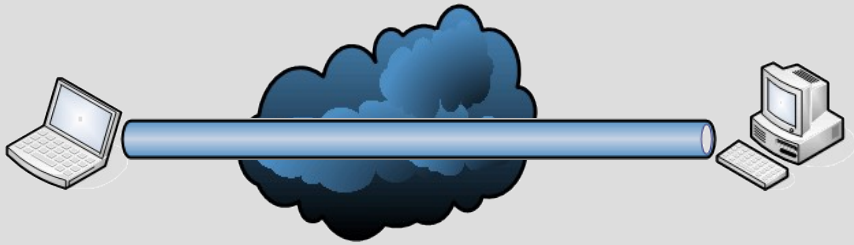
Y36SPS
OpenVPN

OpenVPN

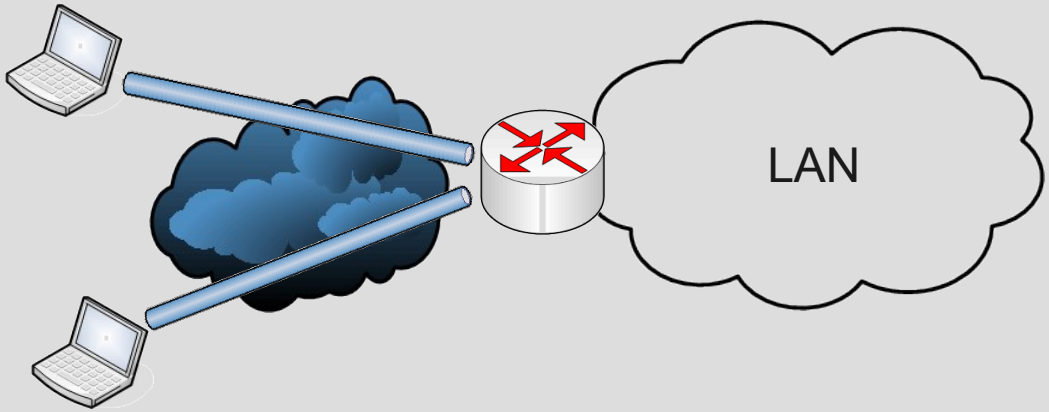
- využívá OpenSSL
- autentizace
  - sdílený klíč
  - certifikáty
  - jméno/heslo
- šifrování
  - knihovna OpenSSL
  - rozšíření HMAC
  - žádné
- protokoly
  - UDP
  - TCP
- režimy
  - „obchodní cestující“
  - host – host
  - síť – síť
  - směrování
  - přepínání
- bezpečnost
  - userspace
  - nonroot
  - chroot
  - mlockall
  - smart cards PKCS#11

