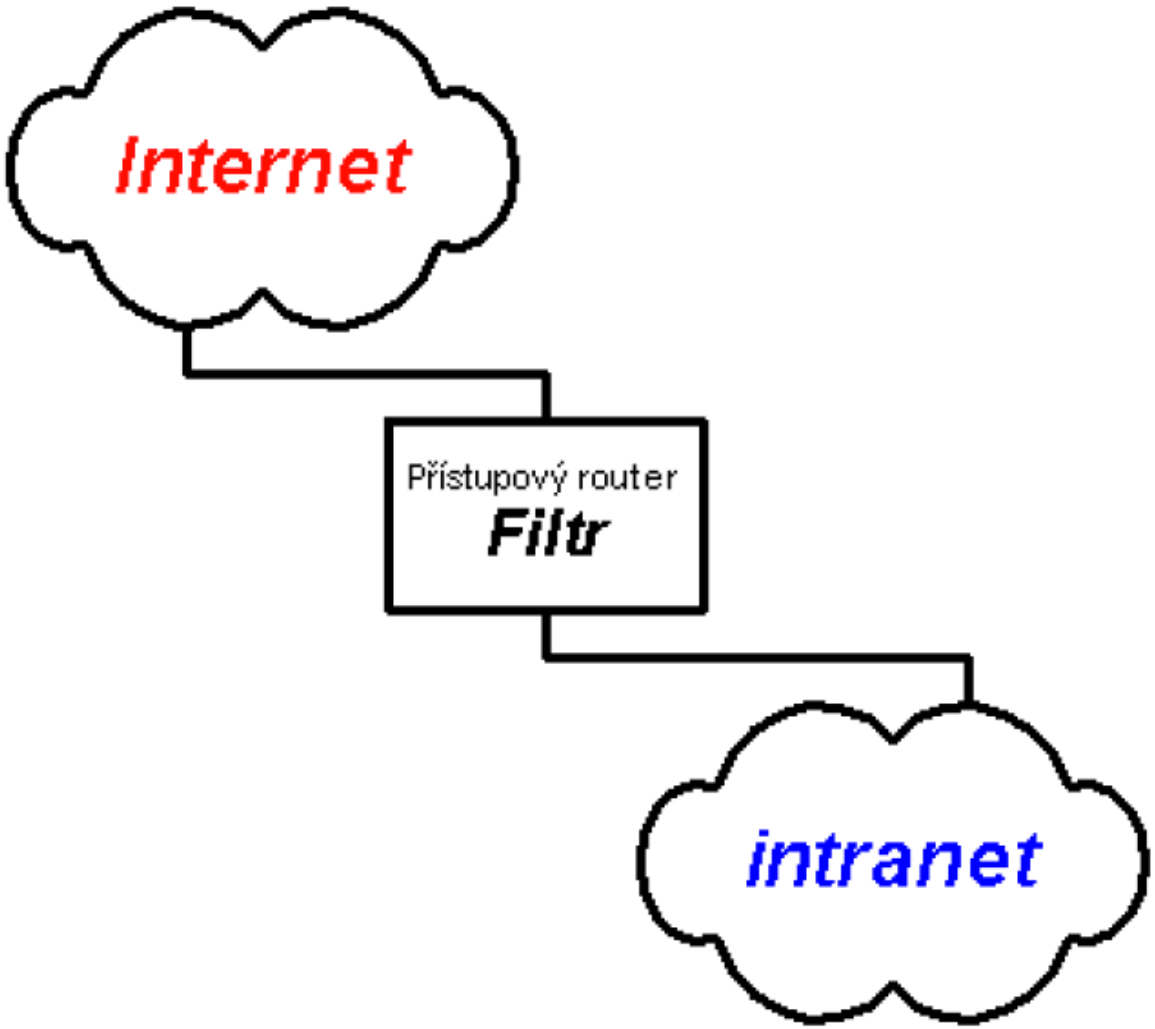
Bezpečnost sítí na bázi IP

Intranet

Vnitřní síť od Internetu izolována pomocí:

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

Filtrace



Filtrace

Filtrace umožňuje oddělit intranet od Interentu pomocí filtrů na přístupovém routeru, kterým je firma připojena do Internetu. Filtrace je vlastností routerů. Jako přístupový router může být použít 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 tohto 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.

