SPS
Bezpečnostní architektura PS

Motivace útoků v internetu

Peníze

Peníze

Peníze

Peníze

Peníze

Sláva

„Něco si dokázat“

.. udržovat nebezpečí, aby bylo komu prodávat bezpečnostní produkty, a to co nejvíce...

Cíle ochrany

data

- utajení
- integrita
- dostupnost

zdroje

- zneužití výkonu
- útok na jiné systémy
- uložení závadného obsahu

pověst

- poškození dobrého jména

Typy útoků

průnik (intrusion)

nedostupnost služby (denial of service)

zcizení informací (information theft)

vnější útok

- přes síť...

vnitřní útok

- z lokální sítě
- vyzrazení interních informací
- provozování nekorektních činností

Řešení - firewall

Firewall – je síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a/nebo zabezpečení.

Nutno rozlišovat:

- Paketové filtry
- Aplikační brány
- Stavové paketové filtry
- Stavové paketové filtry s kontrolou protokolů a IDS
- Bezpečnostní politika firewallu

Pojmy

Router

směrovač, který ovládá směrování potřebných protokolů (viz PSI)

Firewall

viz před chvílí

Brána

pojem používaný pro počítač, připojující síť k internetu. Obvykle se ale jedná o router+firewall

Jak to funguje

Firewall je: hardware + software

- hardware: počítač, který má dostatek rozhraní potřebného typu
- software: kód, který pozná potřebné protokoly a umí vhodně implementovat pravidla bezpečnostní politiky

Možnosti firewallu I

firewall umožňuje

- soustředění bezpečnosti
  - veškerý provoz prochází jedním bodem
  - možnost zaměřit se na zabezpečení jednoho místa
- využití bezpečnostní politiky
  - odstranění potenciálně nebezpečných služeb/protokolů
  - odstranění služeb z nebezpečných zdrojů
- efektivní záznam „internetových“ aktivit
  - veškerý provoz prochází firewallem
- rozdělení vnitřní sítě
  - vnitřní firewally
  - ochrana bezpečnějších částí

Možnosti firewallu II

firewall neumožňuje

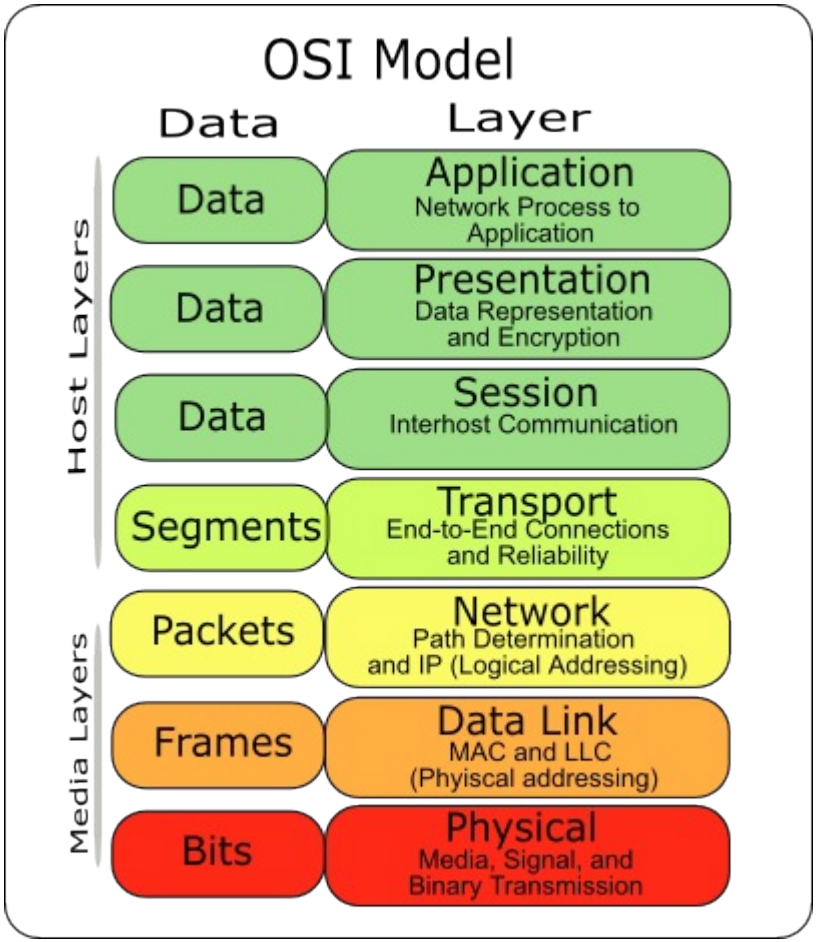
- ochranu proti vnitřnímu nepříteli
  - vnitřní útočník už firewall nepřekonává (lze použít vnitřní firewally a host firewally)
  - ochrana proti odeslání dat selhává na úrovni OS (USB:)
- nechrání proti spojením mimo firewall
  - dial-up a wifi připojení počítače připojeného do vnitřní sítě

