Case Study

THALES

CYBERSECURITY

Customer-Controlled Encryption over LEO Satellite Networks

Enhancing Confidentiality, Control, and Quantum Readiness for Starlink-connected Environments or for organizations using Starlink connectivity

cpl.thalesgroup.com

THALES

CYBERSECURITY

Low-Earth-Orbit (LEO) satellite constellations such as Starlink are redefining global connectivity by offering high-throughput, low-latency communications across the most remote environments. Yet as data traverses networks that span multiple jurisdictions and operators, encryption trust boundaries become blurred.

Who ultimately controls the cryptographic keys and algorithms— the provider such as SpaceX or the customer—and determines whether sensitive data remains confidential, compliant, and future-proof against quantum threats.

This paper examines provider-managed LEO connectivity security models, using Starlink as a reference example, and outlines how customer-controlled encryption can extend confidentiality and compliance for mission-critical users.

Key insights:

- **Native transport protections in Starlink-based deployments** secures radio and satellite links with AES-based encryption, but all keys and firmware controls remain under SpaceX management.
- **Decryption occurs inside SpaceX ground infrastructure**, which creates a potential attack vector before the data re-enters controlled networks.
- **End-to-end assurance requires overlay encryption** managed by customers—typically through certified hardware encryptors or VPN appliances.
- **Compliance frameworks** (FIPS 140-3, Common Criteria, DISP, ITAR) increasingly mandate customer key ownership and verifiable cryptographic boundaries—requirements that a provider-managed native transport model alone cannot meet.
- **Quantum-safe readiness** can be achieved immediately through customer-controlled hybrid or post-quantum encryption overlays, independent of the provider's upgrade path.

1. Introduction and Motivation

1.1 The LEO Revolution

LEO constellations orbiting 500–1,200 km above Earth are rapidly transforming global communications. With thousands of satellites in dynamic mesh networks, providers such as Starlink, OneWeb, and Kuiper now deliver broadband connectivity with 30–50ms latency—comparable to terrestrial fibre.

This capability is invaluable for defense, mining, aviation, maritime, and humanitarian missions operating beyond terrestrial infrastructure.

1.2 Why Encryption Over LEO Matters

Unlike private terrestrial networks, LEO systems cross dozens of national borders in minutes. Terminals, satellites, and gateways often reside in different jurisdictions.

Even if traffic is encrypted in transit, control over where decryption occurs and who holds the keys determines whether data remains sovereign and compliant.

For defense, finance, and energy sectors, link encryption managed by a foreign operator is insufficient; these organizations require end-to-end cryptographic control.

1.3 Market Drivers

- **Adoption and Integration:** Over 10,000 LEO satellites are expected by 2025. Starlink alone exceeds four million users, and enterprises are embedding LEO links into SD-WAN and cloud architectures.
- **Growing Cyber-Physical Risk:** A 2022 satellite attack highlighted vulnerabilities in ground-segment systems, reinforcing that encryption without independent key control offers only partial protection.
- **Regulatory Pressure:** Frameworks such as GDPR, Australia's PSPF, and U.S. FedRAMP increasingly demand domestic cryptographic custody. Classified networks require FIPS- or Common Criteria-validated modules.
- **Quantum Threats:** Data encrypted today may be harvested for later decryption once quantum computers mature. Post-quantum or hybrid key exchange implemented at customer-owned layers provides forward secrecy and long-term resilience.

1.4 From Trust to Control

Satellite operators were once trusted by default, but modern zero-trust architectures assume no implicit carrier trust. As in the cloud security evolution of the past decade, the model is shifting toward "encrypt everything above the provider layer—and own the keys."

2. LEO Connectivity Model: Starlink Example

2.1 Architecture and Traffic Flow

A Starlink-based connectivity deployment typically includes four components:

1. **User Terminal (UT):** The ground antenna and modem ("Dishy").
2. **LEO Satellites:** Thousands of nodes in multiple orbital shells, increasingly linked via optical inter-satellite links (ISLs).
3. **Ground Gateways:** Fibre-connected earth stations bridging satellites to the terrestrial internet.
4. **Network Operations Infrastructure:** SpaceX systems managing authentication, firmware, and key distribution.

Traffic follows a predictable path: encrypted uplink from UT → satellite → ground gateway → decryption → terrestrial handoff.

The customer's private LAN sits behind a carrier-grade NAT boundary; all physical and link-layer encryption is provider-controlled.

