INTELLILINK
GATEWAY™

TECHNICAL PROOF BRIEF

Enterprise Satellite Connectivity — Governance Control Plane

Laboratory and field validation of the Intellilink Gateway™ control plane architecture

DOCUMENT TYPE	VALIDATION	ARCHITECT
Technical Validation Summary	Laboratory + Field (Completed)	Emmanuel Mukwesa

DOCUMENT	Technical Proof Brief
VERSION	2.0
DATE	07 February 2026
STATUS	Technical Validation Summary
PREPARED BY	Intellilink Media LLC™ (USA)
ARCHITECT	Emmanuel Mukwesa · Founder & Architect
CLASSIFICATION	Public — Institutional Release (Anonymized)

SECTION 01

Executive Technical Overview

The rapid adoption of satellite Internet services, particularly low-Earth-orbit (LEO) systems, has significantly improved connectivity resilience for enterprises across Africa. However, many enterprise deployments operate outside traditional Internet Service Provider (ISP) delivery models, reducing visibility, accountability, and alignment with national Internet governance frameworks.

Intellilink Gateway™ introduces a control-plane architecture designed to restore traditional ISP governance characteristics — including local IP anchoring, accountable upstream presence, and auditability — while preserving the performance and resilience benefits of satellite connectivity.

This document summarizes both laboratory and field validation of the Intellilink Gateway™ control plane under real operating conditions.

SECTION 02

Architectural Overview

The Intellilink Gateway™ architecture separates access connectivity from governance enforcement:

ACCESS LAYER — UNCHANGED

- Satellite transport underlay (e.g., Starlink)
- Enterprise retains direct satellite performance characteristics

GOVERNANCE LAYER — INTRODUCED

- Secure gateway node adjacent to satellite CPE
- Encrypted tunnel to a domestic ISP Point of Presence (PoP)
- Policy enforcement, traffic visibility, addressing, and logging at the PoP

LOGICAL TRAFFIC FLOW

```
Enterprise LAN → Satellite CPE (Starlink) → Intellilink Gateway™ Agent Node
                    → Encrypted Tunnel → ISP PoP (Governance Anchor) → Internet
```

The architecture does not replace satellite connectivity. Instead, it re-anchors enterprise traffic into a conventional ISP governance domain.

SECTION 03

Validation Scope

3.1 LABORATORY VALIDATION (COMPLETED)

The following capabilities were validated in a controlled laboratory environment:

- Secure tunnel establishment between Gateway and ISP PoP
- Local IP address assignment under ISP-controlled address space
- Traffic forwarding consistency under tunneled operation
- NAT and routing behavior aligned with traditional ISP models
- Separation of management and traffic planes