Možnosti firewallu III

L5-7 firewally:

- ochrana proti neznámým hrozbám
  - např. neznámá chyba v protokolu
    - lze řešit povolením pouze korektních dotazů
- ochrana proti virům
  - výpočetně náročné rozpoznání dat v komunikaci
  - lepší je nahradit protivirovou ochranou počítačů

ISO/OSI model



L2-L7 - Firewall

L1 – jedině zeď

Informace pro filtrování

linková vrstva

ethernet, FDDI, ATM

síťová vrstva

IP

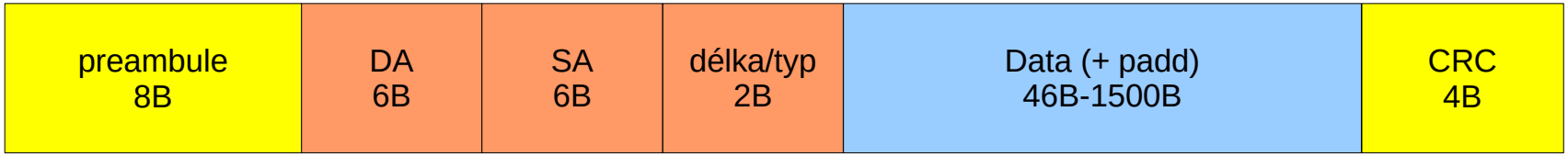
transportní vrstva

TCP, UDP

aplikační vrstva

http, ftp, telnet, smtp ...

