OPENVPN™

Simple, Secure and Flexible VPN solution for home and business

11es Rencontres Mondiales du Logiciel Libre
Du 6 au 11 juillet 2010

me

- Romain Bourgue
  - IT Security and open source fan
  - Works for the french Civil Service since 2003
  - romain.bourgue@gmail.com

Summary

- VPN solutions : multiple choices for multiple situations
- OpenVPN
- « Once upon a time... » - Few tales and demos featuring OpenVPN
- Want more ? Need help ?

Summary

- **VPN solutions : multiple choices for multiple situations**
  - Quick reminder about secure VPN
  - IPsec based solutions
  - SSL based solutions
  - Commercial fake SSL “*VPN*“
- OpenVPN
- « Once upon a time... » - Few tales and demos featuring OpenVPN
- Want more ? Need help ?

VPN solutions overview
Quick reminder about secure VPNs

- Main objective :
  - securely encapsulates data between 2 or more networked devices not on the same private network.
- Responsible for :
  - Authenticate (both ways)
  - Insure data integrity
  - Encrypt/Decrypt
  - Encapsulate/”decapsulate”
- Lots of solutions, very few compatibilty

VPN Solutions
Ipsec based solutions

- IPSec pros :
  - Widely supported
  - Interoperability is achievable for lan-to-lan connectivity
- IPsec cons :
  - Specific protocols AH, ESP
  - No automatic negotiation
  - Difficult to open in firewalls
  - Bad NAT support
  - IPsec in itself is not enough for VPN roadwarriors : Needs specific implementations

VPN Solutions
Ipsec based solutions

- Specific Implementations
  - Vendor specific implementation for endusers : Cisco VPN Client, Checkpoint Secure Client, Juniper IPSec Client...
  - MS PPP/L2TP/IPsec : natively supported in Windows OS and devices

- Still good for : **LAN-to-LAN in heterogeneous situations**

VPN Solutions SSL/TLS based VPN

- Uses SSL/TLS security for authentication, key negociation and session renegociation
- Data encapsulation is still specific.
- Implementations
  - *Clientless* : ActiveX or Java applet based SSL/TLS VPN (transport through loopback listening sockets)
  - Client based commercial solution : Cisco, Juniper, Connectra
  - Openssh, Openvpn
- Good for : Securing endusers connection (roadwarriors, wifi, admin networks...)

VPN Solution
Commercial fake SSL VPN

- Commercially called SSL VPN... they are just https servers with :
  - Reverse proxy to serve internal web ressources
  - Web interfaces to add functionnality : VNC/RDP for remote administration, WebMail, Web access to windows shares...

Summary

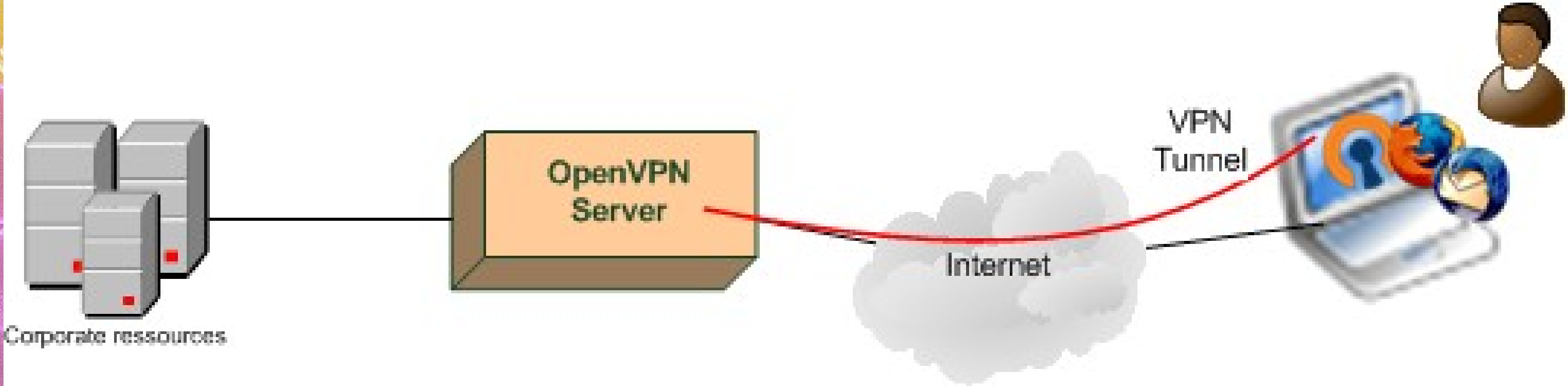
- VPN solutions : multiple choices for multiple situations
- **OpenVPN**
  - Quick facts
  - In-depth presentation
  - Few more things
  - Performances
  - Configuration basis
  - Plugability & Hooks for fun and creativity
- « Once upon a time... » - Few tales and demos featuring OpenVPN
- Want more ? Need help ?

Open VPN
Quick facts

- Created for personal use by James Yonan
- Dual license :
  - Community edition : GPL v2
  - Commercial edition. Adds a distribution server and Client and Management GUI
- Version history
  - May 2001 : v0.9 first release
  - ....
  - Dec 2009 : v2.1.1
- Roadmap for v3.0 : Become a generic network stack with modules for everything...
- Available in : Linux, Solaris, *BSD, Windows (XP to 7 and Mobile), MAC OS, Android, Iphone...

