Client-Based ZTNA Traffic Steering Issues with Secure Client

Contents

Issue

Client-based Zero Trust Network Access (ZTNA) fails to provide access to internal applications when accessed by FQDN or direct IP address, while the same applications remain reachable over VPN connection.

The specific symptoms observed include:

- Secure Client ZTNA cannot reach internal applications by FQDN or direct IP when VPN is disconnected.
- Browser-based ZTNA access functions correctly for the same applications.
- No ZTNA events appear in Activity logs when VPN is down, indicating client traffic is not being routed through the ZTNA path.
- Private app definitions have been verified to match VPN-routable resources with correct IP/port/FQDN configurations.
- ZTNA policies have been confirmed to match the test user and group assignments.

The issue isolates specifically to Secure Client ZTNA traffic steering or enforcement mechanism, as browser-based ZTNA validates that backend publishing and enforcement are functioning properly.

Environment

- Technology: Secure Access - Zero Trust Network Access (ZTNA)
- Components: Client-Based ZTNA, Posture, Enrollment, Private Resource access
- Secure Client with coexisting VPN profiles
- Private applications accessible via both FQDN and direct IP addressing
- Browser-based ZTNA functionality confirmed working

- Policy enforcement configured in Most Specific Match Enforcement Mode

Resolution

The resolution involved configuration adjustments to the ZTA profile and policy validation. The steps described in the next sections were taken to restore client-based ZTNA functionality.

Step 1: Add Private Resources to ZTA Profile

Private Resources were added to the ZTA profile configuration. After this change, blocked events began appearing in the activity logs and screenshots, indicating that client traffic was now being properly routed through the ZTNA path.

Step 2: Policy Verification and Testing

A temporary "permit any" rule was added to validate traffic flow. While this rule was active, client-based ZTNA access functioned correctly, confirming that the traffic steering mechanism was working but policy enforcement needed adjustment.

Step 3: Policy Refinement

The temporary permit-any rule was removed, and the specific access policies were validated. The private resource was confirmed to be accessible under the access policy named Private Ressources_Cyril using the Most Specific Match Enforcement Mode of the platform.

Step 4: Configuration Validation

The user confirmed that client-based ZTNA access began working consistently after the configuration changes. The issue was resolved without requiring additional policy modifications or system changes.

Cause

The root cause was incomplete Private Resource configuration in the ZTA profile. Without proper Private Resources defined in the ZTA profile, client traffic was not being steered through the ZTNA enforcement path, causing it to fall back to local routing mechanisms. This resulted in the traffic bypassing ZTNA policies entirely, which explained why no ZTNA events appeared in the Activity logs when VPN was disconnected.

The issue was specific to client-based ZTNA traffic steering configuration, while browser-based ZTNA continued to function because it uses a different traffic handling mechanism that was properly configured.

Related Content

- Cisco Technical Support & Downloads