

Technologie bezpečných kanálů aneb s OpenVPN na věčné časy

Josef Hajas

hajasj1@fel.cvut.cz

Co nás čeká a nemine

- Motivace, co je to vlastně ta VPN?
- Rozdělení jednotlivých druhů VPN
- Představení nejběžnějších používaných technologií
- Jak pracuje OpenVPN
- Škálovatelnost OpenVPN
- Jaké bezpečnostní mechanismy OpenVPN nabízí

Co je to VPN

Jak komunikujete po síti?

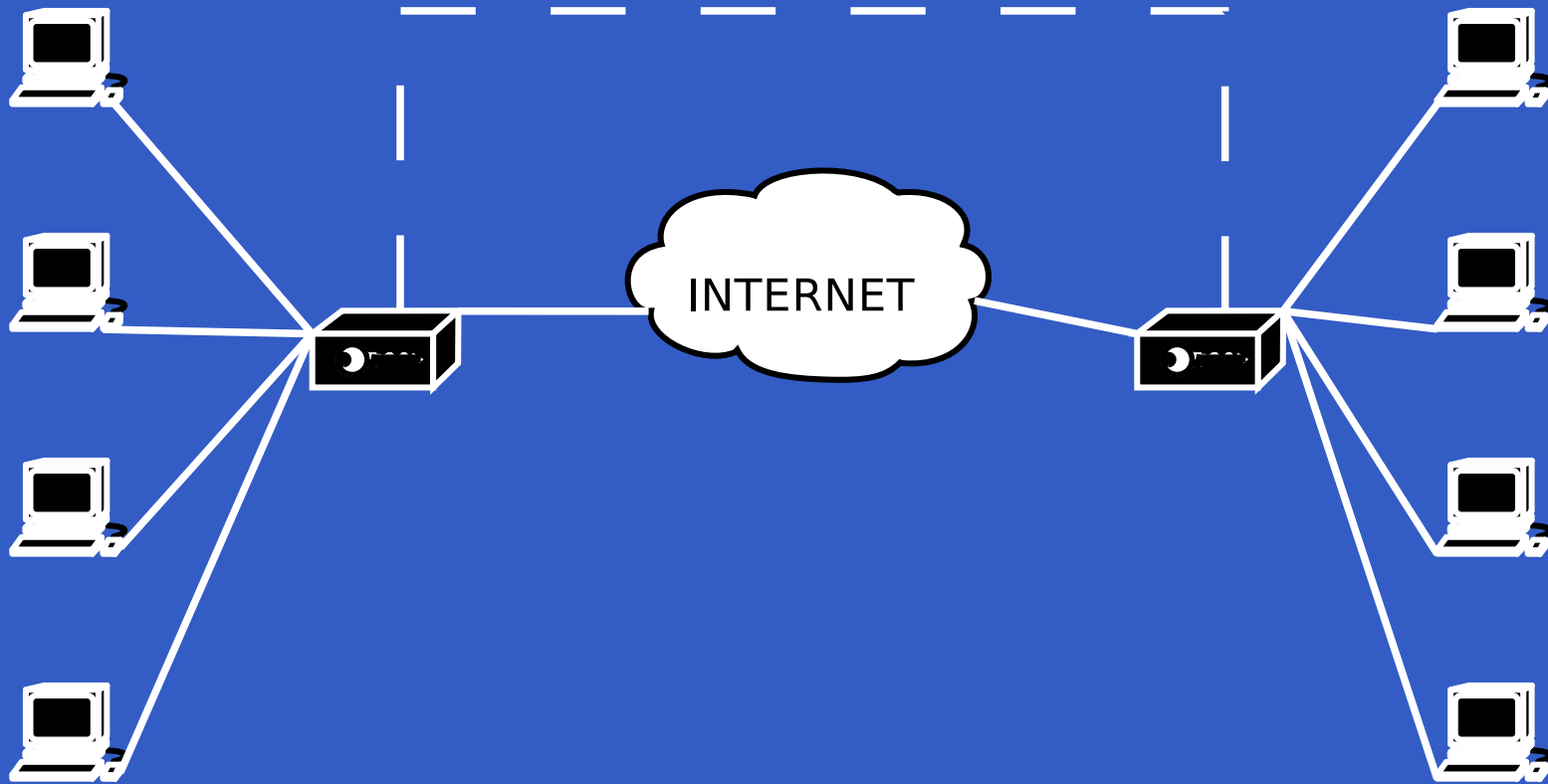
Jak mohu bezpečně komunikovat po síti:

- na úrovni aplikací (ssh, https)
- na síťové úrovni (VPN)

Jakou topologií VPN si budete přát?