3.2 FIELD VALIDATION (COMPLETED)

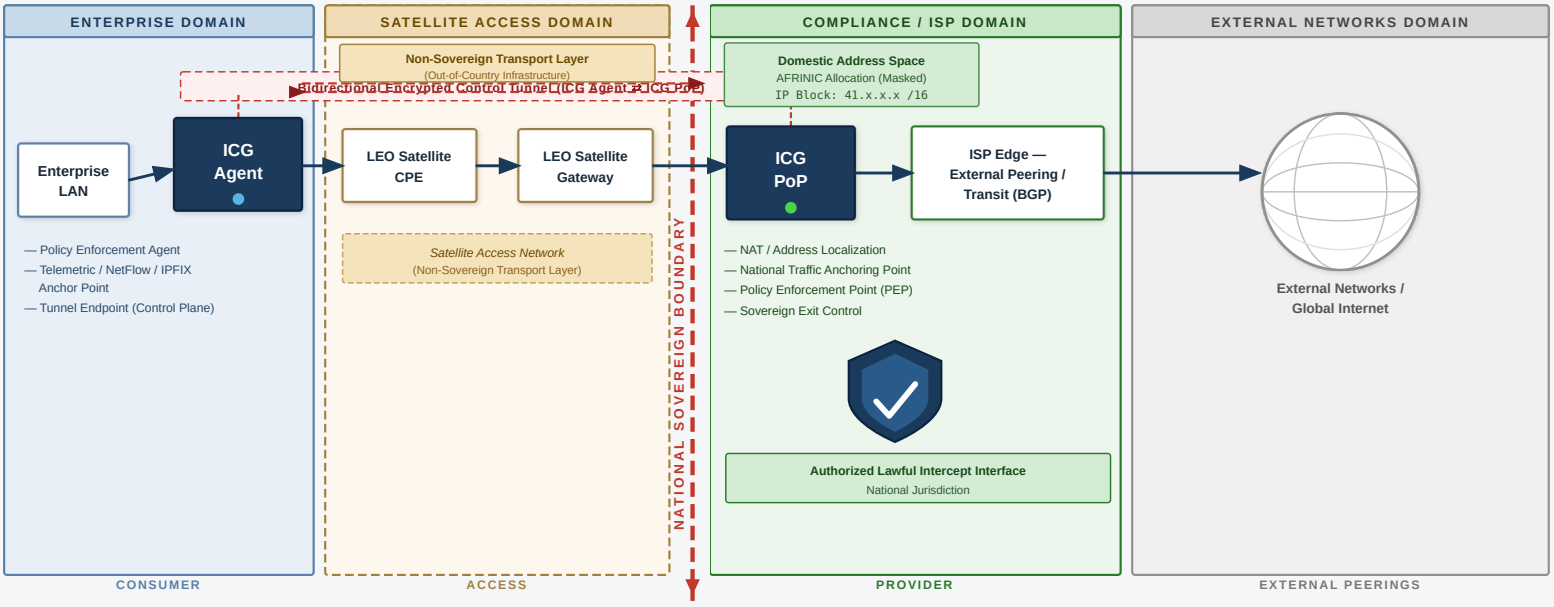
The architecture was deployed and tested in a live production environment with anonymization applied. Deployment components included one domestic ISP Point of Presence, one enterprise network site, active satellite connectivity using Starlink, and real enterprise traffic traversing the governance control plane.

Field validation confirmed: stable tunnel operation, correct traffic anchoring at the ISP PoP, transparent application behavior for enterprise users, and no material performance degradation attributable to the control layer.

Intellilink Compliance Gateway (ICG) — Reference Architecture

Architecture for compliant enterprise satellite connectivity with domestic traffic anchoring and sovereign enforcement.

Document Class: Technical Proof Brief
Revision: 3.0 | February 2026
For Regulatory Review



KEY:

- National Sovereign Boundary (jurisdictional delimiter)
- Bidirectional Encrypted Control Plane (ICG Agent ⇄ ICG PoP) — not visible in traceroute / data plane
- Data Plane — User Traffic
- Authorized Lawful Intercept (LI) Interface — National Jurisdiction
- Non-Sovereign Transport Layer (out-of-country infrastructure — encapsulated)
- Policy Enforcement Point (PEP) — ICG Agent & ICG PoP
- Domestic Address Space — AFRINIC Allocation (Masked) — 41.x.x.x/16
- ISP Edge — External Peering / Transit (BGP)

FIGURE 1 Intellilink Gateway™ Technical Architecture — Governance Control Plane Overlay

The architecture introduces a governance control plane that anchors satellite-originated enterprise traffic within a domestic ISP Point of Presence while preserving satellite access performance. All IP addresses masked for anonymity. Reference architecture — Revision 3.0, March 2026.

SECTION 04

Field Environment (Anonymized)

The following roles were involved in the field validation exercise. All participating entities were anonymized; no enterprise customer data was retained beyond transient packet forwarding requirements.

ROLE	DESCRIPTION
Satellite Underlay	LEO satellite service (Starlink)
ISP Role	Governance anchor and PoP termination — identity withheld
Enterprise Role	Traffic source and destination — identity withheld
Gateway Role	Control-plane enforcement node (Intellilink Gateway™ Agent)

SECTION 05

Governance Capabilities Demonstrated

During validation, the following governance capabilities were demonstrated:

Accountable upstream presence	Enterprise traffic visibly enters an ISP PoP, establishing a transparent and auditable governance boundary
Address sovereignty	Enterprise traffic appears under domestic IP addressing space following tunnel termination at the ISP PoP
Traffic observability	Flow-level monitoring is feasible at the PoP, enabling oversight without modification to satellite infrastructure
Policy insertion point	ISP-side controls are possible without any modification to satellite infrastructure
Audit readiness	Architecture supports integration with lawful intercept and logging systems where legally required

