Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften

Security .Days

<Prague.CZ>
<9-11 April 2024>

GÉANT

lrz

eduVPN at the Leibniz Supercomputing Centre

GÉANT Security Days 2024 | Markus Meschederu

Overview

eduVPN at the Leibniz Supercomputing Centre

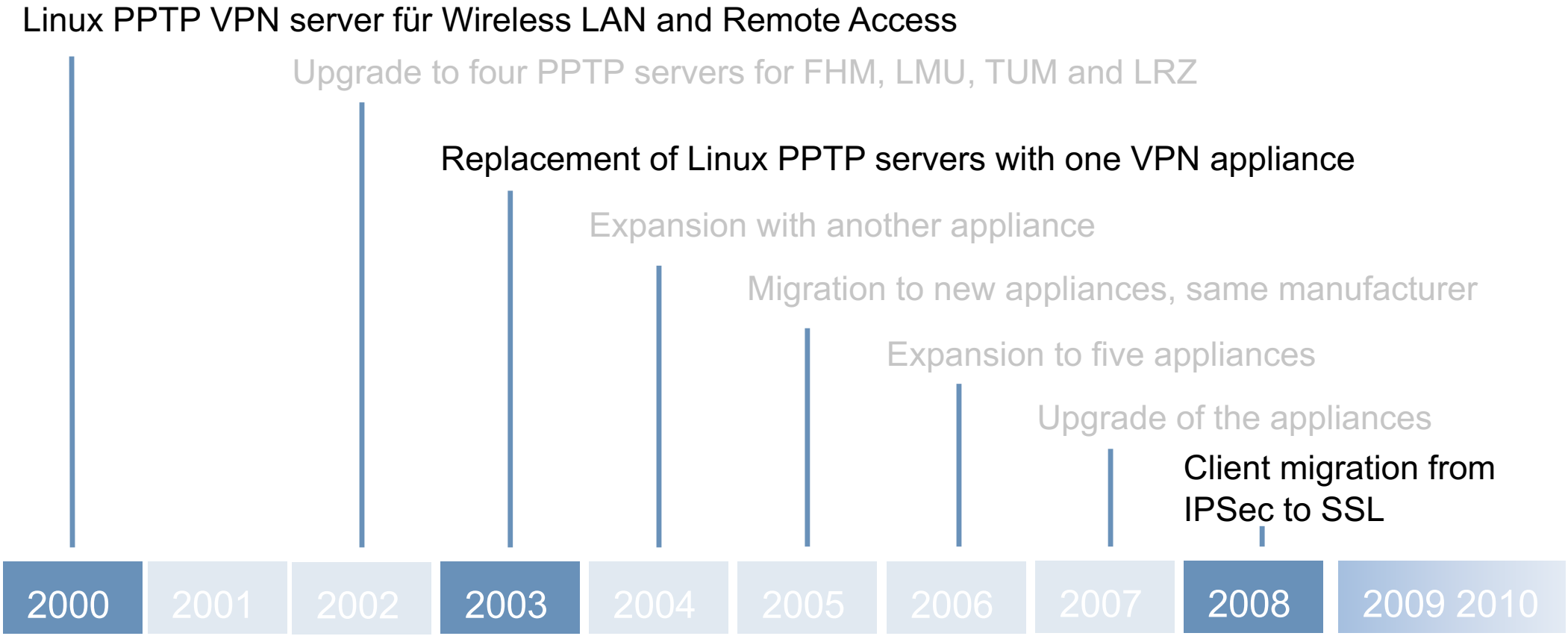
- Migration of an existing VPN solution in the Munich Scientific Network to eduVPN.
- Upgrade from eduVPN version 2 to eduVPN version 3

Munich Scientific Network (Münchner Wissenschaftsnetz, MWN)

- Operated by LRZ
- Connects more than 130 000 users and more than 300 000 devices.
- Services for several universities in the Munich area:
  - Technical University of Munich, TUM
  - Ludwig-Maximilians-University München, LMU
  - HM Hochschule München University Of Applied Sciences, HM
  - Weihenstephan-Triesdorf University of Applied Science, HSWT and smaller ones.

