POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY
FAKULTA BEZPEČNOSTNÍHO MANAGEMENTU

DMZ
z pohledu akademické sféry

Doc. RNDr. Josef POŽÁR, CSc. - děkan
19. 3. 2013

OBSAH

- **Úvod**
- **Firewall a DMZ**
- **Modelové topologie DMZ**
- **Nejčastější chyby DMZ**
- **Závěr**

Firewall **- je síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení, definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje**

Router **– klasický směrovač, obsluhující, oddělující, propojující síťová rozhraní (mezi síťovými vrstvami)**

Paketový filtr **– služba je na Firewallu i routeru (např. IPTABLES)**

Aplikační brány **(gateway, proxy firewally)**

Stavové paketové filtry **- ukládají informace o povolených spojeních, které pak mohou využít při rozhodování, zda procházející pakety patří do již povoleného spojení a mohou být propuštěny, nebo zda musí znovu projít rozhodovacím procesem.**

Demilitarizovaná zóna *(DMZ)*

speciální segment lokální sítě vyhrazený pro servery, které jsou zpřístupněné z Internetu. Z tohoto segmentu není povolen přístup do lokální sítě — v případě napadení serveru v demilitarizované zóně nemůže útočník napadnout další servery a počítače v lokální síti. (FTP, DNS, www server,

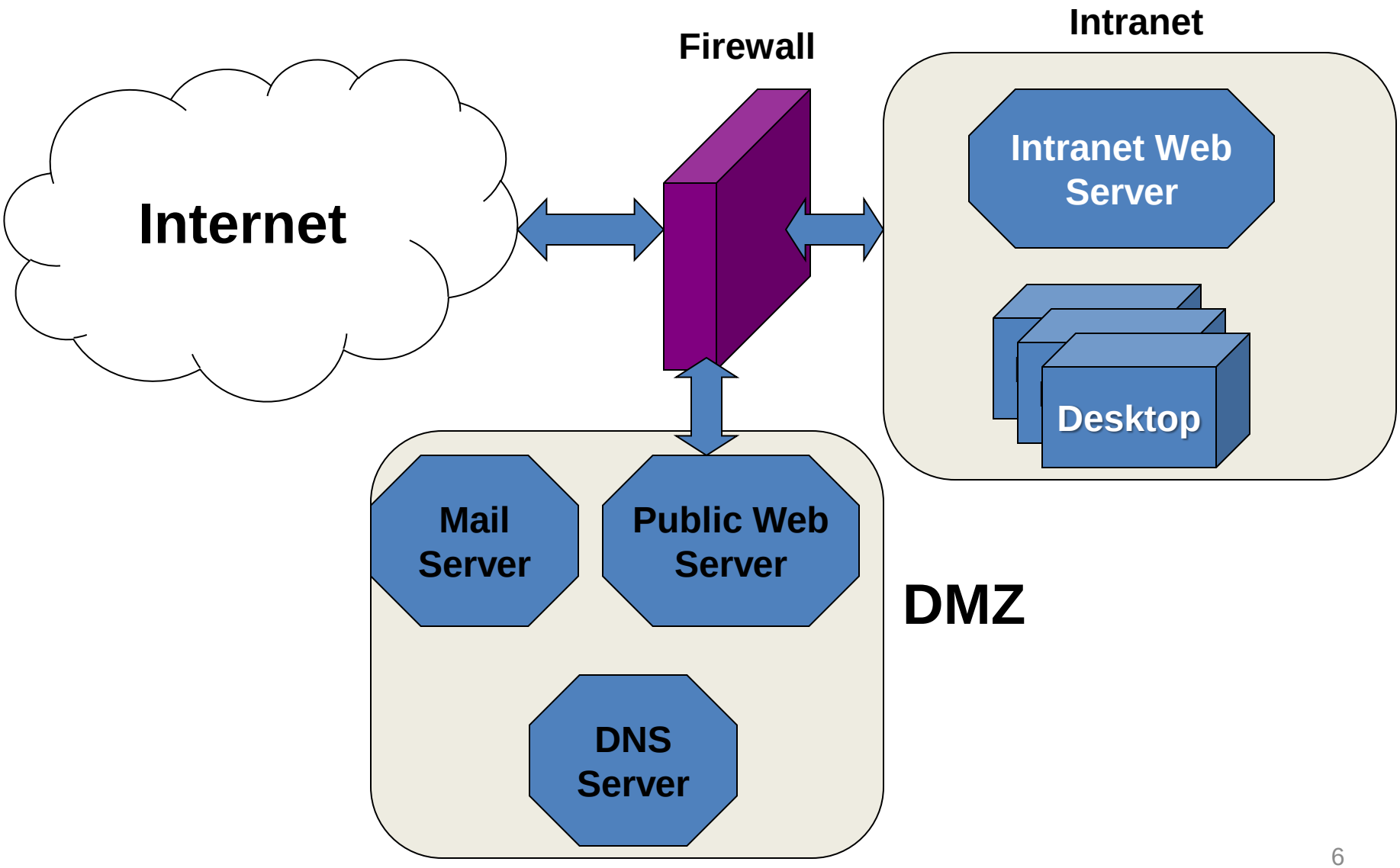
Firewall **se většinou vytváří podle pravidla, že "co není výslovně dovoleno, je zakázáno". Lze jej samozřejmě vytvářet i opačně, tedy "co není zakázáno, je dovoleno", ale první varianta bývá většinou bezpečnější.**