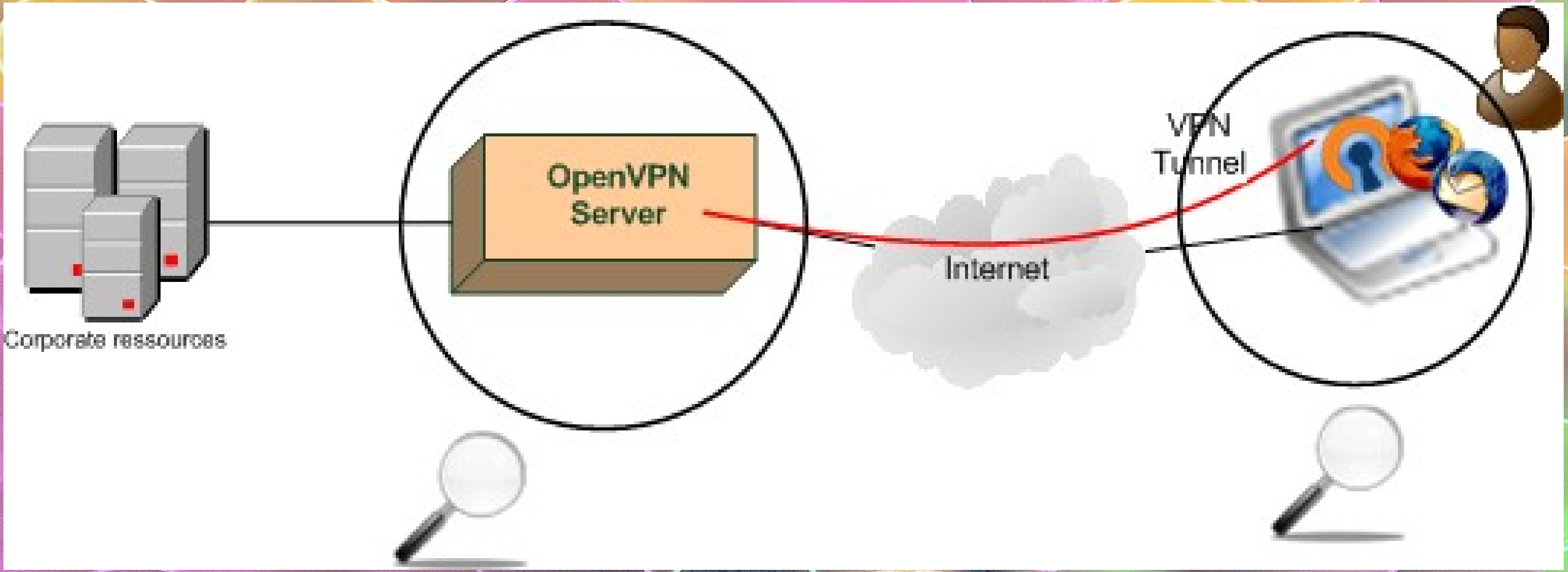
OpenVPN in-depth Architecture

- Case study : simple VPN connection

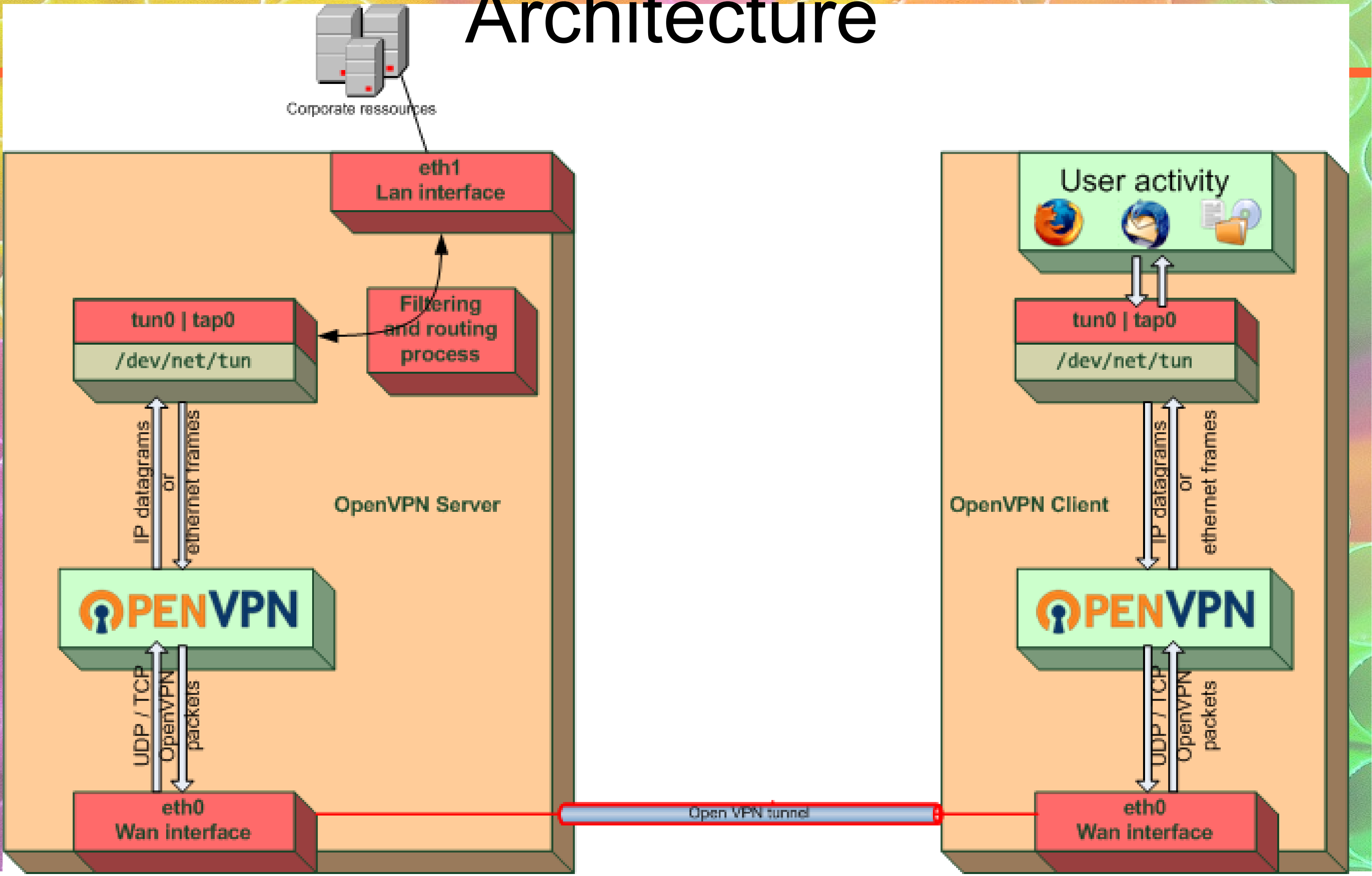


OpenVPN in-depth Architecture

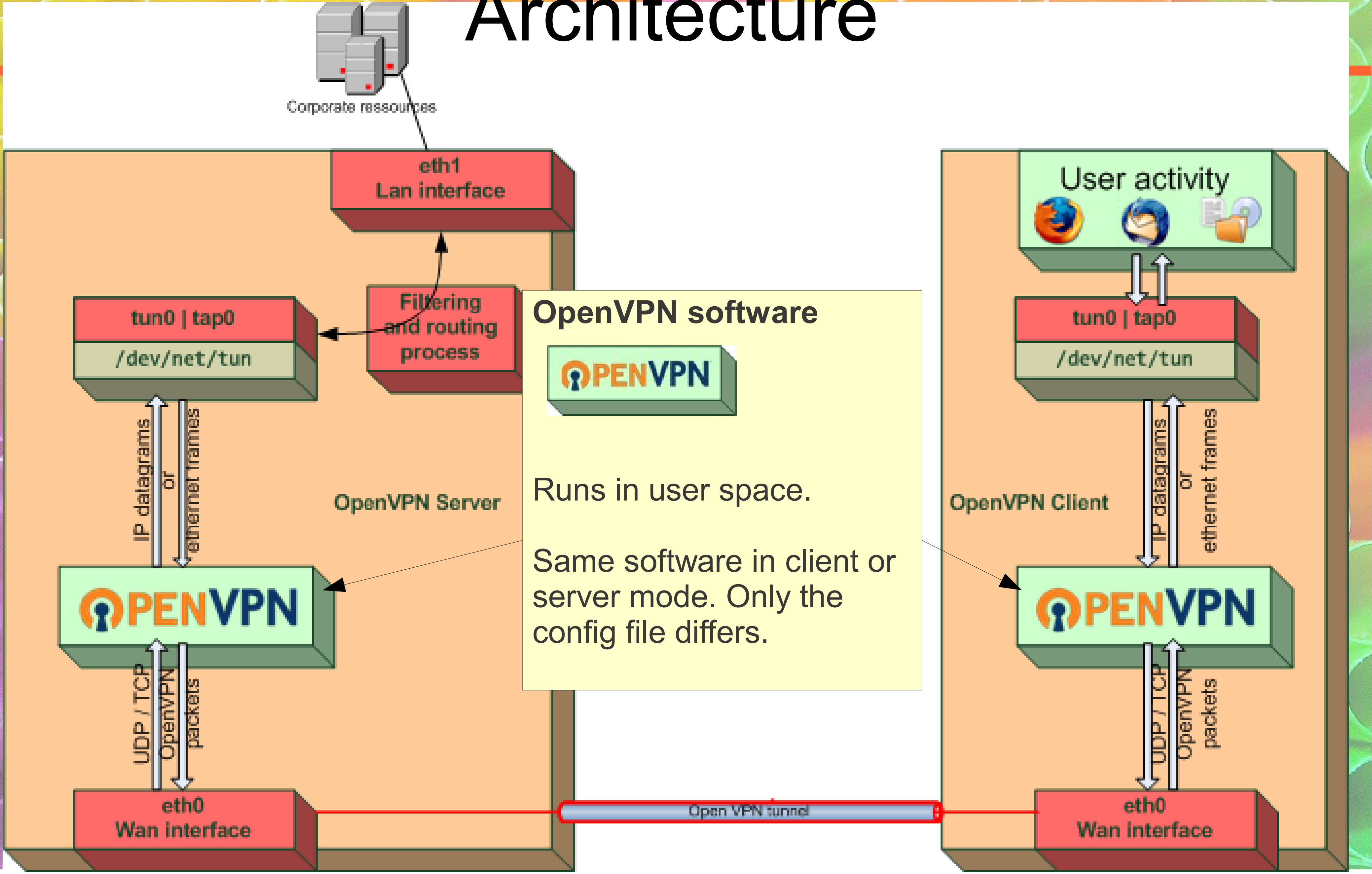
- Case study : simple VPN connection



