GÉANT
Networks • Services • People

eduVPN

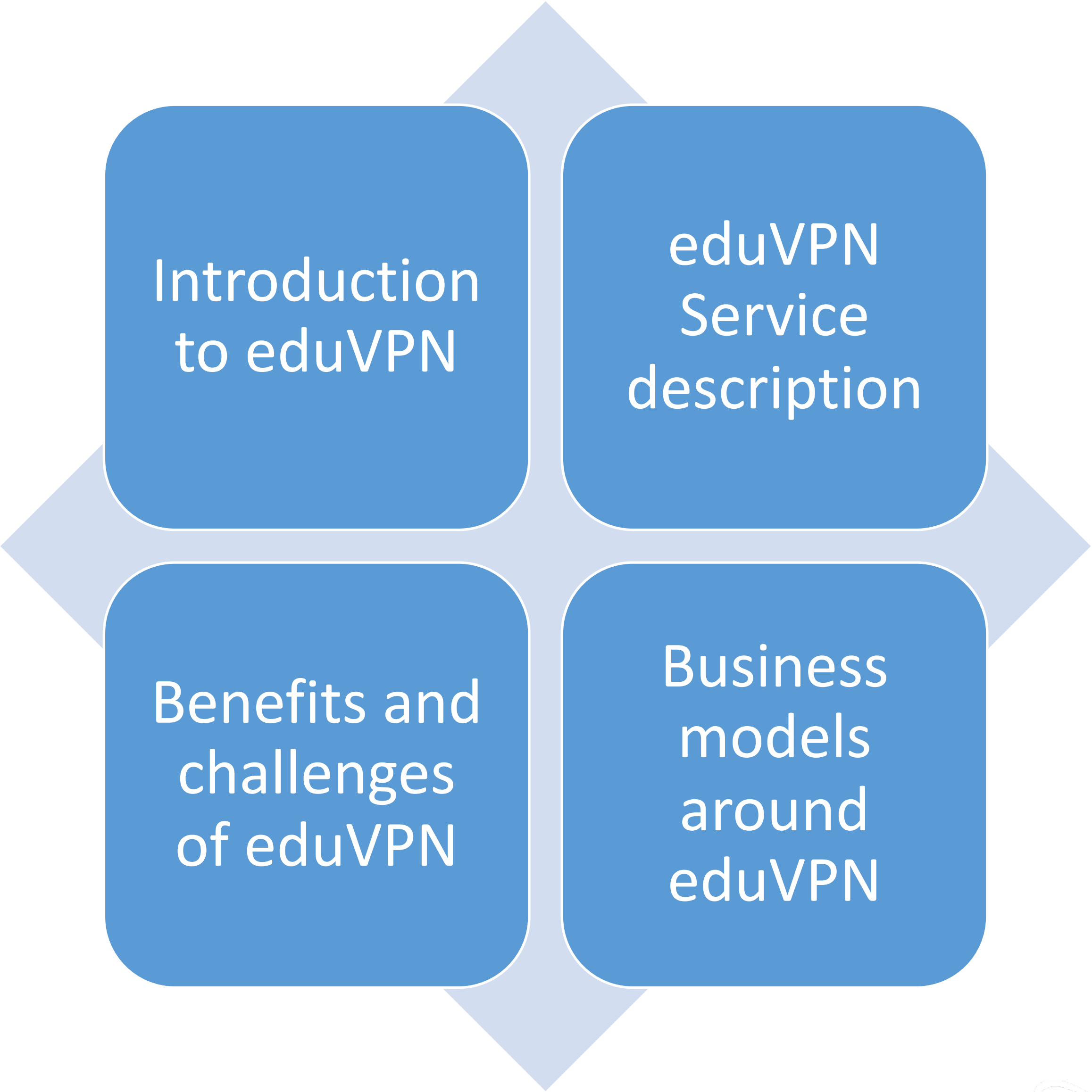
Training for EAP partners – 1st Part

Tangui Coulouarn (DeiC), Rogier Spoor (SURF)

24 February 2022

Public

Goals of the presentation



Introduction to eduVPN

eduVPN Service description

Benefits and challenges of eduVPN

Business models around eduVPN

Which GÉANT services do you currently use?

eduroam?

eduGAIN?

Others?

eduVPN is an edu service built within GÉANT

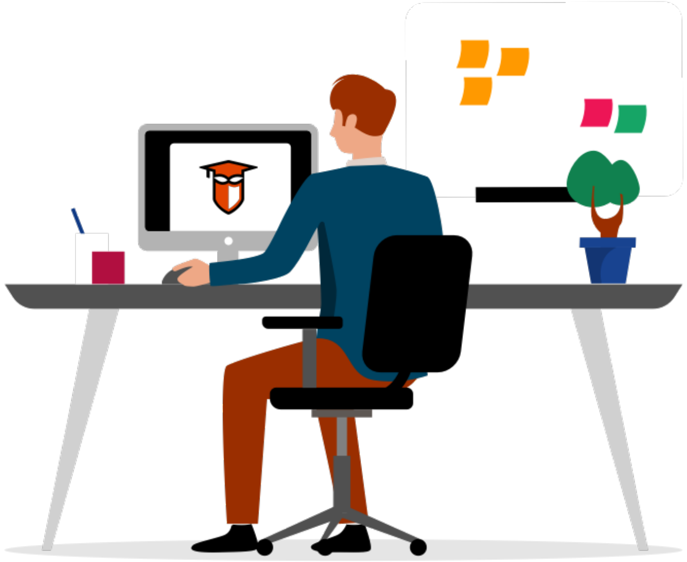
- eduVPN is Free Open Source Software
- Result of collaboration of various NRENs, governed by GÉANT
- Customized for our community and users
- Tested and audited
- Regular security updates and evolution (sovereignty)

What’s the use of eduVPN?

- eduVPN is typically deployed locally by universities

- Typical use case: researcher not on campus needs to access services only available when on the campus network, not publicly accessible over the Internet

- Do you have such services?



A VPN should be like a castle

How to evaluate quality/security of software?

- CVE, short for Common Vulnerabilities and Exposures, is a list of publicly disclosed computer security flaws. When someone refers to a CVE, they mean a security flaw that's been assigned a CVE ID number.

- Severity of a vulnerability is rated: Common Vulnerability Scoring System (CVSS), Scores range from 0.0 to 10.0, with higher numbers representing a higher degree of severity of the vulnerability.

