eduVPN

Webinar

Rogier Spoor, SURF
Tangui Coulouarn, DeiC

Belnet, 12 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.”

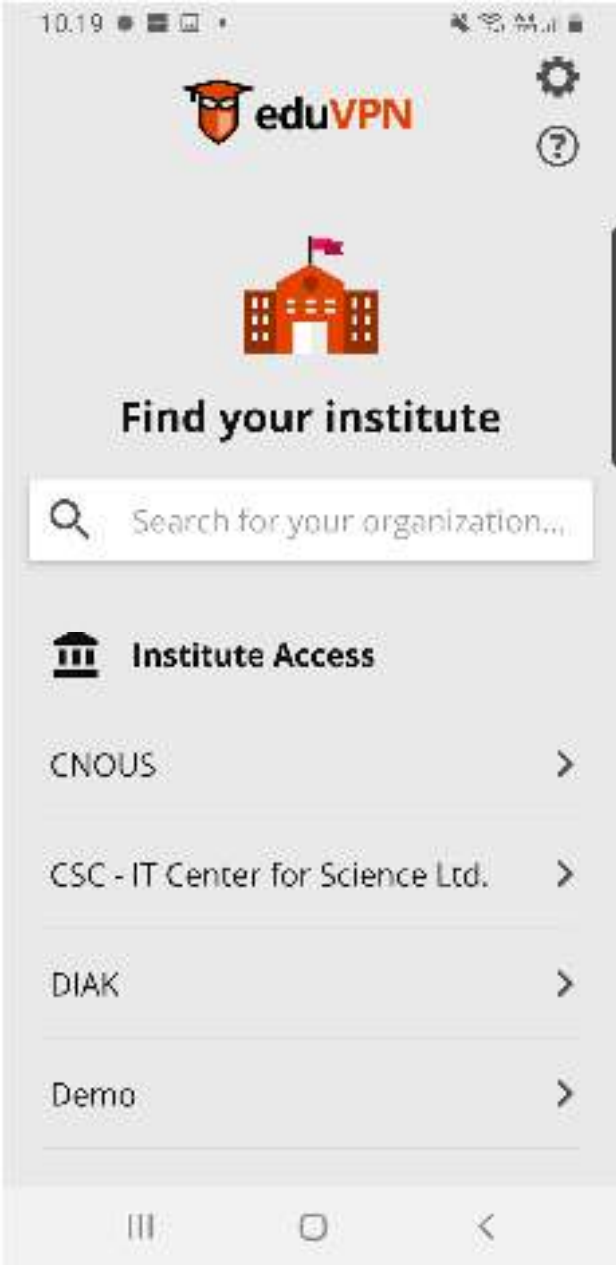
Marco Teixeira, University of Minho, Portugal

Agenda

- What is eduVPN?
- Deployment scenarios
- How does it scale?

eduVPN: a suite of open source software components

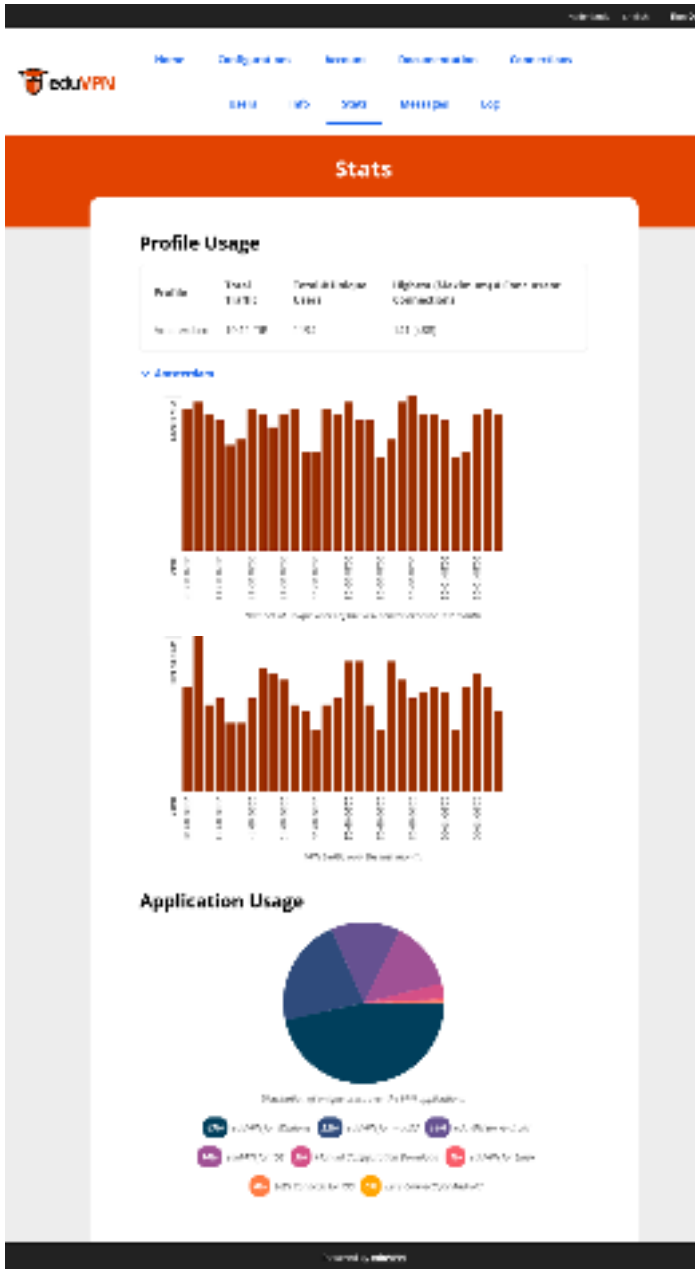
- Server side:
  - Secure configuration of OpenVPN out of the box
  - Connects on UDP and TCP ports
  - Full IPv6 support
  - CA for managing client certificates
- Client side:
  - Native applications available for Windows, iOS, Android, MacOS, Linux



