MULLVAD VPN

PRIVACY GUIDE

Mullvad in depth

Complete guide

This guide explains how Mullvad VPN works and what it really protects: the account with no personal data, anonymous payment, servers that store nothing, WireGuard encryption, quantum-resistant tunnels and the defenses against traffic analysis.

From the anonymous VPN to encrypted, obfuscated traffic

Contents

INTRODUCTION AND BASICS

· How to use this guide 3

· The basic concepts 3

CHAPTERS

01 What Mullvad is and what problem it solves 5

02 The anonymous account: a 16-digit number 7

03 Payments and price 8

04 The no-logs policy 9

05 The 2023 raid 10

06 Diskless servers and external audits 11

07 WireGuard under the hood 12

08 GotaTun and the farewell to OpenVPN 15

09 Quantum-resistant tunnels 16

10 Multihop: two hops instead of one 19

11 DAITA and traffic analysis 20

12 DNS, blockers, kill switch and leaks 21

13 Mullvad Browser and the relationship with Tor 23

14 Limitations and what a VPN cannot do 24

15 Good practices 25

INTRODUCTION

How to use this guide

Audience and prerequisites. You do not need to know anything about networking or cryptography. The "Before you start" section explains from scratch what an IP address is, what DNS is and what exactly a VPN does. After that, the guide raises the level gradually.

State of the product. Mullvad changes often. This guide reflects the current situation: WireGuard only (OpenVPN was retired in January 2026), quantum-resistant tunnels on all desktop and mobile platforms, and GotaTun as its own WireGuard implementation, already available on Android and rolling out to the other platforms. If a detail may have changed, check Mullvad's website and blog.

How to read it. If you are starting from zero, begin with "Before you start". Chapters 1 to 6 explain the privacy model: which data exists and which does not. Chapters 7 to 11 explain the network and encryption technology. Chapters 12 to 15 are practical: leaks, browser, limits and good habits.

BEFORE YOU START

The basic concepts

To understand what a VPN adds, you need to know four pieces of the internet: the IP address, DNS, encryption and who can see what on the path between your device and a website.

The IP address

Every internet connection uses an **IP address**, a number like `203.0.113.45` that works as the postal address of your connection. When you open a website, the server needs to know where to send the reply, so your IP travels with every request.

Your IP is assigned by your operator (the internet service provider, or ISP). It reveals roughly which city you are in and which operator you use. And since the operator knows which customer it assigned the address to, it can link that IP to your name and your home address.

DNS: the internet's phone book

Computers find each other by number, but people use names like `example.org`. **DNS** is the phone book that translates the name into the number. Before visiting a website, your device asks a DNS server "what is the IP of example.org?". By default your operator's server answers that question, so it learns every site you visit, even if the content of the page is encrypted.

Encrypting means hiding the content

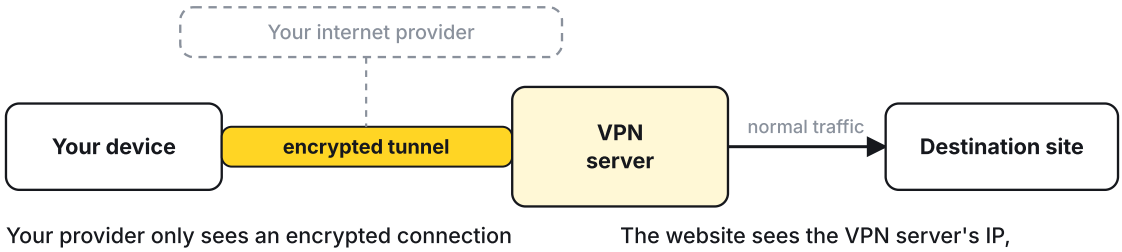
To **encrypt** is to turn a message into a jumble that only someone holding the key can undo. Today almost every website uses HTTPS, which encrypts the content between your browser and the site. But encryption does not hide who you are talking to: your operator can still see which servers you connect to, when, and how much data you exchange.

What each party sees without a VPN

WHO	WHAT THEY SEE WITHOUT A VPN
Your internet provider	Which servers you visit, when and how much data; usually also your DNS queries
The website you visit	Your IP, and with it your approximate city and your operator
A public Wi-Fi network	Which servers you visit and when, unless there is extra encryption
Anyone watching your stretch of the network	The destination of each connection and its volume

What a VPN does

A **VPN** (virtual private network) creates an encrypted tunnel between your device and a server run by the provider. All your traffic goes into the tunnel and leaves for the internet from that server.



What each party sees when you use a VPN.

The effect is twofold:

- Your operator only sees an encrypted connection to the VPN provider, not the sites you visit.
- Websites see the VPN server's IP, not yours.

Notice what changes: the trust moves. Before, your operator saw your traffic. Now the VPN provider does. That is why the important thing about a VPN is not the tunnel, but **what the provider does with what it sees** and what it can prove. That is the question that organizes this whole guide.

