2 Sítě na bázi IP a jejich bezpečnost(2/2)

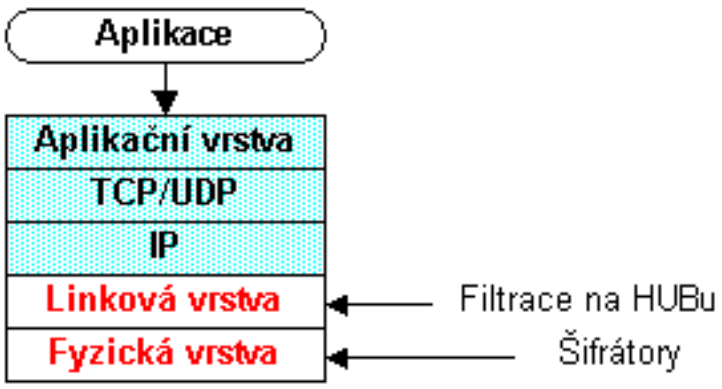
2.1 Jak se bezpečně připojit k Internetu?

Dnes je již obecně vžilo, že LAN nesmí procházet jiným územím než územím vlastní firmy. Avšak na LAN data nebývají nikterak zabezpečena, takže je-li více zaměstnanců na jednom segmentu Ethernetu, pak si vzájemě mohou odchytit hesla v případě, že používají např. protokoly TELNET, FTP, POP3, HTTP atd. Odchytávání hesel lze značně ztížit použitím přepínaných (switched) LAN, tj. každý uživatel má svůj segment LAN a data se opakují jen na ty segmenty, kde je to bezpodmínečně nutné.

Na aktivních prvcích strukturované kabélaže lze také nastavit komunikaci tak, aby spolu mohly na linkové vrstvě komunikovat pouze konkrétní stanice.

Ovšem ani přepínané LAN nezabrání tomu, aby před budovou nezaparkovala dodávka s odposlouchávacím zařízením, které je schpno monitorovat provoz na Vaší strukturované kabeláži a získat tak např. hesla. Takovéto odposlouchávání je zase možné ztížit použitím stíněných rozvodů strukturované kabeláže atd. Samostatným problémem je zabezpečení bezdrátových sítí.

Na sériových linkách (WAN) se pro zabezpečení dat často používají šifrátory, tj. zabezpečnení se provádí na fyzické vrstvě. Dešní routery ale umí šifrovat na IP-vrstvě což je v mnoha případech efektivnější.



Možnosti připojení sítě do Internetu z hlediska bezpečnosti:

- Žádné připojení, tento typ připojení se obecně doporučuje pro připojení vojenských, ale i vybraných průmyslových komplexů strategického významu. Obsluha takovýchto zařízení může mít k dispozici Internet (např. pro mail) jedině na jiném počítači, který není žádným způsobem propojen se strategickou technologií.
- Plné připojení do Internetu bez jakýchkoliv bezpečnostních omezení je druhým extrémem, se kterým se setkáváme např. v akademické sféře.
- Propojeni intranetu s Internetem, tj. máme vybudovanou vnitropodnikovou (privátní) síť na technologijích, které z bezpečnostních důvodů nesnesou přímé připojení intranetu s Interentem. Pro oddělení se používá filtrace, proxy, wrappery a firewally. Speciálním problémem ja pak otázka jak využít Internetu k vytvoření privátní sítě, tj. vytváření tunelů Internetem.
- Plné připojení do Internetu s tím, že používáme takové technologie, které minimalizují bezpečnostní rizika Internetu. Tj. na serverech nepoužíváme služby jako TELNET, FTP, NFS, HTTP atd., ale pouze "bezpečné" služby: SSH, HTTPS, S/MIME atd.

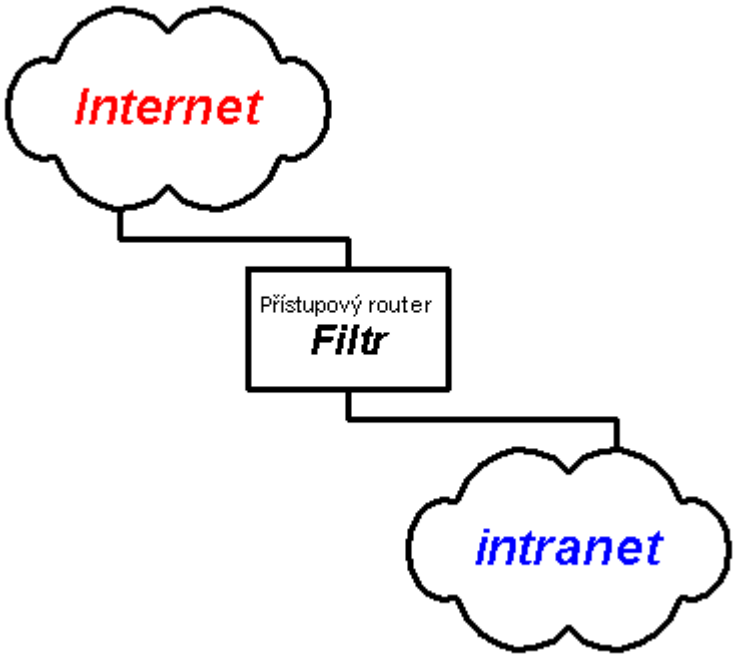
2.2 Intranet

Intranet –vnitřní síť od Internetu izolována pomocí:

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

2.2.1 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 použit klasický router (např. CISCO), ale i počítač se dvěma síťovými rozhraními a operačním systémem UNIX, Novell, NT atd.



