SPS
Bezpečnostní architektura PS

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
- z vnější sítě

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 Y36PSI)

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

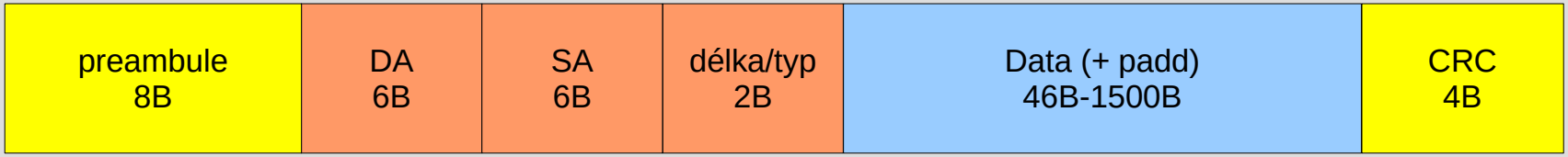
Možnosti firewallu II

- firewall neumožňuje
  - ochranu proti vnitřnímu nepříteli
    - vnitřní útočník už firewall nepřekonává (lze použít vnitřní firewally a host firewally)
    - ochrana proti odeslání dat selhává na USB pamětech
  - nechrání proti spojením mimo firewall
    - dial-up a wifi připojení počítače připojeného do vnitřní sítě
  - ochranu proti neznámým hrozbám
    - např. chybu v http protokolu
  - plnou ochranu proti virům
    - složité rozpoznání dat v komunikaci
    - lze nahradit protivirovou ochranou počítačů
  - automatickou konfiguraci a kontrolu
    - „samo se to nenastaví“
    - špatná konfigurace poskytuje falešný pocit bezpečí

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

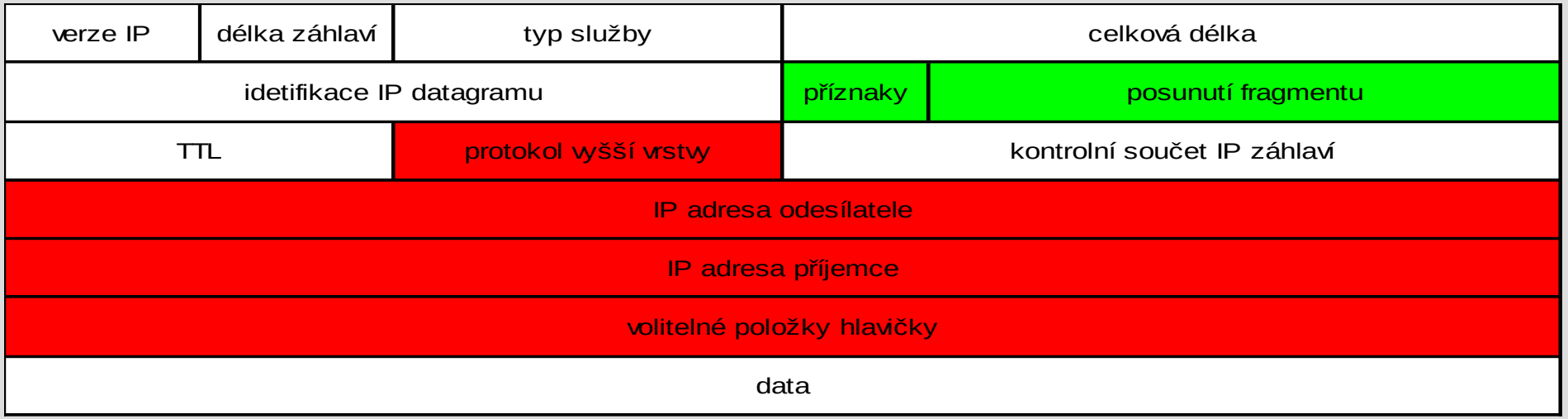
zdrojová MAC adresa
- adresa zdroje
- adresa posledního směrovače

