

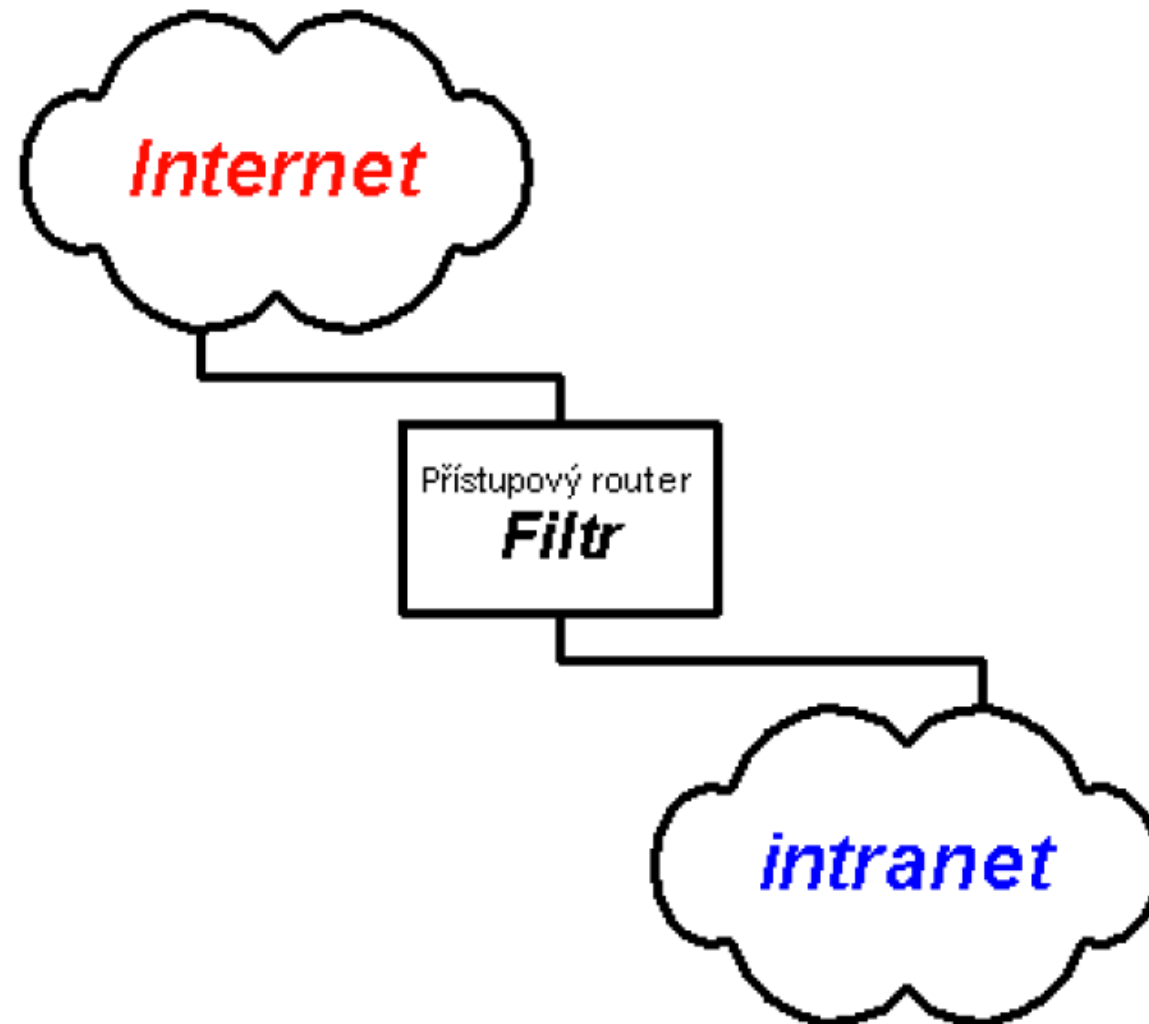
Bezpečnost sítí na bázi IP

Intranet

Vnitřní síť od Internetu izolována pomocí:

- filtrace,
- proxy a gateway,
- skrytých sítí,
- wrapperu,
- firewallu,
- za využití tunelu.

Filtrace



Filtrace

Filtrace umožňuje oddělit intranet od Internetu pomocí filtrů na přístupovém routeru, kterým je firma připojena do Internetu. Filtrace je vlastností routerů. Jako přístupový router může být použit klasický router (např. CISCO), ale i počítač se dvěma síťovými rozhraními a operačním systémem UNIX, Novell, NT atd.

Filtrace

- Filtrací je možné docílit, aby se klienti z intranetu dostali na servery v Internetu, ale aby uživatelé Internetu neměli přístup (neohrožovali) servery intranetu. K dosažení tohoto cíle je nutné provádět filtraci jak na úrovni protokolu IP, tak současně i filtraci protokolu TCP (resp. UDP).
- Filtr se rozhoduje na základě informací uložených v záhlaví IP-datagramu a záhlaví TCP-paketu (resp. UDP-paketu). Filtr "nevidí" do aplikačního protokolu.