Quick glossary

TERM	MEANING
IP	The address of your internet connection
ISP	Your operator or internet provider
DNS	The phone book that translates website names into IPs
VPN	An encrypted tunnel to a server run by the provider
Encryption	Turning data into something unreadable without the key
Key	A secret number that encrypts or decrypts
Server	The provider's computer your traffic exits from
Logs	Records of what happened: who, when, to where

CHAPTER 1

What Mullvad is and what problem it solves

Mullvad VPN is a VPN service offered by the Swedish company Amagicom from Gothenburg. It has been operating since 2009 and stands out less for its tunnel technology, which is standard, than for **how little it knows about you**: almost nothing, by design.

What a VPN does and does not do

You need to separate what a VPN protects from what it does not touch.

A VPN DOES	A VPN DOES NOT
Hide your real IP from the websites you visit	Make you anonymous if you log in with your account
Stop your operator or a Wi-Fi network from seeing the sites you visit	Protect you from viruses or scam pages
Encrypt the stretch between your device and the server	Encrypt the stretch between the server and the website (that is HTTPS's job)
Make you appear to be in another country	Stop your browser from identifying you (fingerprinting)

Threat model

A **threat model** answers three questions: what you want to protect, from whom, and what you are willing to do to protect it. For a VPN, the typical adversaries are these:

1. **Your operator and the networks you connect from** (cafés, hotels, work). A VPN used well stops them from seeing your destinations.
2. **Websites and advertisers**, who use your IP to locate you and cross-reference profiles. The VPN changes that IP, although it does not stop other forms of tracking.
3. **Anyone who can demand data from the VPN provider** (a court, the police). The best defense is for the provider to have no data to hand over.
4. **An observer who watches both ends of the connection.** Against this adversary a VPN helps little; it is explained in chapter 14.

Mullvad is designed mainly for cases 1, 2 and 3. For case 4 it offers partial mitigations (DAITA, multihop), but no tool solves it completely.

The central idea: trust as little as possible

A VPN provider necessarily sees your traffic. Mullvad tries to make that matter as little as possible through four design decisions that the next chapters develop:

- An account that contains no personal data.
- Payments that can be made without leaving a trace.
- Servers that keep no logs.
- External audits and open source code, so that you do not have to take its word for it.

CHAPTER 2

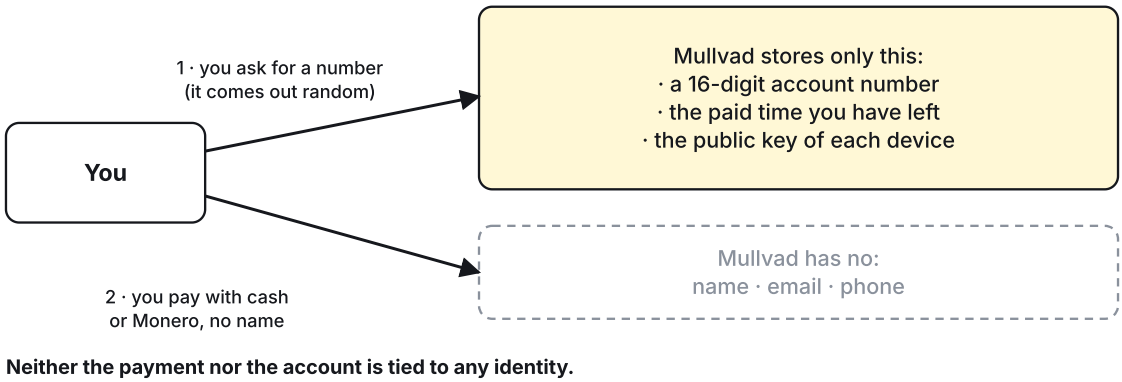
The anonymous account: a 16-digit number

Creating a Mullvad account involves no form. You press a button and the website gives you a randomly generated **16-digit account number**. That number is your only identifier: it works as both username and password.

No name, email or phone number is requested. Mullvad's website sums it up: they ask for no personal information, not even an email.

Why it works

What is not collected cannot be lost, leaked or handed over. If an authority asks Mullvad for "the data of customer X", there is no field in which to look up a name. Nor is there an email list to steal in a breach.



The account is created and paid for with no personal data.

The price of this design

There is no account recovery. If you lose the number, you lose access and the time you paid for: there is no "I forgot my password" because Mullvad has nobody to write to. Store the number in a password manager. And treat the number like a key: whoever has it can use your account.

Devices

Each account supports up to five devices at once. When you add a device, the app generates a WireGuard key pair on it and gives Mullvad only the public key (chapter 7). The private key never leaves the device.

CHAPTER 3

Payments and price

An anonymous account is worth nothing if the payment identifies you. A card payment leaves a trail at the bank and at the payment processor, and that trail links your name to a Mullvad account.

A flat price

Mullvad charges **5 euros a month**, with no discounts for paying years in advance and no free plan. The price does not change with the duration: paying for 12 months costs 12 times one month. There is also no automatic renewal: you pay for time, and when it runs out, the account expires. Mullvad even cancelled the remaining recurring PayPal subscriptions, because a subscription forces it to keep payment data.

