eduVPN

Told by Danes* to Swedes

Tangui Coulouarn & François Kooman, DeiC

Sunet Dagarna 2024, Uppsala, Sweden

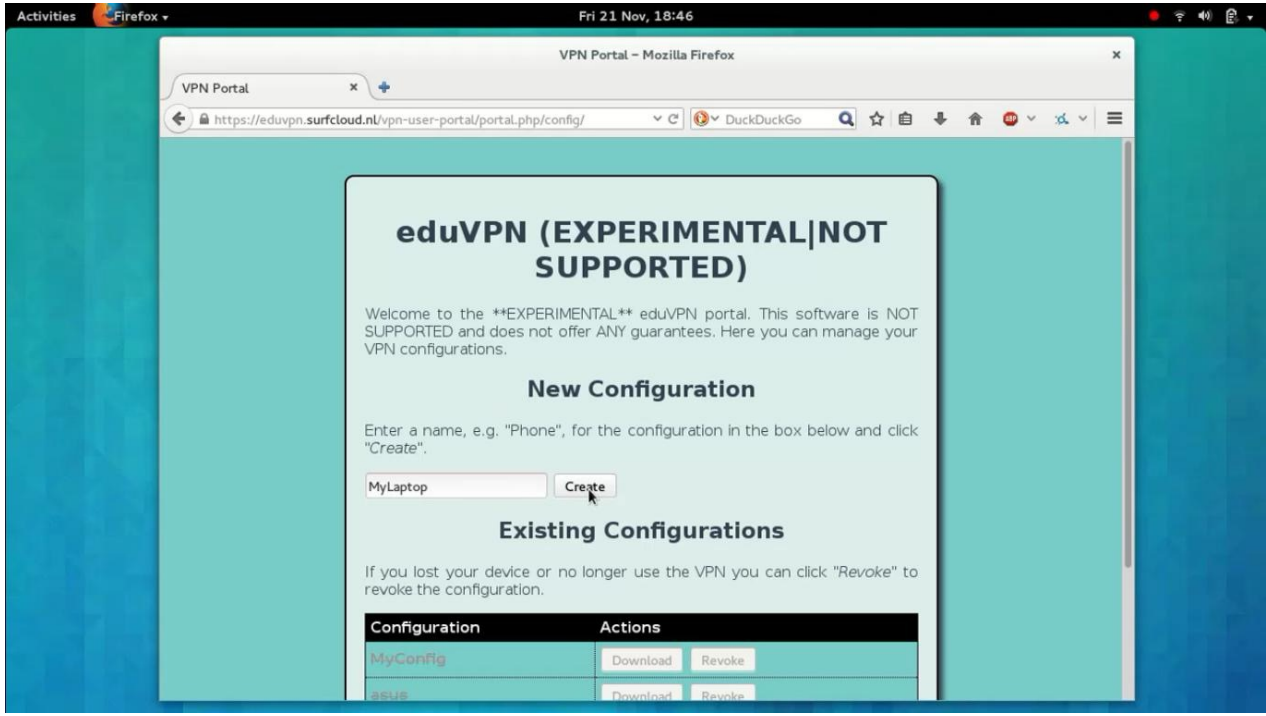
23 April 2024

Summary

- eduVPN is an *edu* service built by collaboration of several NRENs, supported by GÉANT
- Free Open Source Software
- Customized for our community and users
- Tested and audited
- Regular security updates and evolution
- Used in production by 150+ universities and 19 NRENs

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 Intern**et, i.e. access the public internet through trusted gateways



The Institute Access use case

- Replace the corporate VPN solution to let staff and students access resources on a private network
- Tricky due to procurement cycles
- Early adoption in the NL

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 browser WebSSO)

