NetFlow, monitorování IP toků a bezpečnost sítě

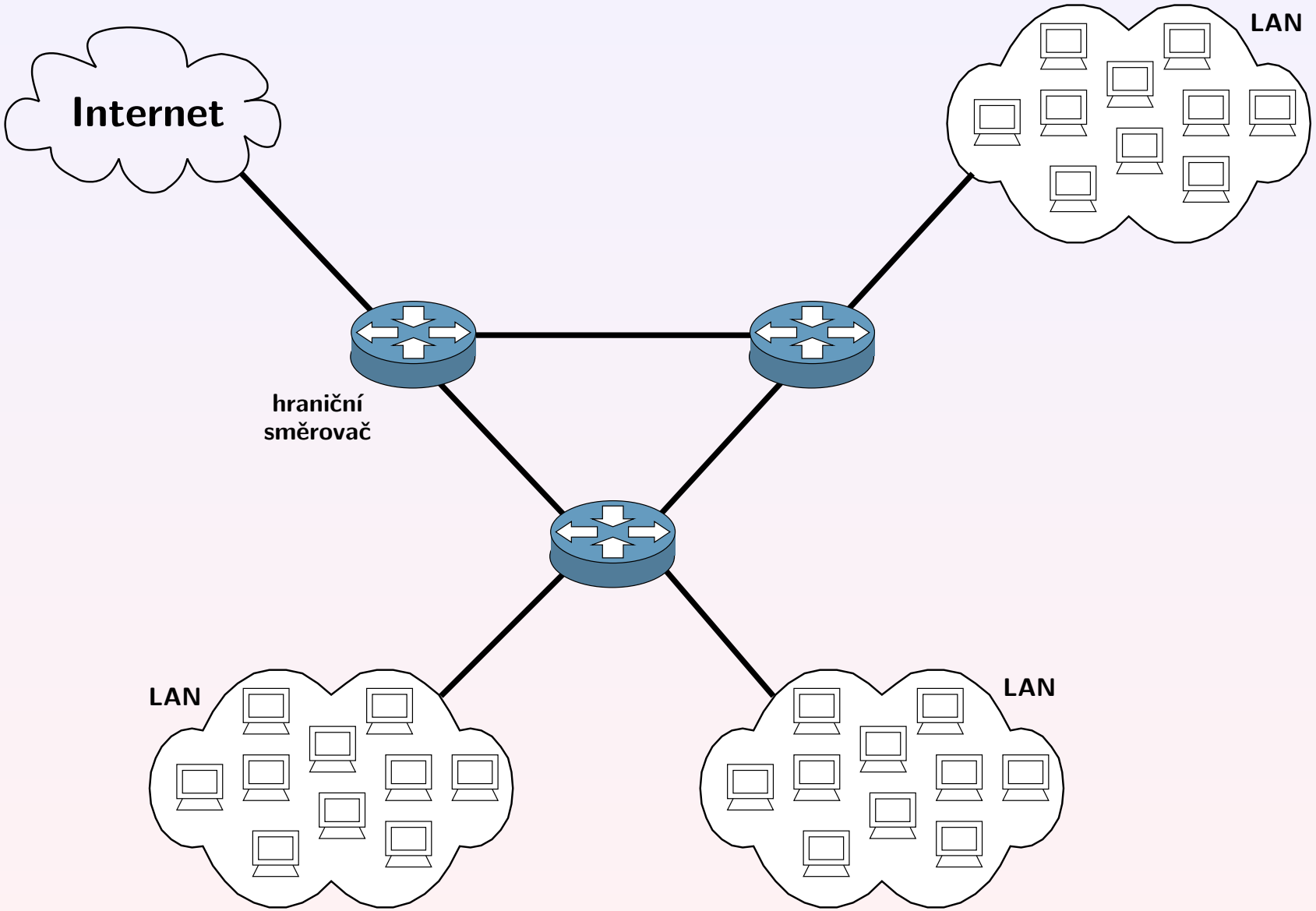
Jan Vykopal

Masarykova univerzita

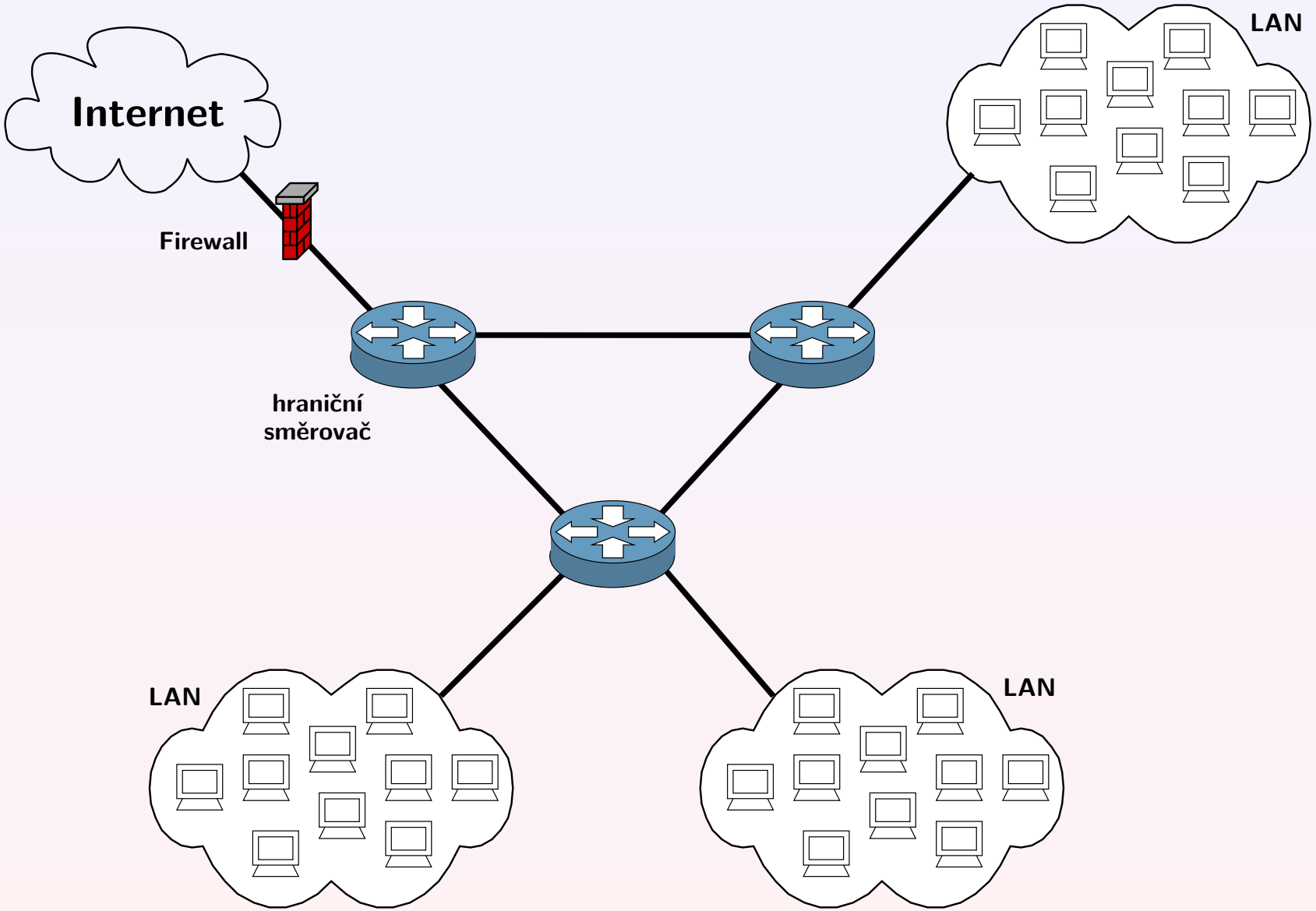
Ústav výpočetní techniky