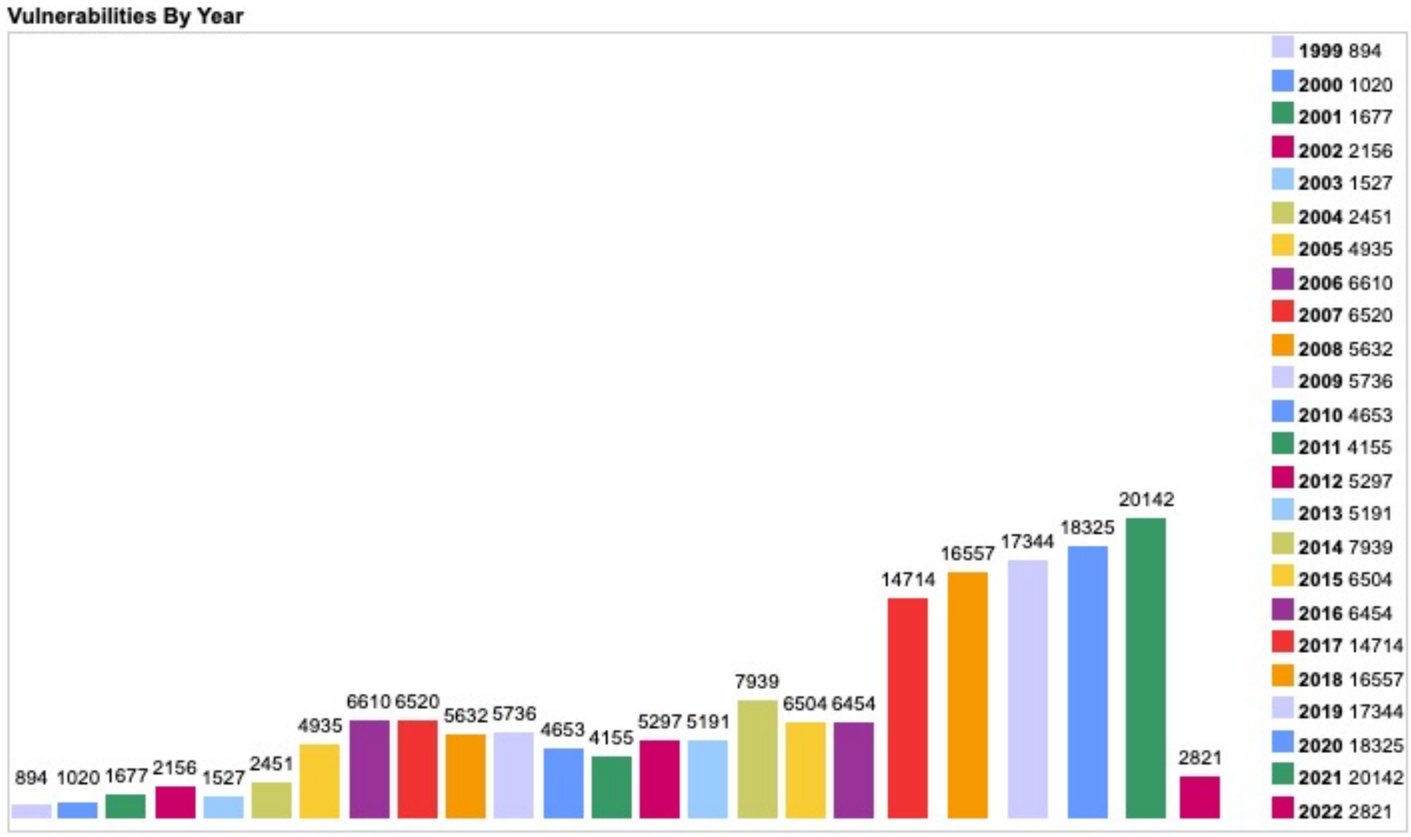
Example of a CVE and CVSS rating

CVE-2018-0101 **CVSS Score 10 (**Critical)

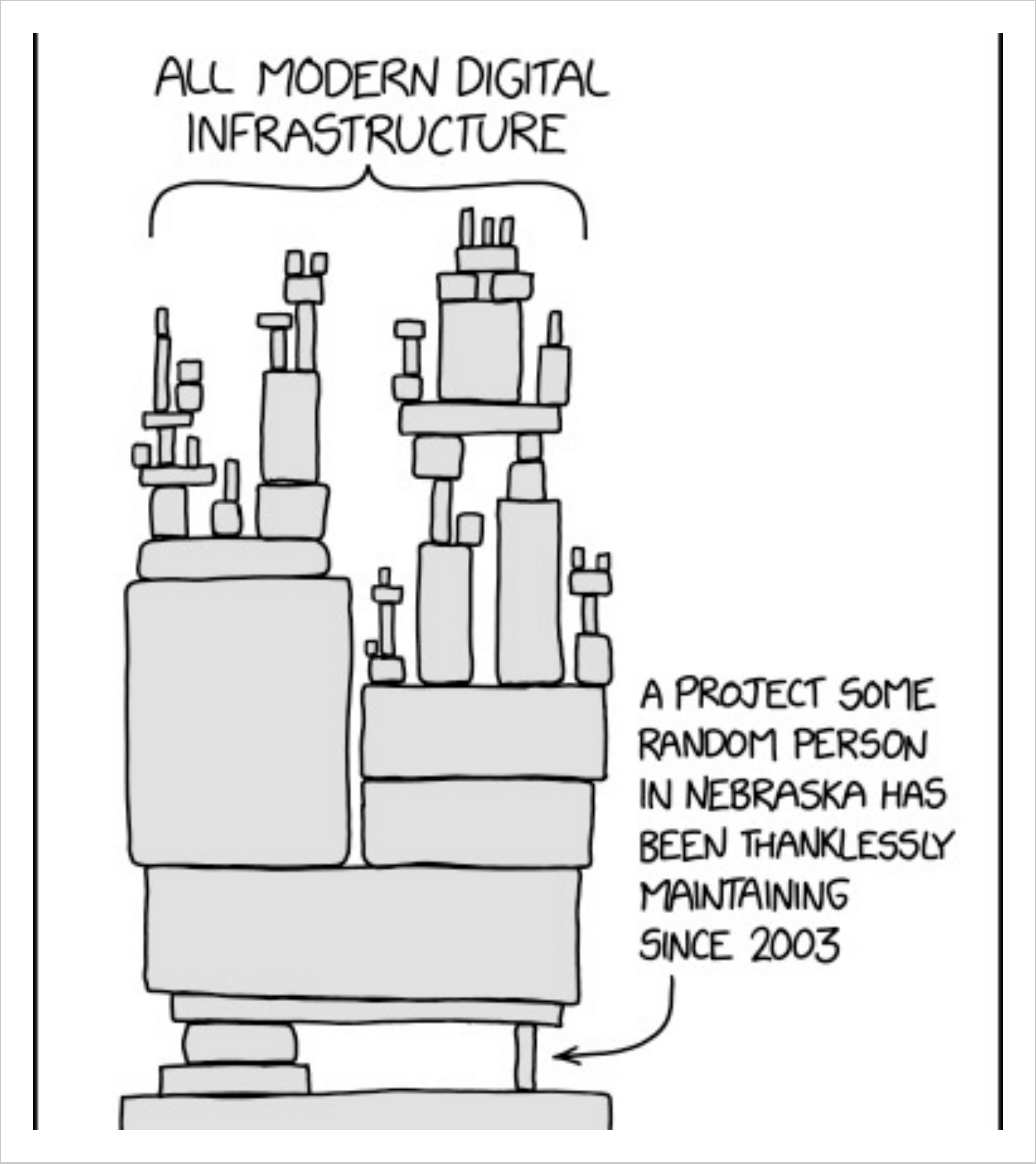
“an unauthenticated remote attacker can exploit execute arbitrary code and obtain full control of the system”

“experts estimate roughly 120,000 to 200,000 vulnerable devices were online”

Vulnerabilities by year



Source: https://www.cvedetails.com/browse-by-date.php

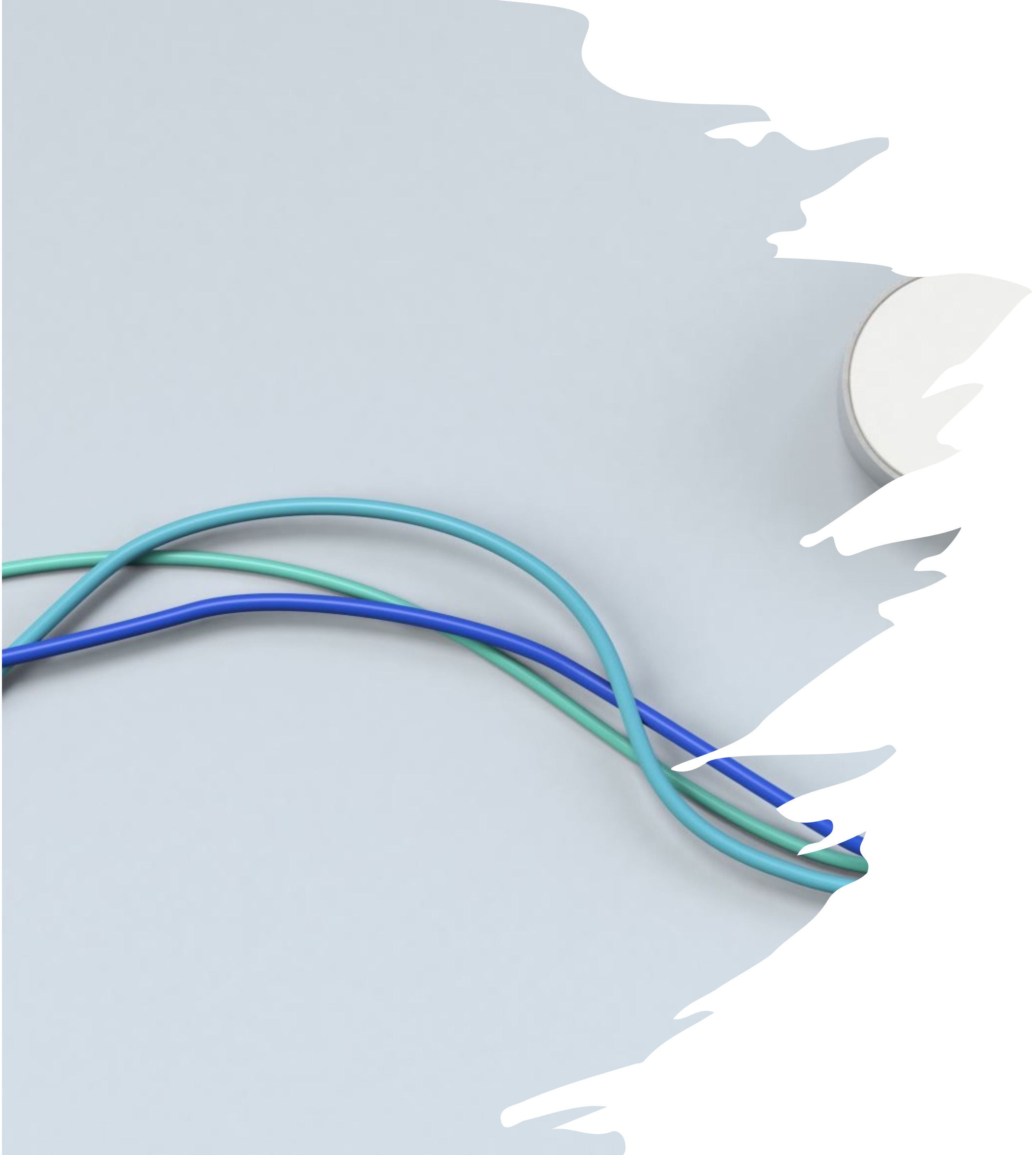

ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

How software is engineered

eduVPN philosophy

- less code and complexity means a more secure service
- writing code is deleting
- only offer features that are required
- evaluate code design/architecture structural
- audits when mayor code change happens
- NRENs can review audits

article: https://www.eduvpn.org/eduvpn-philosophy-less-code-means-a-more-secure-service/



