INTELLILINK
GATEWAY™

FIELD CASE STUDY

Governance Restoration for Enterprise Satellite Connectivity

A controlled field validation of the Intellilink Gateway™ control plane architecture in a live enterprise satellite environment.

VALIDATION WINDOW	ENVIRONMENT	SATELLITE ACCESS
Single-Day Controlled Deployment	Live Enterprise · Anonymized	LEO (Starlink)

DOCUMENT	Field Case Study
VERSION	1.0
DATE	07 February 2026
STATUS	Field Validation Summary
PREPARED BY	Intellilink Media LLC™ (USA)
ARCHITECT	Emmanuel Mukwesa · Founder & Architect
CLASSIFICATION	Public — Institutional Release (Anonymized)

SECTION 01

Case Study Overview

This field case study documents a controlled deployment of the Intellilink Gateway™ control plane architecture in a real operational environment. The objective of the validation exercise was to determine whether satellite-connected enterprise traffic could be re-anchored within a domestic Internet Service Provider (ISP) governance domain while maintaining the resilience and accessibility benefits of low-Earth-orbit (LEO) satellite connectivity.

The deployment focused on three primary validation objectives:

- Routing control — demonstrating that enterprise traffic could be directed through a domestic ISP governance point
- Governance anchoring — confirming that traffic became visible and accountable within a domestic network environment
- Tunnel stability — validating that the encrypted control plane remained stable under live operational conditions

The exercise was conducted as a single-day validation window, using live enterprise traffic while applying strict anonymization to all participating entities.

SECTION 02

Test Environment

The validation deployment consisted of five interconnected components operating in a live enterprise environment:

ENTERPRISE SITE	An operational enterprise network generating normal Internet traffic. Anonymized for public distribution.
SATELLITE ACCESS LAYER	Connectivity provided by a low-Earth-orbit satellite Internet service (Starlink), serving as the access transport underlay.
GATEWAY NODE	An Intellilink Gateway™ Agent Node deployed adjacent to the enterprise satellite terminal, responsible for tunnel origination and policy enforcement.
DOMESTIC ISP POP	An anonymized domestic ISP Point of Presence serving as the governance anchor point for traffic decapsulation, policy enforcement, and regulatory anchoring.
EXTERNAL NETWORK	Standard Internet destinations accessed through the ISP's external transit connectivity, used to verify end-to-end routing path integrity.

All infrastructure participants were anonymized for this public document. No enterprise customer data was retained beyond transient packet forwarding.