OpenVPN in-depth Architecture



OpenVPN in-depth Architecture

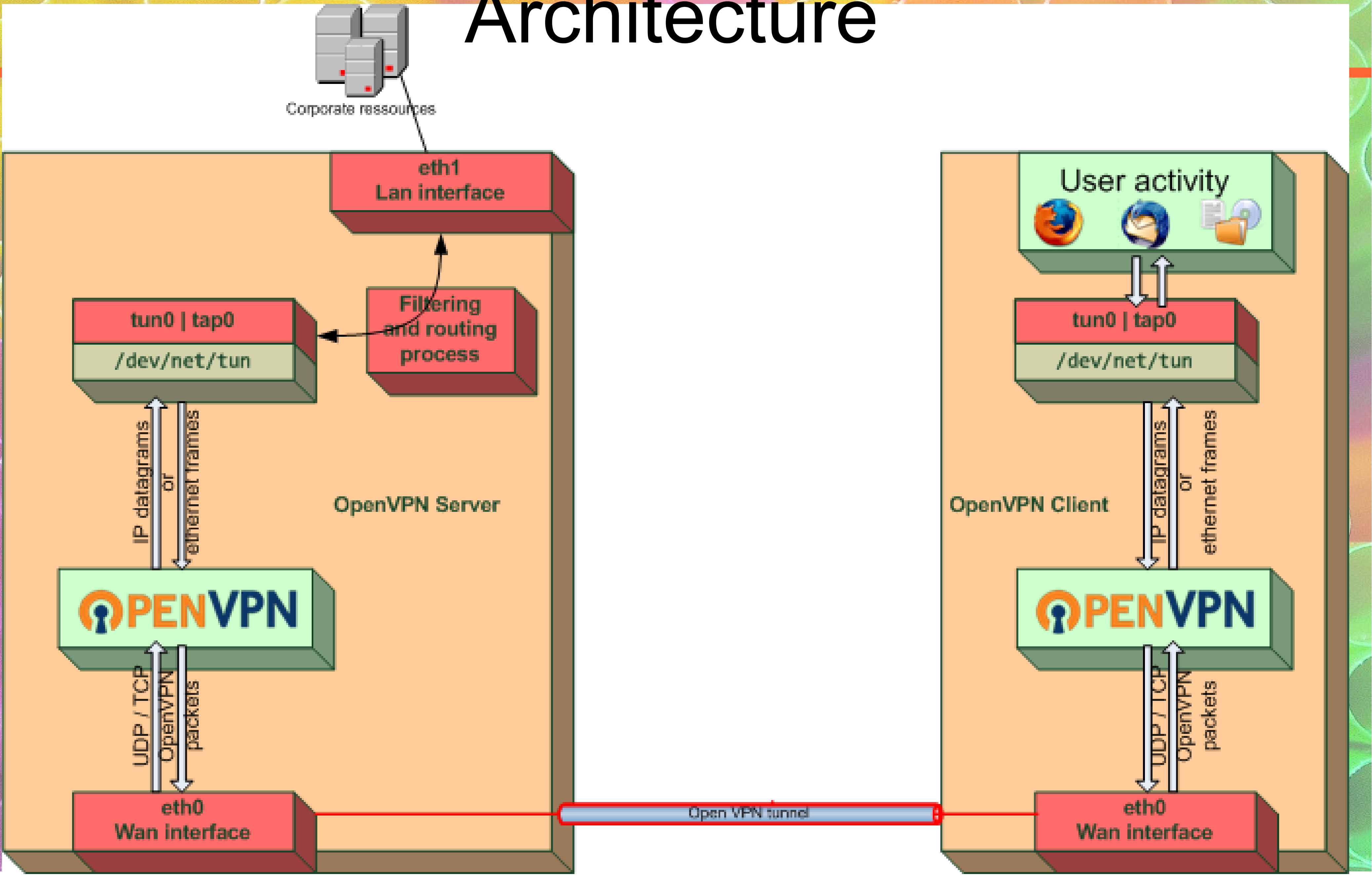


OpenVPN software

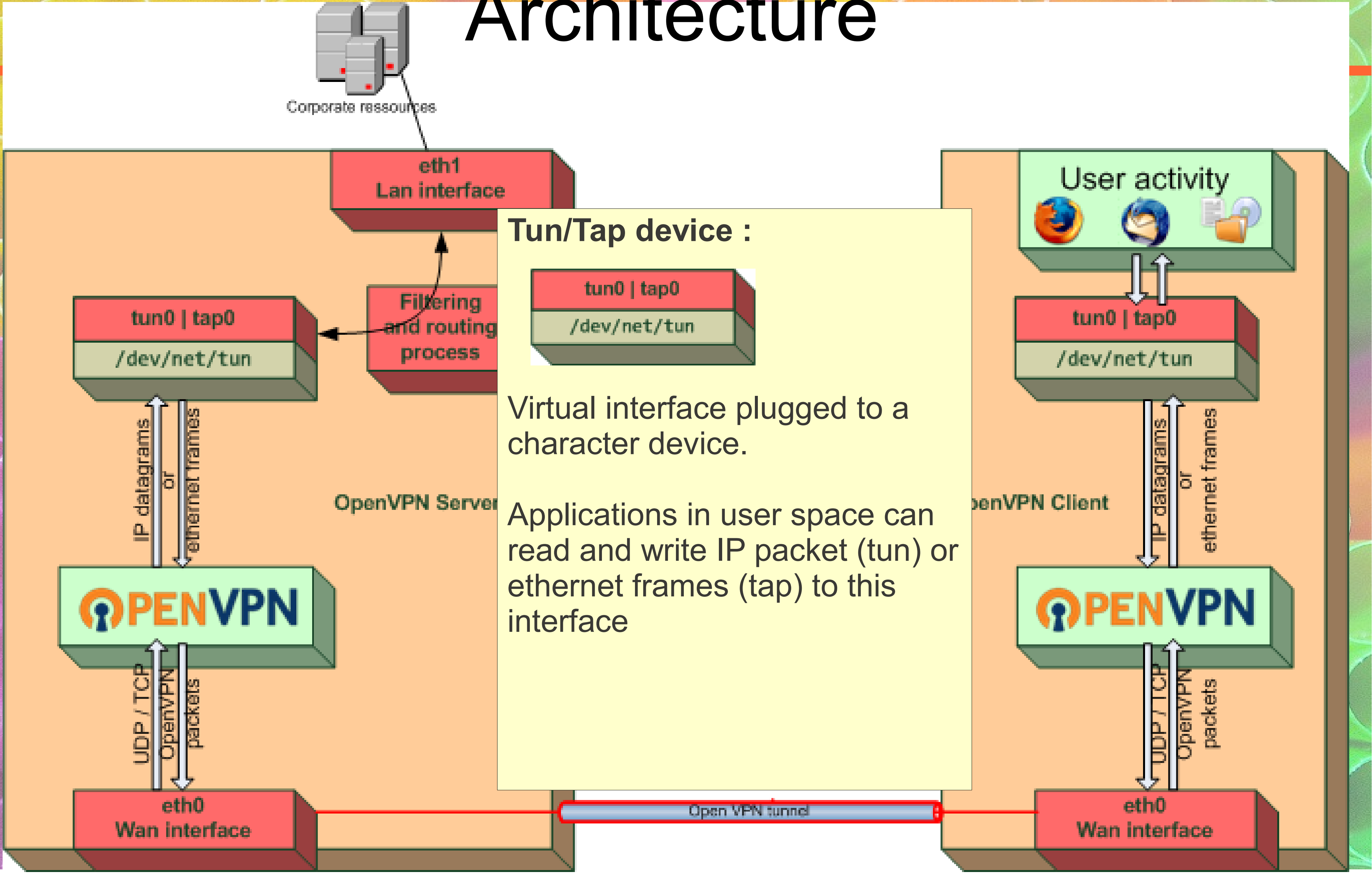
Runs in user space.

Same software in client or server mode. Only the config file differs.