- NREN perspective: 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

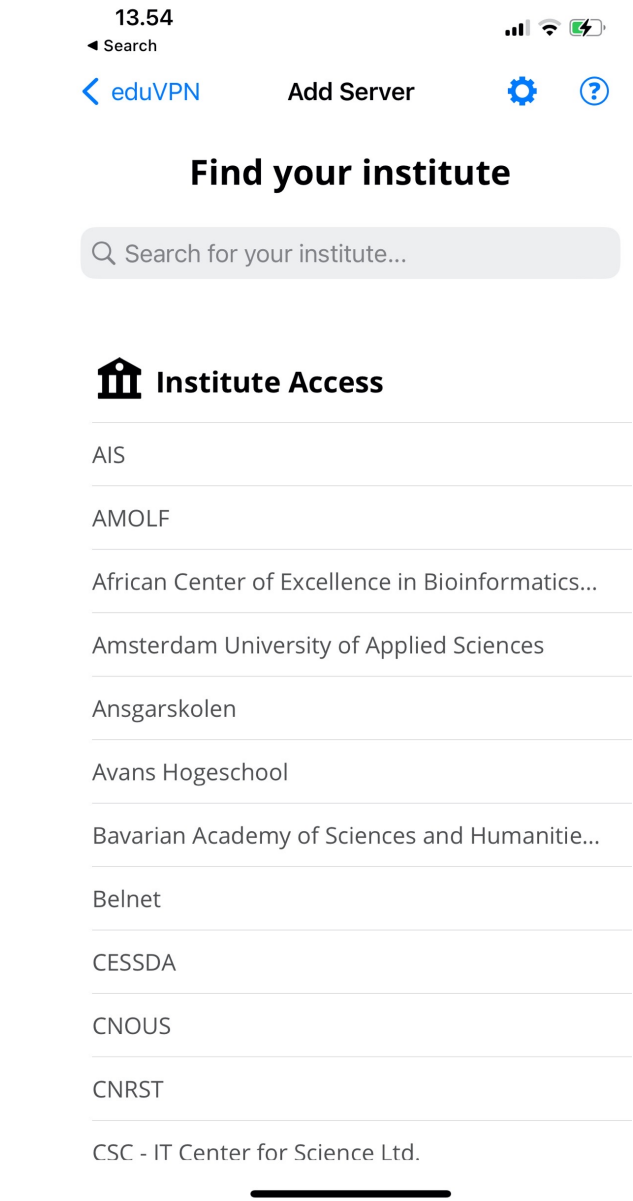
Requirements (2)

- Scale beyond 1 server (not just fail-over)
- Native IPv6 support out of the box
- Available as OS packages on most common Linux server operating systems
  - Easy install
  - But more important: easy updates (apt, yum, dnf)
- No per-seat licensing, so you only pay for hardware (and server administration)

