



# Security, the community way

**Tangui Coulouarn**  
DeiC  
**Rogier Spoor**  
SURF

Internet2 Technology Exchange, Minneapolis

21 September 2023

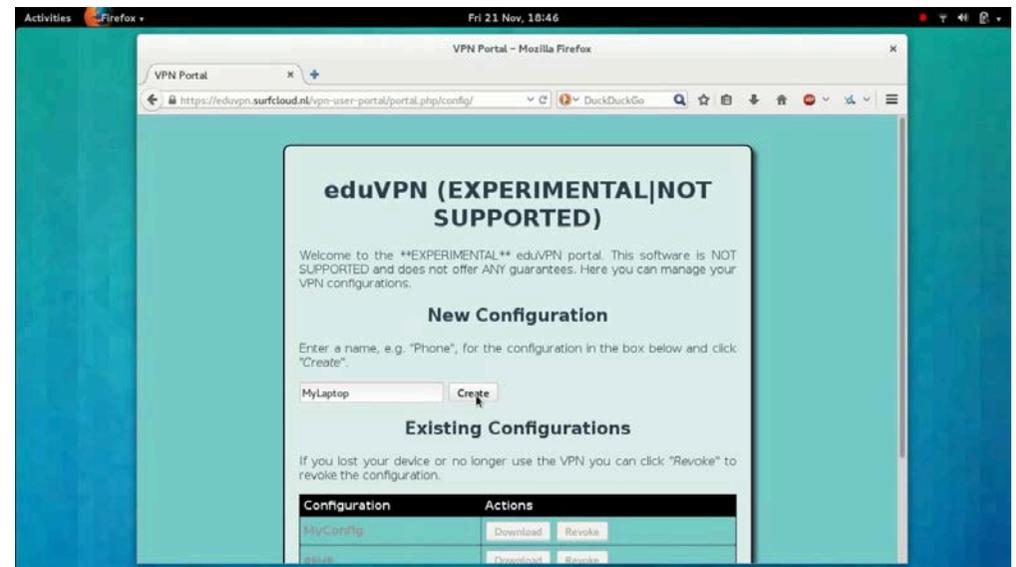
Public

- eduVPN is an edu service built by collaboration by several NRENs, supported by GEANT
- Free and Open Source Software
- Customized for our community and users
- Tested and audited
- Regular security updates and evolution



## How did it start?

- Innovation programme at SURF in 2014
- Realisation that staff and students used a lot of shady VPN services
- First use case: "Secure Internet", i.e. access the public internet through trusted gateways



Screenshot of eduVPN in 2015

## The Institute Access use case

- Replace the corporate VPN solution to let staff and students access resources on a private network
- Emerged right away but tricky due to procurement cycles
- Early adoption in the Netherlands

## Requirements (1)

- Use of open source software as a security requirement: OpenVPN (then)
- Integration with IdM used at universities
  - Do not require users to know the server name, but allow them to search for their institute
  - Re-use the credentials from their institute in a safe way (through WebSSO)
- Allow for hosting the server elsewhere and have a L2 connection to the institute
  - > here WebSSO is even more important... no need to give credentials to VPN provider

## Requirements (2)

- Scales to 100k concurrent users and beyond
- High availability
- Native IPv6 support out of the box
- Available as Linux server packages
  - Easy install
  - But more important: easy updates (apt, yum, dnf)
- No per-seat licensing, so you only pay for hardware (and server administration)

## Involved Organisations

2014

Started simple VPN webservice



2016

Client app development start. SIDN fund co-fund the open-source development. NORDUnet sponsoring.

SIDNfonds

NORDUnet  
Netherlands Gateway for Research & Education



2017

Vietsch foundation co-fund easy-to-use apps. RIPE Community fund co-fund development. Software Governance via Commons Conservancy foundation. AARNet, DeIC, NORDUnet, GÉANT, SURFnet in board. NLnet opened eduVPN fund.