SECTION 03

Deployment Architecture

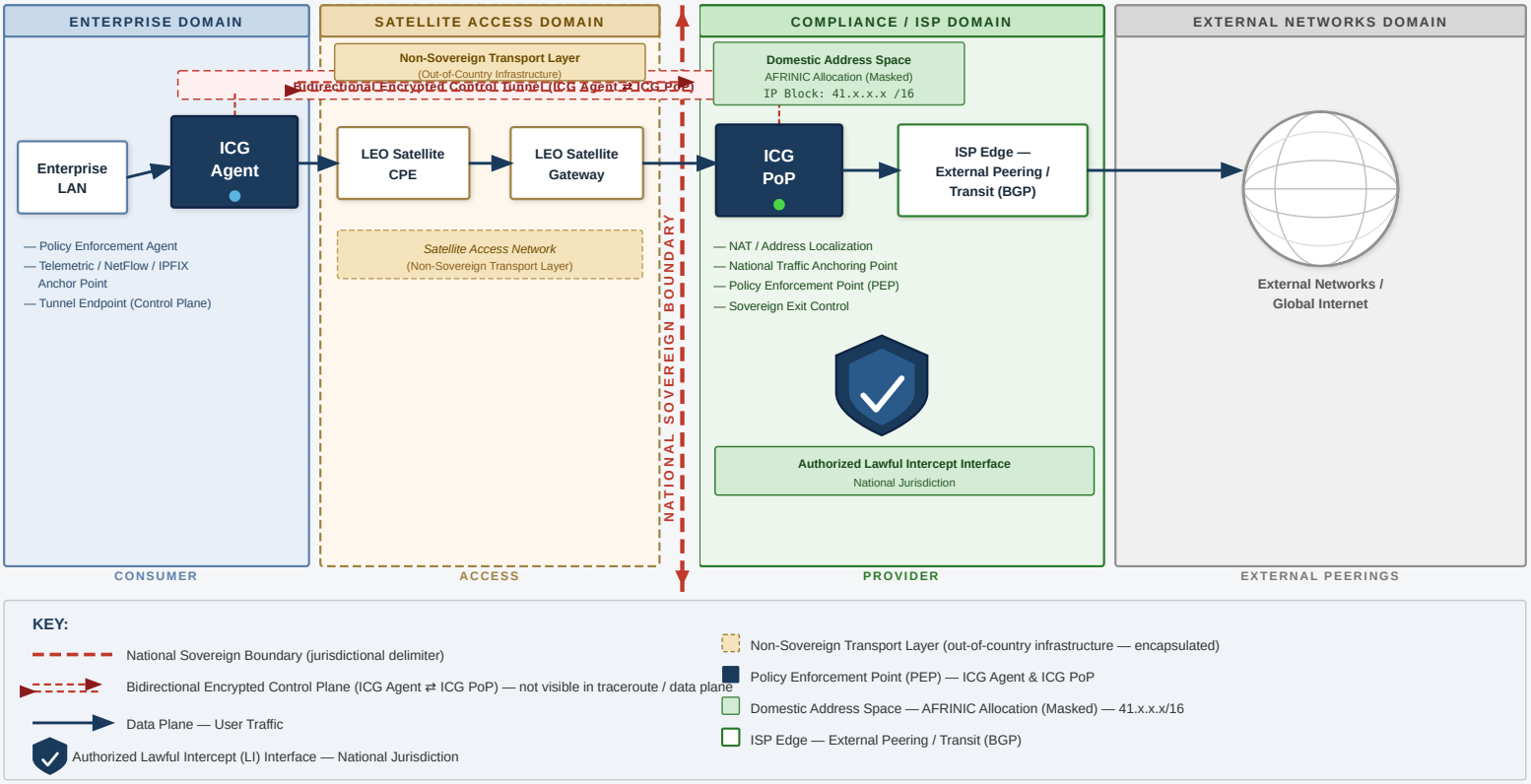
The deployment architecture introduced an overlay governance control plane on top of an existing satellite transport layer. Enterprise traffic originating within the enterprise LAN was first processed by the Intellilink Gateway™ Agent Node, which established an encrypted tunnel toward the Intellilink Compliance Gateway PoP (ICGPoP) located within the domestic ISP domain.

Satellite connectivity served purely as a transport underlay, while governance functions — including traffic decapsulation, policy enforcement, logging, and regulatory anchoring — occurred exclusively within the ISP PoP environment. This architecture effectively separated connectivity transport from governance enforcement, allowing the satellite access layer to remain unchanged while restoring domestic governance visibility.

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™ Architecture Deployed During Field Validation

This diagram illustrates the logical architecture deployed during the validation exercise — the separation between the satellite transport layer (underlay) and the governance control plane anchored within the domestic ISP domain. All IP addresses and infrastructure identifiers are masked for anonymity.

SECTION 04

Routing Behaviour Before Deployment

Prior to deploying the Intellilink Gateway™ control plane, enterprise traffic exited the satellite network directly through upstream satellite provider routing paths. In this configuration, traffic did not traverse a domestic ISP governance anchor point prior to reaching the broader Internet.

This baseline behaviour reduced domestic governance visibility because:

- Upstream accountability was ambiguous — the effective routing authority was the satellite provider's external infrastructure
- Traffic inspection points were absent within national networks prior to external Internet egress
- Routing behaviour was externally determined by satellite provider infrastructure, outside domestic regulatory reach

Traceroute measurements taken during this baseline stage confirmed that traffic exited the satellite transport network into external transit providers before any domestic ISP routing was observed.