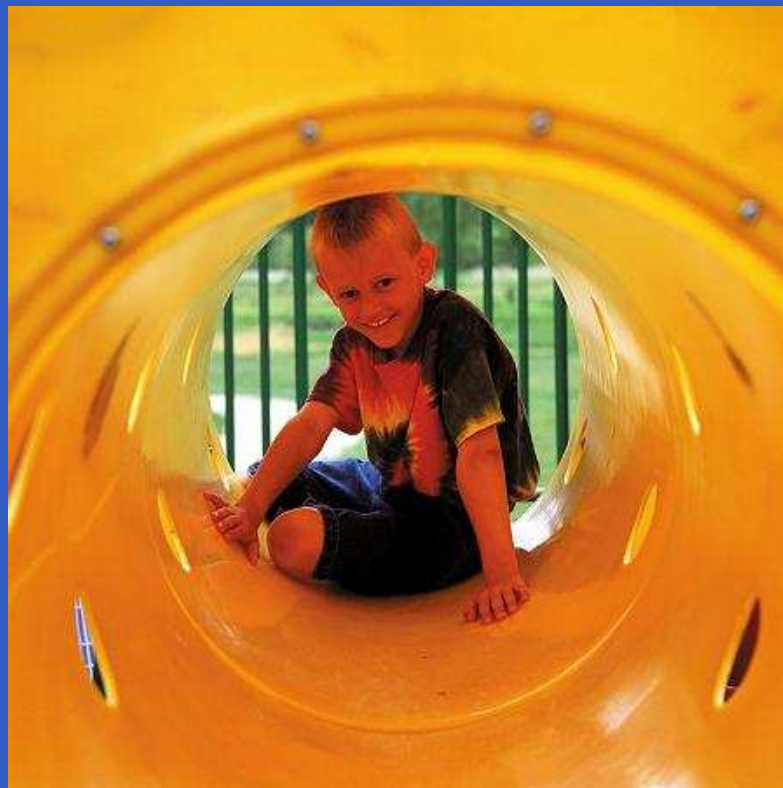
- Gateway to gateway
- Client to gateway
- Host to host