Zero Trust

- Some say "we use cloud" no VPN required
- Zero trust aims at identity, mutual authentication which eduVPN supports
- VPN still useful for additional protection layer
- People working at home -> VPN allows to inspect traffic
- VPN Threat detection with your firewall
- eduVPN with WireGuard can bind IP with identity

eduVPN has reached critical mass

- Today 105 universities use eduVPN as their ”corporate VPN solution”
- They use eduVPN:
    - Technische Universität München
    - Tampere Universities
    - Université de Poitiers
    - Université de Rennes 1
    - Erasmus University Rotterdam
    - Leiden University
    - University of Stavanger,
    - Dalarna University, etc.

2020, the summer of VPNs…

“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.

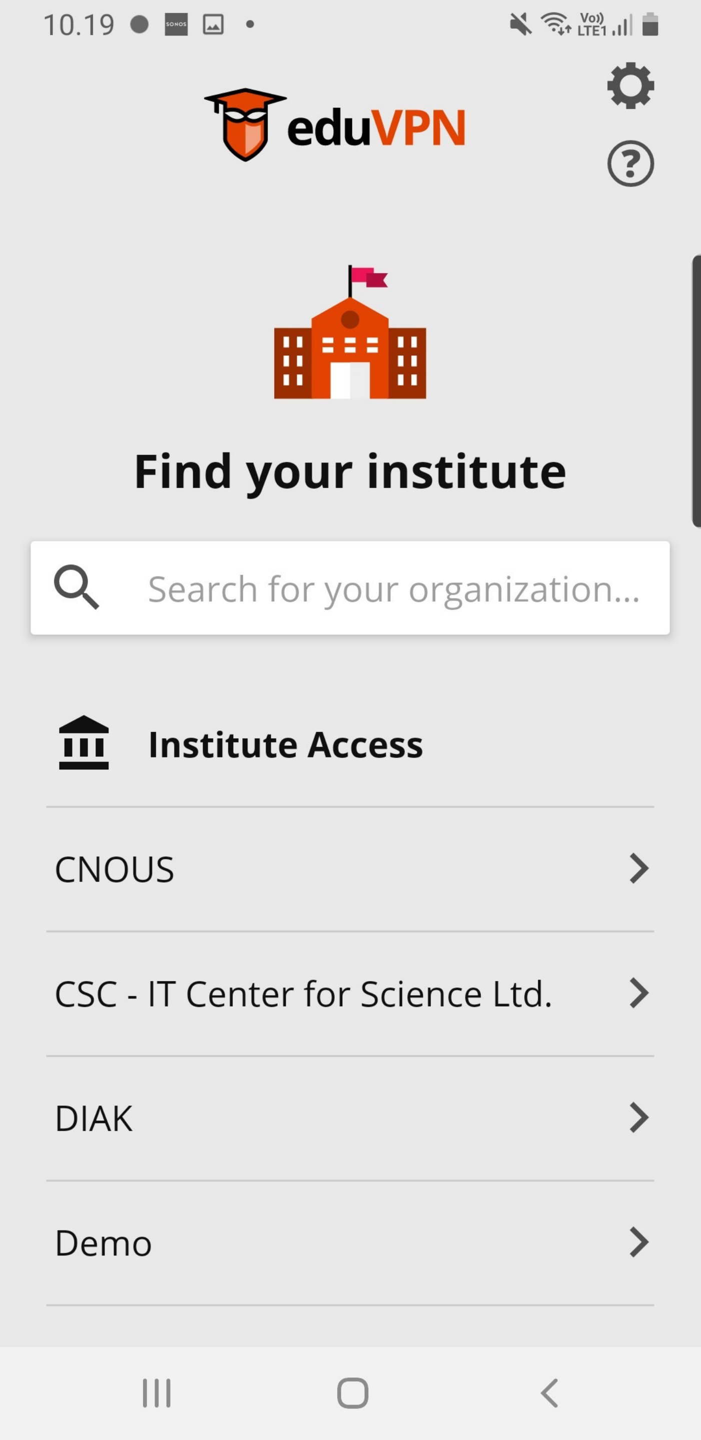
After some research, we preselected the eduVPN, a community project supported by GÉANT. This community project has the features that meet our requirements and is based on well-known and tested open source technologies. After a brief assessment we decided to adopt it.

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

eduVPN: a suite of open source software components

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



10.19

eduVPN

Find your institute

Search for your organization...

Institute Access

CNOUS

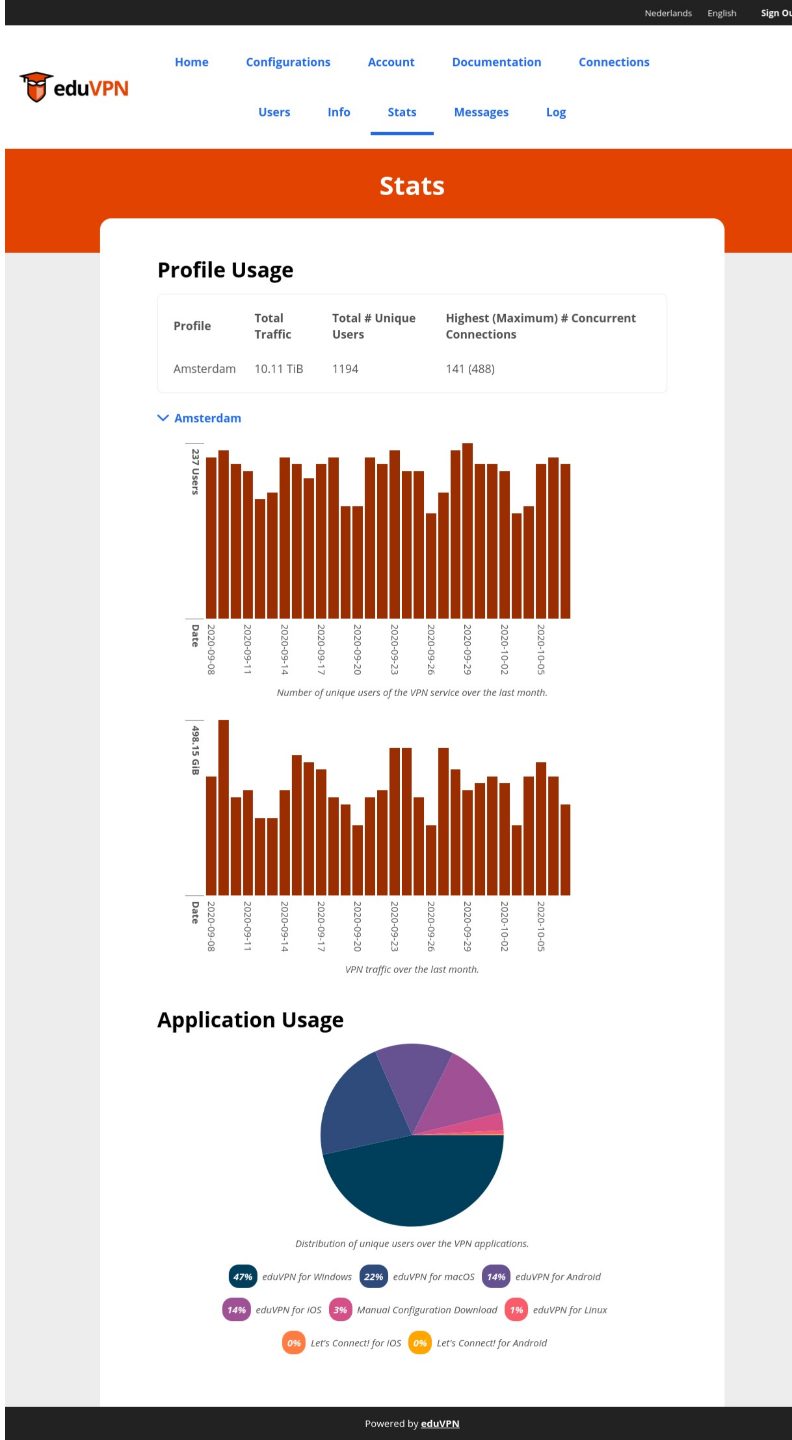
CSC - IT Center for Science Ltd.