2.2 Deployment Scenarios

- **Broadband Access:** Fixed or mobile connectivity for remote enterprises and communities.
- **Corporate Links:** Integration into MPLS or SD-WAN for field operations.
- **Maritime and Aviation:** High-gain mobile terminals for global coverage.
- **IoT and Tactical Networks:** Rapidly deployable connectivity for telemetry and command networks.
- **Government Use:** Often constrained to unclassified missions unless augmented by overlay encryption.

2.3 Private Network Extensions

Through global providers like **Vocus** and **SpeedCast**, Starlink connectivity can be integrated into private Layer 3 VPNs or encapsulated with Layer 2-over-Layer 3 tunnels (VXLAN, GRE). These methods allow fixed addressing and VLAN extension but **do not alter the provider-controlled trust model**—traffic is still decrypted at SpaceX gateways.

3. Security of Information Over Starlink

In Starlink-based transport environments, AES-256 encryption protects communications between terminals and satellites, with dynamic key rotation and mutual authentication. Gateways are hardened, and management channels use TLS 1.3. However, all encryption, firmware, and key management remain under provider control.

3.1 Encryption Boundaries

- Air Interface: AES-256 secures Ku/Ka-band transmissions; keys are provisioned and rotated by SpaceX.
- Ground Segment: Traffic is decrypted at gateways before entering the terrestrial backbone; beyond this, security relies on customer VPNs or TLS.
- Management Plane: Telemetry is encrypted via TLS but terminates in SpaceX's infrastructure, exposing operational metadata.

3.2 Trust Dependencies

- **Ground-Station Integrity:** Customers rely on SpaceX's jurisdictional controls and insider-threat mitigation.
- **Firmware Supply Chain:** Updates are signed and pushed automatically; customers cannot audit or freeze firmware versions.
- **Key Management:** All cryptographic material is generated and held by SpaceX.
- **Operational Opacity:** Customers lack visibility into incident response and audit logs.
- **Legal Exposure:** Data traversing U.S. or partner jurisdictions may be subject to lawful access or subpoena.

Result: Native Starlink transport protections provide strong protection against interception but do not provide customer-owned end-to-end confidentiality or sovereign key control.

4. Why Customer-Controlled Encryption Is Essential

4.1 Principle

Customer-controlled encryption ensures that only customer-owned equipment ever processes plaintext. The provider delivers transport; the customer enforces confidentiality. This model introduces separation of duties, verifiable compliance, and a direct path to quantum-safe cryptography.

4.2 Key Ownership and Separation of Duties

- **Exclusive Key Custody:** Providers see only ciphertext, neutralizing risks from subpoenas or insider access.
- **Crypto Agility:** Customers choose algorithms, lifetimes, and rekey intervals to match their risk model.
- **Operational Transparency:** Local endpoints log cryptographic events into the organization's SIEM for auditability.
- **Functional Separation:** The satellite operator handles RF and routing; the customer manages encryption and key lifecycle, enforcing least-privilege principles.

4.3 Compliance and Certification Alignment

Overlay encryption enables direct adherence to recognised standards:

- **FIPS 140-3:** Certified modules define a trusted cryptographic boundary independent of the provider.
- **Common Criteria (EAL4+):** Demonstrates rigorous design and evaluation.
- **ISO 27001 Controls:** Strengthen policy enforcement and supplier risk management.
- **Sector-Specific Regulations:** Defense and critical-infrastructure programs require national key custody and auditable crypto policy.

Customer-owned overlays provide tangible compliance artefacts—FIPS/CC certificates, HSM logs, key-ceremony records, and configuration baselines—proving governance and control.

5. Quantum Readiness and Future-Proofing

Quantum computing threatens RSA and ECC key exchanges. The provider-managed encryption lifecycle in Starlink-based deployments is opaque to users, but overlay encryptors can deploy hybrid or post-quantum algorithms immediately.

By managing keys and algorithms independently, customers can transition at their own pace, ensuring harvest-now, decrypt-never protection for sensitive data.

Conclusion

Starlink and other LEO constellations deliver transformative connectivity, but the inherent provider-controlled trust model leaves gaps for classified, sovereign, or regulated use cases.

Customer-controlled encryption closes these gaps—ensuring:

- Complete key ownership and jurisdictional control,
- Built-in compliance evidence for audits,
- Seamless migration to quantum-safe algorithms, and
- Predictable, high-performance confidentiality over any link.

In short, it converts Starlink connectivity from "secure transport you must trust" into confidential transport you control.

Encryption Approaches for Starlink Connectivity

Standard residential Starlink services operate behind **Carrier-Grade Network Address Translation (CG-NAT)**, where multiple customers share a single public IPv4 address. While efficient for conserving address space, CG-NAT blocks unsolicited inbound traffic—preventing users from hosting servers, accessing remote SSH sessions, or establishing inbound VPNs.