Gateway to gateway

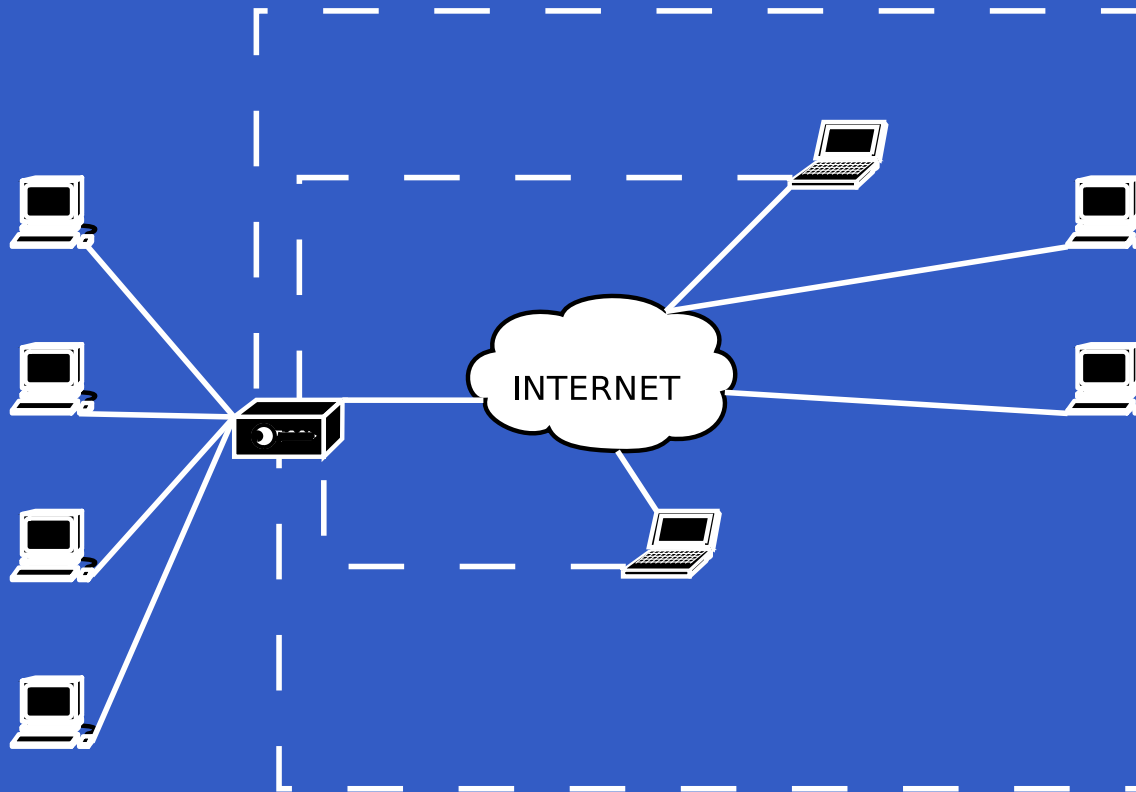


-
-
-

neboli tunel



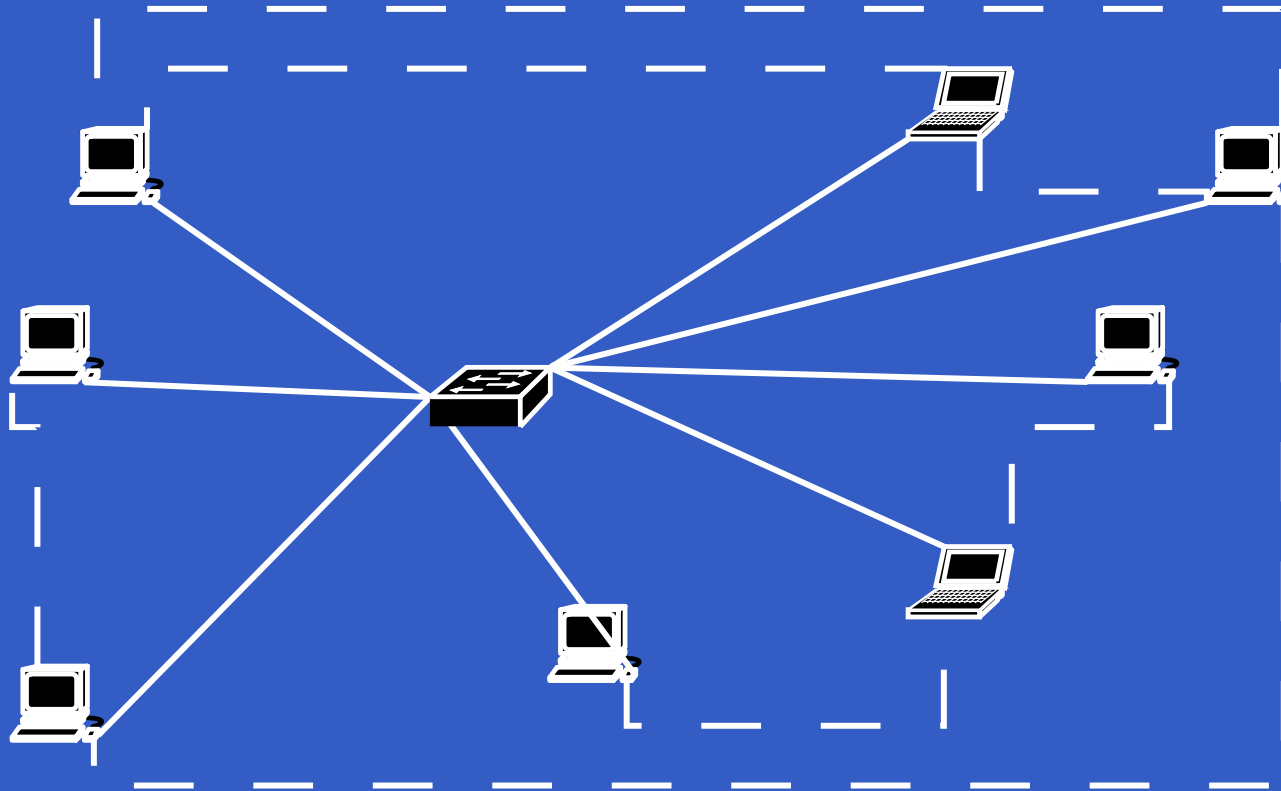
Client to gateway



neboli roadwarrior



Grupáč



Využívané technologie

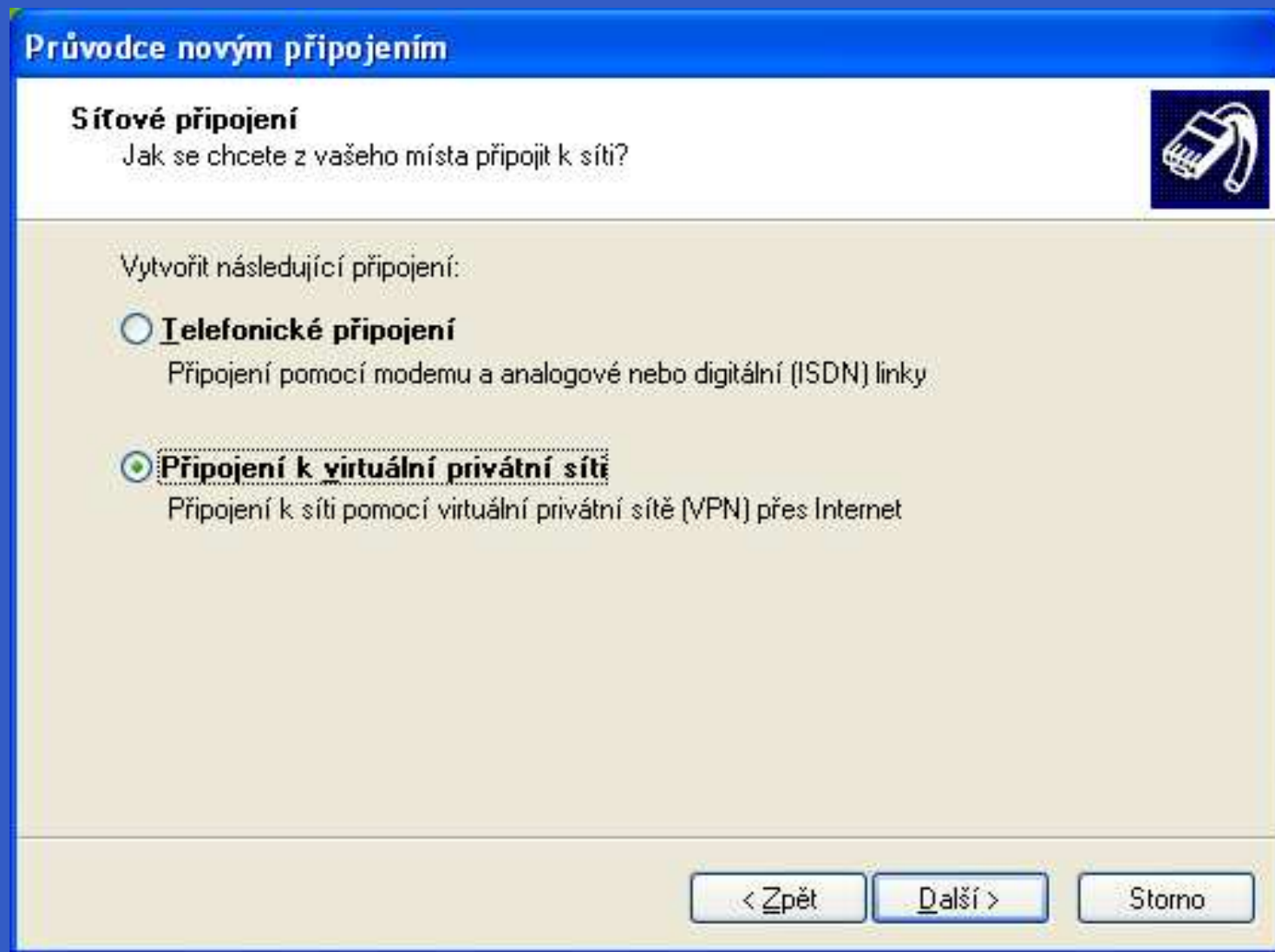
- PPTP
- IPSec
- L2TP over IPSec
- Userland VPN nad OpenSSL