Linková vrstva



protokolu

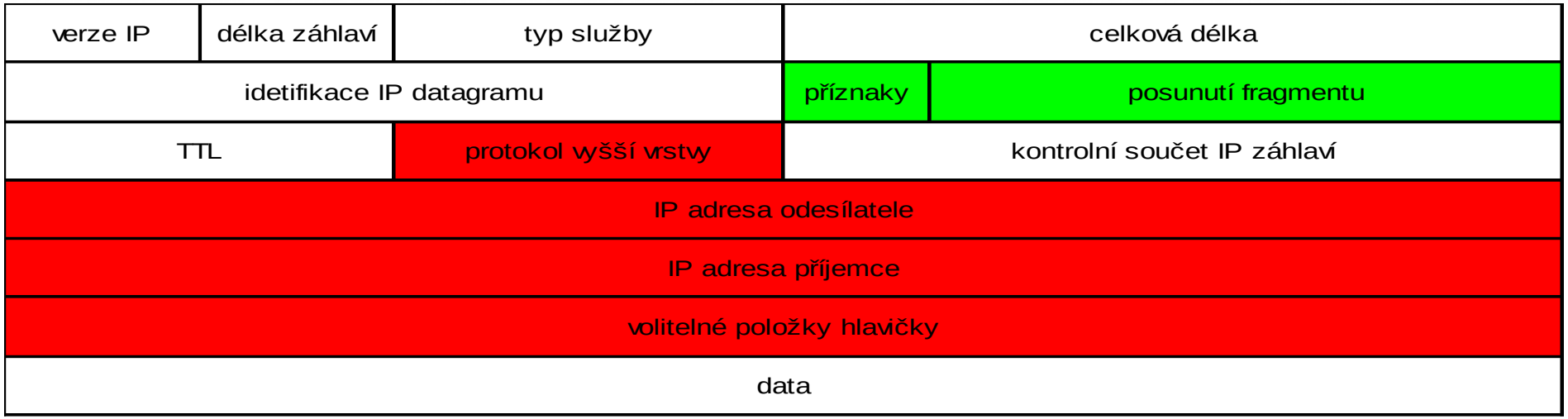
IP
zdrojová MAC adresa

adresa zdroje
adresa posledního směrovače
cílová adresa

většinou adresa odchozího směrovače
špatně použitelné pro filtrování

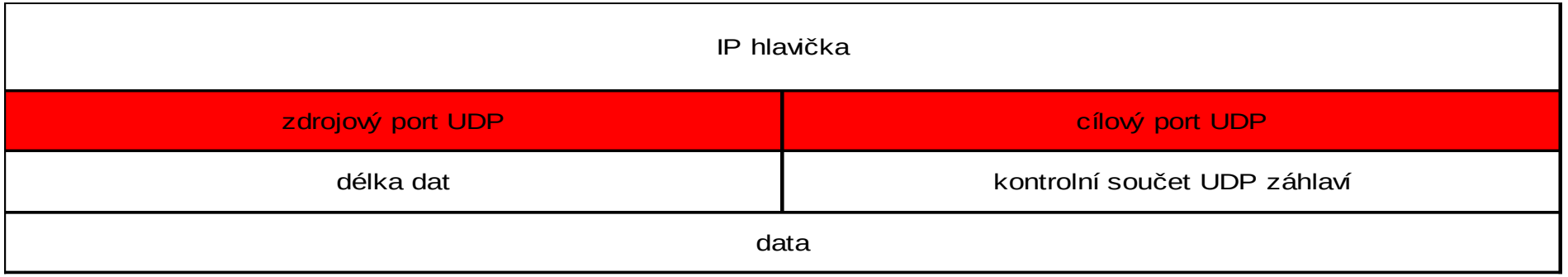
filtrování broadcastů/multicastů

Síťová vrstva



- adresy (identifikace) odesílatele a příjemce
- protokol vyšší vrstvy
  - TCP, UDP, ICMP, OSPF, IPsec …
- volitelné položky
  - většinou prázdné, potenciálně nebezpečné
- Fragmentace
  - problém při analýze protokolu vyšší vrstvy