This architecture complicates **IPSec VPN** deployment. IPSec's **Encapsulating Security Payload (ESP)** protocol runs directly over IP without port numbers, which NAT devices rely on for session mapping. As a result, ESP packets can be dropped or misrouted by Starlink's CG-NAT gateway. To overcome this, **NAT Traversal (NAT-T)** encapsulates IPSec packets within **UDP port 4500**, allowing NAT devices to pass encrypted traffic as standard UDP. Yet, NAT-T adds overhead: roughly **28 bytes** per packet from additional IP/UDP headers, reducing MTU, increasing fragmentation, and introducing extra CPU and latency burdens—especially on routers lacking hardware acceleration.

Thales High Speed Encryption (HSE)

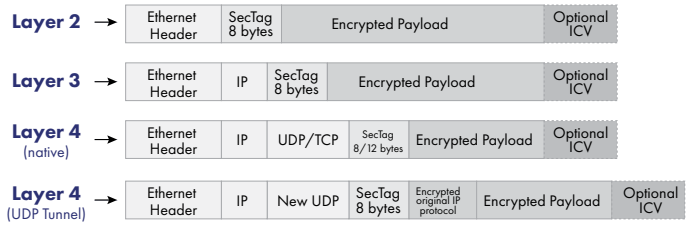
Thales HSE delivers certified, quantum-safe security with negligible latency—less than 10 µs per device—by performing hardware-based, tunnel-free encryption at Layers 2–4, as shown in Figure 1.

Unlike IPSec, which encapsulates and tunnels each packet, Thales native Layer 4 encryption integrates directly with TCP or UDP (optionally adding only a lightweight UDP header to secure protocols other than TCP/UDP).

This approach maintains **line-rate performance**, avoids IPSec's encapsulation and fragmentation penalties, and preserves QoS and routing transparency—critical for **LEO satellite links** with 40–60ms round-trip times.

Combined with **FIPS 140-3 Level 3** and **Common Criteria EAL4+** certifications, and support for **post-quantum** and **Quantum Key Distribution (QKD)** capabilities, Thales encryptors offer sovereign, standards-validated, and **NAT Thales High Speed Encryptors** designed for Starlink and other LEO environments.

Figure 1 - HSE Encryption Layers



Comparison to IPSec

When comparing equivalent Senetas HSE and IPSec encryption modes , there is a 72% reduction in the additional overhead, with further savings achieved by disabling GCM authentication. The IPSec and HSE equivalent packet formats are shown in Figure 2.

GCM authentication. The IPSec and HSE equivalent packet formats are shown in Figure 2.

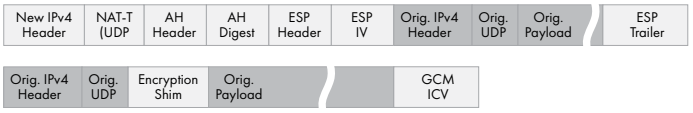


Figure 2 - Encrypted packet formats, IPSec (top) and HSE Layer 4 Encryption overhead highlighted

The efficiency of an encryption solution depends not only on its raw cryptographic performance but also on how effectively it manages protocol overhead. In real-world networks, smaller packets suffer a proportionally greater loss of throughput because headers, authentication tags, and padding consume a larger fraction of each frame.

This effect is illustrated in Figure 3 comparing available bandwidth across varying payload sizes for IPSec and Senetas HSE, with and without GCM authentication. The results clearly demonstrate that HSE devices deliver higher throughput efficiency—especially with small packets—due to their hardware-based encryption engine and optimized packet handling architecture.

The impact of the differing overhead increases significantly as the packet size decreases, as shown in Figure 3.

Website: IPSec Calculator Comparing Senetas AES256-GCM (24-byte shim) encryption with IPSec AH-SHA-HMAC + ESP-GCM256 + NAT-T (88-byte header)

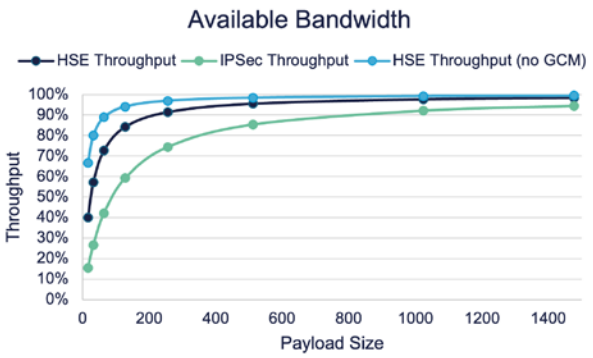


Figure 3: Available Bandwidth per Payload Size

Choice of Encryption Mode

For standard residential Starlink connections operating behind CG-NAT, the recommended setup is Layer 4 encryption with the HSE, as shown in Figure 5. This embeds encryption within TCP or UDP flows, maintaining full NAT compatibility and true end-to-end confidentiality.