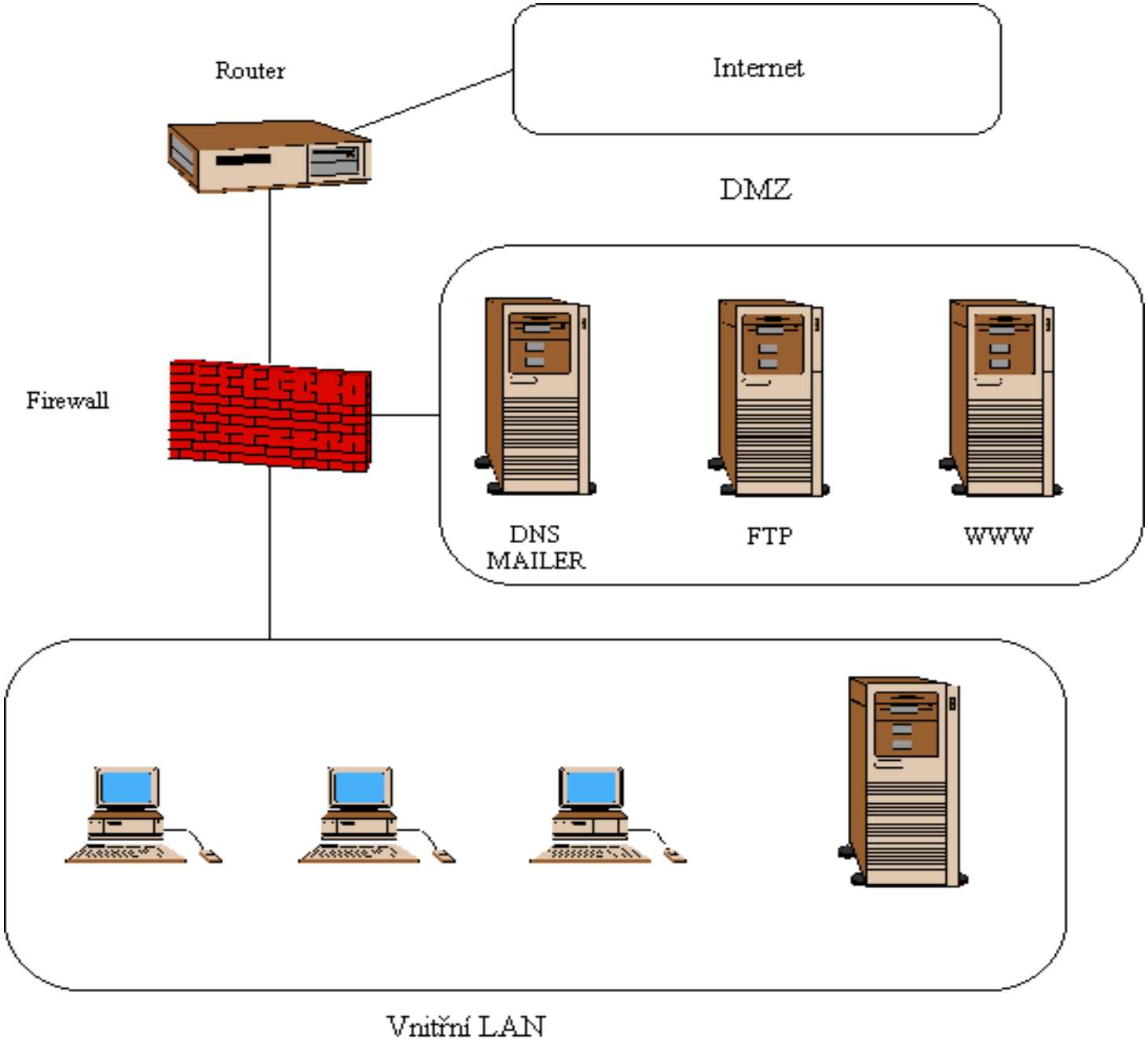
Pravidla server umístěný v demilitarizované zóně. Demilitarizovaná zóna je připojená k rozhraní *DMZ* zařazeného do skupiny *Ostatní rozhraní.*

***Pravidla DMZ*:**

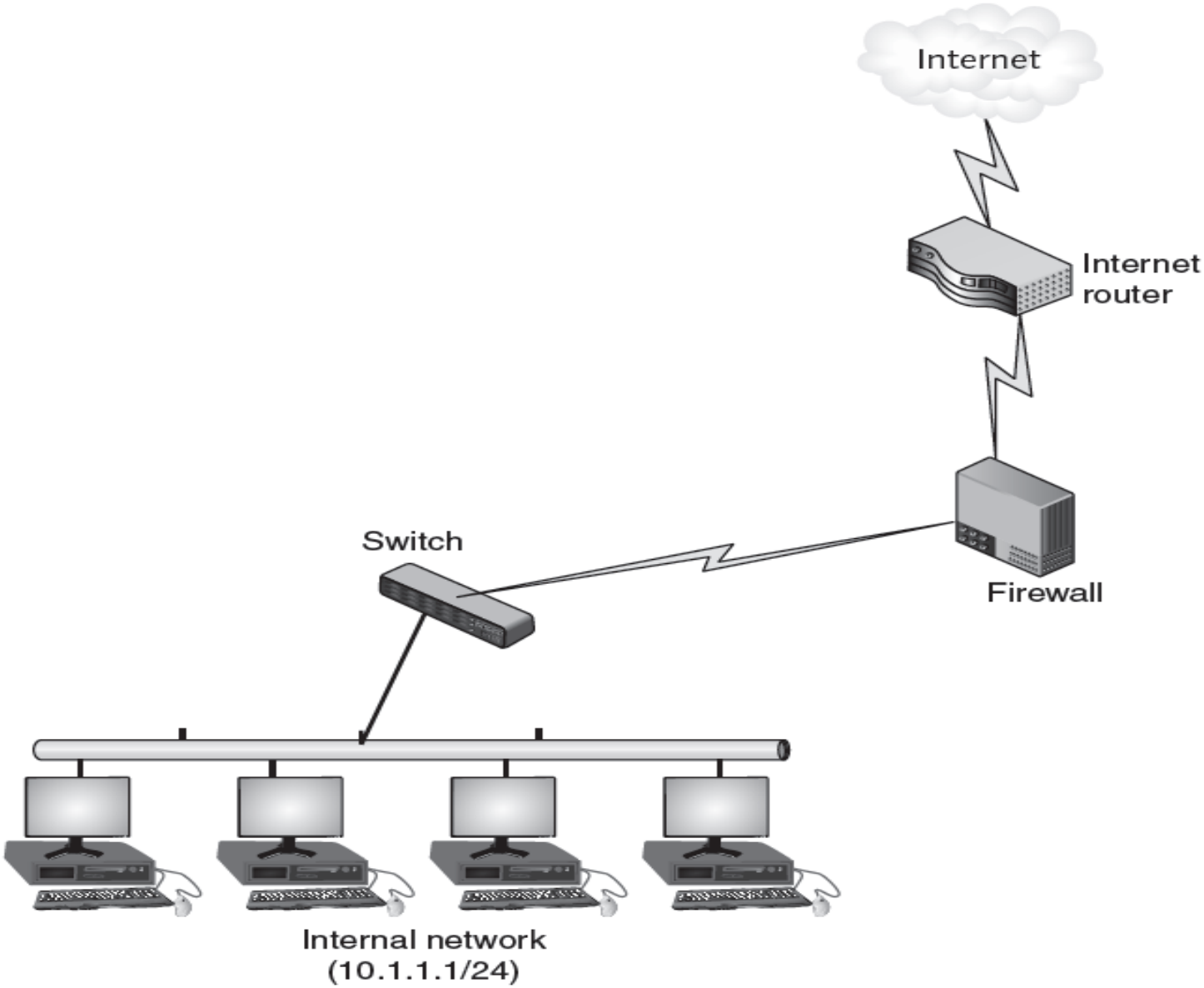
- **Zpřístupnění WWW** serveru z Internetu — mapování služby HTTP na serveru v demilitarizované zóně,
- **Povolení přístupu** z demilitarizované zóny do Internetu prostřednictvím překladu IP adres (NAT) — nutné pro správnou funkčnost mapované služby,
- **Povolení přístupu** z lokální sítě do demilitarizované zóny — zpřístupnění WWW serveru lokálním uživatelům,
- **Zákaz přístupu** z demilitarizované zóny do lokální sítě — ochrana proti napadení lokální sítě z DMZ. Toto je obecně zajištěno výchozím pravidlem blokujícím veškerou ostatní komunikaci.

