Risoluzione dei problemi relativi all'autenticazione SAML basata su Secure Access Browser Visualizzazione di una schermata bianca vuota con EntraID

Sommario

Problema

Quando si configura Cisco Secure Access per imporre l'autenticazione SAML basata su browser su dispositivi senza Cisco Secure Client installato, il processo di autenticazione viene reindirizzato a una schermata bianca vuota anziché visualizzare la pagina di autenticazione EntraID. Questo problema si verifica specificamente nei browser Microsoft Edge in modalità normale (non InPrivate) e Google Chrome. L'autenticazione funziona correttamente quando si utilizza Edge InPrivate. Per il profilo di autenticazione SAML sono abilitate sia la decrittografia che l'autenticazione SSO.

La struttura dei criteri configurata include:

- Consenti criteri per utenti post-autenticazione. (fonte: qualsiasi utente, destinazione: qualsiasi)
- Consenti criterio di autenticazione SAML con profilo di autenticazione SAML. (fonte: IP endpoint, destinazione: 0.0.0.0 TCP (80.443)
- Consenti criterio helper di autenticazione SAML con profilo di autenticazione SAML. (fonte: IP endpoint, destinazione: qualsiasi)
- Blocca criteri. (fonte: IP endpoint, destinazione: qualsiasi)

Ambiente

- Cisco Secure Access (modulo Internet Access)

- EntraID come provider di identità (IdP)
- Autenticazione SAML basata su browser per dispositivi senza Cisco Secure Client
- Profilo di autenticazione SAML con decrittografia e autenticazione SSO abilitate
- Browser Microsoft Edge e Google Chrome

Risoluzione

Il problema viene risolto aggiungendo specifici domini correlati a EntraID all'elenco di esclusione della decrittografia nella configurazione del profilo di autenticazione SAML. In questo modo si evita che il processo di decrittografia SSL/TLS interferisca con il flusso di autenticazione EntraID.

Passaggio 1: Aggiungi domini EntraID all'elenco di esclusione della decrittografia

Configurare i quattro domini EntraID seguenti nell'elenco di esclusione della decrittografia per il profilo di autenticazione SAML:

```
login.live.com
login.microsoftonline.com
msauth.net
msftauth.net
```

Passaggio 2: Applica configurazione ai criteri SAML

Verificare che le impostazioni di esclusione della decrittografia siano applicate a entrambi:

- Criterio di autenticazione Consenti SAML. (fonte: IP endpoint, destinazione: 0.0.0.0 TCP (80.443)
- Criterio dell'helper Consenti autenticazione SAML. (fonte: IP endpoint, destinazione: qualsiasi)

Passaggio 3: Verifica risoluzione

Dopo aver applicato la configurazione di esclusione della decrittografia, verificare il flusso di autenticazione:

- Microsoft Edge (modalità normale): Reindirizzamento alla pagina di autenticazione EntraID riuscito.
- Google Chrome: Reindirizzamento alla pagina di autenticazione EntraID riuscito.
- Entrambi i browser possono visualizzare in modo coerente la schermata di input dell'autenticazione EntraID.

Causa

La schermata vuota è visualizzata quando il processo di decrittografia SSL/TLS in Cisco Secure Access interferisce con il flusso di autenticazione EntraID quando la decrittografia è abilitata per il profilo di autenticazione SAML. Il processo di decrittografia interrompe la comunicazione protetta tra il browser e i server di autenticazione EntraID, impedendo il corretto caricamento della pagina di autenticazione. La modalità InPrivate funziona in quanto gestisce le sessioni SSL/TLS in modo diverso, ignorando l'interferenza della decrittografia. L'aggiunta dei domini EntraID all'elenco di esclusione della decrittografia consente il passaggio del traffico di autenticazione senza decrittografia, mantenendo l'integrità del flusso di autenticazione sicuro.

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).