eduVPN

How to deal securely with generalised remote working

Tangui Coulouarn, DeiC

UbuntuNet Connect, 18 November 2020

Public

www.geant.org

“Amid the COVID19 first-wave pandemic, and the increasing necessity of teleworking that derived from the confinement period, the Information and Communications Systems Services Unit of University of Minho, was tasked with the development of a contingency plan in several areas, regarding this new scenario. Remote Access service (VPN) was one of the areas for which there was the need to increase the service capacity to support an exponential growth in remote workforce.

After some research, we preselected the eduVPN, a community project supported by GÉANT. This community project has the features that meet our requirements and is based on well-known and tested open source technologies. After a brief assessment we decided to adopt it.

The main points in favor are: **i) the absence of licensing and financial costs; ii) simplicity of use for our end-users especially those with mobile clients; iii) has applications for all the major platforms; iv) an architecture capable of horizontal scalability that allowed us to repurpose some servers for the project.**”

Marco Teixeira, University of Minho, Portugal

“In Turku University of Applied Sciences, we use a lot of software that requires access to Licensing servers.

Formerly we had a basic OpenVPN solution for one software, for few student groups so they were able to use it at home. When COVID-19 quarantines began the list of required software got a lot bigger. Luckily, we had already familiarized ourselves with eduVPN in test environment.

We found that benefits with eduVPN are quite markable. Self-enrollment and SAML authentication made it easy to distribute eduVPN to larger number of users. It was also cost effective and we have familiar community to solve possible issues.

For now, eduVPN offers our students, staff and affiliates access to resources that are required to teach and study effectively and safely. We can provide software licenses when license terms allow for remote access. Additional services have already been planned but not yet implemented.”

Simo Lamminen, Turku University of Applied Sciences, Finland

Why eduVPN?

A common and **customised VPN** offer adapted to the **needs** of the **international research and education community**.

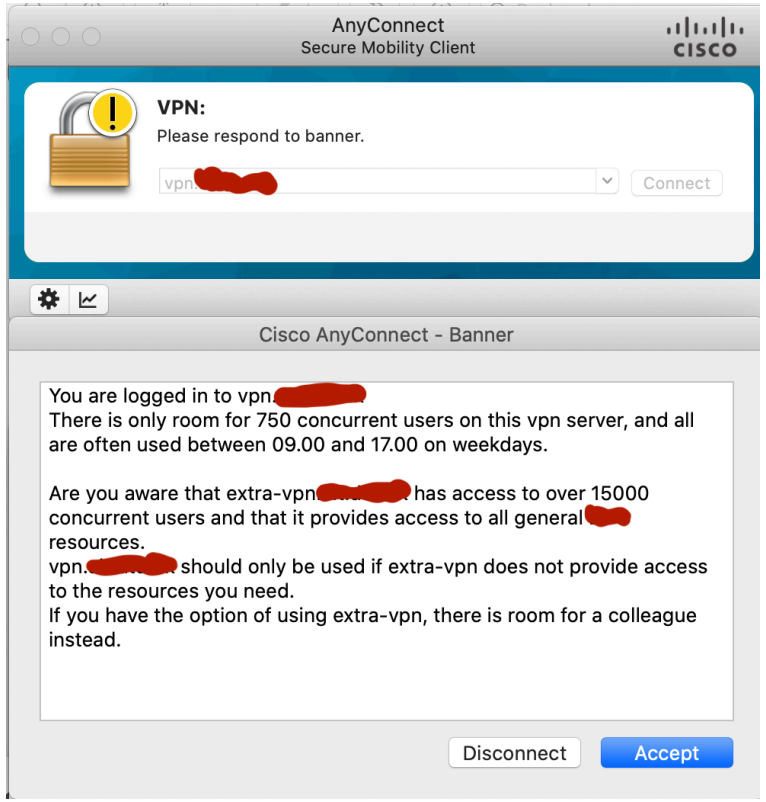
1. Result of **collaboration** of various **NRENs, governed by GÉANT**.
2. Inspired from **eduroam** (UX Oriented)
3. **Open Source**
4. **Customised** for our community and users
5. **Tested** and **approved** by many
6. Regular **security updates** and **evolution** (sovereignty)

We are aware it is 2020 and most universities already have VPN solutions.

