Risoluzione dei problemi relativi al surrogato del cookie di autenticazione SAML SWG per l'accesso sicuro

Sommario

Problema

Gli utenti che accedono alle applicazioni Web tramite Cisco Secure Access riscontrano errori di autenticazione quando le applicazioni eseguono reindirizzamenti tra domini o recuperano risorse da più domini correlati. Il problema si manifesta come:

- Impossibile inizializzare correttamente le applicazioni Web dopo l'autenticazione SAML.
- Le richieste alle risorse tra domini (errore CORS) vengono bloccate per impostazione predefinita dalle regole di negazione.
- Registri attività in cui vengono visualizzate le richieste attribuite all'identità della rete o del tunnel anziché all'identità dell'utente autenticato.
- Errori dei criteri CORS visualizzati nella console del browser per le richieste reindirizzate.
- Applicazioni che funzionano correttamente su macchine fisiche quando si utilizza IP surrogate ma che hanno problemi con gli ambienti desktop virtuali Citrix che utilizzano Cookie surrogate.

Il problema si verifica in modo specifico quando si utilizza l'autenticazione surrogata dei cookie in ambienti virtualizzati, dove le richieste reindirizzate perdono la mappatura da utente a cookie durante il recupero di risorse tra domini.

Ambiente

- Cisco Secure Access con autenticazione SAML configurata
- Autenticazione sostitutiva tramite cookie abilitata per gli ambienti desktop virtuali Citrix

- Autenticazione sostitutiva IP utilizzata per i computer fisici
- Applicazioni Web che eseguono reindirizzamenti tra domini (errore CORS nei registri della console dello strumento di sviluppo Web)
- Ambiente misto con infrastruttura desktop fisica e virtuale

Risoluzione

Il problema viene risolto implementando il bypass del surrogato IP per gli intervalli di rete interessati, consentendo una corretta attribuzione dell'identità dell'utente anche durante i reindirizzamenti tra domini.

Passaggio 1: Passa alla configurazione sostitutiva IP

Accedere al dashboard Cisco Secure Access e selezionare Connect > Users and Groups > Configuration Management > Advanced Settings > IP Surrogate (Connetti > Utenti e gruppi > Gestione configurazione > Impostazioni avanzate > Sostituzione IP).

Passaggio 2: Abilita bypass della rete interna

Aggiungere gli intervalli di rete interessati alla configurazione di bypass della rete interna. In questo modo, il sistema è in grado di mantenere l'attribuzione dell'identità degli utenti per le richieste provenienti da queste reti.

Passaggio 3: Verifica accesso applicazione

Dopo aver implementato il surrogato IP, eseguire il test delle applicazioni interessate per verificare che:

- Le richieste di risorse tra domini vengono attribuite correttamente all'identità dell'utente
- Inizializzazione delle applicazioni completata senza errori CORS

- Nei log attività viene visualizzata l'identità dell'utente anziché l'identità basata sulla rete o sul tunnel per tutte le richieste

Passaggio 5: Monitoraggio dei rapporti attività

Utilizzare Monitor > Ricerca attività per verificare che le richieste siano state correttamente attribuite agli utenti autenticati anziché visualizzate come identità basata sulla rete o sul tunnel.

Causa

Questo comportamento è previsto a causa della natura dell'autenticazione SAML combinata con Cookie Surrogato in ambienti virtualizzati. Quando le applicazioni Web eseguono reindirizzamenti tra domini o recuperano risorse da più domini correlati, è possibile che le richieste reindirizzate non includano il cookie sostitutivo in modo che Cisco Secure Access possa associarsi nuovamente alla sessione utente autenticata.

La causa principale si verifica per i motivi seguenti:

- Cookie surrogato si basa sulla propagazione dei cookie del browser tra i reindirizzamenti.
- I criteri di sicurezza tra domini (CORS) possono eliminare i cookie durante gli scenari 307/redirect.
- Le misure di protezione del browser impediscono la condivisione dei cookie tra domini diversi.
- Gli ambienti desktop virtuali gestiscono la propagazione dei cookie in modo diverso rispetto ai computer fisici.

Una volta persa la mappatura utente-cookie, Accesso sicuro non è in grado di risolvere la richiesta all'utente autenticato, causando l'attribuzione della richiesta solo alla rete registrata/identità diversa come origine e successivamente bloccata dalle regole di negazione predefinite.

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).