Let’s Connect!

François Kooman

<fkooman@tuxed.net>
@fkooman

NLUUG – May 15th 2018, Utrecht

Polling Time!

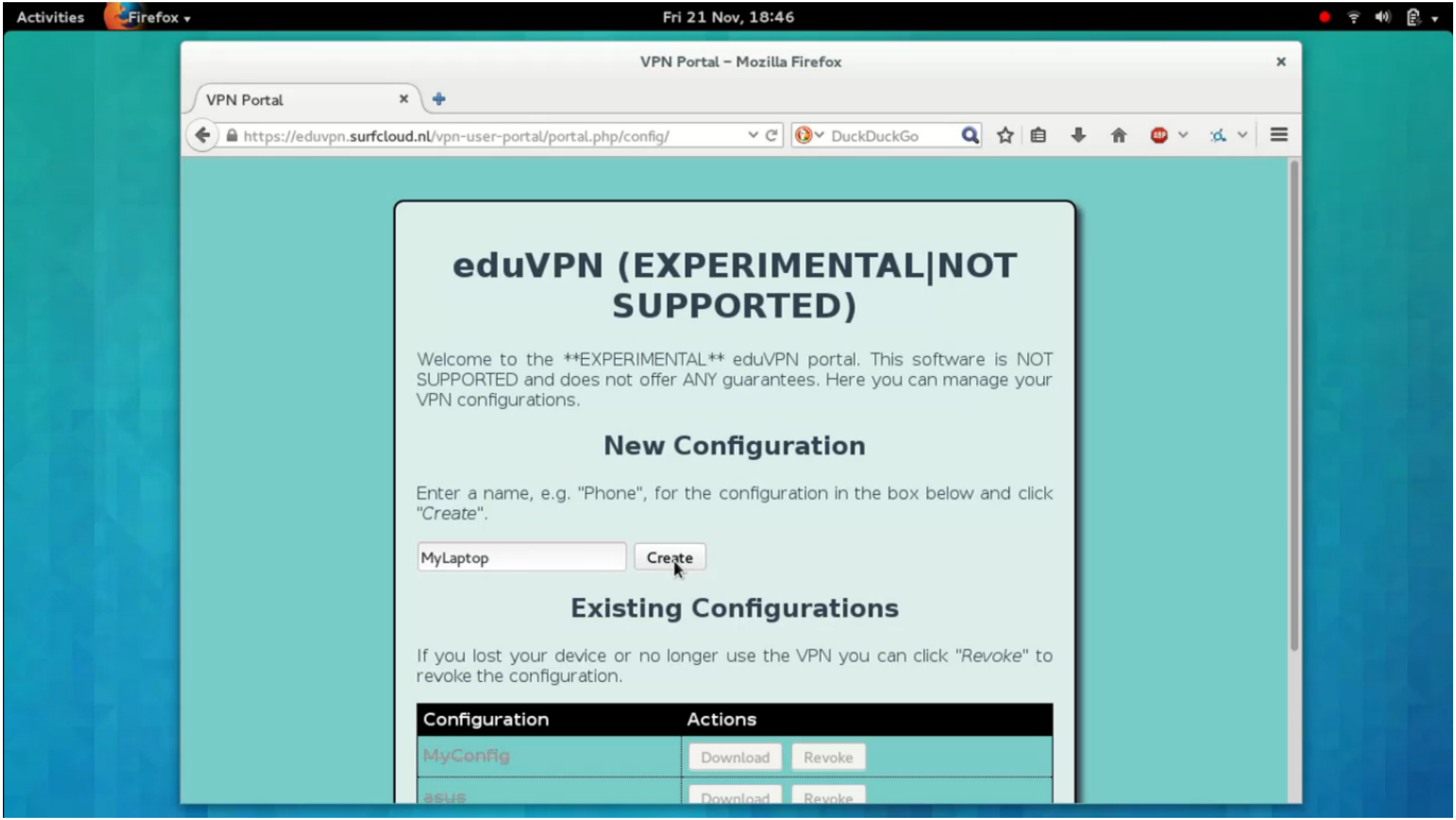
- Who knows what a VPN is? (-:
- Who uses a (commercial) VPN service?
- Who runs their own VPN server?
- Who *wants to run* their own VPN server?

Outline

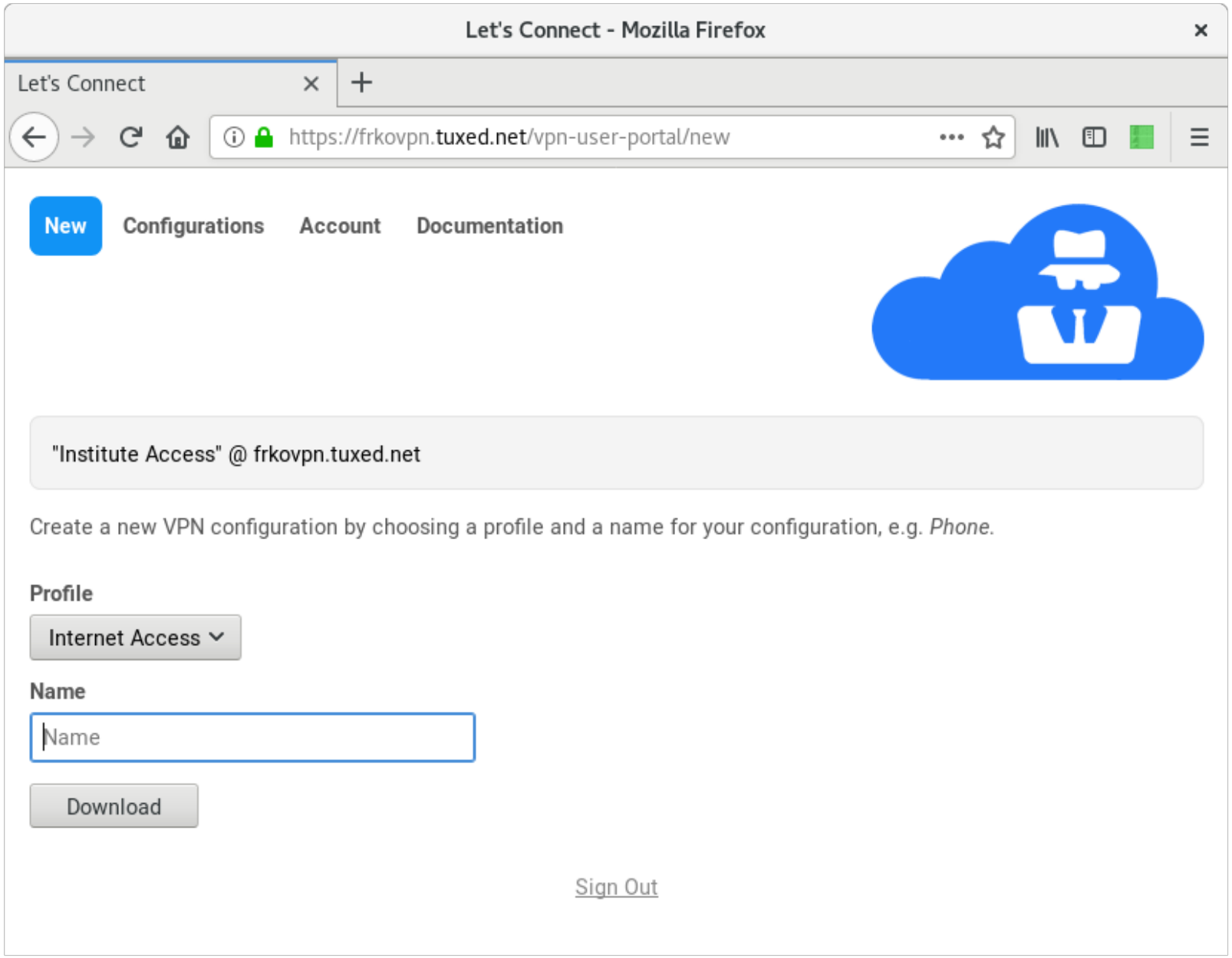
- Screenshot Parade
- Technology
- Application Integration (API)
- Distributed / Federated VPN
- Future Developments