Ease of management

- Admin Portal to manage users, configurations and connections

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



Demo

- Portal
- App

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;

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).

The two main uses of eduVPN

- Secure Internet: 16 NRENs deploy national instances to secure the first mile when people are connecting on unsecure networks.

- **Institute Access: Universities deploy eduVPN as an addition or a replacement of their corporate VPN solutions**

“We had already discussed eduVPN before, but there was no need - a fact that was changed because of Covid-19. The need to supply a significantly higher number of users with our commercial VPN solution would have led to high costs for licenses.”

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

COVID19 and the increase of eduVPN

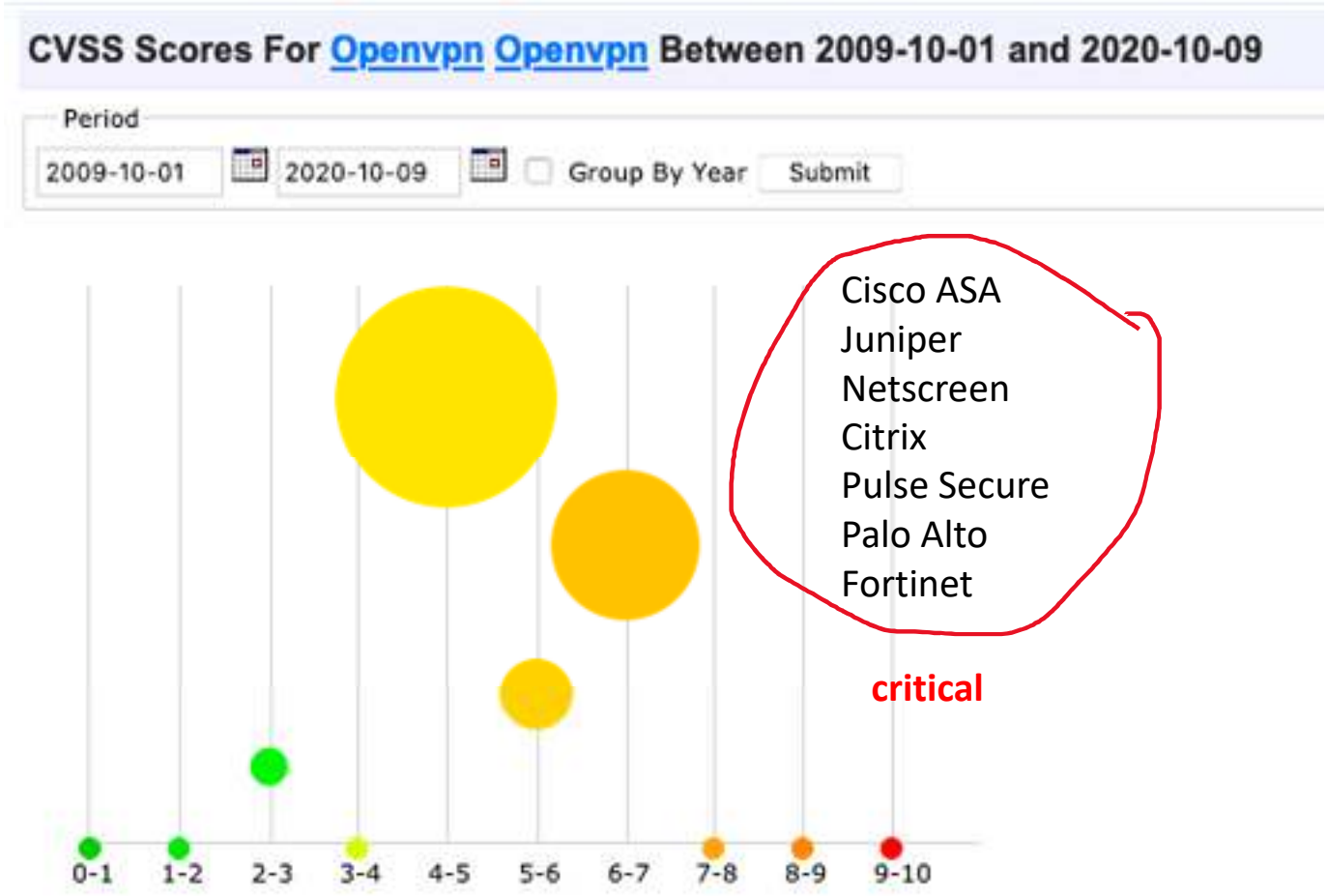
- Universities in Cyprus, France, Indonesia, Kenya, Malaysia, New Zealand, Norway, Portugal, Uganda started using eduVPN.