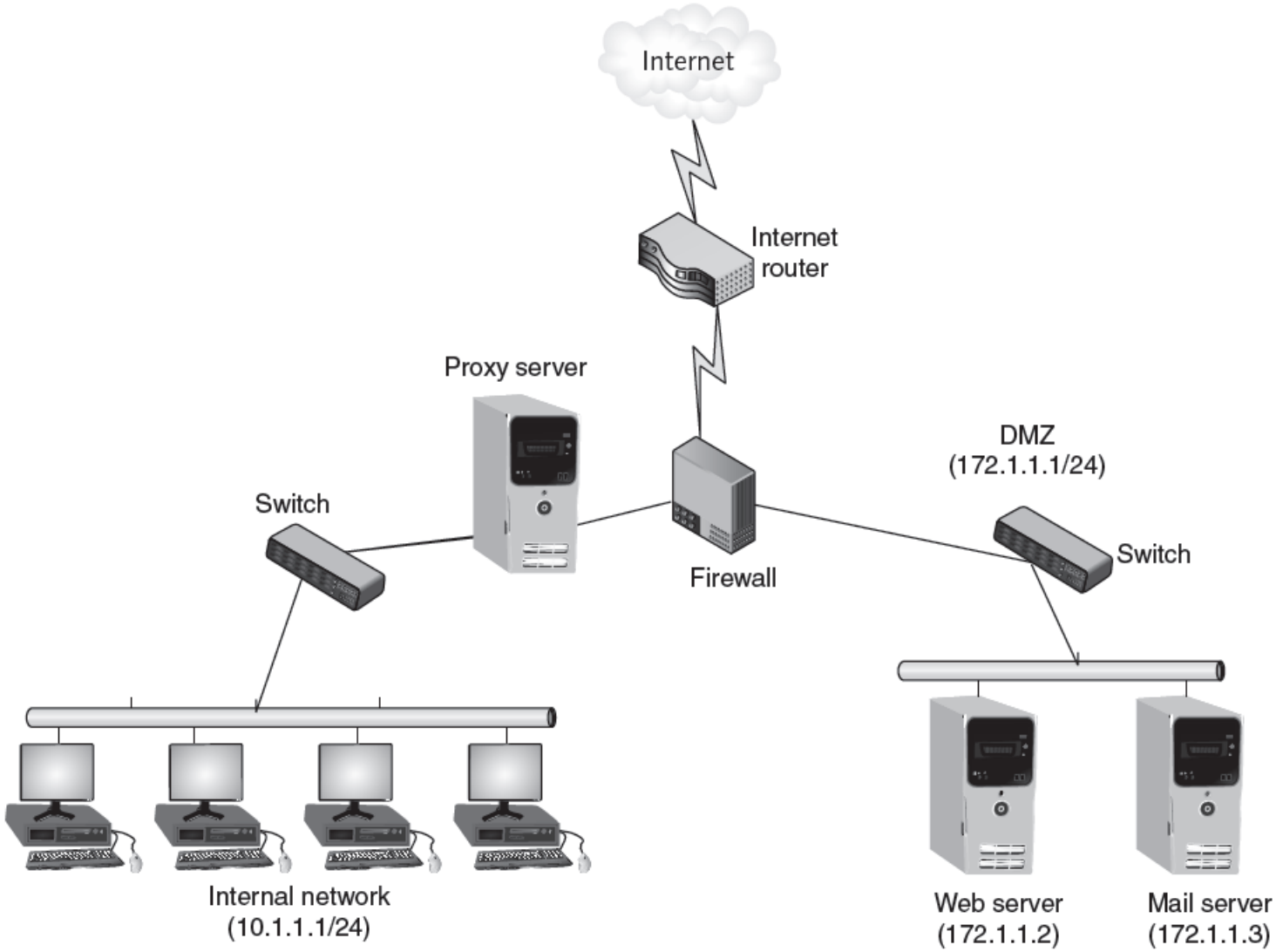
Demilitarizovaná zóna



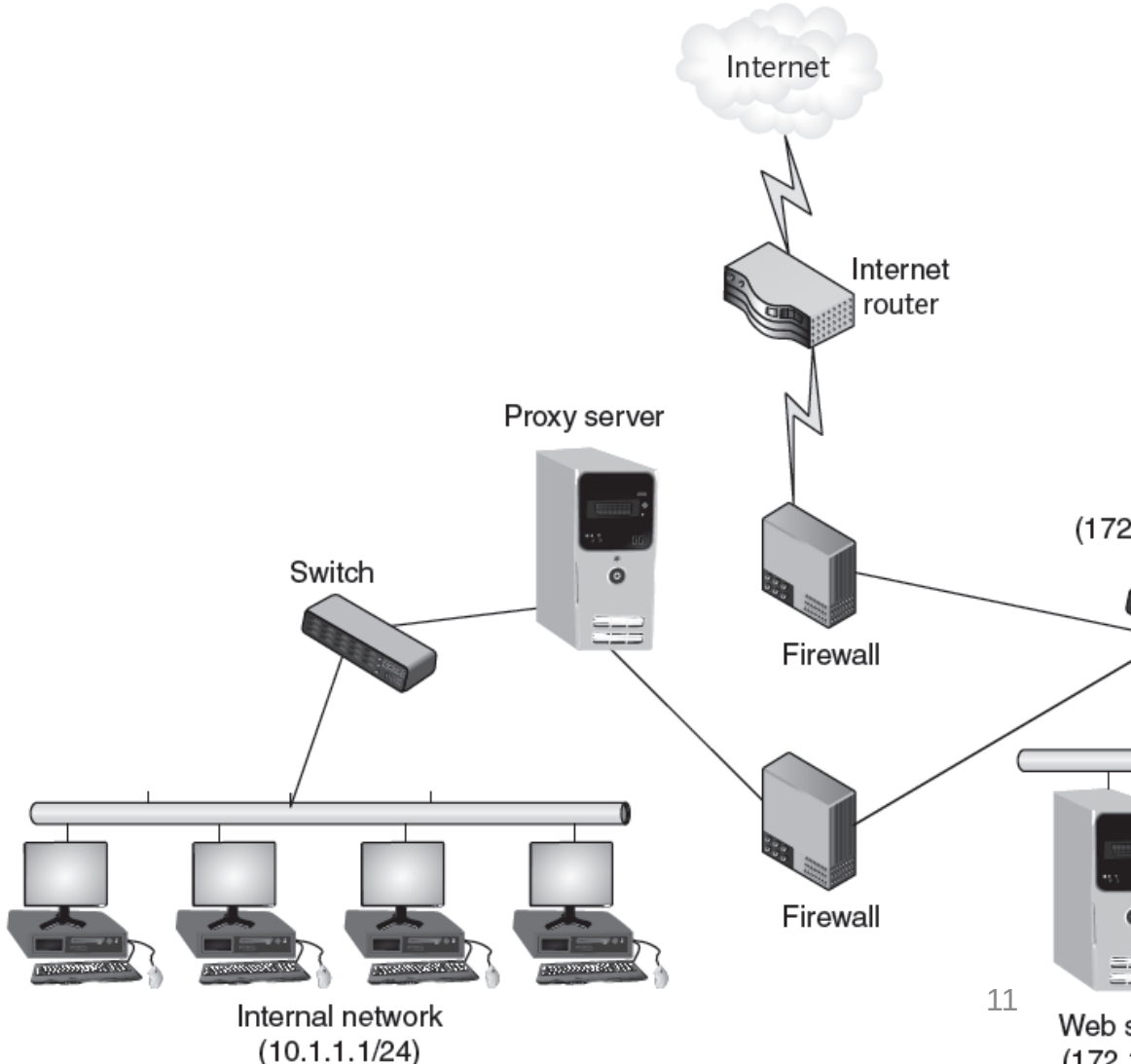

Router
Internet
DMZ