Screenshot Parade

Initial Version...



Now


Let's Connect - Mozilla Firefox
Let's Connect
https://frkovpn.tuxed.net/vpn-user-portal/new
New
Configurations
Account
Documentation
"Institute Access" @ frkovpn.tuxed.net
Create a new VPN configuration by choosing a profile and a name for your configuration, e.g. Phone.
Profile
Internet Access
Name
Name
Download
Sign Out

Let's Connect - Mozilla Firefox

Let's Connect

https://frkovpn.tuxed.net/vpn-admin-portal/users

Connections | Users | Info | Stats | Messages | Log

User ID	Status
fkooman	Active
ash	TOTP Active
sebas	Active

Sign Out

eduVPN - Mozilla Firefox

File Edit View History Bookmarks Tools Help

eduVPN

https://demo.eduvpn.nl/admin/connections

Connections Users Info Stats Messages Log

eduVPN

Powered by SURF NET

Secure Internet

User ID	Name	IP address
d53f8e526186b75a06816999abc684631c91b7c3	globalpc	• 145.90.224.7 • 2001:610:450:10::1005
7f93e33a38a5289ee5a8d5d088c8c92a86cf46b5	lenovo	• 145.90.224.2 • 2001:610:450:10::1000
686904e3d1c3fdbcb879fb389e01f375aa945751	mac	• 145.90.224.36 • 2001:610:450:10::1022
d08076bdf67119eddad6477c9ce62afbbc521a06	PhoneJoe	• 145.90.224.143 • 2001:610:450:12::100d
e8c599b0c3c73614419cca8bc4fe5ae5f25045f9	T440s	• 145.90.224.210 • 2001:610:450:13::1010

eduVPN - Mozilla Firefox

File Edit View History Bookmarks Tools Help

eduVPN

https://demo.eduvpn.nl/admin/stats

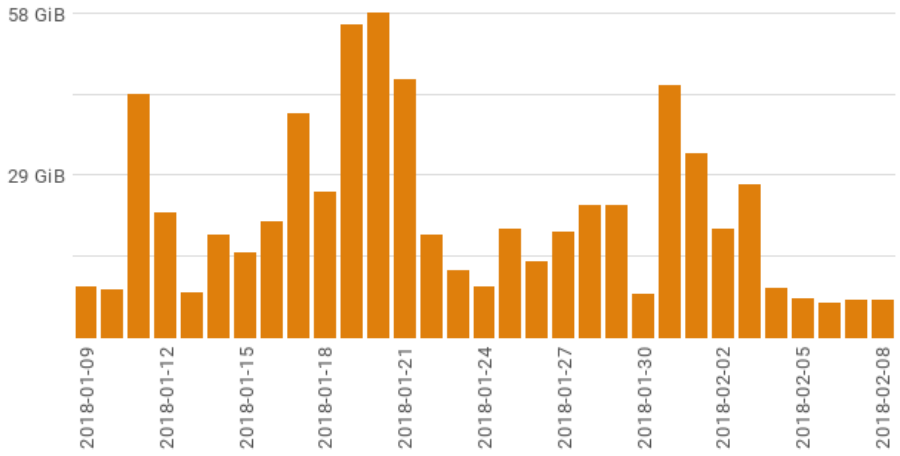
These statistics were last updated on 2018-02-08 23:00:01 (UTC) and cover the last month.

Profile	Total Traffic	Total # Unique Users	Highest # Concurrent Connections
Secure Internet	694.26 GiB	59	12