This model also explains why Mullvad does not do aggressive marketing or pay affiliates: its website says it avoids paid reviews and affiliate programs.

Ways to pay

METHOD	WHAT TRACE IT LEAVES
Cash by mail	The lowest: an envelope with money and your account number, with no mandatory sender
Monero	Very low: the coin itself hides sender, receiver and amount
Bitcoin and Bitcoin Cash	Low, but the blockchain is public and can be analyzed
Card, bank transfer, Swish, others	High: the bank or the processor knows about the payment
Reseller vouchers	Depends on where the voucher is bought

Mullvad officially started accepting Monero in May 2022. It is a choice consistent with its philosophy: Monero hides who pays and how much, just as the Mullvad account hides who you are.

Cash

Paying in cash works like this: on the website you generate a code tied to your account number, put banknotes in an envelope with that code and send it to Mullvad's office. Several currencies are accepted. It is the most anonymous method, though also the slowest.

What is stored about the payment

Mullvad keeps the minimum needed to confirm the payment and avoid duplicates, and as published it deletes it after a few weeks. Methods with an intermediary (card, PayPal) still leave their own record at the processor, outside Mullvad's control. If your goal is anonymity, choose cash or Monero.

CHAPTER 4

The no-logs policy

A **log** is a record of activity: who connected, at what time, from which IP and where they went. Mullvad's **no-logs** policy consists of keeping none of those records.

What it does not store

- Which sites you visit or what content you send.
- Your DNS queries.
- Your real IP or the timestamps of your connections.
- How much bandwidth you use.

What does exist

To work, Mullvad needs a few pieces of data: your account number, the expiry date of the time you paid for, the public keys of your devices and a count of connected devices to enforce the limit of five. None of them says what you do with the VPN.

From promise to architecture

Any VPN can write "no logs" on its website. What matters is that the system could not store them even if it wanted to, and that someone independent verifies it. Mullvad tries to cover both with diskless servers (chapter 6) and with external audits. Even so, a no-logs policy remains, in the end, a statement about a company's behavior. That is why the next chapter is so relevant: it is the one time it has been tested with a court order.

CHAPTER 5

The 2023 raid

On 18 April 2023, at least six officers from the National Operations Department of the Swedish police showed up at Mullvad's office in Gothenburg with a search warrant. They were looking for computers holding customer data.

What happened

According to Mullvad, staff explained to the officers that there is no customer data to seize and showed them how the service works. The police left without taking any equipment or information. Nine days later, the Swedish authorities stated that the search had been carried out at Germany's request, as part of an ongoing investigation.

What it shows and what it does not

The raid is a valuable data point because it is a real test, not a promise: an authority with a court order found nothing to take away. But its scope should be measured carefully.

- It **shows** that, on that date, Mullvad did not hand over customer data and that the police found no records to seize.
- It **does not show** that nothing different will ever happen, or that the physical servers could not be monitored by other means. A single test is not a guarantee.

Mullvad later pointed out that Swedish jurisdiction protects its customers, and that its servers run without disks, something explained in the next chapter.

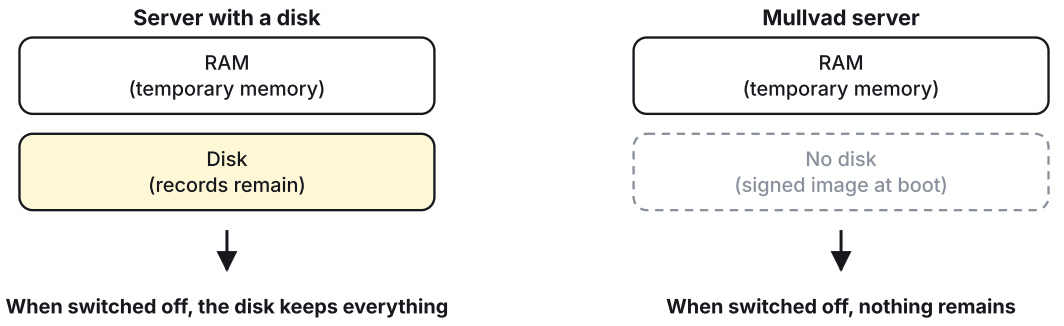
CHAPTER 6

Diskless servers and external audits

A promise is more credible when the architecture makes it hard to break and when an outsider reviews it.

Servers that use only RAM

Mullvad's servers run **without a disk**: the operating system boots from a signed image and works only in RAM. RAM loses its contents when powered off, so any reboot or power cut wipes everything that was on the machine.



RAM is wiped when powered off; a disk is not.

This has two practical consequences:

- Even if someone seized a physical server, nothing would be left to recover once it was switched off.
- It is hard for a bug or a careless installation to leave forgotten records on a disk.

The limit is that RAM does contain data while the server is on. An intervention with the machine running remains a theoretical threat, which is why it matters that the system itself does not accumulate sensitive data.