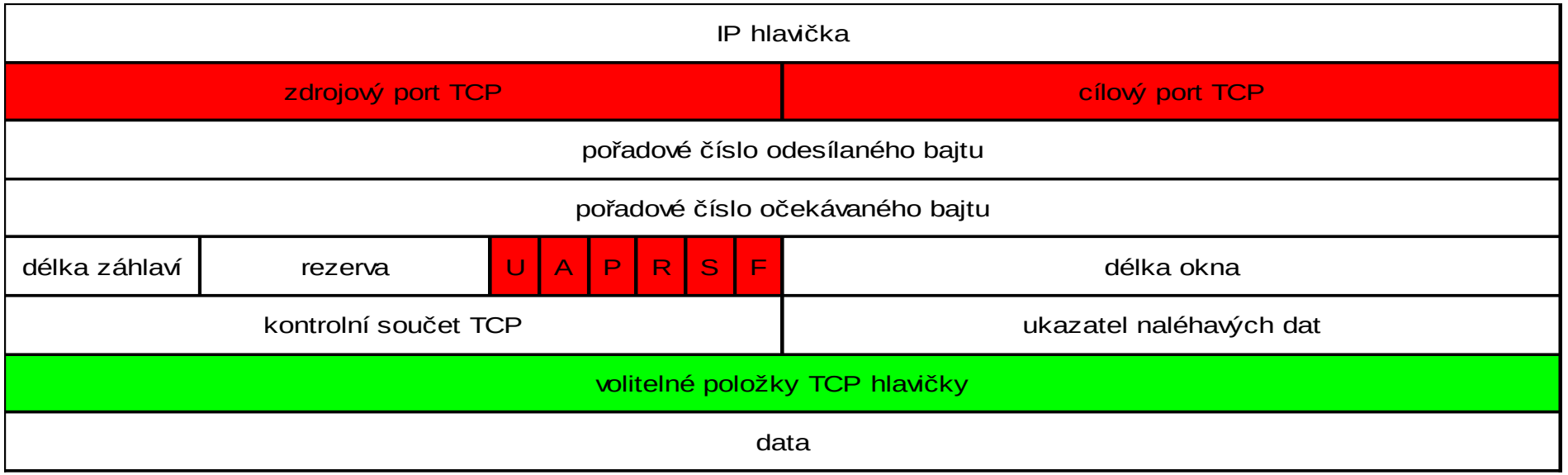
Transportní vrstva – UDP



port odesílatele a příjemce

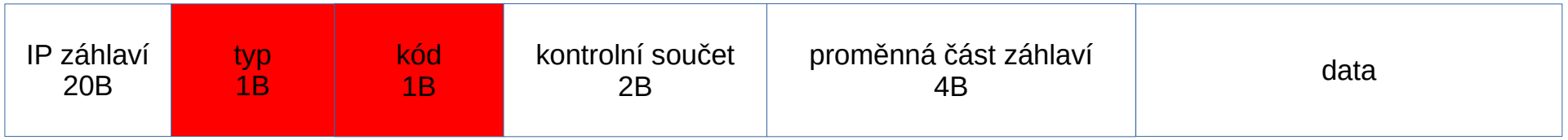
identifikace služby

Transportní vrstva – TCP



- port odesílatele a příjemce
- příznaky
  - určují stav spojení (navázání, ukončení)
- volitelné položky
  - běžně se používají, nepříliš zajímavé pro filtrování

ICMP



typ/kód

0/0 … echo request
8/0 … echo reply
3/* … nedoručitelný IP paket
5/* … změň směrování
…

vhodný protokol pro tunelování – je většinou povolený a dobře se do něho zapouzdřuje…

> není vhodné ICMP povolit úplně, ale na základě typu …

Aplikační vrstva

velké množství protokolů (stovky-tisíce)

časté změny (skype)

uzavřené protokoly (skype)

šifrování (skype)

použití různých portů (skype)