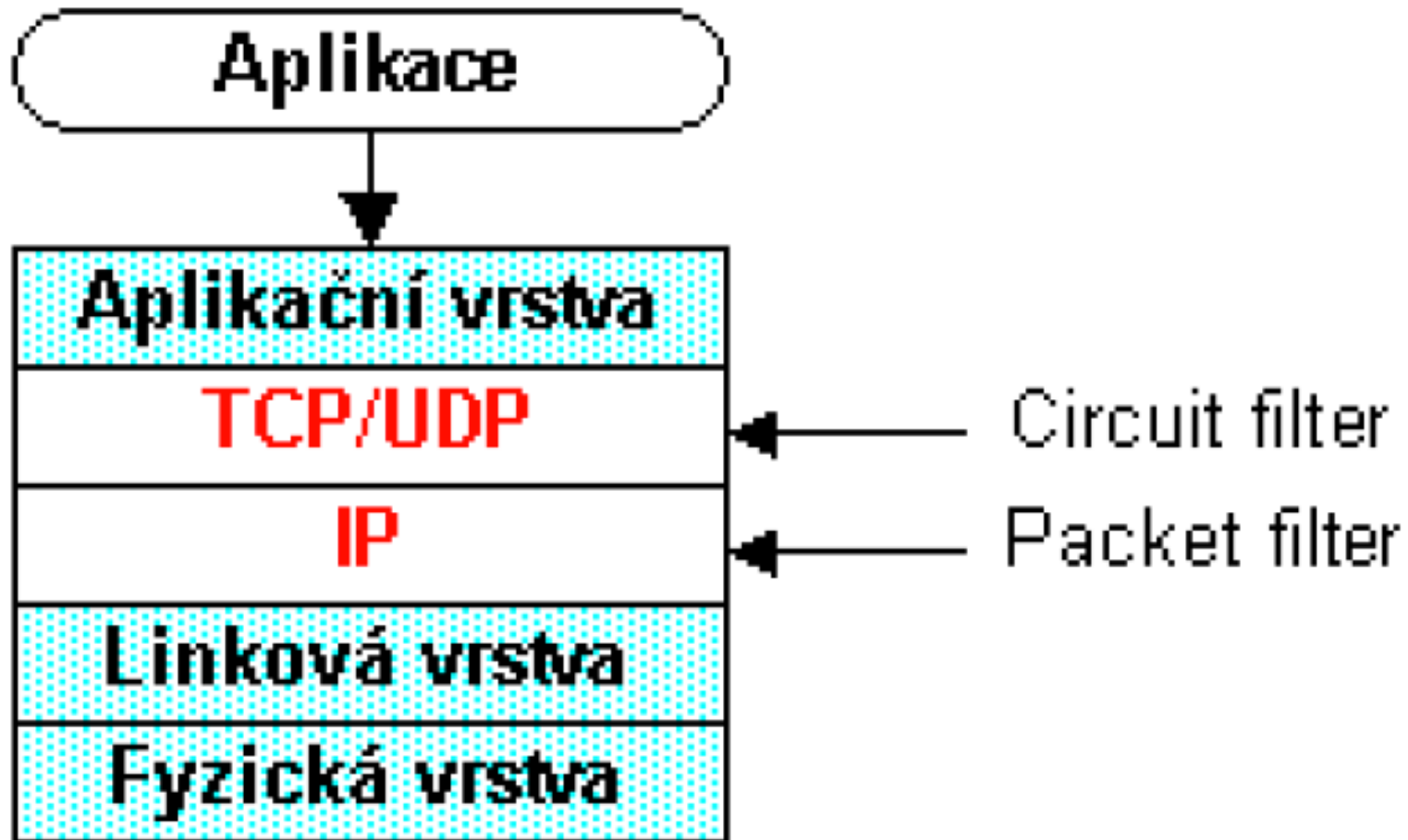
Filtrace

- Problémy s protokolem UDP (tj. zejména DNS) se řeší tzv. aktivními filtry, tj. filtry, které umožňují odesílat datagramy z vnitřní sítě do Internetu, ale odpověď je možné pouze v určitém krátkém časovém intervalu. Nevyžádané odpovědi se zahazují.

Filtrace

- Filtr filtrující podle údajů ze záhlaví IP-datagramu se nazývá Packet Filter.
- Filtr filtrující na základě údajů ze záhlaví TCP (resp. UDP) paketu se označuje jako Circuit Filter.

