VPN technologies

194.144 Privacy-Enhancing Technologies

Dr. Martin Schmiedecker

Outline

VPN technologies

- TLS-based
- Wireguard

VPN-ish alternatives

VPNs

First things first: Trust!

- Whatever you use: trust is key
- ”No logging“ $==$ pinky-promise
- VPNs doing advertisements now ...
- Remember: they get all your traffic!
- Self-hosting is easy

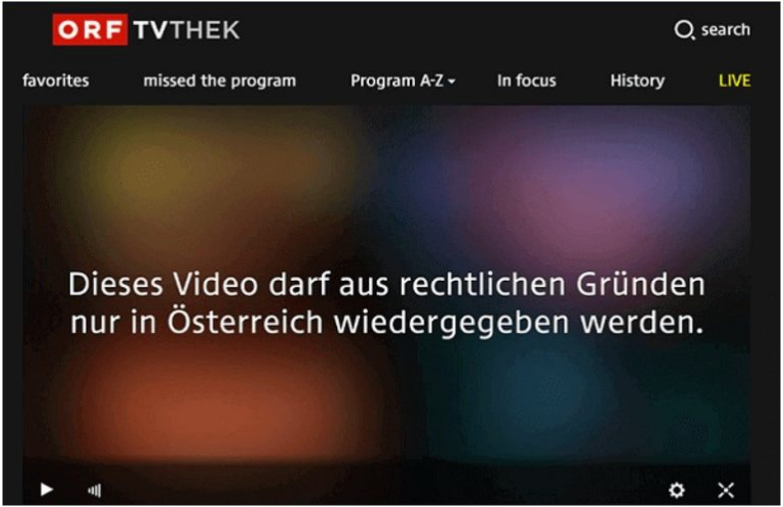
VPNs

VPNs

Why are VPNs important?

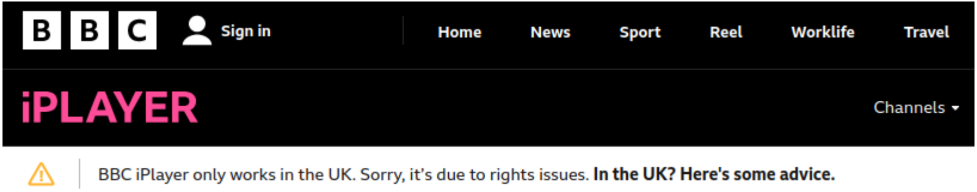
- Corporate world loves them
- Every firewall has a VPN client nowadays
- Geoblocking is a thing!

Geoblocking

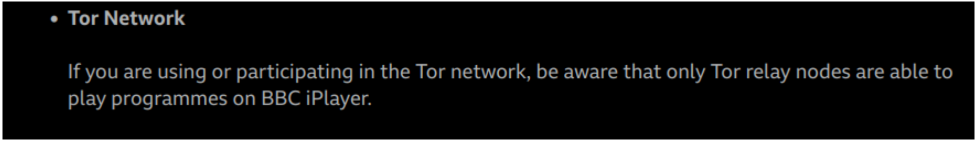


Dieses Video darf aus rechtlichen Gründen nur in Österreich wiedergegeben werden.

Geoblocking



⚠ BBC iPlayer only works in the UK. Sorry, it's due to rights issues. **In the UK? Here's some advice.**