PPTP aneb vylepšený dial-up

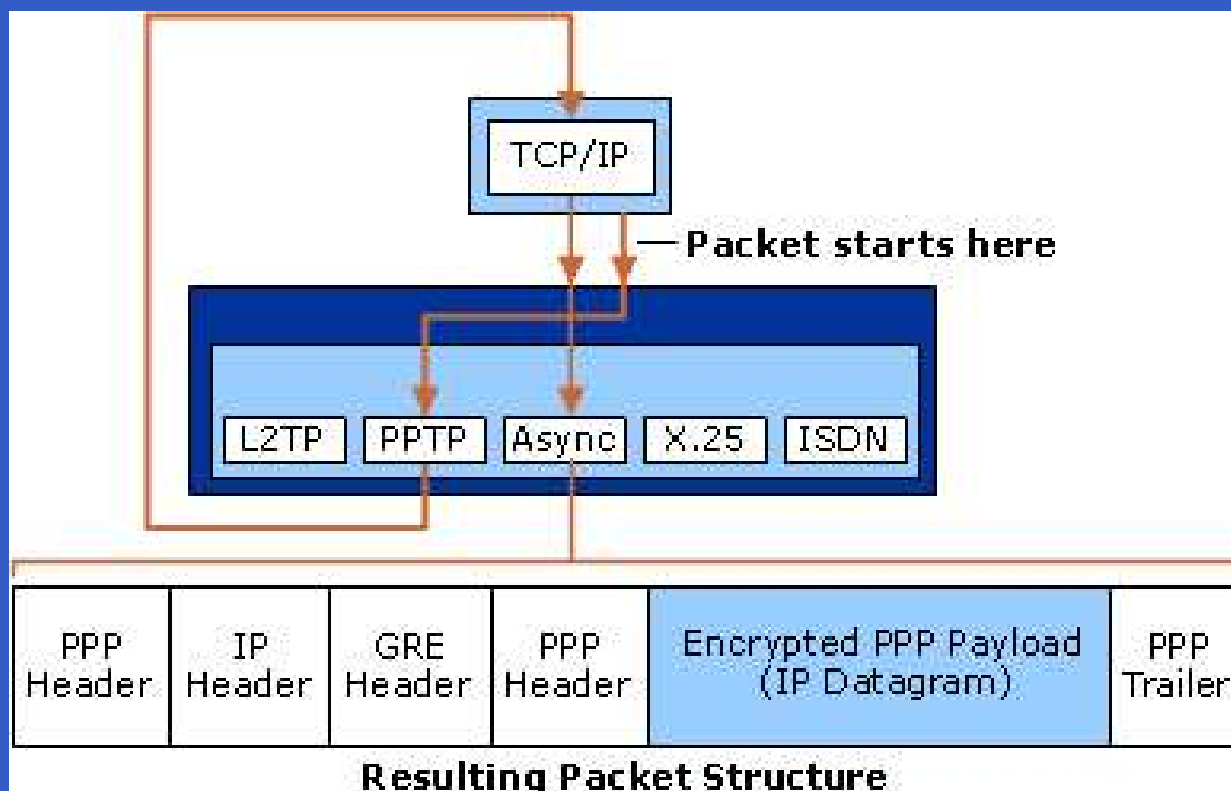
Point-to-Point Tunneling Protocol

- Postaveno na PPP
- Šifrování pomocí MPPE
- Vytvořeno Microsoftem → veliká podpora v jeho produktech