OpenVPN in-depth Architecture



OpenVPN in-depth Architecture



Tun/Tap device :

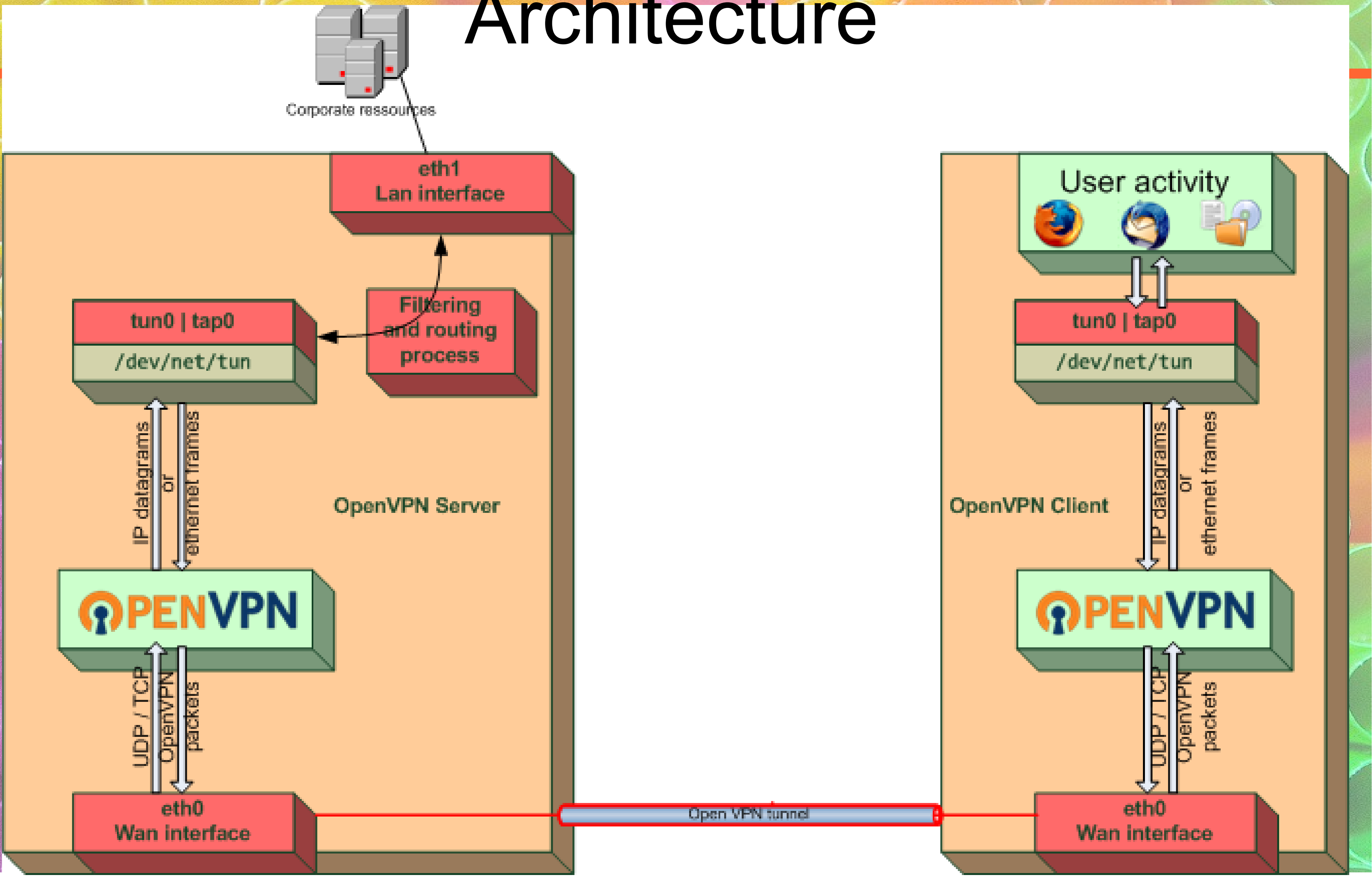
tun0 | tap0

/dev/net/tun

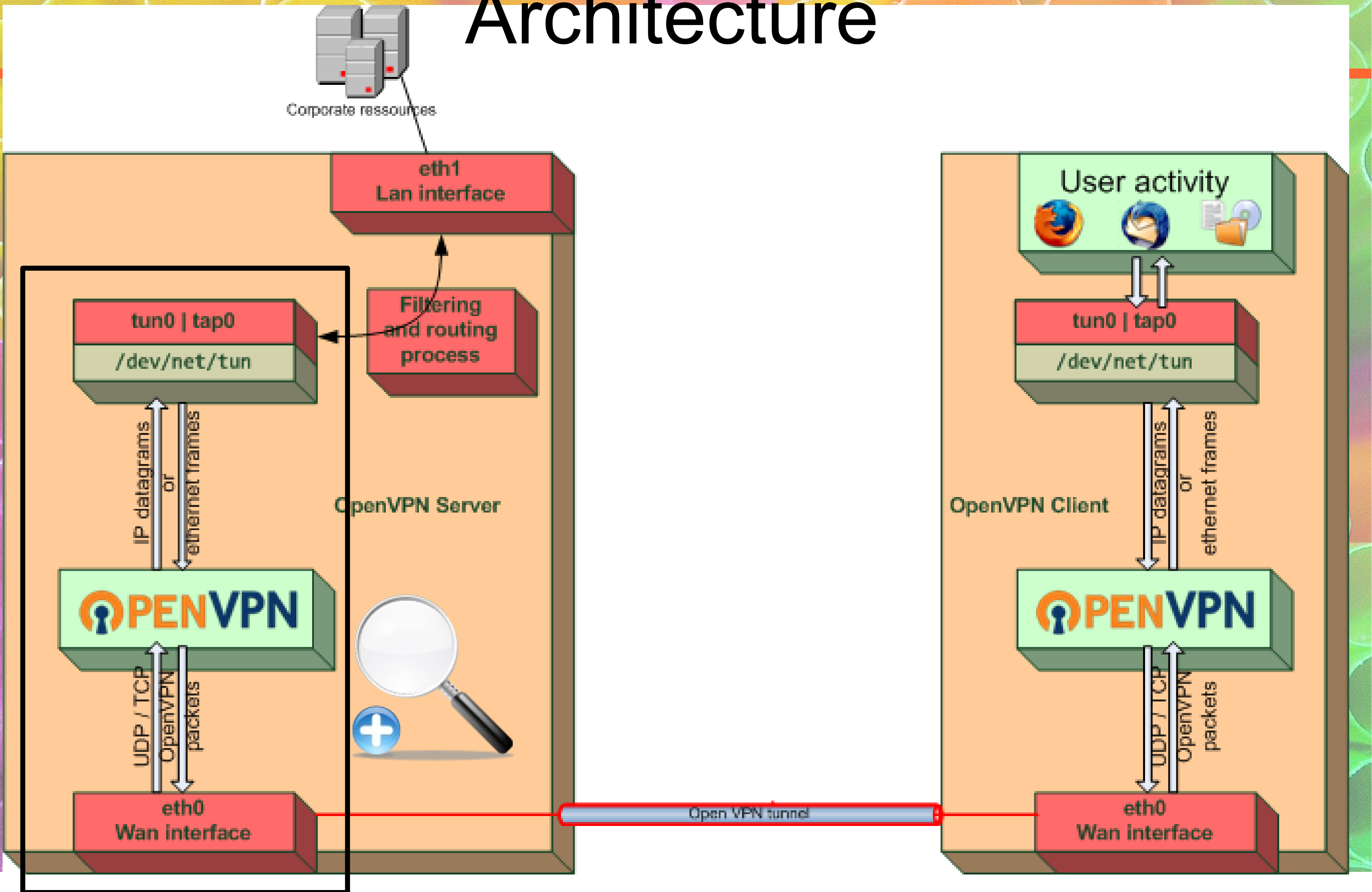
Virtual interface plugged to a character device.