USE CASE: DOMESTIC TRAFFIC ANCHORING FOR SATELLITE BROADBAND NETWORKS

Intellilink Compliance Gateway (ICG)
Traffic Anchoring — Before / After Routing Comparison

Figure 2 — Traceroute-Based Routing Validation | Source: Enterprise LAN (192.168.x.x, Lusaka) → Destination: speedtest.mtn.zm (41.223.117.81)

For Regulatory Review

Document Type: Technical Proof Brief
Revision: 2.0 | Date: February 2026
Prepared For: Telecommunications Regulator
Originator: Intellilink / ICG Architecture Team

Routing Behaviour Comparison Demonstrates how ICG deployment anchors enterprise satellite traffic within national legal jurisdiction, restoring domestic policy enforcement and lawful intercept capability.

⚠ BEFORE ICG
17 hops / 242 ms
8 foreign ASN hops | No LI capability

✓ AFTER ICG
7 hops / 302 ms
0 foreign ASN hops | Full LI capability

Note on latency delta (+60 ms): Increased latency reflects the overhead of domestic traffic anchoring, NAT processing, and compliance enforcement at the ICG PoP. This is consistent with the security and regulatory objectives of the deployment.

LEGEND — Data Plane (User Traffic) | Encapsulated Tunnel (Data Plane) | Control Plane (Encrypted — not traceroute-visible) | Foreign / Non-Sovereign ASN | Domestic ASN (Zambia) | Encapsulated Hop (not data-plane visible) | Sovereign Network Boundary

⚠ BEFORE ICG DEPLOYMENT — NON-SOVEREIGN ROUTING (NON-COMPLIANT)

DATA PLANE ORIGIN
ENTERPRISE LAN
192.168.1.79 — LUSAKA, ZAMBIA

ENTERPRISE DOMAIN
No Compliance Gateway
Traffic exits unencapsulated

SATELLITE ACCESS DOMAIN — NON-SOVEREIGN TRANSPORT
LEO Satellite CPE
Satellite Provider Network
LEO Satellite Gateway
Foreign egress — jurisdiction exit

⚠ SOVEREIGN NETWORK BOUNDARY — TRAVERSED WITHOUT CONTROL

EXTERNAL NETWORKS — INTERNATIONAL TRANSIT (FOREIGN ASN(S))
Foreign ASN Transit
206.224.73.x / 154.66.247.x / 149.6.x.x
No lawful intercept · No domestic policy enforcement

↩ RE-ENTRY INTO NATIONAL JURISDICTION

DOMESTIC ISP DOMAIN (RE-ENTRY — ZAMBIA ASN)
Carrier / ISP Edge
ISP Edge

DATA PLANE DESTINATION
SPEEDTEST.MTN.ZM
41.223.117.81 — MTN ZAMBIA

TRACEROUTE — BEFORE ICG | ENTERPRISE LAN → 41.223.117.81

1	192.168.1.1	112.817 ms	LAN Default GW
2	100.64.0.1	171.163 ms	CGNAT (Sat. CPE)
3	172.16.250.86	170.346 ms	Satellite Provider PoP
⚠ Sovereign Network Boundary crossed — foreign ASN transit begins			
4	206.224.73.68	170.073 ms	Foreign ASN
5	206.224.73.52	170.196 ms	Foreign ASN
6	102.68.115.226	170.877 ms	Foreign ASN
7	154.66.247.66	204.070 ms	Foreign transit
8	154.66.247.106	62.200 ms	Foreign transit
9	154.66.247.99	203.870 ms	Foreign transit
10	* * *		No response (filtered)
11	149.6.144.125	216.014 ms	Foreign transit
← Re-entry into Zambia domestic ASN			
12	41.181.105.163	215.952 ms	Carrier Edge
13	41.181.244.162	339.148 ms	ISP Core
14	41.181.244.205	201.123 ms	ISP Core
15	181.190.133	193.452 ms	ISP Distribution
16	41.223.119.202	238.447 ms	MTN Edge
17	41.223.117.81	242.281 ms	DESTINATION ✓

COMPLIANCE ASSESSMENT — NON-COMPLIANT
- ✗ 8 hops through foreign ASN infrastructure (hops 4–11); traffic exits national legal jurisdiction.
- ✗ No domestic address localization — source IP is not anchored to a national ASN at egress.
- ✗ No lawful intercept capability during foreign ASN transit segment.
- ✗ No policy enforcement point present in path before international egress.
- ✗ Traffic re-enters domestic jurisdiction only at hop 12, without any compliance validation.