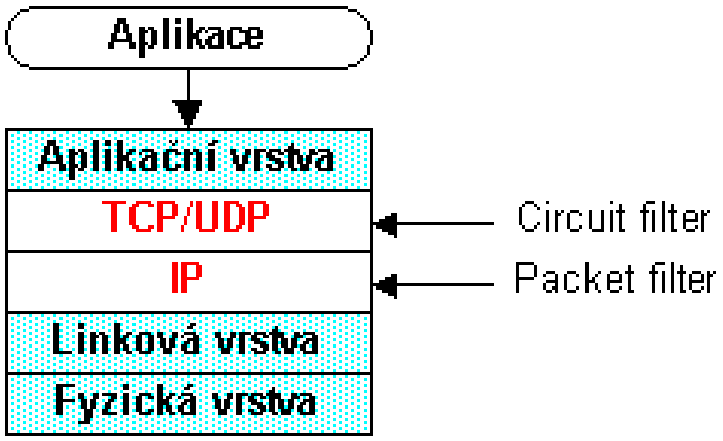
Filtrací je možné docílit, aby se klienti z intranetu dostali na servery v Internetu, ale aby uživatelé Internetu neměli přístup (neohrožovali) servery intranetu. K dosažení tohto cíle je nutné provádět filtraci jak na úrovni protokolu IP, tak současně i fltraci protokulou TCP (resp. UDP).

Filtr se rozhoduje na základě informací uložených v záhlaví IP-datagramu a záhlaví TCP-paketu (resp. UDP-paketu). Filtr "nevidí" do aplikačního protokolu.

Docílit pomocí filtrace stavu, aby klienti vnitřní sítě mohli na servery v Internetu a klienti z Internetu nemohli na servery v intranetu lze snadno pro protokoly TELNET, HTTP, HTTPS, POP, klienty News a několik dalších. Problematický je však

provoz protokolů FTP, SMTP a všech aplikačních protokolů využívajících UDP (tj. zejména DNS). Problém FTP se řeší pomocí tzv. pasivního FTP. Problémy s SMTP a DNS se řeší tak, že se povolí pouze komunikace mezi jedním konkrétním počítačem v Internetu a intranetem. 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.

Terminologická poznámka: 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.



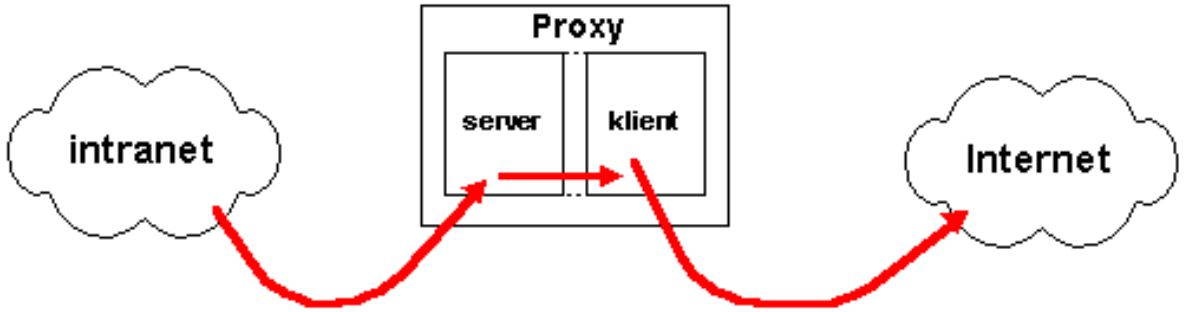
2.2.2 Proxy a gateway

Proxy se instaluje různými zůsoby. Klasickým zapojením je proxy se dvěma síťovými rozhraními (jedno do Internetu a druhé do intranetu).

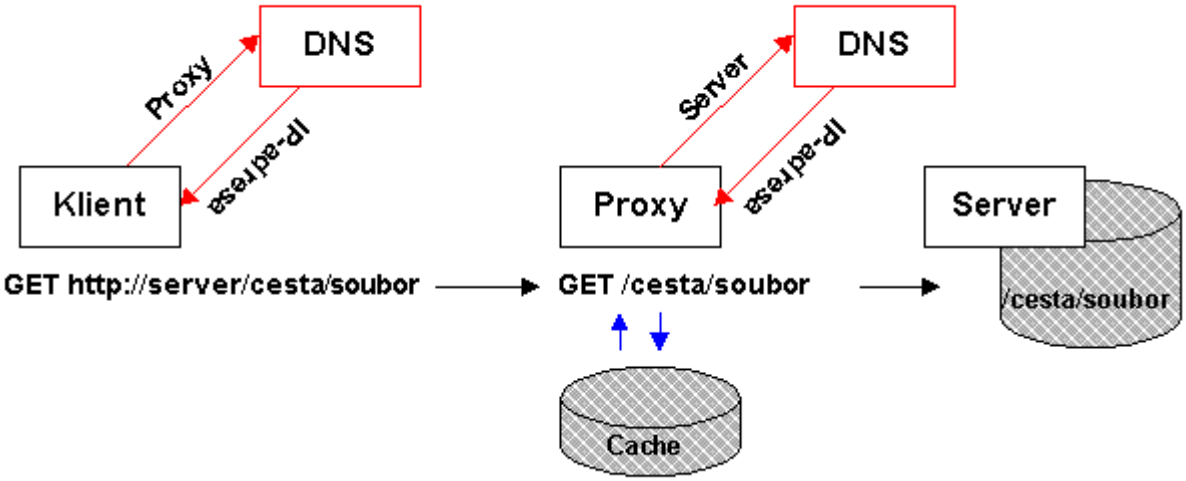
Proxy je aplikace, která je v klasickém případě spuštěná na počítači, který leží na rozhraní intranetu a Internetu. Přitom obě sítě nejsou vzájemně přímo dostupné. Pro přístup z jedné sítě do druhé je nutné se nejprve přihlásit na počítač s proxy.

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.