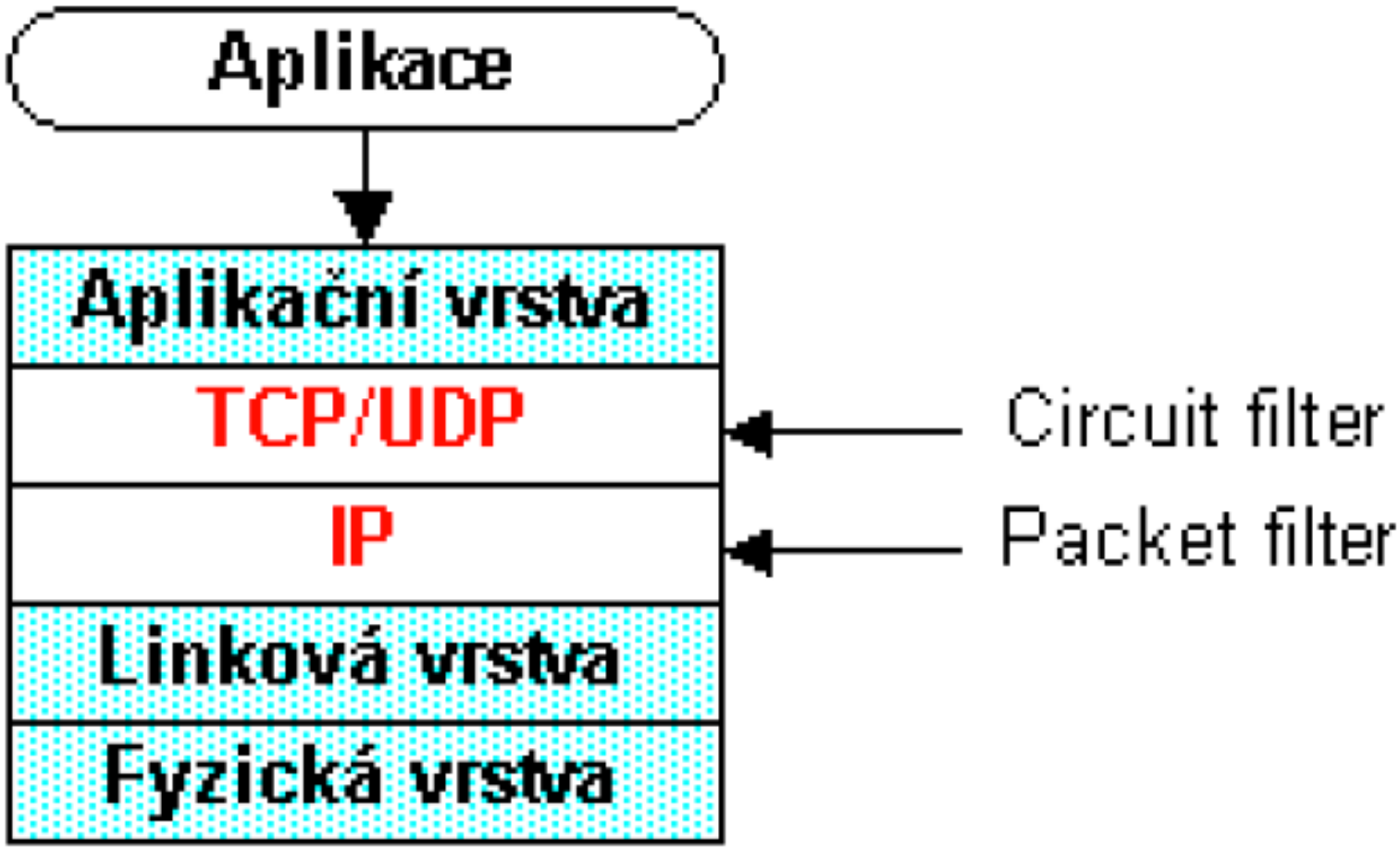
Filtrace

- 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.

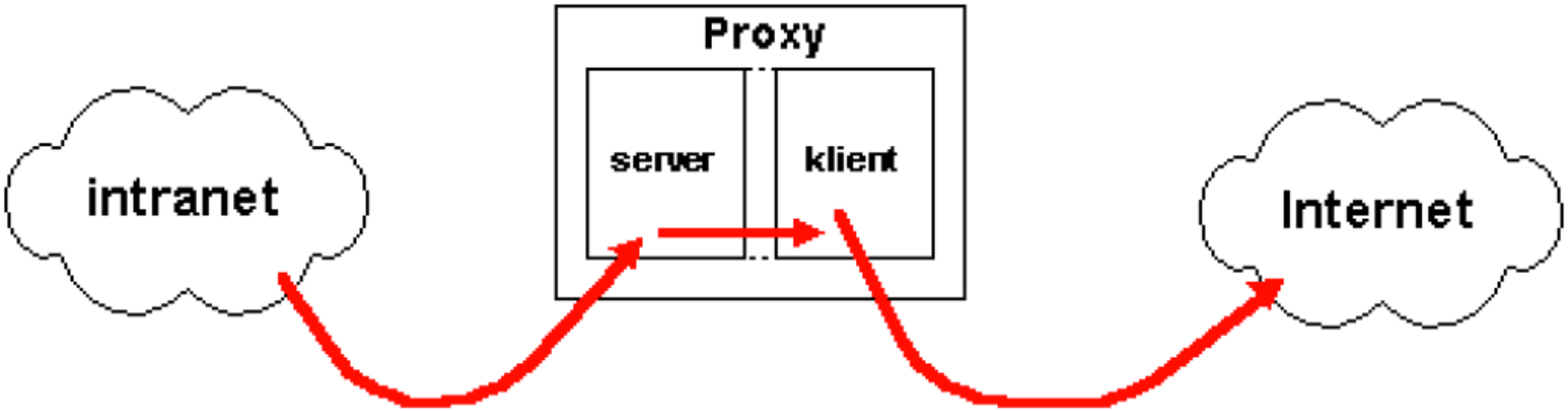
Filtrace


Aplikace
Aplikační vrstva
TCP/UDP
IP
Linková vrstva
Fyzická vrstva
Circuit filter
Packet filter

