SECURITY · TEMPLATE

Affordable Zero-Trust Network Access for Growing Teams

KAANSYSTEMS.COM/LIBRARY/AFFORDABLE-ZTNA-GROWING-TEAMS · SEPTEMBER 16, 2026

ABOUT THIS TEMPLATE

ZTNA replaces the VPN with per-app access gated by identity and device. For a growing team it starts free-to-cheap — Cloudflare Access, Tailscale, or Twingate — not a six-figure platform.

THE TEMPLATE

A VPN-to-ZTNA migration checklist. Work top to bottom — the prerequisites are load-bearing, and moving apps before identity is solid is how rollouts fail.

Prerequisites (do not skip)

- [ ] Single SSO provider fronts the apps you're about to protect
- [ ] MFA on 100% of human accounts; passkeys/FIDO2 on every admin
- [ ] Shared/role logins eliminated — named accounts only
- [ ] An inventory of internal apps + who legitimately needs each

Pick + pilot

- [ ] ZTNA tool chosen to sit closest to your existing identity (table above)
- [ ] First app = your *most sensitive* internal tool, not the easiest one
- [ ] Access policy = SSO group **AND** device posture (managed/encrypted)
- [ ] Pilot with a small group; confirm clientless/agent UX is acceptable

Cut over

- [ ] App reachable through the ZTNA broker for the pilot group

- [ ] VPN route to that app removed (not just deprioritized)
- [ ] Access logs flowing to your central logging/SIEM
- [ ] Break-glass path documented and tested before you rely on it

Expand + retire

- [ ] Next apps migrated one at a time, each with per-app policy
- [ ] Device-posture enforcement tightened (block unmanaged where required)
- [ ] Conditional access on anomalies (new geo/device) challenged or blocked
- [ ] VPN concentrator decommissioned once the last sensitive path is off it