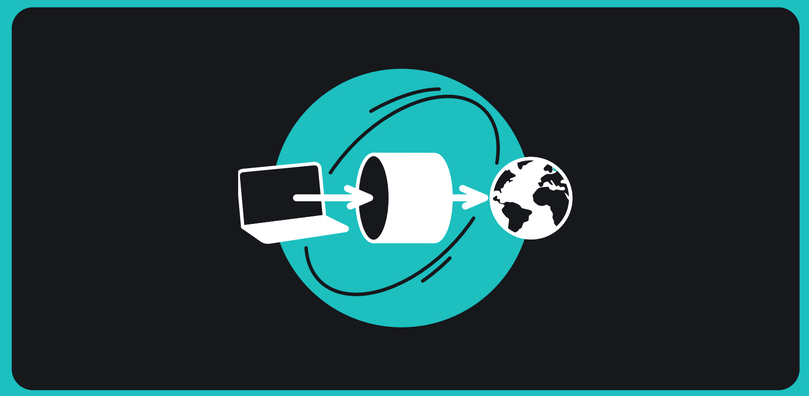
Surfshark's new Dausos protocol: Technical overview

The industry's first customer-centric protocol that boosts speeds by up to **30%**

DAUSOS AT A GLANCE

Dausos is Surfshark's proprietary VPN protocol **engineered for consumer use**, combining high throughput, low overhead, and a fully post-quantum secure design.



Each user gets a **dedicated, private data tunnel** with a split-plane architecture (stateful control, stateless data) to minimize shared server logic and contention.

A hybrid post-quantum key exchange (X25519 + ML-KEM/Kyber768) establishes session keys, self-signed ML-DSA certificates provide peer validation, and **AEGIS-256X2 protects the data channel**.

The result: Consistently higher speeds, stronger user isolation, and future-ready security.

THE PROBLEM

In most consumer VPN setups, multiple users have to share the same processing path around a virtual TUN interface. This creates several constraints:

Poor scalability

Shared logic makes it harder to handle more users smoothly. One-size-fits-all settings (e.g., MTU, batching, worker counts) can force trade-offs across all users instead of optimizing per session.

Restricted performance

Processing every packet on a shared path adds overhead before decryption, which can increase latency and reduce throughput under load. Shared queues and worker pools also amplify “noisy neighbor” effects, as one heavy user can degrade others.

Limited isolation and control

When multiple users share the same datapath, the risk of cross-tenant interference rises. It’s also harder to adjust settings per user and change behavior dynamically, reducing overall efficiency.

THE SURFSHARK DAUSOS DIFFERENCE

Dausos is the first VPN protocol of its kind to give each user their own dedicated private data tunnel, delivering immediate benefits:

Faster speeds

By removing shared datapaths and packet inspection on the data channel, Dausos reduces overhead and can increase user **speeds by up to 30%** compared to other protocols supported by Surfshark.

Enhanced privacy

Fully separated data channels **reduce cross-user correlation**, metadata leakage, and shared exposure.

Stronger security

Sessions use TLS 1.3 with a hybrid X25519 + ML-KEM/Kyber-768 key exchange, ML-DSA certificates for authentication, and AEGIS-256X2 to protect your data.

Lower latency

Per-user workers plus tunable MTU and batching reduce queue buildup and jitter, **smoothing performance on congested links**.

Better reliability

Built-in no-net checks and self-healing allow for **quick recovery from network changes** through reconnection or pulling fresh server IPs via our Everlink service.

More stability

Per-user tunnels and dedicated UDP bindings **minimize any "noisy neighbor" impact**, helping prevent one user's behavior from affecting others.

Per-user optimization

MTU, batching, and read/write worker counts are configurable per session. Users can tune settings for **high bandwidth, battery savings, or a balanced profile**.

Dausos allows achieving 30% higher speeds compared to existing Surfshark protocols, enhances security with post-quantum security, and configures a dedicated tunnel for data traffic automatically, depending on network conditions, and ensures smooth, uninterrupted connectivity.

— Karolis Kačiulis,
Leading System Engineer at Surfshark

KEY TECHNICAL DIFFERENTIATORS

Strict UDP binding

A VPN server running Dausos locks each session to the client IP address and UDP source port that establish the data channel, so the operating system automatically drops packets from any other source, reducing the risk of traffic injection.

Post-quantum secure cryptography

Sessions use **TLS 1.3 with a hybrid key exchange (X25519 curve + ML-KEM)** to establish shared secrets and **ML-DSA for server verification**. All data is **protected with AEGIS-256X2 encryption**.

No packet tampering or inspection

Dausos avoids packet parsing on the data channel to dramatically **improve connection speed and minimize data leaks**.

Each user can adjust their tunnel — on both the server and client side — without affecting anyone else. Rather than having one standard for everyone, the tunnel can be fine-tuned based on your network. It feels like having your own server, even when you're sharing it with hundreds of other users.

