eduVPN

BoF

François, Jeroen, Tangui, Rogier, Maxime

Helsinki

June 8th

tnc26

Co-funded by
the European Union

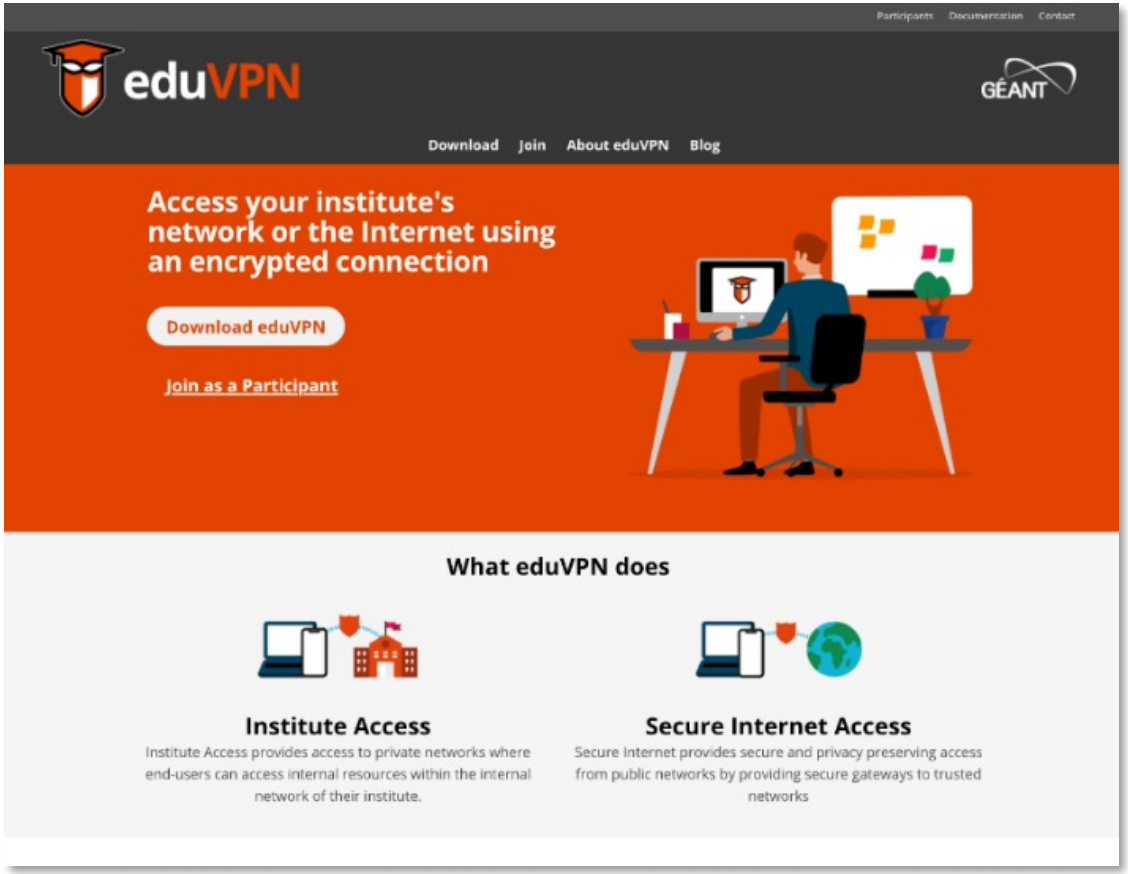
What is eduVPN?

- Project that provides VPN *server* and *client* software
- Server runs on standard Linux distributions (Debian, Ubuntu, Fedora, Enterprise Linux)
- Clients available for all common OSes (Windows, macOS, Linux, Android, iOS)
- Leverages existing VPN technologies (WireGuard + OpenVPN)
  - eduVPN "Innovation": WireGuard over TCP with ProxyGuard
- Uses permissions to allow/restrict access to VPN networks ("Profiles")