Applications in user space can read and write IP packet (tun) or ethernet frames (tap) to this interface

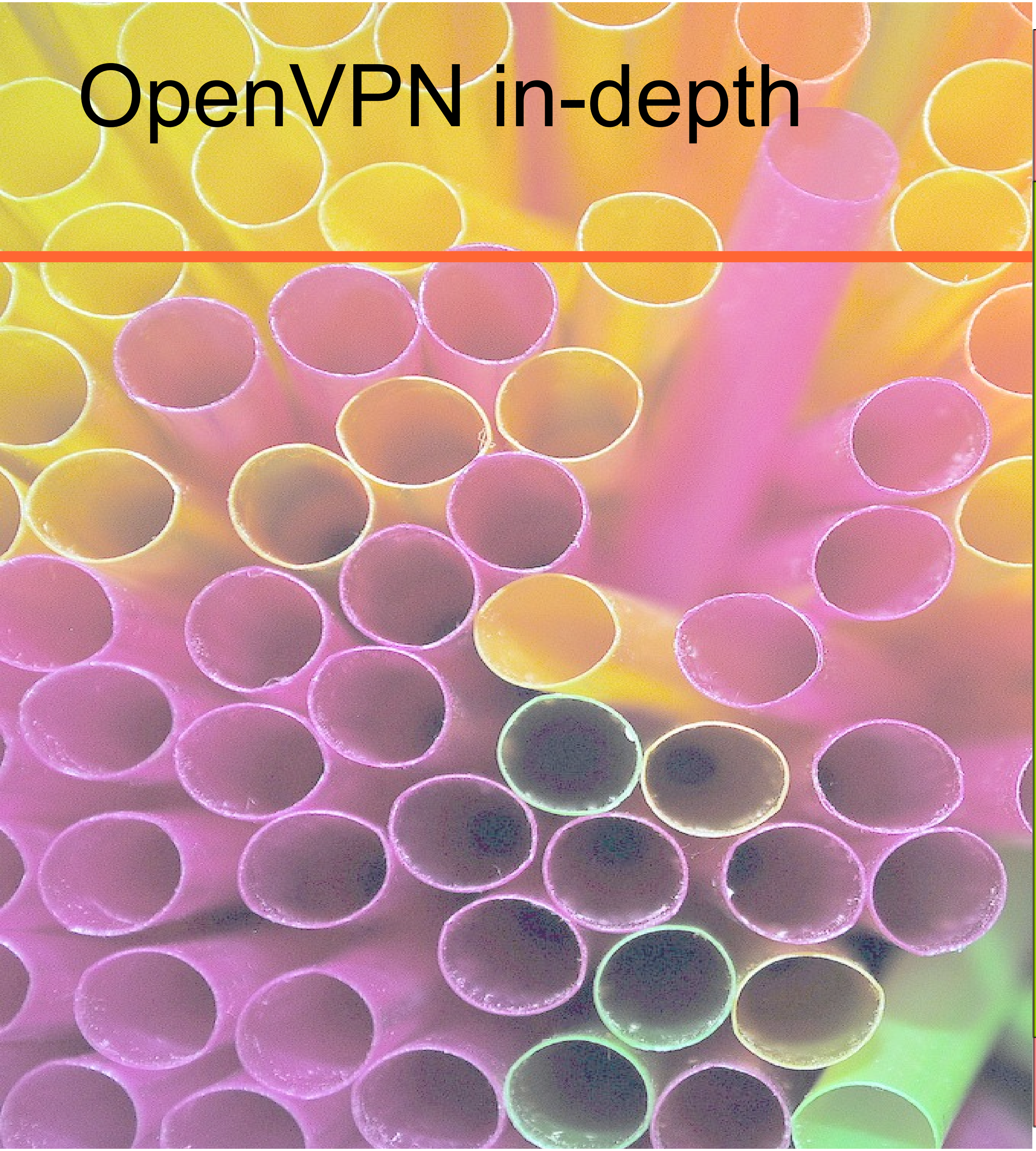
OpenVPN in-depth Architecture

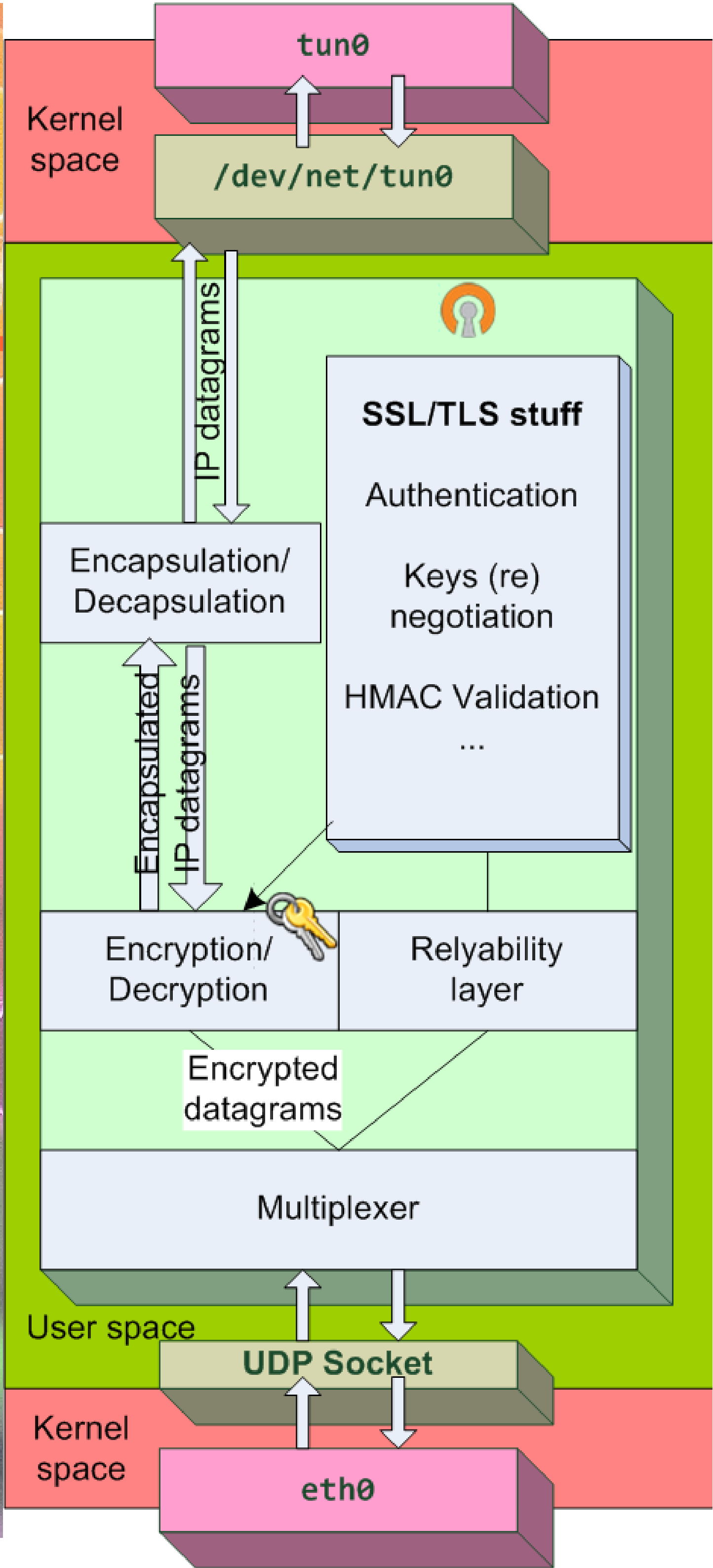


OpenVPN in-depth Architecture



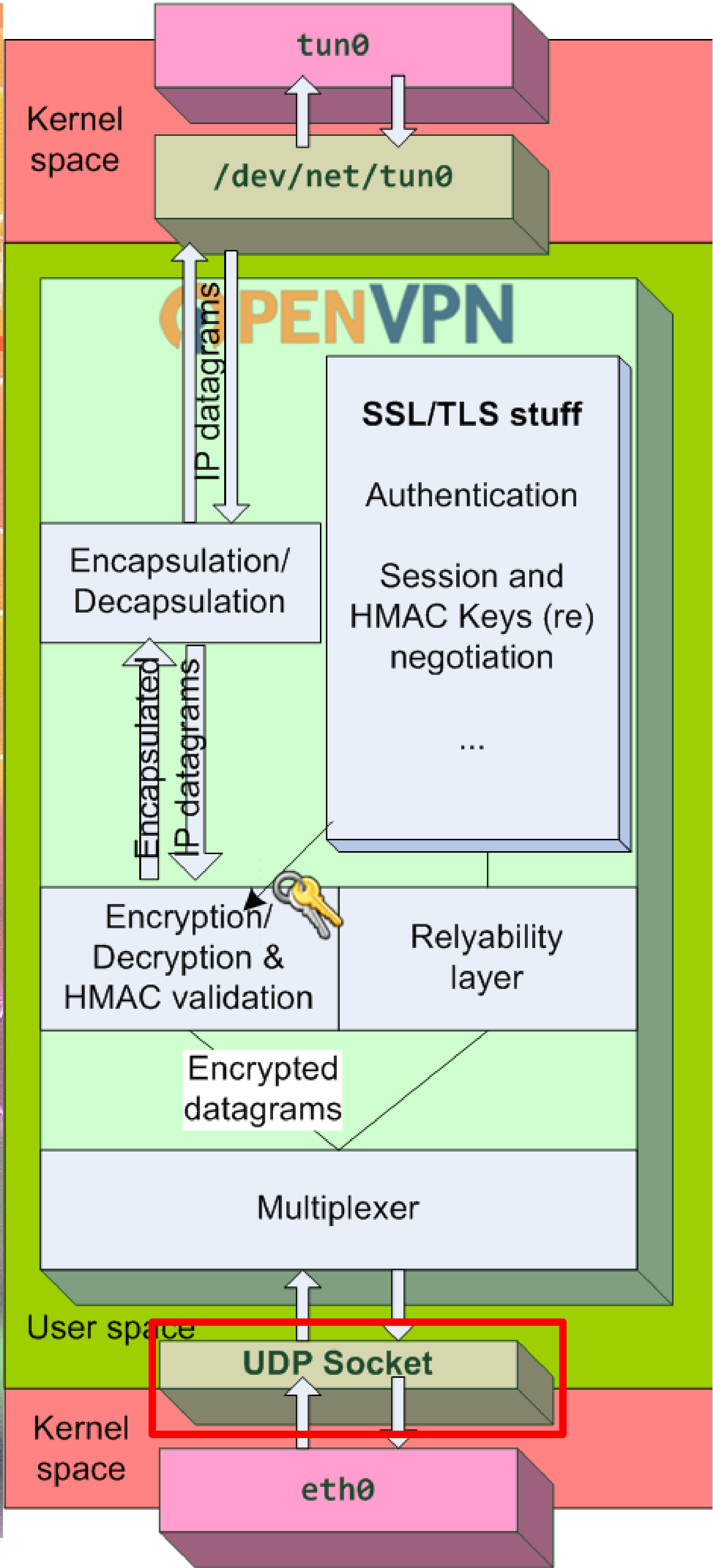
OpenVPN in-depth





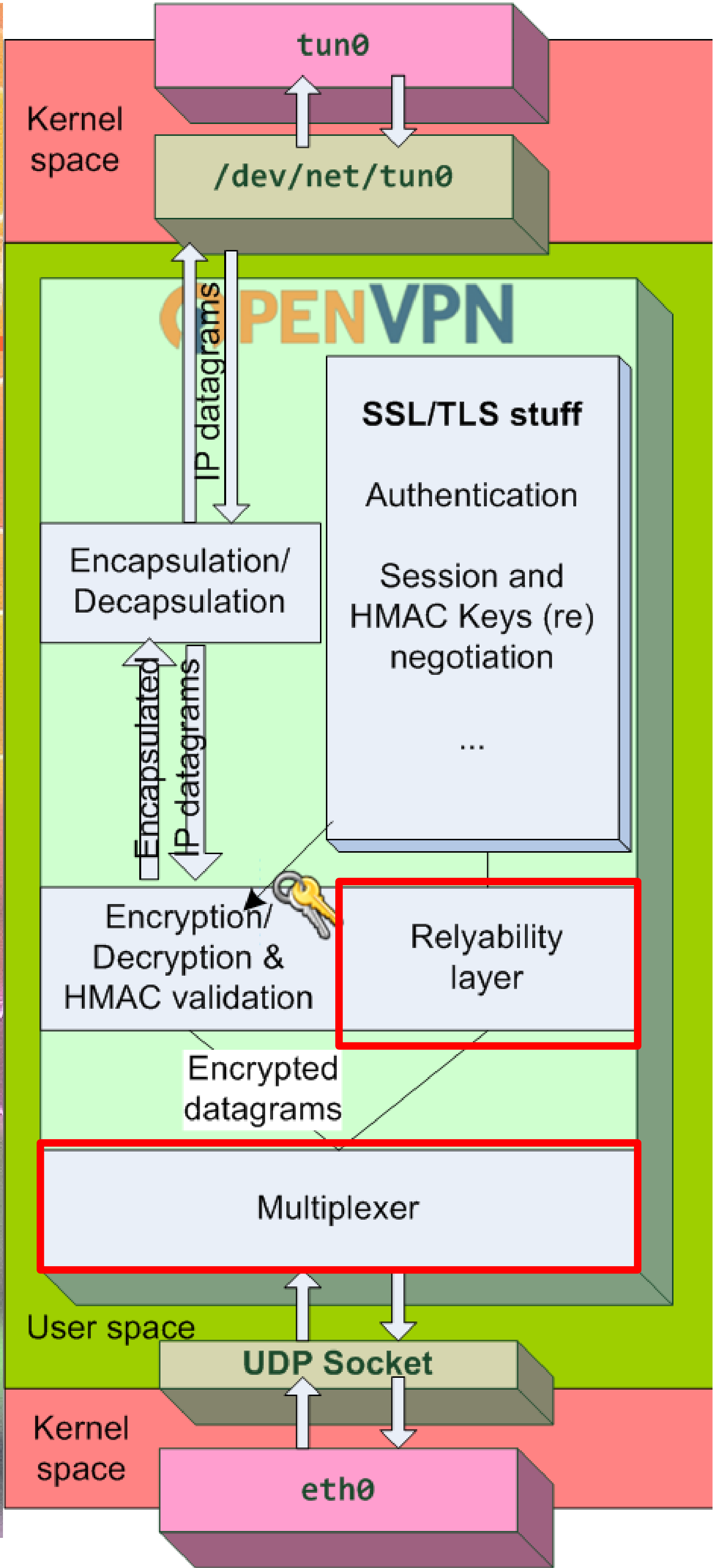