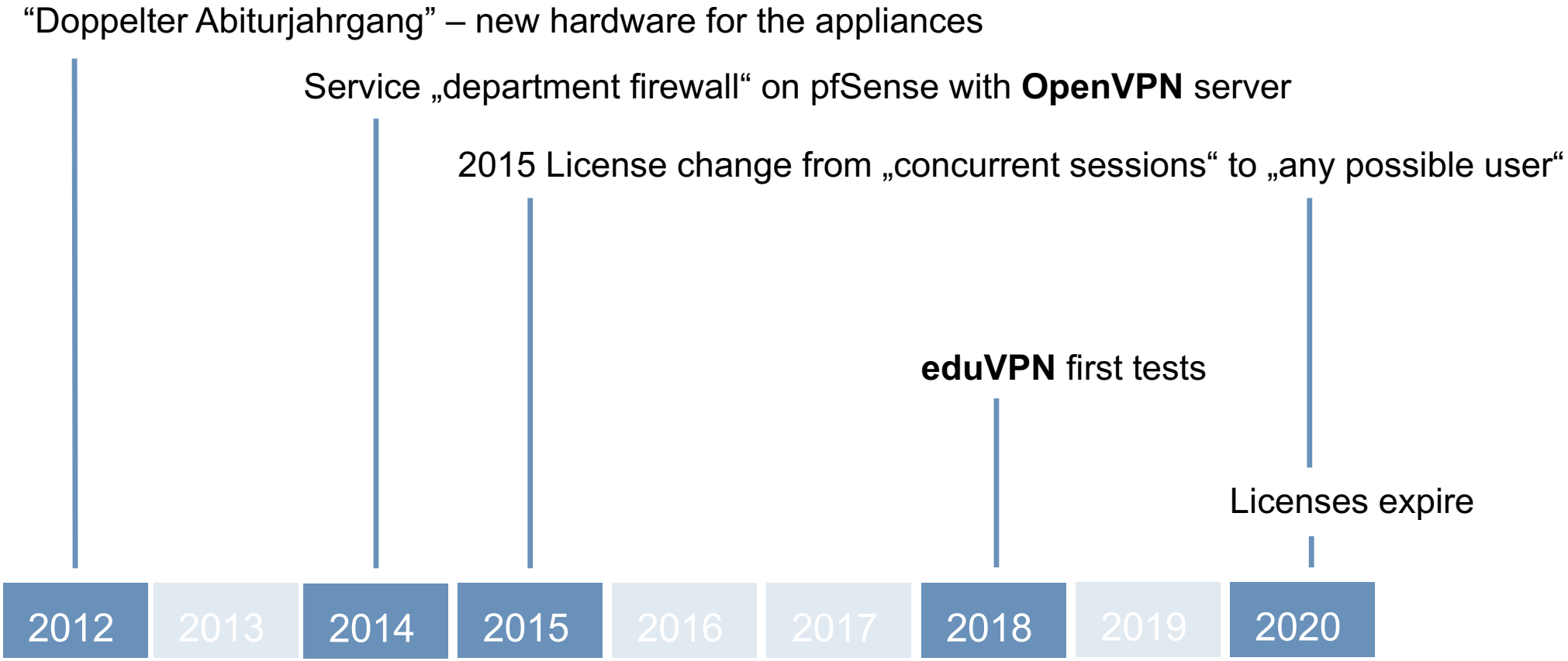
VPN in the Munich Scientific Network (MWN)

First Years 2000 - 2008



VPN in the Munich Scientific Network (MWN)