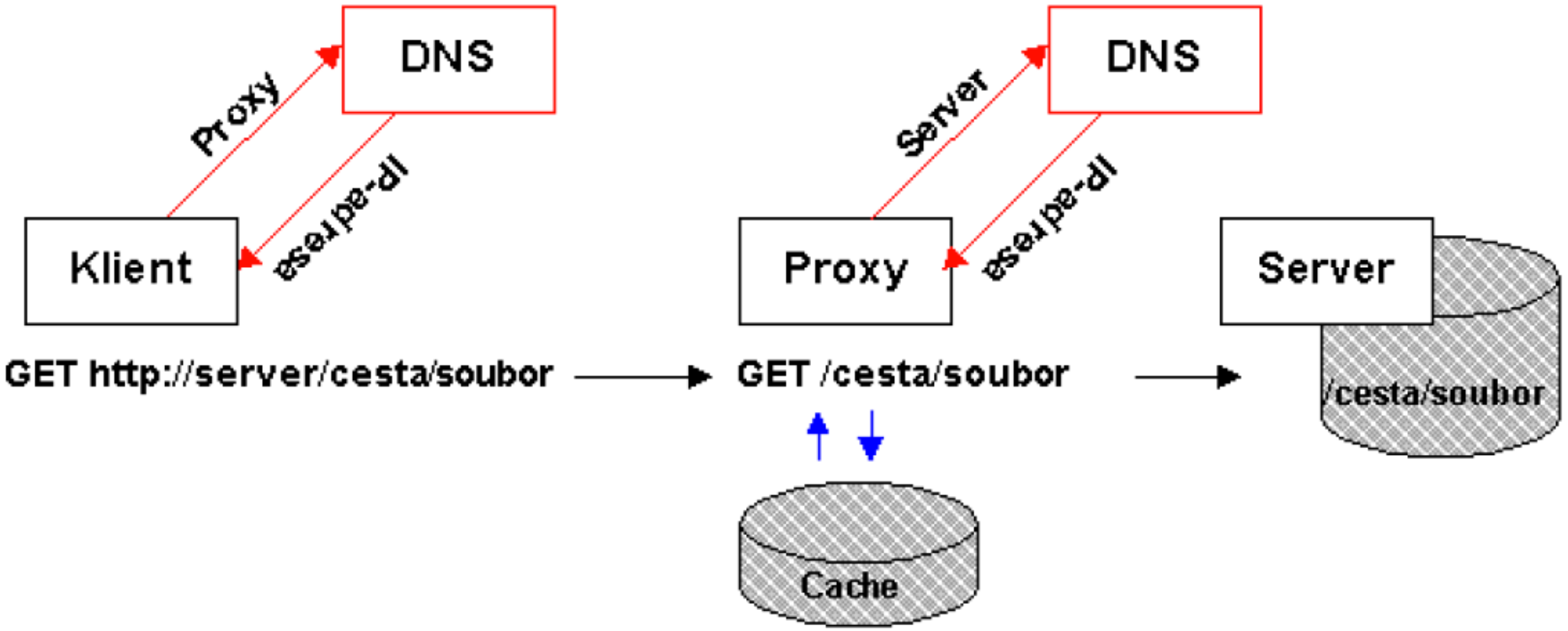
Proxy

- Proxy se instaluje různými zůsoby. 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 musleli 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

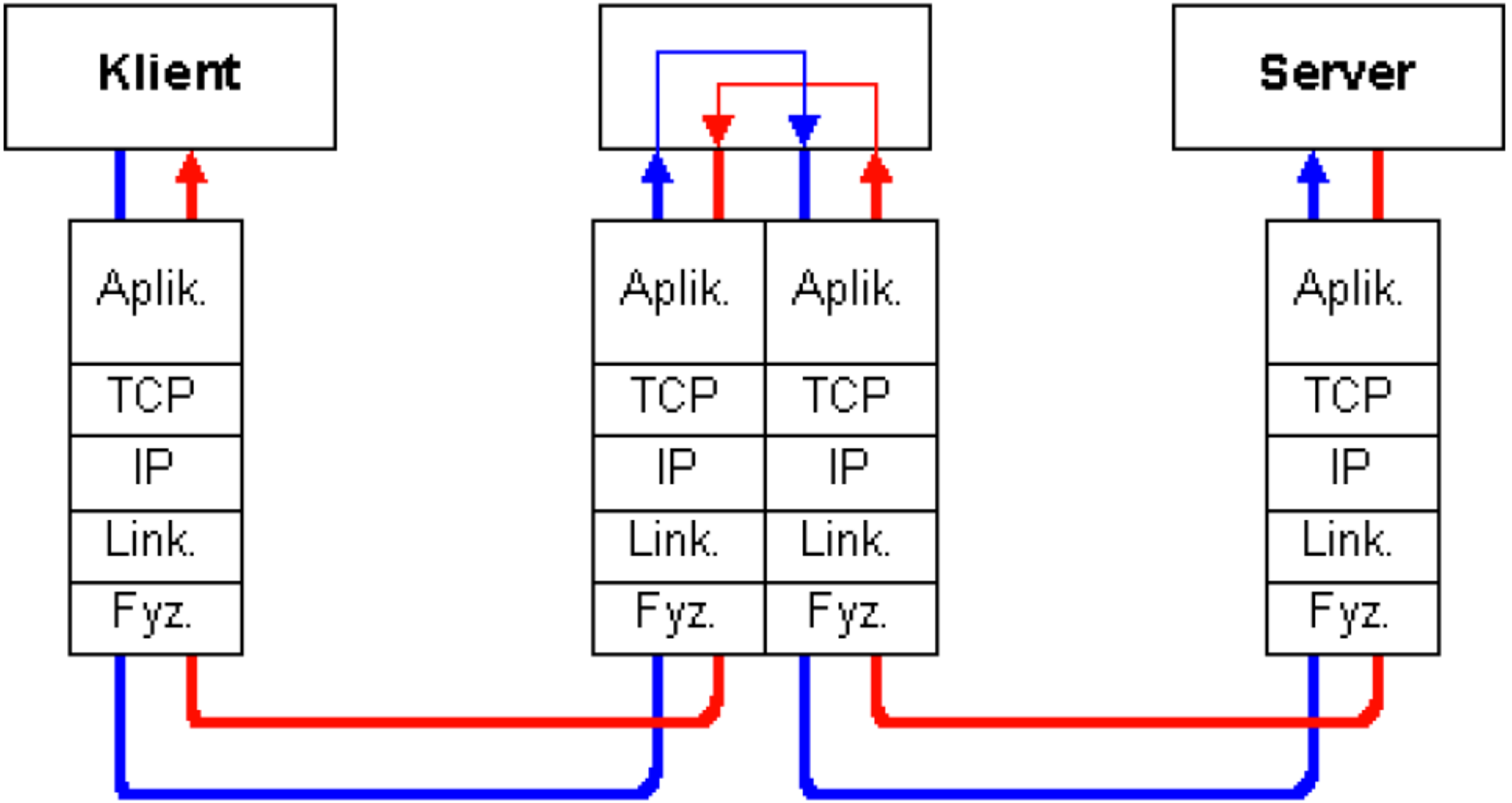
Kategorizace:

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

Proxy

- **Transparentni 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 okaţitě navazuje spojení. Z hlediska klienta se transparentní proxy jeví jako router, tj. klient neví, ţe na cesktě k serveru je nějaká proxy. Transparentní proxy se pouţívá zejména pro protokoly TELNET a FTP.
- **Transparentní generická proxy**. Zatímco gerická proxy umoţňuje různým klientům připojení na jeden konkrétní server, tak transparentní generická proxy umoţňuje různým klientům připojení na různé servery. Transparentni generická proxy je určena zejména pro firemní aplikace.