35. konference EurOpen.CZ – 7. října 2009, Klínovec

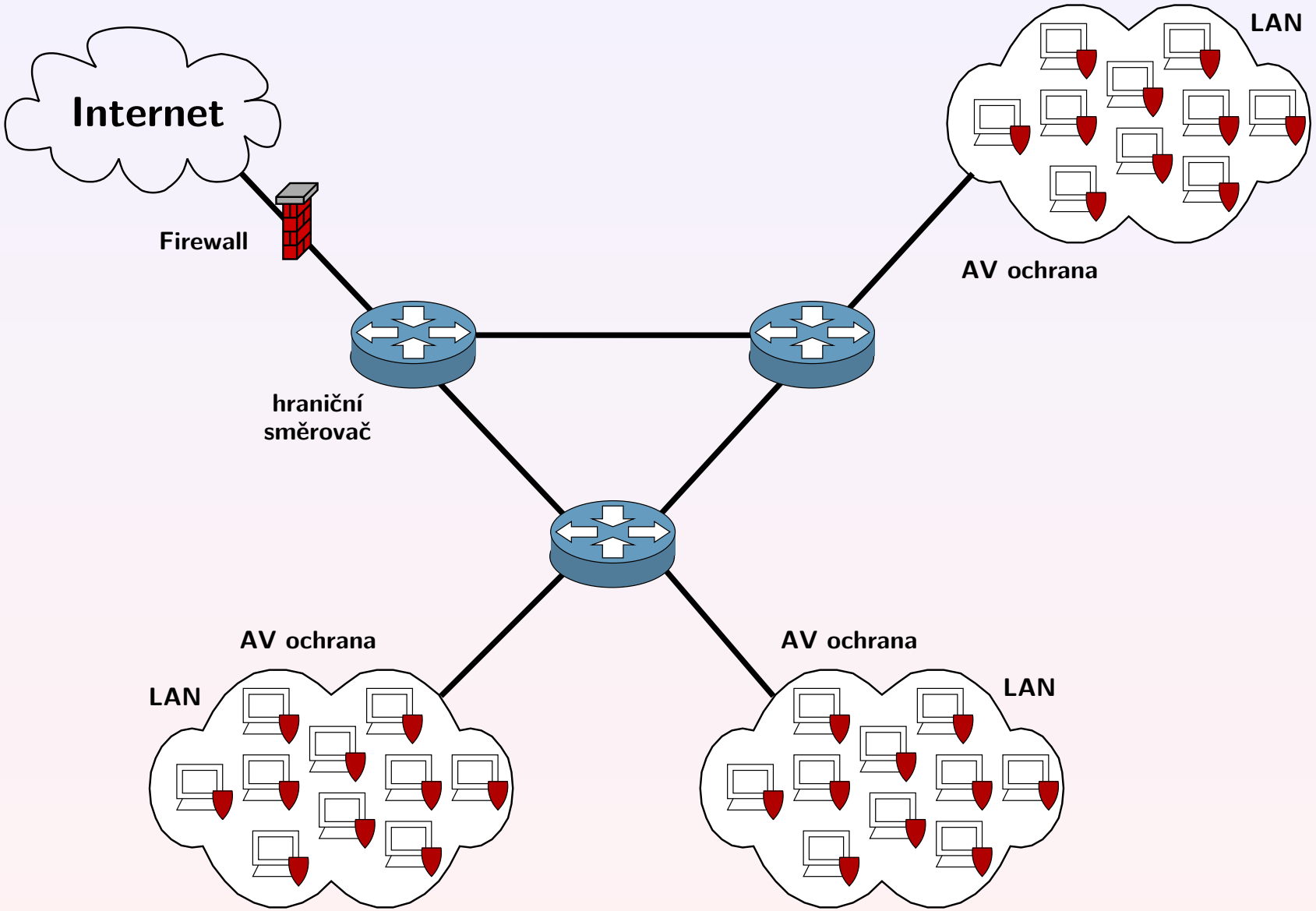
Máte vše pod kontrolou?



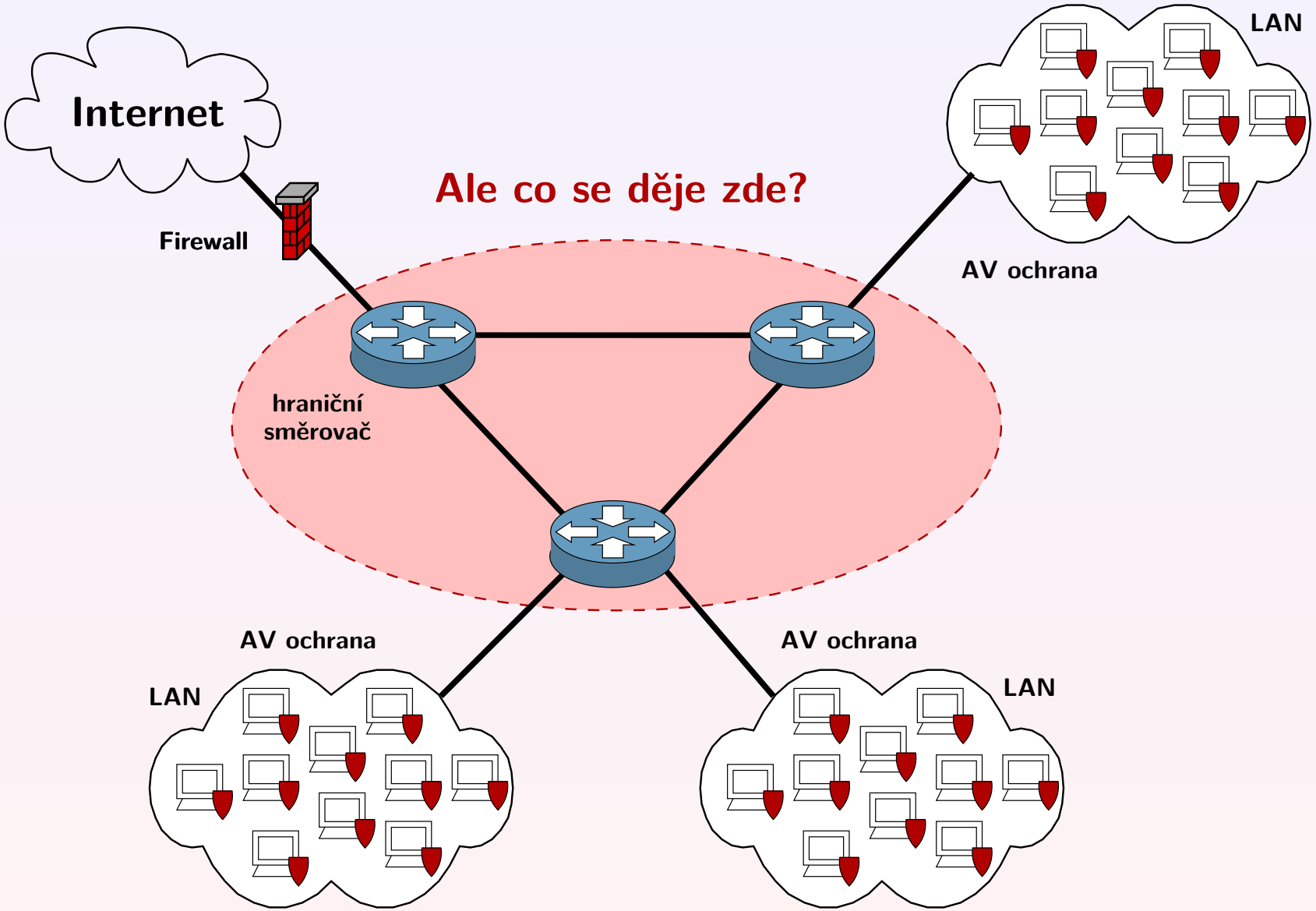
Máte vše pod kontrolou?