Firewall
DNS
MAILER
FTP
WWW
Vnitřní LAN

MODELOVÉ TOPOLOGIE



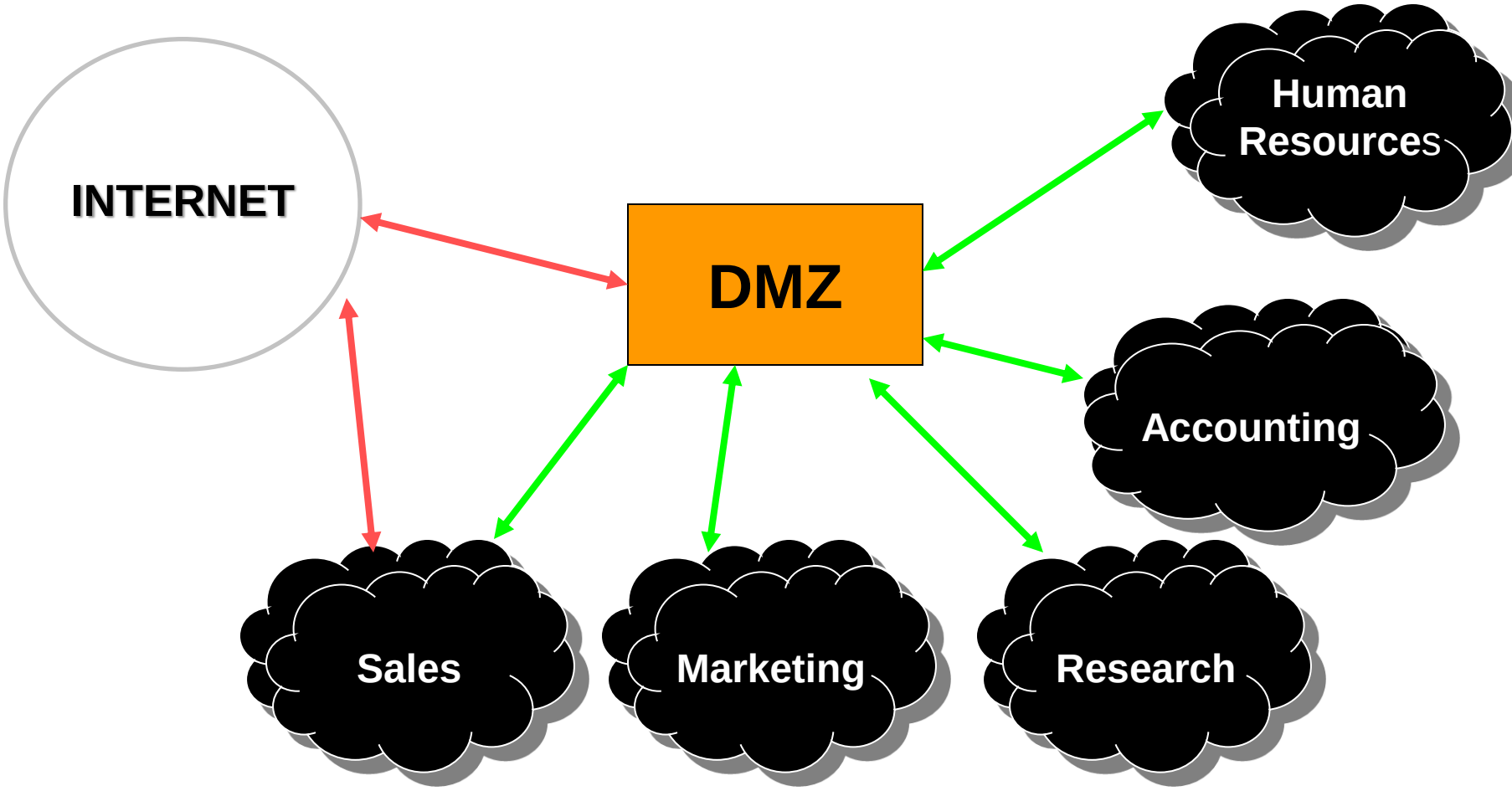


DMZ s jedním firewallem

