Cisco Secure Access RAVPN Protocol Behavior with TLS/DTLS and IPsec(IKEv2) Dual Configuration

Contents

Issue

When both TLS/DTLS and IPsec(IKEv2) protocols are enabled in Cisco Secure Access RAVPN with Primary protocol set to IPsec(IKEv2), connection failures occur when attempting to establish VPN connectivity from networks where IPsec traffic (UDP ports 500/4500) is blocked. The Secure Client defaults to the IPsec option in the client UI dropdown and does not automatically failover to TLS/DTLS when IPsec connectivity fails, resulting in connection errors and inability to establish RAVPN connectivity from restricted network environments.

Environment

- Cisco Secure Access RAVPN with dual protocol configuration
- TLS/DTLS and IPsec(IKEv2) protocols both enabled
- Primary protocol setting configured as IPsec(IKEv2)
- Secure Client with protocol selection dropdown containing separate IPsec and TLS options
- Network environment blocking IPsec traffic on UDP ports 500 and 4500

Resolution

The observed behavior is expected and by design. Cisco Secure Access RAVPN does not perform automatic protocol failover from IPsec(IKEv2) to TLS/DTLS when both protocols are enabled and the primary protocol encounters connectivity issues.

Manual Protocol Selection Required

When connecting from networks that block IPsec traffic, users must manually select the appropriate protocol in the Secure Client:

Step 1: Open the Secure Client application

Step 2: Locate the protocol selection dropdown menu in the client interface

Step 3: Manually change the selection from the IPsec option to the TLS option

Step 4: Initiate the VPN connection using the TLS/DTLS protocol

Protocol Behavior Clarification

The Primary protocol setting in Cisco Secure Access RAVPN determines the default protocol presented in the Secure Client, but does not enable automatic failover functionality. When both TLS/DTLS and IPsec(IKEv2) are enabled:

- The Secure Client displays separate protocol options in the dropdown menu
- The client defaults to the Primary protocol setting (IPsec in this case)
- No automatic switching occurs between protocols based on network connectivity conditions
- Users must manually select the appropriate protocol based on their network environment

Cause

Cisco Secure Access RAVPN is designed without automatic protocol failover functionality. When both TLS/DTLS and IPsec(IKEv2) protocols are enabled, the system requires manual protocol selection through the Secure Client interface. The Primary protocol setting only determines the default selection in the client dropdown menu and does not implement automatic switching logic when connectivity issues are encountered with the primary protocol.

Related Content

- Cisco Secure Access Documentation
- Cisco Technical Support & Downloads