eduVPN today

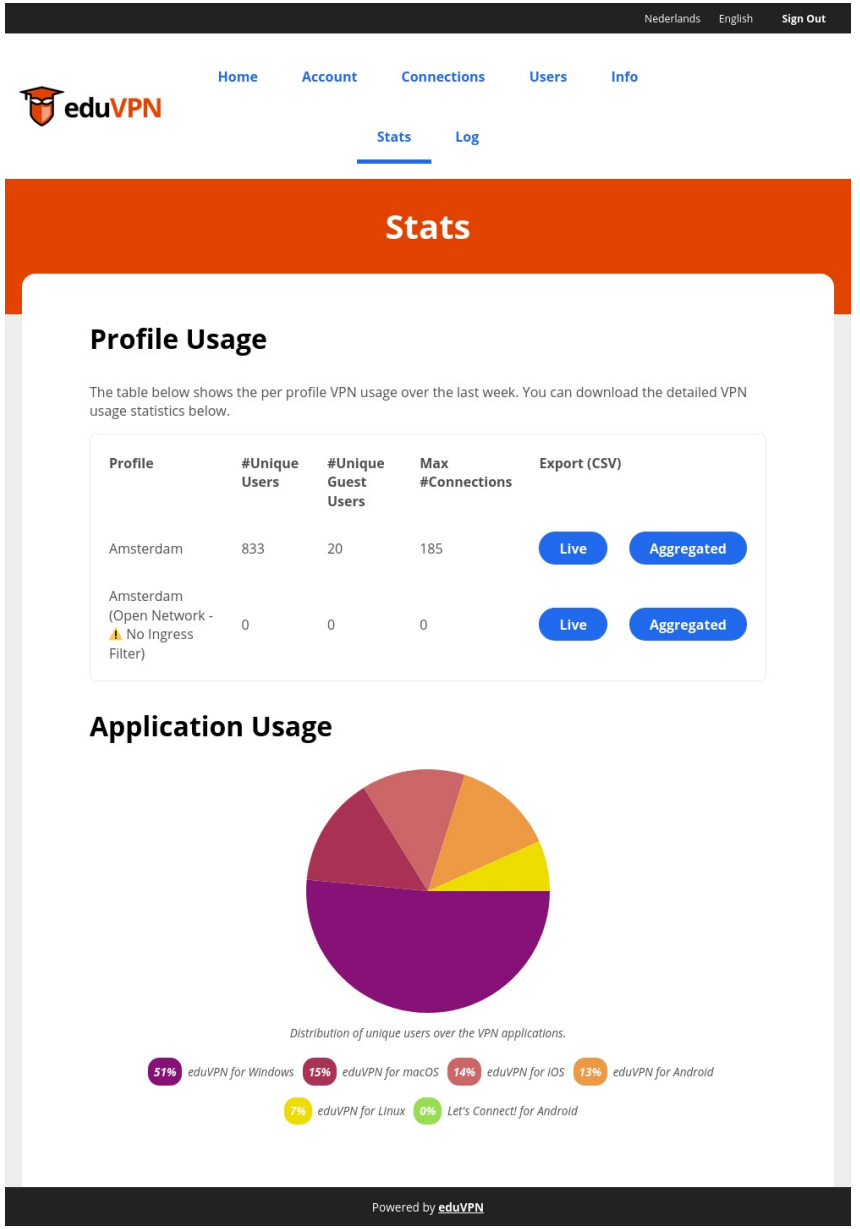
- VPN software package with
  - server side components
  - client apps for Linux, Windows, iOS/macOS and Android
- Supports WireGuard and OpenVPN
- Integrates well with identity management systems at universities (SAML, LDAP, RADIUS, OpenID Connect, Client certificates)
- Granular profiles + possibility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

