eduVPN Roadmap

TNC19 – Forging Digital Societies

Release Schedule

- **eduVPN 3.0**: Q4 2019?

Application Redesign

- Current eduVPN applications require users to know the difference between *Secure Internet* and *Institute Access* and know their “home country”, for some definition of “home”...

Application Redesign

- What if...we follow the flow of other (federated) services:
  - Choose your IdP
  - Select a VPN server you want to connect to (and that is actually available for you)

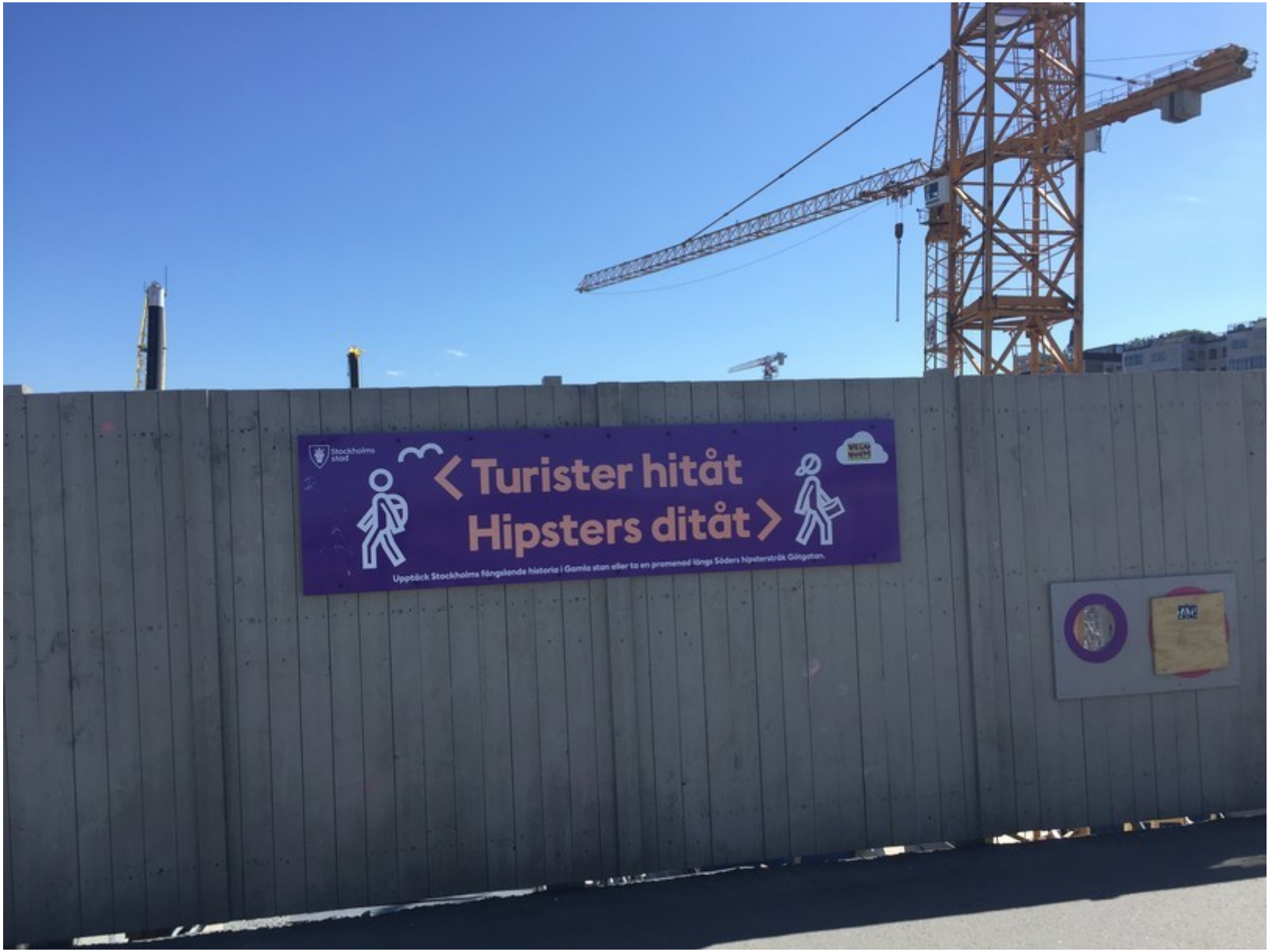
API

Currently the API has too many different calls, reduce this to three calls:

- **Info** (to retrieving server/profile information)
- **Pre-connect** (to see if the connection would be allowed and set up some server state when needed)
- **Post-disconnect** (clean up after the client, when needed)

As a bonus this would also make it VPN-implementation independent...

#road2tnc


Stockholms stad
Turister hitåt
Hipsters ditåt
Upptäck Stockholms fängslande historia i Gamla stan eller ta en promenad längs Söders hipstervräk Götgatan.

Server Development

Make things simpler

- Remove application code
- Remove dependencies
- Remove #required steps to set up a server

Goal

- Work towards (official) inclusion in GNU/Linux, *BSD distributions

Guest User Privacy

Now

- Currently the user identifier of the user at server X is provided verbatim to server Y

Later

- Generate a pseudonym for the user and use that as guest identifier

SAML...

Currently **three** SAML implementation are supported:

- mod_auth_mellon
- Shibboleth
- php-saml-sp

And even more desired/requested:

- simpleSAMLphp

...this is obviously crazy...

SAML...

php-saml-sp was meant to replace them all...

- Keep it simple...
- Focus on only implementing *secure* algorithms, not the kitchen sink...

