Configurazione e sincronizzazione client di Cisco Secure Access Traffic Steering

Sommario

Problema

Quando si rivede la configurazione di Cisco Secure Access Traffic Steering, le impostazioni del profilo VPN e i file XML non visualizzano gli indirizzi IP di destinazione o i domini configurati per il controllo della direzione del traffico. Questo crea confusione sul modo in cui il client Secure Access determina le destinazioni del traffico per le decisioni di controllo e sul modo in cui le modifiche alla configurazione apportate nel portale di gestione vengono sincronizzate con il client.

In particolare, gli amministratori osservano che mentre le impostazioni di controllo del traffico sono configurate tramite l'interfaccia di gestione dei profili VPN, i file XML dei profili VPN corrispondenti non contengono voci visibili per gli indirizzi o i domini di destinazione che devono essere soggetti al controllo del controllo del controllo del traffico.

Ambiente

- Soluzione Cisco Secure Access
- Configurazione del profilo VPN con Traffic Steering abilitato
- Distribuzione client Secure Access

Risoluzione

Il Traffic Steering in Cisco Secure Access funziona tramite un meccanismo di consegna delle regole dinamico anziché tramite voci statiche nel codice XML del profilo VPN. Di seguito viene descritto il funzionamento di questo processo e viene spiegato come convalidare la configurazione:

Processo di recapito delle regole di controllo del traffico

Le regole di controllo del traffico non sono archiviate nel file XML del profilo VPN che gli amministratori possono visualizzare. Al contrario, queste regole vengono inviate dinamicamente dall'headend di Secure Access al client durante la connessione VPN. Il processo funziona nel modo seguente:

1. Quando viene stabilita una connessione VPN, l'headend di accesso sicuro invia le regole correnti di Traffic Steering (Split Tunnel) al client che esegue la connessione
2. Il client riceve queste regole e le scrive direttamente nella tabella di routing del client locale
3. Le decisioni relative alla direzione del traffico vengono prese in base alle voci nella tabella di routing del client e non alle informazioni visibili nel file XML del profilo VPN

Sincronizzazione modifiche configurazione

Le modifiche apportate alle impostazioni di Gestione traffico nel portale di gestione seguono un modello di sincronizzazione specifico:

- Le modifiche alla configurazione apportate nel portale di gestione non hanno effetto durante una sessione VPN attiva
- Nuove regole di direzione del traffico vengono applicate alla successiva connessione VPN
- Per convalidare il comportamento dopo aver apportato modifiche alla configurazione del controllo del traffico, è necessario disconnettere e riconnettere la connessione VPN

Passaggi di convalida

Per convalidare le modifiche alla configurazione di Gestione traffico:

1. Apportare le modifiche desiderate alle impostazioni di controllo del traffico nel portale di gestione Secure Access
2. Disconnetti connessione VPN esistente nel client
3. Riconnetti la VPN per ricevere le regole aggiornate di controllo del traffico
4. Esaminare la tabella di routing client per verificare che le nuove regole siano state applicate

Causa

L'apparente assenza di destinazioni Traffic Steering nel codice XML del profilo VPN è di progettazione. Cisco Secure Access utilizza un sistema di recapito delle regole dinamico in cui le regole di controllo del traffico vengono inviate al client al momento della connessione e implementate tramite voci della tabella di routing anziché essere archiviate come elementi di configurazione visibili nel codice XML del profilo. Questa architettura consente aggiornamenti delle policy in tempo reale e il controllo centralizzato, mantenendo al contempo la sicurezza e le prestazioni.

Contenuto correlato

- Guida alla configurazione di ASA split-tunneling
- 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).