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



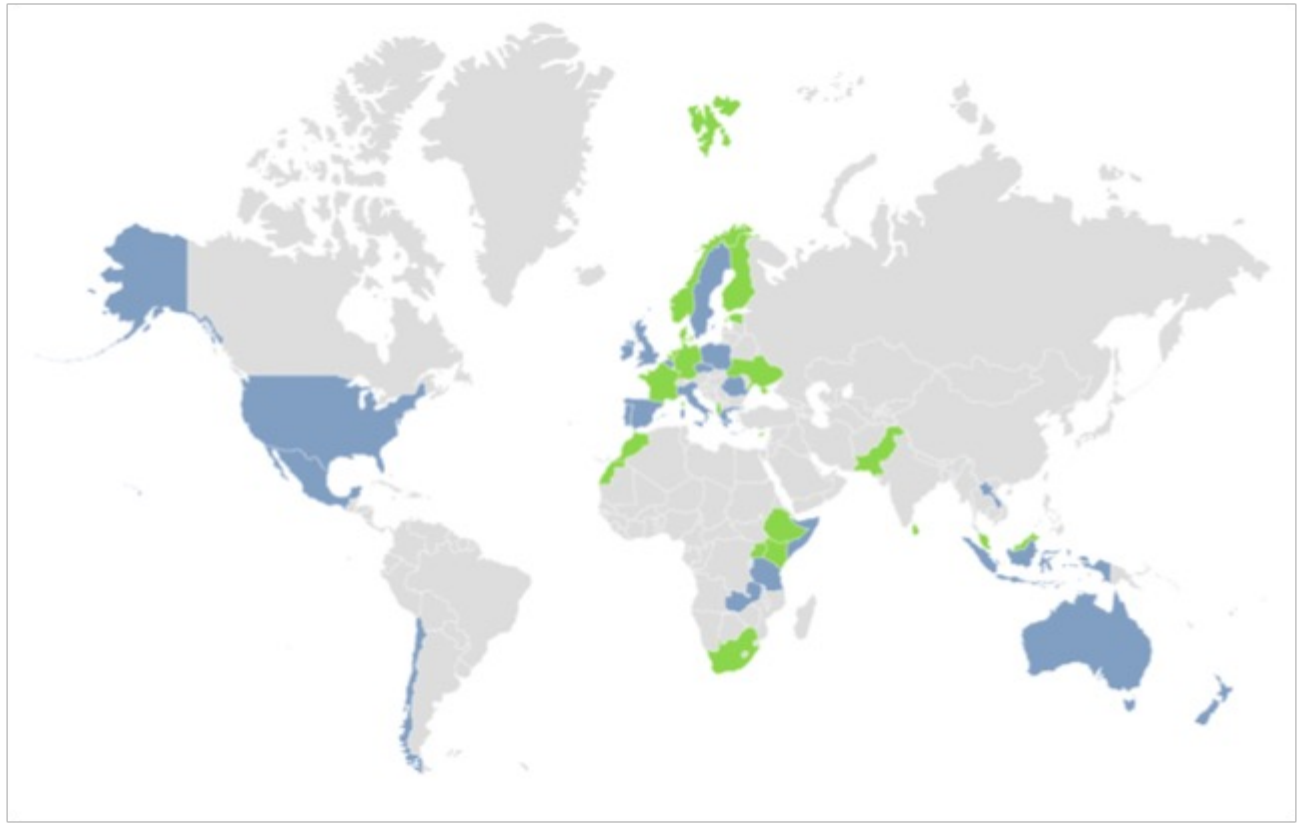
eduVPN today (2)

- 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



eduVPN today (3)

- At least 156 universities and 19 NREN deployments
- Used in (at least) 38 countries
- Most successful in NL (27), Germany (29 universities)
- One university server in Sweden



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

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

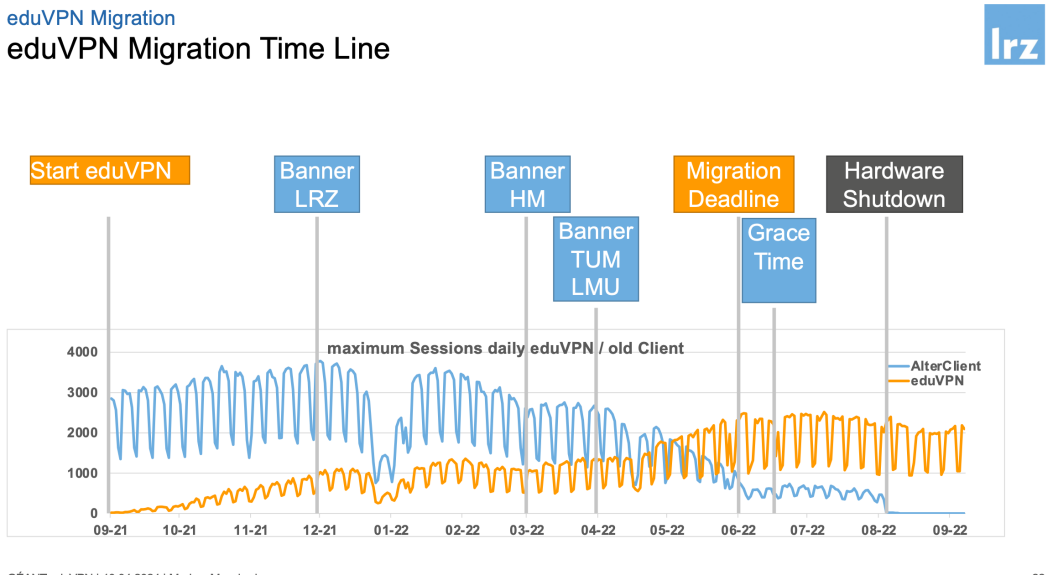
- 11000 students and 6000 staff
- Requirements/features:
  - 1000 concurrent users;
  - Hardware with 10Gbps interfaces;
  - Differentiated access to services according to type of user, equipment used.
- Cost in 2019: 100 kEUR for hardware + 35 kEUR in licenses for 3 years
- Huge supplement for extra 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.

