

Keep your firewall. Extend your WAN.

Lira-VPN helps enterprises keep their existing next-generation firewall (NGFW) investment while adding a secure, resilient WAN overlay across MPLS and 4G/5G, so branches stay encrypted, visible and governed by the same policy.

Connected. Secure. Visible. Resilient. Recoverable.

WHY IT MATTERS

Failover should never create a security downgrade.

The proposition is deliberately simple: keep the controls you already have, connect every site through a secure overlay, and maintain the same security posture whether a branch is running on MPLS or has moved to LTE. Resilience is added to the WAN; the security investment is preserved.

01 · Keep the firewall investment you already trust

Lira-VPN complements the next-generation firewall already in place, extending policy, inspection and visibility across the distributed WAN instead of replacing what works.

02 · Preserve security when MPLS fails over to LTE

Branches stay under the same security posture when the transport changes, so failover does not become a security downgrade.

03 · See health, failover and recovery in one view

Network and security teams gain the telemetry they need to understand path changes, performance and branch availability in context.

The architectural principle: a change in WAN path must not result in a change in security posture.

WHAT LIRA-VPN ADDS

A secure WAN overlay that complements the next-generation firewall.

- Encrypted inter-site connectivity across MPLS, Internet and 4G/LTE.
- Controlled failover that keeps security policy consistent when the transport changes.
- Branch segmentation and least-privilege access across sites.
- WAN telemetry that helps network and security teams act faster.
- Integration with the next-generation firewall rather than duplication of security controls.
- A practical rollout model with pilot, validation and staged deployment.

HOW IT ROLLS OUT

A phased approach designed for real branches.

01 · Validate the current environment

Map the existing WAN, security controls, Internet egress and branch dependencies before deployment.

02 · Pilot with representative branches

Test a reliable MPLS site, a branch that relies on LTE backup and a business-critical location.

03 · Roll out with controlled failover

Onboard branches in phases, verify routing and confirm that policy remains intact during transport changes.

04 · Integrate telemetry and improve

Connect VPN, firewall and monitoring data so operations can see the full security and availability picture.

Four services around one resilient foundation.

Networking, monitoring and security work as one engagement — from a networking product to a recurring managed service.

01 · Secure WAN engineering

- Hub and branch gateway deployment
- Dual-homing across MPLS and 4G/5G
- Failover engineering and tuning
- Multi-link resilience verification

02 · Security architecture review

- Firewall policy and zone alignment across transports
- Branch micro-segmentation by zone
- Least-privilege inter-branch rules
- Internet egress and cloud breakout mapping

03 · Security visibility and telemetry

- WAN telemetry pipeline into the corporate SIEM
- Transport-health and degraded-path dashboards
- Availability and incident trend reporting
- Alerting on transport flaps and anomalies

04 · Continuous security advisory

- Quarterly architecture and resilience reviews
- Controlled failover and recovery drills
- Patch and vulnerability lifecycle audits
- Joint incident-response exercises

BUSINESS OUTCOME

Connected. Secure. Visible. Resilient. Recoverable.

This brochure positions Lira-VPN as the secure WAN foundation for enterprises that want to extend cybersecurity investment across every site without replacing the controls they already own.

- Connected branches without sacrificing control.
- Encrypted transport across the enterprise WAN.
- Consistent policy whether the link is MPLS or LTE.
- Improved resilience, observability and recoverability.

Management buys continuity of corporate connectivity, encrypted communication across infrastructure the enterprise does not fully control, less dependence on one carrier, and a clearer view of branch and WAN health.

Read next: the enterprise cyber-resilience architecture brief (layered security architecture, capability comparison, delivery plan and governance) and the technical architecture brochure are published on the Lira-VPN website.