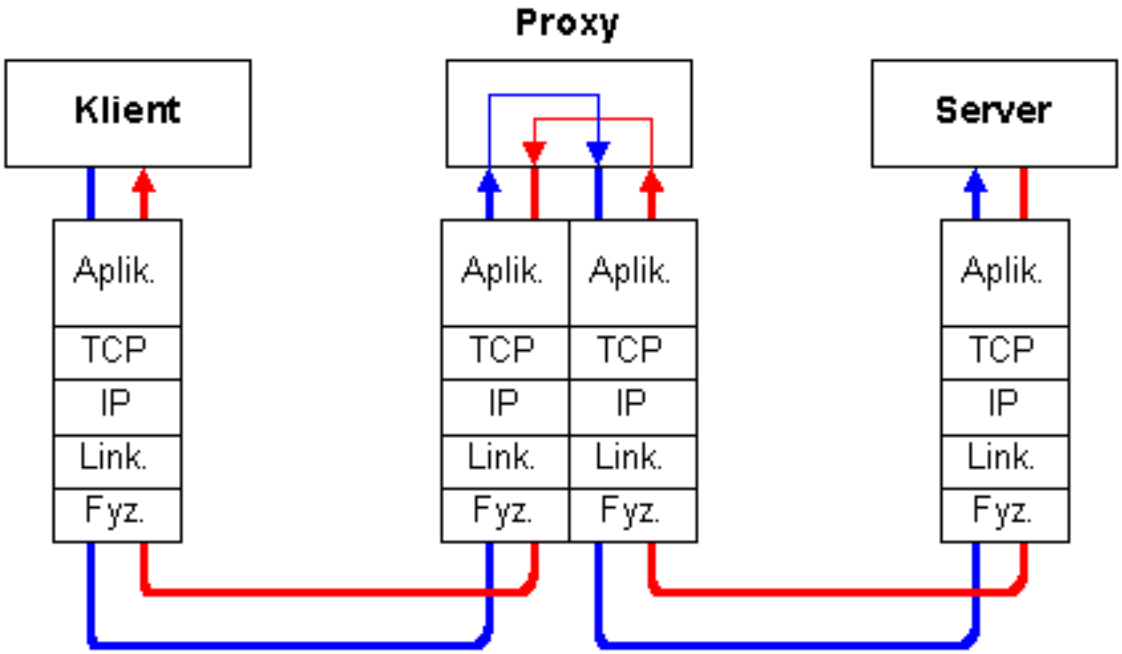
Konkrétně pro protokol HTTP:



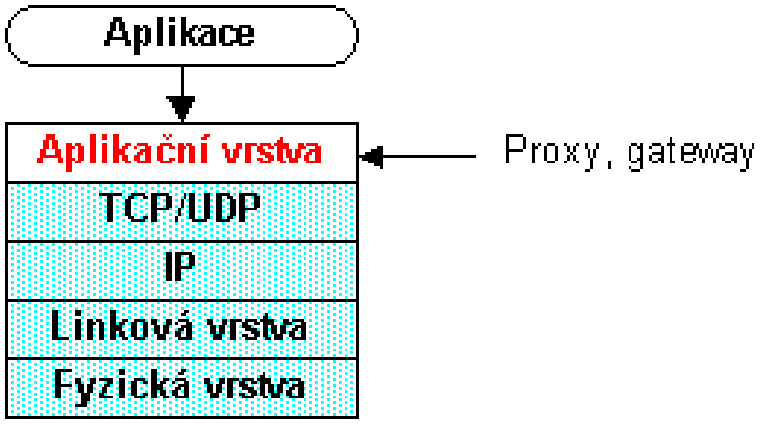
Kategorizace:

- **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.

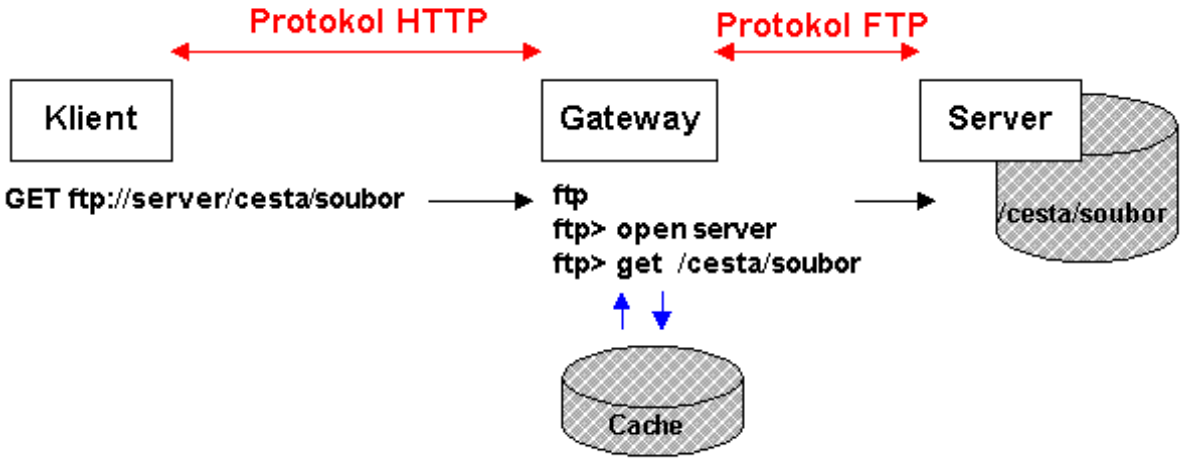
- **Transparentni proxy** - klient adresuje přímo cílový server. Transparentní proxy akceptuje spojení na cílový server a z akceptovaných IP-datagramů se dozví adresu cílového serveru, se kterým klientská část proxy okažitě navazuje spojení. Z hlediska klienta se transparentní proxy jeví jako router,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