- These added to the existing deployments in Finland, Germany, the Netherlands, Pakistan, Poland, South Africa.

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!



Cisco ASA
Juniper
Netscreen
Citrix
Pulse Secure
Palo Alto
Fortinet

critical

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?

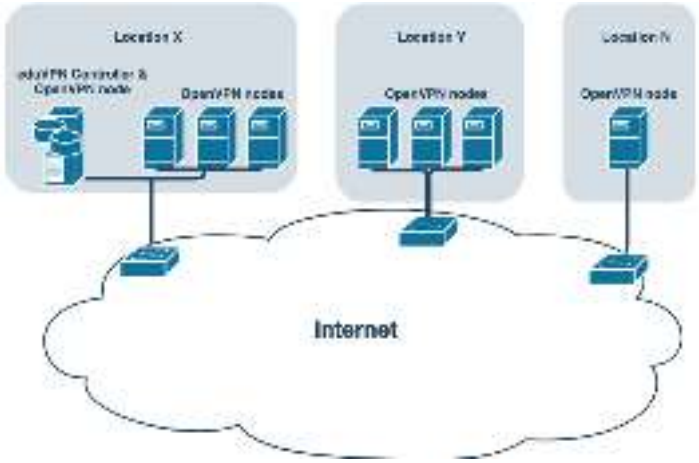
Most organizations start by deploying a single server, which can scale quite well to around 1000 simultaneously connected clients assuming at least 16 CPU cores with AES-NI and adequate network performance, e.g. >= 10 Gbit interface(s).

“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.



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

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”)

How to join eduVPN?

- Check the documentation on GitHub: https://github.com/eduvpn/documentation/blob/v2/README.md#deployment
- Or tutorials on YouTube: https://www.youtube.com/watch?v=yBItHovq4AU&t=5s
- Deploy your own instance
- Integrate with your IDM system
- Check the procedure on https://www.eduvpn.org/join/ to be added to the apps
- Contact us on eduvpn-support@lists.geant.org

Thank you

Any questions?

www.geant.org

© GÉANT Association on behalf of the GN4 Phase 3 project (GN4-3).
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).

Phil Zimmermann (PGP founder) about eduVPN:

“I've always advocated that you should not trust encryption software unless it's open source for peer review, and this includes VPN products. Recently some critical security flaws were detected in proprietary closed-source VPN products.

Using and building carefully engineered open source software that is reviewed by an international community of experts is the way to go for security sensitive software.”

Phil Zimmermann (PGP founder) about eduVPN:

“eduVPN is a software VPN package that delivers this. It is fully open source, both the server and the client applications, and uses strong cryptography. It is tailored to integrate tightly with federated identity systems via the SAML protocol supporting both authentication and authorization. This makes it the perfect fit to deploy in large scale organizations such as a university or research institution. There are no other open source VPN products that provide this level of security and has these federation features.

eduVPN is a bit analogous to eduroam, a federated identity protocol for accessing wifi networks across many European research institutions. I use eduroam every day, and have found that eduroam's federated identity features enable seamless access to wifi all over Europe. I hope one day eduVPN will become just as ubiquitous as eduroam.”