— Nikodemas Žaliauskas,
Senior System Engineer at Surfshark

QUICK LOOK: AEGIS-256X2

AEGIS-256X2 is a cutting-edge AEAD cipher designed for high speed and strong security with 256-bit keys. It provides confidentiality, integrity, and authenticity in a single pass, making it well-suited for VPN data channels.

Why it matters:

Maximum throughput

AEGIS-256X2's efficient, parallel-friendly design reduces per-packet overhead, minimizing latency;

Robust protection

256-bit authenticated encryption secures traffic and detects tampering;

Future-proofing

Combined with Dausos's hybrid post-quantum key exchange and periodic rekeys, AEGIS-256X2 helps keep sessions resilient against emerging threats.

AEGIS delivers high-quality authenticated encryption, guaranteeing both efficiency and high performance. This, combined with enhanced speeds, allows us to advance current VPN technology and offer users a faster, more secure VPN experience.

— Karolis Kačiulis,
Leading System Engineer at Surfshark

HOW DAUSOS WORKS

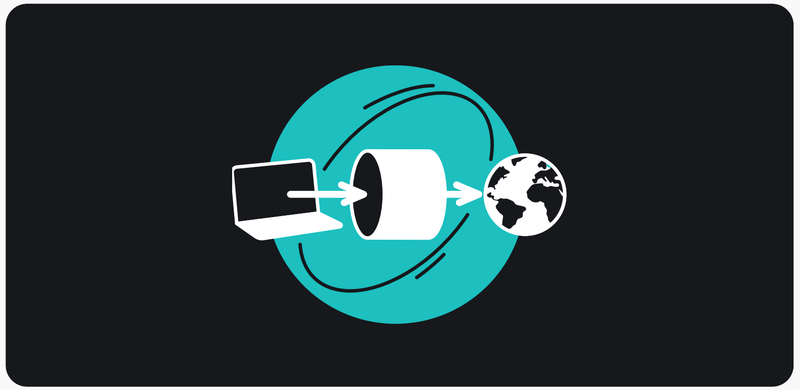
1. Connection and key exchange

Your Surfshark app **opens a secure control channel** (HTTPS over TLS 1.3) to the VPN server. Built-in ML-DSA root certificates are used to verify the server's identity.

During this secure negotiation, the **client and server run a hybrid key exchange** (X25519 + ML-KEM/Kyber768) to derive shared session keys, and the server returns session details (UDP port, internal IPs, MTU, rekey interval).

With keys established, the control channel finalizes setup so your d**ata can flow over an encrypted path**.

2. Private tunnel creation

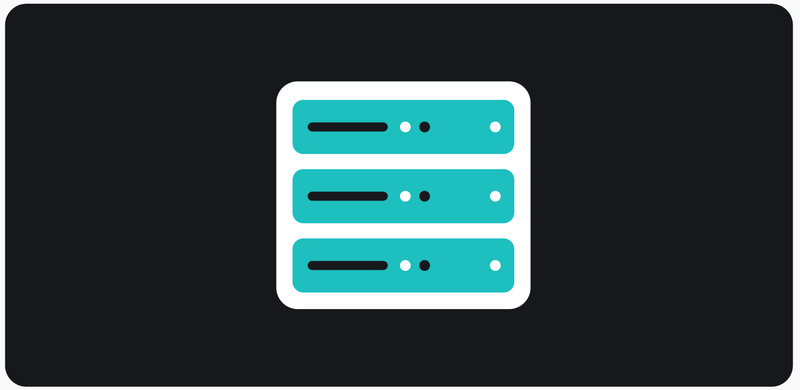


Dausos brings up a dedicated TUN interface for your session on both your device and the VPN server.

It **assigns /31 internal addresses** and binds a single UDP socket to carry your data.

The stateless data channel is protected with AEGIS-256X2, **encrypting everything that leaves the TUN and decrypting everything that arrives**.

3. Data transmission and synchronization



Your traffic flows through the **encrypted UDP data channel** to the VPN server.

The VPN server forwards traffic to the internet and back — **keeping your IP hidden and your data protected**.

Dausos periodically rekeys over the control channel to **achieve post-compromise security**, swapping in fresh keys without interrupting your connection.

WHY CHOOSE DAUSOS?

Faster in the real world

Get higher throughput and lower jitter, especially on congested or high-latency networks.

More consistent privacy

Dedicated tunnels reduce cross-user exposure and metadata bleed by design

Fewer slowdowns

Per-user isolation limits how other users' behavior affects you on shared servers.

Quicker recovery

Built-in reachability checks and self-healing help you bounce back after hiccups and network changes.