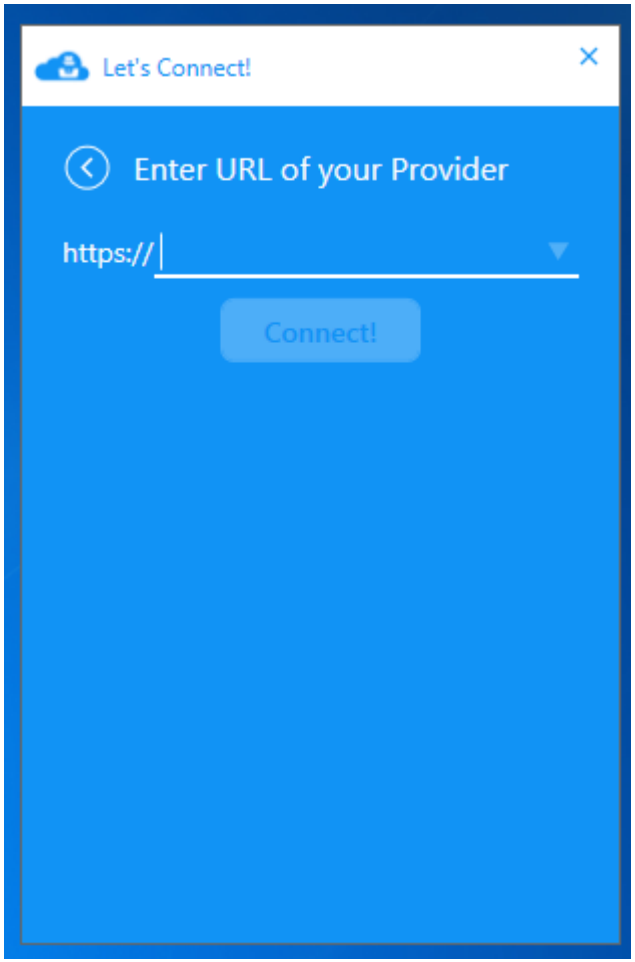
Traffic

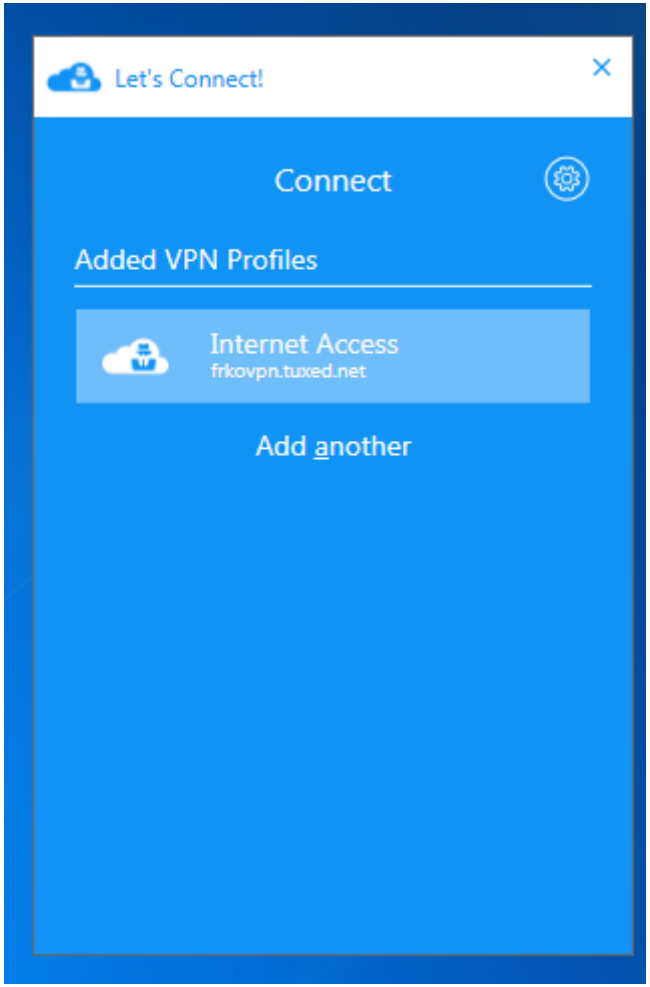
VPN traffic over the last month.