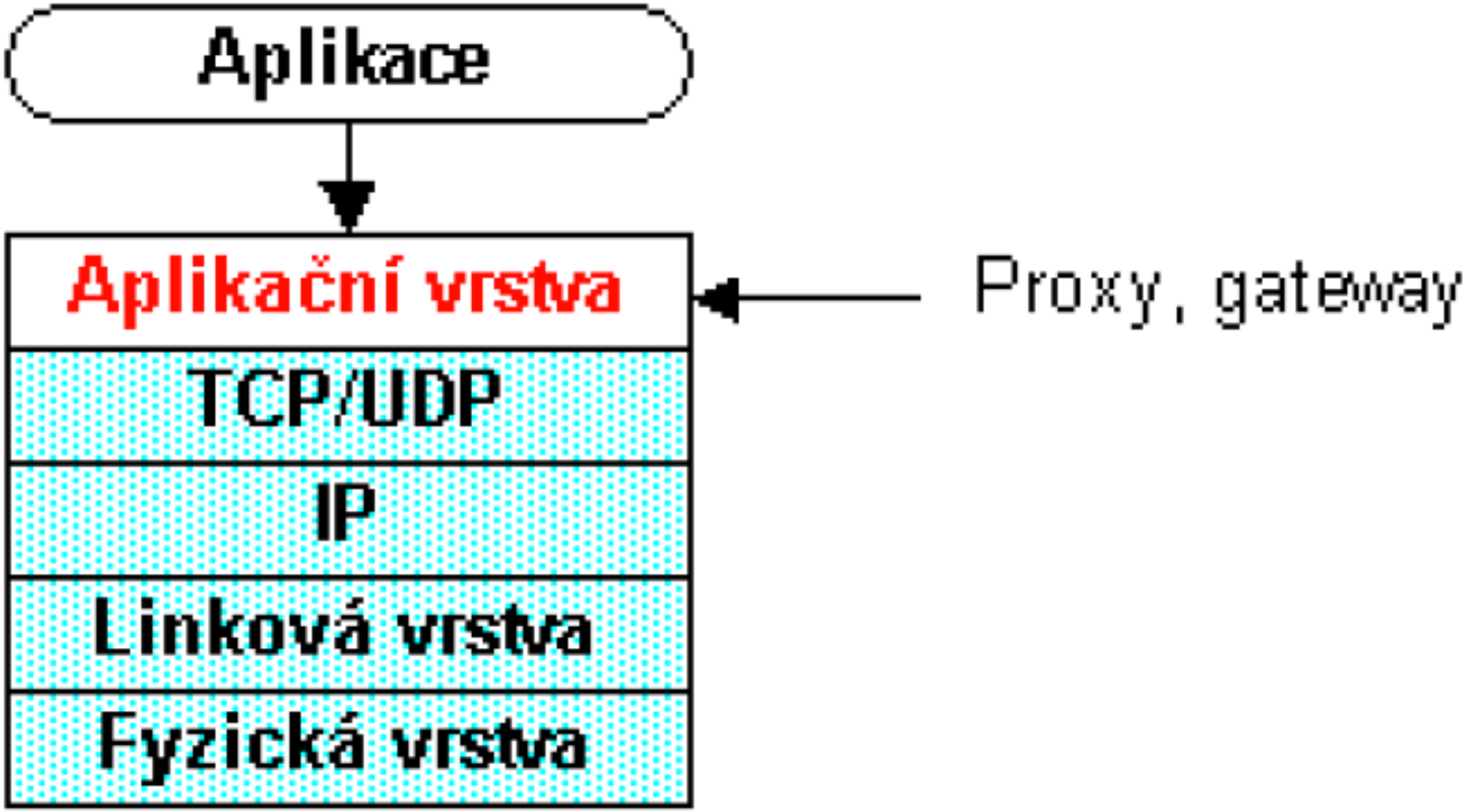
Proxy


Klient
Server
Aplik.
TCP
IP
Link.
Fyz.
Aplik.
Aplik.
TCP
TCP
IP
IP
Link.
Link.
Fyz.
Fyz.
Aplik.
TCP
IP
Link.
Fyz.

Proxy

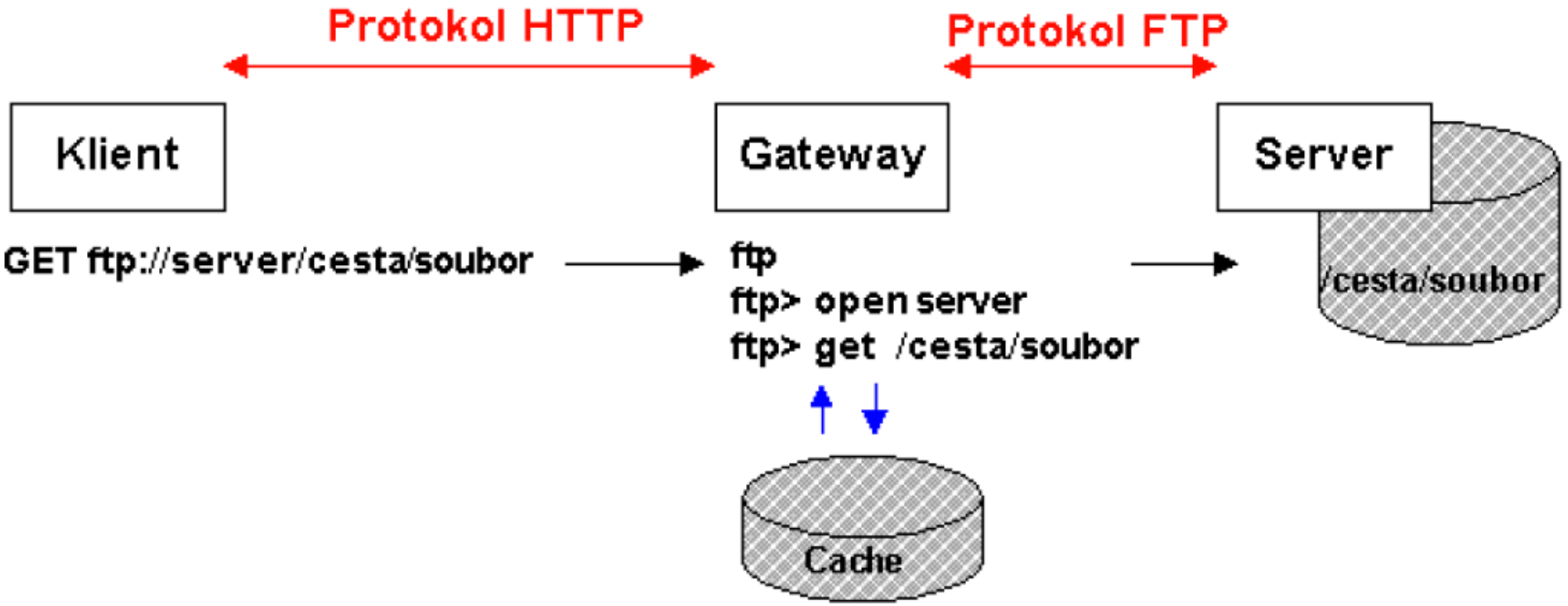
- Proxy pracuje na aplikační vrstvě, tj. proxy vidí do aplikačního protokolu. Je moţné provádět i filtraci při předávání mezi serverovou a klientskou částí proxy. Jelikoţ se jedná o filtraci na aplikační vrstvě, tak je možné touto filtraci např. v protokolu FTP zakázat příkaz PUT a povolit pouze GET.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

