

Comportamento di autenticazione SSO di Secure Access per il traffico Web non di browser

Sommario

Problema

Quando si implementa Cisco Secure Access (CSA) con connettività IPsec, è necessario un chiarimento relativo al comportamento dell'autenticazione SSO nei profili di sicurezza. In particolare, è sorta la domanda su quali tipi di traffico Internet in uscita attivano l'autenticazione SSO quando i siti sono connessi tramite tunnel IPsec.

La preoccupazione principale era capire se l'autenticazione SSO si applicasse solo all'accesso Web basato su browser sulle porte TCP 80 e 443 o se si estendesse anche ad applicazioni e dispositivi non basati su browser, come stampanti o endpoint non Windows che generano traffico Web. Il comportamento richiedeva un chiarimento in merito al momento in cui i prompt di autenticazione e i reindirizzamenti ai provider di identità (IdP) si verificavano per diversi tipi di traffico Web provenienti dai siti connessi.

Ambiente

- Implementazione di Cisco Secure Access (CSA)
- Connettività tunnel IPsec tra i siti e CSA
- Profili di sicurezza configurati con l'autenticazione SSO
- Ambiente misto con vari dispositivi, tra cui stampanti ed endpoint non Windows
- Ispezione HTTPS abilitata
- Integrazione SAML configurata

Risoluzione

Il comportamento dell'autenticazione SSO in Cisco Secure Access è progettato in modo specifico per il solo traffico Web basato su browser. Il sistema esegue un sofisticato processo di ispezione per determinare se le richieste Web devono essere soggette all'autenticazione SSO.

Processo di autenticazione SSO

Prima di reindirizzare una richiesta Web a un provider di identità (IdP), Cisco Secure Access utilizza l'ispezione HTTPS per determinare se una richiesta proviene da un browser che supporta i cookie. Questo processo di ispezione è il meccanismo chiave che distingue tra traffico Web basato su browser e traffico Web non basato su browser.

Classificazione traffico

Traffico basato su browser (soggetto all'autenticazione SSO)

- Richieste Web provenienti da browser che supportano i cookie
- Traffico HTTP/HTTPS sulle porte TCP 80 e 443 dalle applicazioni browser
- Traffico che supera il rilevamento cookie/browser di ispezione HTTPS

Traffico non browser (non soggetto all'autenticazione SSO)

- Traffico Web da stampanti e altri dispositivi di rete
- Applicazioni che non supportano i cookie o non sono identificate come browser
- Endpoint non Windows che generano traffico Web che non riescono a rilevare il browser
- Qualsiasi traffico Web che non supera la verifica del browser di ispezione HTTPS

Prerequisiti per l'autenticazione SSO

Affinché l'autenticazione SSO funzioni correttamente nell'ambiente, è necessario che siano soddisfatti diversi prerequisiti:

- È necessario disporre di una configurazione SAML funzionante.
- Reti proxy con XFF e/o tunnel senza NAT (il surrogato IP richiede visibilità sugli IP privati interni).
- È necessario abilitare l'ispezione HTTPS.
- Le sessioni del browser devono mantenere i cookie (non è consigliabile eliminare i cookie alla fine della sessione o esplorare in modo inconsapevole).
- Indirizzi IP non sovrapposti tra più percorsi o separazione corretta dei siti in caso di sovrapposizione.

Causa

Il comportamento è predefinito in Cisco Secure Access. Il meccanismo di autenticazione SSO è specificamente progettato per gestire le sessioni interattive degli utenti tramite browser Web, consentendo ai sistemi automatizzati e ai dispositivi non interattivi di accedere alle risorse Web senza interrompere l'autenticazione. Questa progettazione impedisce l'interruzione dei processi automatizzati, delle interfacce di gestione dei dispositivi e delle applicazioni che non sono in grado di gestire reindirizzamenti di autenticazione o sessioni basate su cookie.

Contenuto correlato

- [Configurare le integrazioni SAML - Abilitare i surrogati IP per SAML](#)
- [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).