- **Tor Network**

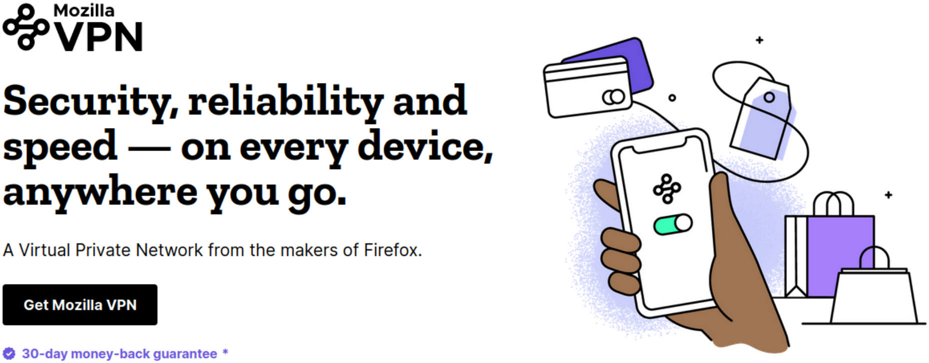
  If you are using or participating in the Tor network, be aware that only Tor relay nodes are able to play programmes on BBC iPlayer.

Different VPNs

Commercial Providers:

- NordVPN
- ProtonVPN
- Mullvad
- RiseupVPN
- Online ads: <insert VPN provider here>

Different VPNs



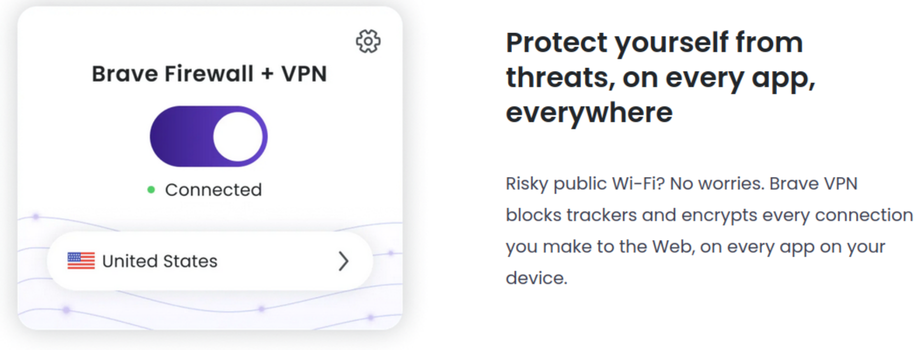
Mozilla VPN

Security, reliability and speed — on every device, anywhere you go.

A Virtual Private Network from the makers of Firefox.

30-day money-back guarantee *

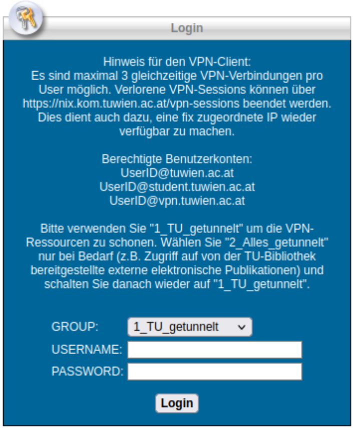
Different VPNs



Protect yourself from threats, on every app, everywhere

Risky public Wi-Fi? No worries. Brave VPN blocks trackers and encrypts every connection you make to the Web, on every app on your device.

Different VPNs



Hinweis für den VPN-Client:
Es sind maximal 3 gleichzeitige VPN-Verbindungen pro User möglich. Verlorene VPN-Sessions können über https://nix.kom.tuwien.ac.at/vpn-sessions beendet werden. Dies dient auch dazu, eine fix zugeordnete IP wieder verfügbar zu machen.

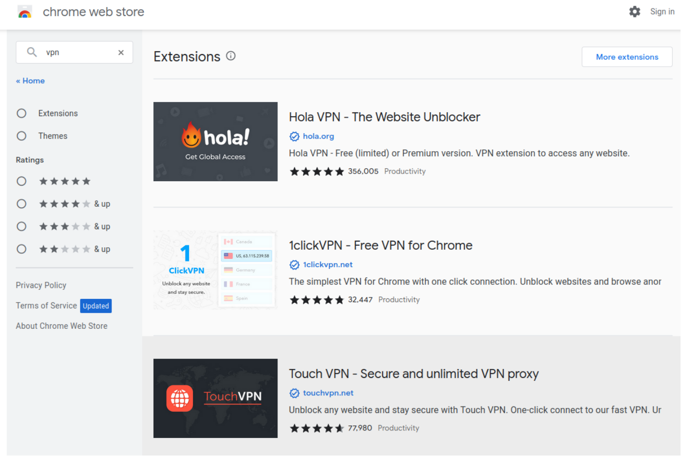
Berechtigte Benutzerkonten:
UserID@tuwien.ac.at
UserID@student.tuwien.ac.at
UserID@vpn.tuwien.ac.at