DeiC  
Dutch Infrastructure Consortium



GÉANT

RIPE



THE COMMONS  
CONSERVANCY



SIDNfonds

NORDUnet  
Netherlands Gateway for Research & Education



2018

eduVPN entered GÉANT project eduVPN software approved by GÉANT. URAN, RENU, UNINETT and DFN run eduVPN pilot.



deutsches forschungsnetz

DeiC  
Dutch Infrastructure Consortium



GÉANT

RIPE



THE COMMONS  
CONSERVANCY



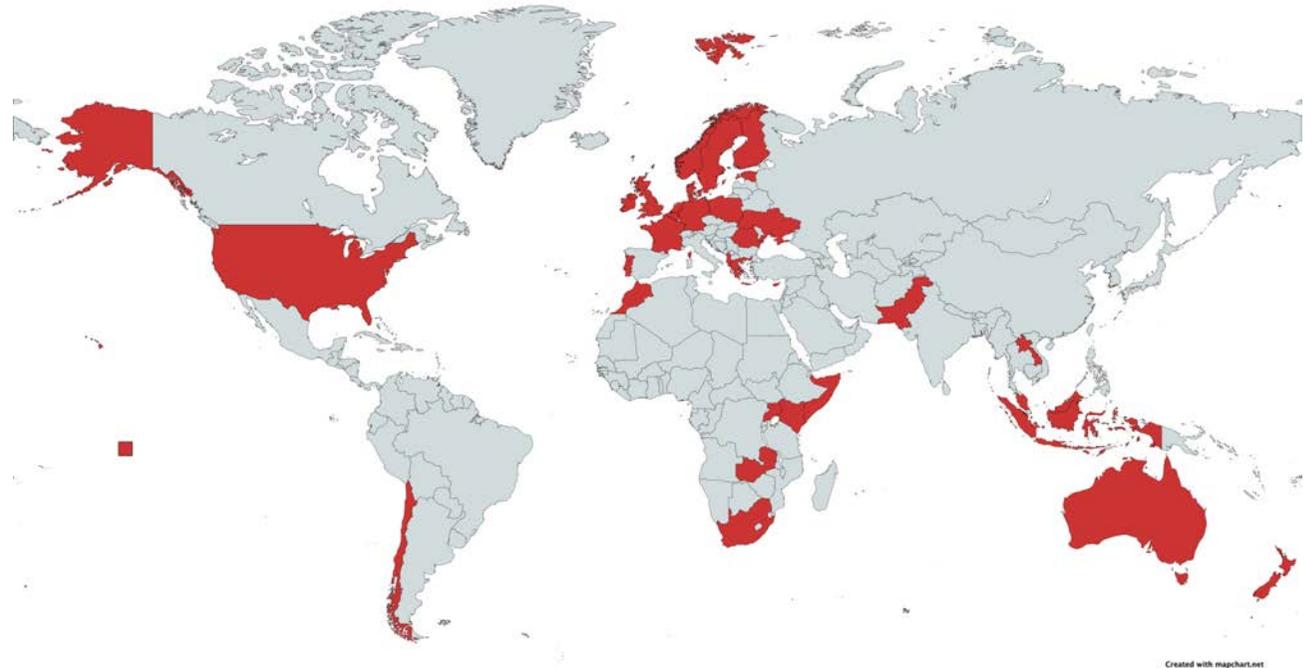
SIDNfonds

NORDUnet  
Netherlands Gateway for Research & Education



## eduVPN today

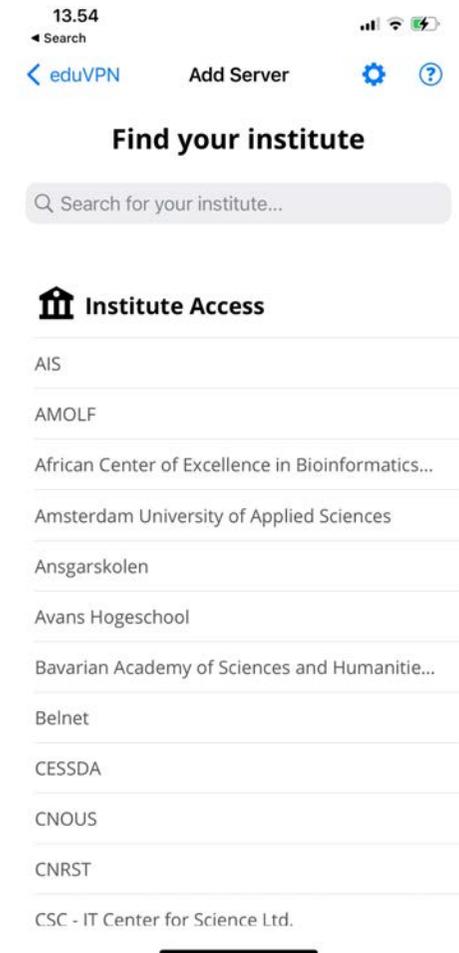
- At least 138 universities and 17 NREN deployments
- Used in (at least) 33 countries
- Most successful in the Netherlands (27), Germany (26 universities), Uganda (9)



## What is eduVPN?

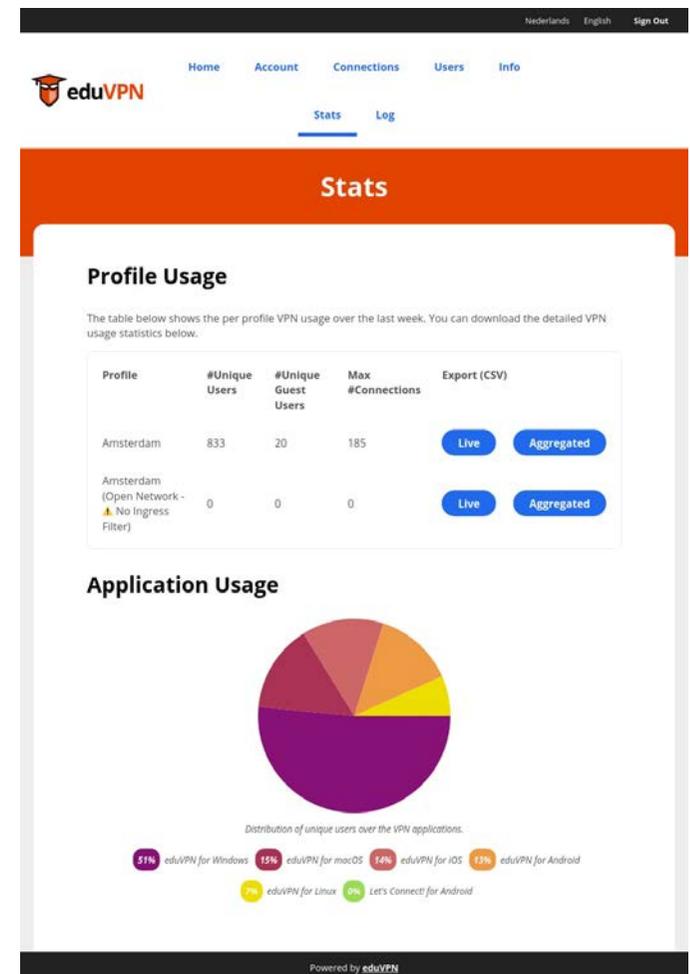
- VPN software package with
  - server side components
  - client apps for Linux, Windows, iOS/macOS and Android
- Supports WireGuard and OpenVPN
- Integrates well with identity management systems at universities (SAML, LDAP, RADIUS, OpenID Connect, Client certificates)
- Granular profiles + possibility to provision managed devices
- Scales from Raspberry Pi to multi-node deployments

See <https://docs.eduvpn.org/server/v3/> for full feature list



## What is eduVPN? (2)

- Used in production by universities (Institute Access) and NRENs (Secure Internet)
- Also used outside R&E as “Let’s Connect!” (+ collaboration with govroam). Apps can be rebranded.
- Software governance via The Commons Conservancy foundation
- Service governance via GÉANT
- 2 main models of deployment: run-by-university or managed by NREN