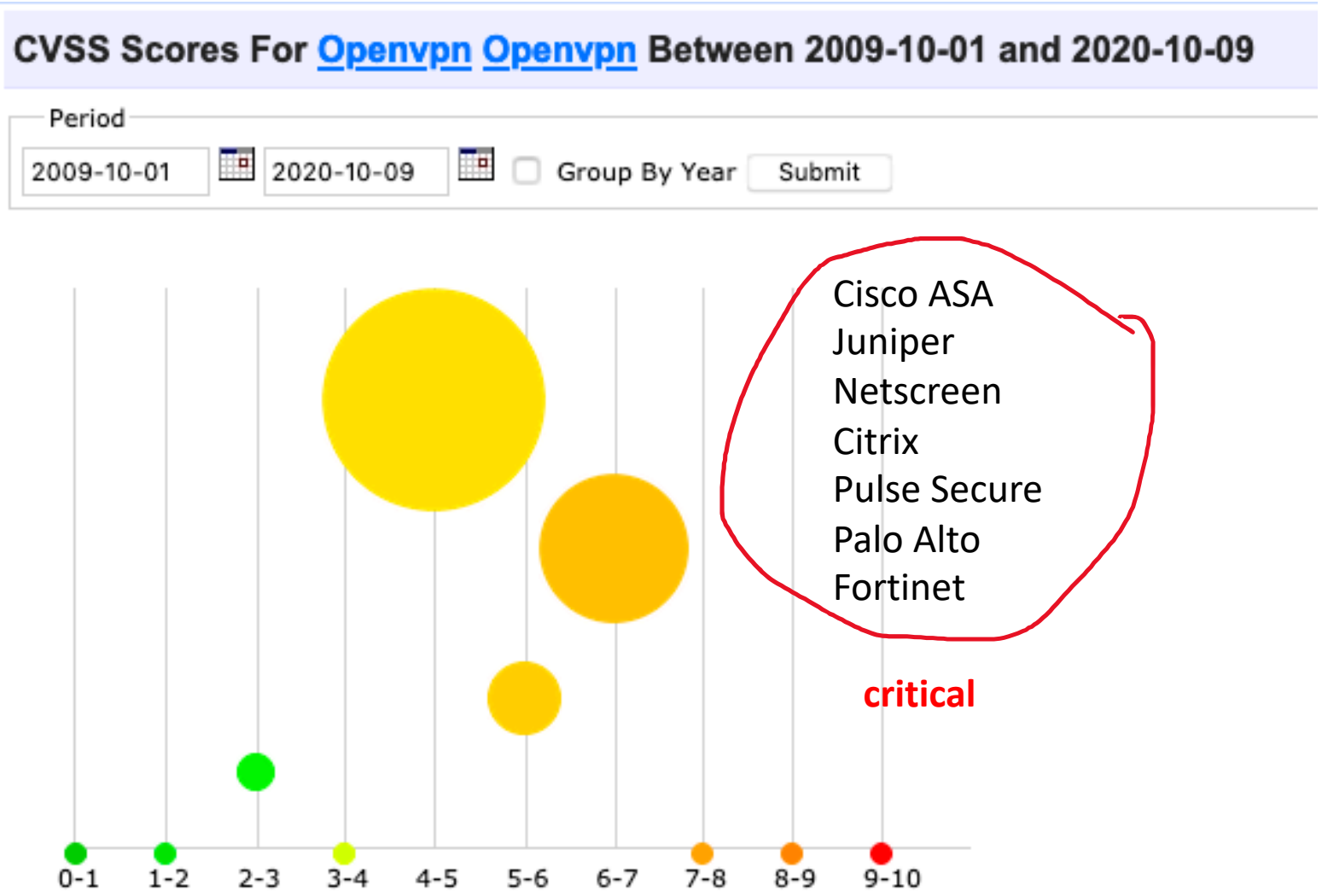
But…

Example of VPN solution for a university in the Nordics without eduVPN

- University with 11000 students and 6000 employees
- Solution for 1000 concurrent users with 10 Gbps interfaces, sophisticated profile management, network access policy
- **HW + SW + License over 3 years: 135 000 EUR**