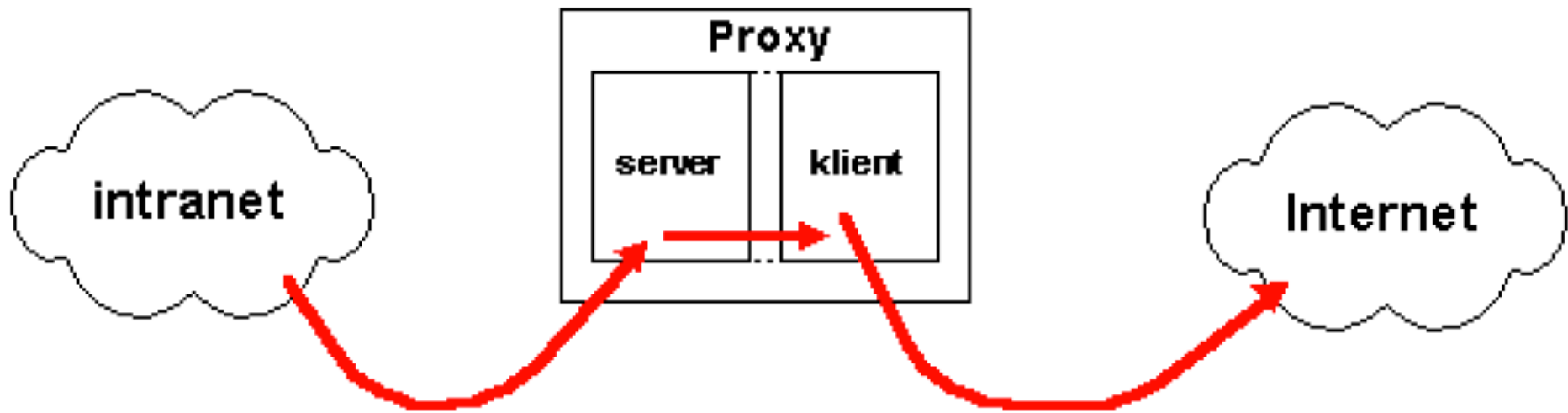
Filtrace



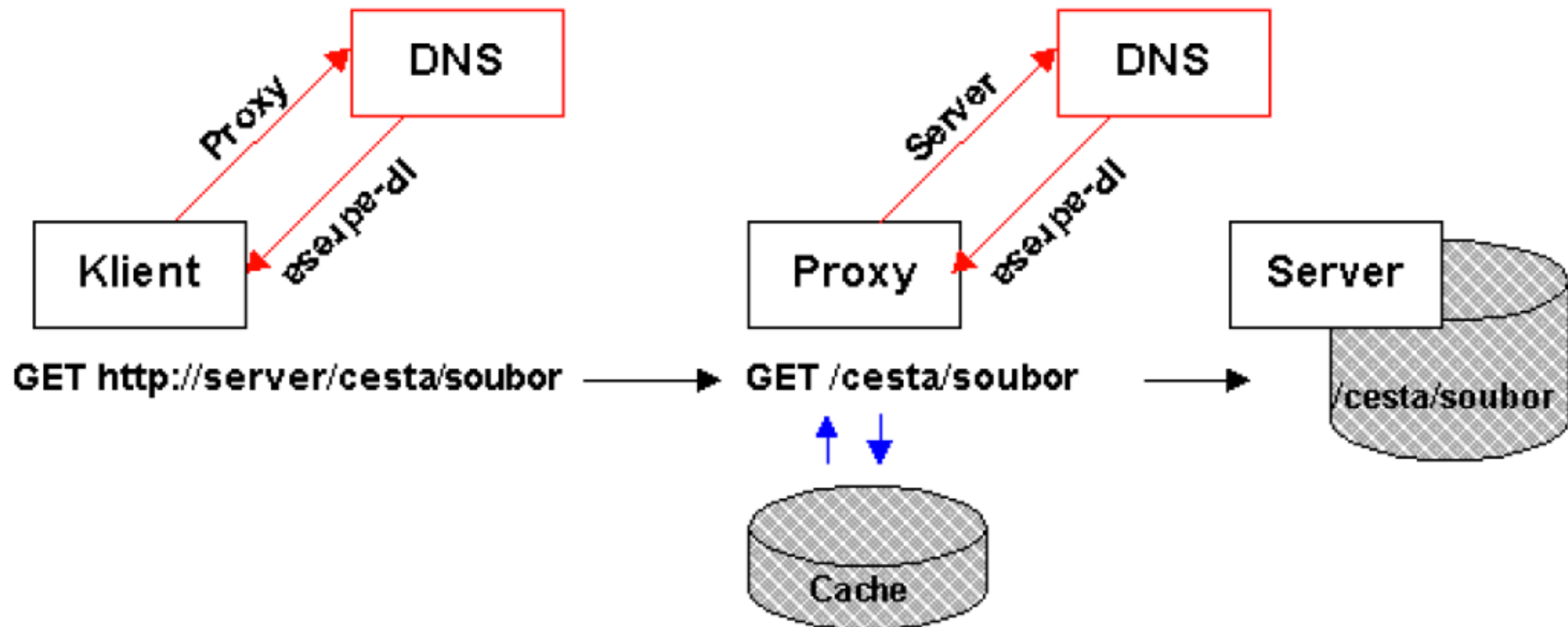
Proxy

- Proxy se instaluje různými způsoby. Klasickým zapojením je proxy se dvěma síťovými rozhraními (jedno do Internetu a druhé do intranetu).
- Proxy je aplikace, která je v klasickém případě spuštěná na počítači, který leží na rozhraní intranetu a Internetu. Přitom obě sítě nejsou vzájemně přímo dostupné. Pro