Intro

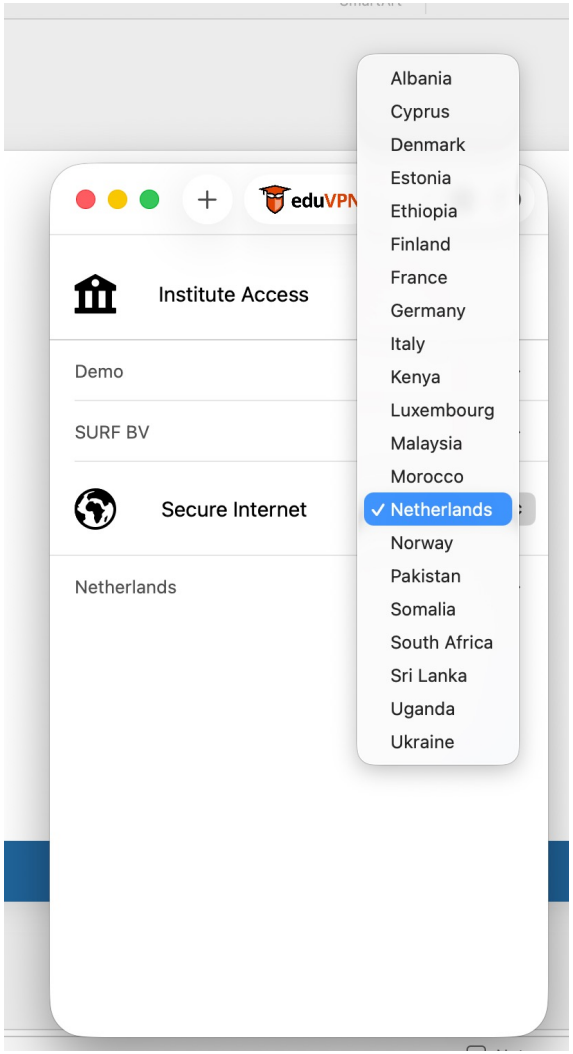
- Institute access:
  - Access resources
  - ~262 servers

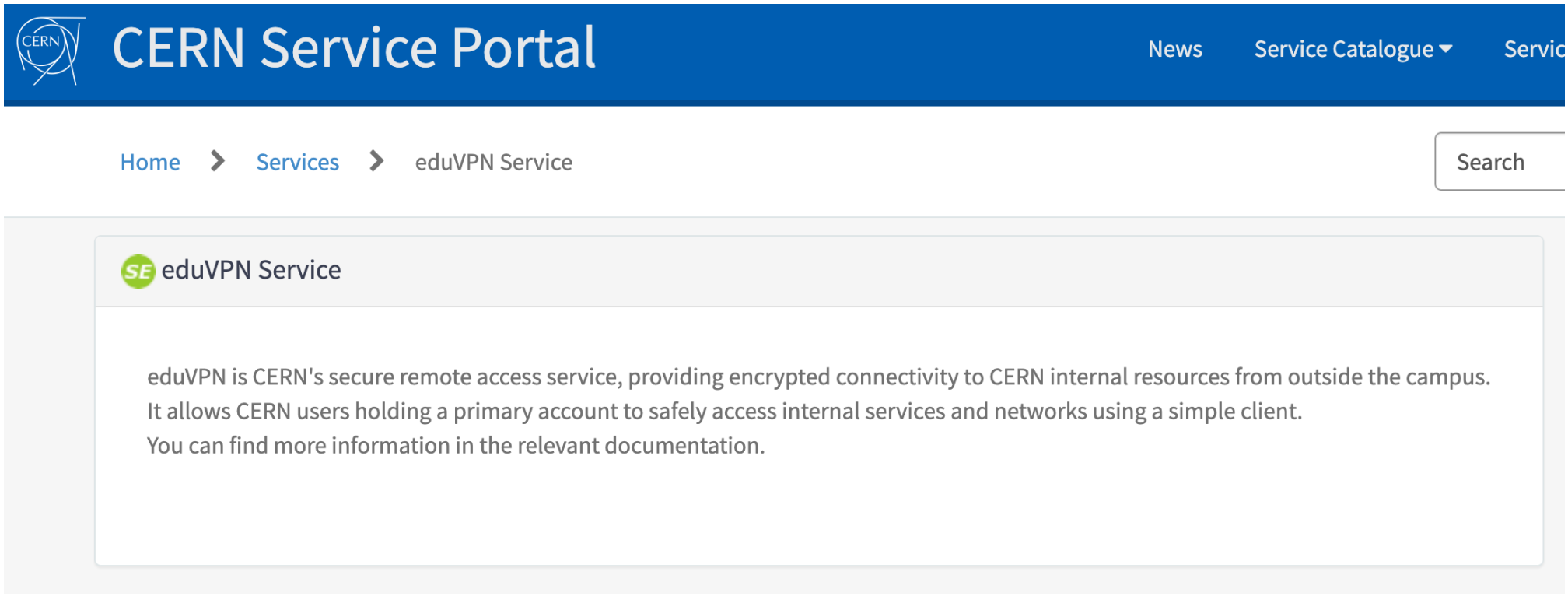
- Clients for:
  - Windows
  - macOS/iOS
  - Linux
  - Android



