispezione della sicurezza Internet. L'identificazione dei flussi di traffico richiesti si è rivelata difficile e alcuni URL di reindirizzamento sono stati particolarmente difficili da tracciare e classificare.
- Vincoli traffico autenticazione: Per alcuni scenari di split-tunnel è necessario escludere il traffico di autenticazione dal proxy. Tuttavia, in base ai criteri esistenti, non è stato possibile ignorare il traffico relativo all'autenticazione dal proxy, con conseguenti conflitti di criteri.
- Rischi per la sicurezza alla disconnessione VPN: Il traffico del tunnel suddiviso viene esposto a Internet aperto quando la VPN si disconnette, creando ulteriori rischi per la sicurezza che devono essere presi in considerazione durante la configurazione.

Durante il processo sono stati inoltre rilevati ulteriori problemi di configurazione che hanno richiesto ulteriori analisi e risoluzione.

## Ambiente

- Famiglia di prodotti: SECACS (Secure Access)
- Tecnologia: Cisco Secure Access (TIA) con funzione di tunneling ripartito
- Configurazione: Scenari di traffico a tunnel diviso con criteri esistenti
- Autenticazione: Gestione del traffico di autenticazione basata su proxy

- Sicurezza della rete: Requisiti di ispezione della sicurezza Internet per il traffico VPN

# Risoluzione

In base alle problematiche di configurazione identificate con il split-tunneling di Cisco Secure Access, è stata inviata una richiesta completa di funzionalità per risolvere le limitazioni e i conflitti di policy identificati.

## Invio richiesta funzionalità

È stata aperta una richiesta di funzionalità (CSE-I-5636) che è stata inviata al team di progettazione per la risoluzione dei problemi di configurazione seguenti:

- Funzionalità avanzate di identificazione del traffico per l'esclusione del traffico VPN dall'ispezione della sicurezza Internet
- Migliore gestione degli URL di reindirizzamento difficili da tracciare e classificare
- Risoluzione dei limiti di bypass del traffico di autenticazione con i criteri esistenti
- Riduzione dei rischi di sicurezza per l'esposizione del traffico del tunnel suddiviso durante la disconnessione della VPN

# Causa

Le problematiche relative alla configurazione derivano dalle limitazioni attuali dell'implementazione del tunneling separato di Cisco Secure Access (TIA) che non risolvono in modo adeguato scenari di implementazione aziendali complessi. In particolare, il sistema non dispone di un controllo granulare sufficiente per l'identificazione e la categorizzazione del traffico, ha limitazioni nell'ignorare il traffico di autenticazione quando sono in atto policy e non fornisce adeguate protezioni di sicurezza per il traffico split-tunnel quando le connessioni VPN vengono interrotte.

# 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).