Independent audits

Mullvad commissions periodic external audits of its app and its infrastructure from companies such as Cure53, Assured Security Consultants and others, and publishes the reports on its website, including findings that do not favor it. The reviews have found minor problems that were

fixed, with no critical findings in the public reports.

A recent example is the audit of **GotaTun**, its own WireGuard implementation (chapter 8). Assured Security Consultants reviewed its code between January and February 2026, and Mullvad published the result in March 2026. It found two low-severity issues and nine informational observations, and none critical, high or medium. One of the two minor flaws was a method of generating session identifiers inherited from the original project, which could give a passive observer some information. Mullvad fixed it in version 0.3.0.

How to read an audit

- An audit reviews a **specific scope** at a specific moment. The GotaTun one, for example, did not cover DAITA.
- That no serious flaws appear is not proof that none exist.
- That the full report is published is a good sign, because it lets anyone check what was said.
- The code of Mullvad's apps is open source, which also allows review by anyone.

CHAPTER 7

WireGuard under the hood

WireGuard is the tunnel protocol Mullvad uses. It was designed by Jason Donenfeld as a simpler and faster alternative to earlier protocols. Mullvad adopted it early, in 2017, and since January 2026 it is the only one it offers.

Why simplicity matters

The less code there is, the fewer places to hide a flaw. WireGuard is much shorter than its predecessors, which makes it easier to audit. It is also opinionated: it offers no lists of algorithms to choose from, but a fixed, modern set. That prevents attacks that force the use of a weak option.

The cryptographic pieces

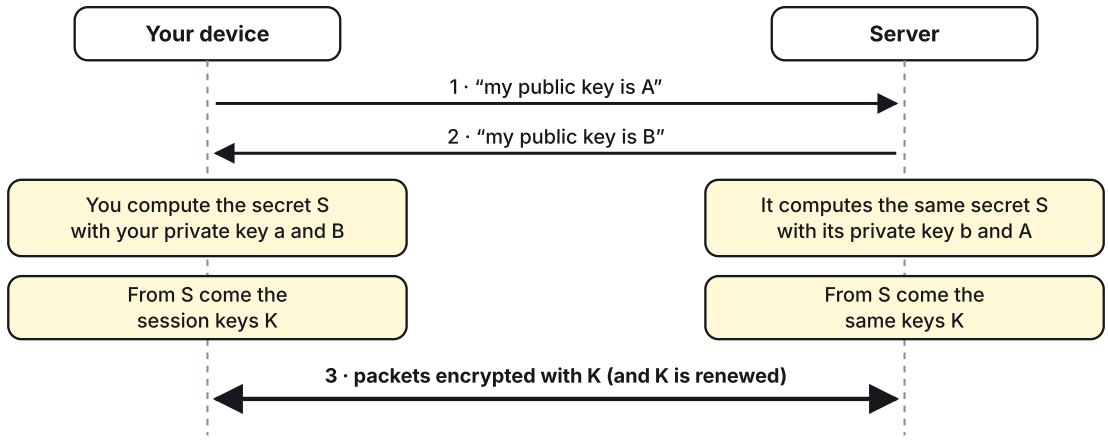
WireGuard is built on the **Noise** framework, which defines how two parties agree on secret keys. Each piece does a specific job:

PIECE	WHAT IT IS FOR
Curve25519	Key exchange: two parties compute a shared secret without sending it
ChaCha20-Poly1305	Encrypts the packets and checks that nobody has altered them
BLAKE2s	Hash function: turns data into a fixed-size fingerprint
HKDF	Derives several keys from one shared secret

How a tunnel is established

1. **Each device has a key pair.** The private key stays on the device; the public one is registered with Mullvad.
2. **Handshake.** The device and the server exchange public keys and compute, with Curve25519, a shared secret that only they know.
3. **Session keys.** Temporary keys are derived from the secret to encrypt the packets.
4. **Periodic renewal.** Session keys are changed frequently. That way, if someone one day obtains a session key, they only decrypt a short stretch of traffic and not the whole past. This property is called **forward secrecy**.

Everything travels over UDP and the system is discreet: if someone sends packets without a valid key, the server does not reply, so from the outside it does not announce itself as an open service.



WireGuard handshake: public keys are exchanged, never the secret.

The key agreement, step by step

The heart of WireGuard is a mathematical trick called **Diffie-Hellman key exchange**. It lets two parties who have never met end up with the same secret by talking in public, without ever sending it. An image: you and the server start from a pot of yellow paint that everyone knows, and each of you adds a secret color of your own. You swap the mixed pots, and each of you adds your secret again to the pot you receive. You both end up with exactly the same mixture. Whoever only saw the pots on the way cannot separate the colors.

KEY FORMULA.

$$S = a \cdot B = b \cdot A = (a\,b) \cdot G$$

In words: you and the server arrive at the same secret number S by each combining your own private key with the other's public key.