Peak VPN and the show must go on



New Challenges

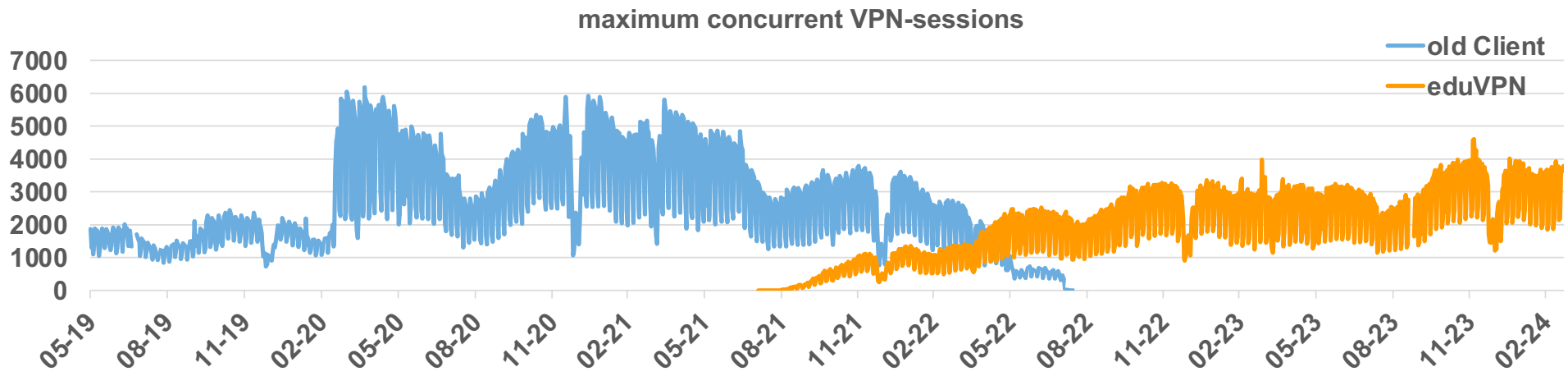
Late March, new challenges, home office, July, OpenVPN field test

September, Start of service **eduVPN**

August, shutdown of the old VPN appliances (EOL, support and licenses)

December, move from eduVPN 2 to eduVPN 3

2020 | 2021 | 2022 | 2023



Selecting eduVPN

Back into 2020 – How continue?

Migrate or keep on going?

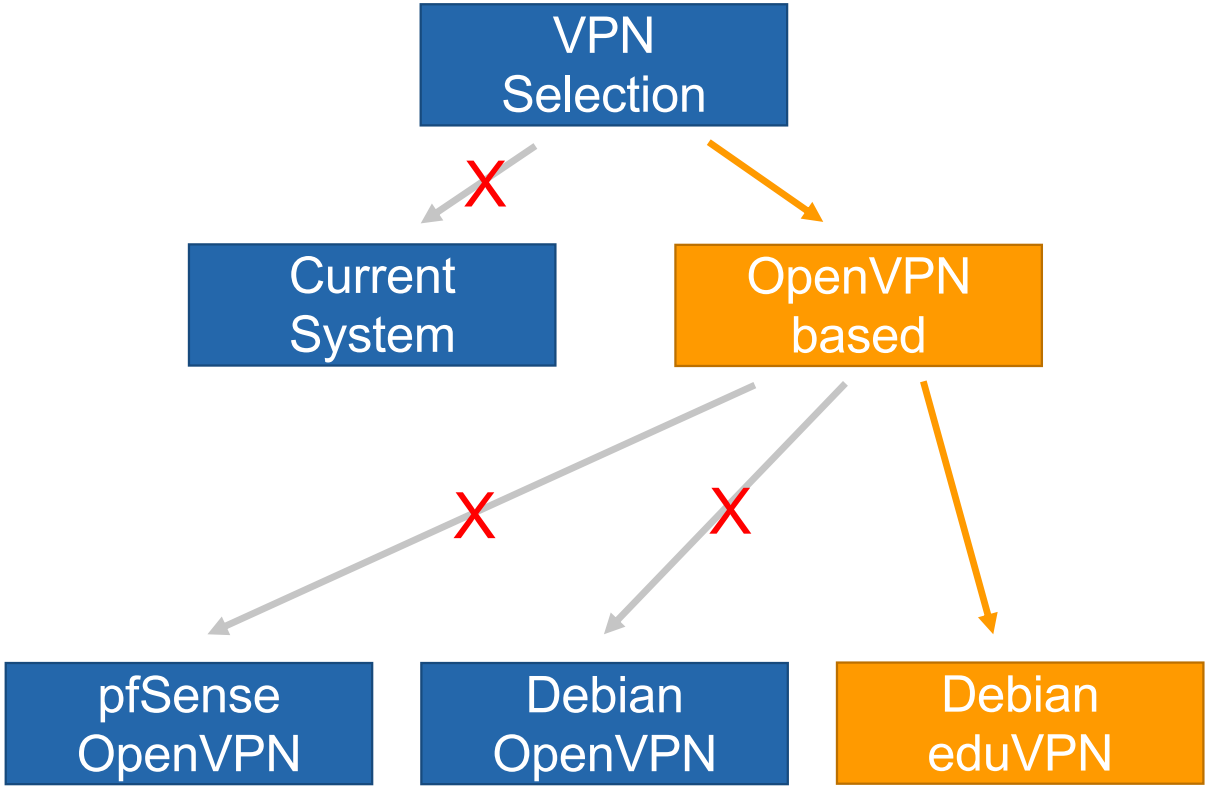
- Appliances, running out of support
- New licensing scheme
- New licenses and hardware
- Current VPN service is running and field-tested