SECTION 05

Routing Behaviour After Deployment

Following deployment of the Intellilink Gateway™ Agent Node, enterprise traffic was encapsulated into an encrypted overlay tunnel directed toward the domestic ISP governance PoP. Upon arrival at the ICGPoP, traffic underwent sequential processing:

01 **Tunnel termination** — the encrypted overlay tunnel was terminated at the domestic ISP PoP

02 **Traffic decapsulation** — encapsulated packets were extracted and presented to the ISP routing environment

03 **Identity binding** — enterprise traffic identity was established within the ISP address space

04 **Policy enforcement** — network policy controls were applied at the ISP PoP before external egress

05 **Observability logging** — flow-level records were generated within the domestic ISP environment

After processing, traffic was routed through the ISP's external peering infrastructure before reaching the public Internet. Traceroute measurements confirmed that enterprise traffic entered the domestic ISP routing environment prior to external Internet transit, demonstrating successful traffic re-anchoring within the domestic governance domain.

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)

Technical Reference Diagram

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	✔ AFTER ICG
17 hops / 242 ms	7 hops / 302 ms
8 foreign ASN hops | No LI capability	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 ASNS)
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	41.181.190.133	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 Behaviour Before and After Intellilink Gateway™ Deployment — Technical Reference Diagram

The comparison illustrates how enterprise satellite traffic that previously exited through external upstream paths becomes anchored within a domestic ISP Point of Presence after deployment of the Intellilink Gateway™ governance control plane. Traceroute data confirms routing re-anchoring within domestic ASN space.

SECTION 06

Governance Restoration

The deployment demonstrated that enterprise satellite connectivity could be integrated into a conventional ISP governance model without modifying the satellite access infrastructure. The following governance properties were successfully restored:

ACCOUNTABLE UPSTREAM PRESENCE

Enterprise traffic visibly entered a domestic ISP Point of Presence, establishing a clear and auditable governance boundary.

ADDRESS SOVEREIGNTY

Enterprise traffic appeared under ISP-controlled addressing space following tunnel termination, restoring domestic address accountability.

TRAFFIC OBSERVABILITY

Flow-level inspection and logging were possible within the ISP environment, enabling oversight without satellite infrastructure modification.

POLICY ENFORCEMENT

Network policy controls could be applied prior to external Internet transit, restoring jurisdictional enforcement capability.

These characteristics align with regulatory expectations for accountable Internet traffic flow within national communications frameworks.

