The Russian Censorship Circumvention. Tom's Traps, and Jerry's VPN: A 5-Year Journey

vitaly_repin@fsfe.org

31 January 2026

Who is who

Who am I?

Senior software engineer with over 20 years of experience. Networking and security background. FSFE supporter.

Past: Nokia OSSO, Maemo, MeeGo. 🇷🇺 ▸ 🇫🇮 ▸ 🇸🇪 ▸ 🇫🇮

Hobbies: cycling, skiing, gardening, and VPNs ☺.

Disclaimer: I do not represent my current employer here. Content of this presentation does not reflect the position of my employer.

Who is Jerry? What is this presentation about?

Jerry is a commercial VPN provider that has been operating for more than a decade. It is established in the market and provides services to customers worldwide. Including Russia.

This presentation is based on my advisory work with Jerry on censorship circumvention in Russia. Jerry is not my employer. However, I cooperate very closely with Jerry's engineering team.

Jerry put limitations on what information can be disclosed publicly:

- No names of the VPN provider, its employees, or customers.
- No disclosure of the methods used by Jerry today to bypass censorship in Russia.

Who are you?

- Software professional familiar with abbreviations such as VPN, DPI, PPTP, IPSEC.
- Have a basic understanding of what VPN and firewall are.
- Used VPN yourself.
- Interested to learn about Consumer VPNs and censorship circumvention issues.

Introduction

VPN usage

- Enterprise VPNs: Used by companies to:
  - allow remote employees to securely access the company network;
  - connect branch offices together over the internet.
  - IoT, Cloud Connectivity, Data Center Interconnect ...
  - You name it!
- Personal (or Consumer, Commercial) VPNs: Used by individuals to protect their online privacy and access geo-restricted content.

Don't mix these two cases! They are very different even if the underlying protocols are the same.

Consumer VPN use cases

Bypassing geo-restrictions Accessing content that is blocked in certain regions.

Secure public Wi-Fi usage Protecting data when using unsecured networks (e.g., coffee shops, airports).

Privacy protection Hiding the user's IP address and encrypting internet traffic to protect against surveillance.

Bypassing censorship Accessing blocked websites and services in countries with internet censorship.

Do you really need commercial VPN?

The Cybersecurity and Infrastructure Security Agency (CISA), 2024:

> *Do not use a personal virtual private network (VPN). Personal VPNs* ***simply shift residual risks from your internet service provider (ISP) to the VPN provider****, often increasing the attack surface. Many free and commercial VPN providers have questionable security and privacy policies.*

Straight to the point, isn't it?

Our focus: VPNs for Censorship Circumvention

There are countries where users need to bypass local ISP-level censorship to access the open Internet.

Examples: China, Russia, Iran.

Commercial VPN is just a tool to get access to the data needed.

Kwangmyong Intranet in North Korea is an extreme example of state censorship where even commercial VPNs (regardless of the underlying technology) are not helpful: *Kwangmyong* is not connected to the global Internet.

Censorship in Russia

Censorship in Russia, 2026. End-user PoV

Note: we focus exclusively on Internet Censorship in this presentation.

- Blocking web sites (e.g., linkedin.com, instagram.com) and messengers (e.g., matrix, signal)
- Slowing down services (e.g., youtube) and messengers (e.g., telegram)
- Devices using blocked services fail to work properly.