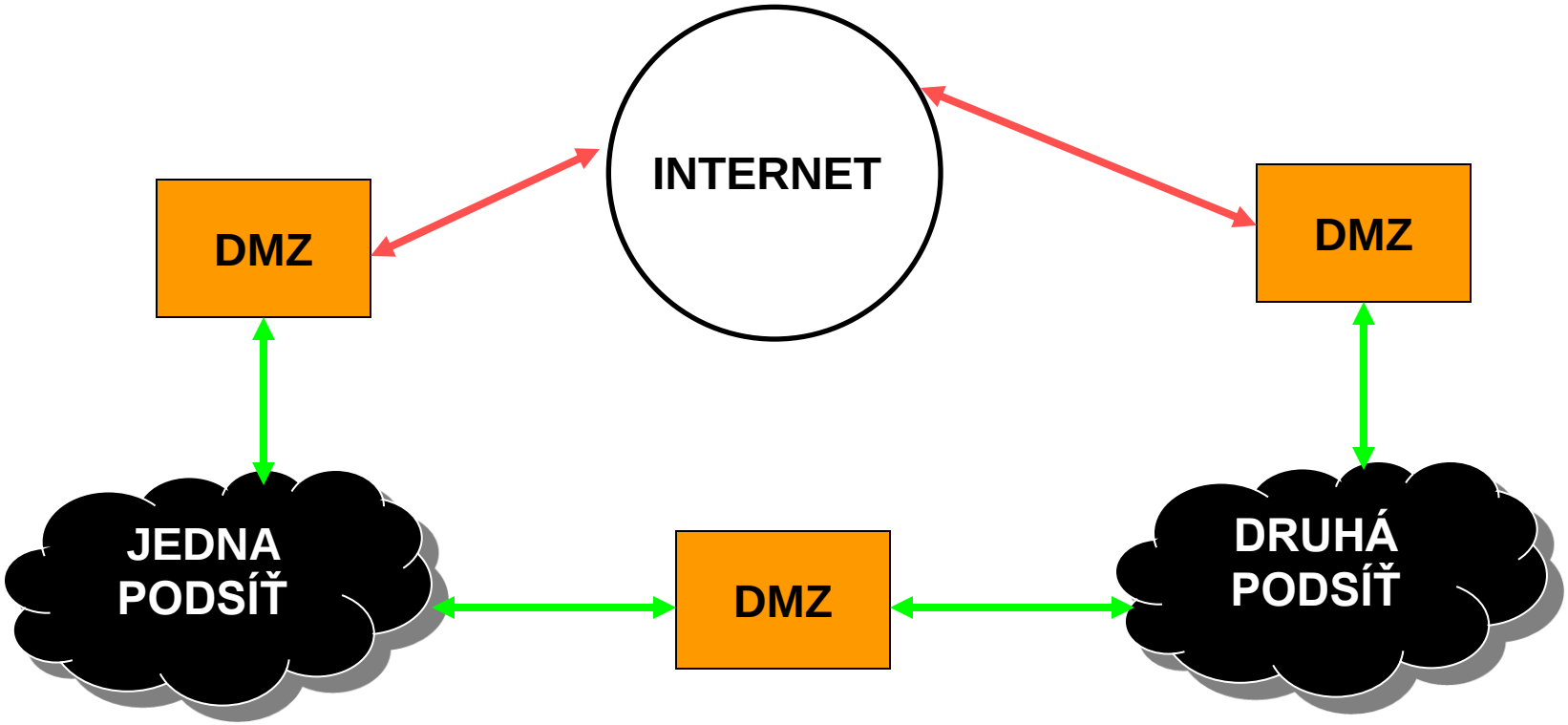

Internet
Internet router
Proxy server
Switch
Firewall
Firewall
Internal network
(10.1.1.1/24)

