SNARKYPUSS

A Private Bridge to Your VPN

Why Snarkypuss?

Commercial VPN services give people a convenient way to route Internet traffic through an encrypted connection to a provider-operated server. For many users, that service has become an ordinary part of protecting their privacy online.

But the VPN application does not have to run on the same computer that you use every day. Snarkypuss starts with a different arrangement: your computer connects through a private WireGuard tunnel to **Your VPS**, a small-footprint hosted virtual server that you control. The commercial VPN runs there instead.

That separation matters if the legal or commercial environment in Canada changes. Snarkypuss does not replace the commercial VPN, defeat Canadian law, or make anyone anonymous. It gives you a privately controlled bridge between your own computer and the VPN service you have chosen.

A Changing Privacy Landscape

Legislative context researched and verified as of 17 September 2026.

Canada's rules for communications security and lawful access are changing. Two measures are particularly relevant to the background of this project: Bill C-8 and Bill C-22.

Bill C-8 — An Act Respecting Cyber Security received Royal Assent on June 15, 2026. It broadens federal authority over the security of Canada's telecommunications networks and enacts the Critical Cyber Systems Protection Act, which places cybersecurity obligations on designated operators in sectors including telecommunications, banking, energy, transportation, and clearing and settlement.

The telecommunications amendments took effect on assent; the operator obligations are being phased in by order of the Governor in Council. The government says these measures are intended to protect essential services from increasingly sophisticated cyber threats.

Privacy Commissioner Philippe Dufresne supported the bill's cybersecurity objectives while urging that the new powers carry limits so they do not have unintended effects on privacy. He recommended a uniform necessity-and-proportionality standard for collecting personal information, notification of his office when an incident involves a material privacy breach, and safeguards on information shared outside Canada. At the Senate stage in May 2026 he acknowledged significant improvements Parliament had already made.

Bill C-22 — the Lawful Access Act, 2026 remains proposed legislation. Introduced on March 12, 2026, it passed the House of Commons on June 18 after the government invoked time allocation to limit debate. As of this brochure's September 2026 snapshot it is before the Senate, which resumes on September 21 and has not yet begun its study.

The government describes lawful access as the ability of law enforcement or the Canadian Security Intelligence Service to obtain information or intercept communications when legally authorized. Part 2 of Bill C-22 would enact the Supporting Authorized Access to Information Act, requiring electronic service providers to maintain the technical capabilities needed to give effect to those authorities.

Government and critics describe the safeguards differently. A spokesperson for the Minister of Public Safety has said the bill would not require companies to build backdoors, and that authorities would still need legal authorization such as a court warrant to obtain data. Critics note that as introduced the bill would also let an officer with reasonable grounds to suspect an offence require a telecommunications provider to confirm whether a person is a subscriber, without prior judicial authorization.

Commissioner Dufresne told the House committee in May 2026 that privacy concerns remain, and made eight recommendations — among them narrowing the definition of subscriber information, limiting which providers can be compelled, and adding an overarching requirement that obligations be necessary and proportionate. Amendments later adopted reduced the maximum metadata-retention period from one year to six months and required the Minister to be satisfied that a retained category is essential to investigations.

Why VPN Providers Care

For a VPN provider built around encryption and a no-logs design, a requirement to create new technical access or data-retention capabilities raises a direct question: can the provider comply without changing the privacy properties it promises its customers?

NordVPN said on May 15, 2026 that it was reviewing Bill C-22, and that if it became subject to mandatory obligations it would not compromise its no-logs architecture or encryption protections. It would instead consider all viable options, including limiting or removing its presence from Canadian jurisdiction. That was a conditional warning, not an announced departure.

Windscribe, which is headquartered in Canada, was blunter. It said the previous day that it would leave the country if the bill passes, noting that a company based elsewhere can simply switch off its Canadian servers while its own head office is here. The encrypted messaging service Signal had said earlier that week that it would rather withdraw from the Canadian market than comply.

These are stated positions, not outcomes. The project does not predict what Parliament, regulators or VPN providers will ultimately do. It provides a privately hosted architecture in which the user's own connection to **Your VPS** remains separate from the commercial VPN provider running beyond it.

What Snarkypuss Is

Snarkypuss is privately hosted, open-source software for building and controlling your own bridge to a commercial VPN service. It is not itself a VPN provider, and there is no Snarkypuss company, subscription service, or central network carrying users' traffic.

You provide two things: your own hosted virtual server and your own account with a supported commercial VPN provider. Snarkypuss supplies the software that connects them and gives you a private control interface for managing the result.