✓ AFTER ICG DEPLOYMENT — DOMESTICALLY ANCHORED ROUTING (COMPLIANT)

DATA PLANE ORIGIN
ENTERPRISE LAN
192.168.101.5 — LUSAKA, ZAMBIA

ENTERPRISE DOMAIN
ICG Agent (Compliance Gateway)
PEP | TUNNEL ENDPOINT
Policy enforcement · Telemetry · Routing control

Control Plane (Encrypted) — ICG Agent ⇄ ICG PoP
Tunnel management · Policy updates · Telemetry
Not visible in traceroute output

SATELLITE ACCESS DOMAIN — NON-SOVEREIGN TRANSPORT (TUNNEL-ENCAPSULATED)
LEO Satellite CPE
Encapsulated tunnel (data plane not exposed)
Satellite Provider Network
LEO Satellite Gateway
Transit only — payload opaque to provider

✓ SOVEREIGN NETWORK BOUNDARY — TRAFFIC ANCHORED DOMESTICALLY

COMPLIANCE / ISP DOMAIN — NATIONAL POLICY ENFORCEMENT ZONE
ICG PoP — Domestic Anchor Point
NAT / ADDRESS LOCALIZATION
PEP | LAWFUL INTERCEPT
National ASN egress · Zambia legal jurisdiction · AFRINIC address space
ISP Edge — National ASN (Lusaka)
Local IXP (Domestic Peering)
MTN Edge

DATA PLANE DESTINATION
SPEEDTEST.MTN.ZM
41.223.117.81 — MTN ZAMBIA

TRACEROUTE — AFTER ICG | ENTERPRISE LAN → 41.223.117.81

1	192.168.101.1	2.020 ms	ICG Agent — LAN GW
→ Satellite segment (encapsulated tunnel — hops not data-plane visible)			
2	172.16.10.1	246.031 ms	ICG PoP ingress — tunnel decap
3	41.x.x.x	243.932 ms	NAT egress — Local ISP ASN (masked)
4	* * *		No response (ICMP filtered)
→ Local IXP / MTN domestic transit			
5	192.32.209.224	291.902 ms	Local IXP
6	41.223.119.202	269.292 ms	MTN Edge
7	41.223.117.81	302.121 ms	DESTINATION ✓

■ Satellite transit hops are encapsulated within the ICG tunnel and are not visible as individual traceroute hops. This is expected behaviour and does not indicate routing anomalies.

COMPLIANCE ASSESSMENT — COMPLIANT
- ✓ Zero foreign ASN hops observed in traceroute. All intermediate addresses within domestic ASN space.
- ✓ Address localization enforced at ICG PoP via NAT; public egress uses domestic ASN address space.
- ✓ Lawful intercept capability present at ICG PoP, within national legal jurisdiction.
- ✓ Policy Enforcement Point (PEP) active at both ICG Agent (enterprise) and ICG PoP (compliance domain).
- ✓ Satellite segment traffic is encapsulated — provider has no access to payload data plane.

POLICY COMPLIANCE OUTCOMES — ICG DEPLOYMENT
- ✓ Domestic traffic anchoring
- ✓ Lawful intercept capability
- ✓ Domestic ASN public egress
- ✓ National jurisdiction enforced
- ✓ Address localization (NAT)
- ✓ Authority visibility restored

LATENCY NOTE — BEFORE VS. AFTER
The observed increase in end-to-end latency (+60 ms; 242 ms → 302 ms) is attributable to the domestic anchoring path via the ICG PoP, including tunnel decapsulation, NAT processing, and local IXP peering. This latency overhead is an inherent and expected consequence of compliance enforcement and is consistent with domestic traffic anchoring obligations.