DMZ

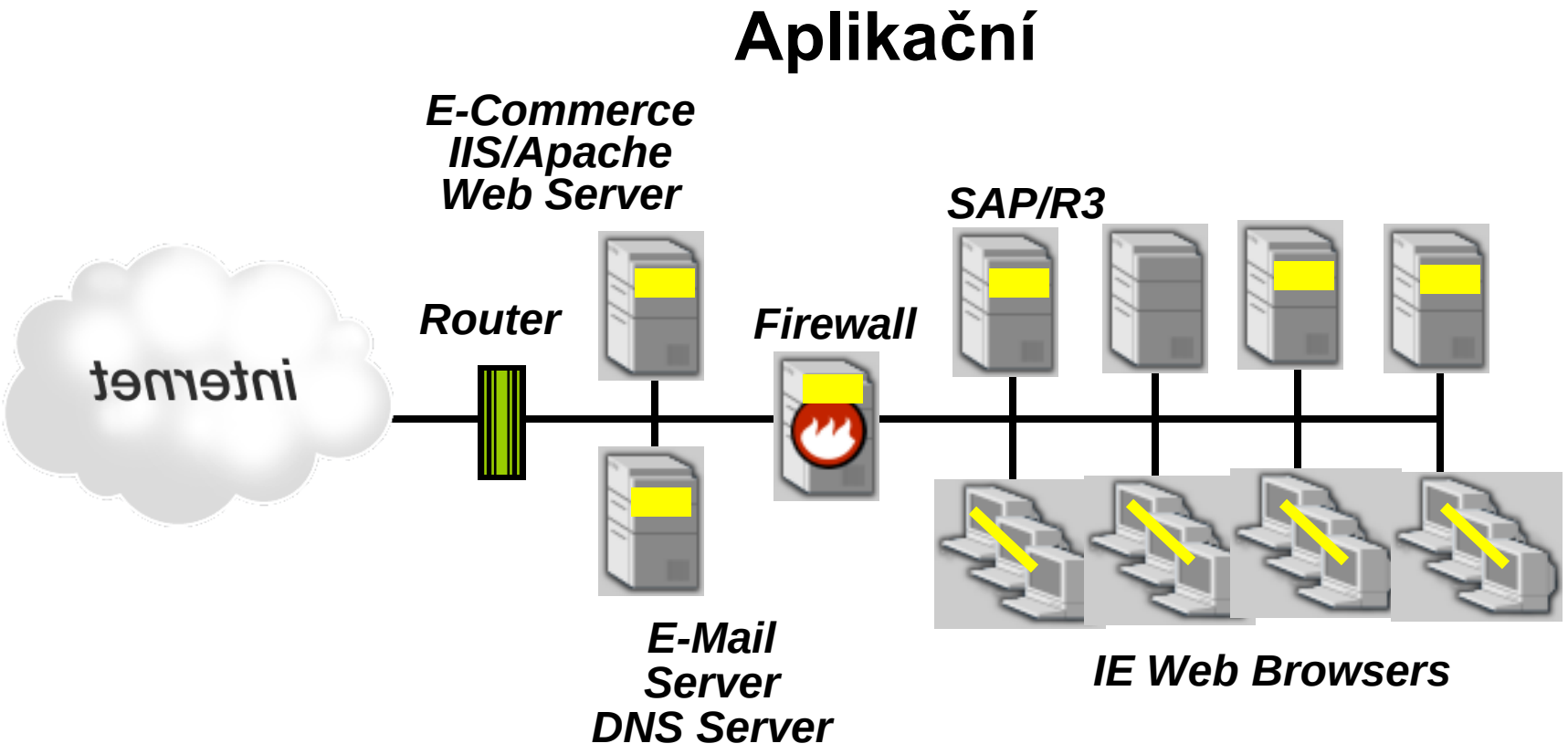
Sample Network Organization



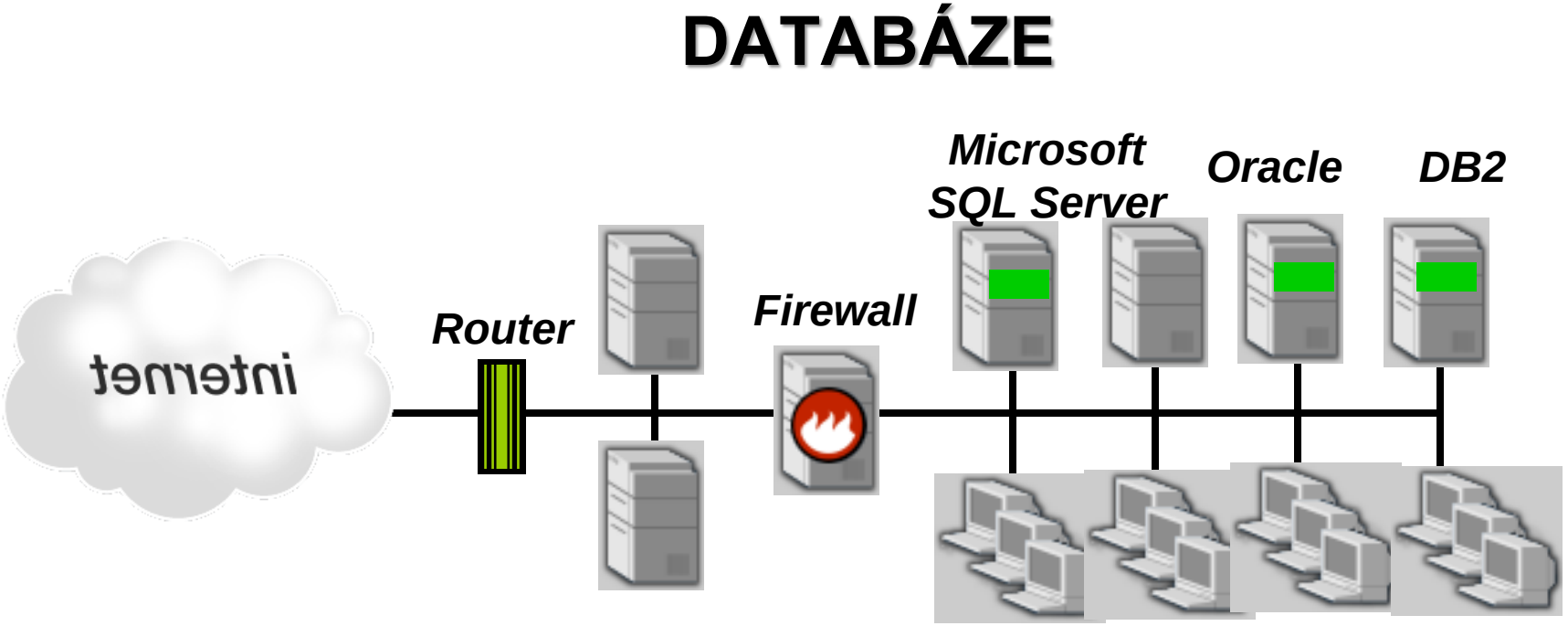
Spojení dvou sítí



