Per-User Identification and Policy Enforcement Challenges in Secure Web Gateway (SWG) for Shared-Computer Environments with SAML Authentication and PAC-Based Traffic Forwarding

Contents

Issue

In Cisco Secure Web Gateway (SWG) deployments utilizing Secure Access with SAML authentication and PAC-based or Branch to Internet traffic forwarding, only the first user logged into a shared computer is correctly identifie user identification and policy enforcement in shared-computer environments and how to ensure correct user mapping.

Environment

- Virtual Appliance for DNS resolution.
- SAML authentication for user identity.
- Mix of traffic forwarding with PAC and without PAC files.
- IP surrogate option enabled, with specific subnets and hosts bypassed for cookie surrogate.
- On-Prem devices; no remote endpoints or users.

Resolution

The issue was resolved by user education and configuration guidance with these points in mind:

- Use Cookie Surrogate identification with PAC files. The traffic can route into or out of a network tunnel.
- Use Cookie Surrogate identification without PAC files, but the traffic has to route through a network tunnel.
- The access policy that you wish to enforce cookie surrogate must have SAML authentication enabled in the se
- Cookie surrogate traffic is for browser-based traffic only. A separate rule is needed to identify non-cookie traffic from the machine (for example, Teams or Webex traffic) with the source identity as the network
- The SWG module must not in-use for cookie surrogate to work.
- When IP surrogate is also enabled, you must add the private IP addresses/subnets that intend to use cookie sur Configuration Management - Advanced Settings).
- The bypass list for cookie surrogate also matches shorter prefixes. For example, if you add 10.10.10.0/24 into
- The cookie surrogate supports user switching from a machine without having to log out to retain multiple iden

A lot of the troubleshooting has been policy testing and activity search.

Cause

The root cause of incorrect user identification in shared-computer environments is primarily due to user education.

Related Content

- Cisco Technical Support & Downloads