eduVPN Training

www.geant.org

Agenda

1. Roundtable

2. eduVPN technical overview

- eduVPN description
- eduVPN use cases
- eduVPN clients availability
- eduVPN requirements
- eduVPN integration

3. Hands on exercises

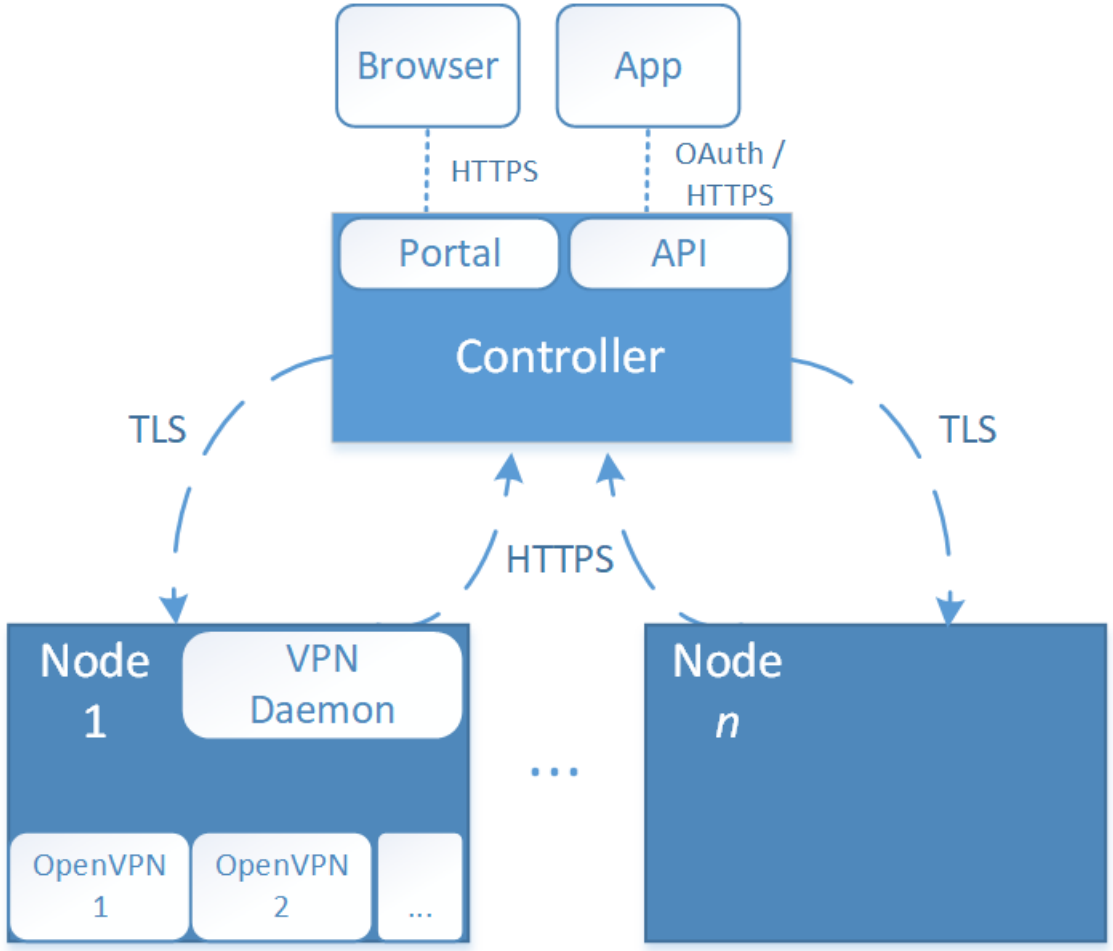
- Instructions related to the training organization
- Instructions related to the training VMs
- Instructions to install and configure eduVPN
- Instructions to connect eduVPN to “SAML IdP” and “LDAP directory”

eduVPN description

The purpose of eduVPN is to provide a more secure access to public and private networks for the international research and education community. The essential eduVPN user experience should be: “open your laptop and be securely online”.

eduVPN service instances offered by NRENs or universities, research labs, etc. (hereafter called "Institutes") allow students, researchers and staff from participating institutions to obtain a VPN on their devices to known end-points to access **private or public networks across the world**.

eduVPN description : eduVPN Architecture



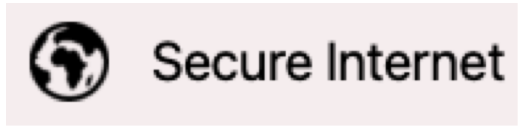
More details : https://github.com/eduvpn/documentation/blob/v2/ARCH.md

eduVPN use cases

"Brand"	What	Audience	User Authentication
Secure Internet	Generic VPN service	NRENs	(National) Identity Federation (SAML)
Institute Access	VPN service that gives access to institute's resources	Institutes	SAML, LDAP, RADIUS, ...