What each symbol is:

- `G`: a fixed, public point on the Curve25519 curve. It is the pot of yellow paint everyone starts from.
- `a` and `b`: the private keys, yours and the server's. They are random numbers and never leave the device.
- `A = a·G` and `B = b·G`: the public keys. They are obtained by "adding G to itself" `a` or `b` times. They can be published because, given `A`, recovering `a` is infeasible (the discrete logarithm problem).
- `·`: here this is not an ordinary multiplication, but adding a point on the curve to itself many times.
- `S`: the shared secret, the same for both.

An example with small numbers. So you can follow it with pencil and paper, we use a simpler version than the curve: 23-hour clock arithmetic (modulo 23) with base 5. The idea is identical.

1. You secretly choose `a = 6` and compute `A = 5⁶ mod 23 = 8`. You publish the 8.
2. The server secretly chooses `b = 15` and computes `B = 5¹⁵ mod 23 = 19`. It publishes the 19.
3. You compute `19⁶ mod 23 = 2`.
4. The server computes `8¹⁵ mod 23 = 2`.

You both hold the 2 without having sent it to anyone. A spy saw the 5, the 23, the 8 and the 19, but not the 6 or the 15. With numbers this small they could try them all; with Curve25519's 256-bit numbers there is not enough time in the universe.

Why it works: the order does not matter when multiplying. You compute `a·(b·G)` and the server computes `b·(a·G)`, and both are `(a·b)·G`. It is the same property as `6 × 15 = 15 × 6`, only applied to points on the curve.

The secret `S` is not used as is. It is passed through a derivation function that produces the session keys, and these feed the encryption of each packet:

$$(\text{encrypted packet},\ \text{tag}) = \text{ChaCha20-Poly1305}(K,\ n,\ \text{message})$$

In words: with the session key `K` and a counter `n` that never repeats, the message comes out unreadable and with a tag that exposes any alteration.

What the server knows

The server knows your public key and the IP you are connecting from at that moment, because it needs it to send packets back to you. Mullvad designs the system so that this information is not written to disk or logged (chapters 4 and 6). That in-memory datum is the equivalent of an active phone line: it exists for as long as the call lasts.

CHAPTER 8

GotaTun and the farewell to OpenVPN

For years Mullvad offered two protocols: **OpenVPN**, the veteran, and WireGuard. Two protocols mean two codebases to maintain, test and audit. In 2025 Mullvad decided to concentrate on one.

The retirement of OpenVPN

Version 2025.14 of the desktop app removed the option to choose OpenVPN. On 15 January 2026 Mullvad switched off the remaining OpenVPN servers, so since then the whole service runs on WireGuard. Anyone using OpenVPN on a router or in a third-party app had to migrate to WireGuard before that date.

The decision rested on the fact that WireGuard now supports what used to be exclusive to OpenVPN, such as the modes for getting around network blocks (UDP over TCP and Shadowsocks).

What GotaTun is

Mullvad's mobile apps used `wireguard-go`, a WireGuard implementation written in the Go language. After years of friction with it, Mullvad created **GotaTun**, its own implementation written in **Rust**. The name pays homage to the Götatunneln tunnel in Gothenburg.

- GotaTun started as a fork of BoringTun, Cloudflare's Rust implementation.
- It is open source under the three-clause BSD license.
- It incorporates Mullvad's own features, such as multihop and DAITA.
- It reached Android first, in late November 2025. Mullvad plans to bring it to the other platforms during 2026.

According to Mullvad's internal data, the user-perceived crash rate on Android fell from 0.40% to 0.01% after adopting GotaTun in version 2025.10, with improvements in speed and battery use.

Why Rust

Most serious security flaws in network software come from memory errors: reading or writing where you should not. Rust is designed to prevent that class of errors at compile time. Writing the piece that handles all your traffic in a language like that reduces the risk.

What is used on each platform

Mullvad uses different WireGuard implementations depending on the platform and the features enabled. On Linux, for example, the kernel implementation is used by default for performance, and GotaTun comes in when features such as multihop or DAITA are enabled. The split changes with versions, so for the exact status it is best to check Mullvad's technical page.

CHAPTER 9

Quantum-resistant tunnels

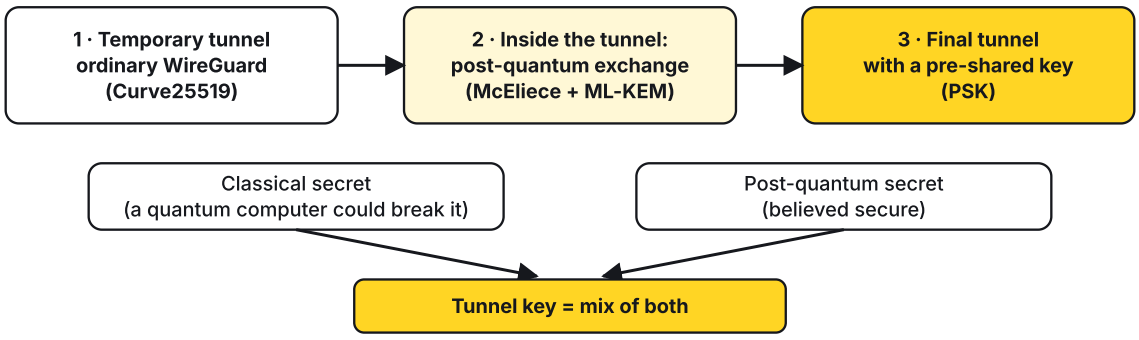
A sufficiently powerful **quantum computer** could break the key exchanges used today, including Curve25519. No capable one exists yet, but there is a risk already present: someone can **record encrypted traffic today** and keep it until the machine that opens it exists. This is what is called "harvest now, decrypt later".