OpenVPN in-depth Transport

- OpenVPN tunnels can be transported over TCP or UDP
- With TCP transport, TCP data are tunneled **over TCP**. Congestion controls are runnning twice and badly interract when congestion occurs
- Still, TCP 443 might be your only way out
- HTTP proxy is also supported



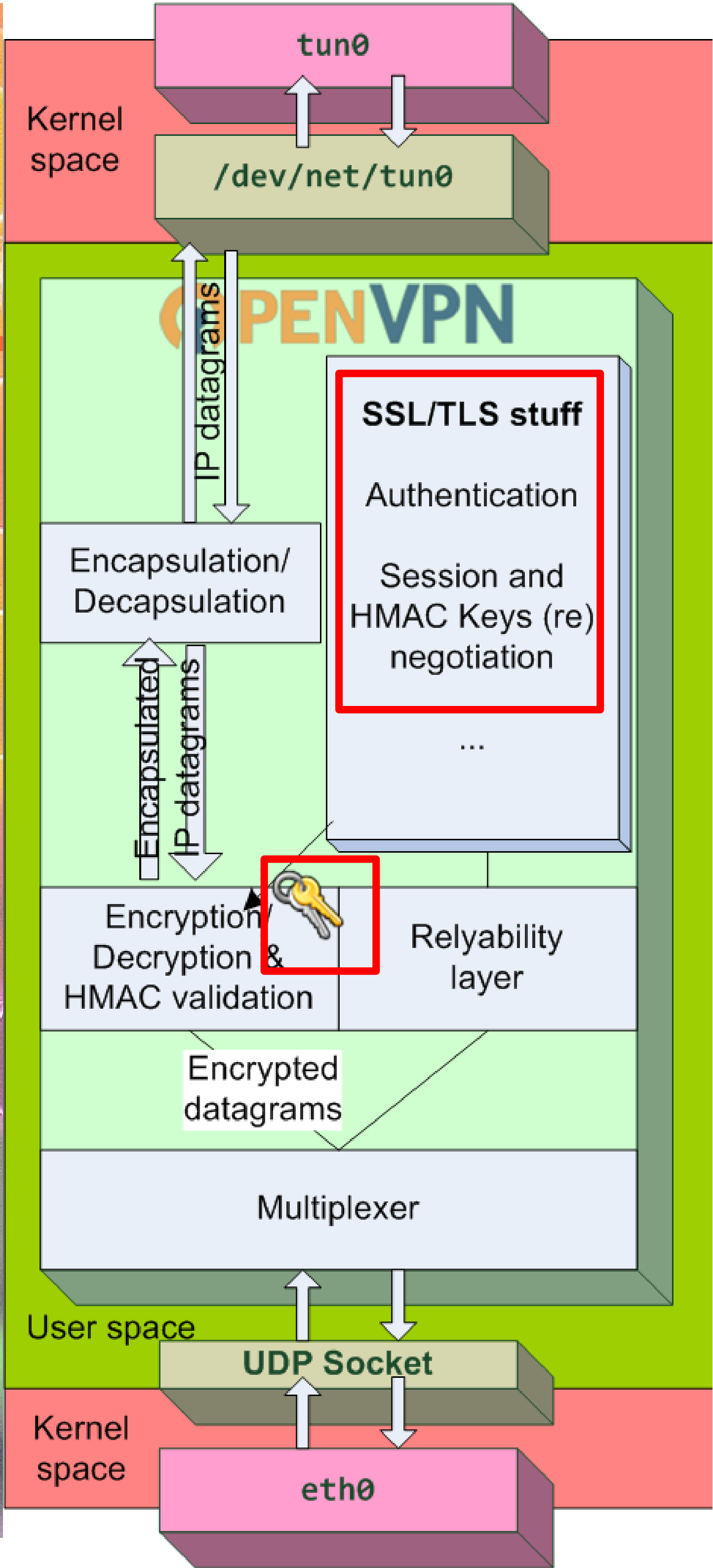
OpenVPN in-depth Multiplexer & Reliability