## Regular audits

Date	Type	By
Q4-2016	Server audit	Radically Open Security
Q4-2017	Windows app audit	Fox-IT
Q1-2018	Server audit	Radboud University
Q3-2018	Android app audit	GÉANT
Q4-2018	iOS/macOS app audit	Radically Open Security
Q4-2019	TunnelKit (iOS/macOS) library “fuzzing”	Guido Vranken
Q4-2020	SAML (php-saml-sp) audit	Cure53
Q1-2021	iOS/macOS app audit	Midnight Blue
Q4-2022	3.x Server audit	Cure53
Q4-2022	Go-library audit (new linux client)	Radically Open Security

## The Commons Conservancy

- The Commons Conservancy is an 'organisation hypervisor' that can spawn and support virtual open source foundations
- Each Programme runs independently from all the others, in perfect isolation
- Each Programme determines its own operating environment (such as bylaws) with templates provided, and has own infrastructure (website etc.)
- Templates to manage the legal stuff + support for the financial stuff



## What does it cost? Examples from the Netherlands

- Costs at university marginal if stand-alone instance: installation costs, price of a VM/bare metal server
  - Typical price: set-up of one VM charged 1200 EUR, 600 EUR per extra server
  - Price per trimester for 2 core, 2GB RAM, 100 GB HDD: 300 EUR
  - Maintenance costs (0.1 FTE)

Costs for university when eduVPN is a hosted service: Depending on university size: in range 937 - 1377 euro per month

## For comparison: cost of commercial VPN solution at a Danish University

- 11000 students and 6000 staff
- Requirements/features:
  - 1000 concurrent users;
  - Hardware with 10Gbps interfaces;
  - Differentiated access to services according to type of user, equipment used.
- Cost in 2019: 100 kEUR for hardware + 35 kEUR in licenses for 3 years
- Supplement for extra licences paid when COVID19 to be able to serve more users
- Cheap extra license renewal in 2022 for 3 years (10kEUR)
- UX is not impressive: username and password + Microsoft second factor
- Maintained by the IT department
- Includes hardware but not network costs, maintenance, power, etc.

## Example 1: Stand-alone instance. Otago University

- Need to scale up because of CoVID-19: use existing nearly EOL hardware. Needed to either buy new concentrators for 300 kUSD or look at alternatives
- Requirement for MFA
- Choice of eduVPN because they could reuse existing compute hardware + use of SAML and by extension leverage Azure Active Directory with conditional access (MFA)
- Use of php-saml-sp (a component we built) as it was easier to setup with Azure AD working out of the box with minimal changes

