

Lira-VPN Enterprise Network Security & Cyber-Resilience

Enhancing an existing next-generation firewall environment across MPLS and 4G/5G branch connectivity — retaining the security investment while introducing an encrypted, resilient WAN overlay.

Connected. Secure. Visible. Resilient. Recoverable.

Key principle: “A change in WAN path must not result in a change in security posture.”

1 · EXECUTIVE SUMMARY

Core proposition.

Your organisation already maintains a substantial cybersecurity foundation through its investment in next-generation firewall (NGFW) infrastructure. The recommendation is straightforward: do not replace or duplicate those capabilities.

The objective is instead to extend that exact security investment across the distributed wide area network. Operating across MPLS and 4G/5G, Lira-VPN delivers an encrypted, resilient WAN overlay that preserves uniform security policy, visibility and control whether a site is on its primary or its failover transport.

2 · Value pillars

Investment protection

Keep the existing next-generation firewall and security controls. No rip-and-replace, no duplicate licensing and no second management overhead.

No security degradation on failover

Branch traffic can move between primary MPLS and secondary 4G/5G without bypassing firewall policy or dropping encryption.

Carrier-independent resilience

A sovereign encrypted overlay across any combination of MPLS, 4G/5G and commercial broadband, without carrier lock-in.

Unified WAN and security telemetry

Tunnel metrics, failover events and latency can be correlated with firewall logs and SIEM pipelines for faster root cause.

Three layers, three responsibilities.

Layer 1 — Security enforcement

Retain and leverage your existing next-generation firewall.

- Stateful enterprise firewalling and deep packet inspection
- Intrusion detection and prevention systems (IDS / IPS)
- Application control, deep protocol analysis and sandboxing
- Dynamic content, URL and web threat filtering
- Centralised internet access and outbound egress control
- Corporate threat prevention, anti-virus and anti-malware
- Enterprise compliance logging, audit trails and event dispatch

Layer 2 — Secure and resilient WAN transport

The Lira-VPN encrypted multi-path WAN overlay.

- Carrier-independent encrypted inter-site tunnel mesh
- Multi-path MPLS and 4G/5G automatic path failover
- Cryptographic confidentiality across public and private links
- Policy enforcement that does not lapse during transport shifts
- Granular branch-to-branch least-privilege segmentation
- High-frequency tunnel health probing and rapid recovery
- Real-time network and tunnel telemetry stream

Layer 3 — Security visibility and response

Correlated telemetry across network, identity and SIEM/SOC.

- Firewall security logs correlated with transport telemetry
- Real-time link degradation, latency and packet-loss alerting
- Integration with enterprise SIEM, SOAR and managed SOC
- Identity-aware access control with directory services and MFA
- Endpoint detection and response context binding
- Centralised DNS security and malicious-domain interception
- Automated incident triage and root-cause determination

Four places the architectural gap usually appears.

Why encrypt carrier MPLS traffic?

MPLS provides private transport SLAs, but private transport must never be equated with cryptographic confidentiality. Unencrypted MPLS remains exposed to carrier misconfiguration, provider infrastructure compromise and traffic interception.

“MPLS provides transport quality; Lira-VPN provides the cryptographic overlay.”

4G/5G failover without a bypass

Cellular connectivity crosses operator cores and the public Internet. Failover to cellular must route through encrypted tunnels into the same inspection stack, preventing uncontrolled Internet breakouts at the branch.

“The physical carrier changes. The security policy, inspection and logging do not.”

Least-privilege branch segmentation

Branches should not be flat extensions of the head-office LAN. Segmentation across user, server, management, IoT and guest zones confines a branch incident locally instead of letting it move laterally across the enterprise.

“Branch-to-branch communication is blocked by default and permitted on documented business need.”

Correlated telemetry for SIEM / SOC

Tunnel health, jitter, packet loss and failover notifications are streamed into existing SIEM or SOC tooling, so transport degradation can be correlated with application response and firewall event logs.

“Distinguish an application fault from a transport change in seconds, not hours.”

Existing foundation versus recommended enhancement.

Area	Capability	Existing foundation	Recommended enhancement
Security	Next-generation firewall	Existing NGFW platform	Retain it and optimise policy rules across all WAN paths
Security	IDS / IPS threat detection	Centralised NGFW IDS/IPS	Extend inspection coverage to 4G/5G failover and inter-branch traffic
Security	Content and web filtering	Head-office appliance	Preserve filtering policy during branch failover; prevent uncontrolled breakout
Network	MPLS transport	Carrier MPLS (unencrypted)	Retain the transport SLA while adding the encrypted overlay
Network	4G/5G connectivity	Ad-hoc backup / internet link	Fully integrate it into the encrypted, policy-enforced WAN overlay
Network	Inter-site encryption	Variable / inconsistent	Consistent enterprise-grade encryption across all transport paths
Network	Failover architecture	Manual or route flapping	Automated, health-checked failover with no lapse in security posture
Operations	Branch segmentation	Flat branch LANs	Micro-segmented zones: users, servers, management, IoT, guests
Operations	Branch-to-branch trust	Unrestricted lateral reach	Explicit, business-driven least-privilege access rules only
Operations	Telemetry and monitoring	Siloed link up/down checks	Correlated WAN telemetry and firewall events in one dashboard
Operations	Incident response	Fragmented troubleshooting	WAN context integrated into SIEM/SOC workflows

6 · INVESTMENT PROTECTION

What is preserved, and what Lira-VPN adds.