DIAK

Demo

Ease of management

- Admin Portal to manage users, configurations and connections
- User Portal to allow users to manage their configurations for their devices



Stats

Profile Usage

Profile	Total Traffic	Total # Unique Users	Highest (Maximum) # Concurrent Connections
Amsterdam	10.11 TiB	1194	141 (488)

Amsterdam

Number of unique users of the VPN service over the last month.

VPN traffic over the last month.

Application Usage

Distribution of unique users over the VPN applications.

47%	eduVPN for Windows
22%	eduVPN for macOS
14%	eduVPN for Android
14%	eduVPN for iOS
3%	Manual Configuration Download
1%	eduVPN for Linux
0%	Let's Connect! for iOS
0%	Let's Connect! for Android

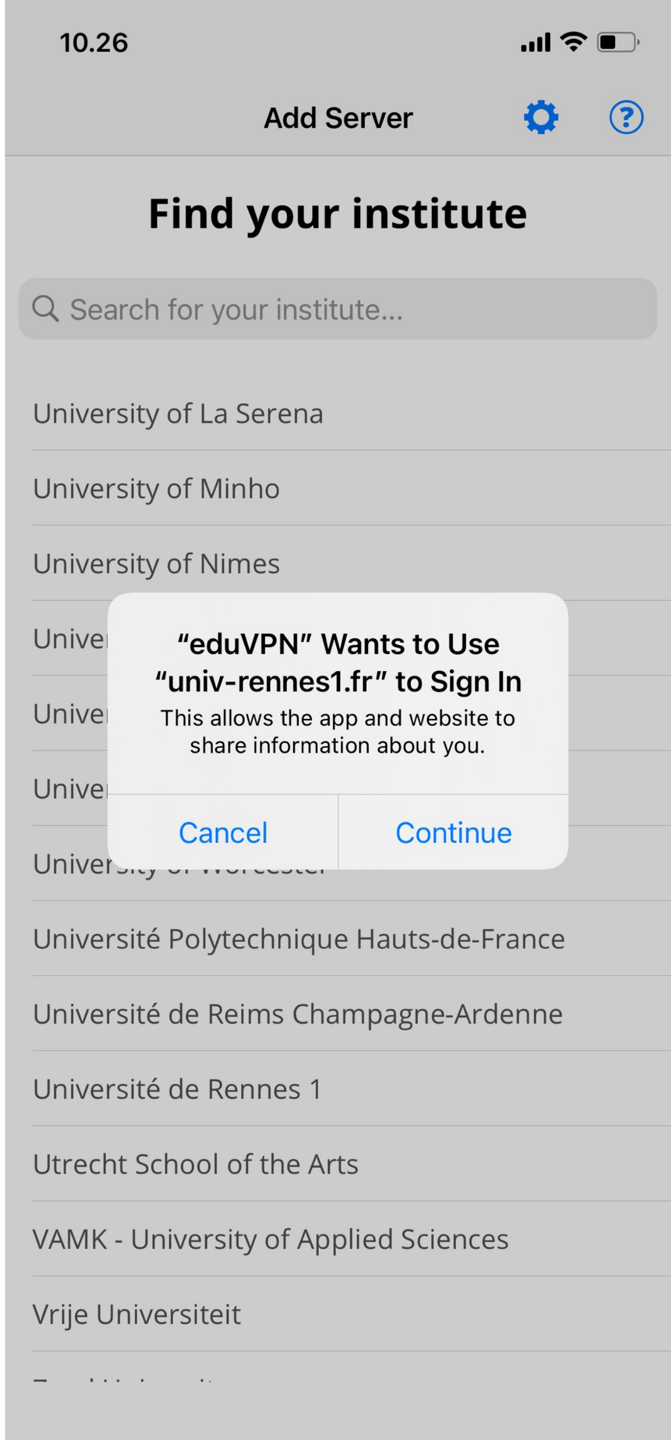
Powered by eduVPN

Integrates with different IDM systems

- Authentication to portals using "static" username and password, LDAP, RADIUS, SAML and Client Certificates;

- Preferred scenario is SAML (own library: PHP-SAML-SP, easy to deploy with support for SAML);

- OAuth 2.0 API for integration with applications;



10.26

Add Server

Find your institute

Search for your institute...

University of La Serena

University of Minho

University of Nimes

Unive

Unive

Unive

University of Worcester

“eduVPN” Wants to Use “univ-rennes1.fr” to Sign In

This allows the app and website to share information about you.

Cancel | Continue

Université Polytechnique Hauts-de-France

Université de Reims Champagne-Ardenne

Université de Rennes 1

Utrecht School of the Arts

VAMK - University of Applied Sciences

Vrije Universiteit

MFA Support

- Supported, if supported by your IdM (SAML, LDAP, ...)

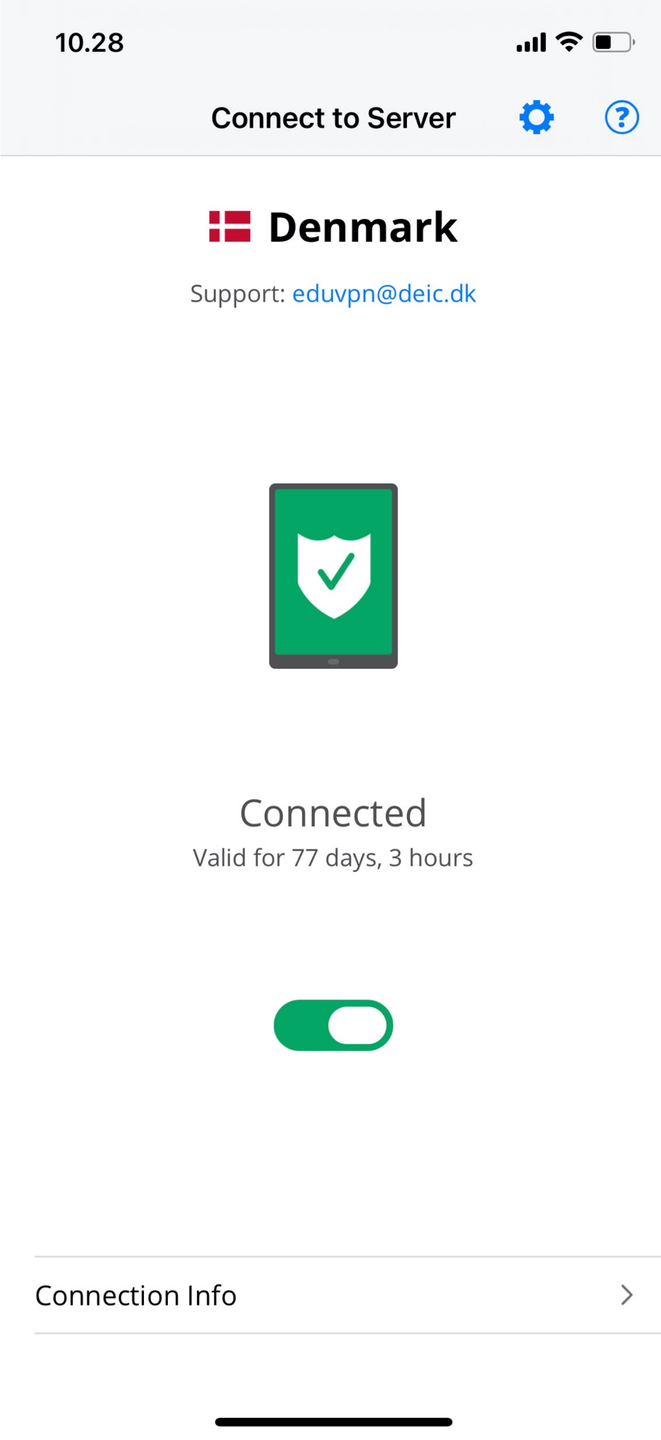
- We do not want to keep (separate) MFA administration in VPN service, because:
  1. Do not want to store MFA credentials @ VPN service;
  2. Do not want to build MFA management interface(s) in the VPN service.

