PV210 Bezpečnostní analýza síťového provozu

Základní prvky zabezpečení sítě

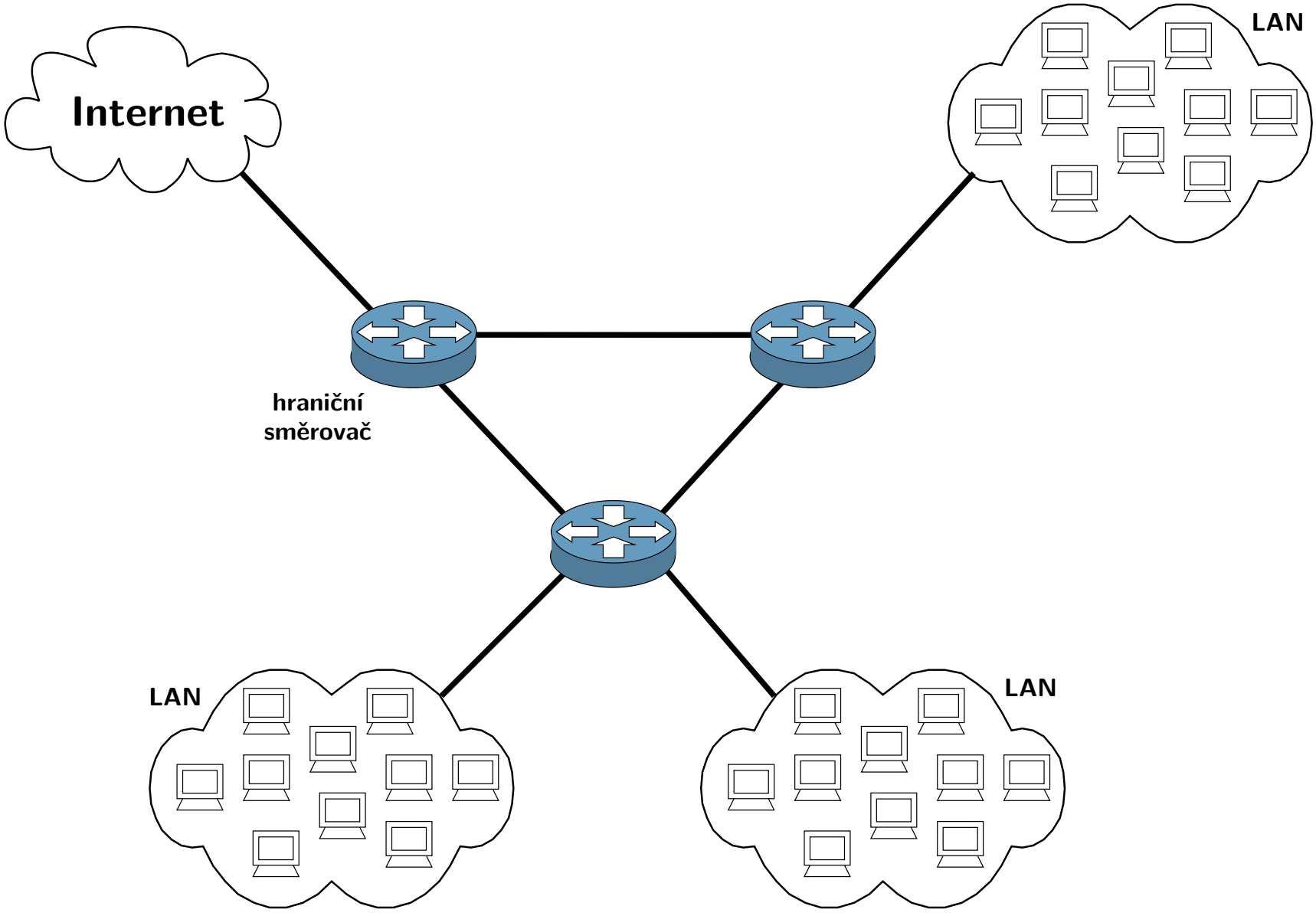
RNDr. Jan Vykopal, Ph.D.