Máte vše pod kontrolou?

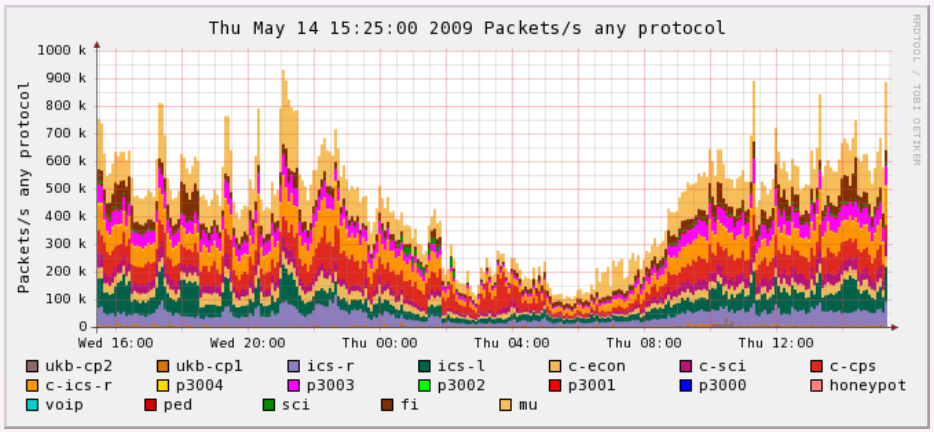


Máte vše pod kontrolou?



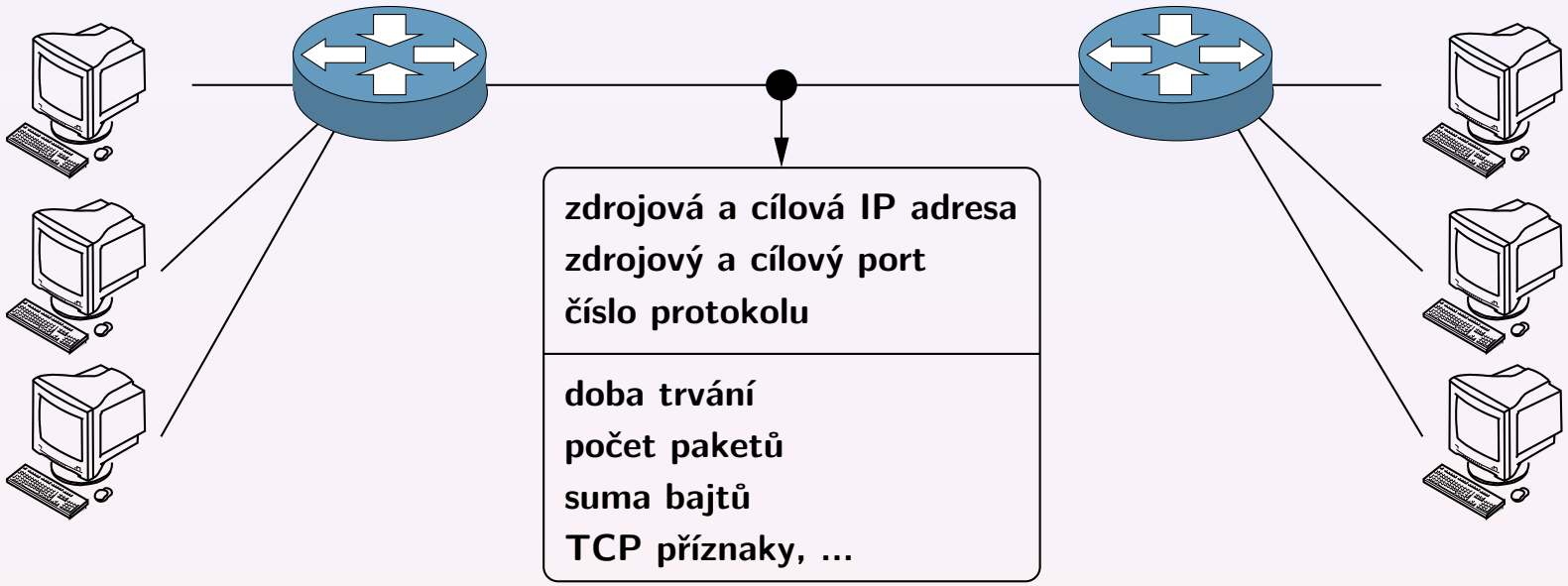
Monitorování toků

- Poskytuje informace o tom kdo, s kým a jak dlouho komunikoval, kolik přenesl dat a jaký protokol použil.
- Vychází z principů technologie NetFlow v5/v9 a IETF IPFIX.
- Umožňuje dlouhodobě sledovat síťový provoz v reálném čase.



Detailní pohled do sítě na základě NetFlow dat.

Princip monitorování toků



Princip monitorování toků


```
Flow start   Duration Proto    Src IP Addr:Port          Dst IP Addr:Port    Flags   Packets  Bytes
09:41:21.763   0.101  TCP     172.16.96.48:15094 ->  209.85.135.147:80      .AP.SF    4       715
```

Princip monitorování toků


```
Flow start   Duration Proto    Src IP Addr:Port          Dst IP Addr:Port   Flags   Packets  Bytes
09:41:21.763   0.101  TCP     172.16.96.48:15094 ->  209.85.135.147:80      .AP.SF    4       715
09:41:21.893   0.031  TCP   209.85.135.147:80    ->    172.16.96.48:15094  .AP.SF    4       1594
```

Dostupná řešení pro monitorování toků

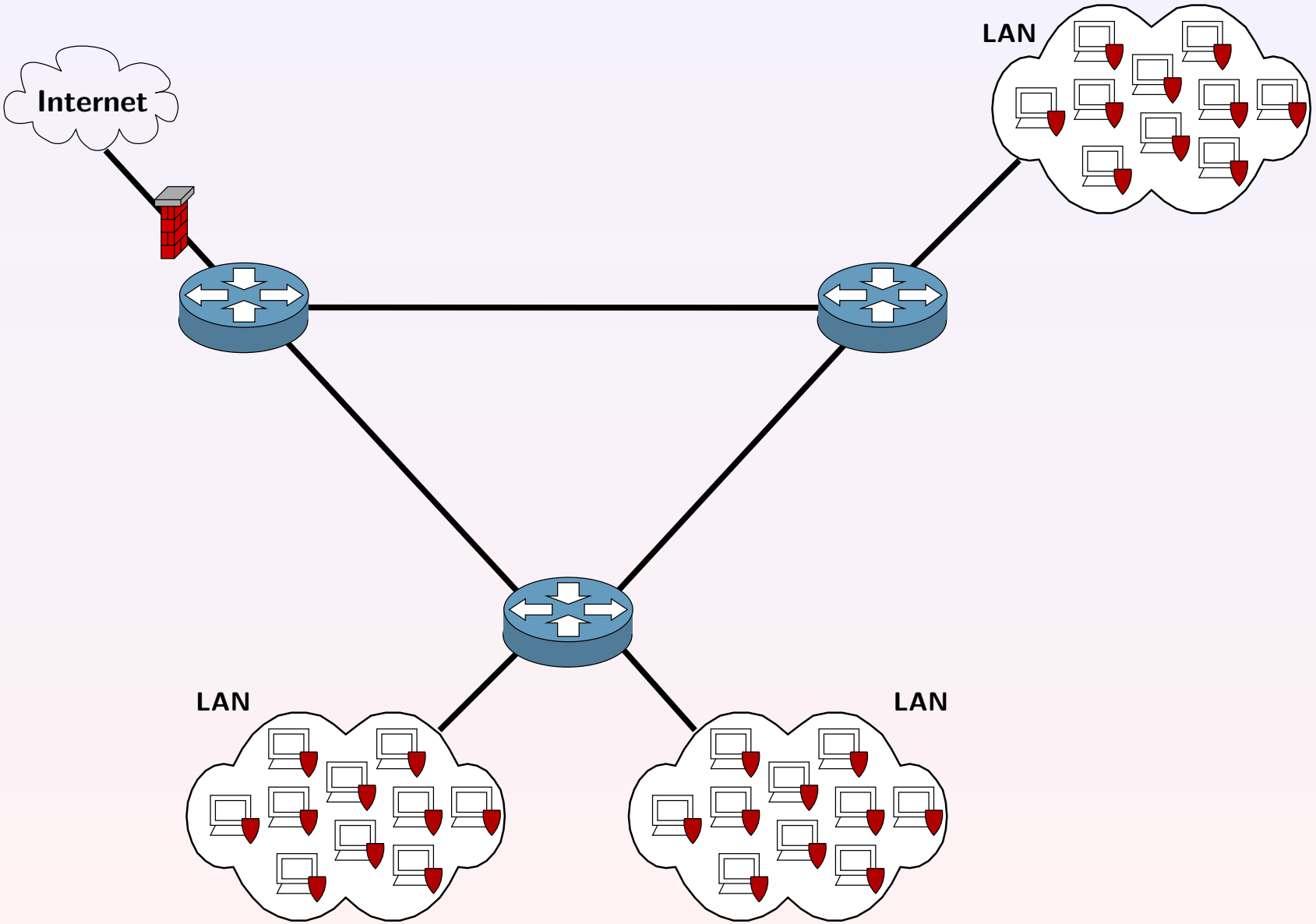
Směrovače – CISCO, Juniper, Enterasys, ...