Další metriky

čas

- pracovní/výuková doba

autentizovaný uživatel

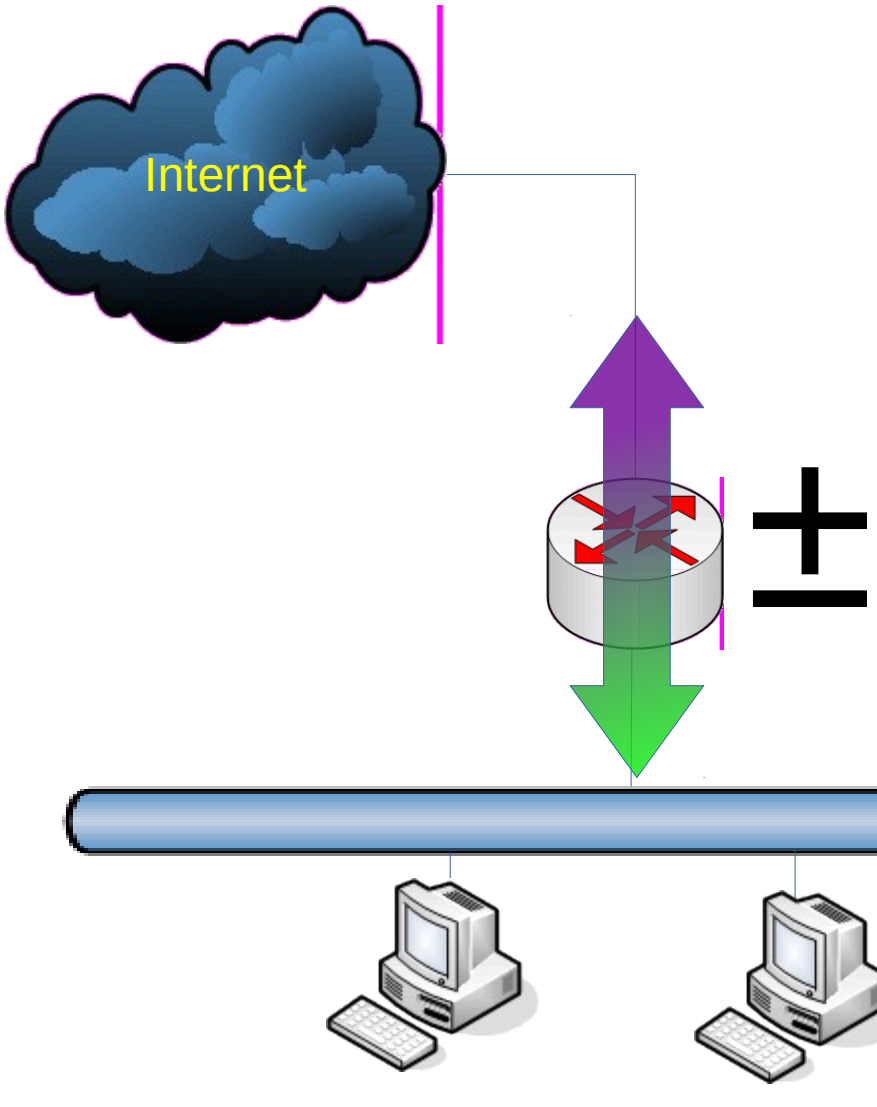
frekvence opakování

- zahlcení ICMP požadavky
- zahlcení otevíráním TCP spojení

stav spojení – stavové filtry

- evidence běžících spojení

Filtr I

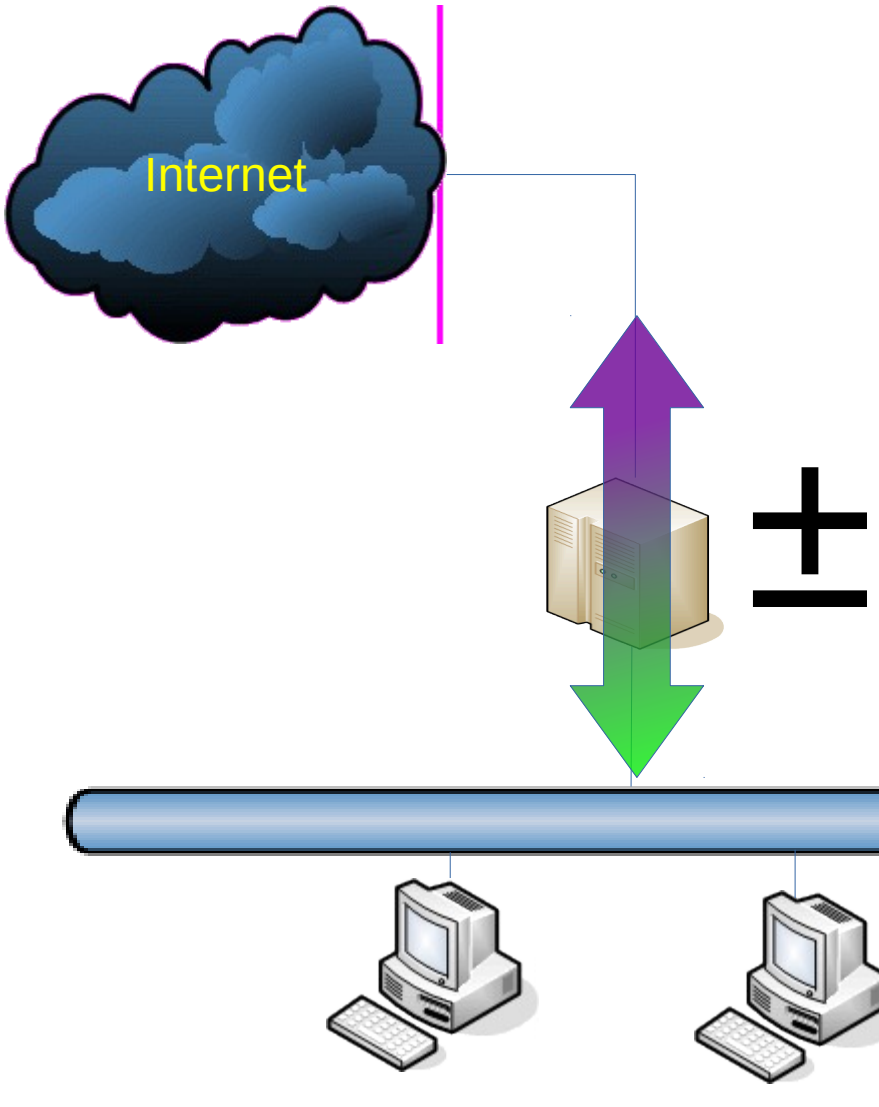


screening router

jednoduchá pravidla

velmi rychlé

Filtr II

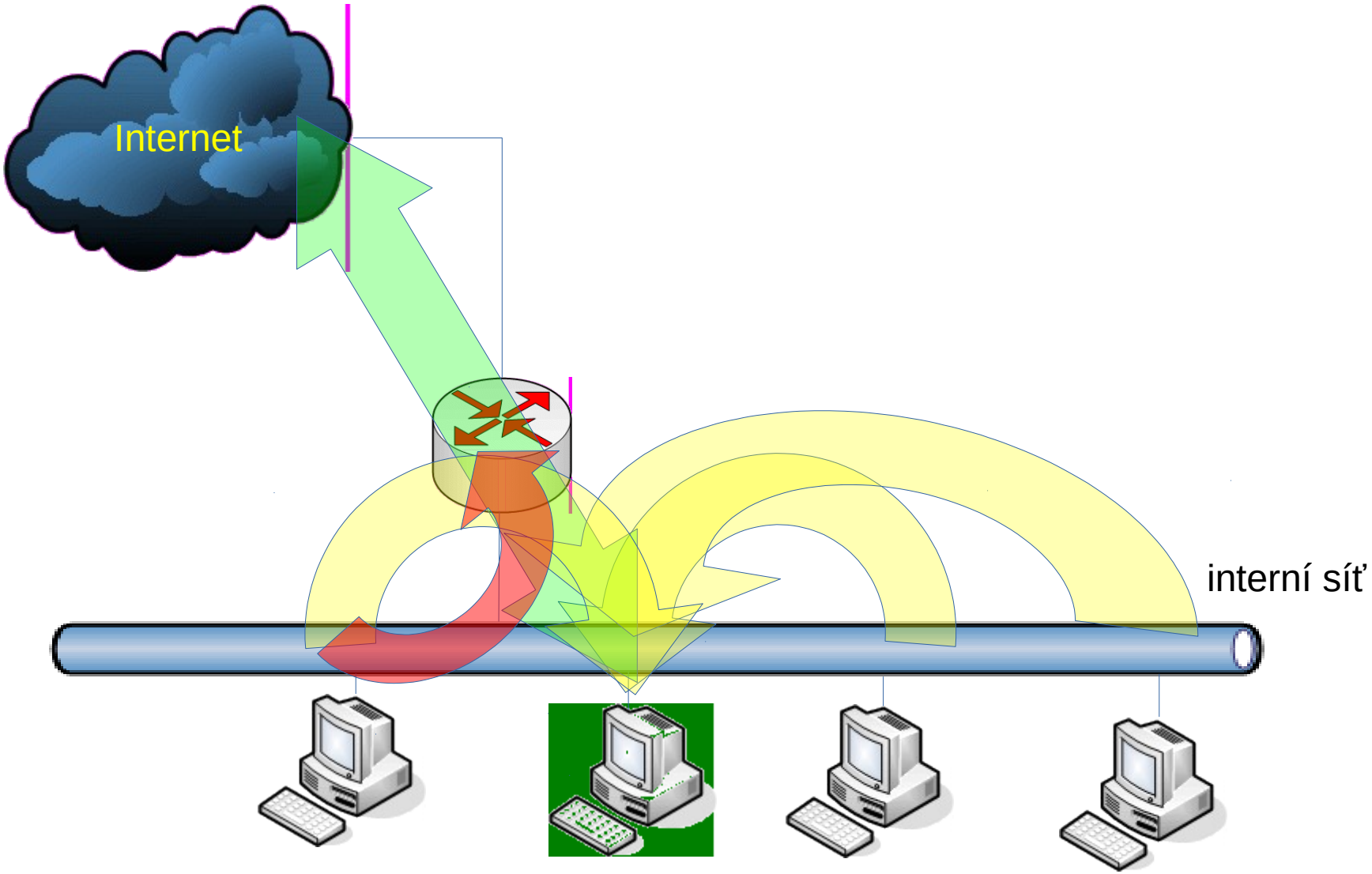