What breaks and what does not

The part that encrypts the packets (ChaCha20) is not the weak point. The weak point is the **key agreement** at the start, because its security depends on mathematical problems that a quantum computer would solve quickly. If the agreement is broken, the key is obtained and the rest falls.

What Mullvad does

Mullvad offers quantum-resistant tunnels on all platforms. The mechanism takes advantage of an option WireGuard already includes, the **pre-shared key** (PSK), which is mixed into the calculation of the session keys.



Quantum-resistant tunnel: two security layers mixed together.

The process is this:

1. The app opens a first, ordinary WireGuard tunnel to the server.
2. Through that tunnel, the device and the server agree on a new secret using **post-quantum algorithms**: Classic McEliece and Kyber (now standardized as ML-KEM).
3. That first tunnel is closed and a definitive one is opened that uses the new secret as a pre-shared key.

The result is a tunnel that is secure if **either** of the two layers holds: the classical one or the post-quantum one. An attacker would have to break both. This is called a **hybrid** design, and it avoids betting everything on new algorithms that have only a few years of analysis behind them.

An image to see why both layers are needed: a safe with two locks in series. Opening it takes both keys. If a future quantum computer gets the first (the classical one), the second (the post-quantum one) stays locked, and vice versa.

KEY FORMULA.

$$K = \mathrm{HKDF}\left(S_{\text{classical}},\ S_{\text{post-quantum}}\right)$$

In words: the tunnel's final key is obtained by mixing the two secrets, the one from the normal key exchange and the one from the post-quantum exchange; without knowing both it cannot be computed.

What each piece is:

- `S_classical`: the secret from the Curve25519 exchange of chapter 7. A quantum computer could compute it.
- `S_post-quantum`: the secret agreed with Classic McEliece and ML-KEM through the first tunnel. It is believed to be secure against quantum computers. In WireGuard it enters through the pre-shared key (PSK).
- `HKDF`: the function that mixes secrets and delivers a key that looks random. If either ingredient is missing, the result is impossible to guess.
- `K`: the key with which the packets of the definitive tunnel are encrypted.

Why it works: HKDF behaves like a one-way blender. If an attacker knows one ingredient but not the other, the mixture is still indistinguishable from a random number. That is why it is enough for one of the two layers to hold.

Current status

In the app, a connection with this protection shows the status "quantum secure connection" in green. Since desktop version 2025.2 it is enabled by default on Windows, so it is now the default behavior on all desktop platforms. Mullvad also reported that its tunnels are not affected by the vulnerabilities in some Kyber implementations that were disclosed at the time.

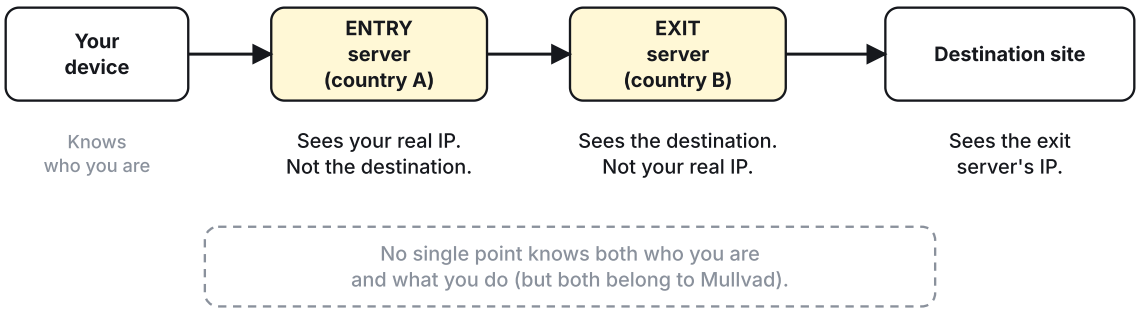
CHAPTER 10

Multihop: two hops instead of one

With an ordinary VPN, a single server sees both your real IP and the destination of your traffic at once. If that server were monitored, whoever watches it could link the two. **Multihop** splits that information between two servers.

How it works

Your traffic enters through an **entry** server, which forwards it to an **exit** server, and the exit server is the one that delivers it to the internet. The two servers can be in different countries.



Multihop: each server knows only half of the information.