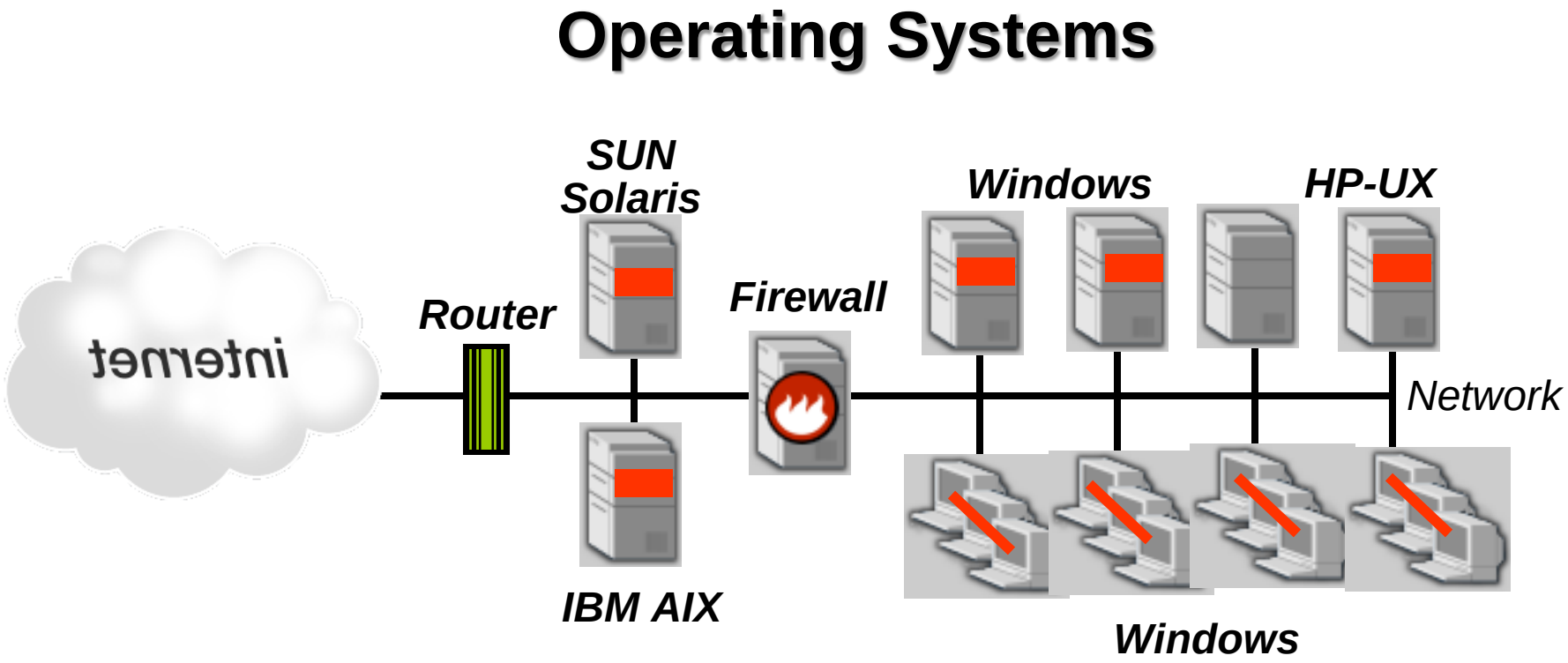
Co je zranitelné?



Co je zranitelné?

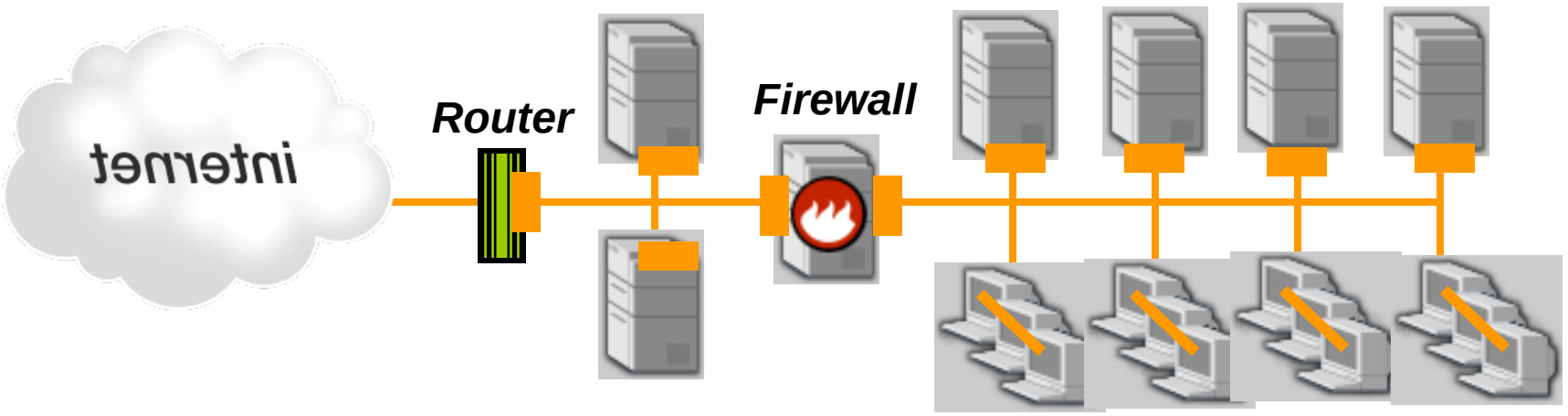


Co je zranitelné?

