Why?

- Policy 1.0 is not as concrete as it could be!
  - Modeled on eduroam policy
  - ...and some elements from Security Incident Response Trust Framework for Federated Identity (Sirtfi)
  - Sometimes (too) vague
- Some stuff is missing...
What’s New?

- Clear separation between “Institute Access” and “Secure Internet”
- (Exhaustive) list of requirements when running the server(s)
- Make many things (more) explicit...
- *Only* relevant if you want to be in the eduVPN apps
Institute Access

• Very few requirements, most is up to the organization(s) running it to decide!
• ...but, security updates MUST be installed periodically (once a week)
• ...be a member of the eduvpn-deploy@ mailing list...
  - ... the person responsible for the eduVPN server MUST read the mails and act on them when required... If not clear, ask!
Secure Internet

- `#include “Institute Access”`
- MUST use `eduPersonTargetedID` or Pairwise Subject ID
- MUST provide IPv4 and IPv6 connectivity to clients
- MUST use public IP addresses
- MUST provide documentation on which (if any) traffic is restricted, and for what purpose
- MUST allow connections over at least UDP/443 and TCP/443
Public IP Addresses

• Yeah we know...
• ...but if you don’t do this...
  – ... you take on the burden of keeping a NAT log to be able to respond to abuse complaint(s)
• Many NRENs have lots of (spare) IPv4 addresses... maybe ask other NRENs to transfer some for the purpose of eduVPN if you ran out? :-)

6 / 8
Abuse

- We finally had an abuse complaint for a Dutch user using the Dutch eduVPN server
- ...we used the “Log” in the eduVPN admin panel to figure out the user identifier...
- ...as it was a “pseudonym” we only knew the originating organization...
- ...referred the complaint to the originating organization to have them deal with it...
- ...we never knew (or had to know) the identity of the user involved!
Questions?

- Contact
  - eduvpn-support@lists.geant.org
- Twitter
  - https://twitter.com/eduvpn_org
- Web
  - https://www.eduvpn.org/