Proxy, gateway



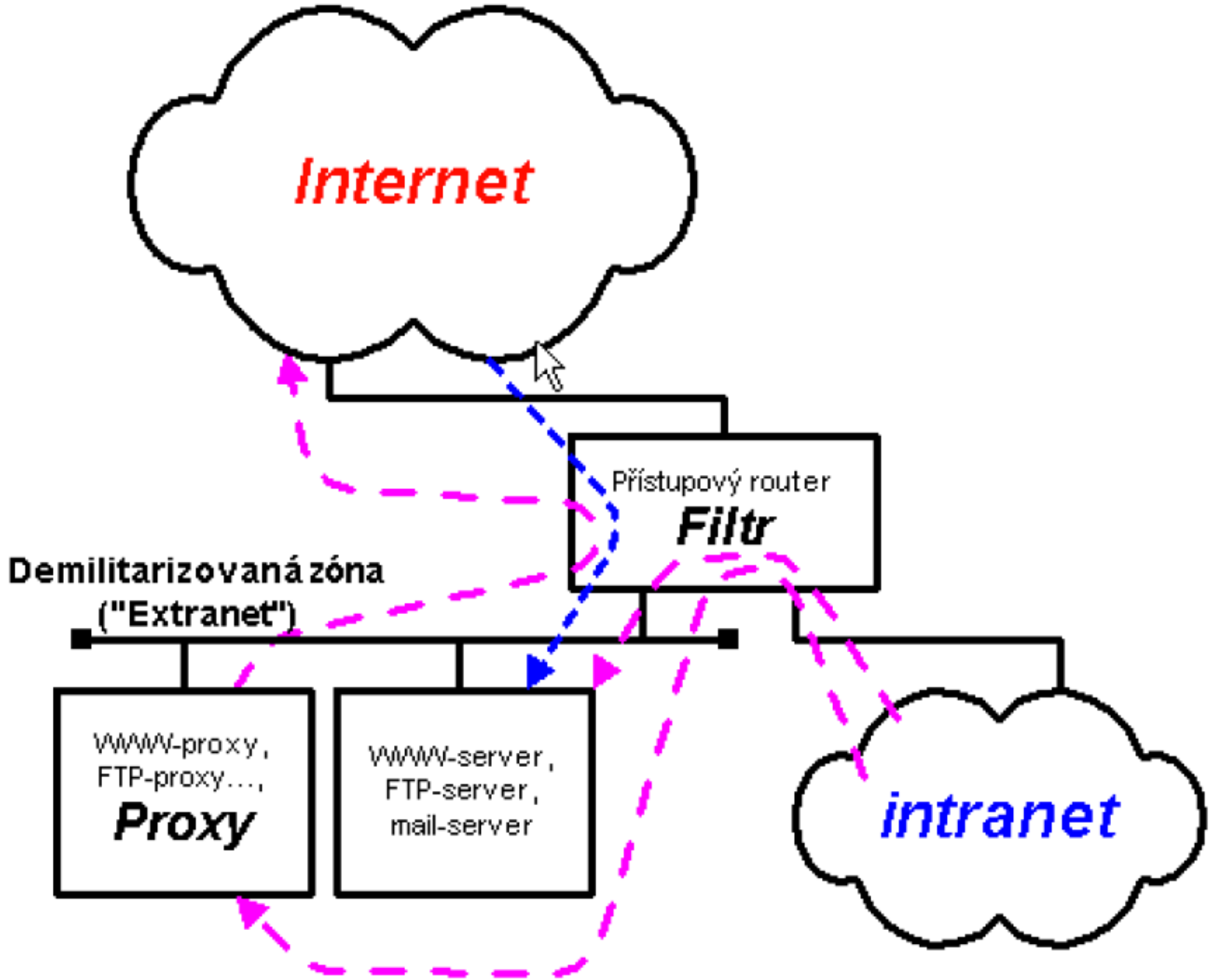
Gateway

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



Oblíbené řešení

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


Internet
Přístupový router
Filtr
Demilitarizovaná zóna
("Extranet")
WWW-proxy,
FTP-proxy...,
Proxy
WWW-server,
FTP-server,
mail-server
intranet

- 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 Interentu 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 moţné, aby aplikace nabízené uţivatelům Internetu (běžící např. na WWW-serveru v Extranetu) přistupovaly k datům v intranetu.