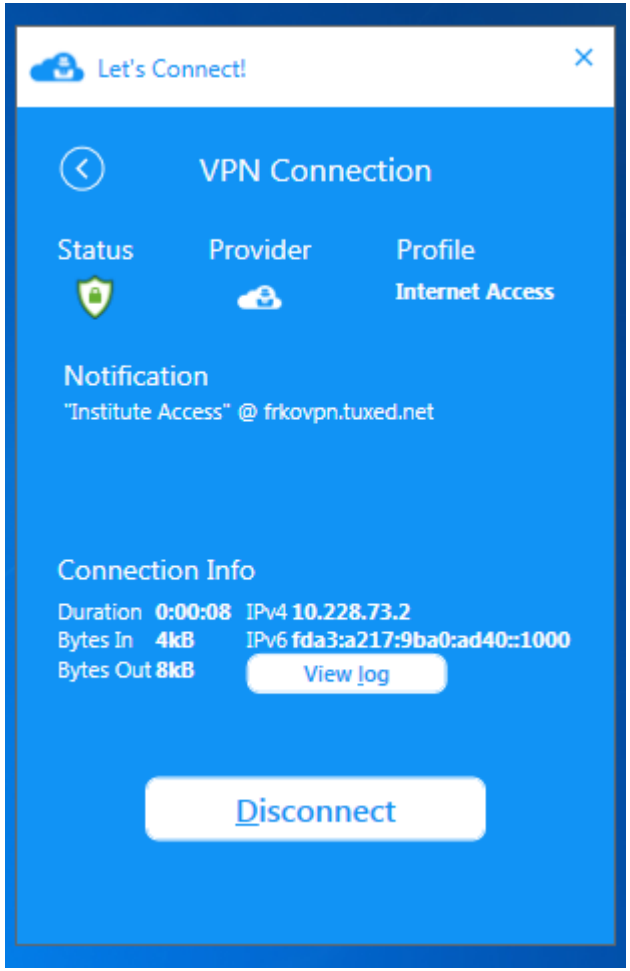
Secure Internet



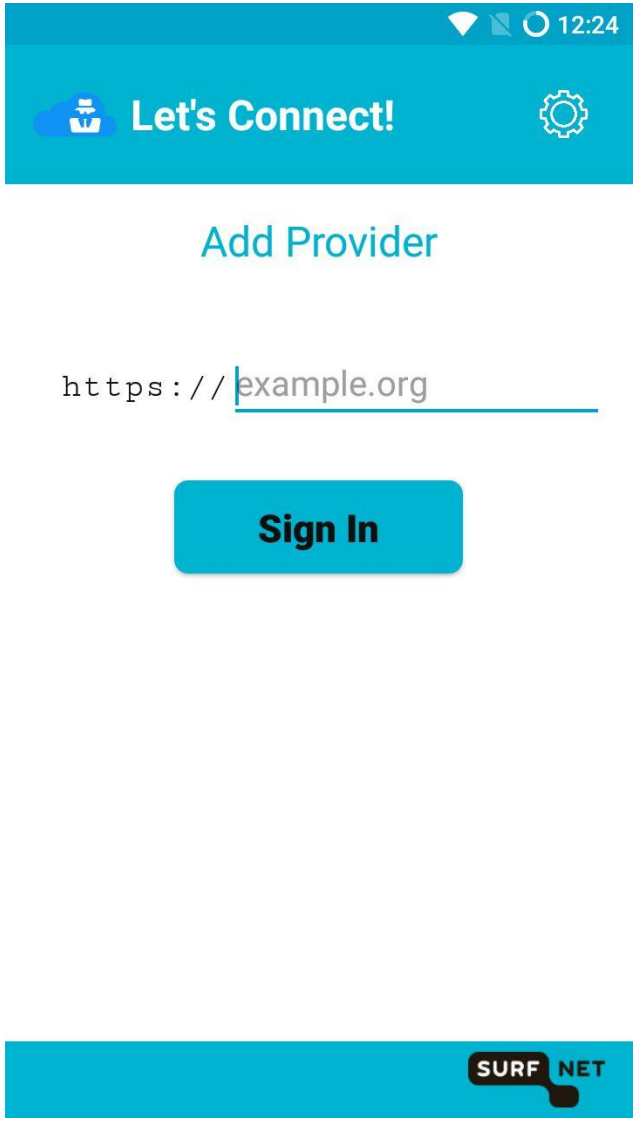
Let’s Connect! for Windows

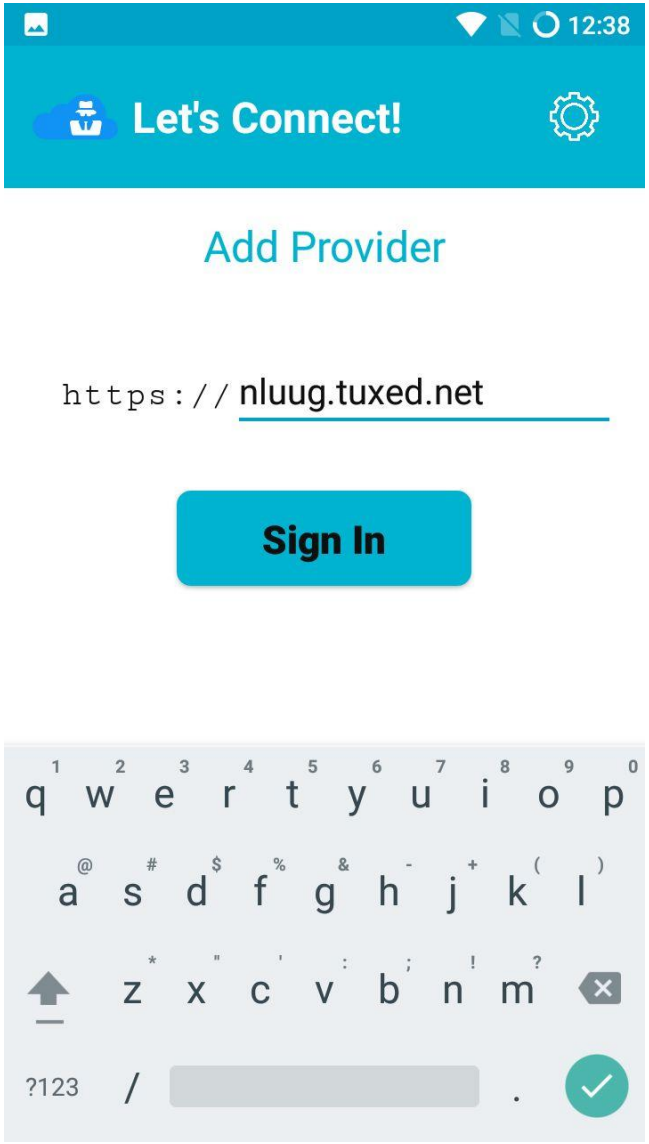


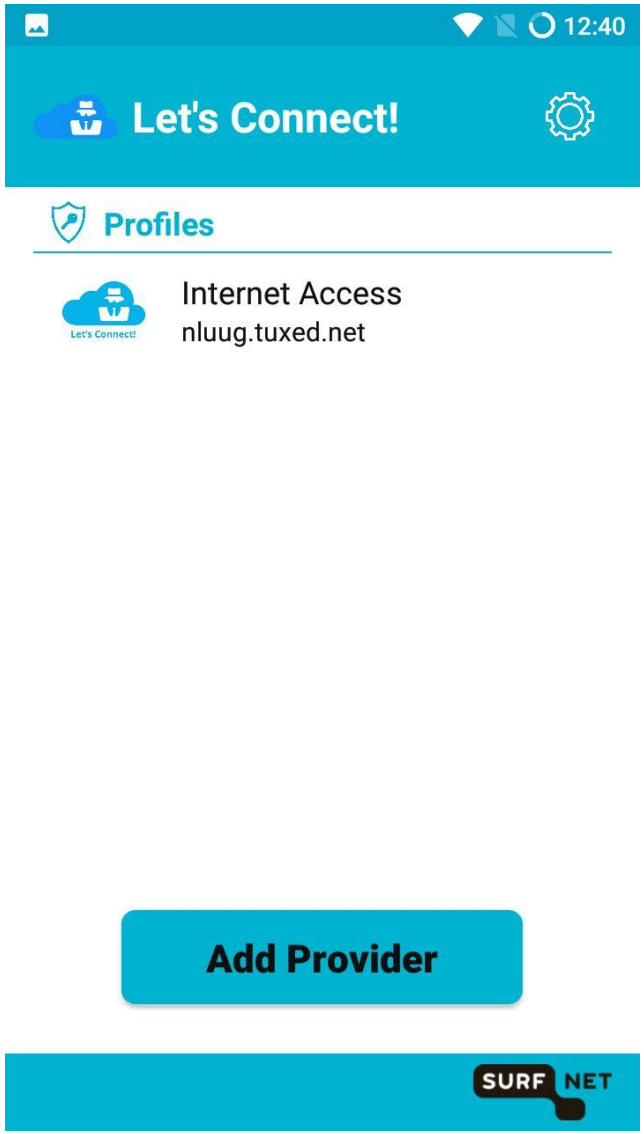


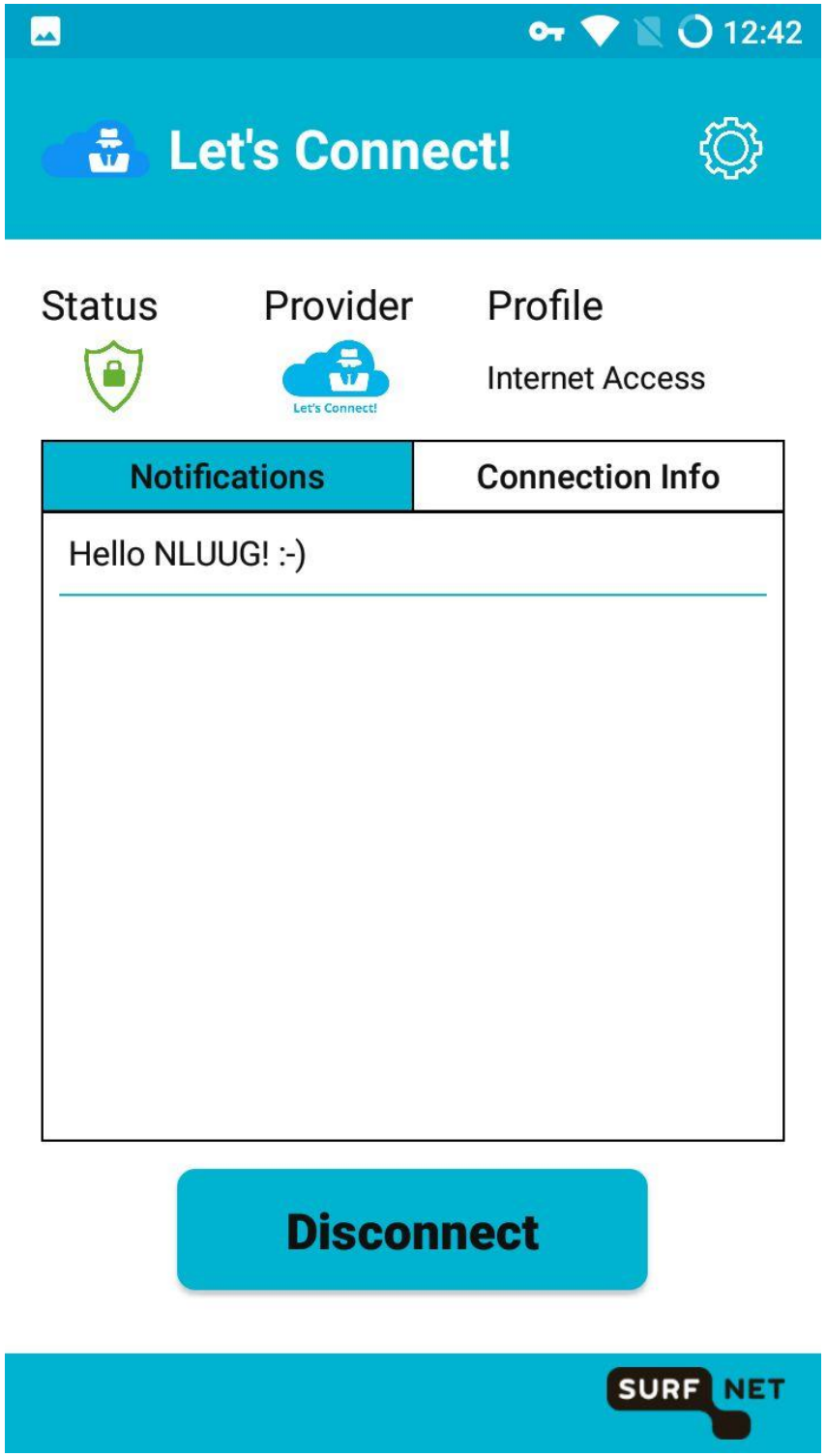


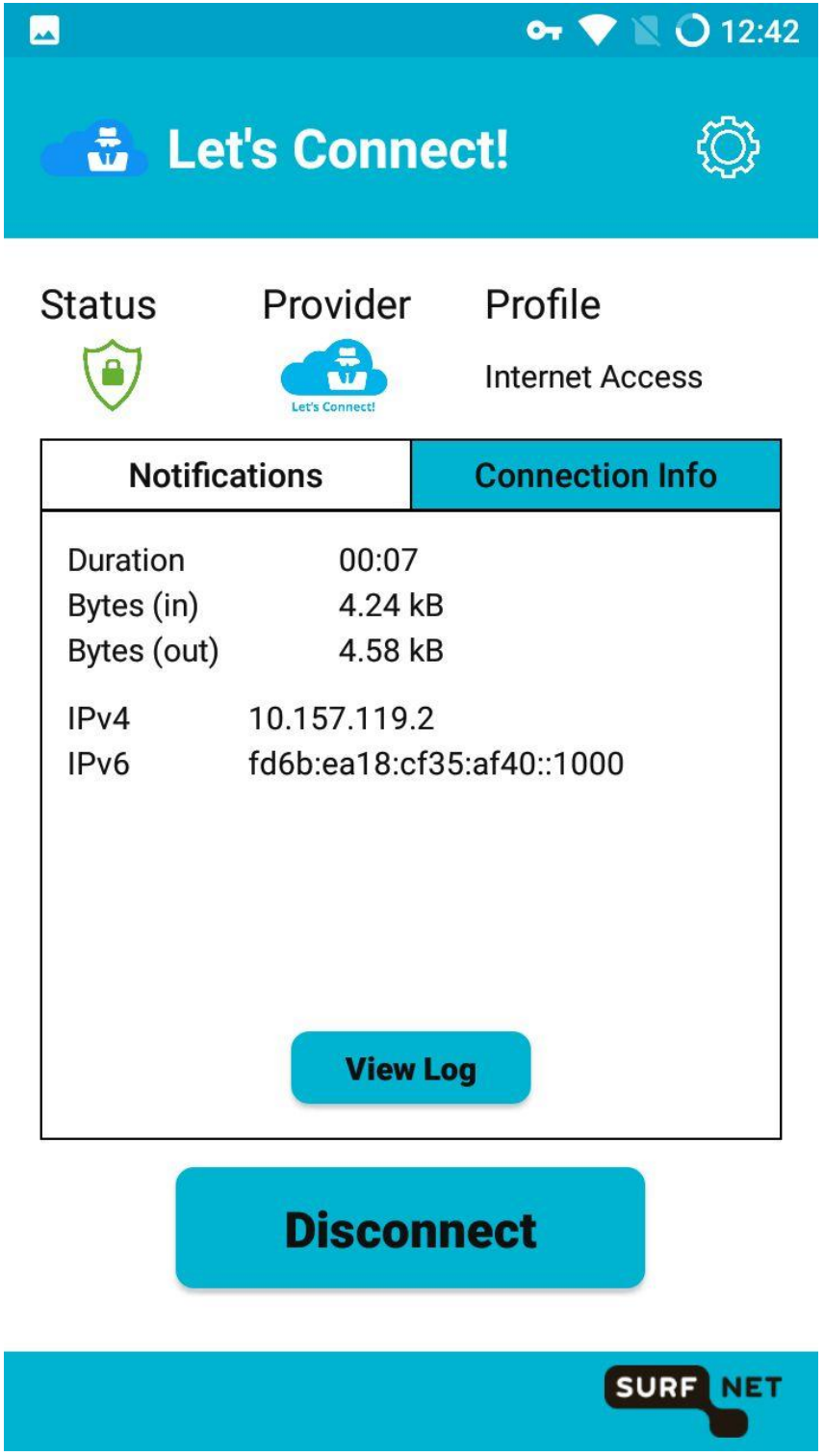
Let’s Connect! for Android








12:42
Let's Connect!
Status
Provider
Profile
Let's Connect!
Internet Access
Notifications
Connection Info
Hello NLUUG! :-)
Disconnect
SURF NET


12:42
Let's Connect!
Status
Provider
Profile
Let's Connect!
Internet Access
Notifications
Connection Info
Duration 00:07
Bytes (in) 4.24 kB
Bytes (out) 4.58 kB
IPv4 10.157.119.2
IPv6 fd6b:ea18:cf35:af40::1000
View Log
Disconnect
SURF NET

What

A **free software**, **easy to use** VPN service you can host **yourself**!

Let’s Connect!

- Project started 3.5 years ago as “eduVPN”
- Initially funded by SURFnet (NL)
- Now many (international) partners involved:
  - GÉANT, NORDUnet, Vietsch Foundation, DeiC, AARnet, RIPE Community Fund, SIDN Fonds, NLnet, Commons Conservancy
- Won ISOC “Internet Innovation Award 2018”!

Use Cases

- Protect against attackers on (insecure) WiFi networks
- Access (private) networks at your organization or at home

Who is this for?

- ISPs;
- Organizations with remote workers;
- Hacker spaces;
- Individuals
  - Cheaper than buying a commercial VPN subscription!
  - Easy to share with your friends!

Let’s Connect!

- FLOSS (Free/Libre Open Source Software)
  - AGPLv3+
- Easy to install on everything from €3/month VPS, Raspberry Pi to 128 core bare metal with 10+GBit network