- Zaneprázdněny směrováním, monitorování toků jako doplněk.
- Monitorování toků není implementované ve všech modelech.
- Fixní umístění, možný cíl útoků.
- Často nezbytné vzorkování, omezené pokročilé technologie.

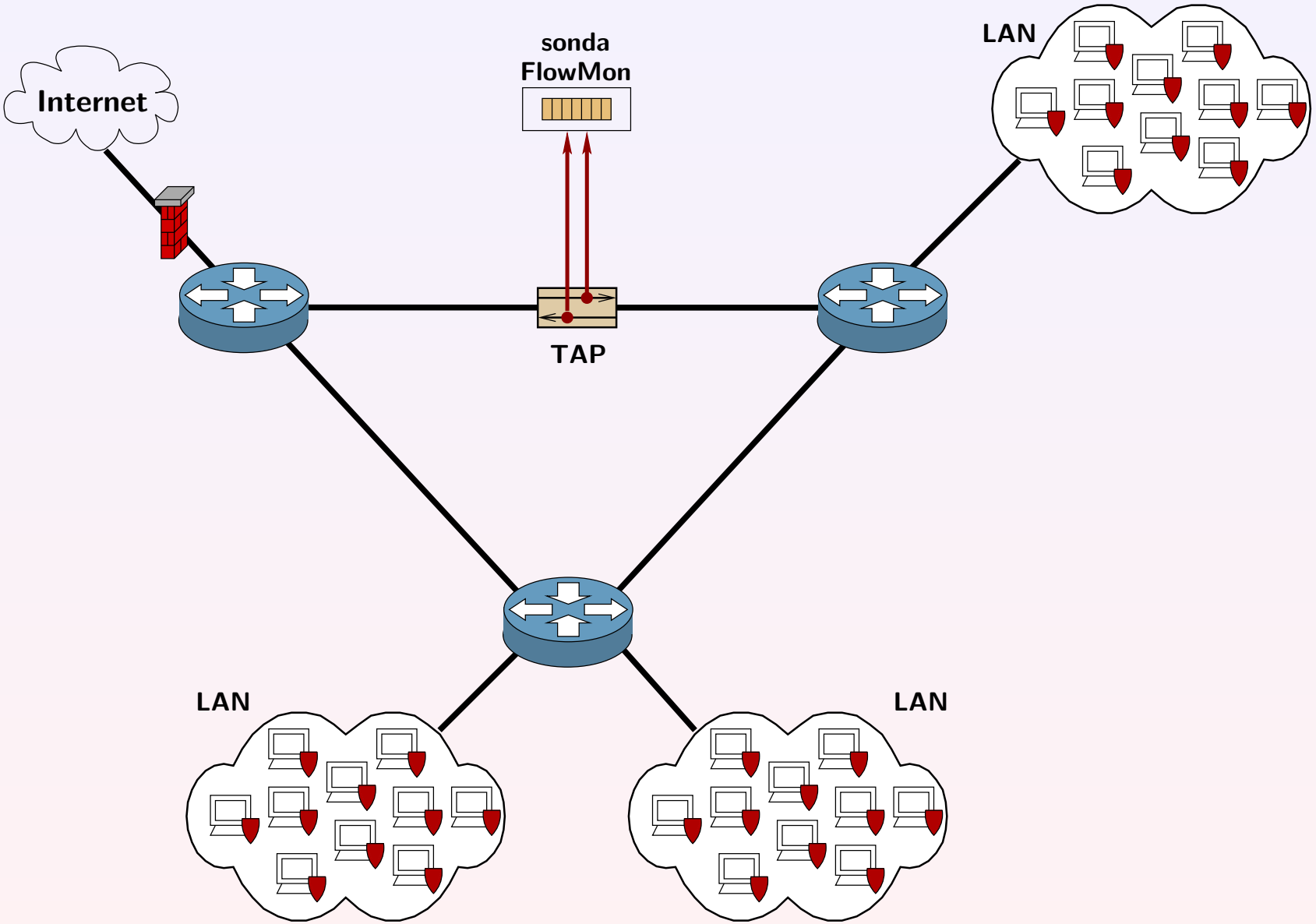
SW NetFlow Sondy – nProbe, fprobe, softflowd, ...

- Založeno na běžném HW – PC a běžných síťových kartách.
- Limitovaný výkon (PCAP, PCI-X) a problémy stability.
- Vyžaduje expertní úpravy a nastavení měřicího systému.
- Zaplňují mezeru kde potřebujeme monitorovat a není čím.