Vestavěný klient PPTP ve Windows XP



PPTP: taneček s packety



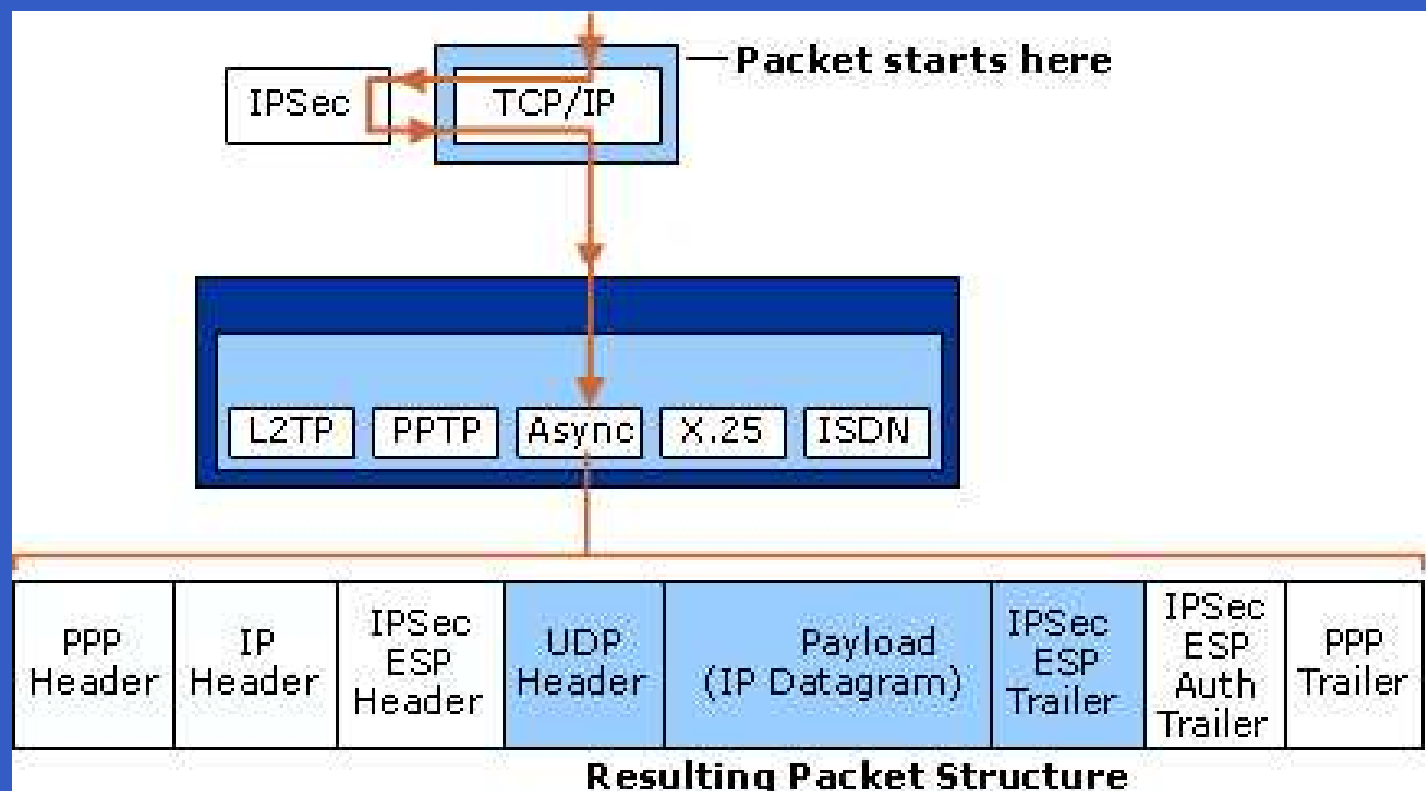
PPTP pass through

- Řídící spojení na TCP portu 1723
- Data chodí přes GRE
 - nezná pojem port
 - údaje o příslušnosti k session udány jinak
 - NAT musí s tímto protokolem umět zacházet
 - např. na FreeBSD nutnost použití specializovaného daemonu
 - Linux potřebuje zvláštní modul

IPSec: dárek IPv6

- první verze v roce 1995
- některé části stále ve vývoji
- velmi komplexní → komplikace pro začátečníka
- nutná podpora kernelu → komplikuje portování
- tunelovací X transportní režim
- zdrojová a cílová adresa součástí zašifrovaných dat → občas také problémy s pass through