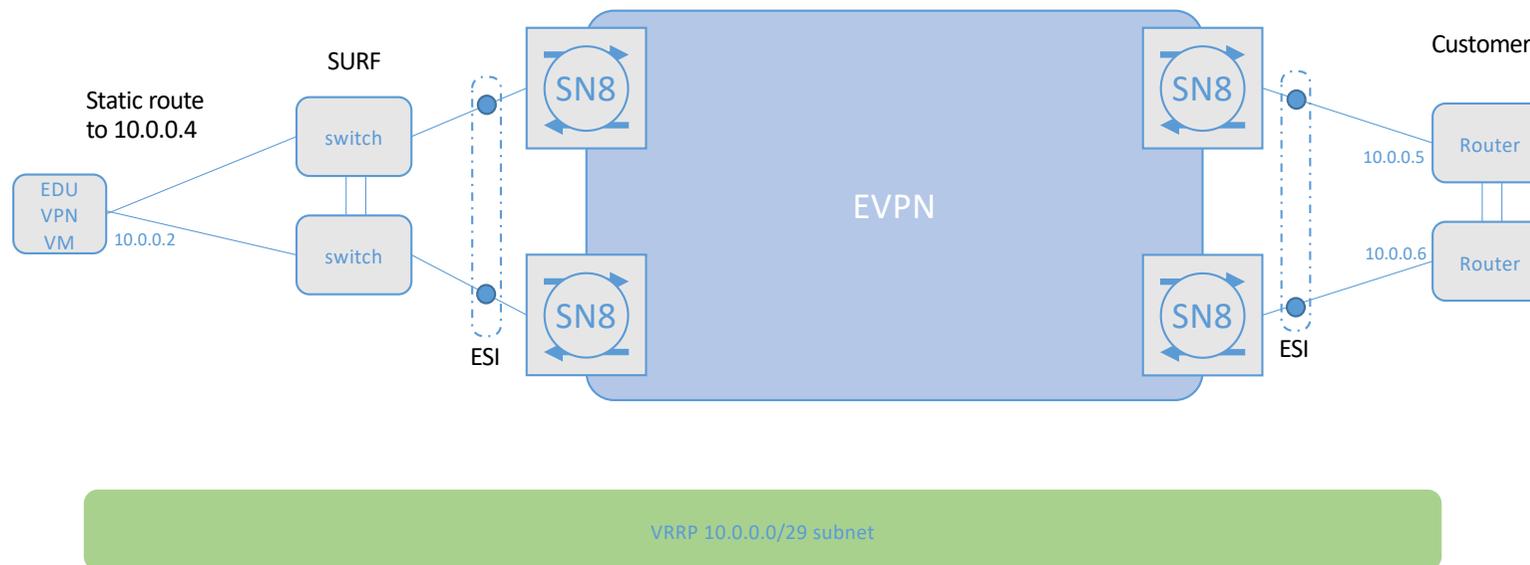
## **Example 2: eduVPN on shared resources. LRZ in Germany.**

- Regional computing centre providing network for several higher education institutions in the Munich area
- During pandemic, often 6000+ concurrent users
- Their solution was EOL
- Standard OpenVPN tested but lacked features (including automatic client configuration updates)
- Now operates eduVPN for most institutions in the greater Munich area
  - Single server for each of the three biggest universities based on VPN user access: TUM, LMU and HM;
  - one “catch all” server for the other institutions;
  - one dedicated server for LRZ.

## Example 3: Institute Access as a Managed Service for a whole NREN

- Model currently implemented in the Netherlands (.BE .NO same implementation model)
- eduVPN instance managed centrally by SURF
- Support by SURF
- No need for hardware on campus or licensing limitations