Starlink's higher-tier services introduce new routing options that affect where encryption is best deployed.

The key benefits of the different services supplied are outlined in Figure 4.

Public IP Access with Bypass Mode

Under Local or Global Priority tiers, Starlink can assign a dedicated public IPv4 address, bypassing CG-NAT and enabling direct VPN or peer-to-peer connections. The Starlink router still performs NAT by default, mapping private LAN addresses to this public IP.

Enabling Bypass (Bridge) Mode on the Starlink terminal disables NAT entirely, assigning the public IP directly to downstream equipment. This removes double NAT and allows use of enterprise routers and security appliances.

Figure 4 - Recommended Encryption Layer

Starlink Configuration	Encryption Layer	HSE Deployment	Key Benefits
Standard Residential (CG-NAT)	Layer 4 – Embedded within TCP/ UDP flows	Inline before Starlink terminal.	• Seamless NAT traversal • Minimal configuration • Deterministic performance • End-to-end confidentiality
Local/Global Priority with Bypass Mode	Layer 3 – Direct public IP to downstream device	Inline HSE between modem and enterprise router (no NAT)	• Eliminates double NAT • Full customer router & NAT control

Network & HSE Configuration

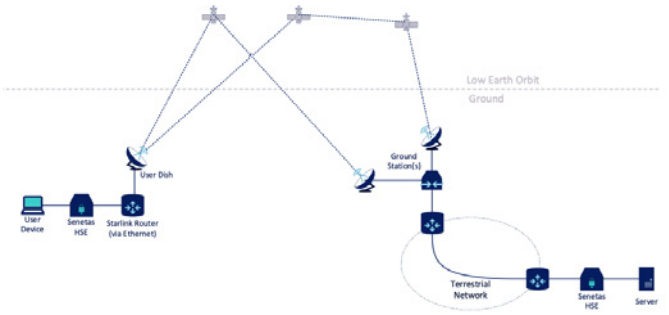


Figure 5 - Network Diagram

Reliable encryption deployment over Starlink requires coordination between network topology and device configuration, as shown in Figure 5. The following procedure establishes a secure, low-latency, and transport-independent encrypted link between a remote endpoint and a server using the HSE. These steps configure encryption for traffic between the remote user and the target server while allowing unencrypted connections to other destinations.

Step	Action	Details / Notes
1	Identify Server IP & Ports	Determine the server's IP address and any port forwarding requirements. This defines the target scope for encryption.
2	Activate Encryptors	Power on both encryptors and verify operational status. Ensure connectivity and basic management access before proceeding.
3	Enable Transport Independent Mode	Configure both encryptors in Transport Independent Mode (TIM) to maintain link integrity across dynamic Starlink transport variations and NAT traversal.
4	Add Key Distribution Key (KDK)	Load a common KDK on both encryptors to establish a secure, mutually authenticated channel..
5	Set PMTU	Configure PMTU Max = 1500 on each encryptor to optimize throughput and avoid fragmentation.
6a	Configure Remote Encryptor Rules	- Set Unlisted Default Action = Bypass.- Add IP rules to Encrypt L4 for all UDP and TCP traffic directed to the server.
6b	Configure Server Encryptor Rules	- Set Unlisted Default Action = Encrypt L4.- Ensure consistent rule definitions for symmetric policy enforcement..
7	Enable Encryption	Set both encryptors to global Encrypt mode to activate end-to-end protection.

Performance Verification

Throughput validation using iPerf demonstrated that enabling HSE encryption resulted in only ~1% performance reduction, with test variance attributed to normal Starlink network fluctuations. This confirms the effectiveness of the configuration in preserving link efficiency while delivering robust confidentiality.

Technical Rationale

Transport Independent Mode (TIM) ensures reliable encryption across adaptive routing and NAT environments, in Starlink-based deployments while Layer 4 encryption provides end-to-end confidentiality with minimal configuration overhead. The combination enables cryptographic assurance without compromising usability or performance.

About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

Thales and the Thales logo are trademarks or service marks of Thales and/or its subsidiaries. All other product names, trademarks, and registered trademarks are property of their respective owners.

© Thales - February 2026 • AC. v5