Secure Client Identity Visibility Issues with MX75 Network Tunnel in Secure Access

Contents

Issue

When endpoints with Secure Client are deployed behind an MX75 network tunnel connecting to Secure Access, roaming client and user identities are not properly visible in the system. The following specific behaviors are observed:

- Backoff settings configured to prioritize Secure Client over network tunnel connections do not function as expected when endpoints are behind the MX75
- Traffic steering rules based on domains do not apply because traffic is attributed only to the network tunnel identity rather than the roaming client
- Activity Search displays incomplete source location information, showing only the network tunnel identity while omitting user and roaming client identities
- Identity-based traffic steering rules (such as those based on Active Directory users or roaming client identity) fail to apply for traffic traversing the MX75 tunnel

This behavior prevents proper identity segregation and policy application for endpoints connecting through the network tunnel infrastructure.

Environment

- Cisco Secure Access deployment
- MX75 appliance with network tunnel configuration to Secure Access
- Secure Client agents installed on all endpoints
- Backoff settings disabled on roaming clients to prioritize Secure Client over network tunnel connections
- Traffic steering rules configured for domain-based routing
- Identity-based policies configured for Active Directory users and roaming clients

Resolution

The issue was resolved by implementing a workaround configuration using a Registered Network approach instead of relying on roaming identity visibility through the MX75 network tunnel.

Workaround Implementation

Step 1: Configure RSM (Roaming Security Module) with Registered Network

Replace the existing network tunnel configuration with an RSM deployment combined with a Registered Network setup. This configuration allows proper identity attribution and policy application.

Step 2: Validate Identity Visibility

After implementing the Registered Network configuration, verify that:

- User identities are properly displayed in Activity Search
- Roaming client identities are visible and attributed correctly
- Traffic steering rules based on user and client identity function as expected

Step 3: Test Traffic Steering Functionality

Confirm that domain-based traffic steering rules and identity-based policies apply correctly with the new configuration.

Alternative Approach

For environments where identity segregation over private networks is not required, consider implementing RSM - Internet configuration. This approach sends RSM traffic directly to the internet rather than through the private network tunnel, which can provide proper identity visibility while maintaining security controls.

Technical Analysis

During troubleshooting, diagnostic output was collected using policy.test.sse.cisco.com to demonstrate the identity attribution behavior when endpoints were behind the MX75 tunnel. The analysis confirmed that while routing roaming identities through a network tunnel is technically possible, it is not a recommended or supported operational flow for this specific deployment scenario.

Cause

The root cause is related to how Secure Access handles identity attribution when traffic traverses through network tunnel infrastructure. When endpoints connect through the MX75 network tunnel, the system attributes all traffic to the tunnel identity rather than preserving the individual roaming client and user identities. This behavior is by design for network tunnel connections, but conflicts with the requirement for individual identity visibility and policy application.

While technically feasible to route roaming identities through network tunnels, this configuration is not recommended or supported as a standard operational flow due to the identity attribution limitations described above.

Related Content

- Cisco Technical Support & Downloads