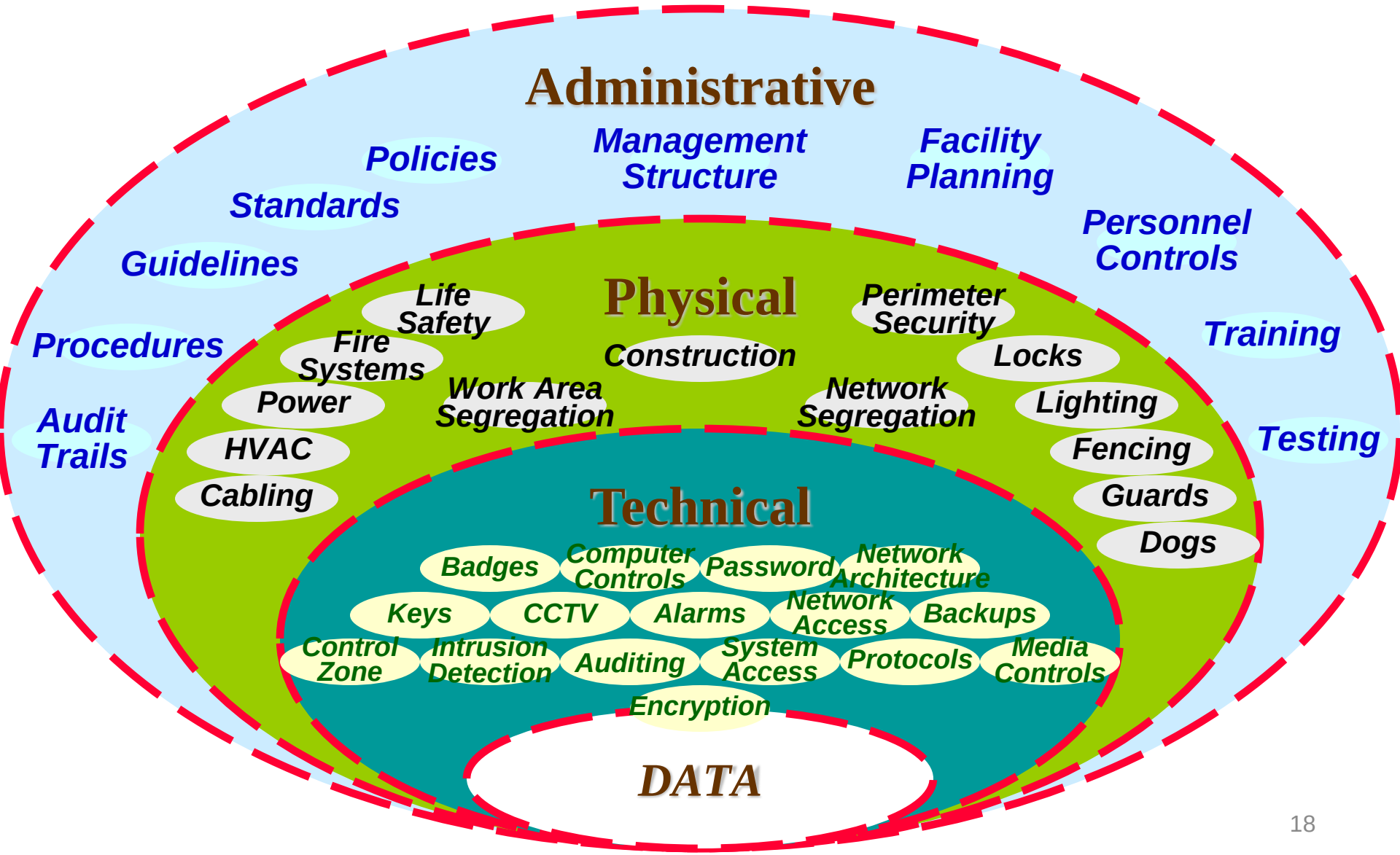


Co je zranitelné?

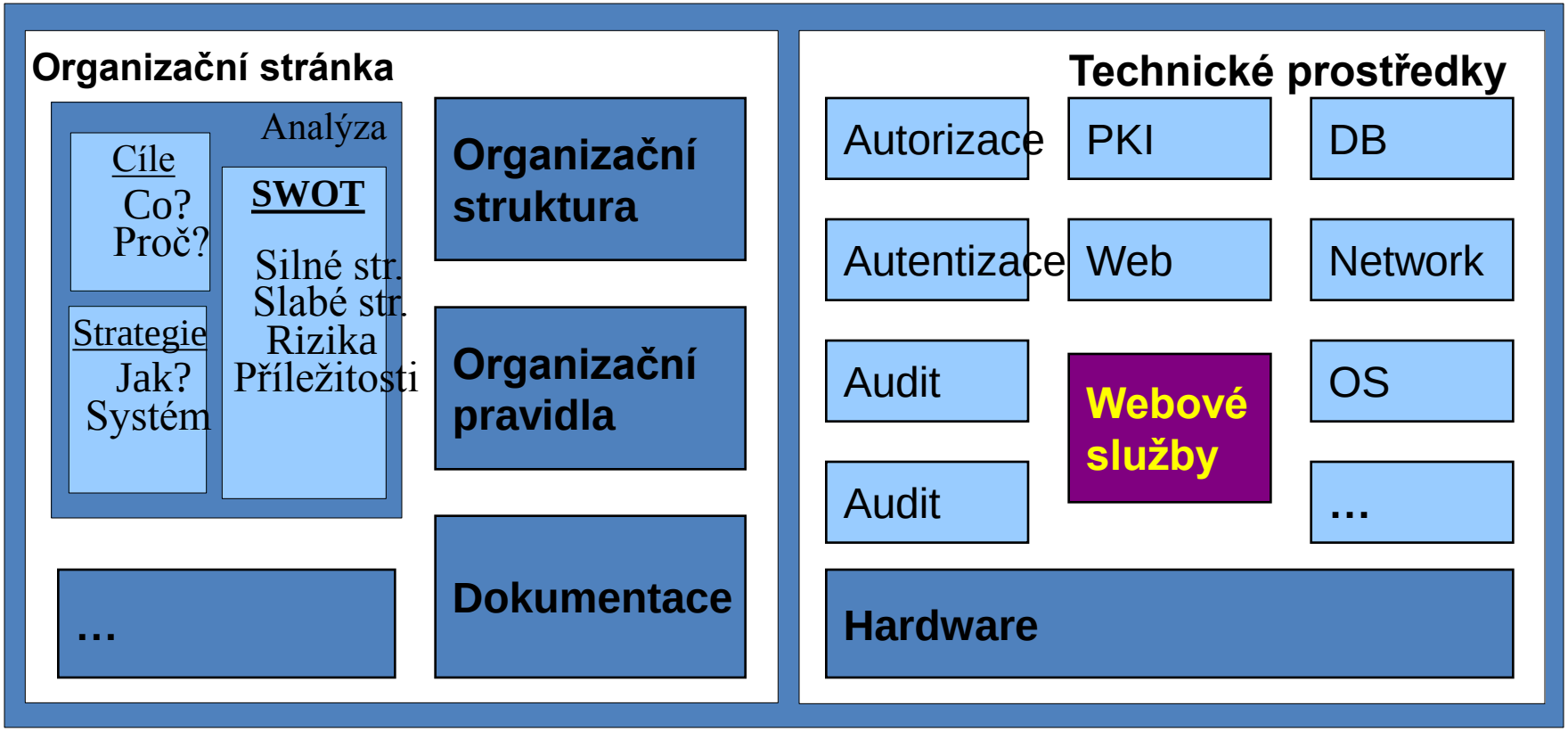
Síťová zařízení



Management Security Controls



Bezpečnostní strategie



PRAMEN: www.komix.cz

Některé chyby DMZ

- Chybná bezpečnostní politika organizace.
- Na počítači, kam se provoz mapuje, musí být nastavena výchozí brána na vnitřní rozhraní počítače.
- Na cílovém počítači běží další firewall, který příchozí provoz zablokuje.
- Chybně nastavená komunikační pravidla.
- Na cílovém počítači neběží daná služba, proto je třeba otestovat přístup lokálně.

pozar@polac.cz