## Institute access redundant design



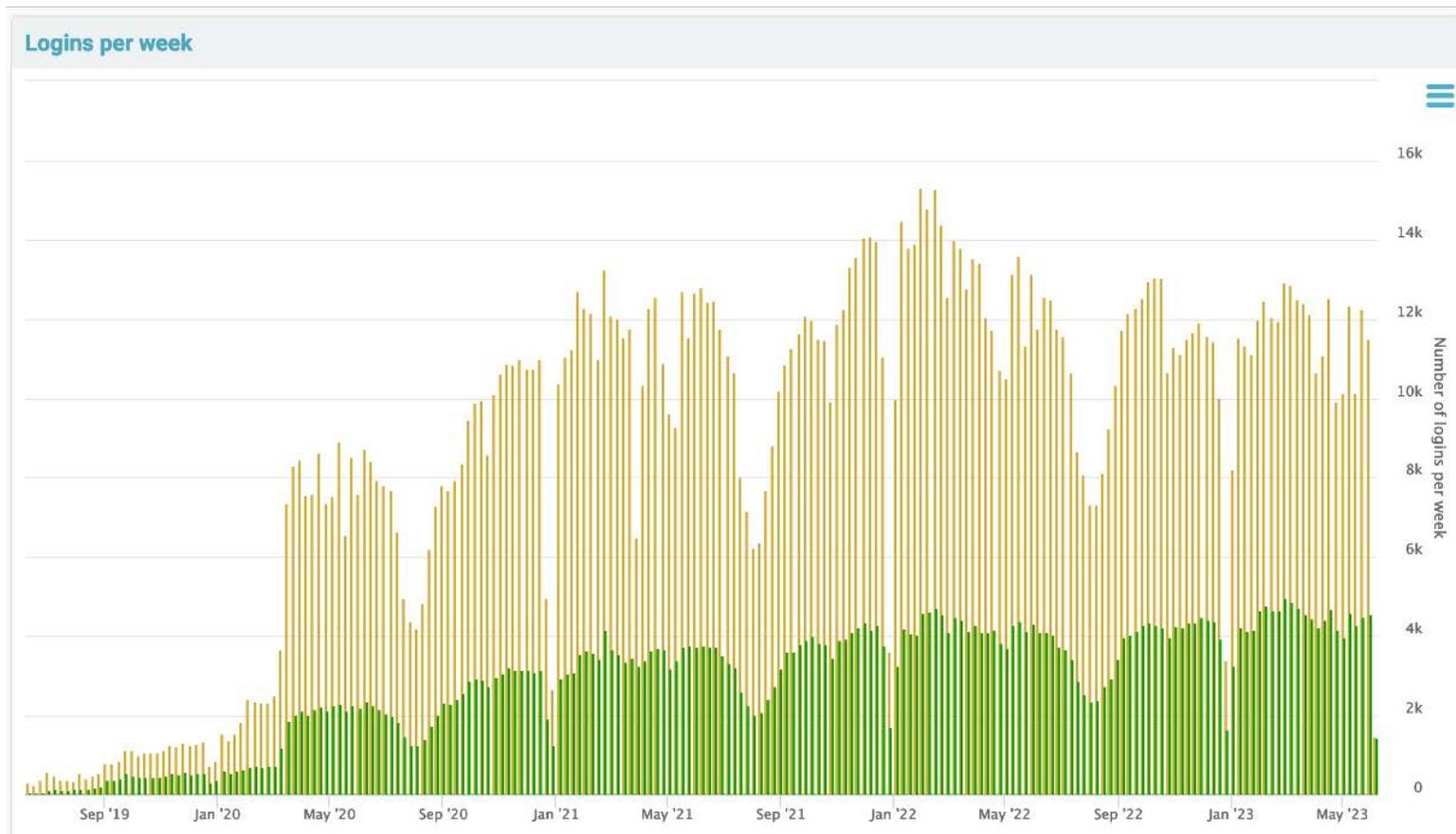
## Currently 34 paying customers in .NL

- Universities: 6
- Research: 4
- Lower educational: 8
- Polytechnics: 9
- Other institutes: 6
- Academic Hospital: 1

Reason why some not interested:

- Recently moved to new VPN concentrator/firewall
- Recently bought firewall has VPN feature too
- Like to do it themselves
- Everything is in the cloud “we don’t need VPN”
- They want managed device VPN (which we are working on)

## Statistics from one university in the Netherlands



## Feedback from the field

- Use eduVPN for bulk-VPN.
- Institute Access: Only create a few profiles.
- Managed Institute Access: experience like a cloud service
- Some institute likes to receive syslog, to be more in control

## Set up your own eduVPN instance in 6 steps

1. get a VM with one of the supported OSes
2. follow the deploy instructions
3. configure network (if necessary)
4. configure authentication
5. test server with eduVPN apps (by specifying hostname in search box)
6. request to be registered in eduVPN apps

<https://docs.eduvpn.org/server/v3/#installation>

## Contact

eduVPN Team: [eduvpn-support@lists.geant.org](mailto:eduvpn-support@lists.geant.org)

Web: <https://www.eduvpn.org>

Documentation: <https://docs.eduvpn.org/>

Me: [tangui.coulouarn@deic.dk](mailto:tangui.coulouarn@deic.dk)



# Thank You

Any questions?

[www.geant.org](http://www.geant.org)



Co-funded by  
the European Union