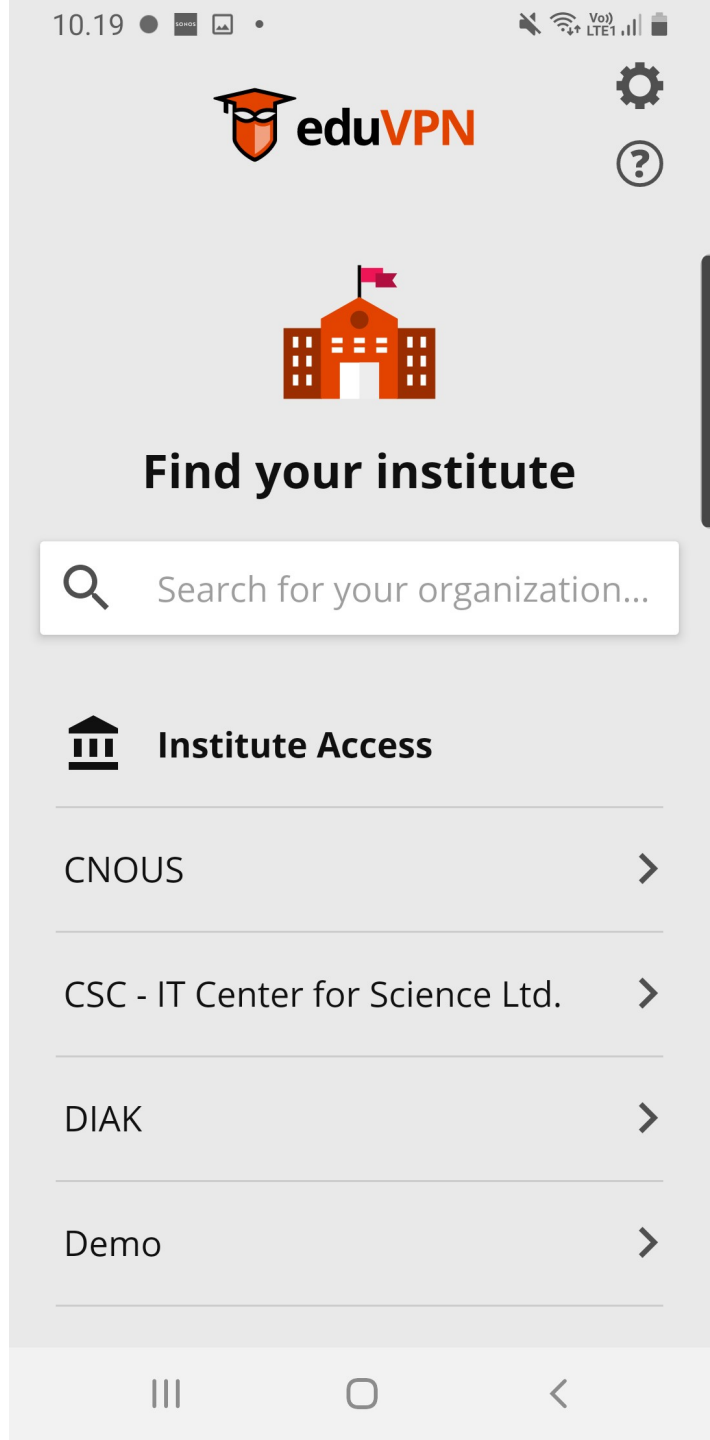
Open-source – only medium issues in 10+ years!



eduVPN: a suite of open source software components

- Server side:
  - Secure configuration of OpenVPN out of the box
  - Connects on UDP and TCP ports
  - Full IPv6 support
  - CA for managing client certificates