- Runs on Debian >= 9, Red Hat Enterprise Linux/CentOS >= 7, Fedora >= 28
- Web interface for users and administrators
- Native Applications (also FLOSS)
- Privacy by Design & Default!
- Survived two source code security audits to date

Development

- **Don’t do:**
  - Containers / Docker / Kubernetes
  - “Cloud”
    - AWS, AMP, CloudFlare, CDNs, Travis-CI, Scrutinizer
  - SPA / JavaScript
  - Frameworks
  - Blockchain
    - **Never** do an ICO, FFS!
  - JWT/JWS

Audits

- 2017
  - Radically Open Security (ROS)
    - Server
- 2018
  - Radboud University, Nijmegen, The Netherlands
    - Server
  - NCC Group / Fox-IT
    - Windows Client

Privacy

- Does not log originating IP address (default)
- **Does** log VPN IP + connection time, removed after 30 days (default)
  - You can find a user identifier/pseudonym with an IP address and time of incident
  - Can block user without knowing the actual identity

Trust (I/II)

- You need to trust

1) Your device (laptop, smartphone)
2) WiFi network / ethernet
3) ISP
4) The service you are using

Trust (II/II)

- VPN helps if you don’t trust 2 and/or 3
  - ISP provides insecure crappy modem
  - ISP is recording metadata / monitoring everything, for fun and profit!
- Sometimes you trust 2 and/or 3 **more** than your VPN provider!
  - Too many stories of untrustworthy VPN providers...
- If you don’t trust 1 and/or 4, it is game over…
  - Your Android phone last received a security update in March 2015…
  - Tinder doesn’t use HTTPS for showing pictures, leaks “swiping” behavior
  - If you use Facebook or Google, oh well...

