NATIVE CLIENT / CONTROLLED CONNECTIVITY

An enterprise client from enrollment to application access

A technical white paper on native client responsibilities, routing, DNS, session lifecycle, and the relationship between VPN and zero trust.

6 September 2026 / Technical edition

Inside this paper

01 / The client is a policy participant

The Antara enterprise client connects a device to the access architecture and supplies the context needed to govern that connection. Its responsibilities include enrollment, authentication, traffic selection, tunnel establishment, network-change handling, and usable diagnostics. The gateway remains an enforcement point; a local connected state is not a blanket application entitlement.

From installation to work

01	Enroll	Bind the installation to tenant and device identity.
02	Authenticate	Establish user identity and certificate trust.
03	Connect	Negotiate the transport and install approved routes.
04	Authorize	Reach resources within the active policy scope.

VPN and ZTNA are complementary deployment tools. Network-level connectivity remains useful for protocols and applications that need it, while application-scoped access reduces unnecessary reachability. Choose the boundary per workload and use a common identity and evidence model across both.

02 / Make routing and DNS one design

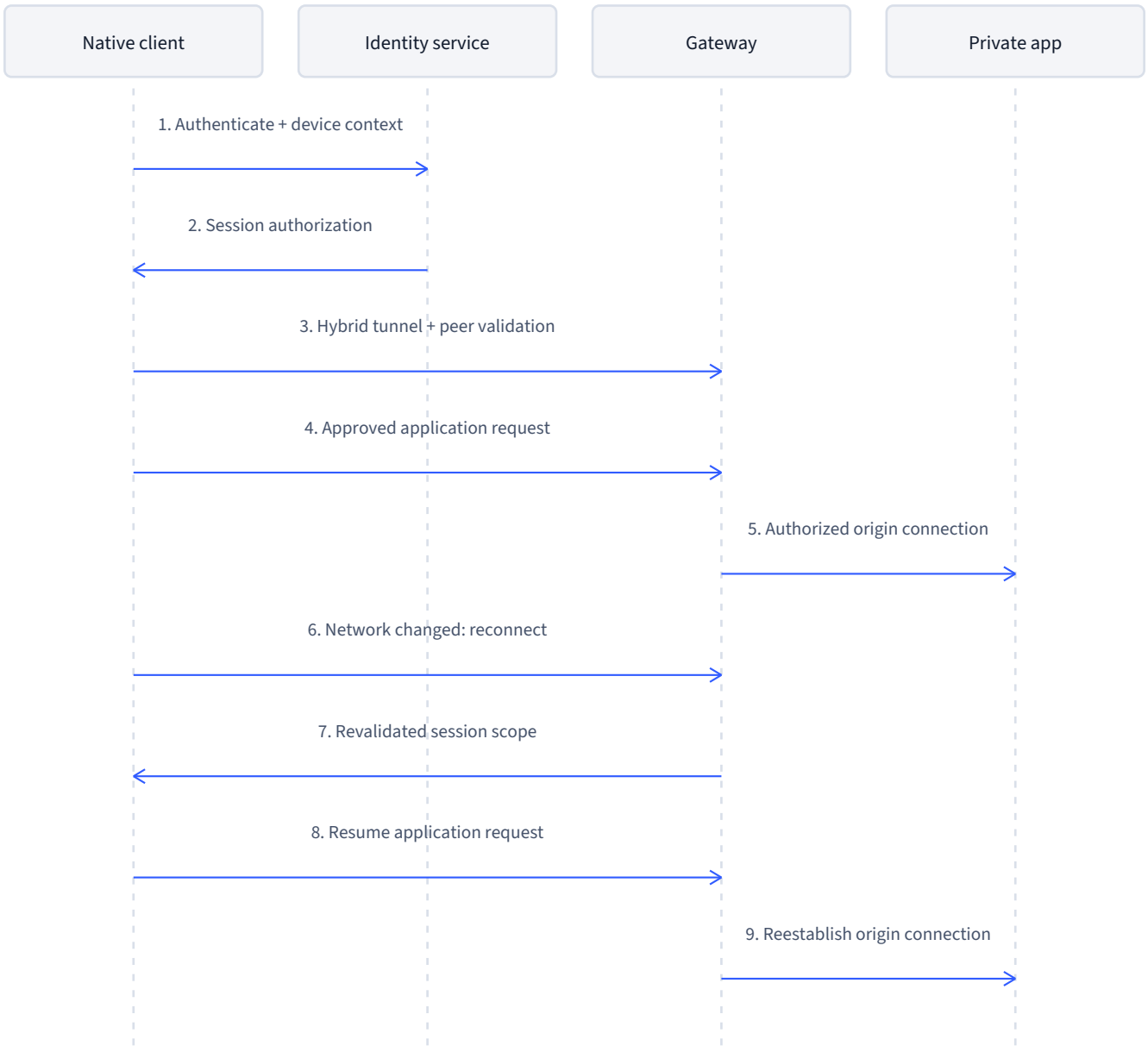
Mode	Appropriate use	Design obligation
Full tunnel	Traffic requiring a common enterprise egress policy.	Capacity, local services, captive portals, and exception handling.
Route split	Defined private prefixes with separate internet egress.	Overlapping ranges, dual stack, and dependency discovery.
Domain-aware selection	Applications located through dynamic DNS.	Resolver ownership, TTLs, aliases, and address changes.
Per-app access	Applications needing narrow connectivity.	Platform support, process identity, and helper processes.