Requirements are defined by existing VPN service

- Selection of different institutions and profiles
- Automatic upgrade of clients and configuration
- Clients for current operating systems
- Centralized authentication, authorization and accounting
- 6.000 concurrent sessions, load balancing
- Multi-factor authentication

Selecting eduVPN - Path of Choice

eduVPN as VPN sucessor



PRO eduVPN

- Client
  - Good interoperability
  - Configuration deployment server side
  - Automatic Updates
- Server
  - Multi-factor authentication supported
  - OpenVPN, WireGuard
- Scalability
- License model
- Future
  - Developed for university environment
  - Further development via a GÉANT project

CONTRA eduVPN

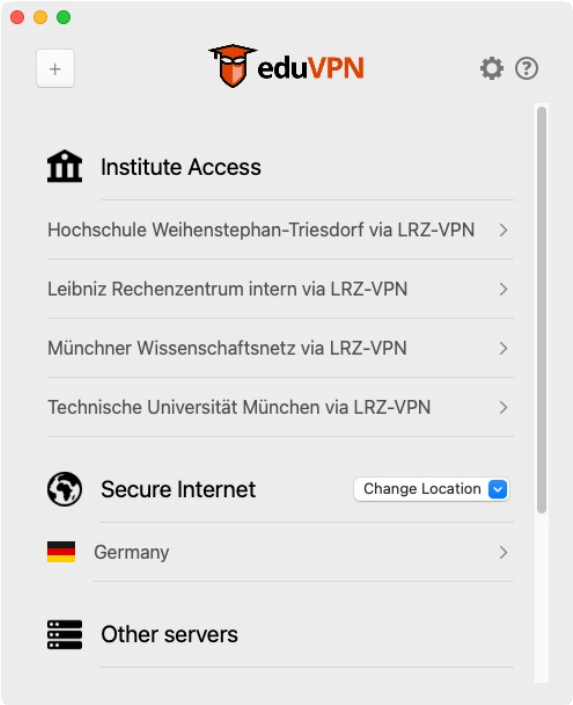
- No operational experience

Selecting eduVPN

eduVPN

General

- OpenSource project (Commons Conservancy, GÉANT)
- OpenVPN as VPN server, WireGuard with eduVPN Version 3
- Two modes of operation, Secure Internet and Institute Access
- OpenVPN with client certificate
  - Automatic renewal of client certificate with eduVPN client
  - New authorization only after „Session Expiry“



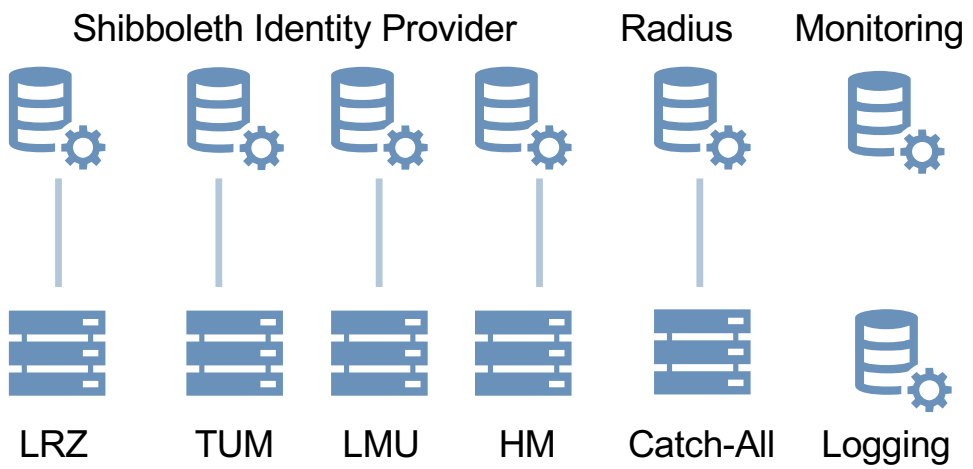
Important for us

- Automatic client upgrade
- Automatic VPN configuration upgrade, multiple profiles
- Selection of home university from user‘s side