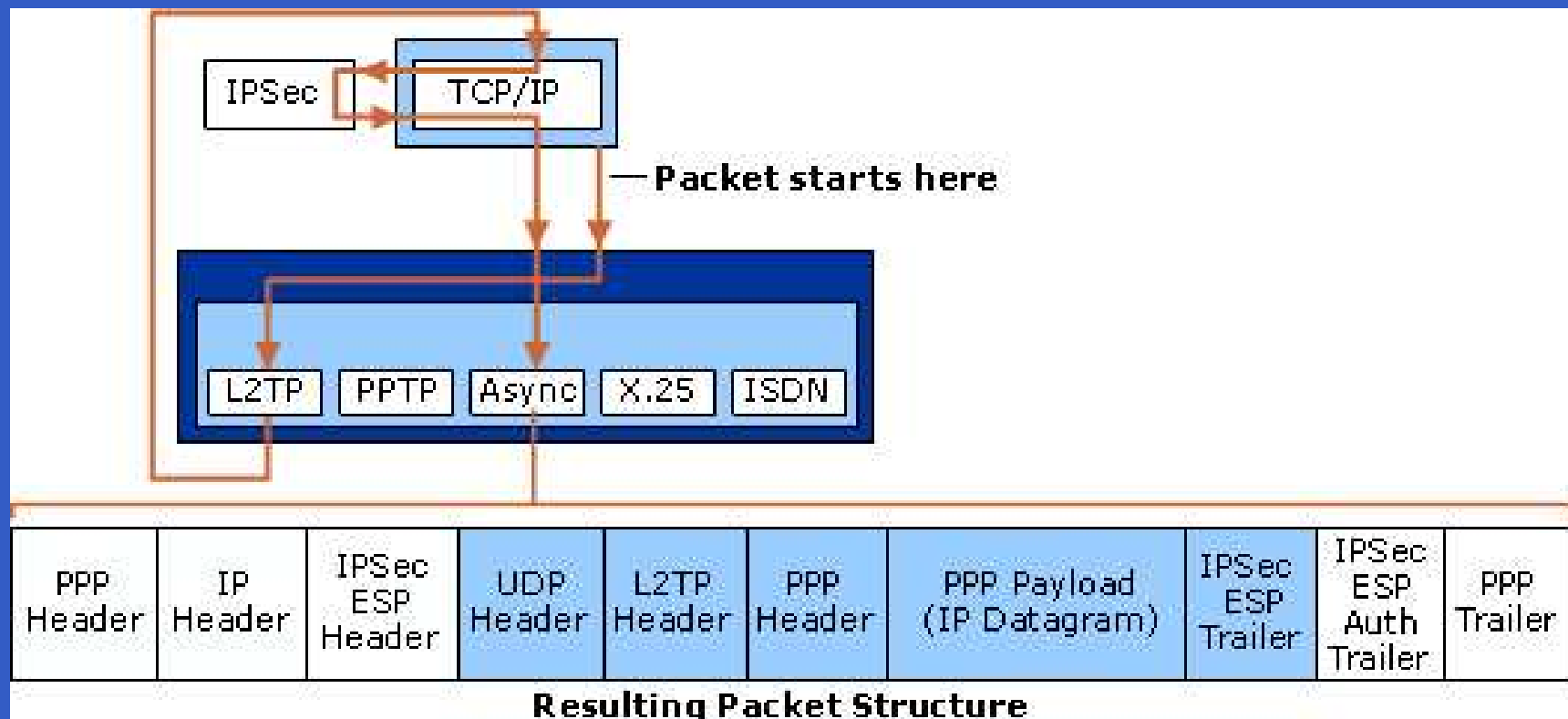
IPSec: taneček s packety



L2TP over IPSec

- Technologie Cisco a Microsoft
- Pro šifrování používá IPSec
- Navíc zavádí autentizaci uživatele
- Velmi drahé :o(

