Secure Access Split-Tunneling Configuration Challenges

Contents

Issue

While configuring Cisco Secure Access (TIA) feature for split-tunnel traffic, multiple complications were encountered during the configuration process that prevented proper deployment:

- Traffic identification challenges: When configuring TIA for split tunneling, all VPN traffic needs to be excluded from Internet security inspection. Identifying the required traffic flows proved difficult, and some redirect URLs were particularly challenging to track and categorize.
- Authentication traffic constraints: Certain split-tunnel scenarios required authentication traffic to be excluded from the proxy. However, based on existing policies, authentication-related traffic could not be bypassed from the proxy, leading to policy conflicts.
- Security risks on VPN disconnect: Split-tunnel traffic becomes exposed to the open internet when the VPN disconnects, resulting in additional security risks that needed to be considered during configuration.

Additional configuration issues were also observed during the process that required further analysis and resolution.

Environment

- Product Family: SECACCS (Secure Access)
- Technology: Cisco Secure Access (TIA) with split-tunneling feature
- Configuration: Split-tunnel traffic scenarios with existing policies
- Authentication: Proxy-based authentication traffic handling
- Network security: Internet security inspection requirements for VPN traffic

Resolution

Based on the configuration challenges identified with Cisco Secure Access split-tunneling, a comprehensive feature request was submitted to address the identified limitations and policy conflicts.

Feature Request Submission

A feature request (CSE-I-5636) has been opened and submitted for review by the relevant engineering team to address these configuration challenges:

- Enhanced traffic identification capabilities for VPN traffic exclusion from Internet security inspection
- Improved handling of redirect URLs that are difficult to track and categorize
- Resolution of authentication traffic bypass limitations with existing policies
- Security risk mitigation for split-tunnel traffic exposure during VPN disconnection

Cause

The configuration challenges stem from current limitations in the Cisco Secure Access (TIA) split-tunneling implementation that do not adequately address complex enterprise deployment scenarios. Specifically, the system lacks sufficient granular control for traffic identification and categorization, has constraints in bypassing authentication traffic when policies are in place, and does not provide adequate security safeguards for split-tunnel traffic when VPN connections are interrupted.

Related Content

- Cisco Technical Support & Downloads