Secure Access RA-VPN IPv6 Connection Fails - Protocol Configuration Issue

Contents

Issue

RA-VPN connections over IPv6 to Cisco Secure Access are failing to establish, with the Cisco Secure Client UI displaying a generic connection failure message. The issue affects testing of IPv6-based remote access connectivity using an existing RA-VPN profile. Research indicates that the SSE RA-VPN profile is not properly setting the protocol field for IPv6 connectivity.

Environment

- Secure Access - Secure Client Remote Access
- Cisco Secure Client attempting IPv6 remote access connection

Resolution

To resolve the IPv6 RA-VPN connection failure, the IP Protocol Supported setting must be properly configured in the RA-VPN profile. Follow these steps to enable IPv6 support.

Step 1: Access Client Settings

Navigate to the **Client Settings** section in the **Cisco Secure Access** management interface.

Step 2: Configure Administrator Settings

Within **Client Settings**, locate and access the **Administrator Settings** section.

Step 3: Set IP Protocol Supported

Configure the IP Protocol Supported dropdown to include IPv6 support. This setting controls which IP protocols the RA-VPN profile supports for client connections.

Step 4: Save Configuration

Save the updated RA-VPN profile configuration to ensure the IPv6 protocol setting is applied.

Step 5: Test Connection

Retest the IPv6 RA-VPN connection using the Cisco Secure Client to verify that the connection now establishes successfully.

Cause

The root cause of the IPv6 RA-VPN connection failure is that the IP Protocol Supported setting in the RA-VPN profile was not configured to support IPv6 connections. The SSE RA-VPN profile requires explicit configuration of the protocol field to enable IPv6 connectivity. Without this setting properly configured, the Cisco Secure Client cannot establish IPv6-based VPN connections to the Cisco Secure Access platform.

Related Content

- Cisco Technical Support & Downloads