Preserved — 100% of the existing foundation

- **Existing next-generation firewall (NGFW)** — Proven security enforcement, custom rules and licensed threat engines remain intact.
- **Existing IDS / IPS systems** — Mature signatures and operational models already invested in by the security team are reused.
- **Content and URL filtering** — Established corporate acceptable-use policies and web classifications are preserved.
- **Endpoint security and EDR** — Works alongside the endpoint agents already deployed on user devices and servers.
- **Identity and directory services** — Interoperates with existing directory services, federated identity and multi-factor authentication.
- **Current carrier MPLS links** — High-SLA circuit contracts are retained while confidentiality is added through encryption.

Added by the overlay

- **Secure WAN overlay** — Wraps inter-site and branch traffic in cryptographic tunnels regardless of the underlying transport.
- **Deterministic multi-path resilience** — Path failover between MPLS and 4G/5G based on observed application health, latency and packet loss.
- **Complete carrier independence** — Removes proprietary telco lock-in and allows multi-carrier or regional cellular connections.
- **Consistent security posture** — Segmentation, access restrictions and inspection requirements stay the same on every path.
- **Continuous WAN telemetry** — Deep diagnostics — jitter, packet loss, reconnects and tunnel health — stream into SIEM/SOC tooling.
- **Lateral threat containment** — Unrestricted branch-to-branch trust is removed, confining a branch incident locally.

Five stages, from validation to continuous improvement.

Stage 1 · Weeks 1–2 — Architecture validation

Audit existing WAN topology, firewall zones, routing tables and critical business applications so the design aligns with live operations.

- Current-state network and security topology map
- Policy gap analysis across transports
- Target overlay and segmentation specification

Stage 2 · Weeks 3–4 — Controlled pilot deployment

Deploy across two or three representative branches: one high-volume MPLS site, one that relies on cellular backup, one business-critical site.

- Pilot gateways installed and dual-homed
- Failover and recovery testing under load
- Pilot acceptance sign-off

Stage 3 · Weeks 5–8 — Progressive branch rollout

Systematic, phased migration of the remaining sites using documented runbooks and controlled cutover windows.

- Phased branch gateway commissioning
- Per-site rollback procedures documented
- Branch micro-segmentation implemented

Stage 4 · Weeks 9–10 — Security and operations integration

Connect overlay telemetry into central firewall logging, SIEM/SOC platforms, directory services and monitoring consoles.

- Event forwarding and alert rules configured
- Unified NOC / SOC operations dashboards
- Incident-response runbooks updated

Stage 5 · Ongoing — Continuous cyber-resilience improvement

Quarterly resilience validation, recovery simulations, policy audits and architecture roadmap refinement.

- Quarterly WAN resilience and failover drills
- Annual architecture review and capacity planning
- Proactive advisory and optimisation reports

8 · RACI GOVERNANCE

Who is responsible, accountable, consulted and informed.

A/R = accountable and responsible · C = consulted · I = informed.

Activity	Client IT	Security team	Lira-VPN team	WAN provider
Next-generation firewall management	A / R	A / R	C	I
Carrier MPLS circuits	C	I	C	A / R
4G/5G backup services	C	I	A / R	A / R
Lira-VPN overlay mesh	C	C	A / R	I
Core enterprise routing	A / R	C	C	C
Security policy enforcement	A / R	A / R	C	I
Branch micro-segmentation	A / R	A / R	C	I
WAN and telemetry monitoring	A / R	A / R	C	C
Security incident response	C	A / R	C	C
WAN degradation incidents	A / R	C	A / R	A / R
Configuration backups	A / R	C	C	I
Resilience and failover drills	A / R	A / R	A / R	C

9 · SECURITY PRINCIPLES

Ten principles that govern the design.

1. Preserve existing investment

Do not replace an existing security capability unless there is a demonstrated business or technical gap.

2. Defence in depth

No single security control is sufficient; security is layered at transport, perimeter and endpoint.

3. Least-privilege access

Only documented, business-justified communication is allowed between sites and network segments.

4. Secure by default

New branches, tunnels and network paths start isolated and controlled until they are validated.

5. Consistent security during failover

A failure of the primary transport must never compromise, bypass or degrade security inspection.

6. Pervasive visibility

All network and security events — from tunnel flaps to firewall drops — are observable and correlated.

7. Granular segmentation

A compromise in one branch or segment must never automatically grant enterprise-wide reach.

8. Cryptographic confidentiality

Sensitive enterprise traffic is encrypted across both private carrier links and public cellular networks.

9. Guaranteed recoverability

Network and security configurations are auditable, versioned, backed up and rapidly recoverable.

10. Continuous improvement

Security and resilience are an ongoing operational discipline, not a one-off project.

Lira-VPN is the secure connectivity layer of a wider security architecture: firewall, identity, endpoint, SIEM and SOC capabilities remain separate, complementary layers.

Companion documents: the secure WAN overlay brochure (commercial summary) and the technical architecture and resilient networking brochure (engineering detail) are published on the Lira-VPN website.