CONTROL PLANE — TRACEROUTE INVISIBILITY
The encrypted control plane tunnel between the ICG Agent and ICG PoP operates independently of the data plane and is not reflected in traceroute output. The satellite transit segment appears compressed to a single logical hop (hop 1 → hop 2) due to tunnel encapsulation. This is expected and does not indicate missing hops or routing anomalies.

LAWFUL INTERCEPT — REGULATORY NOTE
Lawful Intercept (LI) capability is implemented at the ICG PoP, within the national legal jurisdiction. LI interfaces comply with applicable national telecommunications regulations. No interception capability is delegated to the satellite provider or foreign ASN infrastructure.

FIGURE 2 Routing Behavior Before and After Governance Anchoring — Technical Reference Diagram

The diagram illustrates how enterprise traffic that previously exited the satellite network through external upstream paths becomes anchored within a domestic ISP governance domain after deployment of the Intellilink Gateway™ control plane. Traceroute measurements confirm routing re-anchoring within domestic ASN space.

SECTION 06 — 07

Validation Outcomes

WHAT WAS PROVEN

- ✔ Satellite connectivity can be governed without degrading performance
- ✔ ISP accountability can be restored without owning the satellite access link
- ✔ Enterprises can retain connectivity resilience while aligning with national frameworks
- ✔ The model can be deployed using existing ISP infrastructure

EXPLICITLY OUT OF SCOPE

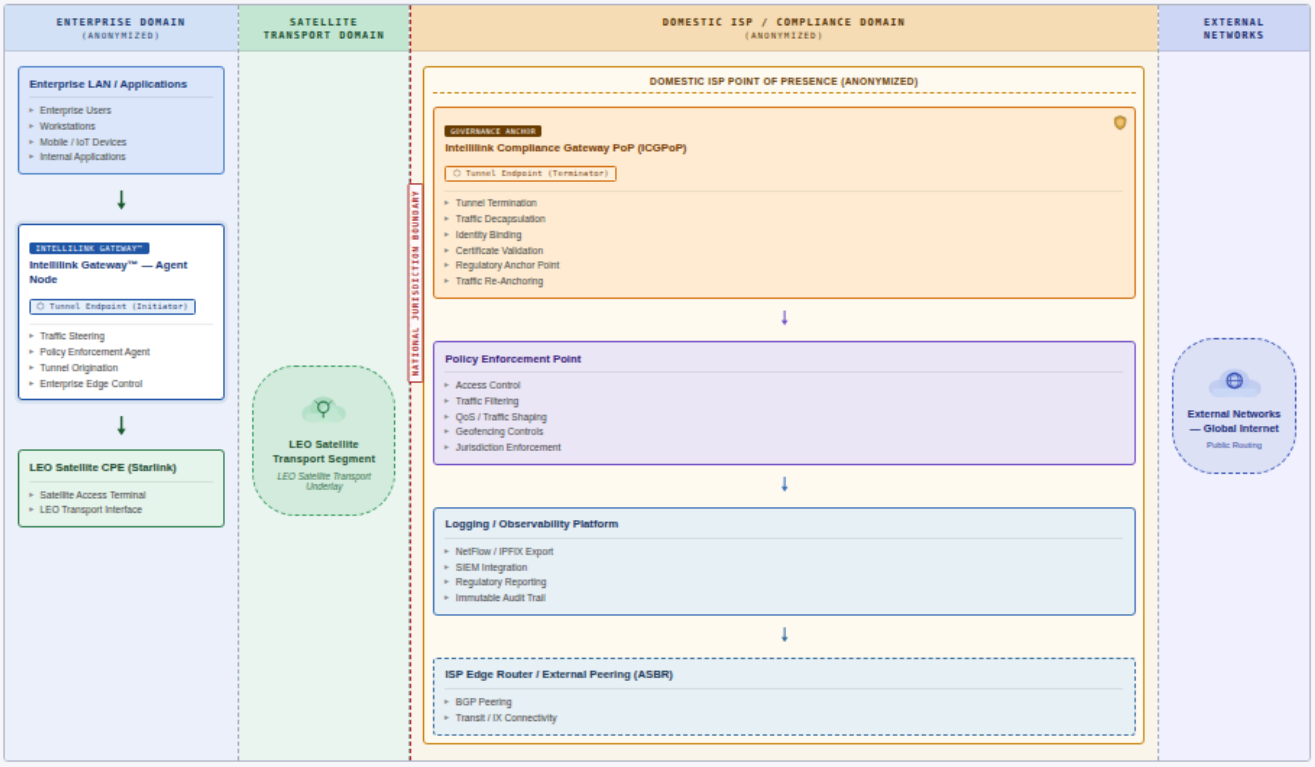
- — Commercial scalability
- — Regulatory certification or approval
- — Lawful intercept system integration (jurisdiction dependent)
- — End-user billing or retail ISP functions

