

February 10th, 2021, eResearch NZ 2021

# Deploying secure and scalable VPN connections with eduVPN

Vlad Menci

RESEARCH NZ



# What is eduVPN and Let's Connect

- eduVPN - also known as Let's Connect
  - Open-source VPN solution
    - VPN Server
      - OpenVPN under the hood
    - VPN Clients
      - Windows
      - Mac OSX
      - Android
      - iOS
      - Or any OpenVPN client - but better use Let'sConnect

## Name difference: eduVPN vs Let's Connect

- Let's Connect is simplified for single organisation use
  - Users just point to one server  
[letsconnect.malaghan.org.nz](https://letsconnect.malaghan.org.nz)
- eduVPN targets R&E community
  - provide secure Internet connection on the go
  - VPN server run for the community - with federated login
  - Any interest in having NZ eduVPN via Tuakiri?

## Why eduVPN

- Strong need for VPN solution
  - More people working from home
  - Existing VPN solution might not cope
    - Hardware firewalls have longer replacement cycles

"Just run OpenVPN on a Linux server"

... and that's what eduVPN does

but in an easy-to-use way (client and server)

## Why eduVPN - performance

### Up to 1000 **concurrent** clients on 1 server

- Split over multiple CPU cores (16 assumed) with AES-NI
- Split via multiple openvpn processes running on alternate ports
- Can also scale higher over multiple nodes
  - with a single controller, also serving as a worker node
- Of course, YMMV - firewalls, other bottlenecks

<https://www.letsconnect-vpn.org/blog/does-it-scale.html>

## Why eduVPN - ease of setup

### Typical deployment - without eduVPN

- install plain openvpn, explore config, setup CA
- craft per-user connection profile
  - manually deploy on end-user device

## Why eduVPN - ease of setup (cont.)

### eduVPN:

- creates openVPN config
- runs a CA
- creates user connection profiles on-demand
  - after user authenticates
- client apps fetch and deploy openvpn profiles
  - authentication is done from within app (built-in or external browser)

## Why eduVPN - web portals

### User Portal:

- Users can manage their configs and devices

### Admin Portal: an admin can manage:

- Users (and their configs and connections)
- View overall stats
- Block users



## Why eduVPN - ease of setup - server side

- Configure authentication: one of
  - LDAP
  - Radius
  - SAML (Tuakiri login)
  - Local username + password
- Optional 2FA
  - Google Authenticator

## Setting up eduVPN - openvpn config

- Configure OpenVPN processes to run
  - one or more ports
  - TCP / UDP (recommended: both)
  - IP addresses to assign to clients (private range)
  - DNS config to push to clients
  - Routes to push
    - split tunnel vs. full VPN

## Setting up eduVPN - firewall

### Use iptables on the host

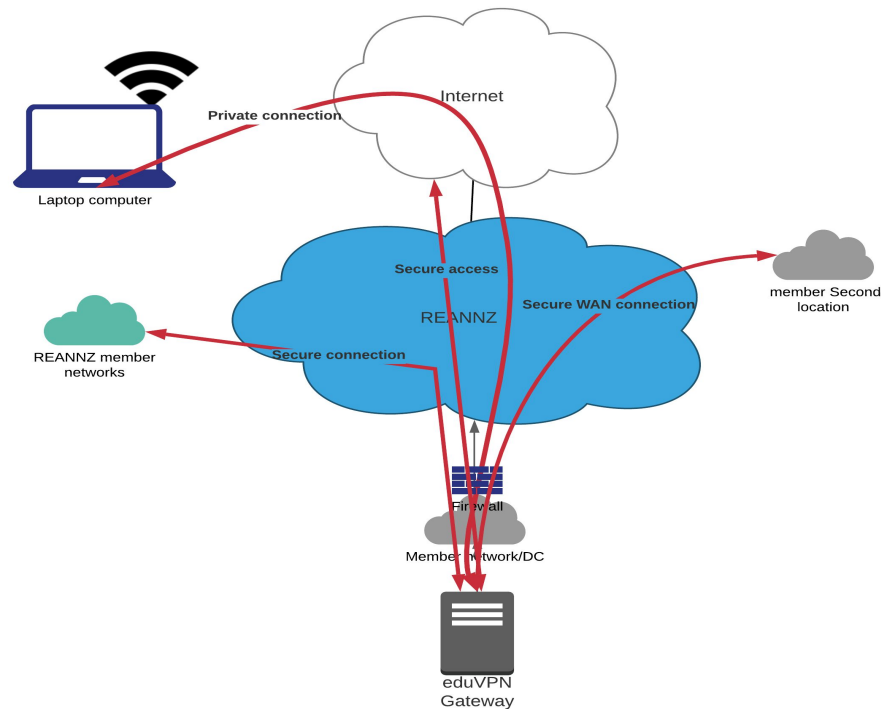
- can do NAT
  - or do NAT and firewalling in a separate firewall
- forward only between VPN tunnel and target interface

### Remember to allow IP forwarding

# Network aspects of eduVPN

- REANNZ network provides connection for eduVPN service
- Integrates to existing network services
- Member network can be extended (via a VLAN) to eduVPN server
- Secure access to Internet via eduVPN server (and from member IP range)
- Minimal config change to REANNZ network
- eduVPN server configures routing - Full VPN or split tunneling possible

Thanks to Yesh Ramesh @ REANNZ



# eduVPN: Security Considerations

eduVPN may not be for everyone:

- Connection profiles do not require any further authentication
  - At connection time, client authenticates with PKI credentials in connection profile
- Authentication is done when retrieving connection profile
  - 2FA supported: built-in Google Authenticator
  - Stronger authentication can be done externally (e.g. SAML IdP)
- No firewall included
  - either rely on iptables on the host
  - or route the traffic via a dedicated firewall

# VPN solution - Malaghan Institute of Medical Research

“Working with the REANNZ team was great - we had a few challenges along the way, but Yesh and Vlad stayed online for hours troubleshooting with me - going way above and beyond!”

Marie Armstrong, Head of IT



<https://www.reannz.co.nz/news-and-events/vpn-solution-malaghan-institute-of-medical-research/>

“Due to the lockdown all my work-related activities had to be moved off-site at short notice. This meant moving large datasets, that included millions of scientific data points, back and forth from our institute’s storage servers to my personal laptop for analysis via the VPN.

Due to the large size of the data only one of these files could be moved and analysed at any given time. As I had several data sets that needed to be analysed and compared to previous results this was extremely tedious and a frustrating experience prior to the improved VPN solution. Transfers sometimes had to be undertaken overnight or even crashed the system. I am very happy with the new VPN solution, as it allows me to transfer my data much quicker, it also communicates much better with the other institute software that we use to process and store these data files.”

Dr Johannes Mayer, a Postdoctoral Research Fellow at Malaghan Institute

## Questions about eduVPN

Happy to answer eduVPN questions now

# REANNZ Update: Tuakiri Hosted IdP

Hosted Tuakiri IdP is now available

- Tuakiri IdP run as a managed service by REANNZ
- Authentication via member-managed backend
- Cloud backend preferred
  - Google Apps
  - Office 365
- Multiple members co-located in hosting
  - Efficient to manage, yet each IdP operates independently
- Interested?
  - Talk to a friendly REANNZ staff member
  - Or just email [engagement@reannz.co.nz](mailto:engagement@reannz.co.nz)



February 10th, 2021, eResearch NZ 2021, Deploying  
secure and scalable VPN connections with eduVPN

# Thank you!

# Questions?

Vlad Menci

REANVZ