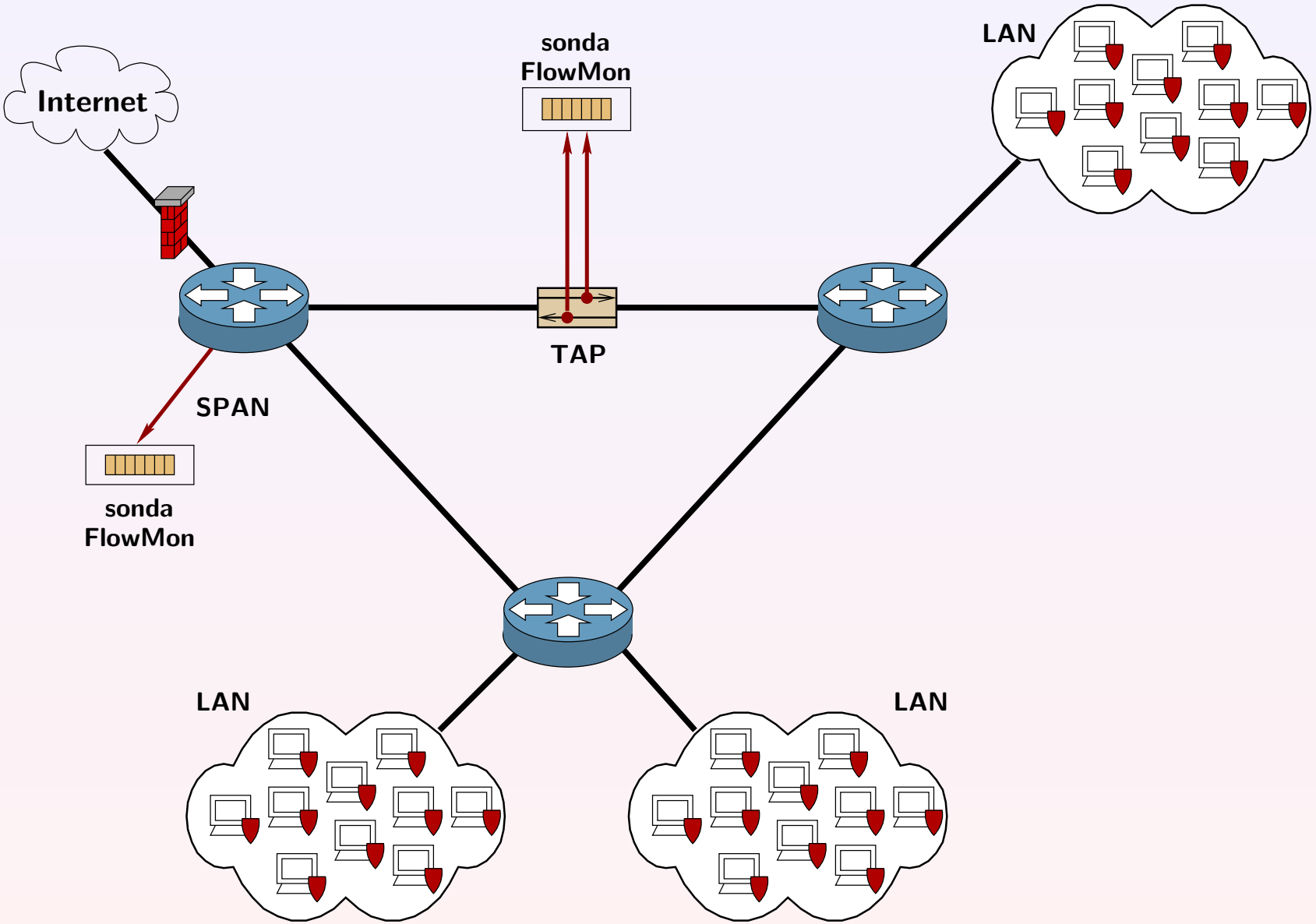
Kam s ním?



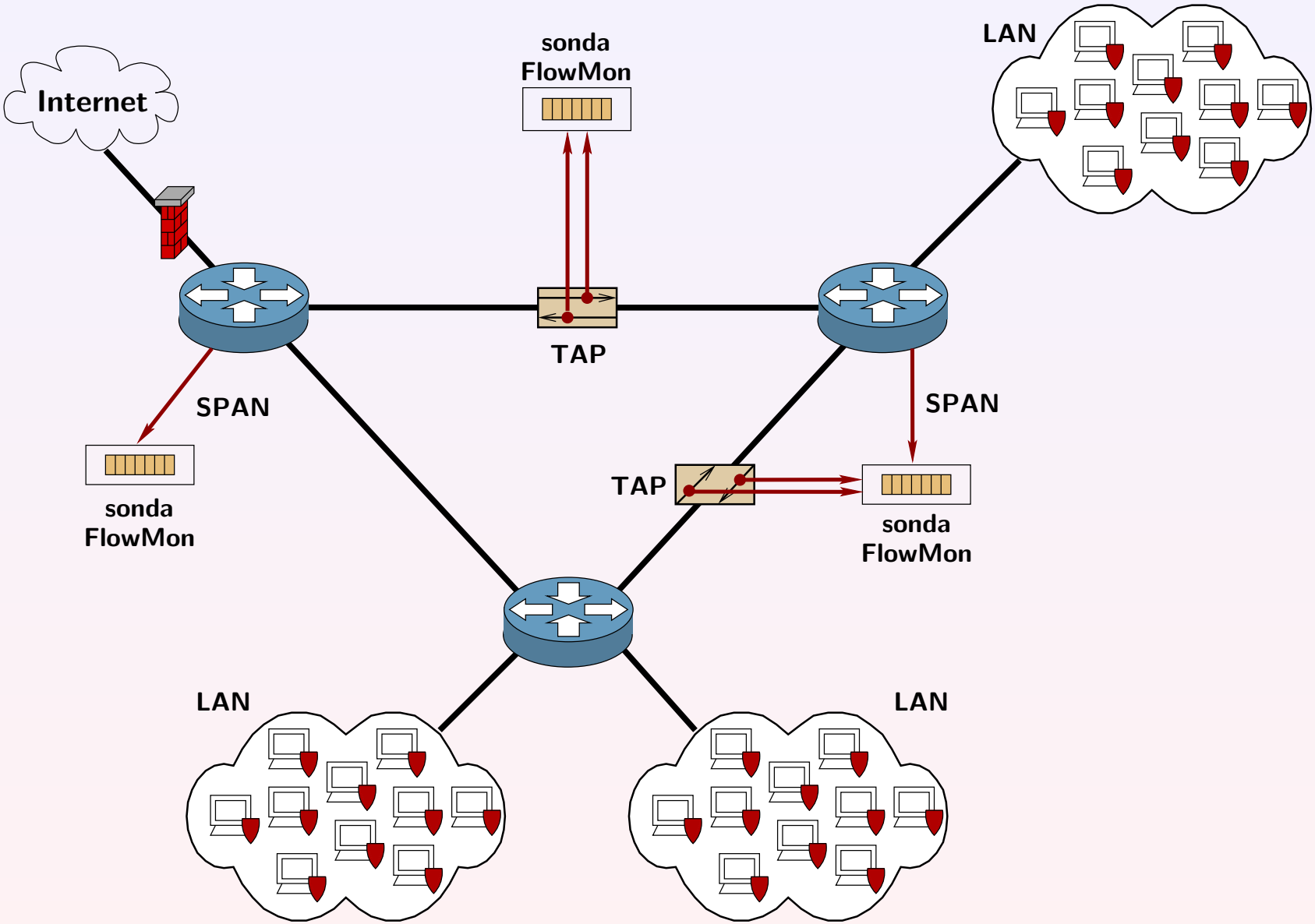
Kam s ním?



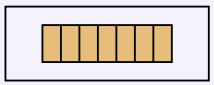
Kam s ním?



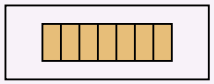
Kam s ním?