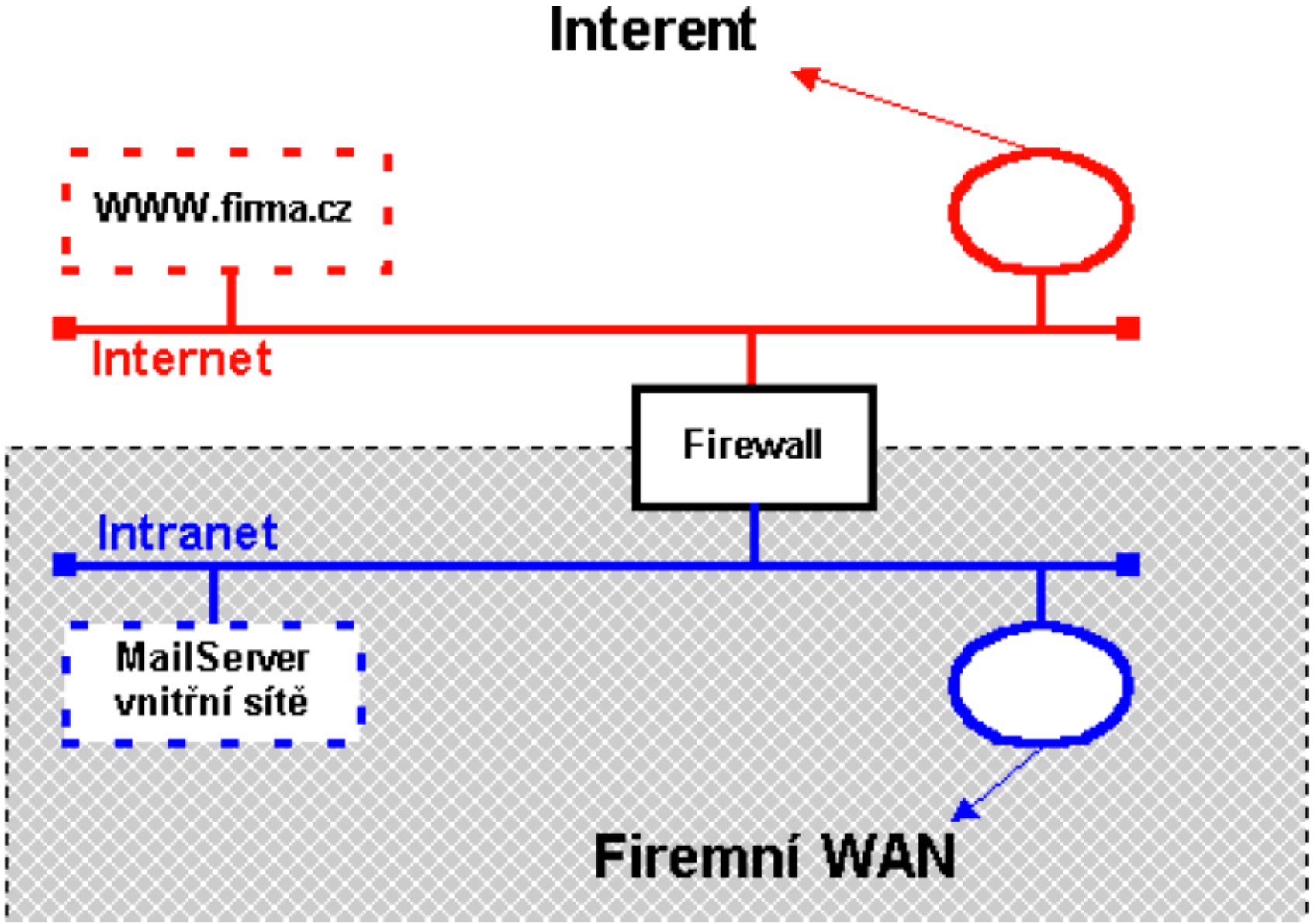
Wrapper

- Wrapper je program, který se automaticky spuští před tím, neţ 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 vytvářená pomocí různých autentizačních pomůcek.

Firewall

- Firewall je dedikovaný počítač nebo soustava počítačů, která nabízí komplex služeb - filtraci, proxy, autentizovaným uţivatelům přístup z Interentu 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 běţí a v případě nečekaných změn systémových souborů generovat událost.

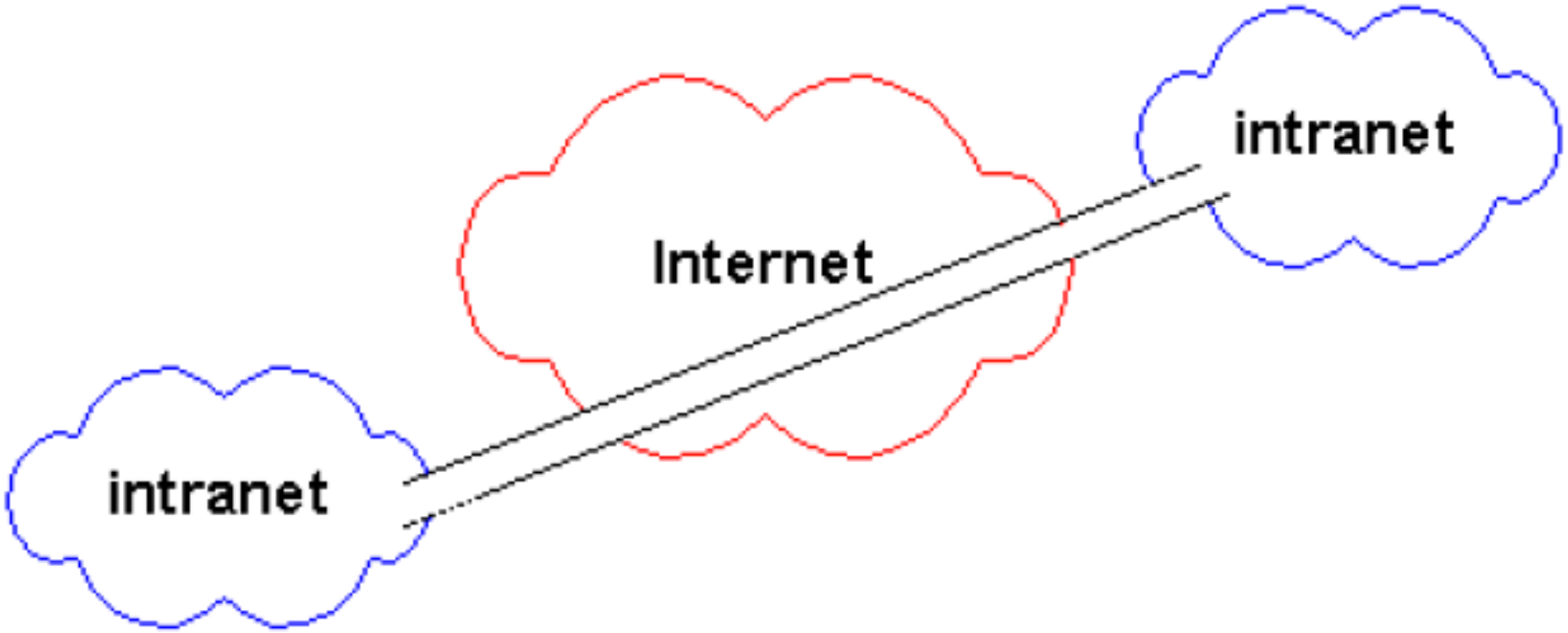
Firewall


Interent
www.firma.cz
Internet
Firewall
Intranet
MailServer
vnitřní sítě
Firemní WAN