přístup z jedné sítě do druhé je nutné se nejprve přihlásit na počítač s proxy.
- Bez proxy bychom museli mít na tomto počítači konto. Proxy je aplikace, která spojení mezi oběma sítěmi zprostředkovává automatizovaně. Z hlediska klienta se proxy chová jako server, z hlediska cílového serveru se chová jako klient.

Proxy



Proxy (konkrétně pro http)



Proxy

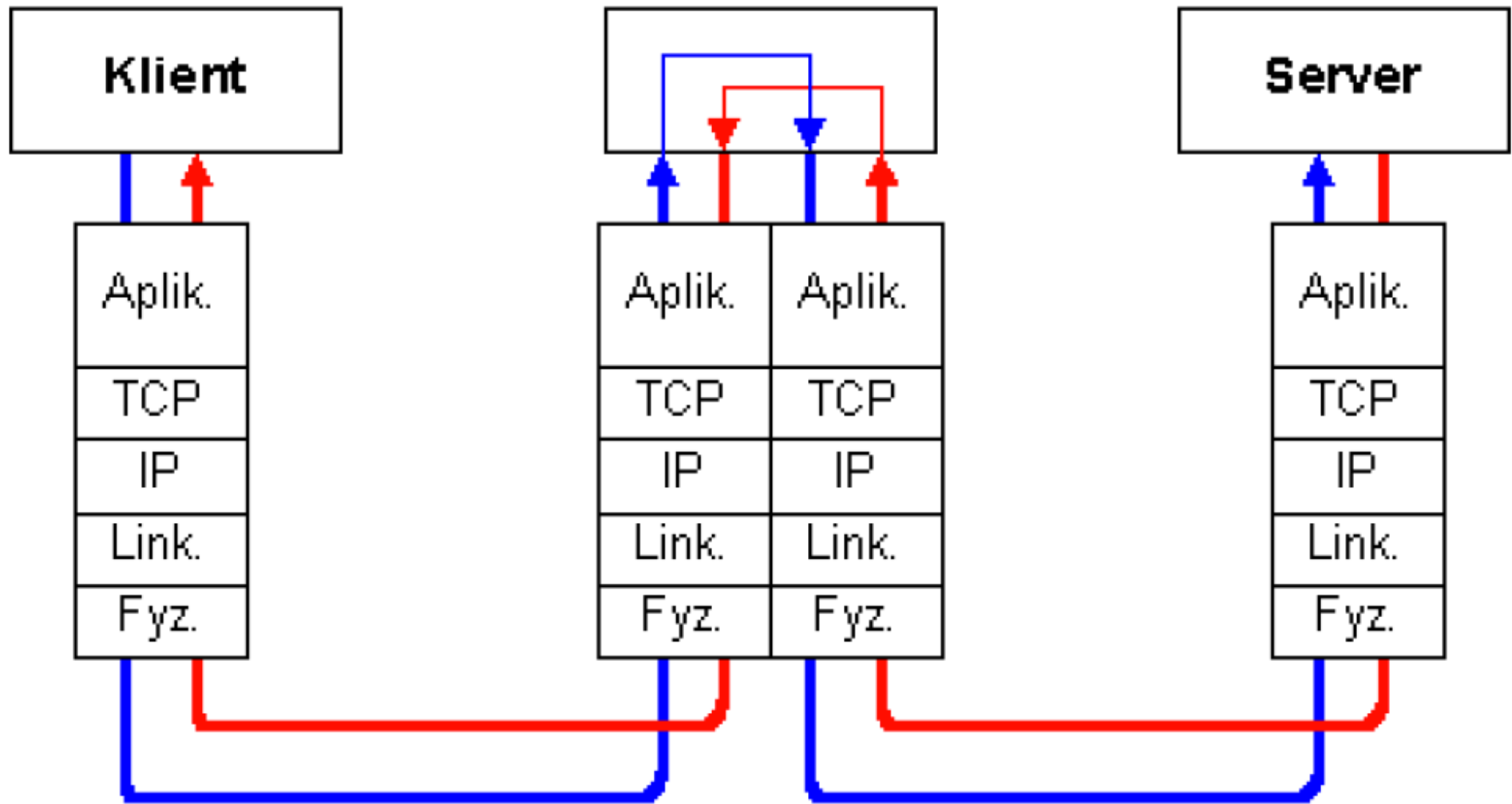
Kategorizace:

- **Klasická proxy** - klient se nejprve přihlásí k proxy, které sdělí jméno cílového serveru, proxy jej pak propojí s cílovým serverem. Klasická proxy se používá zejména pro protokoly FTP, TELNET, HTTP a HTTPS.
- **Generická proxy** - klient nemůže sdělit proxy jméno cílového serveru (neumí to), proto je generická proxy natvrdo nasměrována na jeden konkrétní cílový server. Generická proxy se používá pro protokoly POP, čtení news, firemní aplikace atd.

Proxy

- **Transparentní proxy** - klient adresuje přímo cílový server. Transparentní proxy akceptuje spojení na cílový server a z akceptovaných IP-datagramů se dozví adresu cílového serveru, se kterým klientská část proxy okamžitě navazuje spojení. Z hlediska klienta se transparentní proxy jeví jako router, tj. klient neví, že na cestě k serveru je nějaká proxy. Transparentní proxy se používá zejména pro protokoly TELNET a FTP.
- **Transparentní generická proxy**. Zatímco generická proxy umožňuje různým klientům připojení na jeden konkrétní server, tak transparentní generická proxy umožňuje různým klientům připojení na různé servery. Transparentní generická proxy je určena zejména pro firemní aplikace.

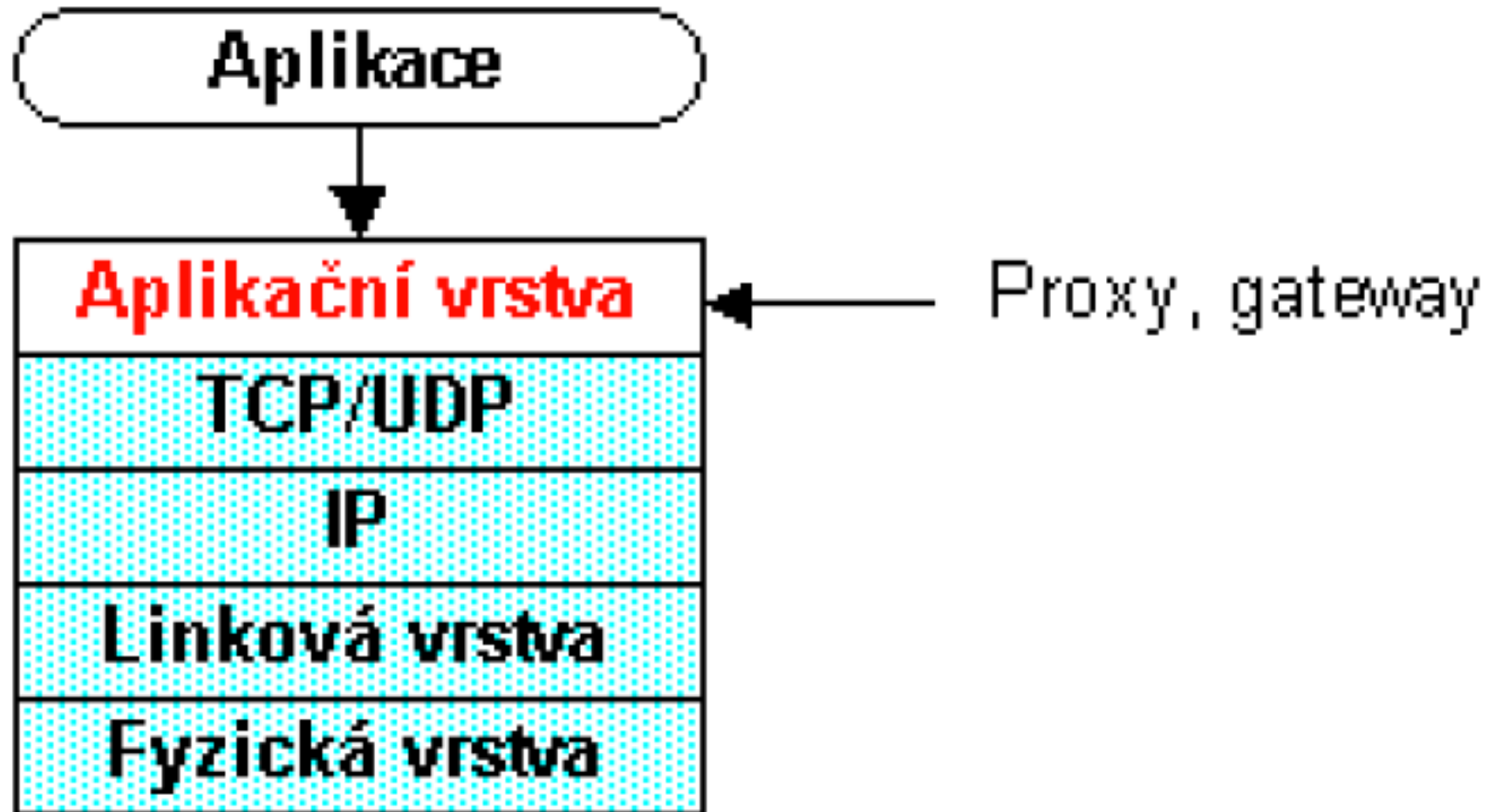
Proxy



Proxy

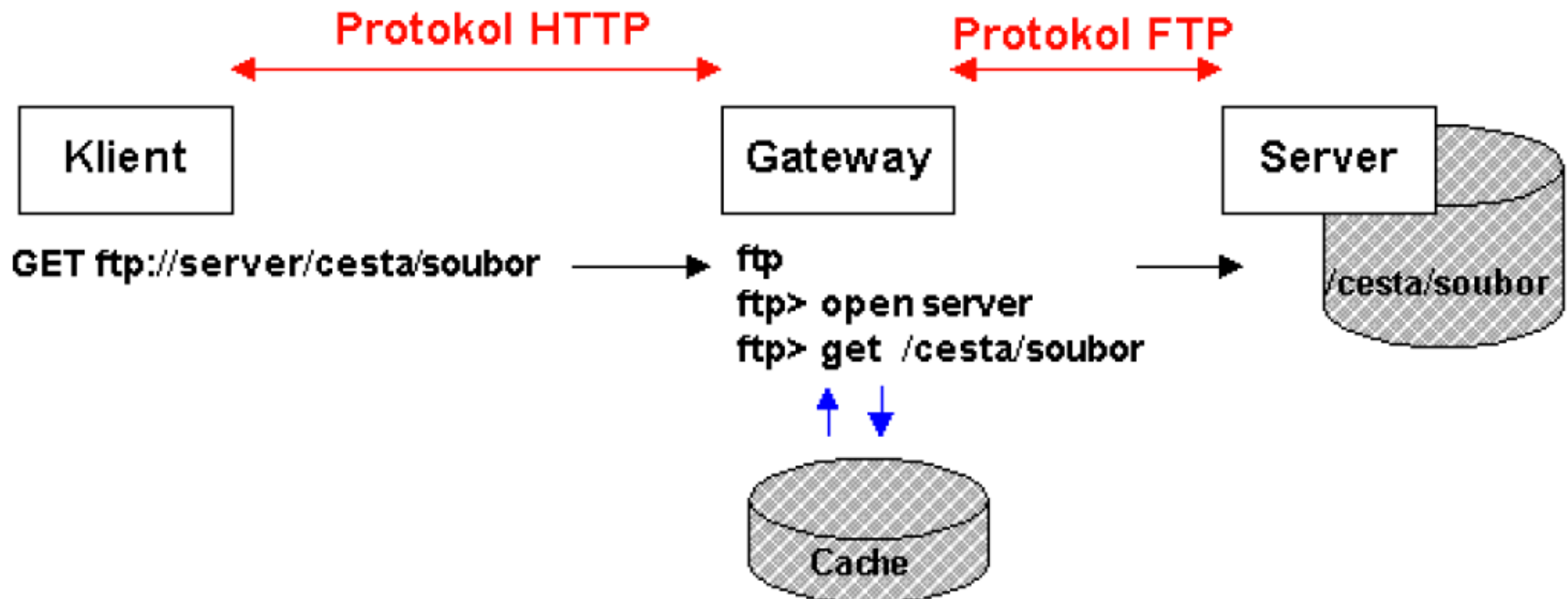
- Proxy pracuje na aplikační vrstvě, tj. proxy vidí do aplikačního protokolu. Je možné provádět i filtraci při předávání mezi serverovou a klientskou částí proxy. Jelikož se jedná o filtraci na aplikační vrstvě, tak je možné touto filtraci např. v protokolu FTP zakázat příkaz PUT a povolit pouze GET. U protokolu HTTP je pak možné omezovat přístup na některá URL atp.