- Packets and frames transport need unreliability but SSL/TLS stuff does...
- The reliability layer provides it (only in UDP mode).
- An optional pre-openSSL HMAC (pre shared key) can be added at this layer



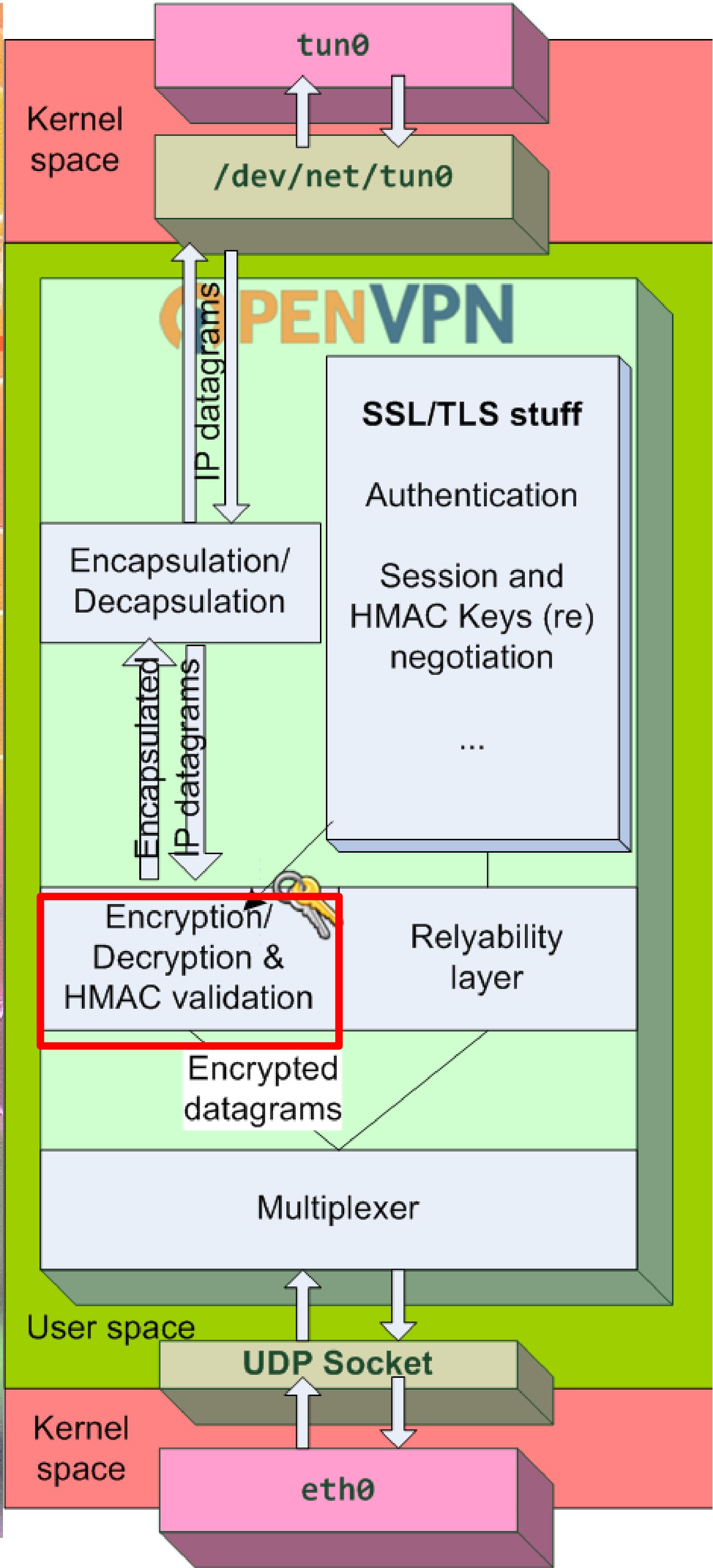
OpenVPN in-depth
- Authentication & key gen

- 2 authentication modes supported :
  - Static pre-shared key (doesn't scale well...)
  - SSL/TLS with certificates for authentication and keys negotiation (preferred)
- easyca provided for simple PKI certificate generation
- Provides keys for encryption & HMAC validation



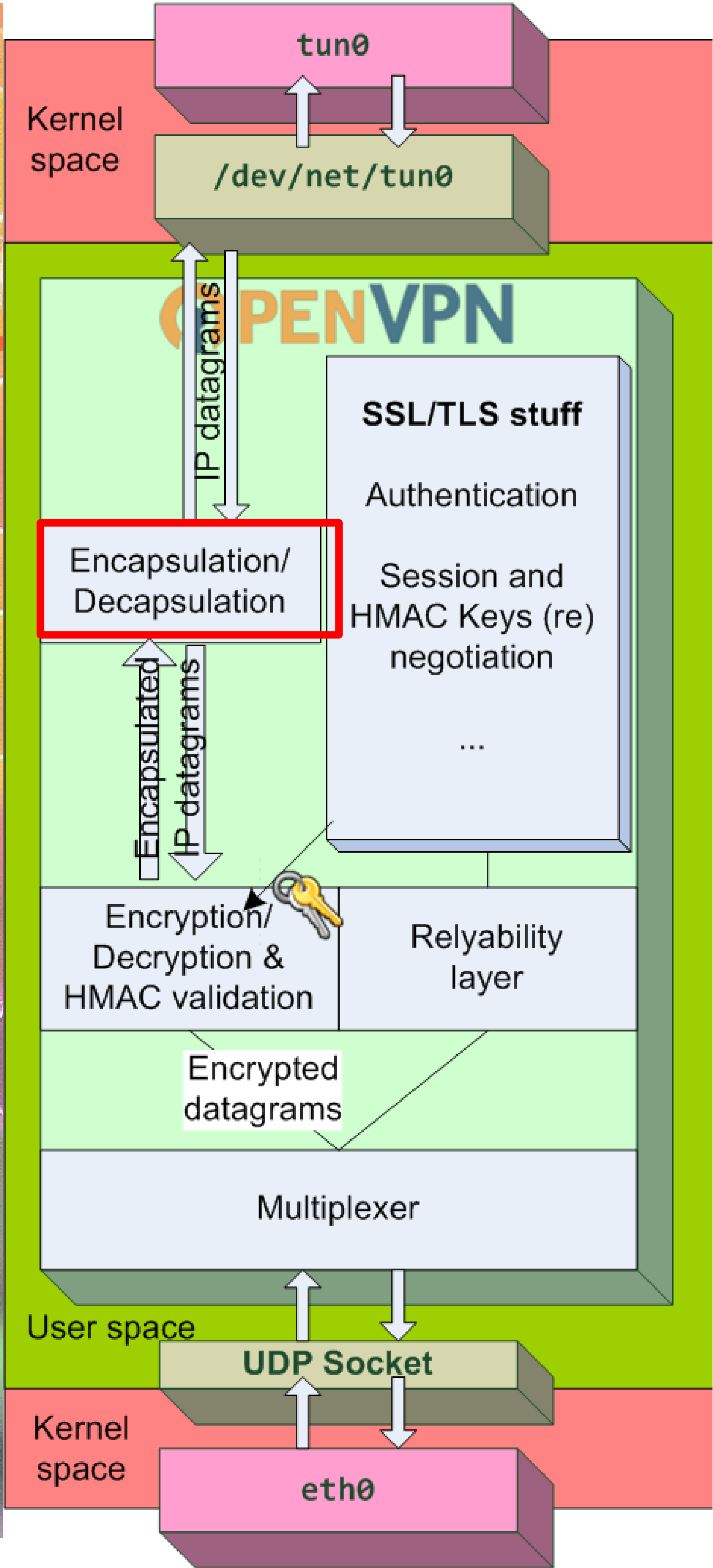
OpenVPN in-depth
Data encryption

- Data Encryption/decryption is made by standard OpenSSL EVP interface with the negociated keys.
- HMAC validation is also made with OpenSSL EVP
- An optional pre-OpenSSL HMAC header can be added.