Currently there are 19 Countries and over 100 Institutional eduVPN participants

eduVPN use cases :



- Offered by NREN for all users belonging to the institute's the NREN services
- Connected to (national) identity federation
- Allows users using VPN services hosted by other NRENs
- Allow users of other NRENs to use your server (reciprocity)
- Allow for rudimentary network filtering by institutes to only allow users coming from the NRENs VPN service if institute is too small to deploy their own VPN service, and filtering on NREN VPN IPs is considered acceptable

eduVPN use cases

- when using public WiFi that is not trusted
- using a network that has restrictions, e.g. blocks SSH, only allows TCP 80/443, etc.
- when traveling abroad to have access to resources only available from within a region/country, e.g. public TV
- Choose a trusted endpoint closest to your current location, e.g. when traveling to reduce latency
- Test your services from different locations
- Avoid service customization based on location, e.g. search results that are tailored to your location

eduVPN use cases :

- Offered by Institute, exclusively for **their** users
- Allows access to internal institute resources, e.g. "intranet"
- Various methods of user authentication (SAML, LDAP, RADIUS, ...)
- Fine grained authorization based on e.g. group membership/permissions
- Self hosted by institute (France, Germany, ...), or hosted by NREN on behalf of institute (Norway, The Netherlands)

eduVPN : demo

eduVPN Client availability :

- eduVPN project started as "server only", supporting all known OpenVPN (compatible) clients
- Improve usability by writing native eduVPN apps for most common platforms (Windows, macOS, Android, iOS, Linux) and implement OAuth API in the server

eduVPN Client availability : user flow without clients

- Users navigates to the web interface of the VPN server
- User authenticates
- User downloads a configuration file
- User imports the configuration file in their VPN client
- User connects to VPN

eduVPN Client availability : user flow with clients

- User starts app
- User chooses/searches for their institute
- Authorization (+Authentication) triggered through browser;
- App shows available VPN profiles for user (iff > 1 available);
- App connects to VPN

eduVPN requirements

- To get started a simple VM suffices:
  - 1 CPU core
  - 1024 MB RAM
  - 5G disk
  - Debian 11
- (We also support CentOS 7, Debian >= 9, Fedora)
- *Ubuntu: works, but no (guaranteed) security updates for some components we rely on from "universe".*

eduVPN challenges

- In practice we notice biggest issue with deploying eduVPN is:
  - Identity Management integration, i.e. SAML
- Strictly speaking this is not an eduVPN problem, but still a barrier to adoption.
- This workshop will focus especially on Identity Management integration, i.e. SAML and LDAP as examples.

How to keep contact and work remotely ?

- Online:
  - Use Rendez-vous for online sessions : https://rendez-vous.renater.fr/eduvpn-training-2022
  - Use Rendez-vous for breakout sessions if you need any help
  - For a better user experience, please use Google Chrome or Firefox

- Offline:

  Please join the channel **https://web.libera.chat/#eduvpn-workshop**
  You would need only a browser and no registration is required.

- VMs:
  - Each participant will have a dedicated VM, from the beginning to the end of the training and for all the hands-on exercises.

VMs –> Check if you have access

- SSH student@eduVPN-00**XX**.vm.geant.org → pass : **!eduVPN2022#**
- **Root access enabled !!! Be careful !!!**
- Replace **XX** by your **VM** number

Participants	VM number
Andrijana	03
Aristos	04
Katarina	05
Nikola	06
Sergey	07
Tural	08
Zurab	09
Dainius	10
Andreas	12

VMs –> Useful info

- **OS :** Ubuntu 20.04.4
- **Firewall** : SSH (port 22, TCP) and tcp/80,tcp/443, udp/1194 and tcp/1194 and UDP 443
- **DNS:** configured with eduVPN-00**XX**.vm.geant.org

- **SSL certificate available here** :
  - SSLCertificateFile /etc/ssl/certs/wildcard_vm.geant.org.crt
  - SSLCertificateKeyFile /etc/ssl/private/wildcard_vm.geant.org.key
  - SSLCACertificateFile /etc/ssl/certs/ca-certificates.crt

Next Steps

- Join **#eduvpn-workshop** channel
- Test access to the VMs
- Start following the hands on exercises :
  - https://github.com/eduvpn/documentation/blob/v2/DEPLOY_DEBIAN.md#base-deploy

To test your eduVPN instance : Test IdP and test LDAP

- **To configure the authentication** we prepared a test IdP and a test LDAP :
  - https://github.com/eduvpn/documentation/blob/v2/DEPLOY_DEBIAN.md#ldap
  - https://github.com/eduvpn/documentation/blob/v2/DEPLOY_DEBIAN.md#saml
- LDAP :
  - LDAP URL : ldaps://eduVPN-0024.vm.geant.org
  - LDAP admin : cn=ldapuser,ou=system,dc=vm,dc=geant,dc=org
  - LDAP admin pass : ldapuser
  - User account : uid=user1,ou=people,dc=vm,dc=geant,dc=org
  - User account pass : password
- IDP :
  - entityID=https://eduVPN-0024.vm.geant.org/idp/shibboleth
  - Metadata URL : https://eduVPN-0024.vm.geant.org/idp/shibboleth
  - User/pass: user1/password

Any questions ????

Thank you

Any questions?

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).