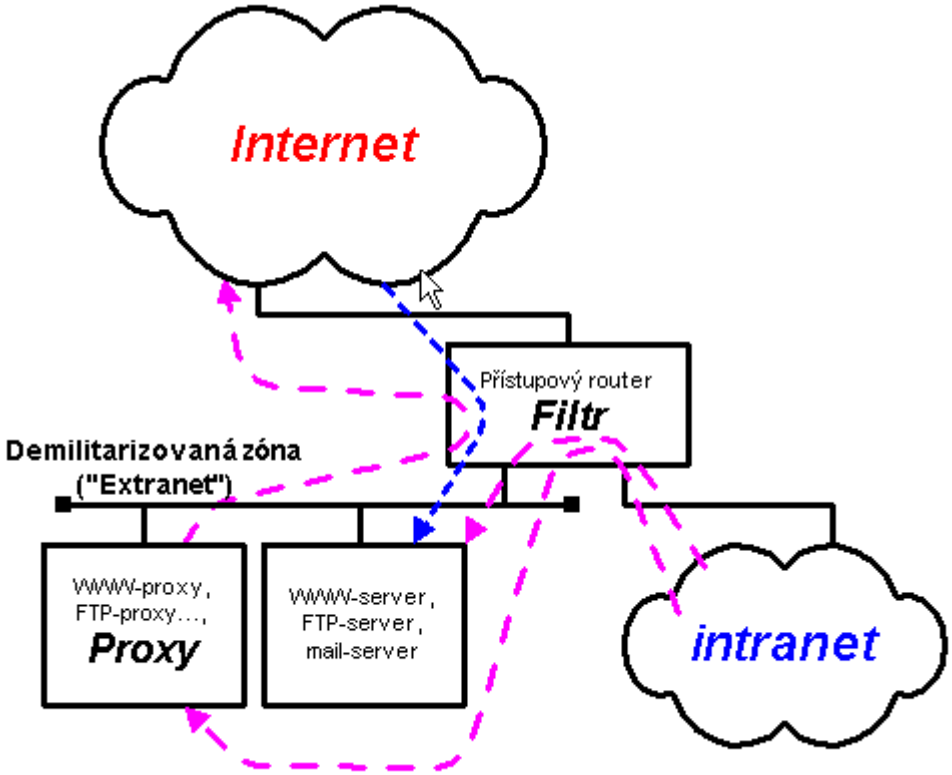
Proxy pracuje na aplikační vrstvě, tj. proxy vidí do aplikačního protokolu. Je možné provádět i filtraci při předávání mezi serverovou a klientskou částí proxy. Jelikož se jedná o filtraci na aplikační vrstvě, tak je možné touto filtraci např. v protokolu FTP zakázat používat říkaz PUT a povolit pouze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



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



V současné době je velmi oblíbená 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 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 možné, aby aplikace nabízené uživatelům Internetu (běžící např. na WWW-serveru v Extranetu) přistupovaly k datům v intranetu.

2.2.3 Privátní (skryté) sítě

Je-li mezi intranetem a Internetem proxy či gateway, pak se navazuje samostatné spojení mezi klientem a proxy a další samostatné spojení mezi proxy a cílovým serverem. Není tedy nutné, aby intranet používal IP-adresy známé v Internetu.
Pro takovéto použití jsou vyhrazeny intervaly IP-adres

10.0.0.0 až 10.255.255.255

172.16.0.0 až 172.31.255.255

192.168.0.0 až 192.168.255.255

Takovéto adresy používají intranety, tj. tyto adresy nejsou jednoznačné, nelze je tedy v Internetu použít, takže počítače intranetu jsou tak chráněny proti přímému navazování spojení.

Není-li na rozhraní mezi Internetem a intranetem proxy nebo gateway, pak je možné použít Network Adress Translator (NAT), který je součástí software přístupových routerů či je realizován softwareově. Ochrana pomocí NAT je obecně chápána jako slabší prostředek.

2.2.4 Wrapper

Wrapper je program, který se automaticky spuští 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 nejpolularnější metodou ověřování totožnosti jsou tzv. hesla na jedno použití vytvářená pomocí různých autentizačních pomůcek.

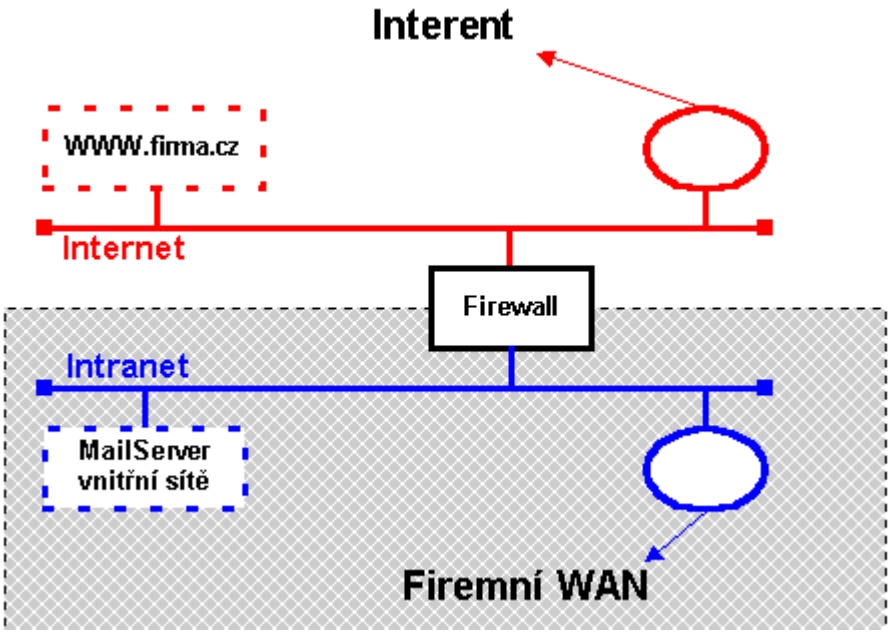
2.2.5 Firewall

Firewall je dedikovaný počítač nebo soustava počítačů, která jako dárkový balíček nabízí komplex služeb - filtraci, proxy, autentizovaným uživatelům 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.:

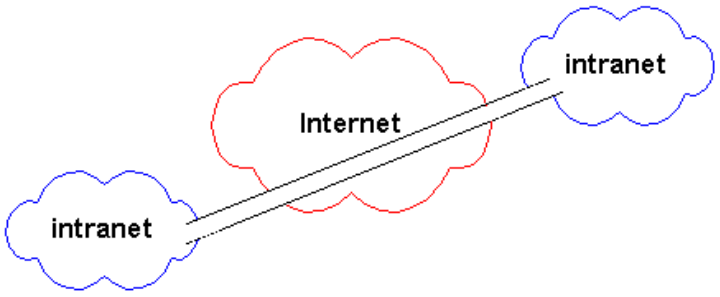
- Potencionálního útočníka zařadit na černou listinu počítačů, se kterými už dále nekomunikuje.
- Uzavřít atakovanou službu, popř. celý firewall.
- Spustit specifikovaný program, který může např. odeslat zprávu správci firewallu atd.
- Sledovat systém, na kterém firewall běží a v případě nečekaných změn systémových souborů generovat událost.