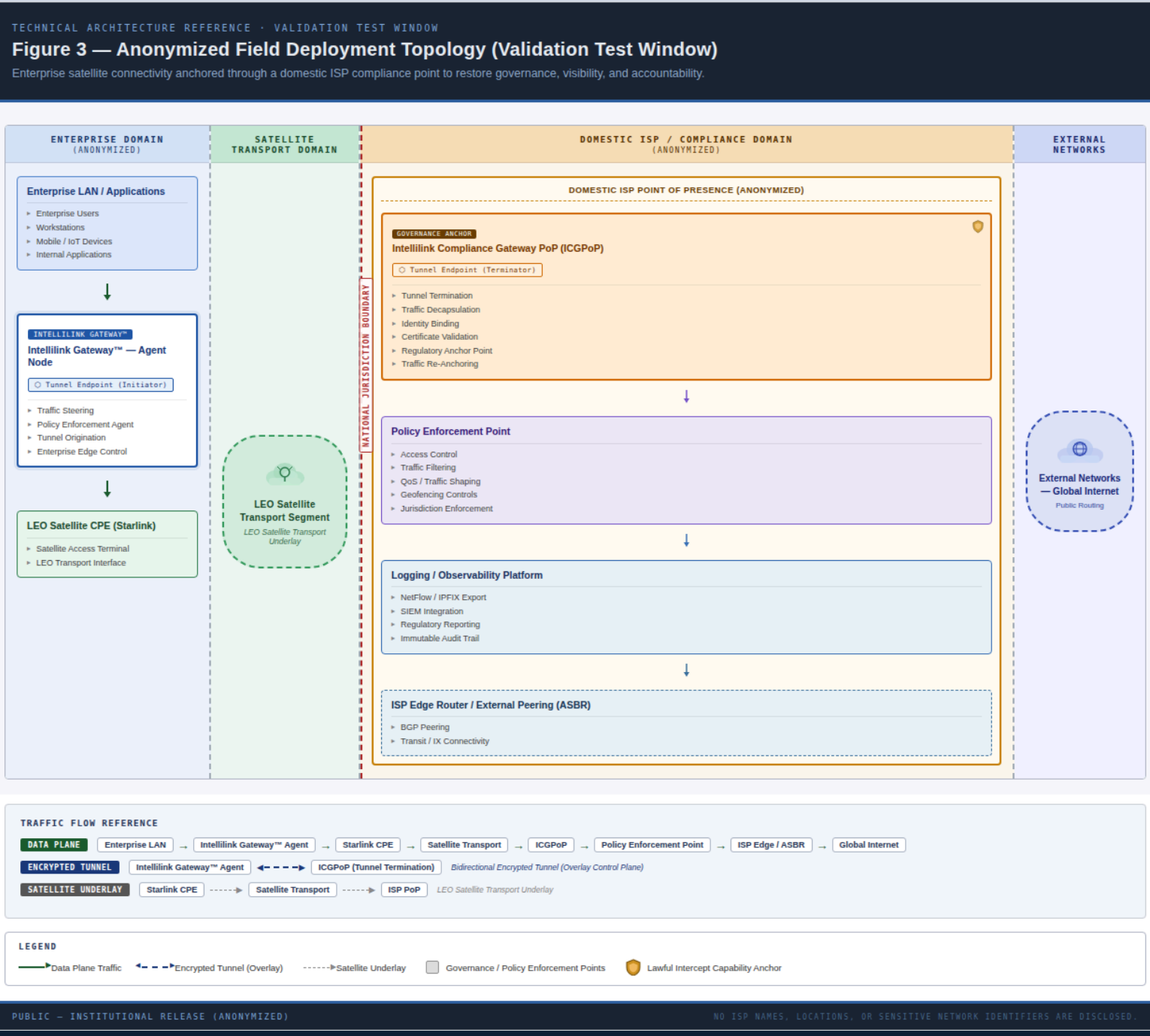


FIGURE 3 Anonymized Field Deployment Topology (Validation Test Window)

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. Logging and governance enforcement occur prior to external Internet transit. No ISP names, locations, or sensitive network identifiers are disclosed.

SECTION 07

Operational Observations

Throughout the one-day validation window, the system demonstrated stable and predictable operational behaviour. Key observations included:

- ✔ Encrypted tunnel stability was consistent throughout the validation window with no observable interruptions
- ✔ Routing behaviour after governance anchoring was predictable and conformed to expected traceroute patterns
- ✔ No observable disruption to enterprise browsing activity — end-user experience was maintained throughout
- ✔ Policy insertion capability at the ISP PoP was confirmed functional
- ✔ Enterprise applications functioned transparently without requiring modifications to end-user systems or configurations

SECTION 08

Limitations of the Validation Window

The field validation was intentionally limited in scope to establish proof of concept under controlled conditions. The exercise did not evaluate:

OUT OF SCOPE — REQUIRES FURTHER EVALUATION

- Commercial-scale enterprise deployments involving multiple simultaneous sites
- Long-duration operational stability beyond a single-day validation window
- Lawful intercept system integration and associated compliance verification
- Enterprise billing models or retail ISP service functions

These areas represent natural progression for future validation phases and are noted for completeness.

SECTION 09

Conclusion

The field validation demonstrates that enterprise satellite connectivity can be integrated into domestic Internet governance frameworks through the use of an overlay control plane architecture. The Intellilink Gateway™ model successfully restored ISP anchoring, routing accountability, and policy enforcement capabilities while maintaining the resilience benefits of satellite connectivity.

These results indicate that satellite innovation and national Internet governance principles can coexist when integration is approached through deliberate architecture design. The Intellilink Gateway™ model provides a replicable framework for regulators, network operators, and enterprise organizations seeking to address the governance challenges posed by satellite Internet adoption.

LEGAL & INTELLECTUAL PROPERTY