Bitte verwenden Sie "1_TU_getunnelt" um die VPN-Ressourcen zu schonen. Wählen Sie "2_Alles_getunnelt" nur bei Bedarf (z.B. Zugriff auf von der TU-Bibliothek bereitgestellte externe elektronische Publikationen) und schalten Sie danach wieder auf "1_TU_getunnelt".

GROUP: 1_TU_getunnelt
USERNAME:
PASSWORD:

Different VPNs

Even chrome extensions??



Hola VPN - The Website Unblocker

hola.org

Hola VPN - Free (limited) or Premium version. VPN extension to access any website.

★★★★★ 356,005 Productivity

1clickVPN - Free VPN for Chrome

1clickvpn.net

The simplest VPN for Chrome with one click connection. Unblock websites and browse anor

★★★★★ 32,447 Productivity

Touch VPN - Secure and unlimited VPN proxy

touchvpn.net

Unblock any website and stay secure with Touch VPN. One-click connect to our fast VPN. Ur

★★★★★ 77,980 Productivity

VPN technologies

VPN technologies

Most VPNs today are TLS-based:

- Plenty of software available
- Libraries, server software, everything
- Fast, and used widely
- Devil is in the details (as always)

Time Flies

Obsolete protocols:

- PPTP
- L2TP
- ?
- cipher suites, e.g. 3DES

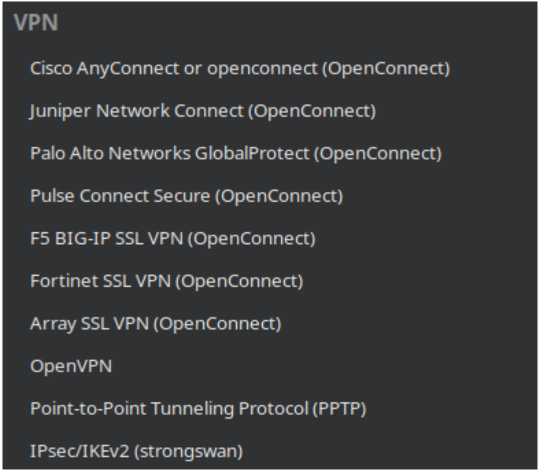
TLS VPN

How its used:

- site-to-site
- user-to-site
- split tunneling, sometimes

TLS VPN

Examples:



VPN

Cisco AnyConnect or openconnect (OpenConnect)

Juniper Network Connect (OpenConnect)

Palo Alto Networks GlobalProtect (OpenConnect)

Pulse Connect Secure (OpenConnect)

F5 BIG-IP SSL VPN (OpenConnect)

Fortinet SSL VPN (OpenConnect)

Array SSL VPN (OpenConnect)

OpenVPN

Point-to-Point Tunneling Protocol (PPTP)

IPsec/IKEv2 (strongswan)

TLS VPN

OpenVPN:

- second-best open-source option for user-to-site
- rather easy to set up
- never used it myself though

TLS VPN

VPN endpoints are commonly exploited:

- always online
- hard to patch
- 2020 and later in particular
- CISA releases list of commonly exploited CVEs[1]