dual-homed host

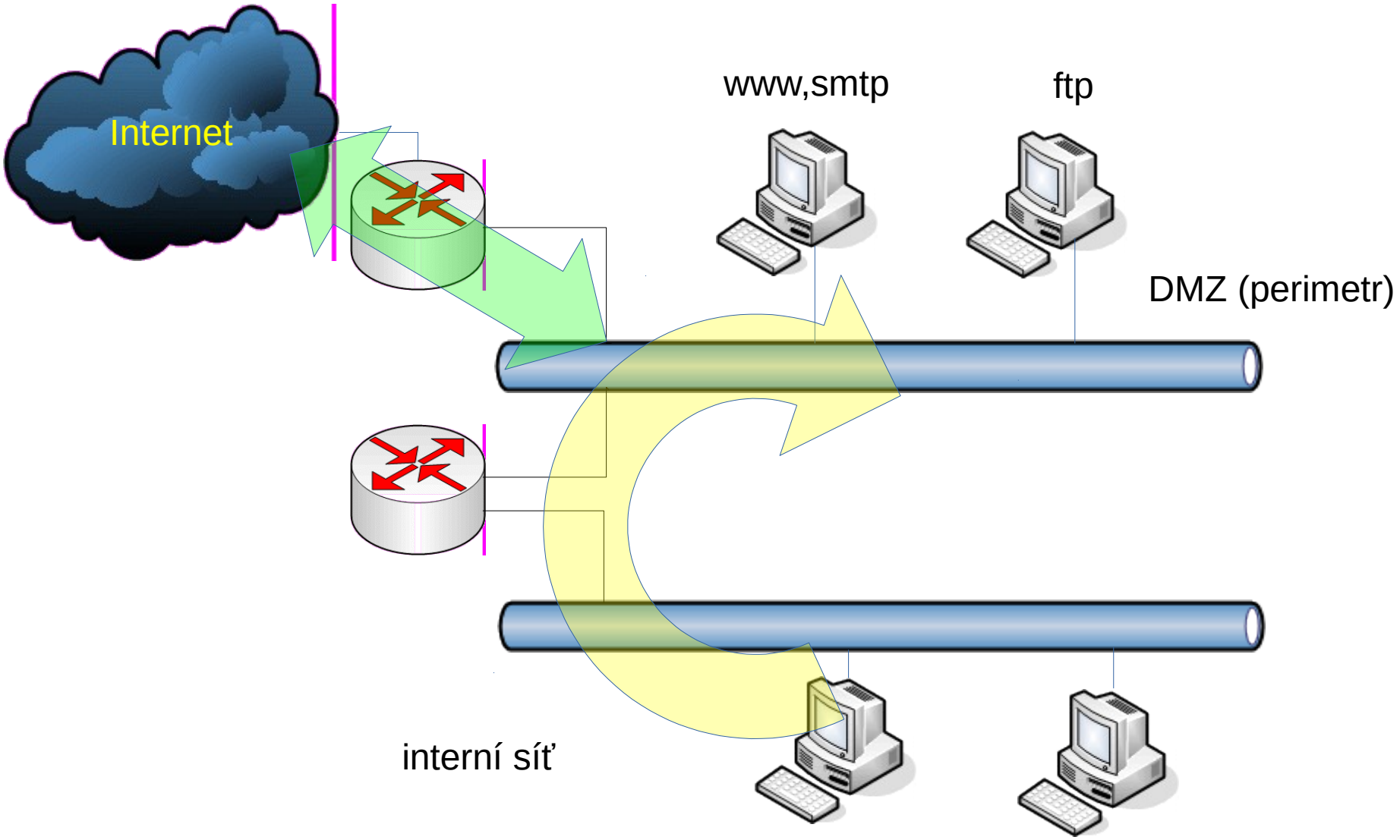
i velmi složitá pravidla

nižší rychlost

Filtr a proxy



Filtry, proxy, DMZ



… a další možné architektury …

Aplikační filtry

rozeberou paket až do 7. vrstvy OSI

např.

- http – kontrola správnosti požadavku (nesnaží-li se klient o cross-site request, či buffer overflow ..)
- ftp – kontrola obsahu souboru
- https – podvržené certifikáty

asi nejznámější – Checkpoint

existují levné nahrážky ..

Unified threat management

nový výraz pro hw/sw, který poskytuje komplexní ochranu před síťovými útoky:

- paketový filtr
- e-mail filtering
- anti-virus
- IDS
- WWW filtering

Literatura

E.D. Zwicky, S. Cooper, D.B. Chapman; Building Internet Firewalls; 2000; O Reilly

Wikipedie

L. Dostálek a kolektiv – Velký průvodce protokoly TCP/IP - bezpečnost