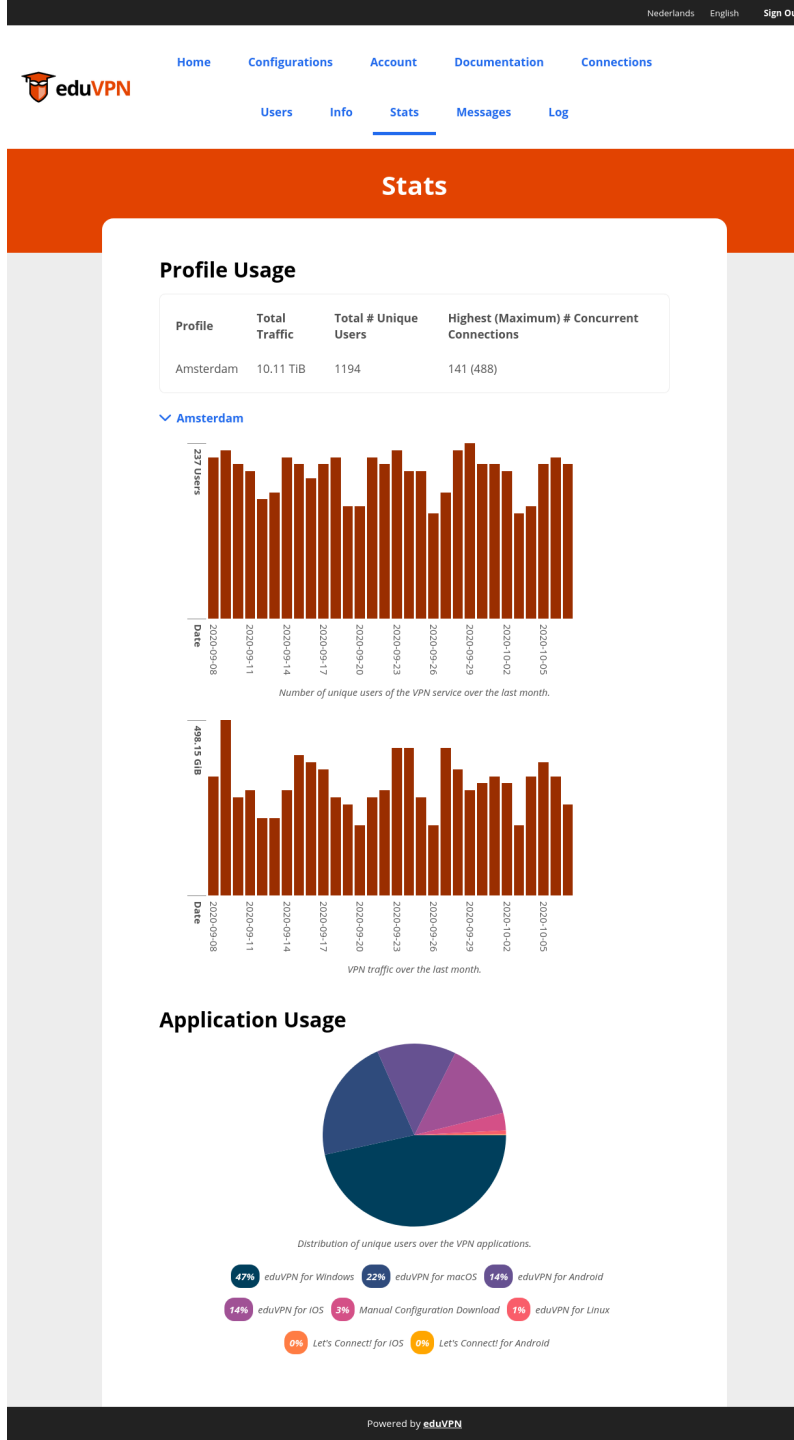
- Client side:
  - Native applications available for Windows, iOS, Android, MacOS, Linux



Ease of management

- Admin Portal to manage users, configurations and connections

- User Portal to allow users to manage their configurations for their devices



Integrates with different IDM systems

- Authentication to portals using "static" username and password, LDAP, RADIUS, SAML and Client Certificates;
- OAuth 2.0 API for integration with applications;
- Two-factor authentication TOTP support with user self-enrollment;

Different deployment scenarios

- Route all traffic over the VPN (for safer Internet usage on untrusted networks);
- Route only some traffic over the VPN (for access to the organization network);
- Client-to-client (only) networking;

Support for multiple deployment scenarios simultaneously

For example CNOUS in France (1 national agency and 28 regional institutions) offers 3 different profiles to its users:

- Encrypted solution between the client device and the central infrastructure of CNOUS for users authorised by their regional organisation (using SAML) to access the Internet.
- Encrypted solution between the client device and the central infrastructure of CNOUS to access the Intranet.
- Specific profiles managed by the regional organisations (to customise which servers an end-user has access to, routing, private and public IP ranges).

Motivation to use eduVPN: license and hardware limitations of current solutions

"So far there have **only been a few questions** to our service desk, although there are already over **700 active and around 60 simultaneous users at the UAS Osnabrück and 1650 active and 240 simultaneous users at the University**. At both universities the commercial solution is still used in parallel. The UAS Osnabrück, however, was able to increase the licensed count of users, while this was not possible at the UOS due to hardware limitations. So the UOS had the pressing need to propagate the new eduVPN solution and unburden the commercial solution."