eduVPN Deployment

Setup

- Dedicated servers for the „big“ institutions
  LMU, TUM, HM
- One catch-all server for the rest
- One dedicated server for LRZ staff
- Per Server: one Controller, two+ nodes with VPN server processes



Controller	Login, Configurations
Node 1	VPN-Server
Node 2	VPN-Server

Authentication: Shibboleth, LDAP or Radius?

Shibboleth for the big universities

- Universities were already registered as Identity providers (IdP)
- Additional security, like MFA, can be deployed on IdPs
- No processing of user passwords on local servers
- Controller have to be registered as service providers (SP)
- shibd daemon is hungry for resources

LDAP had no advantages to Shibboleth

Radius

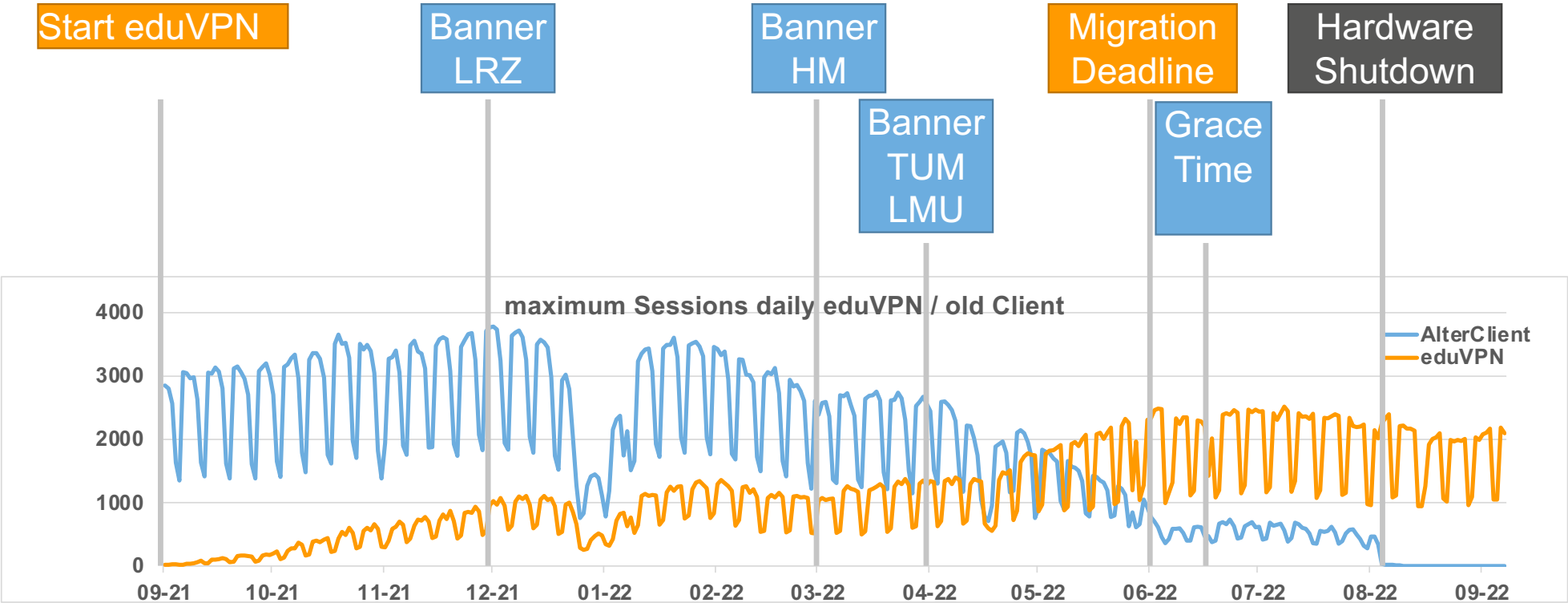
- Radius protocol is used with the catch-all server
- Attribute assignment was only possible with LDAP or Shibboleth
- Attribute assignment was quickly implemented by the eduVPN developer team