Proxy, gateway



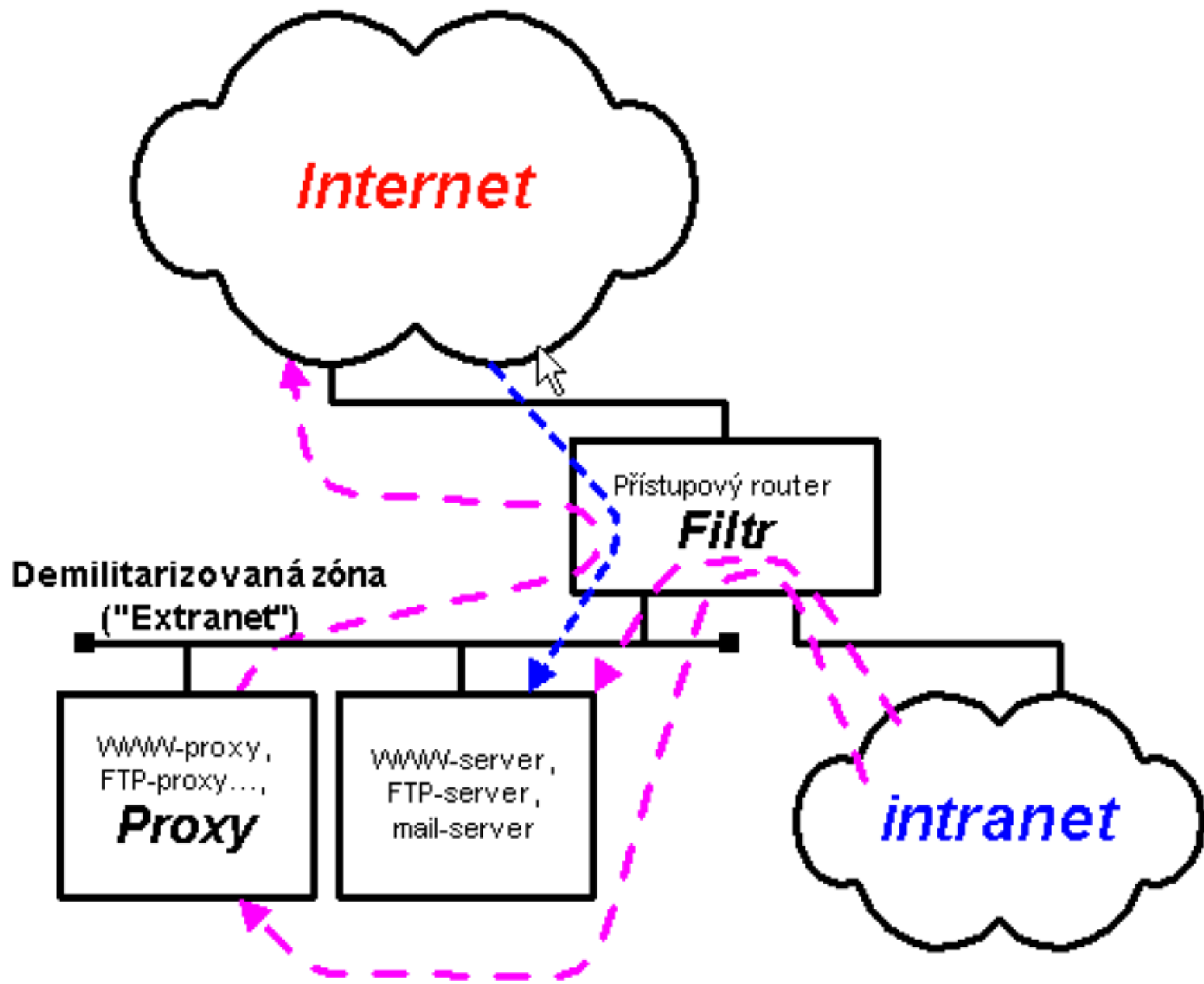
Gateway

Gateway na rozdíl od proxy převádí jeden aplikační protokol na jiný. Např. klient přistupuje na gateway pomocí protokolu HTTP a gateway dále předává požadavky v protokolu FTP:



Oblíbené řešení

kombinace proxy s filtrací na přístupovém routeru, který má více síťových interfejsů



- Tato architektura je-li správně nakonfigurována přináší pro podobný efekt jako firewall, avšak náklady na ni jsou nesrovnatelně nižší.
- Klienti vnitřní sítě nemají přímý přístup do Internetu, přistupují na proxy, která jejich jménem vyřizuje požadavky v Internetu. Proxy je z hlediska uživatelů intranetu server, který vyřizuje jejich požadavky. Z hlediska serverů v Internetu se proxy jeví jako počítač s velkým množstvím klientů (jakoby všichni uživatelé intranetu seděli přímo na tomto počítači).
- Na předchozím obrázku vznikl kromě intranetu a Internetu ještě třetí typ sítě označovaný jako "demilitarizovaná zóna" či "Extranet". Na serveru v Extranetu je přístup jak z Internetu, tak i z intranetu. Je tedy možné, aby aplikace nabízené uživatelům Internetu (běžící např. na WWW-serveru v Extranetu) přistupovaly k datům v intranetu.

Wrapper

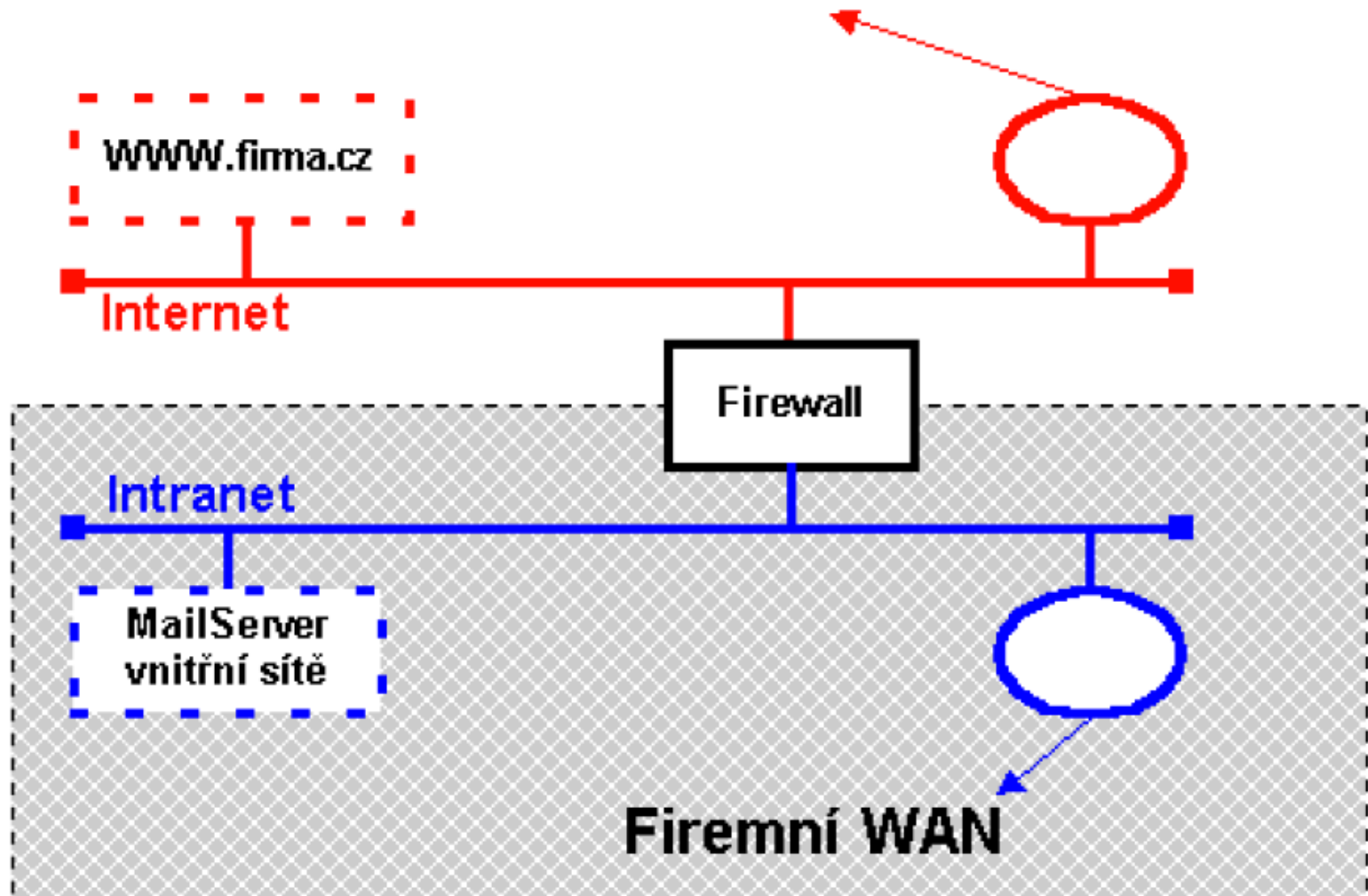
- Wrapper je program, který se automaticky spustí před tím, než se klientovi povoleno přihlásit se k serveru. Wrapper prověřuje totožnost klienta. Je-li klient prověřen, pak je mu teprve spuštěn požadovaný server.
- Wrapper se také často používá pro ověřování totožnosti klienta na serverovské straně proxy. V současné době nejpolulárnější metodou ověřování totožnosti jsou tzv. hesla na jedno použití vytvářené pomocí různých autentizačních pomůcek.