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 …

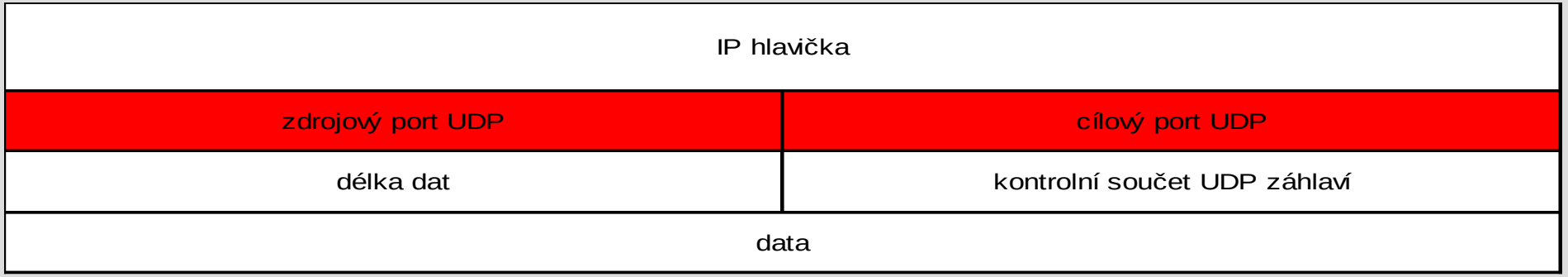
volitelné položky

většinou prázdné, potenciálně nebezpečné

fragmentace

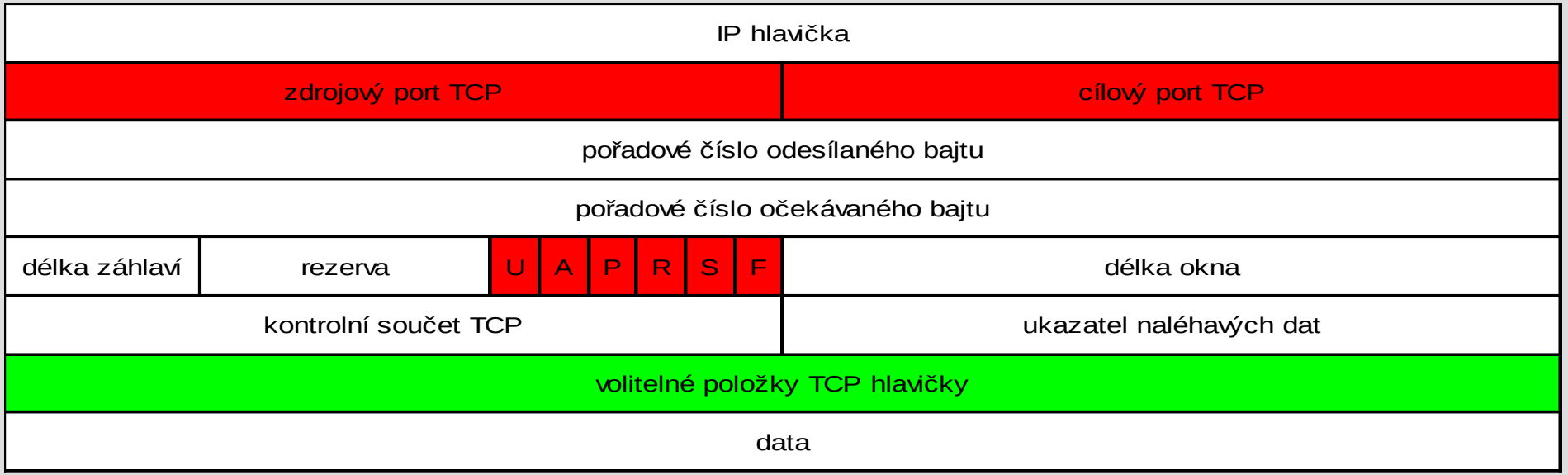
problém při analýze protokolu vyšší vrstvy