Technology

Technology

- OpenVPN
  - OpenVPN >= 2.4
  - Most secure configuration possible (with OpenVPN)
- OAuth 2.0 API
  - Bearer tokens with Public Key Cryptography (Federation!)

OpenVPN

- Why?
  - OpenVPN 2.x audited by multiple well known parties
  - Works over TCP/443 a.k.a. HTTPS port
  - Easy to setup
    - Turned out not so easy to set up *correctly*…
  - Available on many platforms/devices
  - Easy integration with ACLs, 2FA, …

OpenVPN

- Configuration “disasters”, uhhh, opportunities...
  - SELinux
    - Public cloud providers…
  - Network
  - (Adaptive) Compression
  - Verifying 2FA / ACL
  - MTU
  - iOS

OpenVPN

- Reduce opportunities to shoot yourself in the foot:
  - We want *unmodified* (official) OpenVPN **clients** as to work with Let’s Connect!
  - We want *unmodified* OpenVPN **server** as packaged by your server OS to work with Let’s Connect!
    - CentOS / RHEL / Fedora / Debian official OpenVPN >= 2.4 packages are used!

OpenVPN

- We want to use *normal* way of running OpenVPN on Linux
  - Use systemd for service init ☺
  - Work without hard dependency on any of the Let’s Connect! code
    - Except of course when 2FA/ACL is enabled, we need to verify it somehow!

OpenVPN

- Take care of generating
  - Server configuration
  - CA / certificates
  - Packet filter / NAT rules
- Let the OS take care of process management
  - KISS
  - This turns out to be very reliable!

Cryptography

- `AES-256-GCM`
  - hardware accelerated
- `TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384`
  - Mozilla TLS configuration guide
- TLS >= 1.2
- TLS Crypt

Network

- Full IPv6 support
  - In tunnel
  - Outside tunnel
  - Why do we still have to mention this in 2018? 😐
- (IPv6) NAT or Public IP addresses
  - NAT for IPv6 actually works really well… Oh my...

Scaling

- #OpenVPN processes ~= #CPU cores
  - Can quickly become very expensive…
  - AES-NI helps a lot
    - not for connection setup (RSA), but during active connections
- Maximum 64 clients per OpenVPN process
- Current biggest deployment:
  - 8 Profiles
  - ~ 4096 IP addresses (concurrent users)
  - 4096 / 64 = 64 OpenVPN processes
  - Start with 8 cores, can easily grow!

Authentication

- Authentication Backend:
  - SQL
    - SQLite (default)
    - Other SQL servers
  - LDAP
  - RADIUS
  - SAML
- Also supports 2FA (TOTP, YubiKey)
  - For both “portal” access and VPN connections

Authorization / Group Management

- “ACL” on VPN usage
- Only allow members of certain (LDAP) group to access certain VPN profiles