SAML...

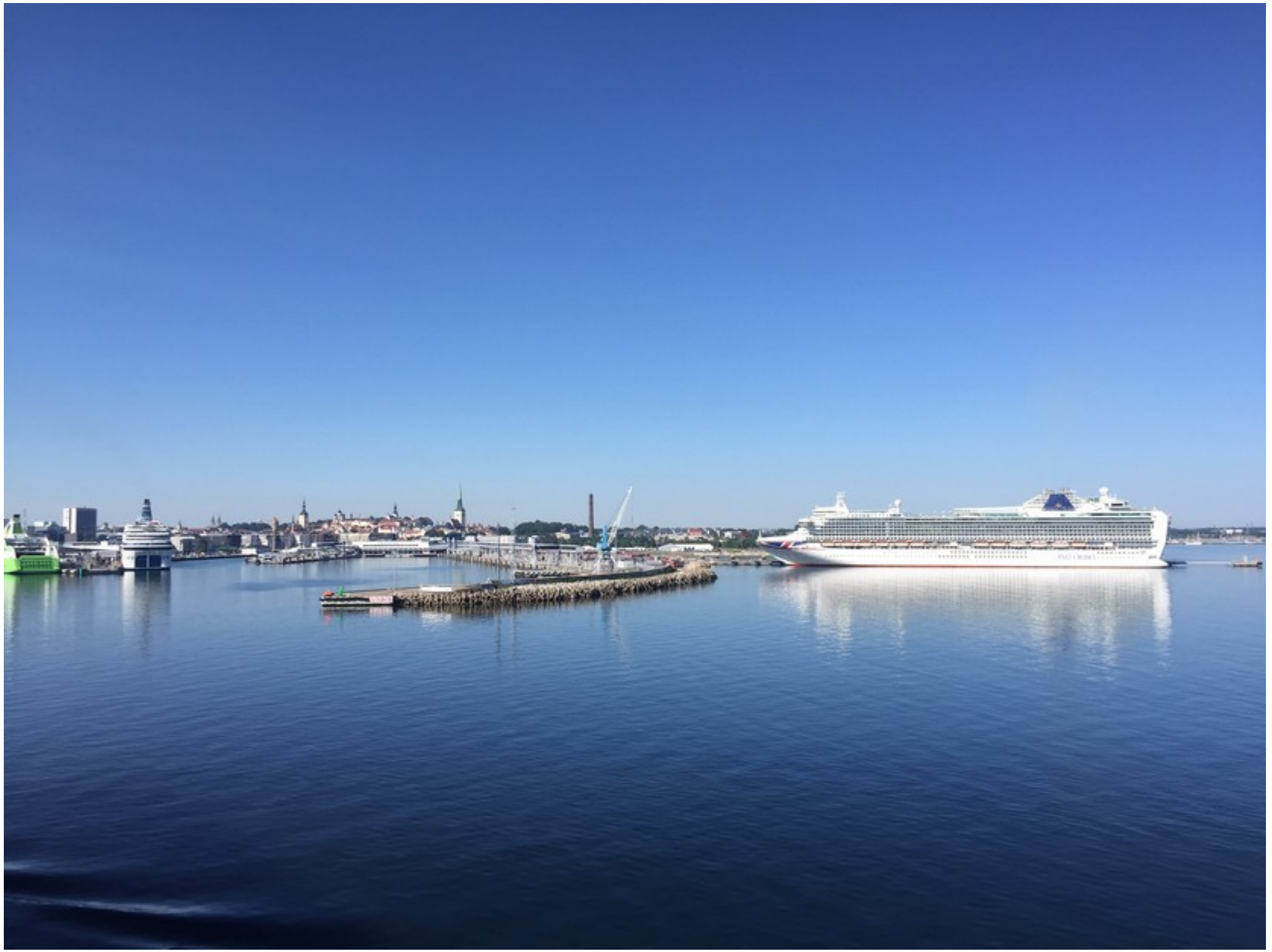
But enter mesh federations...

- Many IdPs use legacy insecure crypto by default...
  - AES-CBC for EncryptedAssertion
  - *How* is SHA1 still a thing?
- Not always a way to force them to use something from after the year 2000 unless the IdP admin manually fixes this...
  - This is all solved by various SAML specifications, but well...

Drop Firewall

- The firewall should really not be part of eduVPN!
  - Filter in switch and/or router!
- Every attempt at automating firewall generation ends up closer to a full firewall management tool...
  - The only winning move is not to play!
- A very simple (NAT) static firewall example will be provided and installed by the “deploy_${DIST}.sh” scripts...

#boat2tnc



OS Support

Only support “modern” OS in eduVPN 3.0

- CentOS 8
  - Expected Release: next month(s)?
  - Red Hat Enterprise Linux 8 was released on 2019-05-07
- Debian 10
  - Expected Release: 2019-07-06

Apply Changes...

At the moment applying configuration changes takes a number of steps...

- We'll create a one-step "apply" command that takes care of everything:
  - Apply configuration changes
  - Restart/enable on boot (required) VPN processes

Configuration

Allow running with (almost) empty configuration file

- Have sane and usable defaults that work for the most common scenario(s)
- Only configure what you need…

Also… don’t have tools modify (and rewrite) configuration files…that was a terrible idea! Don’t touch the admin’s files!

Questions / Remarks?

- Follow us on Twitter: **@eduvpn_org**
- The Web: https://www.eduvpn.org/
  - **With regularly updated blog!**
- Mail: eduvpn-support@lists.geant.org