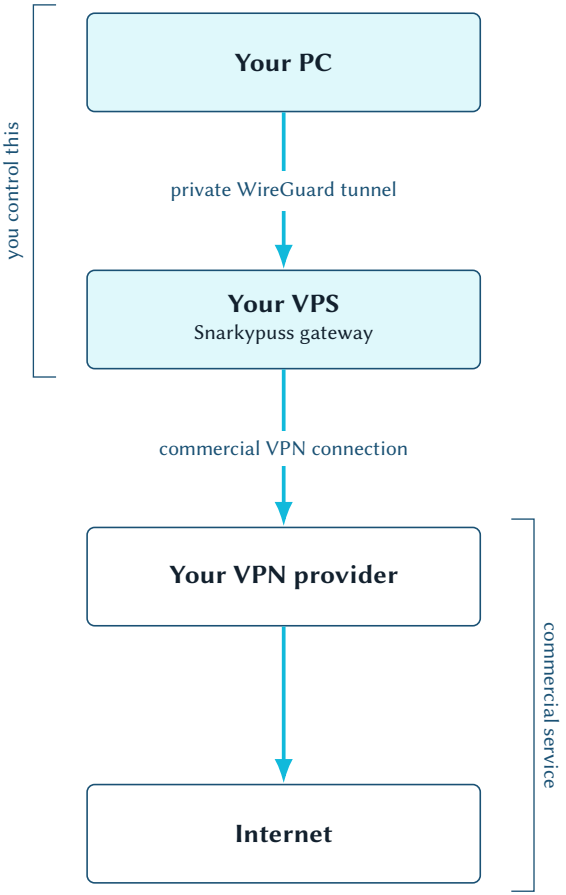
Each installation belongs to its user. The server is under that user's control, the commercial VPN relationship remains between the user and the VPN provider, and Snarkypuss does not change the legal obligations of either.

In short, Snarkypuss is:

- privately hosted
- open source
- non-commercial
- operated on your own VPS
- used with the VPN provider you choose separately
- intended for lawful use

The Basic Idea

The route is simple to describe.



No Snarkypuss-operated service carries your traffic.

Your PC first connects to **Your VPS** through WireGuard, an encrypted point-to-point tunnel. The commercial VPN software runs on the VPS rather than directly on your PC. Internet traffic arriving through WireGuard can then be forwarded through the commercial VPN connection before it reaches the public Internet.

Your VPS (Virtual Private Server) is a small-footprint hosted virtual server. It provides the Internet-connected Linux environment Snarkypuss needs without requiring dedicated hardware. A suitable VPS costs approximately US$5 per month.

This creates two distinct relationships. The WireGuard tunnel between your PC and your VPS is private infrastructure that you control. The onward VPN connection is supplied by the commercial provider you have chosen. Snarkypuss sits between those two pieces and manages the gateway.

There is no shared Snarkypuss relay in the middle. Your traffic does not pass through a Snarkypuss-operated service.

Why Keep the Commercial VPN?

A VPS could send traffic directly to the Internet, but that would make the VPS itself the public exit point. Snarkypuss is designed to preserve the useful properties of a commercial VPN while moving that VPN connection onto infrastructure you control.

A commercial VPN can provide a large pool of shared exit servers, many geographic destinations, provider-operated network infrastructure, and convenient changes of destination. Those are services that a single low-cost VPS is not intended to reproduce.

So the VPS is primarily the private bridge. The commercial VPN remains the outward-facing privacy service.

Snarkypuss can also enter a deliberate **Direct VPS** mode in which traffic exits through the VPS without the commercial VPN, but that is an explicit exceptional state rather than a silent fallback.

Meet SnarkyCtl

For normal use, you do not administer the gateway by typing Linux or VPN commands. SnarkyCtl, the management component of Snarkypuss, provides a private web dashboard reached through the WireGuard tunnel.

The dashboard shows the effective state of the gateway: whether the upstream VPN is protected or disconnected, the current VPN target and server, the public Internet address being used, and the state of important protections such as leak protection and DNS. Status is refreshed automatically while the dashboard is open.

From the same interface you can choose a destination and ask Snarkypuss to connect or disconnect the commercial VPN. The dashboard exposes defined Snarkypuss operations rather than a general-purpose administrator console.

Choosing Where You Connect

A VPN destination in Snarkypuss is called a **target**. Targets are approved choices in the target catalogue, not arbitrary command-line arguments passed to the VPN software.