- Most organizations have IdMs where this MFA management can be done much better! Directly at the "source".

- At least one NREN provides centralized MFA solutions for SAML services

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;



10.28

Connect to Server

Denmark

Support: eduvpn@deic.dk

Connected

Valid for 77 days, 3 hours

Connection Info

eduVPN use cases

Secure Institute Access

eduVPN provides access to private networks where end-users can access internal resources within their institute.

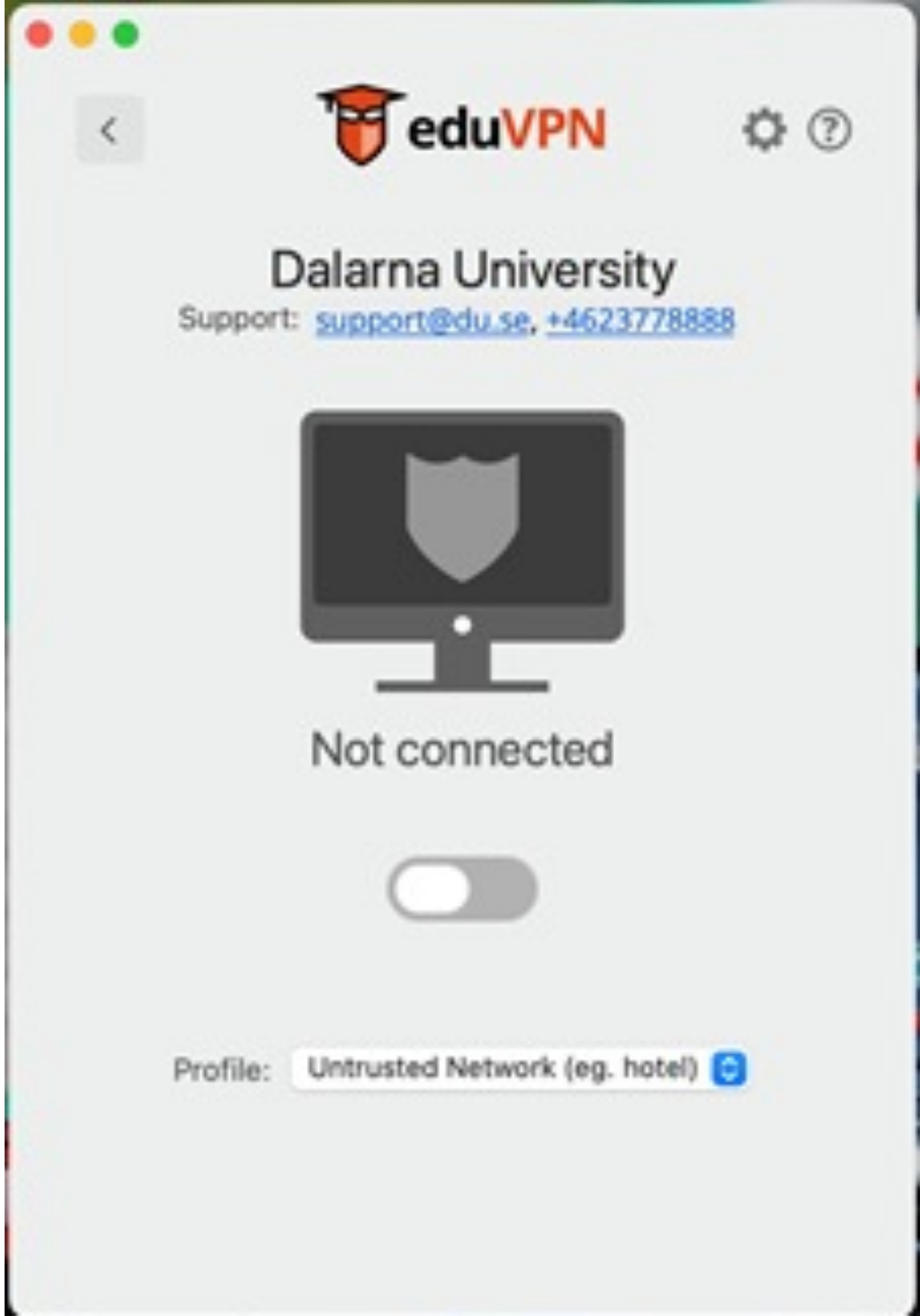
Secure Internet Access

eduVPN provides secure and privacy preserving access from public networks by providing secure gateways to trusted networks

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).



Dalarna University

Support: support@du.se, +4623778888

Not connected

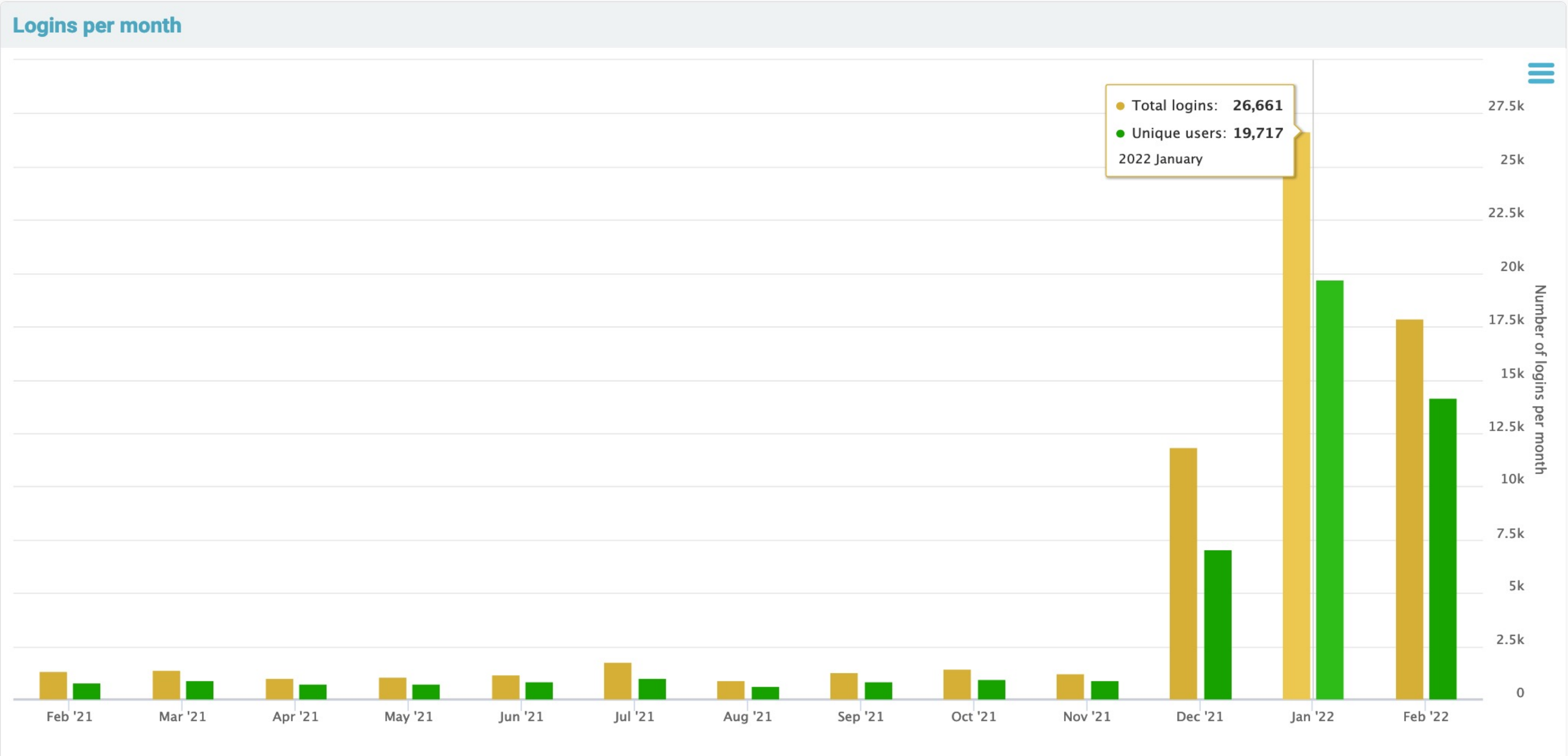
Profile: Untrusted Network (eg. hotel)