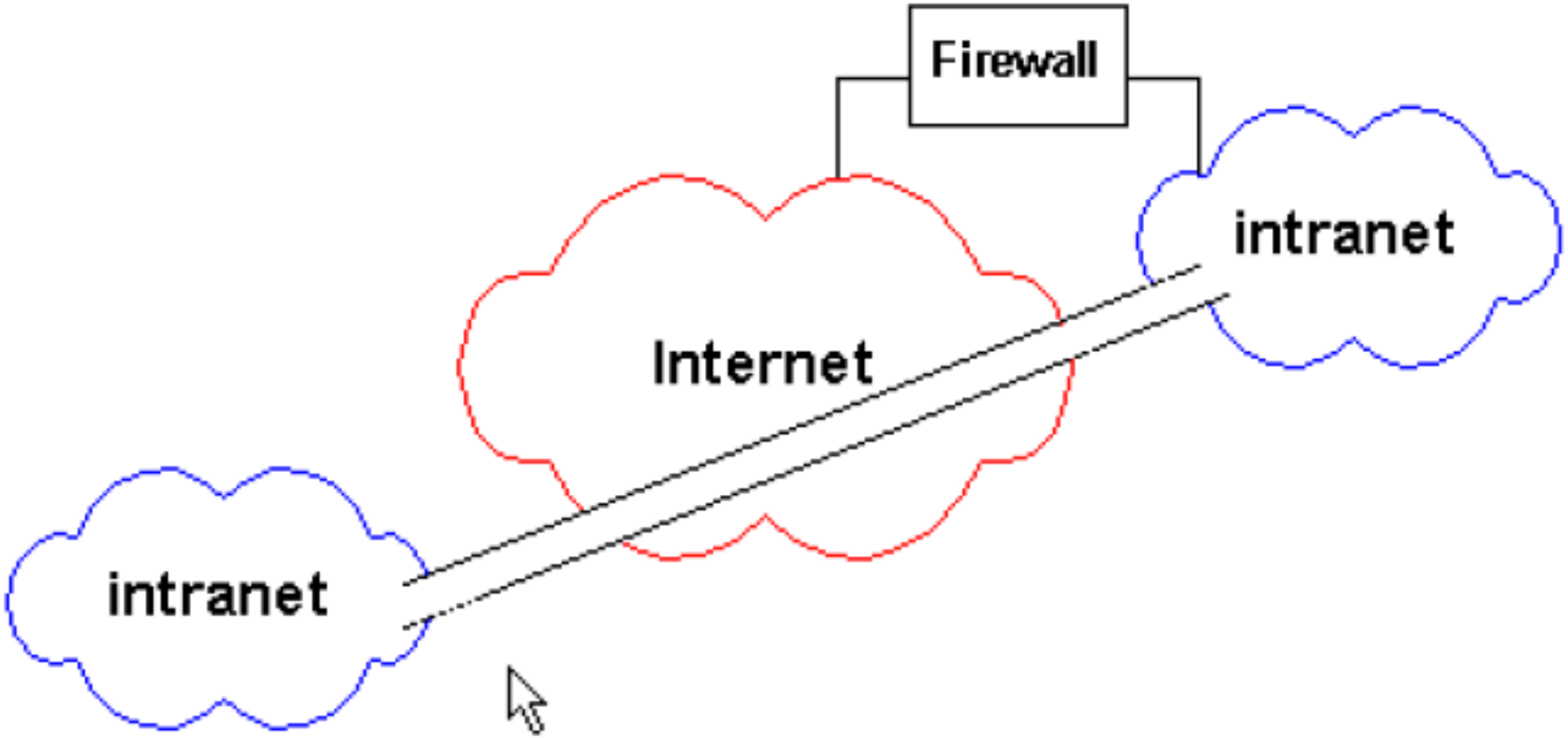
Tunel

- 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.