Intro

- Secure Internet:
  - Connect to a NREN
  - Currently 21 countries
  - Use case: Public hotspots




CERN Service Portal
News
Service Catalogue
Servic
Home
Services
eduVPN Service
Search
eduVPN Service
eduVPN is CERN's secure remote access service, providing encrypted connectivity to CERN internal resources from outside the campus.
It allows CERN users holding a primary account to safely access internal services and networks using a simple client.
You can find more information in the relevant documentation.

Example: University of Turku

- 22000 students & 3400 staff
- Harware EOL
- Requirements:
  - Use public IP addresses and avoid NAT
  - Multiple nodes for load balancing and fault-tolerance
  - webSSO and MFA
  - provide access management that supports separating group members by their own IP addresses
  - Wide client support
  - high performance and coexistence with Microsoft's Always-On VPN (because we also use Microsoft's IPsec-based Always-On VPN to connect Windows laptops to our essential services when outside our campus network)

Client Audits

- We spend 41k on client audits (funded bij Nordunet)
- We hired the best pentesting firm
- The results…. No issues found

- We spend 4 dollar on A.I. pentesting

VPN audit by Midnight Blue

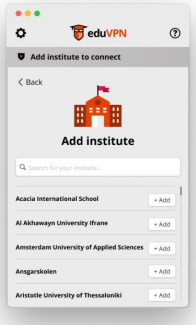
- VVTS (VPN Vulnerability Testing Suite)
- Over 10 attacks tested on multiple operating systems and VPN configurations

eduVPN Client	LocalNet	LocalNet IPv6	ServerIP	ServerIP IPv6	Expanded Subnet	TunnelVision	TunnelVision on Connection Established	TunnelVision IPv6	TunnelVision IPv6 on Connection Established	IPv4 to IPv6 Localnet	NAT64
Windows, Wireguard, local traffic blocked	⊘	⊘	✓	✓	⊘	⊘	⊘	⊘	⊘	⊘[1]	✓[2]
Windows, Wireguard, local traffic allowed	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓[2]
Windows, OpenVPN	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓[2]
macOS, Wireguard	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗[3]	✓
macOS, OpenVPN	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗[3]	✓
Linux, Wireguard, local traffic blocked	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓[2]
Linux, Wireguard, local traffic allowed	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓[2]
Linux, OpenVPN	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓[2]
Android, Wireguard	✓	✓	✓	✓	✓	✓[4]	✓[4]	✓	✓	✓	✓
Android, OpenVPN	✗	✗	✓	✓	✓[5]	✓[4]	✓[4]	✓	✓	✓	✓
iOS, Wireguard	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗[3]	✓
iOS, OpenVPN	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗[3]	✓

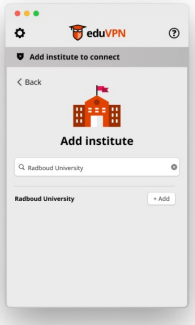
https://github.com/MidnightBlueLabs/VVTS/

UX Recommendations – funded by Nordunet

Screen 1A — Welcome screen



Screen 2A — Institute search



Screen 2B — Institute search with input

Future

- eduVPN server v4
  - webGUI config editing
  - Focus on large deployments (HA/failover)
  - No more OpenVPN
- New client UX
- Student research

Thank you

Any questions?

Rogier.Spoor@SURF.nl

tnc26

Co-funded by
the European Union