Jelikož jsou na jednopočítačový firewall kladeny velké bezpečnostní nároky, tak není možné, aby na něm běžely aplikace, na které budou přímo přistupovat jednotliví uživatelé (např. WWW-server, mail server atd.). WWW-server se umísťuje na demilitarizovanou zónu a poštovní server, interní WWW-server do vnitřní sítě.



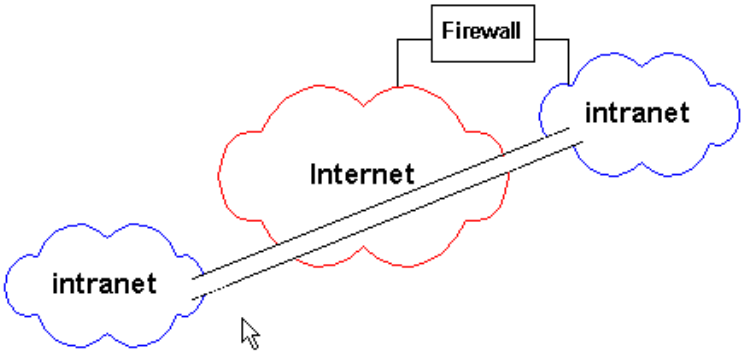
2.3 Tunel

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.

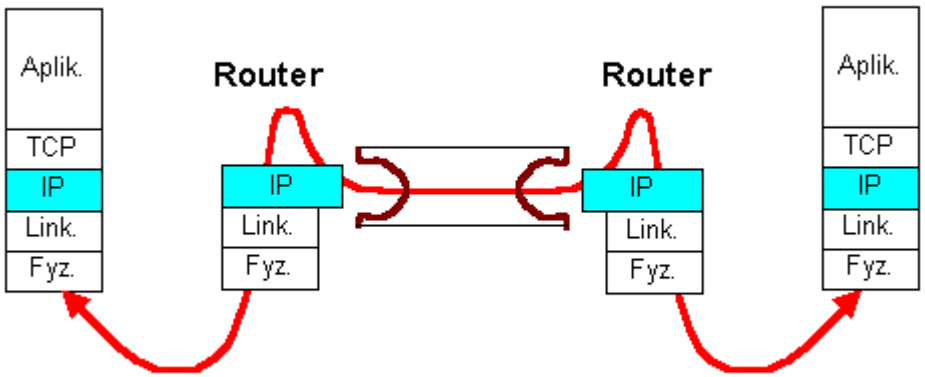


Není ani vyloučeno, aby jedna lokalita měla spojení do Internetu.

Vzdálenou lokalitou propojenou přes tunel může být síť, ale i samostatný uživatel.

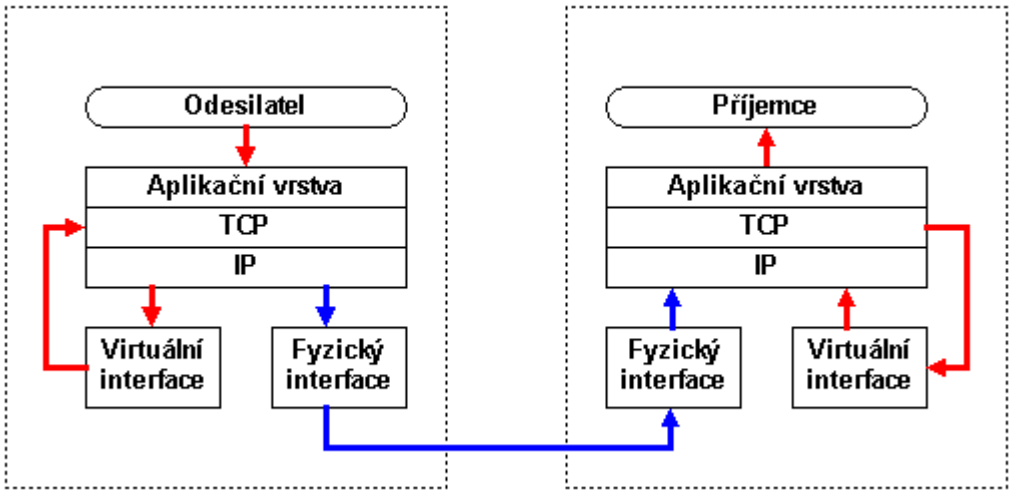


Zabezpečení přenosu dat může být prováděno na přístupových routerech tak, že v každém přenášeném datagramu se ponechá IP-záhlaví a TCP-záhlaví (resp. UDP) a datová část každého paketu se na vstupu do Internetu šifruje a na výstupu dešifruje. Takto pracují např. tunely realizované routery firmy CISCO.



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.



2.4 Bezpečné služby

Pro autentizaci tyto nástroje používají asymetrickou kryptografii. Pro přenos vlastních dat pak používají symetrickou šifru.

2.4.1 PGP

Program PGP je určen pro šifrování a elektronické podepisování souborů (dávek). Takoto zašifrovaná zpráva pak může být přenášena elektronickou poštou, na magnetickém médiu či jiným způsobem. Příjemce zprávu jako dávku dešifruje a následně využije (přečte či data počítačově zpracuje).