Future-proof security

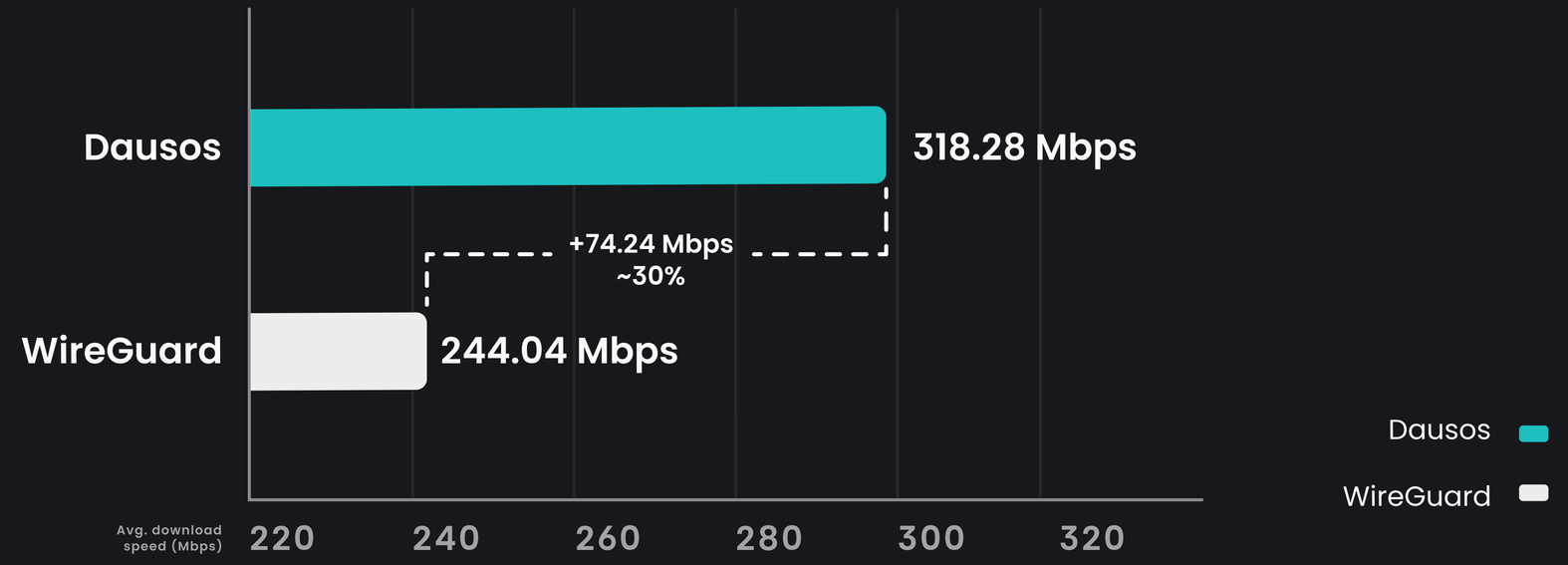
Protect yourself with hybrid post-quantum key exchange plus 256-bit authenticated encryption and periodic relays.

DAUSOS VS. WIREGUARD: SPEED TESTS

Dausos is built to deliver the fastest, most efficient VPN experience. The protocol offers each user a dedicated tunnel, so your connection doesn't share resources with any others.

In our head-to-head speed tests, Dausos users achieved average download speeds up to 30% higher than those on WireGuard.

Note: Dausos might not be faster than WireGuard in all conditions. Performance can vary by network, server, and use case.



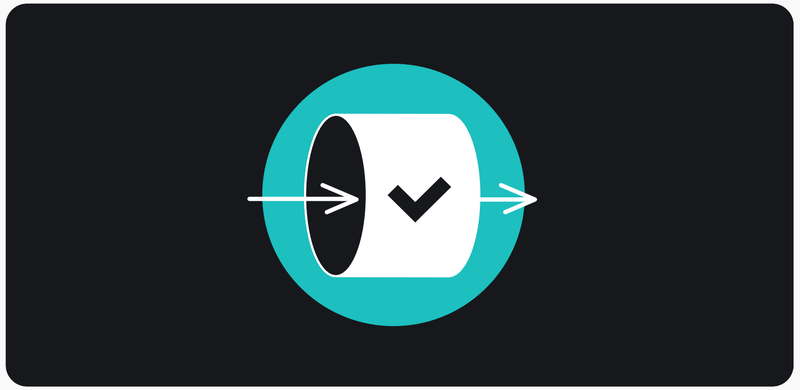
INDEPENDENTLY VERIFIED AND AUDITED

The Surfshark Dausos protocol was independently audited in March 2026. With a focus on architecture and cryptography, the report verified our findings and assessed Dausos to be a stable, resilient protocol with no critical vulnerabilities or significant flaws. It specifically highlighted Dausos's:

Post-quantum security

Hybrid TLS 1.3 (ML-KEM + ECDH) with ML-DSA authentication that safeguards data against tomorrow's quantum attacks.

Private VPN tunnels



Robust control/data channel design with strong session management and rekeying to deliver reliable connections.

Powerful encryption

256-bit keys with AEGIS for protected, high-performance client-server traffic.

Read the full Cure53 report

DAUSOS:
KEY TAKEAWAYS

Dausos reframes how a personal VPN should work with:

- A customer-first design;
- Dedicated, isolated data paths;
- Post-quantum secure cryptography and AEGIS-256X2 encryption.

By removing shared bottlenecks and giving sessions their own performance levers, Dausos delivers higher throughput, steadier latency, and stronger privacy. Designed for today's networks and tomorrow's threats, it offers a cleaner, faster, and more resilient foundation for private internet access.