Internet
sonda
FlowMon
LAN
TAP
SPAN
SPAN
sonda
FlowMon
TAP
sonda
FlowMon
LAN
LAN

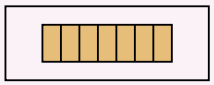
Architektura systému



sonda
FlowMon



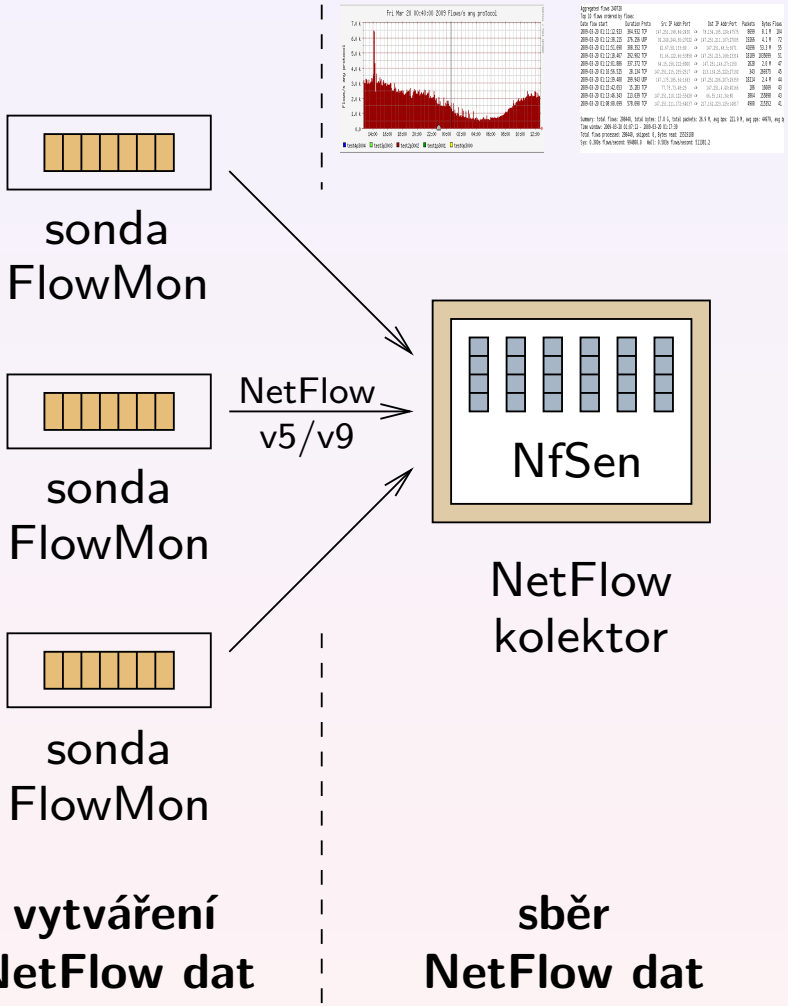
sonda
FlowMon



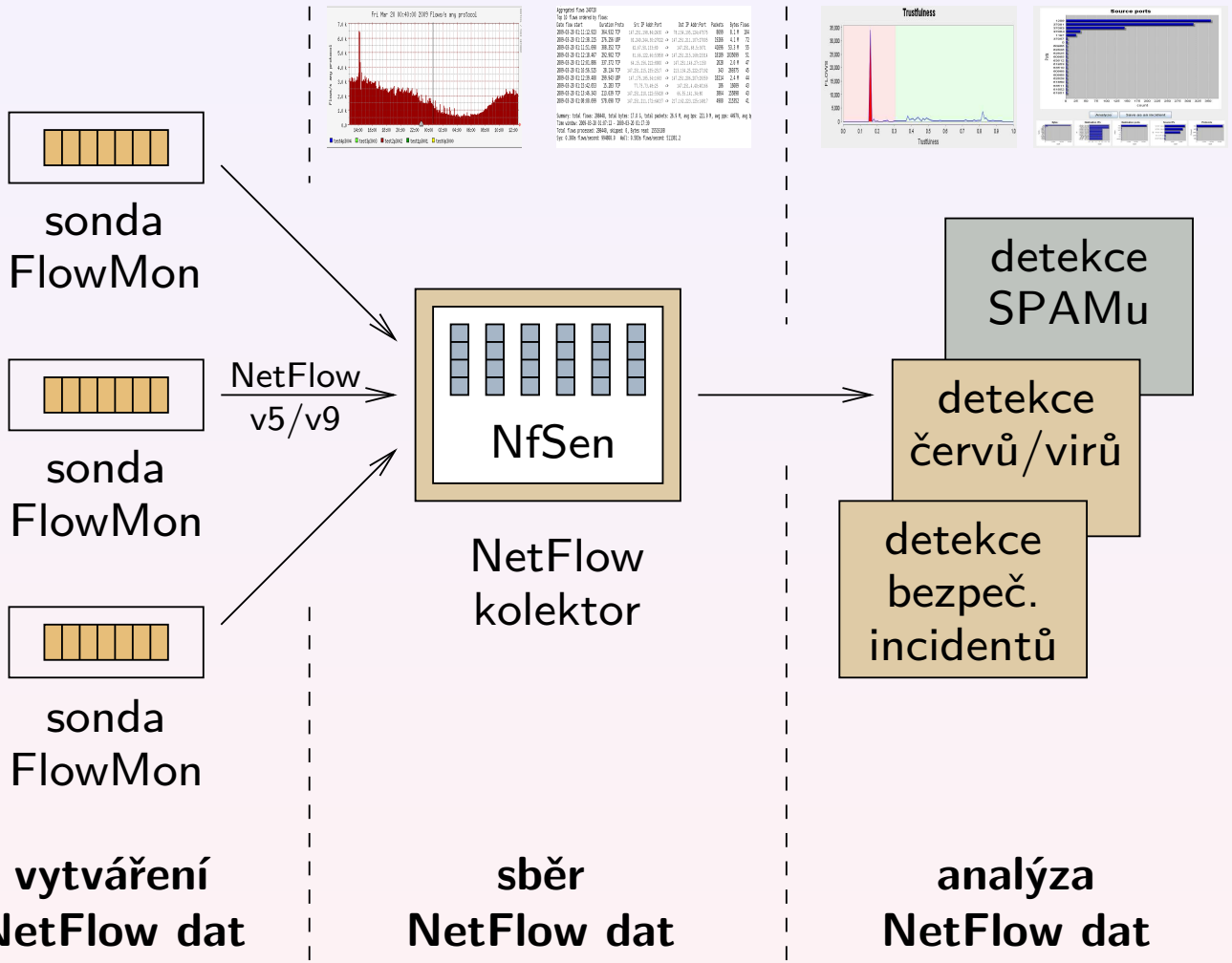
sonda
FlowMon

vytváření
NetFlow dat

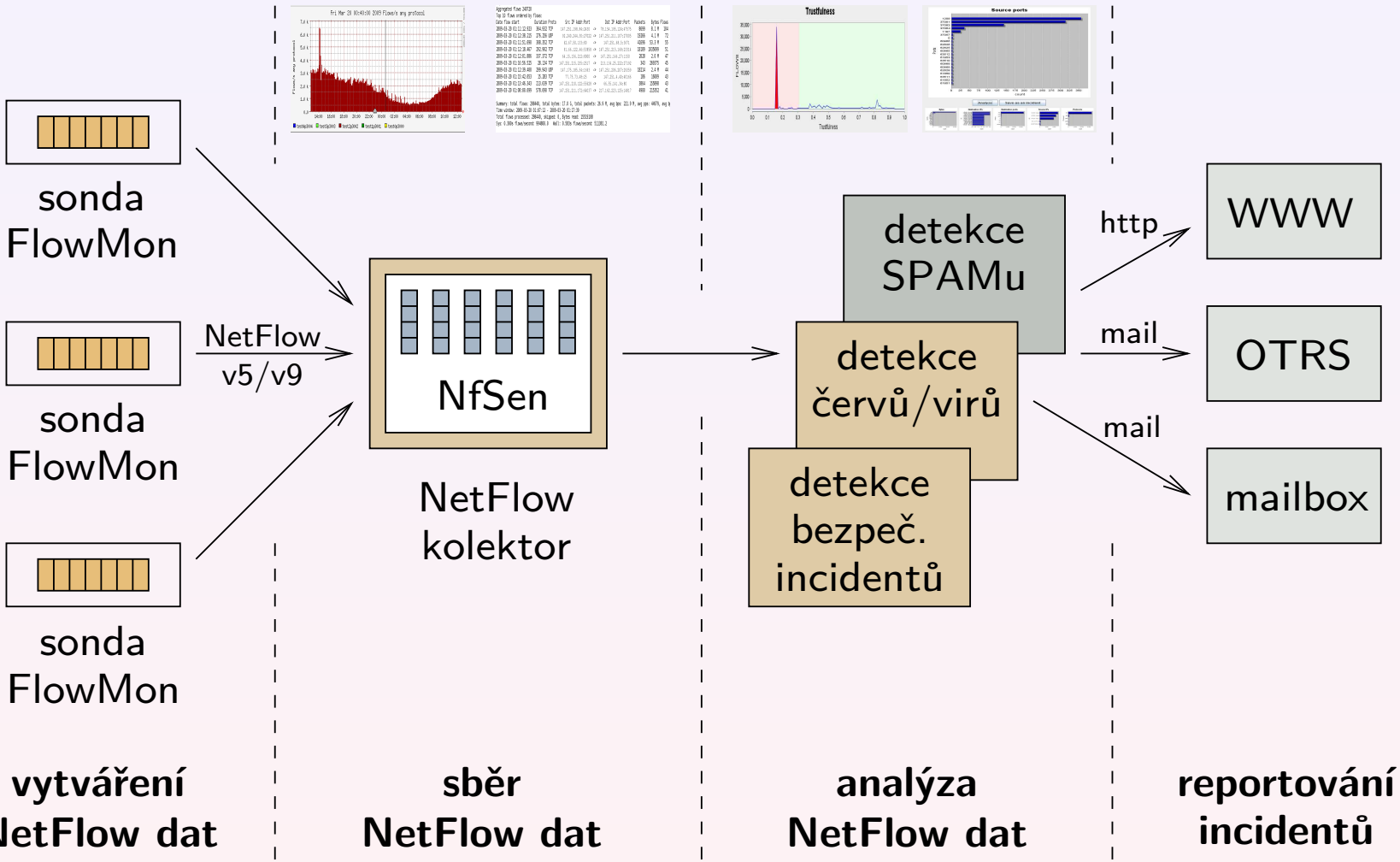
Architektura systému



Architektura systému

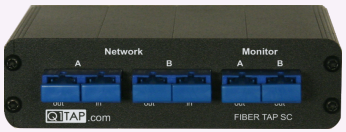


Architektura systému



HW sonda FlowMon

Prostor pro dalšího řečníka. :-)



Optický TAP

Sonda FlowMon karta COMBO6X

Kolektor

Jak funguje SW NetFlow sonda?

Standardní síťovka + aplikace nad *libpcap*

- Extrakce klíčových položek, agregace.
- Export na kolektor ve formátu NetFlow v5/9/IPFIX(?).
- Řešení *out-of-the-box*, ale . . .
- . . . nízká propustnost.
- Open source zástupce aplikace: fprobe.

Akcelerovaný příjem paketů + aplikace nad *libpcap*

- Propustnost 1 Gb/s i na běžném serveru, ale . . .
- . . . vyžaduje zkušenost a ladění.
- Open source zástupce akcelerace: PF_RING.

Jak používáme NetFlow na ÚVT pro MU

Oddělení bezpečnosti počítačové sítě – CSIRT MU

- Sledování dodržování bezpečnostních politik.
- Dohledávání bezpečnostních incidentů.
- Detekce virů a červů v síti MU.
- Monitorování a detekce slovníkových útoků na SSH.
- Monitorování e-mailového provozu (SPAM).
- Monitorování provozu přicházejícího na honeypoty.

„Nebezpečnostní“ využití NetFlow dat

- Statistiky objemů přenášených dat v síti MU.
- Monitorování přístupu k elektronickým zdrojům.
- Podpora pro výzkum a vývoj v oblasti počítačových sítí.

Sledování dodržování bezpečnostních politik

Každý den po půlnoci vyhodnocujeme provoz z předchozího dne.

