Beveiligde toegang tot SSO-verificatiegedrag voor webverkeer buiten de browser

Inhoud

uitgeven

Bij de implementatie van Cisco Secure Access (CSA) met IPsec-connectiviteit was er behoefte aan verduidelijking met betrekking tot het SSO-verificatiegedrag in beveiligingsprofielen. Concreet ontstond de vraag welke soorten uitgaand internetverkeer SSO-verificatie activeren wanneer sites via IPsec-tunnels worden verbonden.

De primaire zorg was om te begrijpen of SSO-verificatie alleen van toepassing is op browsergebaseerde webtoegang via TCP-poorten 80 en 443, of dat het zich ook uitstrekt tot niet-browsertoepassingen en apparaten zoals printers of niet-Windows-eindpunten die webverkeer genereren. Het gedrag dat moet worden verduidelijkt met betrekking tot wanneer authenticatieverzoeken en omleidingen naar Identity Providers (IdP) zouden plaatsvinden voor verschillende soorten webverkeer afkomstig van de verbonden sites.

milieu

- Cisco Secure Access (CSA)-implementatie
- IPsec-tunnelconnectiviteit tussen locaties en CSA
- Beveiligingsprofielen geconfigureerd met SSO-verificatie
- Gemengde omgeving met verschillende apparaten, waaronder printers en niet-Windows-eindpunten
- HTTPS-inspectie ingeschakeld
- SAML-integratie geconfigureerd

resolutie

Het SSO-verificatiegedrag in Cisco Secure Access is specifiek ontworpen om alleen webverkeer op basis van een browser te targeten. Het systeem voert een geavanceerd inspectieproces uit om te bepalen of webverzoeken moeten worden onderworpen aan SSO-verificatie.

SSO-verificatieproces

Voordat een webverzoek wordt doorgestuurd naar een Identity Provider (IdP), gebruikt Cisco Secure Access HTTPS-inspectie om te bepalen of een verzoek afkomstig is van een browser die cookies ondersteunt. Dit inspectieproces is het belangrijkste mechanisme dat onderscheid maakt tussen browsergebaseerd en niet-browserwebverkeer.

verkeersclassificatie

Browsergebaseerd verkeer (afhankelijk van SSO-verificatie)

- Webverzoeken afkomstig van browsers die cookies ondersteunen
- HTTP/HTTPS-verkeer op TCP-poorten 80 en 443 vanuit browsertoepassingen
- Verkeer dat de HTTPS-inspectiecookie/browserdetectie passeert

Niet-browserverkeer (niet onderworpen aan SSO-verificatie)

- Webverkeer van printers en andere netwerkapparaten
- Toepassingen die geen cookies ondersteunen of niet als browsers worden geïdentificeerd
- Niet-Windows-eindpunten die webverkeer genereren dat niet wordt gedetecteerd door de browser

- Elk webverkeer dat de HTTPS-browserverificatie niet doorstaat

Vereisten voor SSO-verificatie

Om SSO-authenticatie goed te laten functioneren in de omgeving, moet aan verschillende voorwaarden worden voldaan:

- De werkende SAML-configuratie moet aanwezig zijn.
- Proxynetwerken met XFF en/of tunnels zonder NAT (IP-surrogaat moet zichtbaar zijn voor interne privé-IP's).
- HTTPS-inspectie moet zijn ingeschakeld.
- Browsersessies moeten cookies onderhouden (het verwijderen van cookies aan het einde van de sessie of incognito browsen wordt niet aanbevolen).
- Niet-overlappende IP-adressen op verschillende locaties, of de juiste sitescheiding als er sprake is van overlapping.

Oorzaak

Het gedrag is ontworpen in Cisco Secure Access. Het SSO-authenticatiemechanisme is specifiek ontworpen om interactieve gebruikerssessies via webbrowsers te targeten en tegelijkertijd geautomatiseerde systemen en niet-interactieve apparaten toegang te geven tot webbronnen zonder authenticatieonderbreking. Dit ontwerp voorkomt verstoring van geautomatiseerde processen, interfaces voor apparaatbeheer en toepassingen die geen authenticatieomleidingen of op cookies gebaseerde sessies kunnen verwerken.

Verwante inhoud

- SAML-integraties configureren - IP-surrogaten inschakelen voor SAML
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.