WHO	WHAT THEY SEE
Entry server	Your real IP, but not the final destination
Exit server	The destination, but not your real IP: it only sees the entry server's IP
The destination website	The exit server's IP

What it adds and what it does not

- It **adds** that no point in the chain knows both who you are and what you do, as long as the same actor does not control both servers. It is especially useful if you are worried about a single country or a single data center.
- It **costs** more latency, because the traffic travels a longer path.

- It **does not turn Mullvad into two companies**: both hops belong to Mullvad, so you still trust the same provider. Multihop helps against an isolated server or a monitored environment, not against the provider itself.

CHAPTER 11

DAITA and traffic analysis

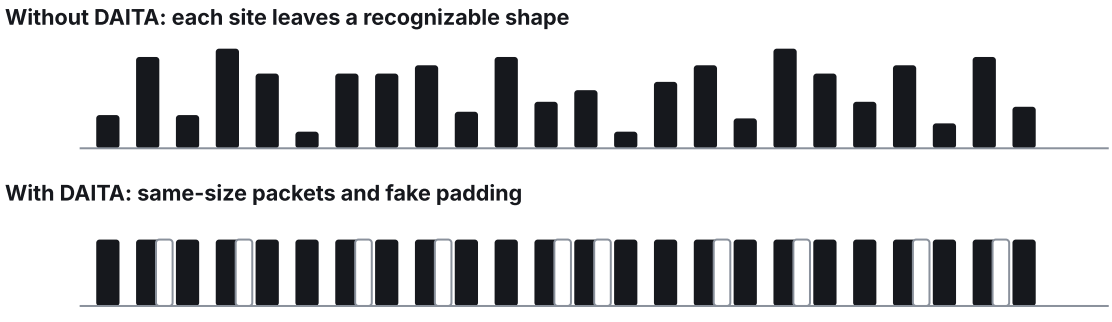
Encryption hides the content, but it does not hide the **shape** of the traffic: the size of the packets, the rate at which they arrive and how long each burst lasts. That shape is a fingerprint.

The problem

Each website produces a recognizable traffic pattern. Loading a newspaper page generates a different sequence of packets than loading a video or a webmail site. An observer who sees your encrypted connection, such as your operator, can train an **artificial intelligence** system to recognize those patterns and work out which websites you visit **without decrypting anything**. This is called traffic analysis or *website fingerprinting*.

The defense: DAITA

DAITA (short for "defense against AI-guided traffic analysis") is a feature of the Mullvad app that adds noise to spoil that fingerprint.



DAITA hides the shape of the traffic with padding and fixed-size packets.

It does three things:

1. **Random fake traffic**: it sends filler packets at unpredictable moments, so that it cannot be seen when you are really active.
2. **Pattern distortion**: while you visit a website, it inserts fake packets in both directions so that the resulting pattern does not resemble that website's.
3. **Constant size**: it makes all packets the same size, so that small ones give nothing away.

DAITA is based on **Maybenot**, an open source framework for defining defenses of this kind. Mullvad helps fund it and developed it together with Karlstad University, with research published in the open.

Limitations

- It has a cost: the fake traffic consumes bandwidth and can slow things down.
- For now it is available only on a selection of servers, which Mullvad may expand.
- It makes traffic analysis harder, but not impossible: it is a reduction of risk, not a guarantee.
- The GotaTun audit did not cover DAITA, so this feature has a less extensive review history than the basic tunnel.

CHAPTER 12

DNS, blockers, kill switch and leaks

A VPN can have a perfect tunnel and still give you away if something escapes outside it. These are the three places where it usually happens.

DNS inside the tunnel

Remember that DNS is the phone book that reveals which websites you want to visit. When you use Mullvad, **all your DNS queries go through the encrypted tunnel** and Mullvad resolves them on the server itself, instead of sending them to your operator. If those queries went outside the tunnel, your operator would still see every website you visit even with the VPN switched on. That is a **DNS leak**.

Content blockers

The app lets you turn on **DNS-level content blockers**: when an app or a website asks for an advertising, tracking or malware domain, the DNS server answers that it does not exist and the request never goes out. They can be enabled by category. It is a convenient help and works across the whole device, but it is a basic layer: it does not replace an ad blocker in the browser and does not stop tracking that does not depend on known domains.

The kill switch

What happens if the tunnel drops for a second? Without protection, the device goes back to sending traffic over the normal connection and reveals your real IP. The **kill switch** prevents that: if there are connectivity problems with the VPN on, the app automatically blocks all network traffic until the tunnel comes back. The app also includes a stricter blocking mode, so that nothing goes out if the VPN is not connected.

Other common leaks

LEAK	WHAT IT IS	HOW TO AVOID IT
IPv6	Your device uses a second address that does not go through the tunnel	Use the official app, which handles IPv6; check with a leak test
WebRTC	The browser can reveal your real IP to a website through a video-calling technology	Use a browser that blocks or limits it (such as Mullvad Browser)
Apps outside the tunnel	Some apps leave the VPN because of the local network configuration	Review split tunneling and turn it off if you do not need it
Connecting before the VPN	The device connects to the internet before the VPN starts	Enable the app's auto-connect and the blocking mode

Mullvad offers on its website a **connection check** that shows which IP and which DNS websites see. It is a good habit to run it after installing or changing the configuration.