8. 10. 2014

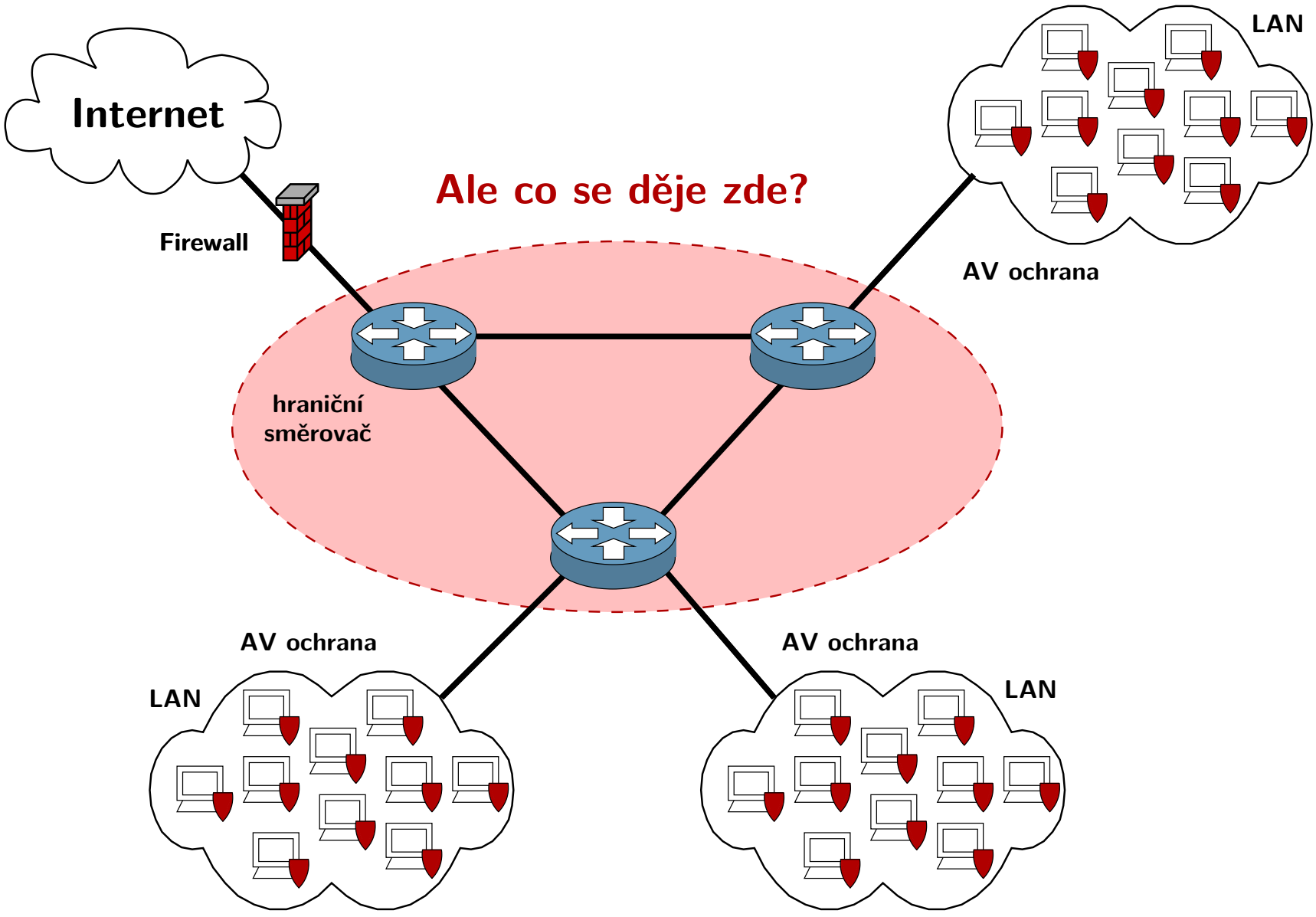
Útoky na počítačové sítě

- Nezohlednění bezpečnosti v návrhu běžných protokolů podmínilo vznik velkého množství útoků napříč všemi síťovými vrstvami.
- Většinou jde o aktivní útoky = obecně je lze detekovat.
- Existuje mnoho volně dostupných nástrojů realizující všemožné útoky.
- Proti mnoha útokům existuje účinná obrana, jiné jsou v principu nevymýtitelné (např. podvržení IP adresy).

Běžná topologie sítě



Kde a čím se bránit útokům? I



Kde a čím se bránit útokům? II

- Firewall – síťový checkpoint.
- Antivirus, antispamový filtr.
- Systém *detekce* průniků, Intrusion Detection System (IDS).
- Systém *prevence* průniků, Intrusion Prevention System (IPS).
- Síťová past, honeypot.

Firewall – základní prvek síťové bezpečnosti

- Dnes neexistuje jednoznačná definice.
- Na počátku (konec 80. let) firewall = paketový filtr.
- Wikipedia:

  A firewall's basic task is to regulate some of the flow of traffic between computer networks of different trust levels.
- Může to být HW, SW nebo i kombinace.
- Do linky zapojen *sériově*.
- Obvykle vymezuje v síti zóny s různou úrovní důvěry: žádná, vysoká a demilitarizovaná zóna (DMZ) – „něco mezi".