Fred-Oliver Jury, Osnabrück University of Applied Sciences &
Marc Langer, Osnabrück University, Germany

eduVPN Institute Access as a stand-alone instance

- Institute deploys eduVPN on their own, signs the policy and asks to be included in the apps
- Model adopted by vast majority of universities
- Policy: necessity to comply with minimal requirements in order to be hard coded in the client apps (e.g. updating software, providing support contact, etc.)
- But possibility to use eduVPN totally freely as well

eduVPN Institute Access as a Managed Service

- Model currently implemented in the Netherlands (SURF) and Norway (Uninett)
- eduVPN instance managed centrally by the NREN
- Lightpath back to the private resource
- Support by the NREN
- No need for hardware on campus or licensing limitations

How does it scale?

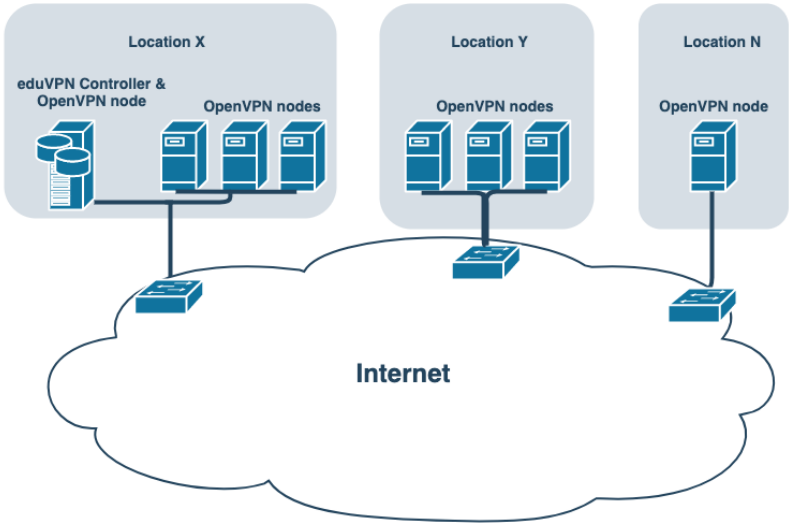
Most organizations start by deploying a single server, which can scale quite well to around 1000 simultaneously connected clients assuming at least 16 CPU cores with AES-NI and adequate network performance, e.g. >= 10 Gbit interface(s).

"Our largest university handles 750 concurrent users on a VM with a load average of 2 (CPUs). Based on this we expect a 16 CPU core VM would be capable of handling up to 5k concurrent users. The **eduVPN** software supports multi server scaling as well and we are now deploying an **eduVPN** cluster with 4 VMs in order to handle 10k+ concurrent users"

Melvin Koelewijn, SURF, The Netherlands

Deploying eduVPN on multiple servers

- distinction between controller and node(s).
  - controller runs the portal and API,
  - node runs the OpenVPN process(es).
- a typical deploy looks like this:
  - Machine 1 has both controller and node functionality in location X;
  - Machine 2 has node functionality in location Y;
  - Machine n has node functionality in location N.



eduVPN Service Policy

- The *service* governance is defined in a **policy document**
  - Inspired by eduroam
  - Largely up to national operators (NRENs) to ensure compliance in a country
  - Security and incident response obligations
- GÉANT plays a central role to support the deployment of the service
- Mostly relevant for the federated service deployed by NRENs and allowing guest usage (“Secure Internet”)

Governance and policy for eduVPN

- The *technical* governance of eduVPN lies in the Commons Conservancy

- Same model as Filesender:
  - CC offers an infrastructure;
  - A board decides on new technical directions for the software

- For example this is where we explore basing eduVPN on WireGuard

How to join

- Check the documentation: https://github.com/eduvpn/documentation/blob/v2/README.md#deployment
- And the tutorials, e.g. https://www.youtube.com/watch?v=yBItHovq4AU&t=11s
- Deploy eduVPN
- Integrate with your IDM system, make sure the connectivity is right
- Follow the procedure to be added in the apps: https://www.eduvpn.org/join/

At any time, please contact us or your NREN at eduvpn-support@lists.geant.org

Thank you

eduvpn-support@lists.geant.org

www.geant.org

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).