One choice is always available: **Fastest available server**. This is the provider's built-in recommended destination. It is a special Snarkypuss target and does not have to be added to the catalogue before it can be selected.

For more control, the catalogue can contain provider-supported choices such as a country, city, server group, or a specific server. A fresh installation does not invent any of these choices for you; you add the destinations you actually want to use.

Snarkypuss can discover available destinations from the installed VPN provider rather than depending on a server list frozen into the application. If a previously saved destination is no longer available, Snarkypuss does not silently substitute a different one.

Privacy Includes Failure

Connecting successfully is only the happy path. A privacy gateway also has to answer a more important question: **what happens when something goes wrong?**

The commercial VPN can disconnect. A connection attempt can fail. Routing can be incomplete. DNS can be misconfigured. A service can restart after an upgrade or reboot. And sometimes the software may be unable to establish with confidence what route traffic is actually taking.

Snarkypuss therefore describes the effective gateway state rather than treating a successful connect command as proof that the connection is safe.

Protected VPN

Traffic from WireGuard is forwarded through the commercial VPN. Snarkypuss can verify the expected protected route.

Traffic leaves: through the provider.

Locked

Public forwarding is blocked. The private SnarkyCtl interface stays reachable through WireGuard.

Traffic leaves: it does not.

Direct VPS

A deliberate exceptional mode for administration or troubleshooting. Never an automatic fallback.

Traffic leaves: through the VPS, unprotected.

Unknown

Snarkypuss cannot establish the effective state with confidence, and does not claim protection it cannot verify.

Traffic leaves: not asserted.

Protected VPN is the normal state. Internet traffic arriving through WireGuard is forwarded through the commercial VPN, and Snarkypuss can verify the expected protected route.

Locked is the safe disconnected state. Public Internet forwarding is blocked. You can still reach the private SnarkyCtl interface through WireGuard, but ordinary Internet traffic is not allowed to escape through the VPS simply because the commercial VPN is unavailable.

Direct VPS is an explicit exceptional mode. It deliberately allows Internet traffic to leave through the VPS public connection without the commercial VPN. This can be useful for administration or troubleshooting, but it is not presented as VPN-protected traffic and it is never intended to become the automatic fallback from a failed VPN connection.

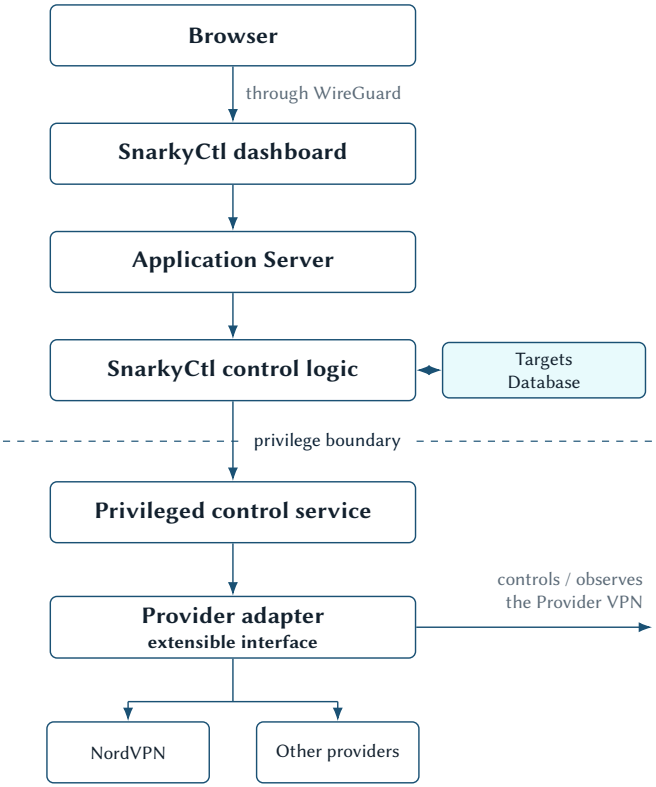
Unknown means exactly that: Snarkypuss cannot establish the effective safety state with sufficient confidence. It does not turn uncertainty into a reassuring green light.

Loss of the upstream VPN must not silently become an unprotected Internet connection.

Under the Hood

The internal design separates two ideas that are easy to confuse: controlling the gateway, and carrying Internet traffic through it. They are not the same path.

