Autenticazione SSO Cisco Secure Access con Duo IdP per il traffico SWG del client mobile

Sommario

Problema

Quando si tenta di utilizzare l'autenticazione SSO con un Duo IdP per il traffico SWG (Secure Web Gateway) di accesso sicuro proveniente da un client in roaming, agli utenti non viene richiesta l'autenticazione Duo SSO e l'identità dell'utente non viene popolata nel dashboard di accesso sicuro. Sebbene il traffico Web corrisponda alla regola SWG desiderata con l'autenticazione abilitata e il traffico venga decrittografato, il flusso di autenticazione non viene avviato per il traffico client mobile, impedendo l'identificazione dell'attività Web a livello utente.

In particolare, è stato osservato il seguente comportamento:

- L'attività e la registrazione SWG hanno mostrato che il traffico corrispondeva alla regola SWG desiderata e che il traffico di destinazione è stato decriptato
- I registri e la visualizzazione attività Accesso sicuro mostrano solo l'identità del PC e l'identità della rete; non è stata osservata nessuna richiesta di verifica dell'autenticazione Duo/SAML, reindirizzamento SSO o prompt interattivo
- Le voci dei criteri riportavano solo le informazioni sul roaming e sull'origine; nessuna identità utente presente prima dell'aggiunta ad AD
- Quando la VM di test è stata aggiunta ad Active Directory durante la risoluzione dei problemi, l'identità dell'utente è diventata visibile in Ricerca attività accesso sicuro, ma il prompt interattivo Duo/SAML non si è ancora verificato

Ambiente

- Cisco Secure Access con funzionalità SWG
- Secure Client versione 5.1.13.17
- Duo IdP configurato per l'autenticazione SSO
- Sottoscrizione organizzazione: Secure Access Essentials
- Intervallo di riautenticazione proxy Web impostato su Giornaliero

- Nessun file PAC o VPN in uso durante i test
- Test dell'ambiente con la configurazione del computer mobile

Risoluzione

Dopo un'analisi e un test approfonditi, è stato determinato che l'autenticazione SSO tramite SAML non è supportata per il traffico client in roaming di Secure Access a causa di limitazioni nella progettazione del prodotto. Per confermare questa limitazione, sono state eseguite le seguenti operazioni di risoluzione dei problemi:

Passaggio 1: Risoluzione dei problemi e riproduzione dei comportamenti in tempo reale

Il test ha confermato che la corrispondenza dei criteri SWG e la decrittografia SSL sono state eseguite correttamente, ma il flusso di autenticazione (reindirizzamento e richiesta SSO SAML/Duo interattivi) non è stato avviato per il traffico client mobile.

Passaggio 2: Modifiche a regole e origini

L'origine della regola SWG è stata modificata da nome computer comune a identità utente specifica durante i tentativi di riesecuzione. I servizi Secure Client sono stati riavviati ed è stata osservata la propagazione dei criteri. Queste modifiche non hanno risolto il problema del flusso di autenticazione.

Passaggio 3: Test di aggiunta ad Active Directory

La macchina virtuale di test è stata aggiunta ad Active Directory per determinare l'effetto sulla visibilità dell'identità utente. Anche se questo ha reso visibile l'identità dell'utente in Secure Access Activity Search, il prompt interattivo Duo/SAML non si è ancora verificato, confermando che il problema non era correlato alla sola visibilità dell'identità dell'utente.

Passaggio 4: Analisi bundle DART

È stato raccolto e analizzato un pacchetto DART. L'analisi ha confermato l'applicazione della policy SWG, ma non ha mostrato alcuna inizializzazione del flusso di autenticazione per il traffico dei client in roaming, confermando la conclusione che questo comportamento è di progettazione.

Passaggio 5: Convalida configurazione Duo IdP

Sono stati eseguiti test indipendenti della configurazione e dei metadati del Duo IdP, che hanno confermato che la configurazione Duo non è all'origine del problema.

Passaggio 6: Convalida interna

L'autenticazione SSO tramite SAML non è supportata per il traffico client in roaming di Secure Access come limitazione della progettazione del prodotto.

Conclusione: Nessuna configurazione errata rilevata nell'installazione. La mancanza di istruzioni SSO interattive è stata attribuita a una limitazione esplicita del supporto del prodotto piuttosto che a un problema di configurazione risolvibile.

Causa

Il problema è causato da una limitazione della progettazione del prodotto in cui l'autenticazione SSO tramite SAML (inclusa l'integrazione con Duo IdP) non è supportata per il traffico client in roaming Secure Access. Si tratta di una limitazione inerente all'architettura corrente della piattaforma Secure Access e non è correlata a problemi di configurazione o bug software.

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).