- NAT není firewall!

Firewall jako paketový filtr

- Pracuje bez kontextu/stavu, provádí akce (*accept, reject, drop, log, . . .*) na základě klíčových položek jednotlivých paketů.
- Součástí mnoha (i desktopových) operačních systémů nebo jako samostatné zařízení pro celou síť, obvykle pracuje na spojové až transportní vrstvě (např. MAC adresy až TCP porty).
- Bezstavová filtrace je poměrně levná operace.
- Základní učebnicové pravidlo: **blokujte vše**.
- . . . ne vždy to ale jde, nebo to chceme (např. univerzitní síť).
- Zástupci: *iptables* (nejen paketový filtr), *Access Control List* v Cisco IOS a dalších aktivních prvcích

Firewall jako aplikační proxy

- Na rozdíl od paketového filtru „rozumí” i protokolům vyšších vrstev (DNS, HTTP, FTP, . . .).
- Odděluje sítě – dvě spojení místo jednoho, vykoupeno nižší propustností a větší latencí.
- Poprvé se objevil začátkem 90. let, jako cachovací proxy.
- V současnosti se používá pro filtrování provozu, přístup ke zdrojům z vnějšku sítě.
- Zástupce: např. *WinRoute*, *Squid*.
- Dnes se vrací v podobě Web Application Firewall – např. ochrana před XSS, SQL injection a dalšími webovými útoky.

Stavový firewall

- Bere v úvahu kontext, provádí *stateful packet inspection*.
- Pravidla firewallu mohou být podmíněna i stavem spojení (TCP, ale i UDP a ICMP).
- To vyžaduje více zdrojů – např. je nutno udržovat tabulku aktuálních spojení.
- Typicky omezujeme provoz při navázání spojení a propouštíme již existující spojení.
- Lepší volba než paketový filtr (např. účinná obrana proti záplavě TCP SYN paketů).
- Zástupce: opět *iptables* (nejen stavový firewall) a aktivní prvky síťové infrastruktury.

Systém detekce průniků

- Intrusion **Detection** System (IDS).
- První zmínka v roce 1980 (vojenský výzkum USA).
- Pracují na úrovní sítě (Network IDS) nebo hostitele (Host IDS).
- V síti pasivním prvkem.
  Na hostiteli musí být nainstalován SW.
- Většina síťových je bezzubých v případě šifrovaného provozu, ale zase škálují a naopak.

Systém prevence průniků

- Intrusion **Prevention** System (IPS).
- Stejně jako IDS pracují na úrovně sítě (Network IPS) nebo hostitele (Host IPS).
- V síti nejsou pasivním prvkem, jsou zapojeny sériově (podobně jako firewally).
- Kromě detekce dokáži útoku zabránit (proto nelze jednoznačně rozlišit mezi pokročilými firewally a IPS).

Principy detekce průniků

- Hledání vzorů (signature matching)
- Např. hledání výskytu souboru `freepics.exe` v příloze e-mailu.

- Detekce anomálií (anomaly detection)
- *Profil* normálního chování: objem e-mailového provozu je v pracovní době od 8 do 16.30 nejvýše 10 % celkového provozu.

- Stavová analýza protokolů (stateful protocol analysis)
- Odpovědi na překlad doménového jména na adresu musí předcházet korektní požadavek.

Honeypot

- Síťová past na útočníky.
- Vycházíme z předpokladu, že legitimní uživatelé nespadnou do pasti.
- Existuje více druhů členění:
  - nízko- a vysokointeraktivní,
  - serverové a klientské,
  - virtuální,
  - systémy a informace (honeytokeny),
  - vývojové a produkční,
  - ...
- Viz `http://www.honeynet.org/project`.

Shrnutí

- Firewall je základní nástroj implementující bezpečnostní politiku sítě.
- IDS/IPS tvoří další vrstvu ochrany a kontroly.
- Honeypoty jsou módním ale v praxi použitelným konceptem (eliminují falešné poplachy).

Další literatura

- K. Scarfone, P. Hoffman: *Guidelines on Firewalls and Firewall Policy*
  `http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf`
- K. Scarfone, P. Mell: *Guide to Intrusion Detection and Prevention Systems (IDPS)*. Recommendations of the National Institute of Standards and Technology, 2012.
  `http://csrc.nist.gov/publications/drafts/800-94-rev1/draft_sp800-94-rev1.pdf`
- N. Provos, T. Holz: *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*. Addison-Wesley, 2007.

Zadání 1. úkolu

Viz interaktivní osnova v ISu:
`https://is.muni.cz/auth/el/1433/podzim2014/PV210/index.qwarp`
První úkol – hledání útoku v PCAPu (Wireshark)