Způsob spojení

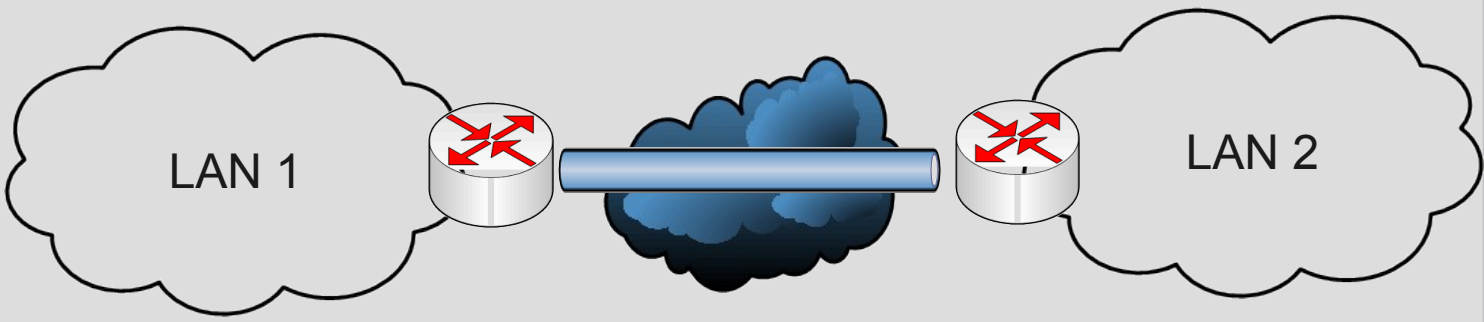
host – host



„obchodní cestující“



síť – síť



minimální konfigurace

server

```
dev tun
ifconfig 10.8.0.1 10.8.0.2
secret static.key
```

client

```
remote server.cz
dev tun
ifconfig 10.8.0.2 10.8.0.1
secret static.key
```

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

rozšíření konfigurace

```
comp-lzo

keepalive 10 60
ping-timer-rem
persist-tun
persist-key

user nobody
group nobody
daemon
```

```
comp-lzo

keepalive 10 60
ping-timer-rem
persist-tun
persist-key

route 192.168.1.0 255.255.255.0
```

certifikáty a šifrování

```
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
;duplicate-cn
;tls-auth ta.key 0
;cipher BF-CBC
;cipher AES-128-CBC
;cipher DES-EDE3-CBC
```

```
ca ca.crt
cert client.crt
key client.key
;ns-cert-type server
;tls-auth ta.key 1
;cipher BF-CBC
;cipher AES-128-CBC
;cipher DES-EDE3-CBC
```

směrováná vpn

dev tun
server 10.1.0.0 255.255.255.0

dev tun

přepínaná vpn

dev tap

server-bridge 10.8.0.4 255.255.255.0 10.8.0.50 10.8.0.100

dev tap

- nastavení bridge v OS
- (bridge-utils)

předávání informací

```
push "route 192.168.10.0 255.255.255.0"
push "route 192.168.20.0 255.255.255.0"
push "redirect-gateway"
push "dhcp-option DNS 10.8.0.1"
push "dhcp-option WINS 10.8.0.1"

pull
```

ostatní volby

client-to-client
ifconfig-pool-persist ipp.txt
max-clients 100
status openvpn-status.log
log openvpn.log
log-append openvpn.log
verb 3

remote-random
resolv-retry infinite
http-proxy
mute-replay-warnings
ns-cert-type server

směrování do sítí klientů

client-config-dir ccd

route 192.168.4.0 255.255.255.0

client-to-client
push "route 192.168.4.0 255.255.255.0"

[ccd/client1] iroute 192.168.4.0 255.255.255.0

Pokud bude čas

Secure Shell (ssh)

- terminálový přístup
- přenos souborů
- port forwarding
- X11 forwarding
- podpora vpn
- lze použít jen pro tunelování TCP
- autentizace
  - heslo
  - rhosts
  - rhostsRSA
  - veřejné klíče

ssh tunel I

ssh -L2001:localhost:143 imap.cvut.cz
ssh -L2001:imap.cvut.cz:143 imap.cvut.cz

ssh tunel II

ssh -R2001:localhost:143 hk.cvut.cz

ssh tunel III

ssh -L2001:imap.cvut.cz:143 ssh.cvut.cz

vpn - vlastnosti

- transparentní spojení
- nižší zatížení oproti vzdálenému terminálu
- složité nastavení klientů
- rozdílné prostředí
- lokálně instalované aplikace
- složitá implementace IDS

Vzdálený přístup bezpečnostní rizika

- chybné nastavení tunelu
  - X11 ssh tunneling
- kompromitování klienta
  - útok zevnitř sítě
  - nová brána do Internetu
  - nastavení osobního paketového filtru
- složitý dohled sítě
  - IDS ...

Literatura

- http://www.rfc-editor.org
- http://crypto-world.info
- Pavel Satrapa, IPv6, Cesnet, 2002
- Wenbo Mao, Modern Cryptography, Prentice Hall, 2004
- Barrett, Silverman, SSH, O'Reilly, 2003
- Northucutt, Network Perimeter Security, New Riders, 2003
- http://www.openssl.org/
- http://www.openvpn.net

A mnoho dalšího ...