Censorship in Russia, 2026. VPN business PoV

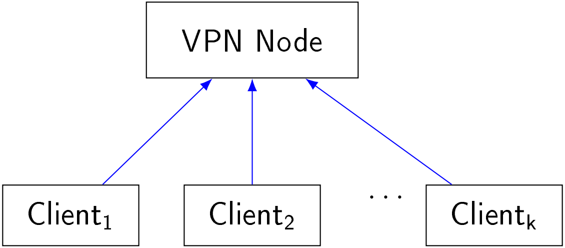
- Deplatforming: application removal requests to app stores (making it harder for the regular users to access VPN apps).
- Hosting block: disallowing non-Russian legal entities to buy VPS hosting in Russia.
- Cutting income streams: ban on advertising in the biggest ads systems (Yandex Ads) and card prosessing for VPN providers.
- Marketing challenges:
  - Propaganda campaign: “VPNs are unsafe, never use them or your money will be stolen!“.
  - Blocking VPN providers web sites.
  - 01.03.2024 ban on popularizing (VPN) services that enable circumvention of internet blocking. Exception: scientific, technical, and statistical information.
  - 30.11.2024 Exception is removed ☺.

Censorship in Russia, 2026. Engineer's PoV

- State-level Internet Filtering Infrastructure. Let's call it *"The Great Russian Firewall"* (GRF) for the sake of simplicity.
- All customer traffic goes via TSPU (ТСПУ, "Технические Средства Противодействия Угрозам" — "Technical Measures to Combat Threats.")
- TSPU boxes are installed in ISPs premises but state has direct control over these boxes.
- Active probing: Немного интеллекта для грубой силы (In Russian, "A bit of brains for the brutal force")
- Different settings for different ISPs, different regions, different times.
- Flexible, dynamic. Looks like as it is under active development.

VPN provider and GRF

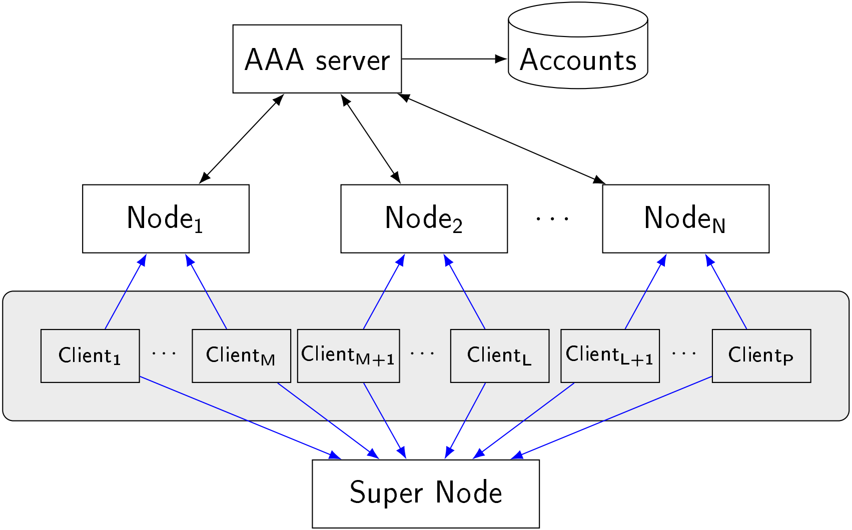
Architecture of your home (personal) VPN



→ Are controlled by GRF. Subject to blocking.

VPN node provides one or several standard VPN protocols (e.g., OpenVPN, WireGuard, IPsec, PPTP, L2TP etc).

Oversimplified architecture of a commercial VPN provider



→ Are controlled by GRF. Subject to blocking.

Evolution of The Great Russian Firewall (GRF), VPN PoV

Approximate timeline based on VPN provider observations:

pre 2022	No VPN blocks
2022-2023	DNS blocks, IP blocks
2023	DPI: blocking of standard VPN protocols (PPTP, L2TP, OpenVPN etc)
2025-	DPI: blocking OpenVPN with XOR obfuscation
2025	White Lists

Jerry's stories

Jerry's strategy

There is no way for a small VPN provider to win against GRF in a direct confrontation. If GRF detects VPN infrastructure, it will be blocked.

Statistical hypothesis testing (GRF):

- H_0: server is not a part of VPN provider infrastructure.
- H_1: server is a part of VPN provider infrastructure.
- Type II error (false negative): H_0 is not rejected although H_1 is true.
- Jerry's goal: maximize the Type II error probability.

