Cisco Secure Access SSO-Authentifizierung mit Duo IDp für Roaming-Client-SWG-Datenverkehr

Inhalt

Problem

Wenn Sie versuchen, SSO-Authentifizierung mit einer Duo-ID für SWG-Datenverkehr (Secure Web Gateway) von einem Roaming-Client zu verwenden, werden die Benutzer nicht zur Duo-SSO-Authentifizierung aufgefordert, und die Benutzeridentität wird nicht in das Dashboard für sicheren Zugriff übernommen. Obwohl der Web-Datenverkehr mit aktivierter Authentifizierung der beabsichtigten SWG-Regel entspricht und der Datenverkehr entschlüsselt wird, initiiert der Authentifizierungsfluss keinen Roaming-Client-Datenverkehr, wodurch eine Identifizierung der Web-Aktivität auf Benutzerebene verhindert wird.

Konkret wurde folgendes Verhalten beobachtet:

- Bei der SWG-Protokollierung und -Aktivität wurde festgestellt, dass der Datenverkehr der beabsichtigten SWG-Regel entsprach und der Zieldatenverkehr entschlüsselt wurde.
- Protokolle und die Aktivitätsanzeige für sicheren Zugriff zeigten nur die PC-Identität und die Netzwerkidentität an. Es wurde kein Duo/SAML-Authentifizierungsproblem, keine SSO-Umleitung oder interaktive Eingabeaufforderung beobachtet.
- Die Richtlinieneinträge enthielten nur Roaming- und Herkunftsangaben; Keine Benutzeridentität vor AD-Beitritt vorhanden
- Als die Test-VM während der Fehlerbehebung mit Active Directory verbunden wurde, wurde die Benutzeridentität in Secure Access Activity Search angezeigt, die interaktive Duo/SAML-Eingabeaufforderung trat jedoch immer noch nicht auf

Umwelt

- Cisco Secure Access mit SWG-Funktion
- Secure Client Version 5.1.13.177
- Duo IdP für SSO-Authentifizierung konfiguriert
- Organisationsabonnement: Grundlagen von Secure Access

- Erneute Authentifizierung des Webproxyintervalls auf "Daily" (Täglich) eingestellt
- Während der Tests wird keine PAC-Datei oder kein VPN verwendet.
- Testumgebung mit Roaming-Computerkonfiguration

Auflösung

Nach umfassenden Analysen und Tests wurde festgestellt, dass die SSO-Authentifizierung mithilfe von SAML für den Roaming-Client-Datenverkehr mit sicherem Zugriff aufgrund von Einschränkungen beim Produktdesign nicht unterstützt wird. Die folgenden Schritte zur Fehlerbehebung wurden durchgeführt, um diese Einschränkung zu bestätigen:

Schritt 1: Live-Fehlerbehebung und verhaltensbasierte Wiedergabe

Die Tests bestätigten, dass der SWG-Richtlinienabgleich und die SSL-Entschlüsselung ordnungsgemäß durchgeführt wurden, der Authentifizierungsfluss (interaktive SAML/Duo SSO-Umleitung und Herausforderung) jedoch nicht für den Roaming-Client-Datenverkehr initiiert wurde.

Phase 2: Regel- und Quellcodeänderungen

Die Quelle der SWG-Regel wurde während der Wiederholungsversuche vom Roaming-Computernamen in eine bestimmte Benutzeridentität geändert. Die Secure Client-Dienste wurden neu gestartet, und es wurde eine Richtlinienpropagierung beobachtet. Das Problem mit dem Authentifizierungsfluss konnte durch diese Änderungen nicht behoben werden.

Schritt 3: Active Directory-Zugangstests

Die Test-VM wurde mit Active Directory verbunden, um die Auswirkung auf die Transparenz der Benutzeridentität zu ermitteln. Dadurch wurde die Benutzeridentität bei der Suche nach Aktivitäten für sicheren Zugriff sichtbar, die interaktive Duo/SAML-Eingabeaufforderung trat jedoch immer noch nicht auf, und es wurde bestätigt, dass das Problem nicht allein mit der Sichtbarkeit der Benutzeridentität zusammenhängt.

Schritt 4: DART-Paketanalyse

Ein DART-Paket wurde erfasst und analysiert. Die Analyse bestätigte die SWG-Richtlinienanwendung, zeigte jedoch keine Initiierung des Authentifizierungsflusses für den Roaming-Client-Datenverkehr und stützte die Schlussfolgerung, dass dieses Verhalten vom

Design her zutrifft.

Schritt 5: Validierung der Duo IDp-Konfiguration

Unabhängige Tests der Duo IdP-Metadaten und -Konfiguration wurden durchgeführt und erfolgreich abgeschlossen. Dabei wurde bestätigt, dass die Duo-Konfiguration selbst nicht die Ursache des Problems war.

Schritt 6: Interne Validierung

SSO-Authentifizierung mithilfe von SAML wird für Roaming-Client-Datenverkehr mit sicherem Zugriff als Einschränkung des Produktdesigns nicht unterstützt.

Fazit: Im Setup wurde kein Konfigurationsfehler gefunden. Das Fehlen interaktiver SSO-Eingabeaufforderungen wurde auf eine explizite Einschränkung des Produktsupports zurückgeführt und nicht auf ein behebbares Konfigurationsproblem.

Ursache

Das Problem wird durch eine Einschränkung des Produktdesigns verursacht, bei der die SSO-Authentifizierung mithilfe von SAML (einschließlich Duo IdP-Integration) für den Roaming-Client-Verkehr mit sicherem Zugriff nicht unterstützt wird. Dies stellt eine inhärente Einschränkung der aktuellen Secure Access-Plattformarchitektur dar und hat nichts mit Konfigurationsproblemen oder Softwarefehlern zu tun.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.