

SSO-Authentifizierungsverhalten bei sicherem Zugriff für Nicht-Browser-Web-Datenverkehr

Inhalt

Problem

Bei der Implementierung von Cisco Secure Access (CSA) mit IPsec-Verbindungen bestand Klärungsbedarf hinsichtlich des SSO-Authentifizierungsverhaltens in Sicherheitsprofilen. Insbesondere stellte sich die Frage, welche Arten von ausgehendem Internetverkehr SSO-Authentifizierung auslösen, wenn Standorte über IPsec-Tunnel verbunden sind.

Die Hauptsorge bestand darin, zu verstehen, ob die SSO-Authentifizierung nur für den browserbasierten Webzugriff über die TCP-Ports 80 und 443 gilt oder ob sie sich auch auf nicht-browserbasierte Anwendungen und Geräte wie Drucker oder Endgeräte außerhalb von Windows erstreckt, die Webdatenverkehr generieren. Das Verhalten musste geklärt werden, wann Authentifizierungsansagen und -umleitungen an Identity Provider (IdP) für verschiedene Arten von Web-Datenverkehr erfolgen, der von den verbundenen Websites ausgeht.

Umwelt

- Cisco Secure Access (CSA)-Bereitstellung
- IPsec-Tunnelverbindung zwischen Standorten und CSA
- Mit SSO-Authentifizierung konfigurierte Sicherheitsprofile
- Gemischte Umgebung mit verschiedenen Geräten, einschließlich Druckern und Nicht-Windows-Endgeräten
- HTTPS-Prüfung aktiviert
- SAML-Integration konfiguriert

Auflösung

Das SSO-Authentifizierungsverhalten in Cisco Secure Access wurde speziell dafür entwickelt, nur auf browserbasierten Web-Datenverkehr auszurichten. Das System führt einen ausgeklügelten Prüfprozess durch, um zu bestimmen, ob Web-Anfragen einer SSO-Authentifizierung unterliegen müssen.

SSO-Authentifizierungsprozess

Bevor eine Webanforderung an einen Identitätsanbieter (IdP) umgeleitet wird, verwendet Cisco Secure Access die HTTPS-Überprüfung, um zu ermitteln, ob eine Anforderung von einem Browser stammt, der Cookies unterstützt. Bei diesem Prüfprozess wird zwischen browserbasiertem und nicht-browserbasiertem Web-Datenverkehr unterschieden.

Klassifizierung des Datenverkehrs

Browserbasierter Datenverkehr (abhängig von SSO-Authentifizierung)

- Webanfragen von Browsern, die Cookies unterstützen
- HTTP-/HTTPS-Datenverkehr über die TCP-Ports 80 und 443 von Browseranwendungen
- Datenverkehr, der das HTTPS-Überprüfungscookie/die Browsererkennung besteht

Datenverkehr, der nicht über den Browser läuft (unterliegt nicht der SSO-Authentifizierung)

- Webdatenverkehr von Druckern und anderen Netzwerkgeräten
- Anwendungen, die keine Cookies unterstützen oder nicht als Browser identifiziert werden
- Nicht-Windows-Endgeräte generieren Webdatenverkehr, der nicht vom Browser erkannt wird

- Webdatenverkehr, der die HTTPS-Prüfung des Prüfungsbrowsers nicht besteht

Voraussetzungen für die SSO-Authentifizierung

Damit die SSO-Authentifizierung in der Umgebung ordnungsgemäß funktioniert, müssen mehrere Voraussetzungen erfüllt sein:

- Die SAML-Konfiguration muss funktionsfähig sein.
- Proxy-Netzwerke mit XFF und/oder Tunnel ohne NAT (IP-Surrogat benötigt Transparenz für interne private IPs).
- HTTPS-Inspektion muss aktiviert sein.
- In Browser-Sitzungen müssen Cookies gespeichert werden (das Löschen von Cookies am Sitzungsende oder das Anonymisieren von Browsern wird nicht empfohlen).
- Nicht überlappende IP-Adressen an mehreren Standorten oder korrekte Standorttrennung bei Überschneidungen

Ursache

Das Verhalten ist in Cisco Secure Access festgelegt. Der SSO-Authentifizierungsmechanismus wurde speziell dafür entwickelt, interaktive Benutzersitzungen über Webbrowser zu steuern und gleichzeitig automatisierten Systemen und nicht interaktiven Geräten den unterbrechungsfreien Zugriff auf Webressourcen zu ermöglichen. Dieses Design verhindert Unterbrechungen von automatisierten Prozessen, Geräteverwaltungsschnittstellen und Anwendungen, die keine Authentifizierungsumleitungen oder Cookie-basierten Sitzungen verarbeiten können.

Verwandte Inhalte

- [Konfigurieren von SAML-Integrationen - Aktivieren von IP-Surrogaten für SAML](#)
- [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.