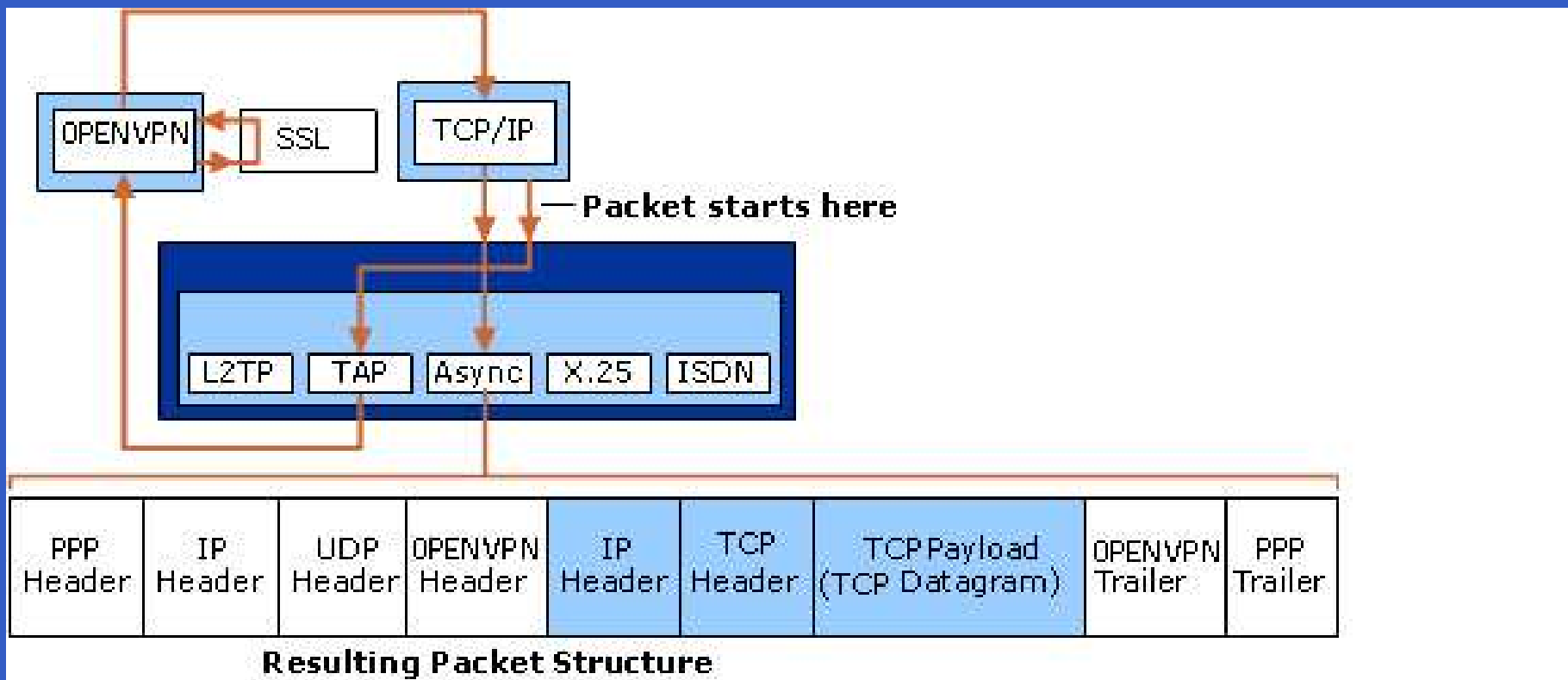
L2TP: taneček s packety



User space VPN

- v jádře pouze tun/tap síťový driver
- k šifrování využívá velký potenciál knihovny OpenSSL
- pro dané spojení využije jen jeden port (UDP nebo TCP)

OpenVPN: taneček s packety



TCP nebo UDP?

- Až do verze 1.6 pouze UDP, proč?
- TCP oproti UDP zajišťuje následující:
 - potvrzování packetů
 - řízení toku
- tedy overhead

Chceme tenhle overhead přenášet 2x?

Nejjednodušší spojení

Na stroji v Moskvě necháme OpenVPN
poslouchat na UDP portu 5000

```
moscow# openvpn --dev tun0  
--ifconfig 10.4.0.1 10.4.0.2
```

a z Prahy se na něj připojíme

```
prague# openvpn --remote  
moscow.example.com --dev tun0  
--ifconfig 10.4.0.2 10.4.0.1
```

Předsdílený klíč

Symetrické šifrování: společný klíč

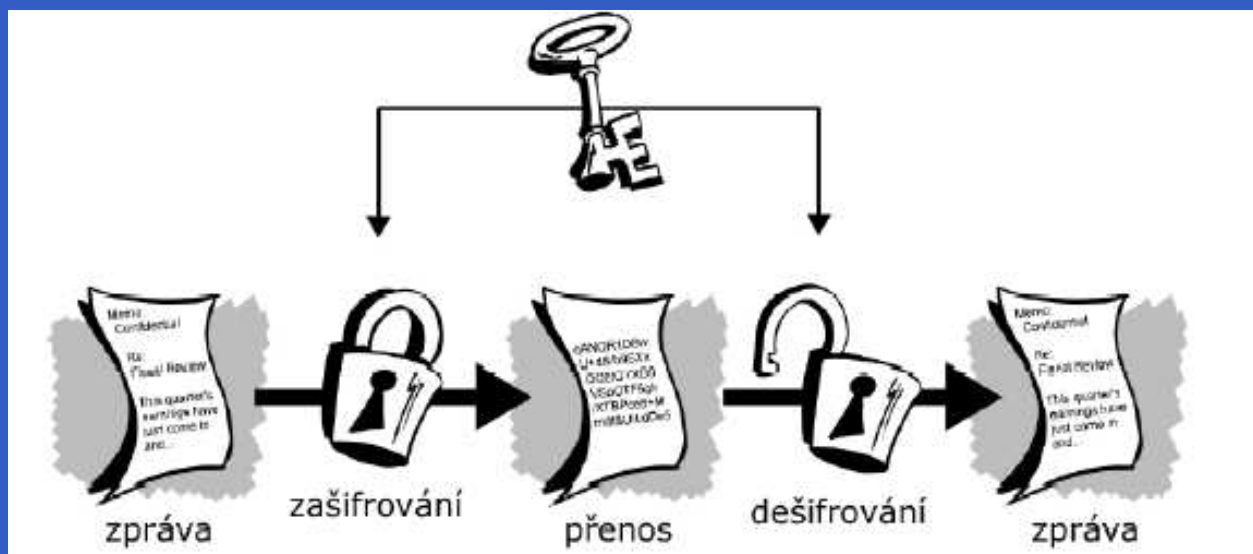
```
moscow# openvpn --genkey --secret  
tajny.key
```

```
moscow# openvpn --dev tun0  
--ifconfig 10.4.0.1 10.4.0.2  
--secret tajny.key
```

```
prague# openvpn --remote  
moscow.example.com --dev tun0  
--ifconfig 10.4.0.2 10.4.0.1  
--secret tajny.key
```