Deployment example 1: Stand-alone instance. Otago University

- Need to scale up because of CoVID-19: existing VPN used nearly EOL hardware. Needed to either buy new concentrators for 500 kNZD (275kEUR) 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 / Microsoft Entra ID with conditional access (MFA)
- Use of php-saml-sp as it was easier to setup with Azure AD working out of the box with minimal changes

Deployment 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.
- See Markus’ presentation: https://events.geant.org/event/1515/contributions/1696/attachments/954/1472/eduvpn-GSD-2024-04.pdf



Deployment 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
- L2 circuit back to the private resource
- Support by SURF
- No need for hardware on campus or licensing limitations

4 most asked features

- Multi Factor Authentication
- High Availability / Redundancy (HA/R)
- Real Time Authorization
- Managed devices

Multi-Factor Authentication

- “First Factor”: Username & Password
- “Second Factor”: (T)OTP, Hardware Token, WebAuthn, Biometrics, ...
- Where does MFA belong?
  - Service
  - IdM

- We chose for *not* managing MFA for the institutes
  - MFA in IdM
  - MFA in separate system, e.g. PrivacyIDEA

HA/R (1)

- Architecture
  - Portal / controller
    - Web interface, API, Database, Authentication, Authorization, Logging, (Server) Administration, ...
  - Node
    - Handles VPN connections

- Each component takes different approach
  - Portal
    - HA/R DB, Session Storage, Hot Spare, Failover, ...
  - Node
    - Simply have >1 and have the portal(s) direct user to one that is “up”
    - Complexity obviously in the Portal

HA/R (2)

- Portal
  - memcached (Session Storage)
  - PostgreSQL / MariaDB* (Database)
  - keepalived (Failover)

- Node
  - When a client connects, it is directed to a “Node”
    - ... that is “up”
    - ... not under heavy load*

Real time authentication

- Common in R&E to use SAML (“WebSSO Profile”)
  - Session is a valid for ~8 hours
  - No way to verify session after initial authentication
    - User disabled?
    - Permissions changed?
  - Having users authenticate (possibly with MFA) every 8 hours is *not great UX…*

- Some Ideas
  - Use *SAML* for Authentication, *LDAP* for “Real Time” Authorization
  - Use *OpenID Connect* for Authentication *and* “Real Time” Authorization*

Managed devices (1)

- Devices owned and managed by the organization “System VPN”
  - Bound to *device*, not necessarily user
  - Always on
  - Active *before* user authenticates to device
    - For example: Kerberos/LDAP/AD only reachable over VPN

- Enrollment
  - Obtain a *per device* VPN configuration file through the eduVPN Server “Admin API”
  - Deploy WireGuard on device
  - Copy a device specific VPN configuration file to device
  - Enable WireGuard service on system boot

- Conceptually it is *very* easy!

Managed devices (2)

- Practice
  - GPO works for Windows, but not (out of the box) with macOS
  - Intune works for Windows and macOS, but you can’t send a (device specific) configuration file to the device from what we understand...
- Approaches
  - Try to make Intune work anyway (script runs on device to obtain configuration)
  - Take separate approaches for macOS and Windows
- Pilot with institute in NL this year
  If you know an organization that has:
- Windows / macOS Managed Devices
  - Uses Intune and/or GPOs, or other software to control the devices
  - Wants to use eduVPN
  - Have the knowledge/resources to help us test it and provide feedback

Roadmap

- 3.x
  - WireGuard + TCP
    - Already works! (except on iOS/macOS)
    - Some networks block UDP, or have MTU issues
    - Send WireGuard traffic over TCP (actually, over TLS through the Web Server in (Reverse) Proxy Mode
- 4.x (Release: 2025-05?)
  - Drop OpenVPN
  - “User Defined” Networks
  - Move Server Configuration to DB
    - Allow server admins to change (some) configuration through Web UI