2.4.2 SSH

SSH je tvořeno mj. programy:

- ssh (pro vzdálené přihlášení)
- scp (pro přenos souborů)
- program na generování dvojice veřejný/soukromý klíč

Program ssh (resp. scp) je určen pro interaktivní práci. Nahrazuje "nebezpečné" programy: rlogin či telnet. Program scp nahrazuje programy rcp či ftp. Programy pro vzdálené přihlášení a přenos souborů se používají pro práci na serveru. Dnes je používají nejčastěji správci systému či vývojáři, tj. úzký okruh uživatelů pro které není na překážku předat správci serveru svůj veřejný klíč např. na disketě.

2.4.3 Bezpečný mail

Pod pojmem bezpečný mail dnes rozumíme takový systém, který zprávu zašifruje (resp. elektronicky podepíše či obojí) a odešle běžným (nezabezpečeným) elektronickým mailem, tj. protokolem SMTP či ESMTP. Výhodou takovéhoto řešení je, že nevyžaduje žádný zásah do stávajících poštovních systémů Internetu.

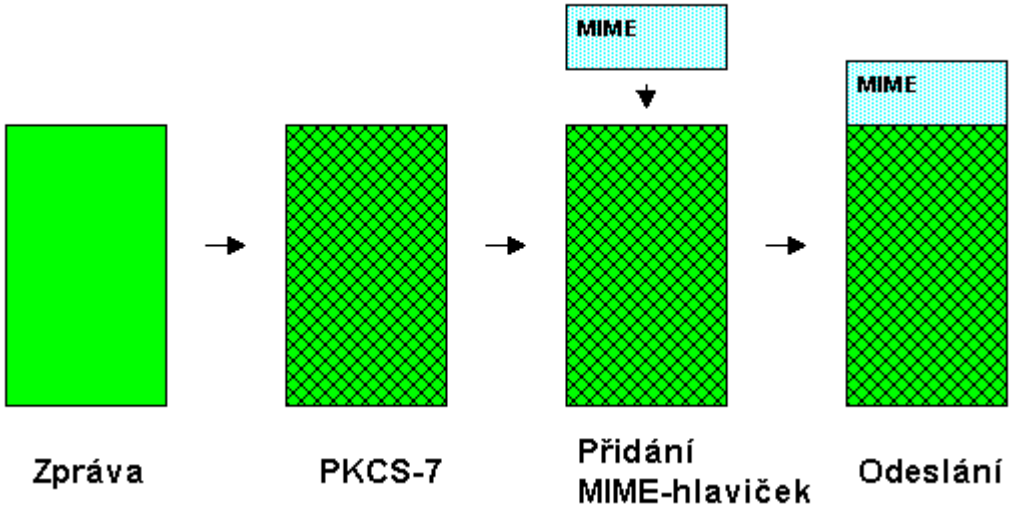
Systémy, které se snaží nešifrovanou zprávu přenášet bezpečným kanálem (např. SMTP či POP over SSL) se neujaly, protože by vyžadovaly zásahy do stávajícího poštovního systému Internetu.

Nejjednodušším mechanizmem je využití PGP pro šifrování či elektronické podepisování. Tj. zprávu pořídíme textovým editorem, zašifrujeme PGP a odešleme stávající poštovním mechanizmem. Toto řešení se nejeví jako perspektivní, protože se špatně automatizuje (i když i pro PGP se objevilo MIME/PGP). Řešením, které se asi prosasadí je S/MIME. S/MIME přinesla firma Netscape. Výhodou tohoto řešení je mj. i to že je velmi podbné interaktivnímu SSL, takže obojí lze řešit pomocí týž knihoven, čehož firma Netscape i využívá.

S/MIME se orientuje na využití certifikátů. Pro bezpečný mail jsou vhodné i certifikáty certifikačních autorit třídy 1 jejiž certifikáty lze získávat jednoduše bez osobní přítomnosti uživatele na certifikační autoritě.

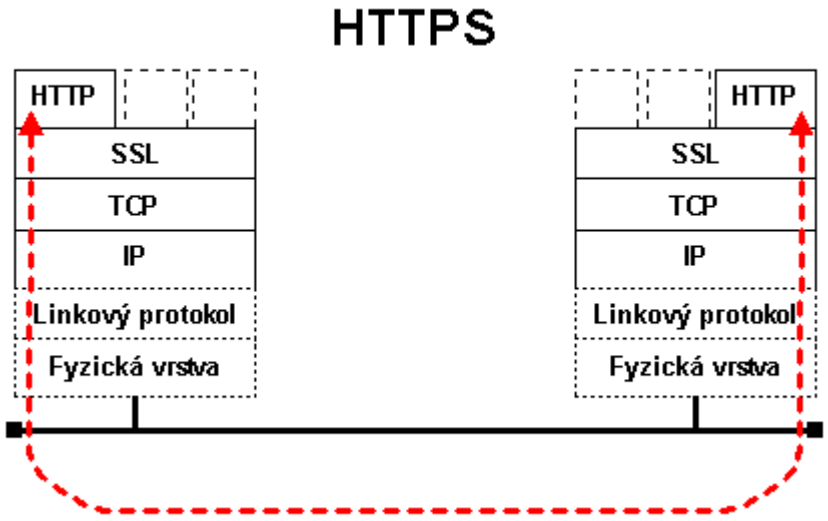
S/MIME je velice vhodné pro veškeré aplikace mající dávkový charakter. Umožňuje autentizaci, šifrování i elektronický podpis

jednotlivých zpráv (elektronický podpis transakcí není např. u SSL zabezpečen).



2.4.4 SSL a HTTPS

SSL je "prezentrační vrstva" umísťující se mezi protokol TCP a aplikační protokoly. SSL umožňuje prokazovat totožnost serveru. V případě neanonymních serverů může být požadováno prokazování totožnosti klienta. SSL umožňuje se autentizovaně přihlásit aniž by se sítí přenášelo heslo. Dále SSL zabezpečuje šifrování a integritu přenášených dat.