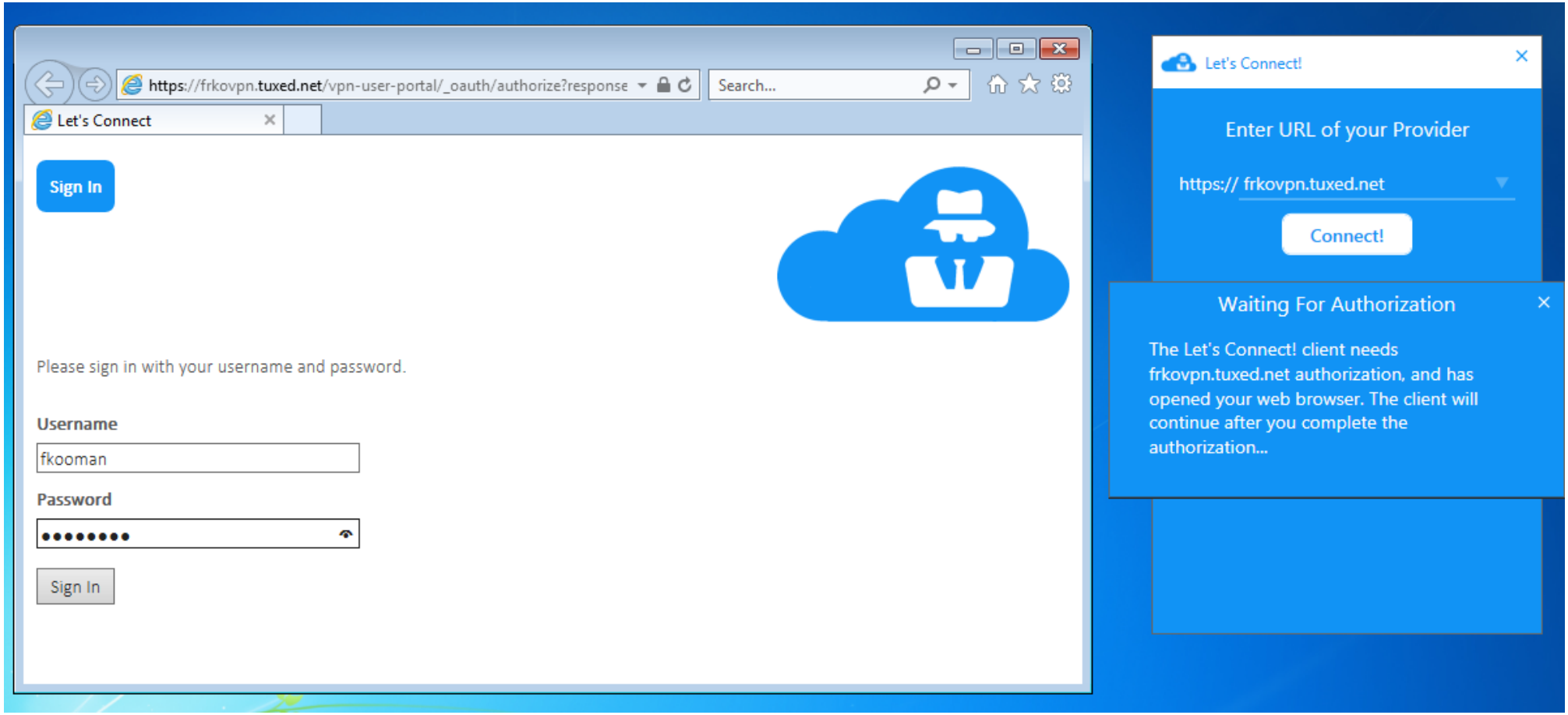
Application Integration

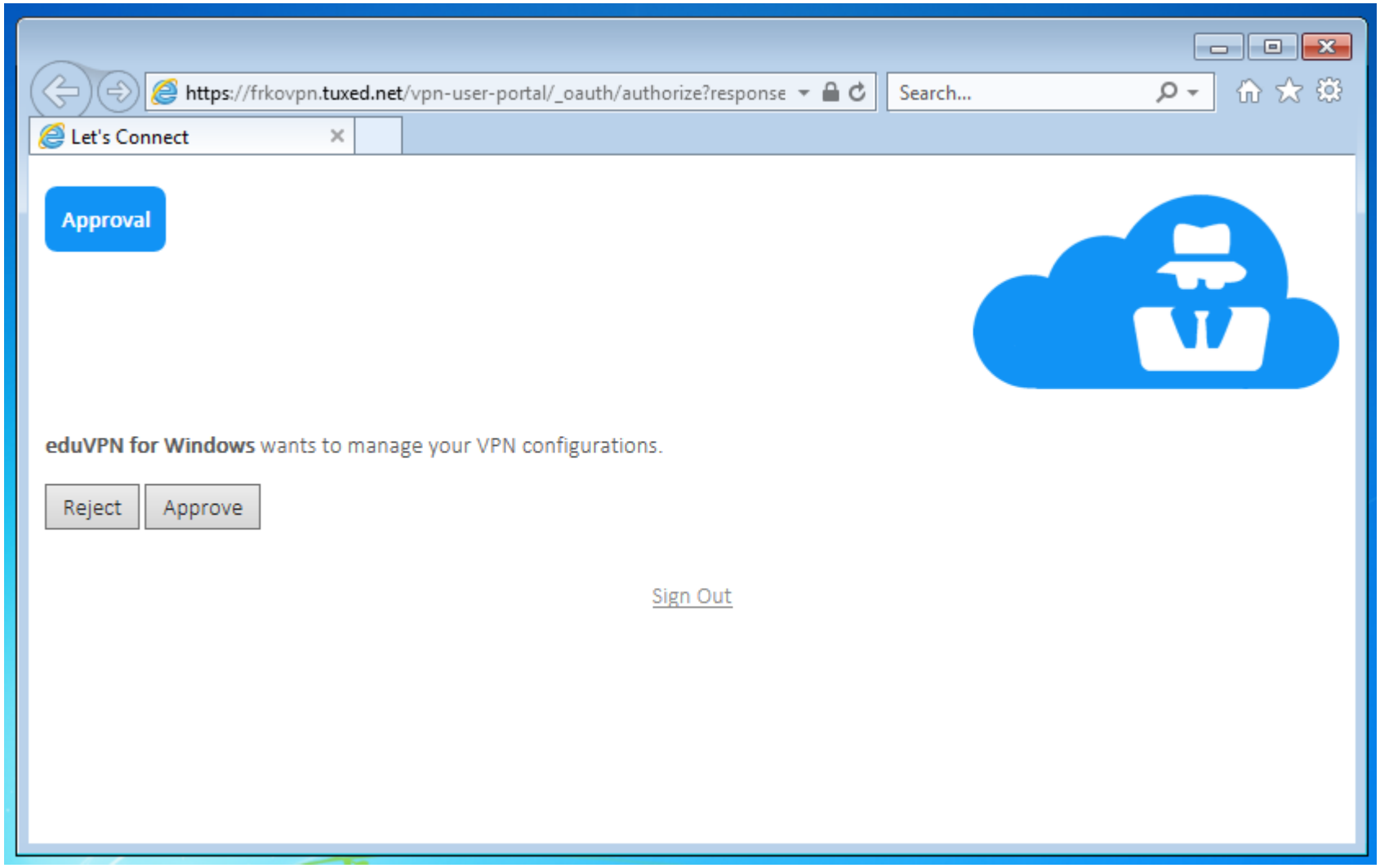
OAuth

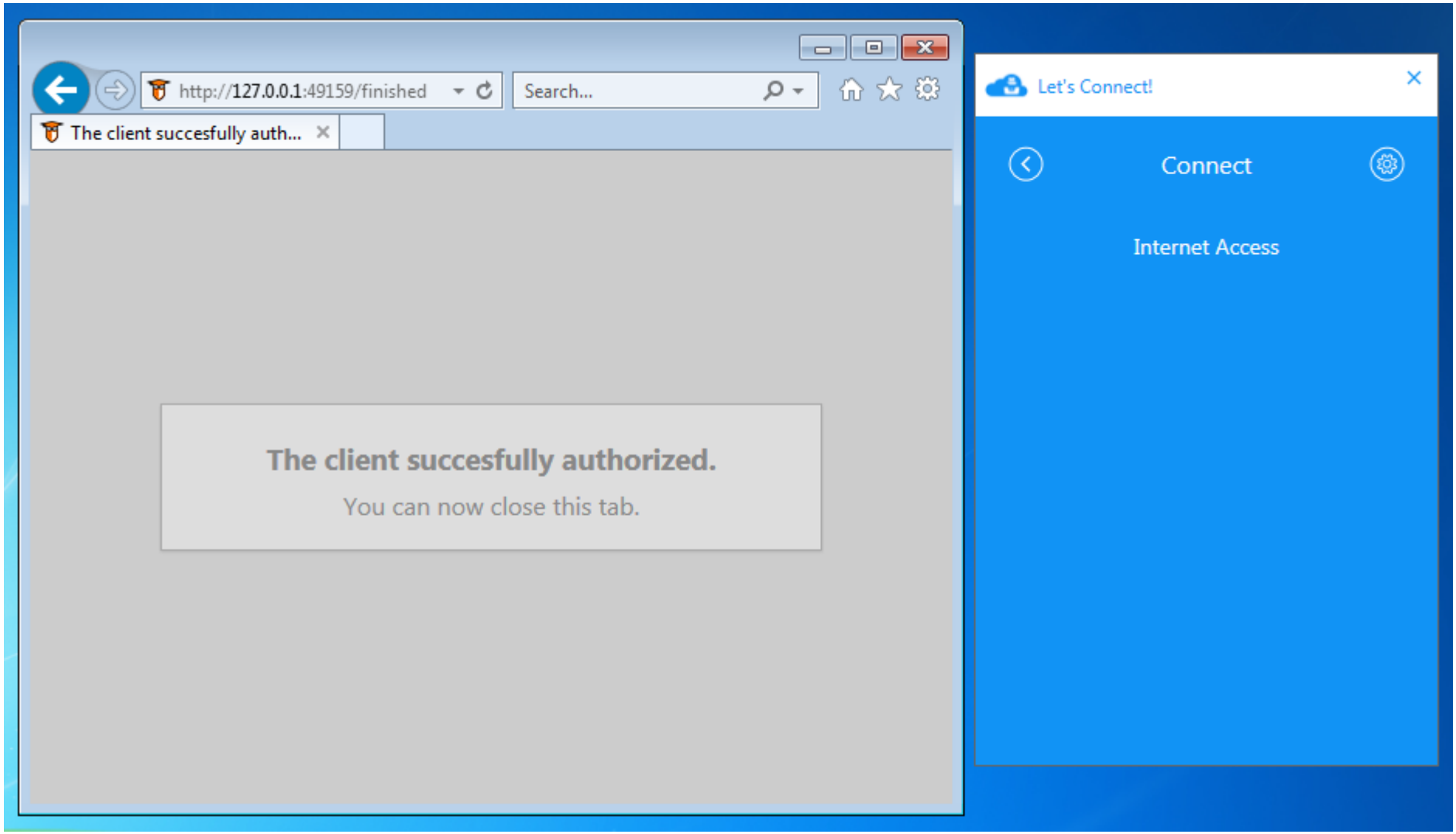
- Protocol (framework) to **authorize** (native) applications to act on your behalf

