eduVPN 3.0

eduVPN Deployers Meeting 2021-03-25

What is (in) eduVPN 3.x?

- WireGuard support
- New crypto defaults for OpenVPN
- New OAuth token format
- Dropping support for old(er) server OS

Previously…

- Plan for eduVPN 3.x as far back in November 2019
- Still didn’t happen…
  - Nobody likes re-installing their server
  - We were able to fix/add many things in 2.x

Why eduVPN 3.x?

- Allows us to make VPN clients *reauthorize*
- Allows us to ask the operator/admin to do a little more than simply install updates...
- Allows us to require new server OS version
- Allows us to bump Go and PHP version requirements

Why Now?

- **OpenVPN 2.5**
  - became available (upgrade from 2.4)
- **Debian 11**
  - almost available (expected summer 2021)
- **WireGuard**
  - became stable and integrated in more OSes so we can leverage that without 3rd party repositories
- **OAuth**
  - OAuth 2.1 draft RFC available

When?

We aim for **Q4-2021**

OpenVPN 2.5

- TLSv1.3
- EdDSA (Ed25519) keys
  - RSA key generation is *very* slow
  - ECDSA has questionable security
- Will require modern clients
  - All current eduVPN applications already support this baseline

Debian 11

- OpenVPN 2.5
- PHP 7.4
- Go 1.15
- WireGuard

WireGuard

- Support WireGuard “out of the box”
- Support for **official WireGuard** clients as well as **eduVPN clients**
  - Full support in all eduVPN clients may take a while…
  - We have an eduVPN for Android app with WireGuard support (PoC)

OAuth

- OAuth 2.1 specification becomes (much) more strict
- Most of the new requirements were already implemented in our OAuth server
- **Missing**: refresh_tokens are only allowed to be used once

Server Requirements

- We will officially support:
  - Debian >= 11
  - Fedora >= 34
- We recommend **Debian 11**
- An upgrade path will be provided for eduVPN 2.x running on Debian 10

CentOS

- CentOS 8 is EOLed, no longer 10 years of support...
- CentOS Stream is a “rolling release” containing future RHEL 8 updates
  - Might as well run Fedora?
- **Still** missing EPEL for CentOS 8 / Stream
  - php-sodium
  - Various PHP libraries / tools we depend on
- Red Hat wants you to run proprietary Red Hat Enterprise which can now be obtained for free for some use cases

Ubuntu

- Some deployers are running Ubuntu (using the Debian packages)
- **Q:** Why Ubuntu when there is Debian?
- Ubuntu is much less “LTS” than you’d hope (universe/multiverse)…
  - See /usr/bin/ubuntu-security-status
- We *might* support Ubuntu >= 21.04

Upgrade Path

- **Assumption**: currently on Debian 10 & eduVPN 2.x
- Upgrade your server to Debian 11
  - eduVPN 2.x also supports Debian 11
- Upgrade to eduVPN 3.x

Our TODO (1)

- High Availability / Load Balancing
  - Implemented in eduVPN app, servers share one OAuth token
- Update OAuth server to be OAuth 2.1 draft compatible
- Merge vpn-daemon and wg-daemon
- Introduce “API 3.0” for clients that reduces number of calls
  - Only “info”, “setup”, “connect” and “disconnect” calls
  - Support client-side generated keys (for WireGuard)
- Packaging work for Debian for some Go dependencies

Our TODO (2)

- Use pseudonym for user IDs through “Guest Usage” (Secure Internet)
- OpenVPN “tls-cryptv2” support?
- Support IPv4 and/or IPv6 only VPN?
- Switch to https://franto.tuxed.net/ from JWT?
  - Although that sounds like spending another “innovation token” ;-)
- Keep (aggregated) usage stats longer than 30 days

Our TODO (3)

- Support expiring VPN sessions in the night instead of exactly 7, 30, 90 days later, but don’t forget to consider timezones ;-)
- Limit the number of active connections per user

References

- **OpenVPN 2.5:** https://github.com/OpenVPN/openvpn/blob/release/2.5/Changes.rst
- **OAuth 2.1:** https://tools.ietf.org/html/draft-ietf-oauth-v2-1-02