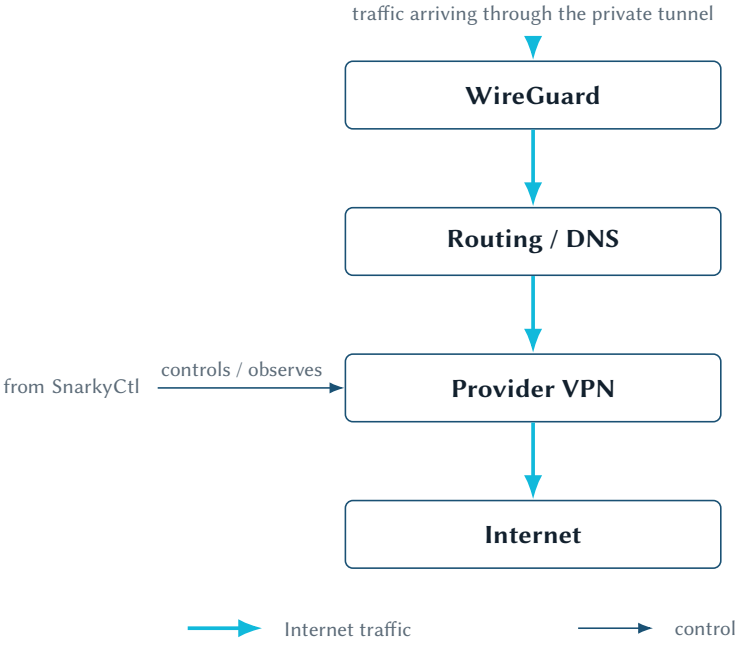
SnarkyCtl Control



The dashboard can request only defined, validated operations.

Network Gateway

Internet packets arriving through WireGuard follow the routing and DNS configuration to the provider VPN and then onward to the Internet. They do **not** pass through the SnarkyCtl web application.



Your browser reaches the dashboard through the private WireGuard connection, and operations that genuinely require administrator access are performed by a restricted privileged control service. SnarkyCtl controls and observes the provider connection, but it sits beside the packet path rather than inside it.

The reference deployment runs on Linux on a privately controlled VPS, and the architecture is intentionally provider-independent.

More Than `nordvpn connect`

At first glance, Snarkypuss can sound like a very small project. Install WireGuard on a VPS, forward some packets, put a web page in front of commands such as `nordvpn connect`, and the job appears to be finished.

That describes the demonstration. It does not describe a dependable gateway.

A real system has to coordinate several pieces of networking state. WireGuard must remain reachable while the upstream VPN changes routes. IP forwarding has to send traffic to the correct interface. DNS has to follow the intended path. Firewall and leak-protection rules must agree with the selected operating mode. The software has to distinguish a provider that is disconnected from one that is connected but not actually carrying traffic as expected.

Destinations introduce another problem. VPN providers change their networks, so Snarkypuss discovers the provider's current choices instead of assuming that an embedded server list stays correct.

Then there is lifecycle engineering: installation, configuration, upgrades, service startup, reboots, database changes and recovery from mistakes. A networking tool that works only until the next reboot is not much of a gateway.

None of these problems is individually exotic. The complexity comes from making them work together while preserving one simple promise: the dashboard should report the route that Snarkypuss can actually verify.

What Snarkypuss Does—and Doesn't Do

Snarkypuss creates and controls a private network path from your computer, through your own VPS, and onward through a commercial VPN provider. It also tries to make the effective state of that path visible, so that a failed VPN connection is not mistaken for a protected one.

That is useful, but it is not the same thing as anonymity. Snarkypuss does not prevent websites or services from identifying you by other means, does not change anyone's obligations under applicable law, does not defeat lawful legal process, and does not control what your VPS host or VPN provider records, retains or is required to disclose.

The Snarkypuss Project

Snarkypuss is an open-source, non-commercial software project. There is no Snarkypuss company, hosted VPN service, central relay network or subscription.

NordVPN is the currently supported and tested commercial VPN provider. Provider-specific commands are isolated behind an adapter so that other providers can be added without redesigning the application.

Snarkypuss itself is free software. You separately pay for a low-cost VPS, approximately US$5 per month, and whatever commercial VPN subscription you choose.

snarkypuss.ca — documentation, and the source at **github.com/topquark22/Snarkypuss**

The current release is **Snarkypuss 2.0.0**.

Brochure edition 1.0.1 · built 17 September 2026. Legal and policy content on pages 2–4 reflects the 17 September 2026 snapshot and is not updated by rebuilding.

Your connection. Your server. Your choice.

SNARKYPUSS

PRIVATELY HOSTED · OPEN SOURCE · NON-COMMERCIAL

snarkypuss.ca