SSL se rovněž orientuje na využívání certifikátů.

SSL slouží aplikačním protokolům k zabezpečnení přenosu, tj. bezpečnostní problému řeší za aplikační protokoly. Podle toho jaký aplikační protokol využívá SSL, pak hovoříma např. o Secure LDAP (LDAP over SSL), HTTPS (HTTP over SSL) atd.

SSL bere data od aplikačního protokolu a šifrované je předává protoklu TCP, tj. nevidí do aplikačních dat. Není tedy schopno rozlišovat jednotlivé aplikační transakce (např. prodej jedné letenky) a jednotlivé transakce nemůže tedy ani elektronicky podepisovat. Tento problém si musí řešit aplikace sama. Otázkou pak ale je, že když si tento problém bude řešit aplikace sama, tak už si i sama vyřeší všechny ostatní bezpečnostní aspekty, tj. obejde se bez SSL.

SSL slouží pro autentizaci a pro zabezpečení dat mezi klientem a serverem. Znemožňuje přístup neautorizovaným uživatelům, dále zabezpečuje privátnost (šifrování) přenášených dat a zabezpečuje integritu přenášených dat pomocí kontrolního součtu (nikoliv elektronického podpisu), ale nezabezpečuje elektronický podpis jednotlivých transakcí.

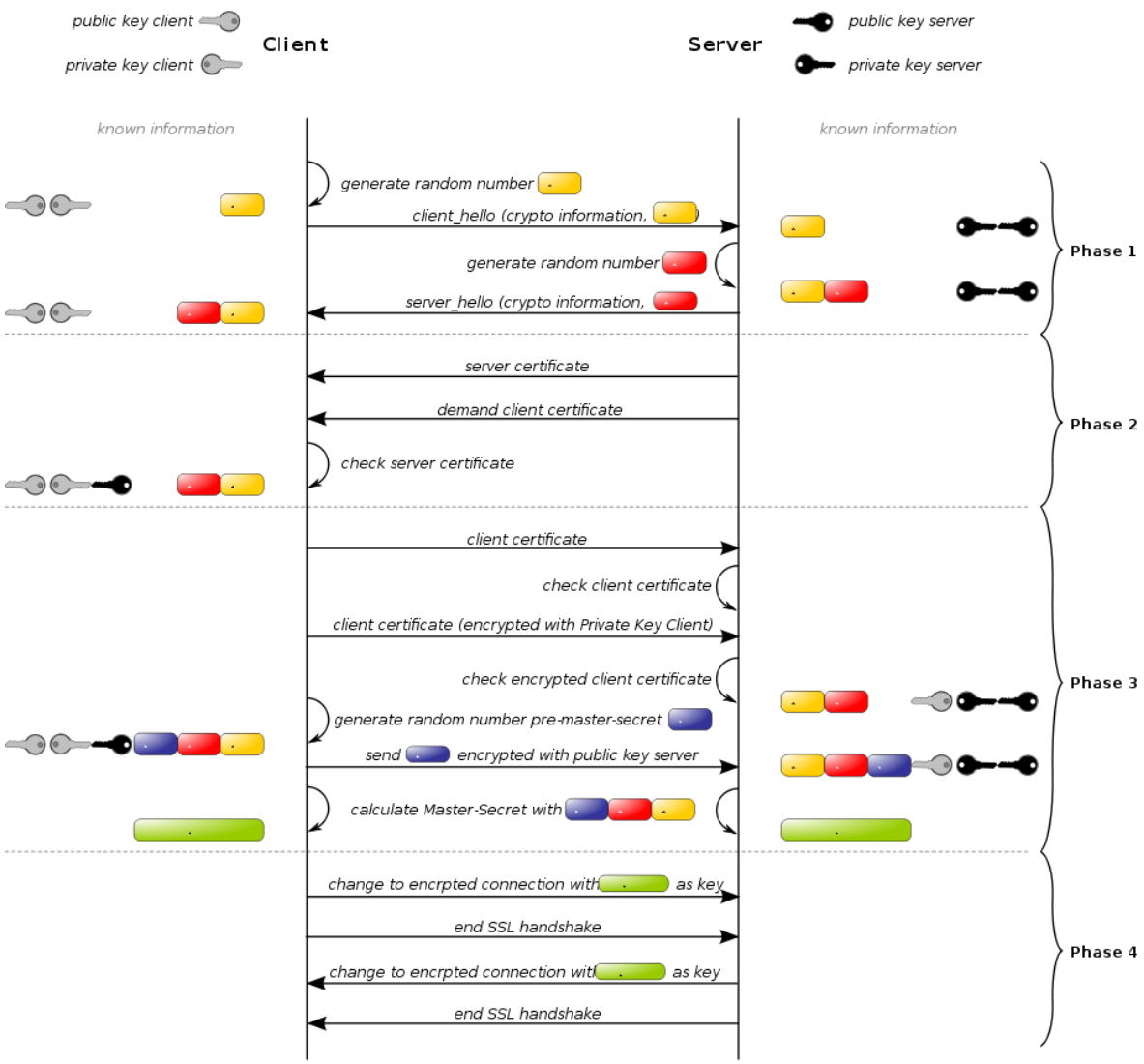
Protokol SSL se využívá pro bezpečnou komunikaci s internetovými servery pomocí HTTPS,.po vytvoření SSL spojení je komunikace mezi serverem a klientem šifrovaná.

Ustavení SSL spojení funguje na principu asymetrické šifry[1], kdy každá z komunikujících stran má dvojici šifrovacích klíčů – veřejný a soukromý. Ustavení SSL spojení (SSL handshake) probíhá v principu následovně:

- Klient pošle serveru požadavek na SSL spojení, spolu s různými doplňujícími informacemi (verze SSL, nastavení šifrování atd.).
- Server pošle klientovi odpověď na jeho požadavek, která obsahuje stejný typ informací a hlavně certifikát serveru.