Set up your own eduVPN instance in 6 steps

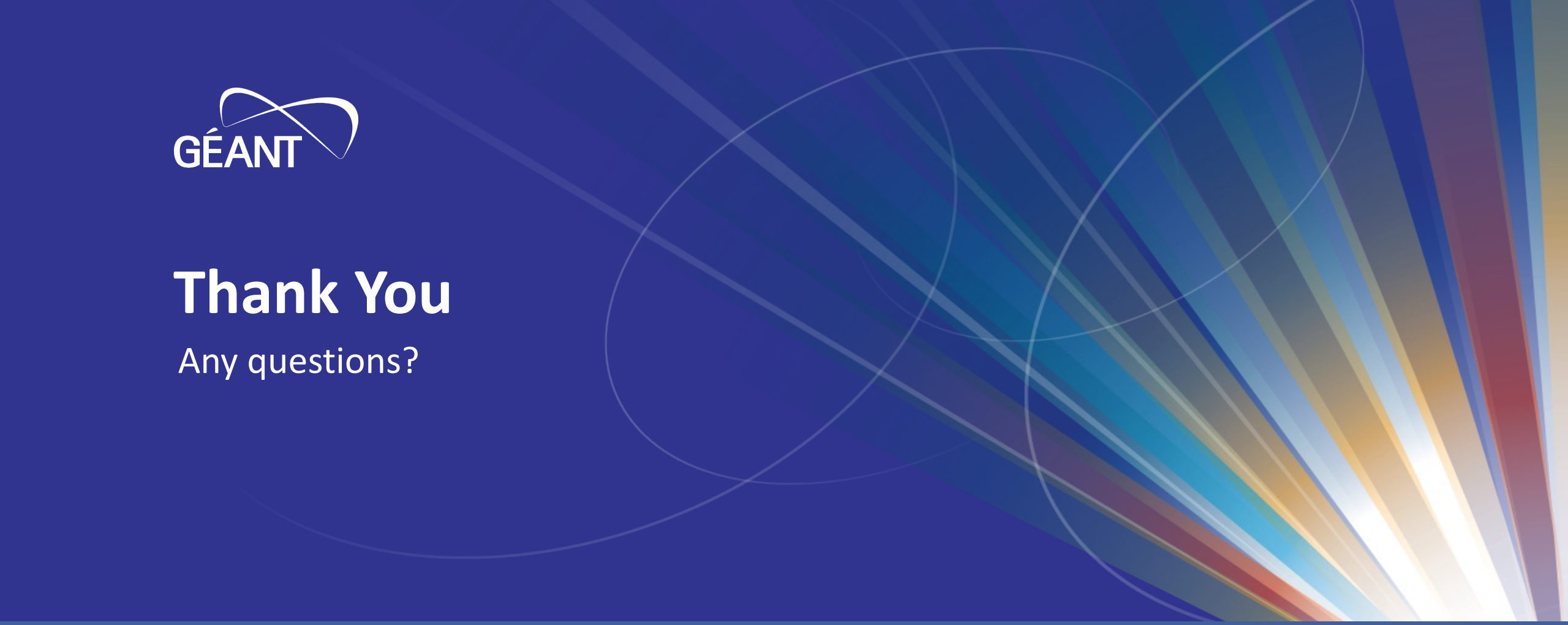
1. get a VM with one of the supported OSes
2. follow the deploy instructions
3. configure network (if necessary)
4. configure authentication
5. test server with eduVPN apps (by specifying hostname in search box)
6. request to be registered in eduVPN apps

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

Contact

eduVPN Team: eduvpn-support@lists.geant.org

Web: https://www.eduvpn.org



Thank You

Any questions?

www.geant.org

Co-funded by
the European Union

The Commons Conservancy

- 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

THE COMMONS CONSERVANCY