Server setup

- Debian
- VM-Ware
  - Controller and Nodes: 2 CPU cores and 4 GB RAM
  - Nodes: two network interfaces with source-based routing
- Configuration with puppet
- Monitoring with Check_MK
- Load balancing with round robin distribution on nodes
- IP-Pools are distributed to multiple OpenVPN server processes

Migration I

eduVPN Migration Time Line



Migration I – Summary and Lessons learnt

- Migration from old running VPN to eduVPN finished
- Technical problems are easy to fix, but it's the little things that cause big problems
- Communication with the universities' IT-service centres
  - Important, on a regular base
  - Take their problems and concerns seriously
  - Be prepared for a wave of support request at the service desks
- Good documentation does not do any harm
- Start of new terms helps with the migration
- Despite of information, circular email, login banner on every login you will not reach out to every single user
- Keep in mind of the language barrier (technical – academic)

Moving from eduVPN Version 2 to Version 3

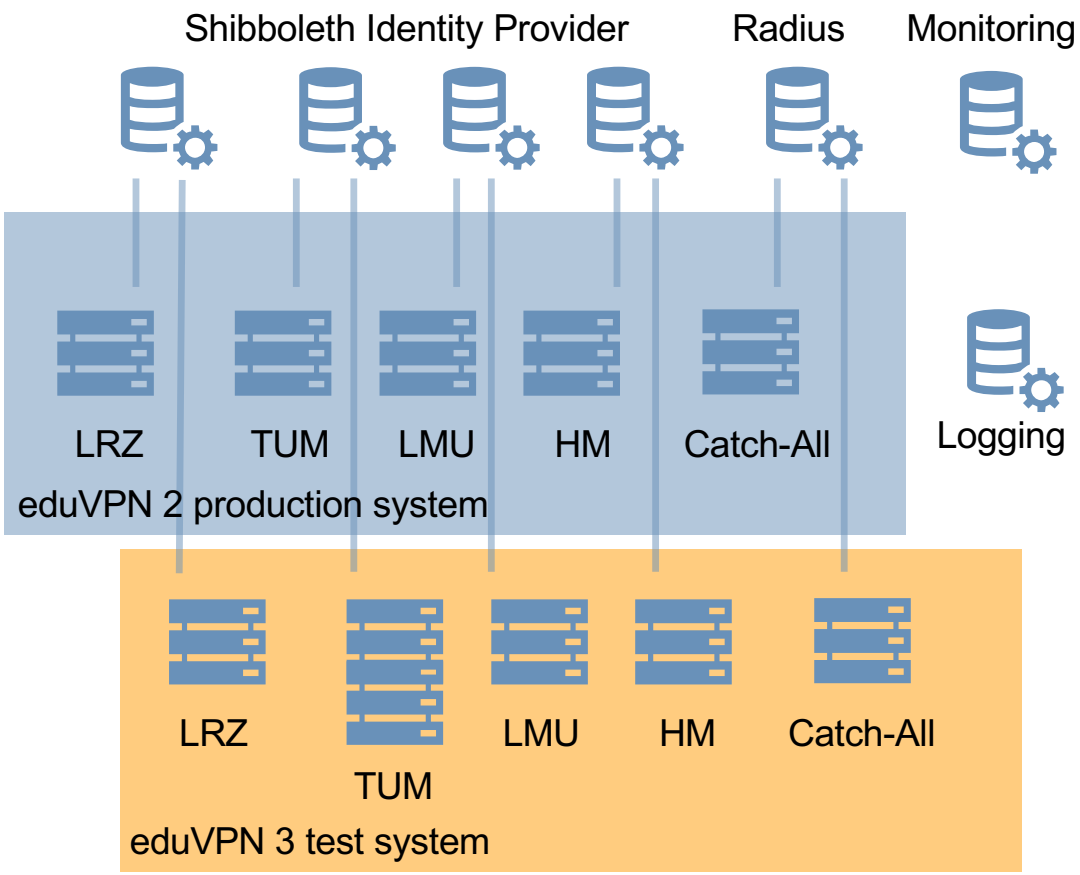
What happened next – Moving from eduVPN 2 to eduVPN 3

Why? When? How?