[1] Veřejný klíč je možné zveřejnit a pokud tímto klíčem kdokoliv zašifruje nějakou zprávu, je zajištěno, že ji bude moci rozšifrovat jen majitel použitého veřejného klíče svým soukromým klíčem.

- Podle přijatého certifikátu si klient ověří autentičnost serveru. Certifikát také obsahuje veřejný klíč serveru.
- Na základě dosud obdržených informací vygeneruje klient základ šifrovacího klíče, kterým se bude šifrovat následná komunikace. Ten zašifruje veřejným klíčem serveru a pošle mu ho.
- Server použije svůj soukromý klíč k rozšifrování základu šifrovacího klíče. Z tohoto základu vygenerují jak server, tak klient hlavní šifrovací klíč.
- Klient a server si navzájem potvrdí, že od teď bude jejich komunikace šifrovaná tímto klíčem. Fáze handshake tímto končí. Je ustaveno zabezpečené spojení šifrované vygenerovaným šifrovacím klíčem.



Během první fáze ustanovení bezpečného spojení si klient a server dohodnou kryptografické algoritmy, které budou použity: pro výměnu klíčů např. RSA, Diffie-Hellman nebo DSA; pro symetrickou šifru: IDEA, DES, 3DES nebo AES; pro hašovací funkce: MD5 nebo SHA, viz literatura.

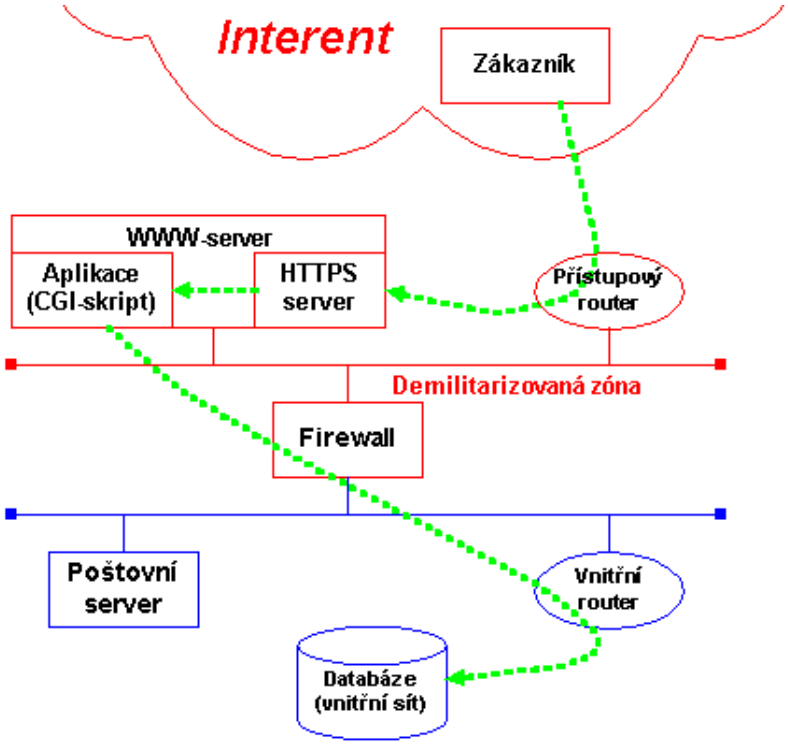
2.4.5 Certifikáty

Certifikát je datová struktura (řetězec bitů) pomocí které se zveřejňují údaje o uživateli a zejména uživatelův veřejný šifrovací klíč (v případě RSA šifer). Certifikát je elektronicky podepsán (ověřen) certifikační autoritou. Z certifikátu je možné zíkat veřejný
šifrovací klíč uživatele, který je možné použít k prokazování totožnosti uživatele. V případě, že certifikát obsahuje šifrovací klíč
určený také k šifrování dat, pak je možné i tento klíč z certifikátu použít k šifrování dat odesílaných uživateli.

2.5 Příklad realizace

Problém nabídky dat pomocí protokolu HTTPS spočívá v tom, že data jsou umistěna ve vnitřní síti za firewallem. Přitom WWW-server musí být umístěm před firewallem, tj. musí být dostupný z Internetu. Aby byl možný z WWW-serveru přístup na data ve vnitřní síti, tak musí být umístěn v demilitarizovéné zóně firewallu, tj. na LAN firewallu, která je chráněna filtrací na přístupovém routeru do Internetu.

Firewall je nastaven jako circuit filter pro komunikaci mezi WWW-serverem a databází ve vnitřní síti. Pro filtraci je nutné nastavit jen minimalní možnost průchodu firewallem tak, aby komunikace ještě bzla možná. Existuje i druhá varianta konfigurace firewallu, kdy se firewall nekonfiguruje jako filter, ale jako generická proxy umožňující opět pouze komunikaci mezi WWW-serverem a databází.



Literatura

Alena Kabelová, Libor Dostálek: Velký průvodce protokoly TCP/IP a systémem DNS, Computer Press, Praha, ISBN: 80-7226-675-6

Libor Dostálek a kol.: Velký průvodce protokoly TCP/IP: Bezpečnost. Computer Press, Praha, ISBN: 807226513X

Simson Garfinkel, Gene Spafford: Bezpečnost v UNIXu a Internetu v praxi. Zabezpečení počítačových systémů. Computer Press, Praha, ISBN: 8072260820

Hacking bez tajemství. Joel Scambray, Stuart McClure, George Kurtz. Computer Press, Praha, ISBN: 80-7226-644-6

Počítačový útok. Detekce, obrana a okamžitá náprava. Chris Prosise, Kevin Mandia. Computer Press, Praha, ISBN: 80-7226-682-9,

PGP - Pretty Good Privacy - Šifrování pro každého. Simson Garfinkel. Computer Press, Praha, ISBN: 8072260545