A route rule and a DNS rule must agree. Resolving an internal name through an unrelated public resolver can fail or disclose internal naming. Sending a public answer into an unrelated private route can make the application appear intermittently broken. Specify the resolver, suffixes, included destinations, and IPv6 behavior in the same review.

Treat overlapping private addresses as an application design problem rather than adding ever broader routes. Validate home-network collisions, local printers, conferencing media, and applications with multiple background connections. The operating system's VPN and network extension facilities determine which controls are available on a given platform.

03 / A connection across changing networks

Network change and authorized recovery



When Wi-Fi changes to cellular, transport addresses and reachability can change while the user expects work to continue. Recover the tunnel within the session policy, refresh stale context, and restore only the intended routes. Some applications can resume; others must reconnect. Do not equate tunnel recovery with preservation of every application socket.

- Detect captive portals before applying a policy that prevents portal completion.
- Specify whether a failure blocks traffic, permits an approved recovery path, or leaves selected local services available.
- Use bounded reconnect backoff to avoid battery drain and synchronized gateway retry storms.

- Distinguish a gateway failure from failed DNS, identity expiry, and an unreachable origin.
- Give the user a clear recovery action when administrator intervention is required.

04 / Identity and post-quantum transport

Pair user authentication with device enrollment so a stolen session token is not treated as the entire device identity. Store private credentials in the operating system's protected key facilities where supported. Define renewal and revocation behavior for devices that sleep, roam, or remain offline for extended periods.

Apply post-quantum policy to the actual transport in use. A hybrid TLS path and an IPsec path require different implementation evidence. Product evaluation should confirm negotiated algorithms per transport and client release instead of assuming every protocol inherits a TLS setting. Client and server certificate authentication have their own compatibility requirements.

Client deployment intent

```
profile: finance-managed
identity:
  tenant: enterprise-example
  require_device_enrollment: true
routing:
  private_resources: [finance-erp, internal-git]
  internal_dns_suffixes: [internal.example]
  ipv6_policy: explicit
transport:
  require_hybrid_where_supported: true
  unsupported_path: administrator-review
recovery:
  captive_portal: guided
  restore_only_authorized_routes: true
diagnostics:
  redact_credentials: true
```

Use this worksheet to agree deployment intent with network, identity, and endpoint teams. Translate it into the managed configuration supported by the chosen client release; it is not an installable profile.

05 / An evidence-led support path

The most useful support bundle connects a user-visible error to a specific layer: enrollment, identity, certificate trust, DNS, route selection, tunnel, or origin. Include timestamps, release versions, selected gateway, resource identity, and policy version. Exclude secrets and constrain any packet capture to a documented scope and retention window.

The agentic auditor can use that context to assemble an investigation: identify the affected cohort, correlate the first failure with a policy or network change, retrieve relevant connection evidence, and present a reviewable explanation. A recommendation to change routing should remain distinguishable from an approved configuration change.

Test	Include	Success evidence
Network transitions	Wi-Fi, cellular, sleep, captive portal.	Recovery behavior and application impact.
Traffic policy	Allowed app, denied app, DNS and IPv6.	Expected route and enforcement result.
Credential lifecycle	Renewal, expiry, revoked enrollment.	Correct reauthentication or denial.
Gateway resilience	Member failure and capacity pressure.	Recovery with intended scope.
User experience	Battery, accessibility, error guidance.	Task completion and support findings.

References and continued reading

Product overview

Integration guide

Operations and evaluation