OpenVPN in-depth Encapsulation

- Packets are read/written from the tuntap device
- The MSS is adjusted by OpenVPN request to avoid fragmentation



Summary

- VPN solutions : multiple choices for multiple situations
- **OpenVPN**
  - Quick facts
  - In-depth presentation
  - Few more things
  - Performances
  - Configuration basis
  - Plugability & Hooks for fun and creativity
- « Once upon a time... » - Few tales and demos featuring OpenVPN
- Want more ? Need help ?

Few more things

- Authentication
  - Can also be :
    - Without client certificate
    - and/or login password validated with user script (pam, ldap, OTP, db...)
  - Dual factor PKCS11 and MS cryptoapi supported
- Clients management :
  - OpenVPN server acts as a DHCP server. DHCP options supported.
  - IP pool management with sticky address
  - Routes can be pushed from server
- LB & FailOver :
  - Natively supported in client config file

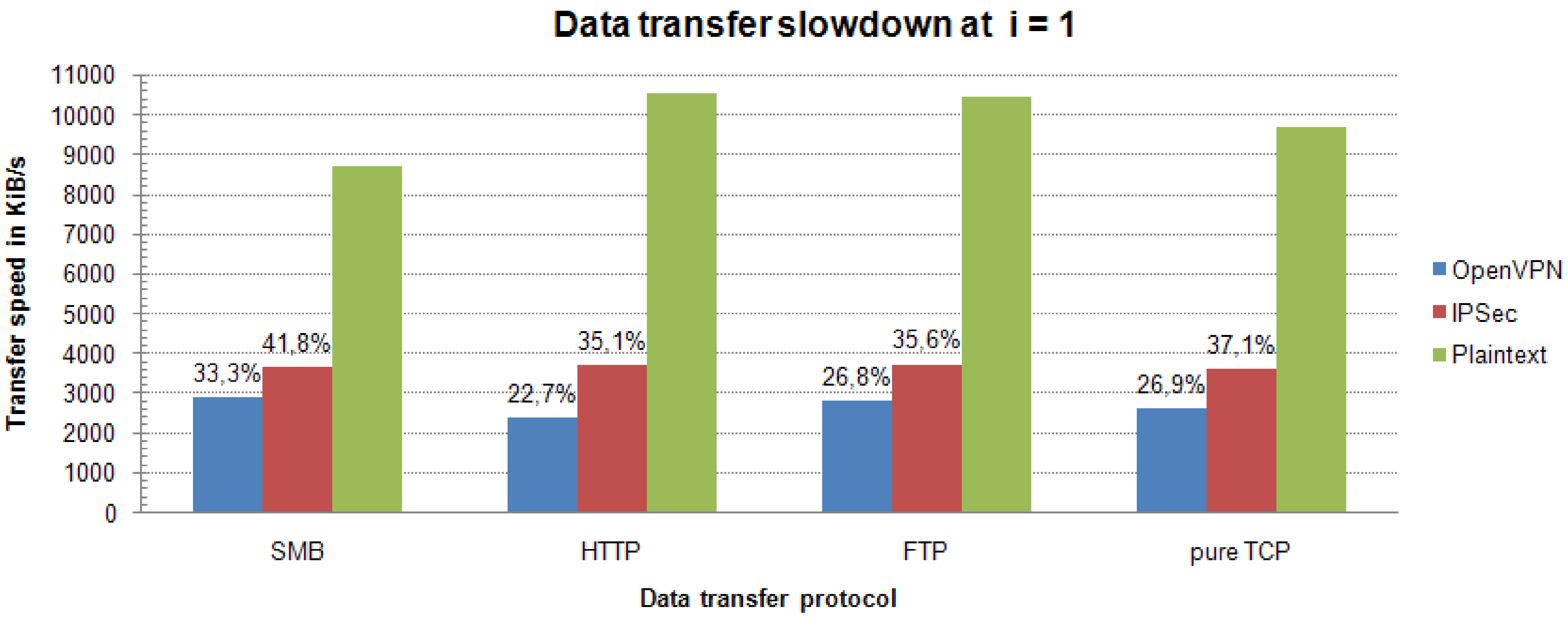
Hardening OpenVPN

- Tls-auth : A simple but efficient HMAC

  A shared static key is used to add an integrity header to vpn packets. If the HMAC is false : packet drooped. Prevent bruteforce, tempering, libssl exploitation.
- root privilege dropping
  - After init
  - With sudo for iproute
  - In chrooted environment

Performances

- Due to heavy kernel space/user space data transferts, OpenVPN performances are not as good as Ipsec's



Source : http://stuff.skoberne.net/IPSec_and_OpenVPN_Performance.pdf

Using OpenVPN : configuration basis

- Installing and running openvpn on linux
  - (apt-get|yum|urpmi|...) install openvpn
  - /etc/openvpn/ for config file(s)
  - /etc/init.d/openvpn start [configfile]
- Configuration
  - 2 modes : commands args and/or config file

Plugability & Hooks for fun and creativity

Client and server side user defined scripts can be easily called on multiple events :

- Tunnel up/down
- Certificate verification
- Login/password verification
- Client authenticated (*server* side)
- Remote IP address change
- Route up (*client* side)
- Client disconnected
- New route/MAC address added to the server

Lots of environment variables are set before calling the scripts.

Telnet management interface

Summary

- VPN solutions : multiple choices for multiple situations
- OpenVPN
- **« Once upon a time... » - Few tales and demos featuring OpenVPN**
  - Tale I : “Home sweet home : The Simple 4 Lines Config“
  - Tale II : “Escaping the evil proxy“
  - Tale III : “The OpenVPN server, the CAS WebSSO, and the brave firewall“
- Want more ? Need help ?

Tale I : “Home sweet home : The Simple 4 Lines Config“

- Goal : configure a host-to-host connection for accessing your home network (192.168.1.0/24) anywhere.
- Static key generation :

```
openvpn --genkey --secret static.key
```

- Server config :

```
dev tun
ifconfig 10.1.0.1 10.1.0.2
secret static.key
```

- Client config :

```
remote serveraddress
dev tun
ifconfig 10.1.0.2 10.1.0.1
secret static.key
route 192.168.1.0 255.255.255.0
```

Tale II : “Escaping the evil proxy“

- Objective : transport your VPN over an http proxy and route everything to it

- Change to tcp mode : `proto tcp`
- And just add this to the client configuration :

```
http-proxy [proxyaddress] [proxyport]
```

Tale III : OpenVPN with CAS sso authentication

- Objective : Using scripts capabilities of openvpn, delegate authentication on a CAS web SSO server
- Ingredients :
  - A CAS Web SSO server
  - A firewall
  - A gatekeeper : web application relying on CAS SSO
  - An OpenVPN server
  - A client
  - Few scripts

Tale III : OpenVPN conf

- Connection to openVPN is made without authentication : --certificate-free.
- --ha-mac is used to prevent total strangers
- User's VPN IP is blocked by a firewall
- An application relying on cas authentication allow the IP address on the firewall upon successful SSO authentication.

- An action script is triggered when client disconnects to clear the IP on the firewall

Summary

- VPN solutions : multiple choices for multiple situations
- OpenVPN
- « Once upon a time... » - Few tales and demos featuring OpenVPN
- **Want more ? Need help ?**

Want more ? Need help ?

- Useful links :
  - http://openvpn.net → community
  - Wiki : https://community.openvpn.net/openvpn/wiki/
  - Related projects : https://community.openvpn.net/openvpn/wiki/RelatedProjec
- Official Quickstart, manuals, HOWTO
- Mailing list : users and developers
- IRC chan : #openvpn on irc.freenode.net
- Get involved : git repository, IRC weekly meeting, Wiki, bug fixes and patch submission, donation...
- Book : “OpenVPN: Building and Integrating Virtual Private Networks”