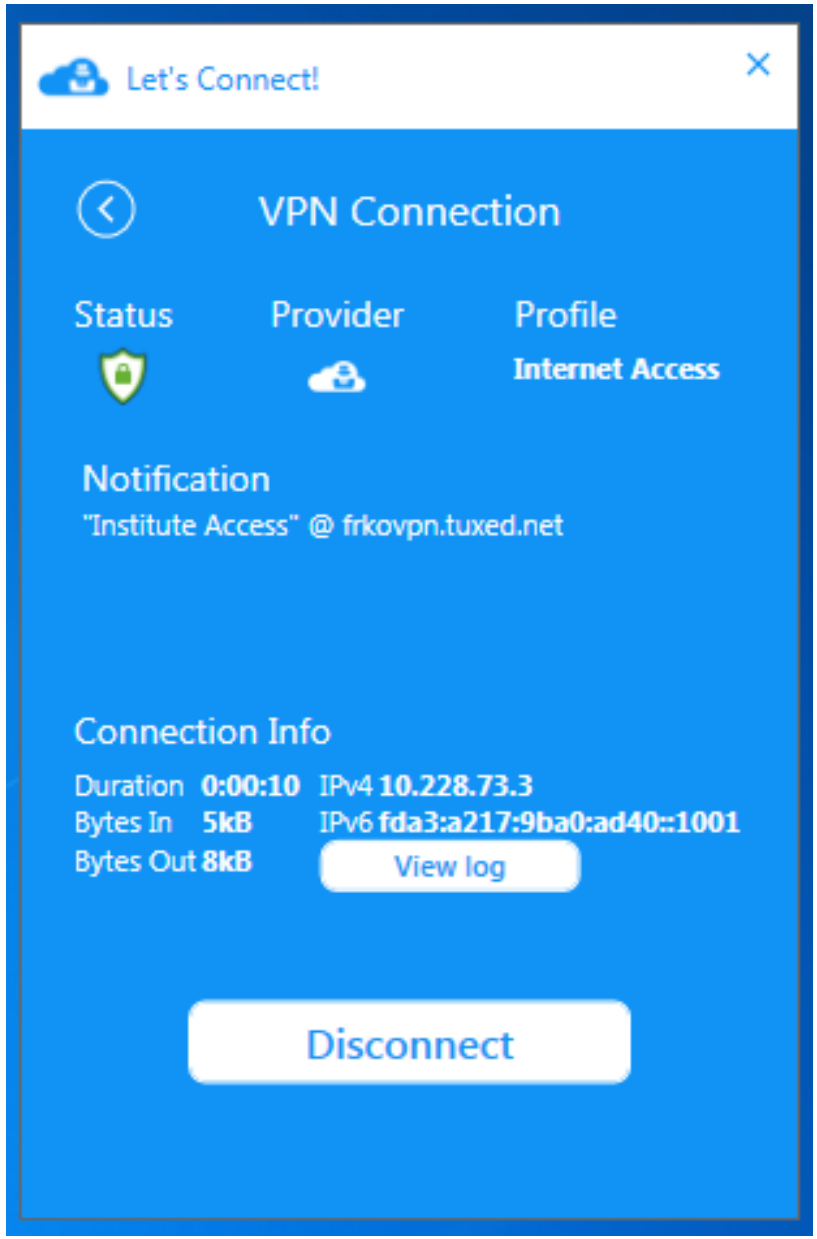
OAuth

1) *Client* opens browser with URL of *authorization server* (AS)
2) AS makes sure user is **authenticated**, and then prompt for **authorization**
3) Browser redirects back to client
   - Special URL scheme, “localhost”, claimed HTTPS URL
4) Client exchanges authorization code for access token
5) Client uses access token to talk to API


https://frkovpn.tuxed.net/vpn-user-portal/_oauth/authorize?response
Search...
Let's Connect
Sign In
Please sign in with your username and password.
Username
fkooman
Password
Sign In
Let's Connect!
Enter URL of your Provider
https:// frkovpn.tuxed.net
Connect!
Waiting For Authorization
The Let's Connect! client needs frkovpn.tuxed.net authorization, and has opened your web browser. The client will continue after you complete the authorization...


https://frkovpn.tuxed.net/vpn-user-portal/_oauth/authorize?response
Search...
Let's Connect
Approval
eduVPN for Windows wants to manage your VPN configurations.
Reject
Approve
Sign Out


http://127.0.0.1:49159/finished
Search...
The client succesfully auth...
The client succesfully authorized.
You can now close this tab.
Let's Connect!
Connect
Internet Access


Let's Connect!
VPN Connection
Status
Provider
Profile
Internet Access
Notification
"Institute Access" @ frkovpn.tuxed.net
Connection Info
Duration 0:00:10
Bytes In 5kB
Bytes Out 8kB
IPv4 10.228.73.3
IPv6 fda3:a217:9ba0:ad40::1001
View log
Disconnect

Distributed Operation

- Allow establishing **trust** between multiple Let’s Connect! deployments

Why?

- “Load balancing”
- Sharing costs for creating a distributed VPN provider network
- Route around “errors” on the network when reaching certain destinations
- Leveraging existing “trust” networks, e.g. Hacker spaces/communities to create a trusted VPN provider network
- Allow users choice of VPN server to use (latency, jurisdiction, ...)

How?

- Leverage OAuth 2.0 Bearer tokens used for Native Application integration
- Public Key Signatures over Bearer tokens

Future

- Use ECC (without CA, patches for OpenVPN exist)
- Look into using WireGuard as a replacement for OpenVPN (simplicity, efficiency, licensing?)
- High(er) level implementation OpenVPN for all platforms (using native VPN APIs)
- Get first-class Debian packages…
- Setup a (distributed) not for profit “friends of friends” VPN service with Let’s Connect as testing ground?

Test Let’s Connect! Yourself

- Use your own OpenVPN client
  - Manually download configuration https://nluug.tuxed.net/ and use your own OpenVPN client, see “Documentation” after authenticating for instructions
- Use Let’s Connect! App
  - Windows: https://letsconnect-vpn.org/apps/
  - Android:
    - https://app.eduvpn.org/android/ (`LetsConnect-1.2.2-0.dev.apk`)
    - Or use “eduVPN” app with “Add other provider” from Google Play store
  - macOS, iOS: expected later this month
- Authentication
  - Username: `nluug`
  - Password: `nluug2018`
  - **Please don’t change password or enable 2FA!**

Questions / Discussion

https://letsconnect-vpn.org/

François Kooman
<fkooman@tuxed.net>
@fkooman