SCOPE NOTICE

The items listed as out of scope are intentionally outside this validation exercise and represent natural areas for future evaluation phases.

Figure 3 — Anonymized Field Deployment Topology (Validation Test Window)

Enterprise satellite connectivity anchored through a domestic ISP compliance point to restore governance, visibility, and accountability.



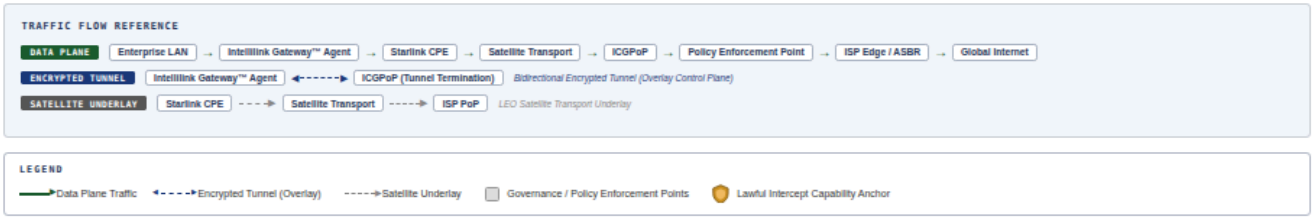


FIGURE 3 Anonymized Field Deployment Topology (Validation Test Window)

Enterprise traffic originates within the enterprise LAN and is steered by the Intellilink Gateway™ Agent through an encrypted overlay tunnel terminating at the Intellilink Compliance Gateway PoP (ICGPoP) within the domestic ISP domain. Upon tunnel termination, traffic undergoes decapsulation, identity binding, and policy enforcement before entering the ISP routing environment. No ISP names, locations, or sensitive network identifiers are disclosed.

SECTION 08

Limitations & Next Validation Steps

Future evaluation phases may include:

- Multi-site enterprise deployments at commercial scale
- Formal lawful intercept integration (jurisdiction dependent)
- Long-term performance analytics under sustained operational conditions
- Multi-satellite transport support across different orbital layers

---

SECTION 09 — SUPPLEMENTARY REFERENCE

Control Plane vs Data Plane Separation

The following diagram illustrates the architectural separation between the data plane (traffic flow) and the control plane (overlay governance), clarifying where each layer operates, where policy is enforced, and where national jurisdiction re-applies.