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

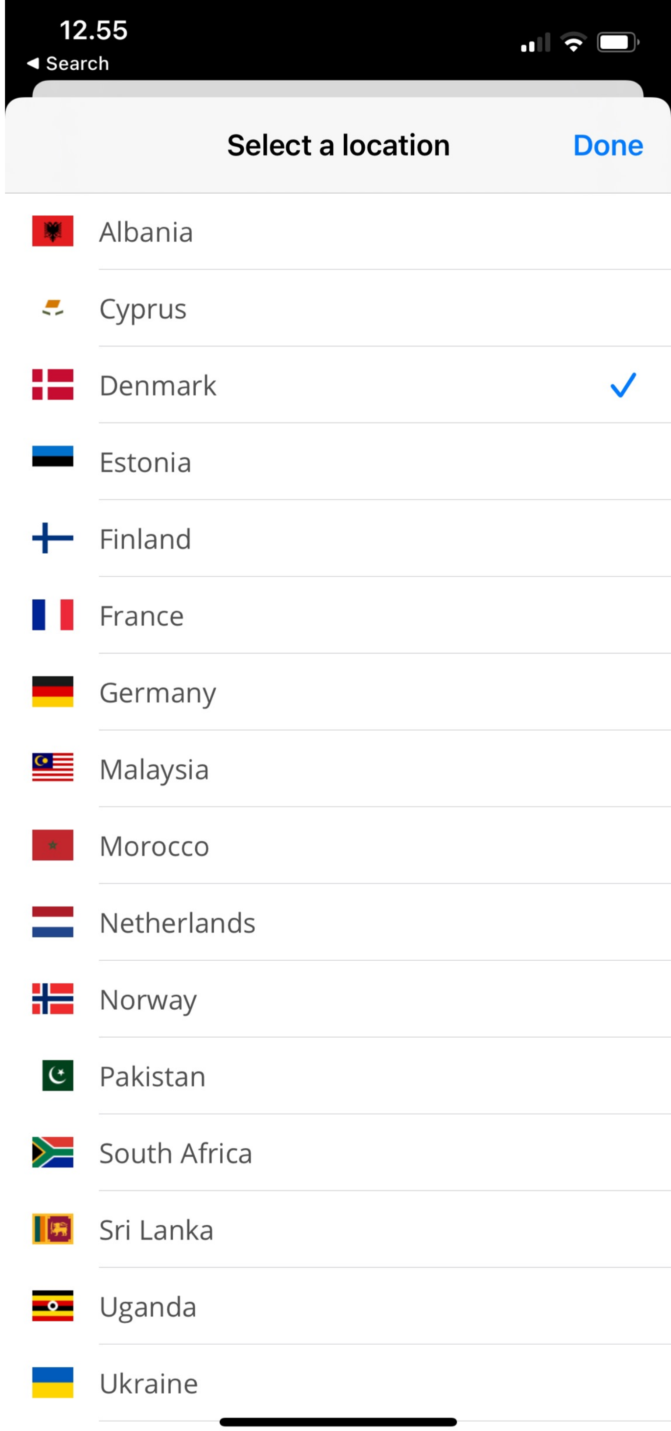
Saxion.nl – largest (as we are aware of)



eduVPN usage

- 150k+ users in Africa, Asia, Europe, Latin America and Oceania.
- 16 national gateways
- More than 100 institute access servers

But how is it deployed in practice?



12.55

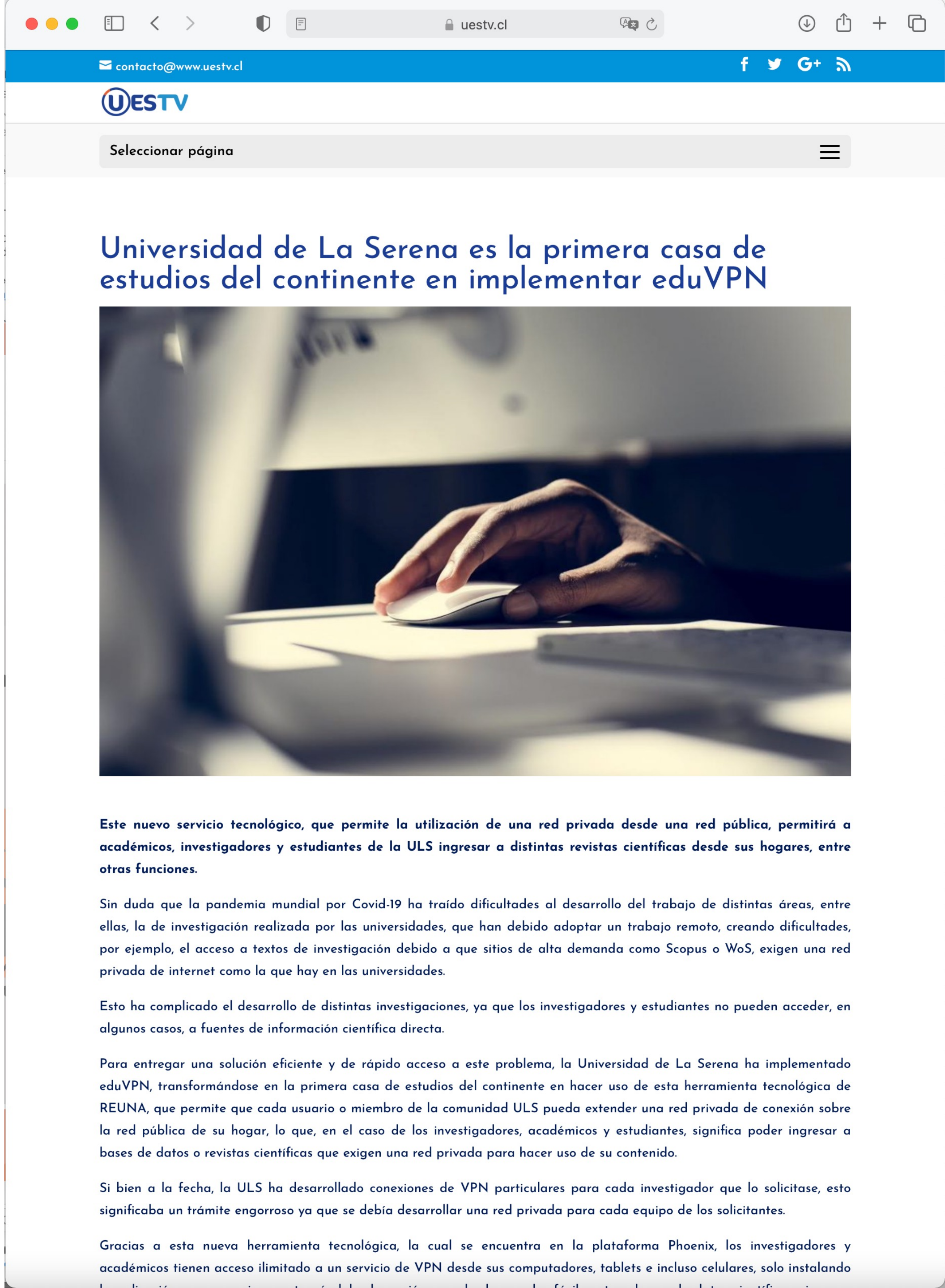
◀ Search

Select a location Done

- Albania
- Cyprus
- Denmark ✓
- Estonia
- Finland
- France
- Germany
- Malaysia
- Morocco
- Netherlands
- Norway
- Pakistan
- South Africa
- Sri Lanka
- Uganda
- Ukraine

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.)



Universidad de La Serena es la primera casa de estudios del continente en implementar eduVPN

Este nuevo servicio tecnológico, que permite la utilización de una red privada desde una red pública, permitirá a académicos, investigadores y estudiantes de la ULS ingresar a distintas revistas científicas desde sus hogares, entre otras funciones.

Sin duda que la pandemia mundial por Covid-19 ha traído dificultades al desarrollo del trabajo de distintas áreas, entre ellas, la de investigación realizada por las universidades, que han debido adoptar un trabajo remoto, creando dificultades, por ejemplo, el acceso a textos de investigación debido a que sitios de alta demanda como Scopus o WoS, exigen una red privada de internet como la que hay en las universidades.

Esto ha complicado el desarrollo de distintas investigaciones, ya que los investigadores y estudiantes no pueden acceder, en algunos casos, a fuentes de información científica directa.