Blockings observed by Jerry

Two types of blocks:

1. VPN node is fully blocked. No traffic reaches the node.
2. No traffic comes to all the ports except 443. And first packet of SSL handshake comes to the server!

Jerry's conclusion: In the second case, Tom is not exactly sure that the server is a VPN node. Therefore, we have chances to keep this server functional. At least temporary, until Tom improves his detection methods.

SNI-based blocking

Blocks access to VPN nodes and supernodes based on the content of TLS Hello (SNI field).

Note, news report, November 2024:

> *The use of Transport Layer Security Encrypted Client Hello (TLS ECH) violates Russian legislation and is restricted by technical threat countermeasures Roskomnadzor stated on Thursday. The agency called on Web-based resource owners to disable the extension "or, preferably, use a domestic CDN service."*

DNS-based detection

- Each VPN node had domain name like `node1.vpnprovider.com`.
- Tom started to block freshly configured nodes in a matter of days.
- Root cause: domain names. If the service like spur.us detects your IP as a VPN node, expect Tom to block it soon.

Protocols-based detection

- VPN node had standard VPN protocols enabled (e.g., OpenVPN, L2TP).
- Tom was able to detect and block such nodes in a matter of days.
- Root cause: standard VPN protocols are easily detectable by DPI.

OpenVPN XOR obfuscation detection

- OpenVPN traffic can be obfuscated using XOR encryption.
- Tom finally learnt to detect it and started to block VPN nodes with such traffic in a matter of hours.

But it was an evolution of the GRF capabilities, not a revolution:

- In the beginning, it was enough to switch ports.
- When it stopped helping, changing of the obfuscation mask worked.

It took more than a year for Tom (GRF) to fully close this window of opportunities for Jerry.

White Lists

In 2025 “White Lists” were introduced: only traffic to pre-approved IP addresses and ports is allowed. Usually activated temporary.

Very challenging for Jerry and alike.

Regional and operator differences

GRF tends to work different in different areas and within different ISPs.

It often means beta-testing of new GRF capabilities.

Don't ignore support requests from your users in non-populated regions. It can be an early warning of new Tom's traps coming soon.

Conclusion

Recommendations for VPN providers

- Try to predict new Tom's traps before they are deployed in the field.
- Do not rely on pure hacks (exploiting bugs in the GRF) as a long-term solution.
- Fly under the radar as much as possible.
- Don't focus only on technical aspects. This is just a part of the game, not the whole game.

The future for Russian Internet is dark, perhaps even darker

My personal opinion:

Scenario 1: Kwangmyong Intranet.

- Russian Intranet without connectivity to the global Internet. Except selected officials and institutions.
- This will be the end of the game for VPN providers in Russia.

Scenario 2: GFW, Great Chinese Firewall.

- GRF becomes more sophisticated and mature.
- Tom and Jerry game continues.

Thank you for your attention! Additional reading.

Diwen Xue et al.
OpenVPN Is Open to VPN Fingerprinting.
In Proceedings of the 31st USENIX Security Symposium (USENIX Security 22), pp. 483–500, Boston, MA, USA, August 2022.
Available at: https://www.usenix.org/conference/usenixsecurity22/presentation/xue-diwen

A bit of brains for the brutal force presentation (In Russian).
Available at
https://www.youtube.com/watch?v=4wSxp7t6huA

Acknowledgements

- **China lock icon** (`China.svg`):
  Source: `https://openclipart.org/detail/332036/china-lock`
  License: Creative Commons Zero 1.0 Public Domain License
- **Kwangmyong logog** (`Naenaranewlogo.svg`):
  Source: `https://commons.wikimedia.org/wiki/File:Naenaranewlogo.svg`
  License: Creative Commons CC0 1.0 Universal Public Domain Dedication.

All other graphics and diagrams created by the author using TikZ.