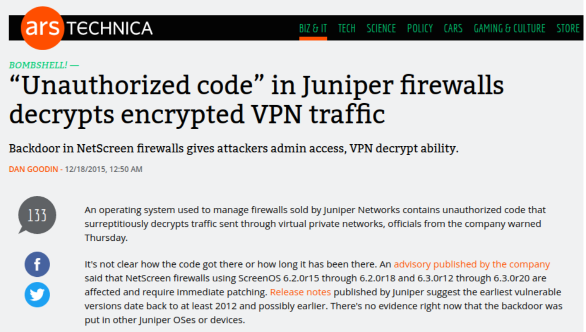
[1] Source here

TLS VPN

“Two backdoors, and a command injection”[2]:

TLS VPN

Examples:



BOMBSHELL! —

“Unauthorized code” in Juniper firewalls decrypts encrypted VPN traffic

Backdoor in NetScreen firewalls gives attackers admin access, VPN decrypt ability.

DAN GOODIN - 12/18/2015, 12:50 AM

An operating system used to manage firewalls sold by Juniper Networks contains unauthorized code that surreptitiously decrypts traffic sent through virtual private networks, officials from the company warned Thursday.

It's not clear how the code got there or how long it has been there. An advisory published by the company said that NetScreen firewalls using ScreenOS 6.2.0r15 through 6.2.0r18 and 6.3.0r12 through 6.3.0r20 are affected and require immediate patching. Release notes published by Juniper suggest the earliest vulnerable versions date back to at least 2012 and possibly earlier. There's no evidence right now that the backdoor was put in other Juniper OSes or devices.

IPSec

Whats in the box?

- Can provide authentication, and encryption
- Rather complex protocols
- 50+ RFCs
- telco-heavy, and 90ies touch

IPSec

Protocols in use within IPSec:

- Authentication Header (AH)
- Encapsulating Security Protocol (ESP)
- Security Association (SA): key exchange(s), such as IKEv2

IPSec

Different modes:

- Transport mode: only payload encrypted/authenticated
- Tunnel mode: everything encrypted/authenticated
- Tunnel mode is packet-in-packet
- Destination is thus encrypted

Wireguard

Current champion:

- easy, fast, simply better
- part of linux kernel
- numerous implementations: go, rust, C, ...
- Mikrotik and FritzBox (experimental)

Wireguard

Under the hood:

- X25519 for key exchange
- ChaCha20 for symmetric encryption
- Poly1305 for message authentication codes
- BLAKE2s for cryptographic hash function
- UDP-only

VPNs

What is missing:

- Apple Private Relay
- Tailscale
- Algo & Streisand?
- mobile use cases, Google Jigsaw

VPN-ish alternatives

SSH Tunnel

SSH for SOCKS proxy

- not only for remote admin
- -N while connecting, and a port (-D)
- point browser to local port
- use remote IP

MACsec

802.1AE aka MACsec

- for local networks, layer 2
- AES-GCM-128 with implicit integrity protection
- easy in Linux, routers, and some switches

Direct Links

Point-to-point links:

- Layer 2, over wifi
- 5 GHz, and 60 GHz
- 1+ Gbs throughput
- Funkfeuer in Vienna
- line-of-sight necessary

Other things

Trust, but verify:

- private APN: trust the provider
- MPLS: trust the provider
- private 5G networks: trust the provider

Starlink

Why bother with local ISP(s)?

- works everywhere
- rather cheap
- thousands of satellites in lower-earth orbit
- great talk from Lennert Wouters at Blackhat 2022

"May you always live in interesting times"

What’s ahead of us?

Airtags:

- dead-cheap Bluetooth trackers
- every Apple device in range uploads position of them
- cryptographically tied to owners Apple ID
- check out the paper(s) by Seemoo Labs[3]
- AirGuard from Playstore

[3] See here

What’s ahead of us?

Future funky stuff:

- ODoH, DoQ, DNSSEC? IPv6?

Ecosystems:

- Apple, Cloudflare, AWS, Azure, …

What’s ahead of us?

MOAR of everything:

- devices
- connectivity
- complexity
- users & user expectations

And just like that,
it’s a wrap!

FIN

That’s it:

- it was our pleasure!
- see you at the exam
- no clue yet how 6 ECTS is going to look like