Firewall

- Firewall je dedikovaný počítač nebo soustava počítačů, která nabízí komplex služeb - filtraci, proxy, autentizovaným uživatelům přístup z Internetu do vnitřní sítě atd.
- Dále firewall umožňuje zaznamenávat (logovat) akce prováděné firewallem. Aktivní firewally umožňují v případě konkrétně definovaných událostí provádět např.:
 - Potencionálního útočníka zařadit na černou listinu počítačů, se kterými už dále nekomunikuje.
 - Uzavřít atakovanou službu, popř. celý firewall.
 - Spustit specifikovaný program, který může např. odeslat zprávu správci firewallu atd.
 - Sledovat systém, na kterém firewall běží a v případě nečekaných změn systémových souborů generovat událost.

Firewall

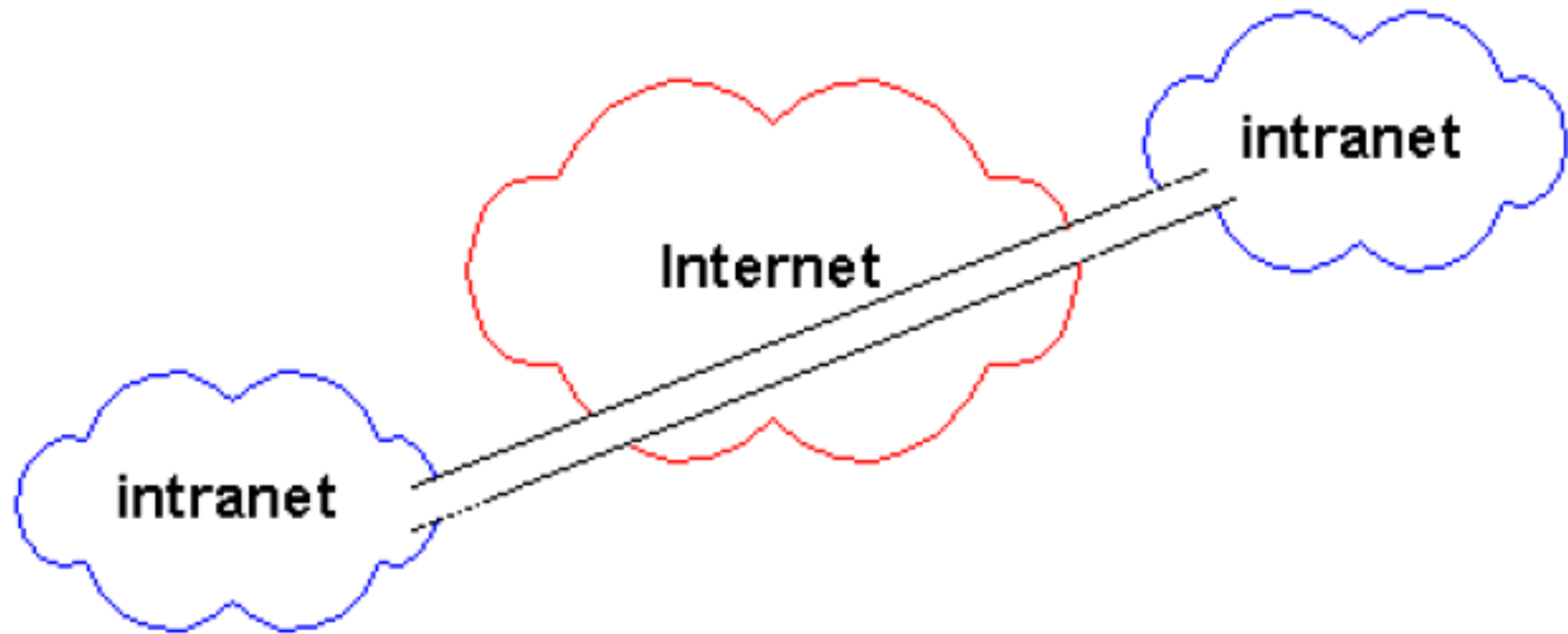
Interent



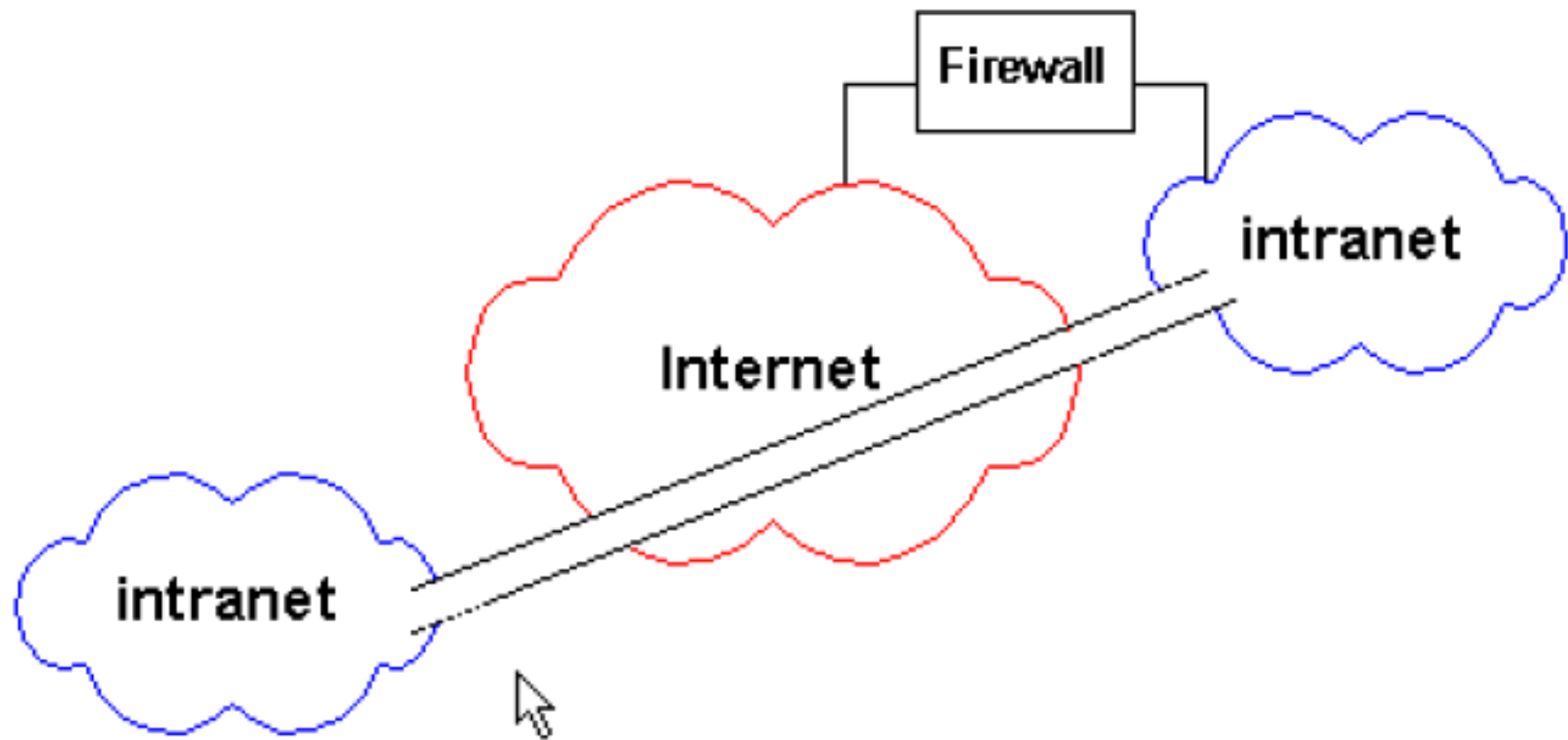
Tunel