Každý stroj v sítí MU musí mít reverzní DNS záznam

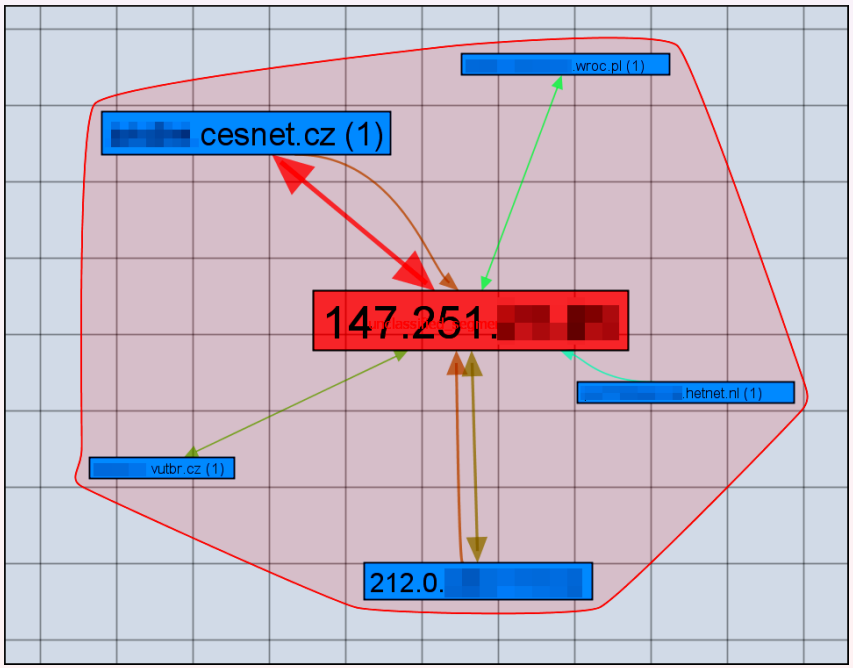
- Patří k „dobrým mravům“ (definováno v RFC).
- IP bez záznamu může ukazovat na zapomenutý stroj (= potenciální slabé místo).

Mail ze sítě MU lze odesílat jen přes vybrané SMTP servery

- Prevence spamu.
- Sledování objemových anomálií v provozu.
- Zachycení neúspěšných spammerů a chyb v konfiguraci.

Inteligentní útoky proti SSH serverům

- Napadení desítek strojů „SSH trojanem“.
- Nezbytná kontrola všech strojů, zda byly napadeny.
- Na síťové úrovni pomohla analýza odchozího provozu.
- NetFlow data ukázala další napadené stroje.
- V případě velkého množství toků napomůže vizualizace pomocí nástroje MyNetScope.

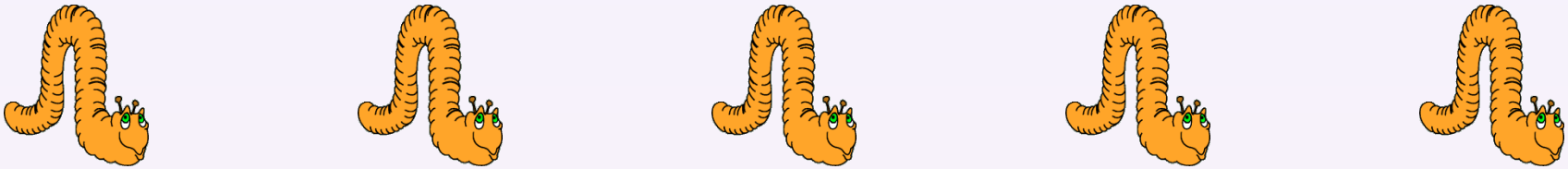


Databáze komunikujících strojů

- NetFlow data poskytují velkou agregaci informace.
- Přesto jde o gigabajty dat denně (duben 2009: 128 GB).
- Není možno klást interaktivní dotazy - vyhodnocení jednoduchého dotazu trvá minuty.
- Často je třeba znát odpověď na otázku: *Komunikoval někdy stroj A.B.C.D s nějakým naším strojem?*
- Databáze komunikujících párů usnadní práci analytiků („první přiblížení“).

Detekce virů a červů v síti MU - I

Viry a červy se snaží šířit dál – skenují další stroje v síti. Chceme ochránit především svoji síť, kterou máme pod kontrolou.



Jak funguje detekce?

- Každých 5 minut procházíme NetFlow data z vnitřních sond.
- Hledáme počítače, které skenují vybrané síťové porty.
- Každý počítač v síti MU patří do určitého segmentu, za který je někdo zodpovědný.
- Mailovací robot zašle správci/studentovi upozornění.
- V případě adres přidělených studentům dojde k zablokování přístupu na 14 dní nebo do vyřešení problému.