- Reasons
  - eduVPN 2 goes EOL in June 2024
  - Demand for WireGuard
- Which date will be the best?
  - During or outside semester/term?
  - Last week in 2023
- Which migration path will be the best?
  - Parallel service causes confusion
  - Upgrading servers during downtime to risky
  - Build new servers with latest operating system and eduVPN 3 as a test system
  - Hard switchover with rollback option

Migration Setup

- Test systems are built parallel to production systems
- Accessible directly via “test-FQDN” in eduVPN client
- Switch production and test system by changing DNS entries and configuration.
- Rollback option



Controller	Login, Configurations
Node 1	VPN-Server
Node 2	VPN-Server

Migration process

How it should work:

- Shut down eduVPN services on controller and nodes
- Point server FQDN to new controller in DNS (TTL)
- Rename controller
- Configure nodes for new controller

How it actually worked:

- Server migration went through without greater problems
- Clients, which made a new connection with authorization worked out of the box
- Clients with still valid authorizations had to rediscover
- Easy workarounds, quickly documented

Problems and Lessons learnt

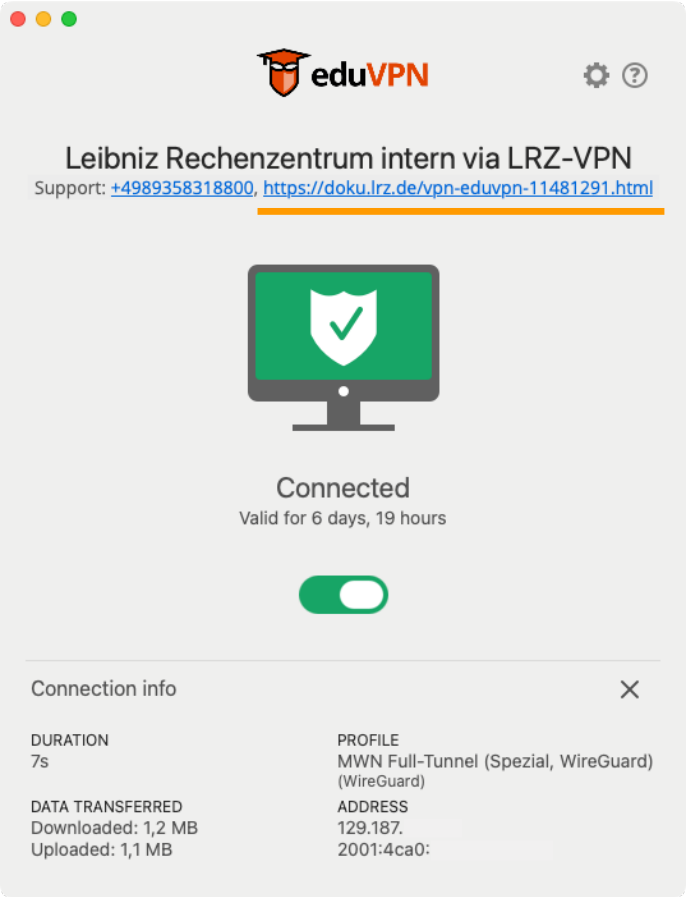
Problems

- Linux with firewalld blocked WireGuard (IPv6rpfilter)
- Low WireGuard throughput due to broken path MTU discovery (provider)

Lessons learnt

A lot of incidents came in, which were mostly resolvable with a simple workaround

- Guide your users to self-service and self-solve
- Useful support information in eduVPN window
- Link to documentation where users can help themselves
- Reduction of incidents



Resume

- Switching to eduVPN proved to be the right decision.
- Secure access to internal university resources.
- End user support does not show any unsolvable problems.
- Architecture of eduVPN makes it easy to add additional resources.
- Support of the eduVPN developer team leads to quick and satisfying problem solutions.

Questions?

Links

- eduVPN Homepage https://www.eduvpn.org
- eduVPN Server Documentation https://docs.eduvpn.org/server/v3/index.html

- eduVPN at LRZ https://doku.lrz.de/vpn-eduvpn-11481291.html