Transportní vrstva – UDP



port odesílatele a příjemce
- identifikace služby

Transportní vrstva – TCP



port odesílatele a příjemce

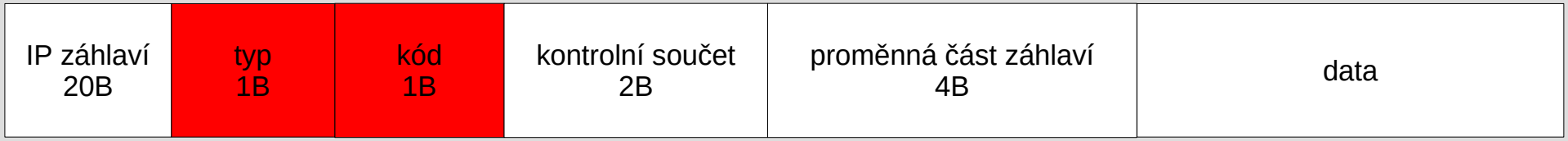
příznaky

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)
časté změny
uzavřené protokoly
šifrování
použití různých portů
…

Další metriky

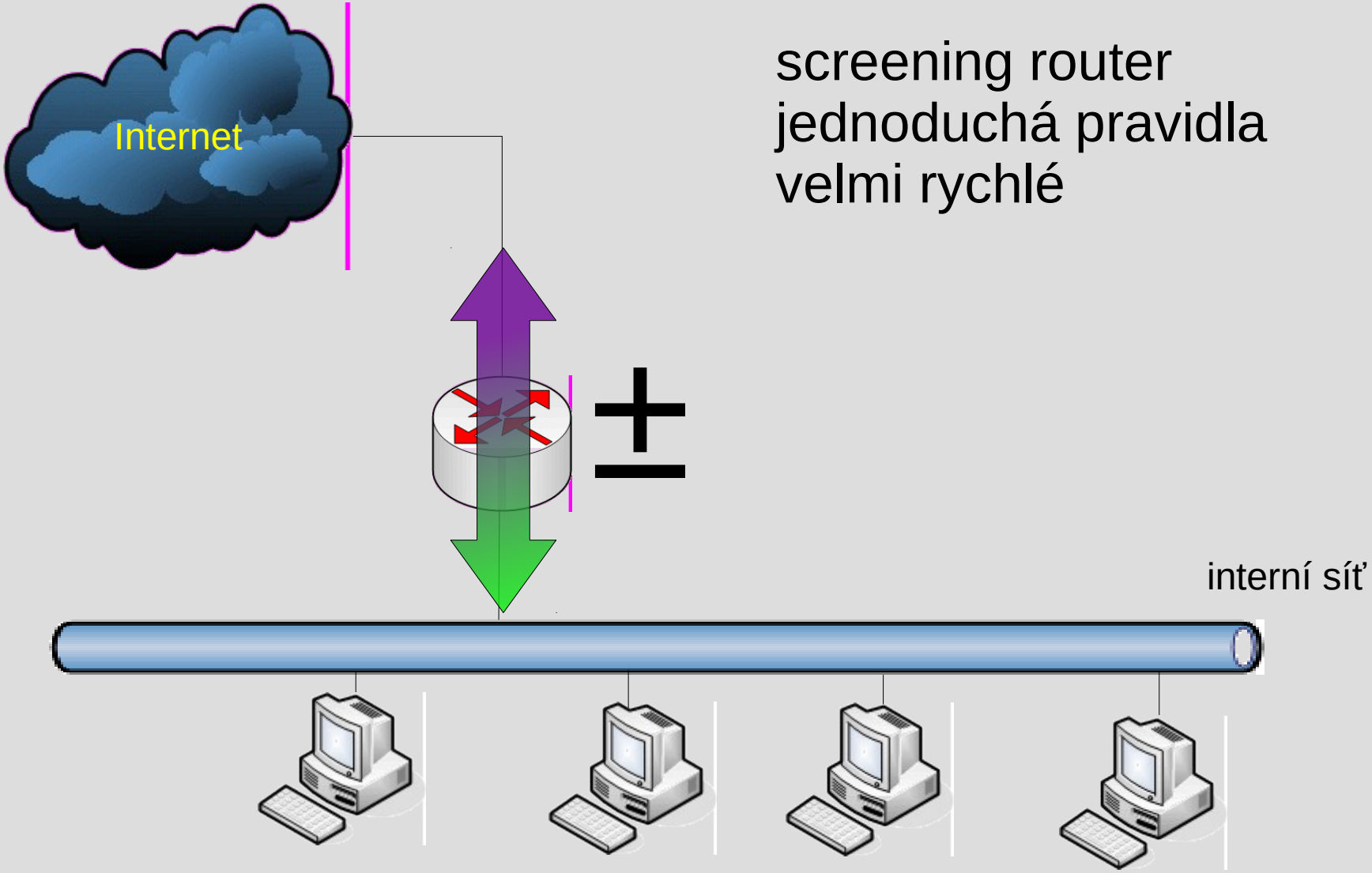
- čas
  - pracovní doba
- autentizovaný uživatel
- frekvence opakování
  - zahlcení ICMP požadavky
  - zahlcení otevíráním TCP spojení
- stav spojení – stavové filtry
  - evidence běžících spojení

