Secure Access SSO Authentication Behavior for Non-Browser Web Traffic

Contents

Issue

When implementing Cisco Secure Access (CSA) with IPsec connectivity, there was a need for clarification regarding the SSO Authentication behavior in Security Profiles. Specifically, the question arose about which types of outbound internet traffic trigger SSO authentication when sites are connected via IPsec tunnels.

The primary concern was understanding whether SSO authentication applies only to browser-based web access over TCP ports 80 and 443, or if it also extends to non-browser applications and devices such as printers or non-Windows endpoints that generate web traffic. The behavior needed clarification regarding when authentication prompts and redirects to Identity Providers (IdP) would occur for different types of web traffic originating from the connected sites.

Environment

- Cisco Secure Access (CSA) deployment
- IPsec tunnel connectivity between sites and CSA
- Security Profiles configured with SSO Authentication
- Mixed environment with various devices including printers and non-Windows endpoints
- HTTPS inspection enabled
- SAML integration configured

Resolution

The SSO authentication behavior in Cisco Secure Access is specifically designed to target browser-based web traffic only. The system performs a sophisticated inspection process to determine whether web requests must be subject to SSO authentication.

SSO Authentication Process

Before redirecting a web request to an Identity Provider (IdP), Cisco Secure Access uses HTTPS inspection to determine if a request originates from a browser that supports cookies. This inspection process is the key mechanism that differentiates between browser-based and non-browser web traffic.

Traffic Classification

Browser-Based Traffic (Subject to SSO Authentication)

- Web requests originating from browsers that support cookies
- HTTP/HTTPS traffic on TCP ports 80 and 443 from browser applications
- Traffic that passes the HTTPS inspection cookie/browser detection

Non-Browser Traffic (Not Subject to SSO Authentication)

- Web traffic from printers and other network devices
- Applications that do not support cookies or are not identified as browsers
- Non-Windows endpoints generating web traffic that fail the browser detection
- Any web traffic that does not pass the HTTPS inspection browser verification

Prerequisites for SSO Authentication

For SSO authentication to function properly in the environment, several prerequisites must be met:

- Working SAML configuration must be in place.
- Proxy networks with XFF and/or tunnels without NAT (IP surrogate needs visibility to internal private IPs).
- HTTPS inspection must be enabled.

- Browser sessions must maintain cookies (deleting cookies at session end or incognito browsing is not recommended).
- Non-overlapping IP addresses across locations, or proper site separation if overlapping exists.

Cause

The behavior is by design in Cisco Secure Access. The SSO authentication mechanism is specifically engineered to target interactive user sessions through web browsers while allowing automated systems and non-interactive devices to access web resources without authentication interruption. This design prevents disruption to automated processes, device management interfaces, and applications that cannot handle authentication redirects or cookie-based sessions.

Related Content

- Configure SAML Integrations - Enable IP Surrogates for SAML
- Cisco Technical Support & Downloads