Cisco Secure Access Traffic Steering Configuration and Client Synchronization

Contents

Issue

When reviewing Cisco Secure Access Traffic Steering configuration, the VPN profile settings and XML files do not display destination IP addresses or domains that are configured for traffic steering control. This creates confusion about how the Secure Access client determines traffic destinations for steering decisions and how configuration changes made in the management portal are synchronized to the client.

Specifically, administrators observe that while Traffic Steering settings are configured through the VPN profile management interface, the corresponding VPN profile XML files do not contain visible entries for the destination addresses or domains that should be subject to traffic steering control.

Environment

- Cisco Secure Access solution
- VPN profile configuration with Traffic Steering enabled
- Secure Access client deployment

Resolution

Traffic Steering in Cisco Secure Access operates through a dynamic rule delivery mechanism rather than static entries in the VPN profile XML. The following explains how this process works and how to validate the configuration:

Traffic Steering Rule Delivery Process

Traffic Steering rules are not stored in the VPN profile XML file that administrators can view. Instead, these

rules are dynamically pushed from the Secure Access head-end to the client during VPN connection establishment. The process works as follows:

1. When a VPN connection is established, the Secure Access head-end pushes the current Traffic Steering (Split Tunnel) rules to the connecting client
2. The client receives these rules and writes them directly into the local client routing table
3. Traffic steering decisions are made based on the entries in the client routing table, not from information visible in the VPN profile XML

Configuration Change Synchronization

Changes made to Traffic Steering settings in the management portal follow a specific synchronization pattern:

- Configuration changes made in the management portal do not take effect during an active VPN session
- New Traffic Steering rules are applied at the next VPN connection establishment
- To validate behavior after making Traffic Steering configuration changes, the VPN connection must be disconnected and reconnected

Validation Steps

To validate Traffic Steering configuration changes:

1. Make the desired changes to Traffic Steering settings in the Secure Access management portal
2. Disconnect the existing VPN connection on the client
3. Reconnect the VPN to receive the updated Traffic Steering rules
4. Examine the client routing table to verify that the new rules have been applied

Cause

The apparent absence of Traffic Steering destinations in the VPN profile XML is by design. Cisco Secure Access uses a dynamic rule delivery system where Traffic Steering rules are pushed to the client at connection time and implemented through routing table entries rather than being stored as visible configuration elements in the profile XML. This architecture allows for real-time policy updates and centralized control while maintaining security and performance.

Related Content

- ASA split-tunneling configuration guide
- Cisco Technical Support & Downloads