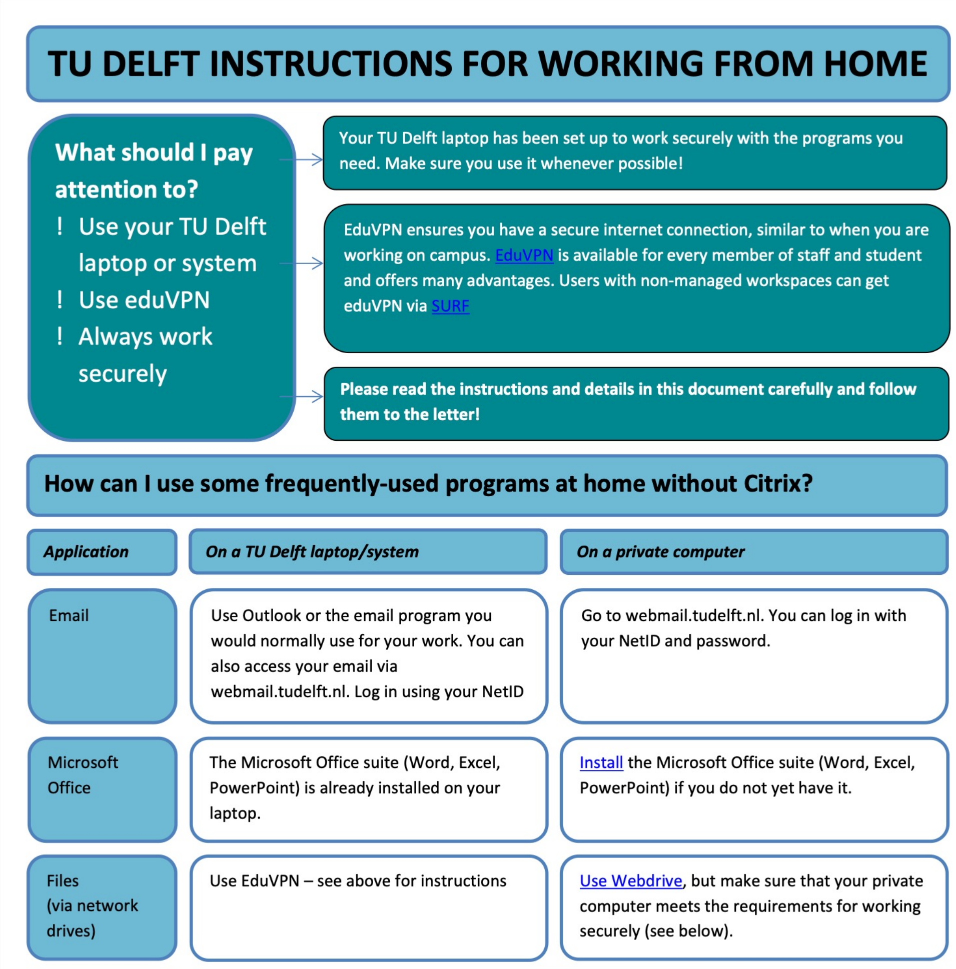
Para entregar una solución eficiente y de rápido acceso a este problema, la Universidad de La Serena ha implementado eduVPN, transformándose en la primera casa de estudios del continente en hacer uso de esta herramienta tecnológica de REUNA, que permite que cada usuario o miembro de la comunidad ULS pueda extender una red privada de conexión sobre la red pública de su hogar, lo que, en el caso de los investigadores, académicos y estudiantes, significa poder ingresar a bases de datos o revistas científicas que exigen una red privada para hacer uso de su contenido.

Si bien a la fecha, la ULS ha desarrollado conexiones de VPN particulares para cada investigador que lo solicitase, esto significaba un trámite engorroso ya que se debía desarrollar una red privada para cada equipo de los solicitantes.

Gracias a esta nueva herramienta tecnológica, la cual se encuentra en la plataforma Phoenix, los investigadores y académicos tienen acceso ilimitado a un servicio de VPN desde sus computadores, tablets e incluso celulares, solo instalando

eduVPN Institute Access as a Managed Service

- Model currently implemented in Belgium (Belnet), the Netherlands (SURF) and Norway (Uninett)
- eduVPN instance managed centrally by the NREN
- Layer 2 circuit back to the private resource
- Support by the NREN
- No need for hardware on campus or licensing limitations



TU DELFT INSTRUCTIONS FOR WORKING FROM HOME

What should I pay attention to?

! Use your TU Delft laptop or system

! Use eduVPN

! Always work securely

Your TU Delft laptop has been set up to work securely with the programs you need. Make sure you use it whenever possible!

EduVPN ensures you have a secure internet connection, similar to when you are working on campus. EduVPN is available for every member of staff and student and offers many advantages. Users with non-managed workspaces can get eduVPN via SURF

Please read the instructions and details in this document carefully and follow them to the letter!

How can I use some frequently-used programs at home without Citrix?

Application	*On a TU Delft laptop/system*	*On a private computer*
Email	Use Outlook or the email program you would normally use for your work. You can also access your email via webmail.tudelft.nl. Log in using your NetID	Go to webmail.tudelft.nl. You can log in with your NetID and password.
Microsoft Office	The Microsoft Office suite (Word, Excel, PowerPoint) is already installed on your laptop.	Install the Microsoft Office suite (Word, Excel, PowerPoint) if you do not yet have it.
Files (via network drives)	Use EduVPN – see above for instructions	Use Webdrive, but make sure that your private computer meets the requirements for working securely (see below).

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).

- E.g. SURF manages a single server with up to 4000 simultaneous users without any issues

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:
  - TCC offers an infrastructure;
  - A board decides on new technical directions for the software
- For example the integration of WireGuard is funded by NORDUnet through The Commons Conservancy

Phil Zimmermann (PGP Founder)

“Virtual Private Networks are becoming an essential tool for travelers, or anyone trying to use the Internet in a hostile local environment.

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.

Building on established open source software and open sourcing the VPN product would most likely have prevented this, or it at least could have been discovered earlier. 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.”

2. Benefits and challenges of eduVPN

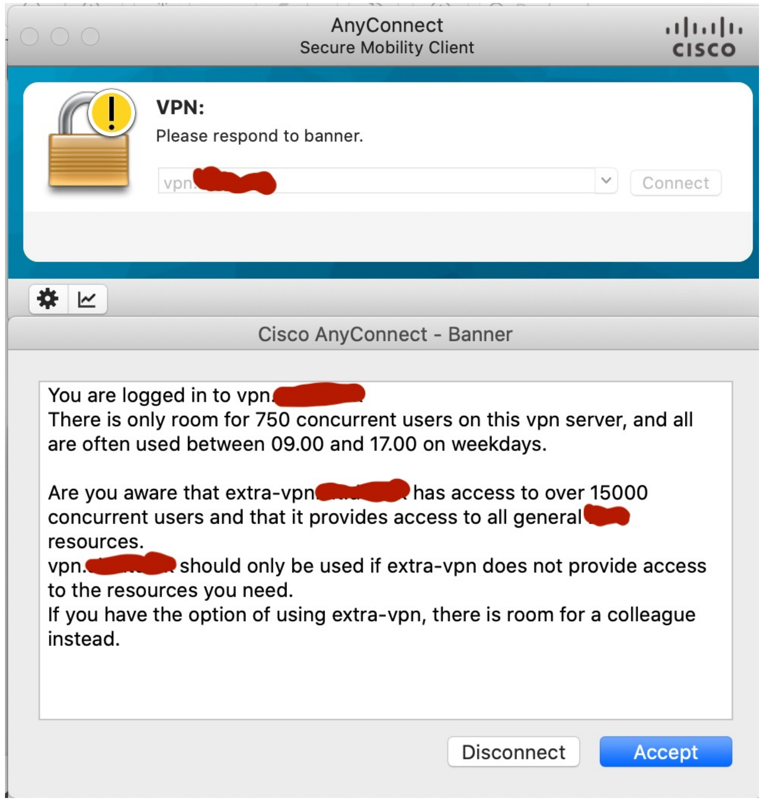
- The main drivers for growth in the last 3 years:
  - COVID:
    - License costs
    - Scaling
  - Security

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**



VPN:

Please respond to banner.

vpn[redacted]