- Tunel vytváří spojení mezi dvěma či více stranami (portály) skrze jinou síť. Tunel se vytváří buď za účelem transportu jiného síťového protokolu přes existující síť nebo za účelem bezpečného spojení dvou lokalit přes Internet.

Tunnel



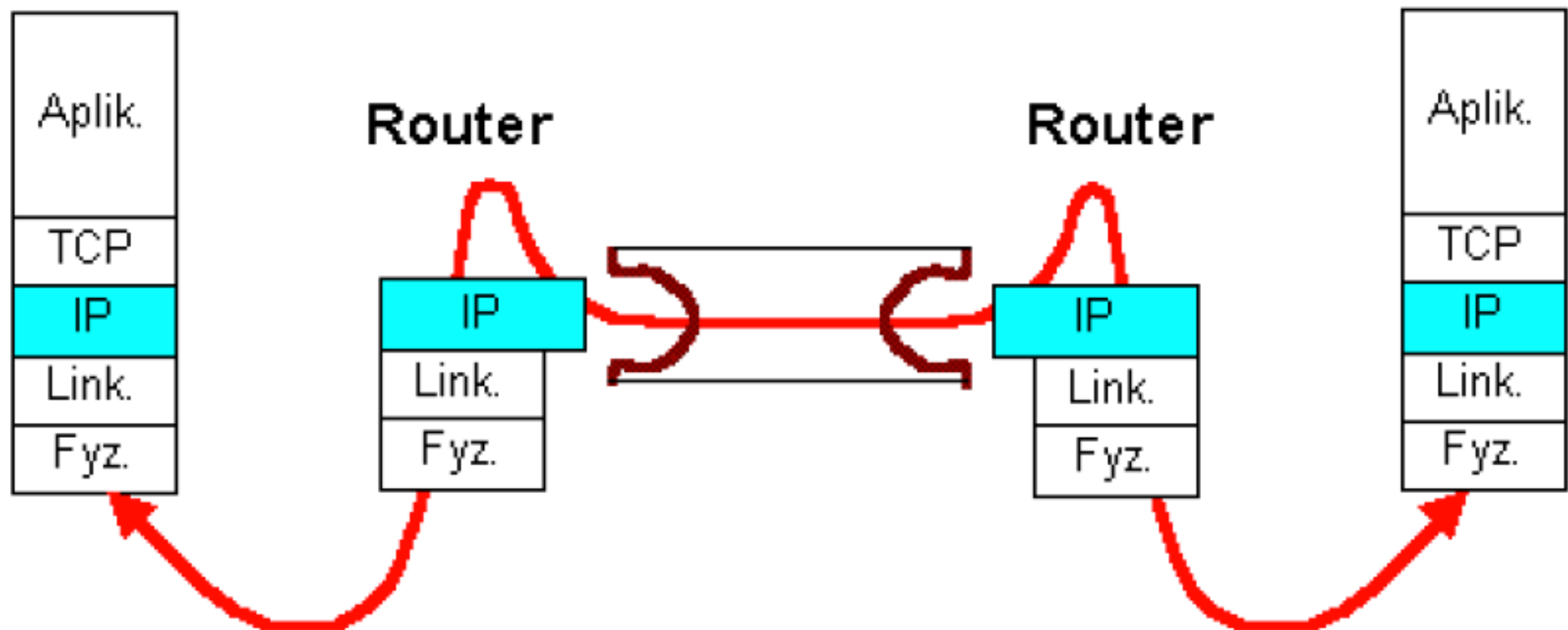
Tunnel



Tunel

- Zabezpečení přenosu dat může být prováděno na přístupových routerech tak, že v každém přenášeném datagramu se ponechá IP-záhlaví a TCP-záhlaví (resp. UDP) a datová část každého paketu se na vstupu do Internetu šifruje a na výstupu dešifruje. Takto pracují např. tunely realizované routery firmy CISCO.

Tunel



Tunel

- Druhou eventualitou je pak celý IP-datagram zašifrovat a vložit do nového TCP nebo UDP paketu jako data.
- Toto řešení používá např. OpenVPN. Výhodou tohoto řešení je, že i vzdálená lokalita může používat adresy pro skryté sítě, tj. např. adresu sítě 10. Vzdálená lokalita se tak stává integrální součástí intranetu.