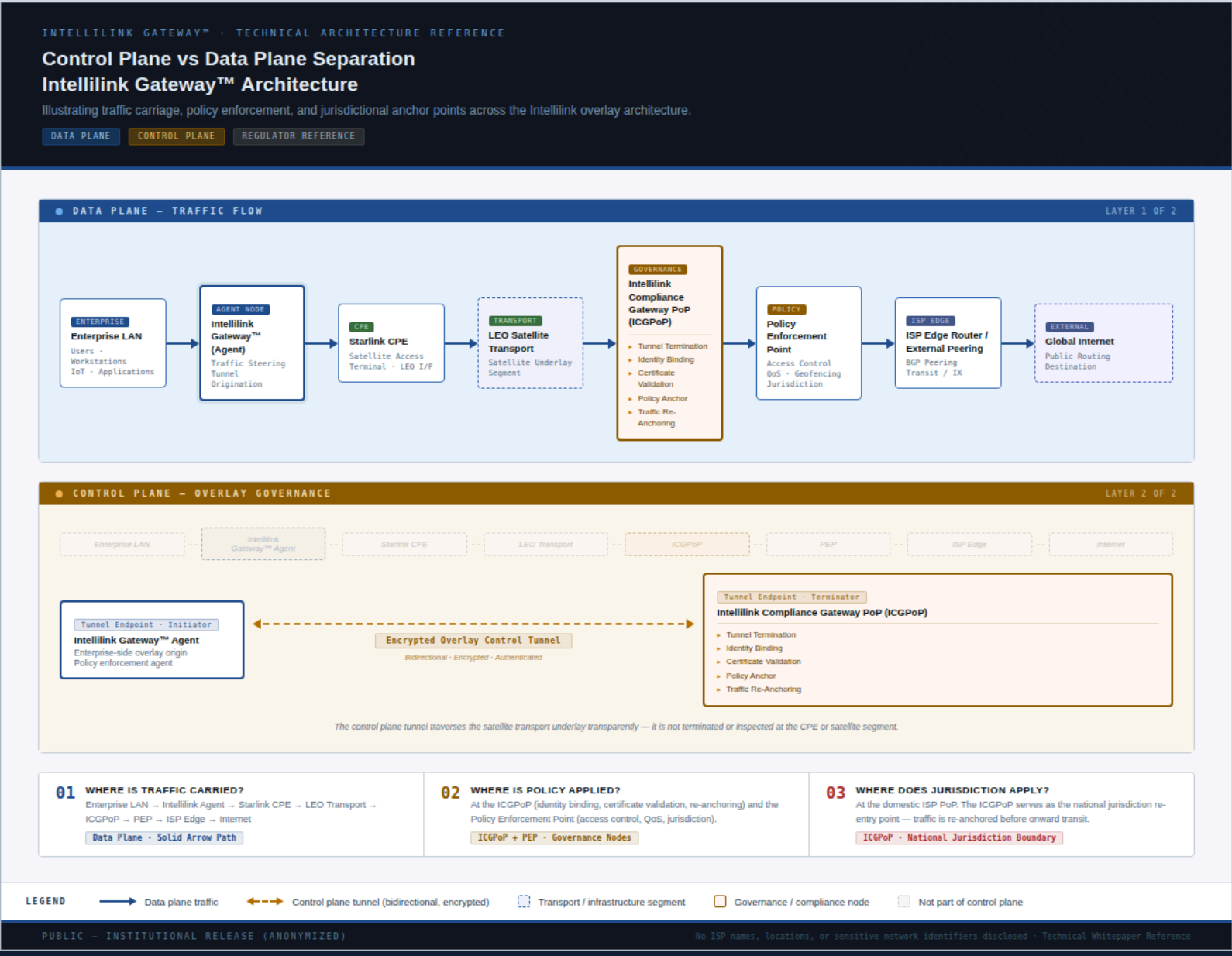


FIGURE 4 Control Plane vs Data Plane Separation — Intellilink Gateway™ Architecture

Illustrating traffic carriage, policy enforcement, and jurisdictional anchor points across the overlay architecture. The data plane carries enterprise traffic through the satellite underlay; the control plane (encrypted overlay) enforces governance at the domestic ISP PoP, independently of the satellite transport layer.

SECTION 10

Conclusion

The Intellilink Gateway™ control plane architecture has been validated under both laboratory and live field conditions. The validation confirms that satellite-connected enterprise traffic can be re-anchored within a domestic ISP governance domain without disrupting connectivity or modifying satellite access infrastructure.

> These results provide a technical foundation for informed dialogue between satellite operators, domestic ISPs, enterprises, and communications regulators — demonstrating that satellite innovation and national Internet governance principles can coexist through deliberate architectural design.

LEGAL & OPERATIONAL DISCLAIMER

This document describes a technical architecture and validation outcomes only. It does not constitute a commercial offer, regulatory certification, or service guarantee.

The Intellilink Gateway™ control plane operates independently of satellite providers and does not imply endorsement or partnership with any satellite operator.

INTELLECTUAL PROPERTY NOTICE

The Intellilink Gateway™ architecture, control-plane design, and operational workflows described herein are proprietary intellectual property of Intellilink Media LLC™.

Unauthorized reproduction or redistribution is prohibited.