Tunel



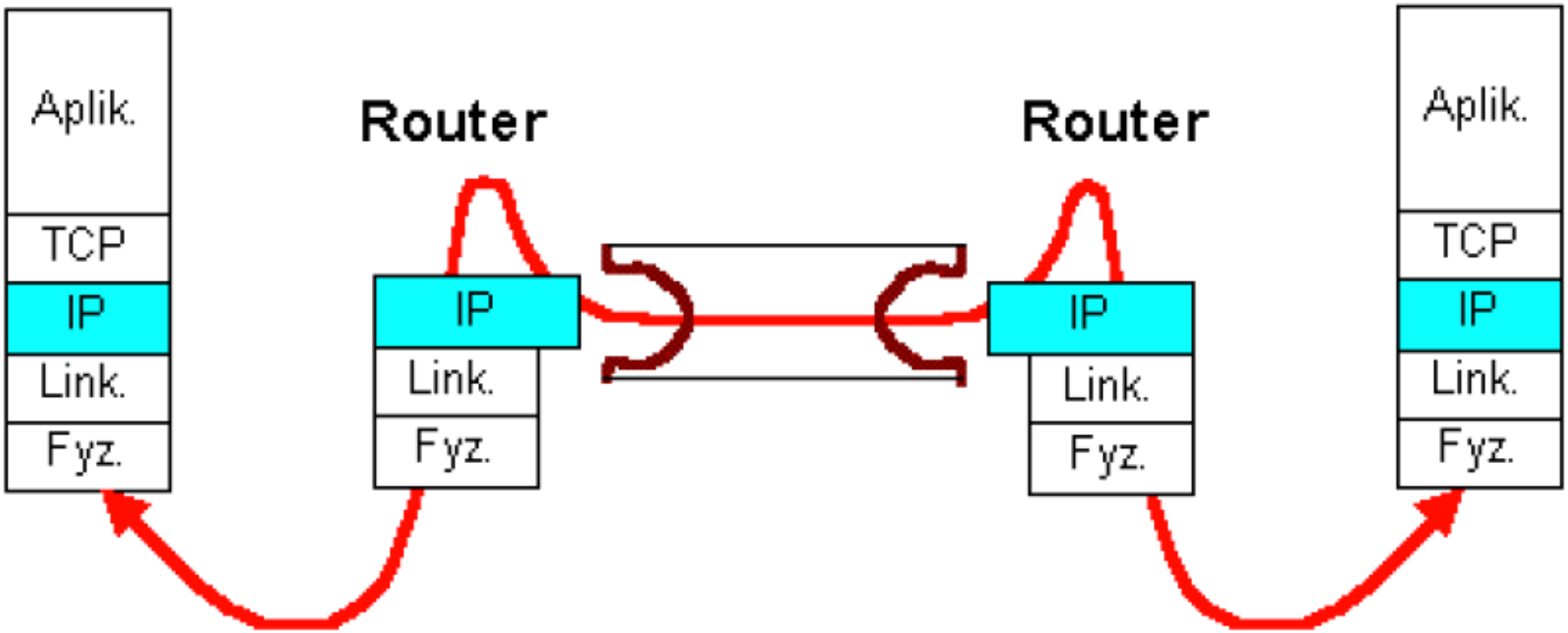
Tunel



Tunel

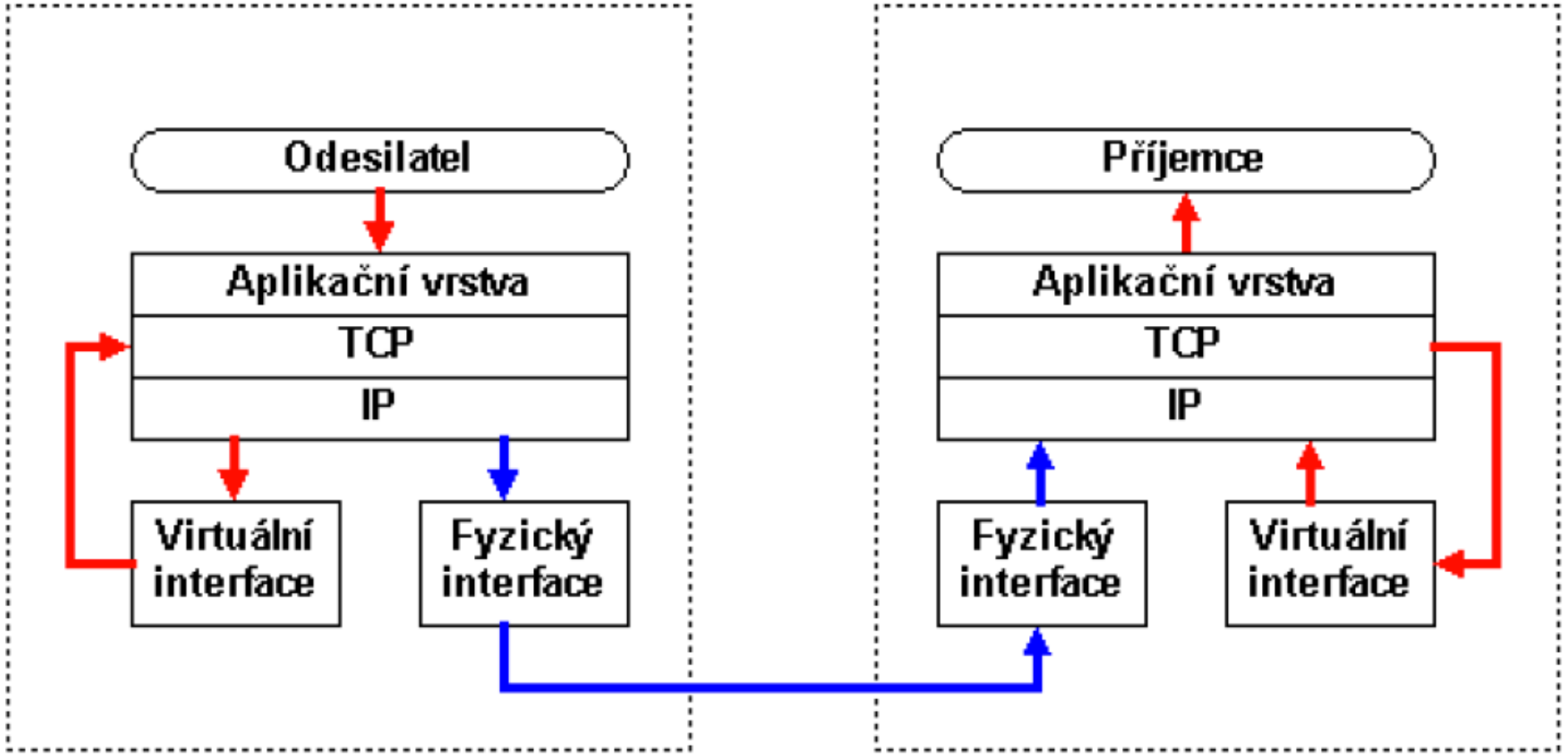
- Zabezpečení přenosu dat může být prováděno na přístupových routerech tak, že v každém přenášeném datagramu se ponechá IP-záhlaví a TCP-záhlaví (resp. UDP) a datová část každého paketu se na vstupu do Internetu šifruje a na výstupu dešifruje. Takto pracují např. tunely realizované routery firmy CISCO.

Tunel


Aplik.
TCP
IP
Link.
Fyz.
Router
IP
Link.
Fyz.
Router
IP
Link.
Fyz.
Aplik.
TCP
IP
Link.
Fyz.

Tunel

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


Odesilatel
Aplikační vrstva
TCP
IP
Virtuální interface
Fyzický interface
Příjemce
Aplikační vrstva
TCP
IP
Fyzický interface
Virtuální interface