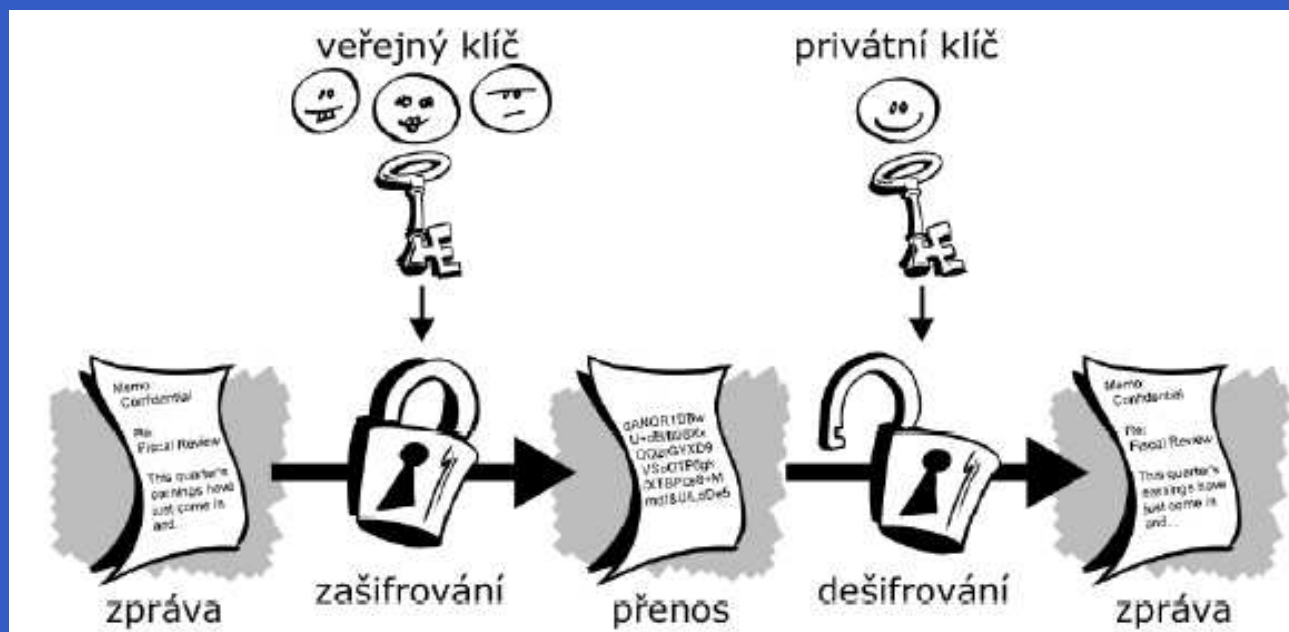
Předsdílený klíč: co nám vadí

- kompromitace jednoho počítače → kompromitace celé sítě
- získáním klíče odhalí útočník i všechnu dosavadní komunikaci



Nesymetrické šifrování

- Co zašifruje veřejný klíč, rozšifruje jen privátní
- Co podepíšete privátním klíčem, ověříte veřejným klíčem



Těžký kalibr: SSL/TLS

- založeno na certifikátech
- předpokládá se využití vlastní certifikační autority
- po představení si obě strany vygenerují klíče a předají si je přes bezpečný kanál vytvořený nesymetrickým šifrováním
- změny klíčů mohou probíhat vždy po nějaké době
- TLS závisí na spolehlivém transportu TCP → vlastní vrstva nad UDP pro TLS výměny

Obrana proti Denial Of Services

- SSL/TLS podsystém poměrně robustní a složitý (mnoho řádek kódu i na zamítnutí)
- tedy snadno zahlitelný chybnými požadavky
- řeší podepisování předsdíleným klíčem (tedy symetrické)
- zároveň chrání před případným buffer overflow v OpenSSL

Další nekryptografické výhody

- adaptivní komprese pomocí knihovny LZO
- adminuje se stejně jako klasický unix daemon/služba ve windows
- klasický routovaný režim (jen IPv4) nebo bridge režim (IPv6, IPX...)
- žádné problémy s NATem
- pro routery po cestě klasické UDP nebo TCP packety
- chroot a běh s definovanými právy

Co budoucnost?

Finišuje verze 2.0, která mimo jiné přinese:

- autentizaci uživatele proti PAM modulu
- jeden server daemon pro více klientů
- konfigurace vnucená serverem
- vzdálená správa za běhu (management interface) → rozhraní pro externí GUI

Má snad někdo otázky?

Radši se mne na nic neptejte, protože nic dalšího už stejně nevím :o)

