OpenVPN for eduVPN

François Kooman

<fkooman@tuxed.net>

@fkooman

OpenVPN-nl

- Uses /dev/random and not /dev/urandom?
- Minimal system uptime first;
- PRNG fiddling (entropy size);
- **tls-cipher**:
  - TLS-DHE-RSA-WITH-AES-256-GCM-SHA384
  - TLS-DHE-RSA-WITH-AES-256-CBC-SHA256
  - TLS-DHE-RSA-WITH-AES-256-CBC-SHA
- **cipher**: AES-256-CBC
- **auth**: SHA256
- **prng**: SHA256

eduVPN 1.0 (OpenVPN 2.4)

- OpenVPN >= 2.3 clients;
- **tls-cipher**:
  - TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384 (OpenSSL 1.0.1+, or PolarSSL 1.3+)
- **auth**: SHA256
- **cipher**: AES-256-CBC
  - OpenVPN 2.4 clients will use AES-256-GCM (via NCP)
- Other:
  - **tls-auth**
  - **tls-version-min**: 1.2
  - **dh**: none (enforces ECDHE)

eduVPN 2.0 (OpenVPN 2.4)

- OpenVPN >= 2.4 clients;
- Use EC for CA as well?
  - Probably not...
- **tls-cipher**:
  - TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384 (OpenSSL 1.0.1+, or PolarSSL 1.3+)
  - TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384 (?)
- **cipher**: AES-256-GCM only (disable NCP?)
- **auth**: SHA256 (SHA384?)
- Other:
  - **tls-crypt** (instead of **tls-auth**, breaks existing client configurations, and does not yet work on OpenVPN Connect (iOS/Android), NetworkManager)