CHAPTER 13

Mullvad Browser and the relationship with Tor

A VPN hides your IP, but your browser still hands over a lot of information about you.

The browser fingerprint

Every browser reveals details such as window size, installed fonts, language, resolution or the type of graphics card. Combined, they form an almost unique **fingerprint**, and a website can recognize you by it without cookies and even if you change IP. A VPN changes none of this.

Mullvad Browser

Mullvad Browser is a free browser developed by the **Tor Project** at Mullvad's request. The idea is for users to look as much alike as possible, so that your fingerprint is lost in a crowd. It achieves this with several measures:

- **Similar fingerprints**: all users present an almost identical configuration.
- **Letterboxing**: it adds gray bands around the page so that scripts cannot deduce the exact size of your window.
- **uBlock Origin** included, to block third-party trackers.
- **Private mode by default**: it does not keep cookies between sessions and isolates third-party cookies.
- **No telemetry**.

Its official description defines it as a Tor browser without the Tor network. It does not include a VPN: Mullvad recommends combining it with a trusted VPN, because the browser on its own does not hide your IP.

VPN and Tor: they are not the same

	VPN (MULLVAD)	TOR NETWORK
How many intermediaries	One (or two with multihop), all from the same company	Three relays run by different volunteers
Whom you trust	The provider	That the relays do not collude
Speed	High	Lower
Best for	Daily use, downloads, video, protecting the local network	Strong anonymity in browsing and specific services

They are different tools and can be used together, but each combination has nuances. For daily use, the pairing of VPN plus Mullvad Browser gives broad protection with little effort. When anonymity is critical, the Tor network spreads trust among many independent actors and is usually the more suitable option.

What happened to Mullvad Leta

In 2023 Mullvad launched Leta, a search engine that acted as a privacy intermediary for searches. Mullvad shut it down on 27 November 2025. It is a useful reminder that services change: always check what is still available.

CHAPTER 14

Limitations and what a VPN cannot do

An honest guide has to say where the protection ends.

You have to trust the provider

All your traffic passes through Mullvad. The audits, the open source code, the diskless servers and the 2023 raid are reasons to trust, but they are not definitive proof. A VPN changes **whom you trust**; it does not eliminate trust. Mullvad tries to make trusting it as cheap as possible, by not knowing who you are.

Traffic correlation

If an adversary can observe at once your connection to the server and the server's exit toward the website, they can compare the timing and volume of the data and deduce that they are the same communication, even though everything is encrypted. It is a very hard attack for an ordinary actor to carry out, but possible for someone who watches large parts of the internet. DAITA and multihop reduce the risk, and do not eliminate it.

Browser fingerprint and accounts

If you log in to your email, your social networks or your bank, the website knows who you are with or without an IP. And if your browser has a unique fingerprint, you are recognized between sessions. The VPN does not protect against this, which is why Mullvad Browser exists.

The shared IP

Many users reach the internet through the same server IP. That mixes you into a crowd, which is good for privacy, but has a practical cost: some websites block or limit VPN IPs, ask for extra checks or deny access to certain services. Mullvad is not aimed at unblocking video platforms and says so clearly. Nor does it offer port forwarding, which it removed in May 2023.

Payments with a trail

If you pay by card or bank transfer, your bank or the processor knows about the payment. That does not reveal what you do with the VPN, but it does reveal that you are a customer. For anyone who needs real anonymity, choose cash or Monero.

There is no account recovery

If you lose the 16-digit number, you lose the account. It is the counterpart of not storing data about you.

CHAPTER 15

Good practices

A well-configured VPN is far stronger than a badly used one. This summary gathers the

essentials.

1. **Store the account number** in a password manager and do not share it.
2. **Choose the payment method according to your goal.** For anonymity, cash or Monero; for convenience, card.
3. **Turn on the quantum-resistant tunnels** if they are not already the default on your platform.
4. **Keep the kill switch and the blocking mode on**, and have the app connect by itself at startup.
5. **Test your connection** with Mullvad's tool after installing and after changing the configuration.
6. **Use Mullvad Browser** or a hardened browser, and do not log in to personal accounts when you want to keep your identity separate.
7. **Use multihop or DAITA** if your threat model includes a network observer, knowing that they cost speed.
8. **Keep the app up to date.** Mullvad publishes fixes and improvements often, and the migration to GotaTun arrives through updates.
9. **Do not expect the VPN to solve everything.** It is one layer within a whole: a secure device, accounts with strong authentication and care with what you share.

Sources

This guide draws on Mullvad's official website and blog (the "Why Mullvad VPN", DAITA and Mullvad Browser pages and the posts on OpenVPN, GotaTun and Leta), on CyberInsider's and TechRadar's analysis of GotaTun and its audit, on Ghacks and CyberInsider's coverage of the 2023 police search, on AlternativeTo's article about quantum-resistant tunnels and on PCWorld's and CNET's coverage of pricing and payment methods.