Detekce virů a červů v síti MU – II

Zkušenosti z provozu

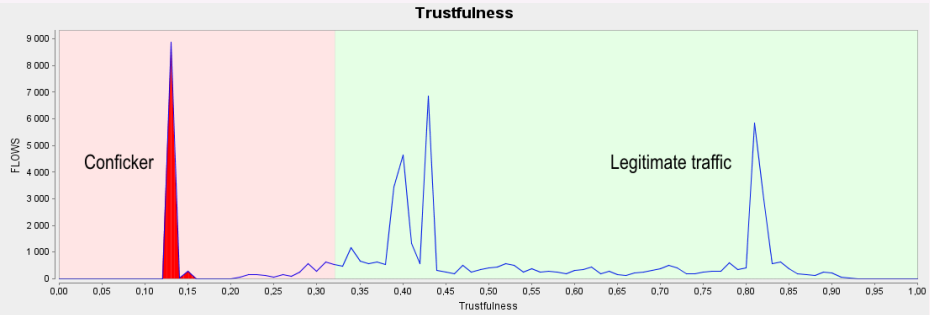
- Za první měsíc provozu (04–05/2009) odesláno přes 100 upozornění.
- Zejména na šíření červu Conficker.
- Nalezeny nové, dosud neznámé formy virů.
- Kladná odezva správců.
- Chladnější odezva studentů, ale „čistší“ síť.
- Automatizované upozorňování šetří čas bezp. analytikům.
- Semestr je už v plném proudu. :-)



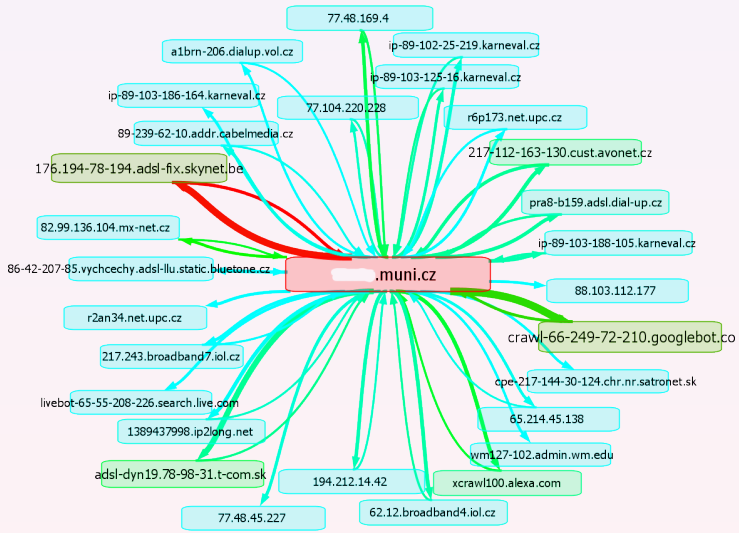


Prostor pro dalšího řečníka č. 2. :-)

- NetFlow data z hardwarově akcelerovaných FlowMon sond.
- Autonomní detekce a vizualizace anomálií.
- Řešitelé ČVUT a MU - zdroj financování U.S. ARMY.
- Vznik spin-off společnosti Cognitive Security s.r.o. na ČVUT.



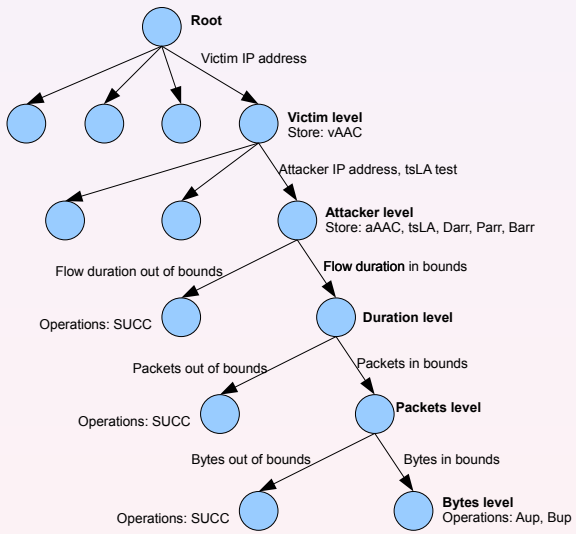
Histogram detekovaných anomálií.



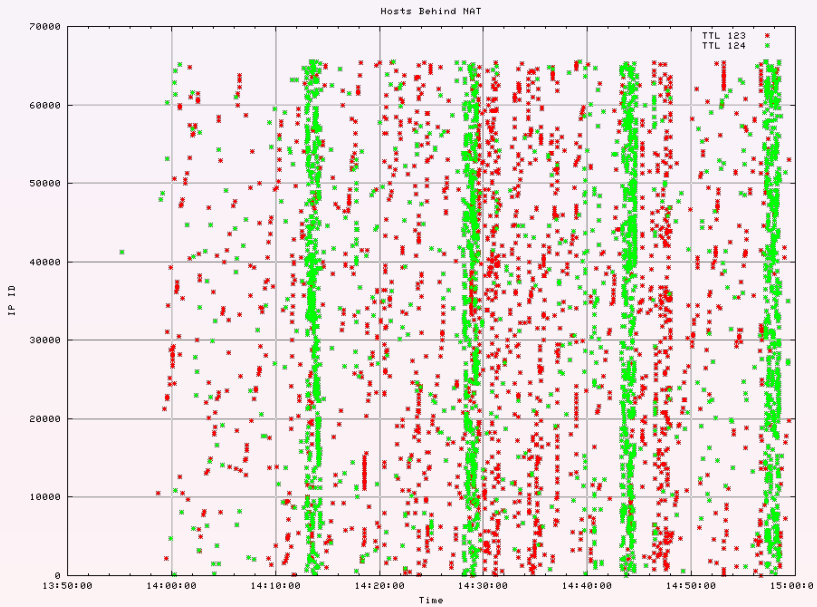
Vizualizace nástrojem NFVis - Mycroft Mind, a.s.

CYBER Grant Ministerstva obrany ČR

- Detekce slovníkových útoků na SSH (MyNetScope).
- Vytváření profilů důležitých strojů MU.
- Detekce infiltrace cizího zařízení v síti (detekce NAT).
- Integrace různých bezpečnostních vrstev se systémy typu CS-MARS a Enterasys DSCC.



Detekce slovníkových útoků dynamický rozhodovací strom.



Počet strojů za NATem.

Inteligentní logovací server

Motivace

- Mnoho heterogenních datových zdrojů: NetFlow sondy, honeypoty, linuxové servery (syslog), blacklisty...
- „Ruční korelace" událostí je velmi namáhavá.

Implementace

- Maximální využití existujících nástrojů (nechceme znovu vynalézat kola).
- Pouze jeden komunikační protokol mezi jednotlivými moduly: široce rozšířený Syslog.
- Budeme implementovat jen jádro (vč. modulu detekce anomálií) a syslogové „adaptéry" pro existující nástroje.

Závěr

NetFlow@MU

- Základní stavební kamen síťové bezpečnosti na MU.
- Vyřešeno: sběr dat, ukládání. V běhu: další zpracování.
- Stavíme na něm další výzkum.

- Nutno spojit s dalšími datovými zdroji (např. v rámci projektu Fondu rozvoje CESNETu), samotné NetFlow není samospasitelné.

Odkazy

Sondy

- **frobe-ng**[1]: http://sourceforge.net/projects/fprobe/
- **nProbe**: http://www.ntop.org/nProbe.html
- **FlowMon**: http://www.invea-tech.com/cs/products/flowmon-probes

Kolektory

- **nfdump**: http://nfdump.sourceforge.net/
- **NfSen**: http://nfsen.sourceforge.net/

[1] Najdete i jako balíček ve svých repozitářích.

Děkuji za pozornost

NetFlow, monitorování IP toků a bezpečnost sítě

Jan Vykopal
vykopal@ics.muni.cz

Masarykova univerzita

Ústav výpočetní techniky