Firewall

zařízení pro ochranu sítě
různé typy
- HW – paketový filtr
- HW – dual-homed host
- HW – skupina paketových filtrů, DMZ, proxy
- SW – ochrana koncového uzlu (Win, Linux)

firewall zahrnuje i politiku (nastavení)
složitá konfigurace
složité testování

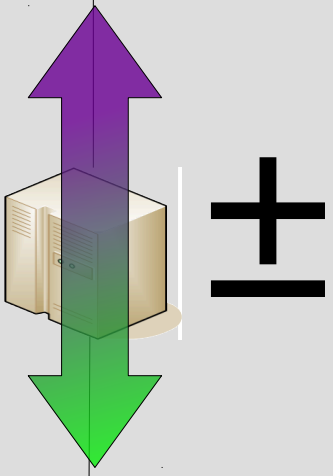
Filtr I



screening router
jednoduchá pravidla
velmi rychlé

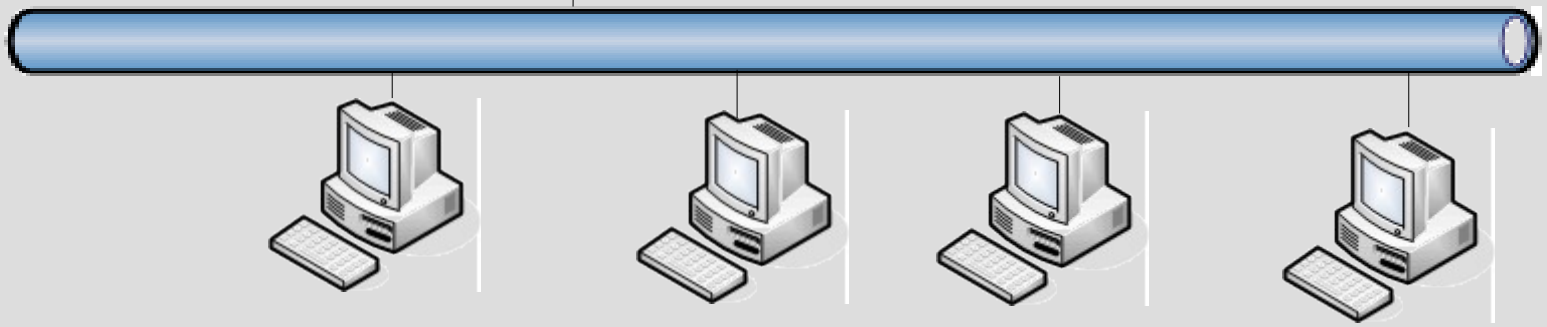
Filtr II

dual-homed host
i velmi složitá pravidla
nižší rychlost

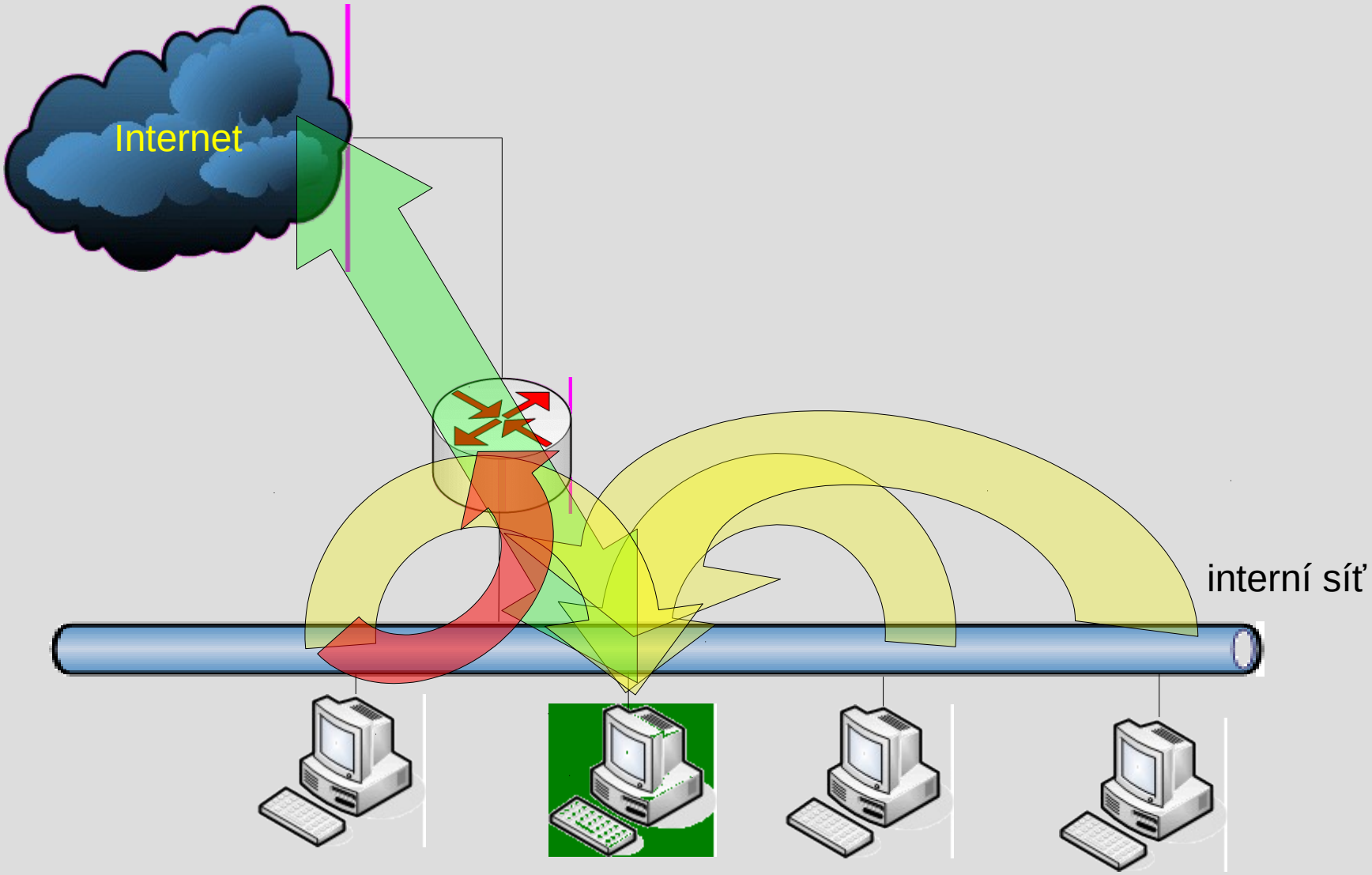


±

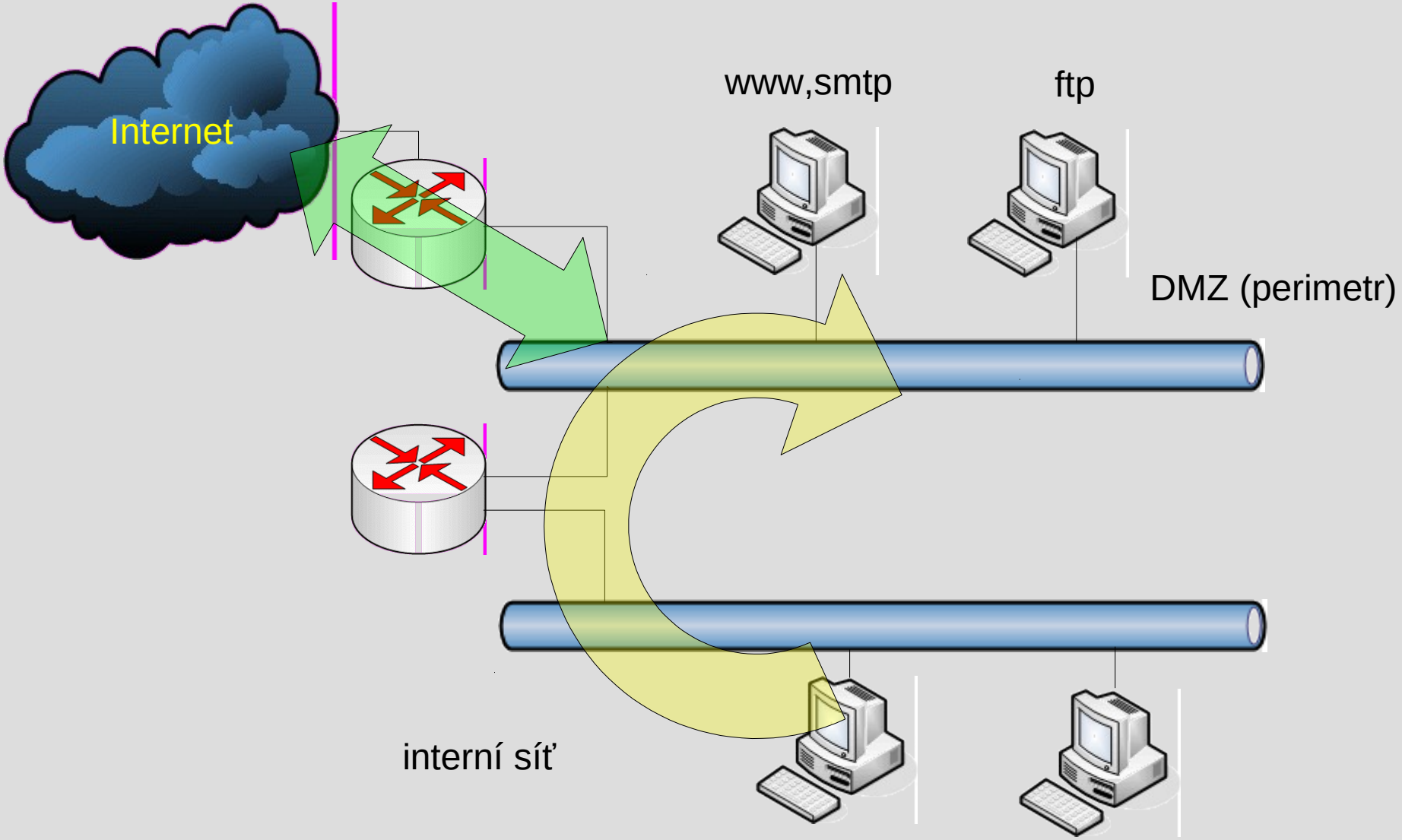
interní síť



Filtr a proxy



Filtry, proxy, DMZ



… a další možné architektury …

Pravidla pro paketové filtry

L3 / L4

výchozí politika (default policy)

- accept, reject, drop, mirror, log (a další)

zpracování pravidel

- sekvenční (cisco ACLs)
- strom (netfilter/iptables)

bezstavová

stavová

Typické PF: Linux/BSD, či jednoduché domácí „router/firewally“

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 ..

Intrusion Detection System

L3-L7 prvek, kontrolující obsah spojení
pasivní: zaznamená útok do deníku (log), notifikuje operátora
reaktivní: automaticky provede akci (zablokování, notifikace...)

Typicky: Snort, Checkpoint SmartDefense, Cisco IDS

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

Firewall – omezení

omezení funkcionality aplikací
omezení možností (=schopností) uživatelů
zálohování – firewall je single point of failure,
  když nejede, nejede biznis..
vysoká dostupnost
problémy s dohledem
SPRÁVA – je nutné mít někoho, kdo tomu
  rozumí
    místní administrátor (zaměstnanec)
    outsourcing (SLA)

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

…
pravidla na cvičení
vzdálené připojení – vpn – jindy
…