Cisco AnyConnect - Banner

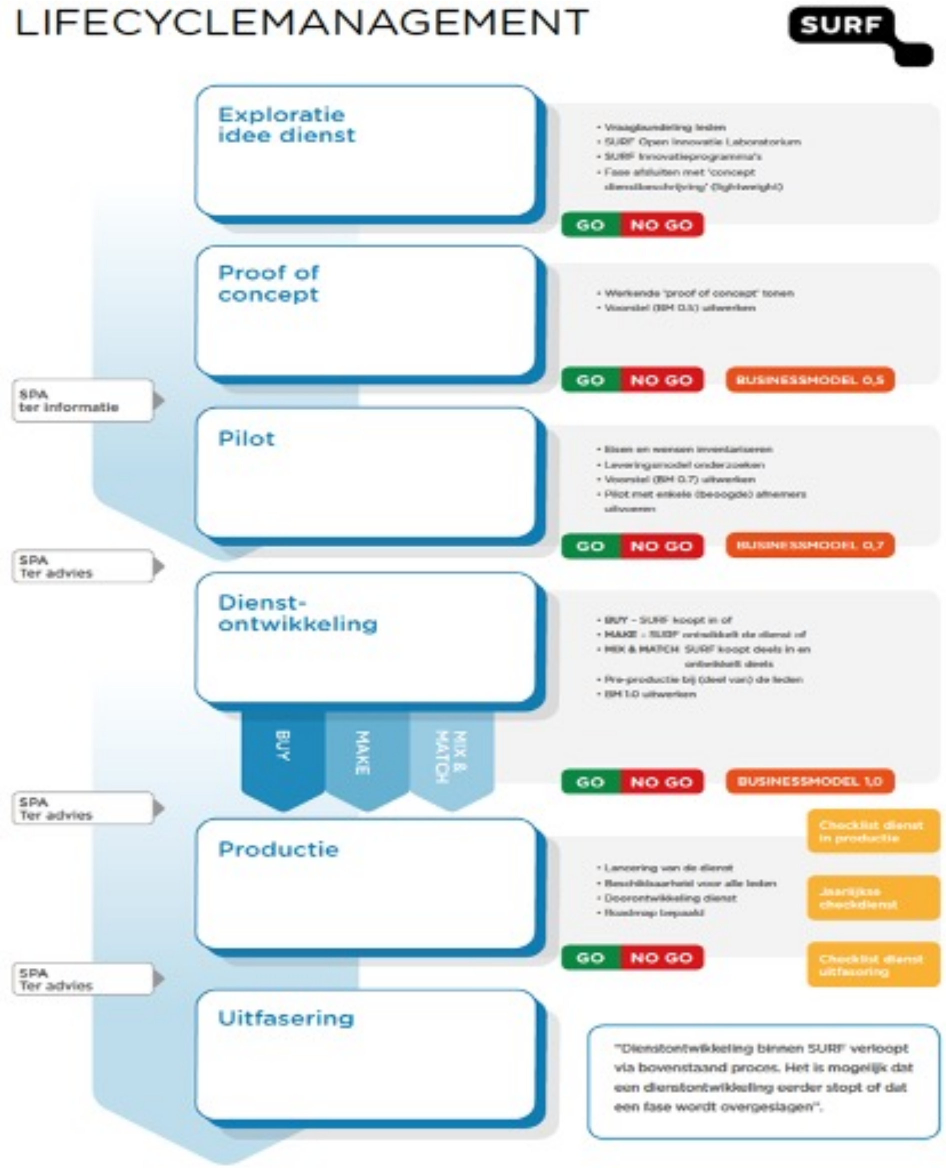
You are logged in to vpn.[redacted]
There is only room for 750 concurrent users on this vpn server, and all are often used between 09.00 and 17.00 on weekdays.

Are you aware that extra-vpn[redacted] has access to over 15000 concurrent users and that it provides access to all general [redacted] resources.
vpn.[redacted] should only be used if extra-vpn does not provide access to the resources you need.
If you have the option of using extra-vpn, there is room for a colleague instead.

3. Business Models around eduVPN – a managed service

- Model currently implemented in the Netherlands
- eduVPN instance managed centrally by SURF
- Layer-2 path back to the private resource
- Support by SURF
- No need for hardware on campus or licensing limitations

Service introduction process @SURF



- Vraagbundeling testen
- SURF Open Innovatie Laboratorium
- SURF Innovatieprogramma's
- Fase afsluiten met 'concept dienstbeschrijving' (lightweight)

- Werkende 'proof of concept' tonen
- Voorstel (BM 0.5) uitwerken

- Eisen en wensen inventariseren
- Leveringsmodel onderzoeken
- Voorstel (BM 0.7) uitwerken
- Pilot met enkele (beoogde) afnemers uitvoeren

- **BUY** – SURF koopt in of
- **MAKE** – SURF ontwikkelt de dienst of
- **MIX & MATCH** SURF koopt deels in en ontwikkelt deels
- Pre-productie bij (deel van) de leden
- BM 1.0 uitwerken

- Lancering van de dienst
- Beschikbaarheid voor alle leden
- Doorontwikkeling dienst
- Roadmap bepaald

"Dienstontwikkeling binnen SURF verloopt via bovenstaand proces. Het is mogelijk dat een dienstontwikkeling eerder stopt of dat een fase wordt overgeslagen".

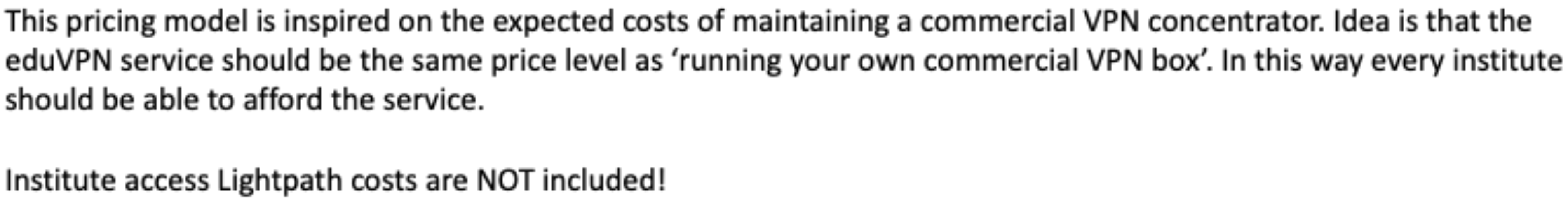
life cycle & portfolio management: steps

The business model has three phases. Every phase requires approval.

Final version 1.0, contains: SLA, DAP, GDPR compliance, risk analyses, contract outsourcing partner, business case calculations

EduVPN pricing in .NL

Total Size institute	Costs
0 – 1.000	€ 106,00 per month
1.001 – 5.000	€ 529,00 per month
5.001 – 15.000	€ 900,00 per month
15.001+	€ 1.324,00 per month



This pricing model is inspired on the expected costs of maintaining a commercial VPN concentrator. Idea is that the eduVPN service should be the same price level as ‘running your own commercial VPN box’. In this way every institute should be able to afford the service.

Institute access Lightpath costs are NOT included!

eduVPN in .NL income 2022

- 7 polytechniques: 103 K EURO
- 7 universities: 107k EURO
- Others institutes in total 19: 44k

- Total 255K

How to ‘sell’ eduVPN

Establish eduVPN as your ‘official’ NREN service

Guarantee the service for at least 3-4 years

Be sure you’ve enough knowledge about the product in order to convince an institute

Make sure support is available

Key is integration with your federation service

How to ‘sell’ eduVPN (SURF strategy)

- Marketing & communication aspects
- Few times tech presentation at .NL CSIRT meetings
- Service launch @annual security conference
- Offer trial accounts to people in the CSIRT community
- “try out a few months” for free
- First year low price ->“how it’s being used”
- Have trustworthy people involved
- Security/crypto implemented like .NL government
- GDPR compliant
- Audits on all components
- Mention eduVPN @community meetings

How to manage the service (outsourcing)

- The eduVPN maintenance (eduVPN server upgrades, OS updates, VM configuration, SAML configuration) has been outsourced
- We searched for a partner with VPN knowledge: Greenhost.nl
- Greenhost.nl does all change management and uses ansible scripts

Institute access experiences

- Setup of institute access takes quite some effort
- We use a questionnaire to ask how an institute likes to use institute access. Find out if they need VLAN's, ipranges, which user groups etc
- We schedule a personal intake meeting onsite with IdM, network, security, workstation and other people
- In general we visit the institute roughly 3 times in order to discuss the details of the setup.
- Many emails to discuss, technical details.

Currently 33 paying customers in .NL

Reason why some not interested:

- Recently moved to new VPN concentrator/firewall
- A full redundant setup was difficult to integrate with local network
- 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

3 different ways to offer eduVPN to your community (1)

1- Promote eduVPN and offer first level support to your institutions that are interested to deploy eduVPN

You would need to:

- train your teams to be able to offer 1st line of support
- Translate documentations related to eduVPN
- Promote eduVPN to your community

3 different ways to offer eduVPN to your community (2)

2- Promote and offer first level support to your institutions that are interested to deploy eduVPN

+ Offer a national instance of eduvpn

- You would need to —> **STEP 1 +** deploy a national instance of eduVPN and maintain it

- It will enable you community to access your national VPN and other VPNs around the world

3 different ways to offer eduVPN to your community (3)

3- Promote eduVPN and offer first level support to your institutions that are interested to deploy edu VPN

+ Offer a national instance of eduvpn

+ eduVPN Institute managed service

You would need to do —> **STEP 1 + STEP 2**
+ Define your business model, and deploy an infrastru cture to host vpns for your institutions

How can we help you in the next weeks or couple of months ?

As it’s a pre-requisite
to train your teams, we will provide a technical training dedicated for them.

GÉANT
Networks • Services • People

Thank you

eduvpn-support@lists.geant.org

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).