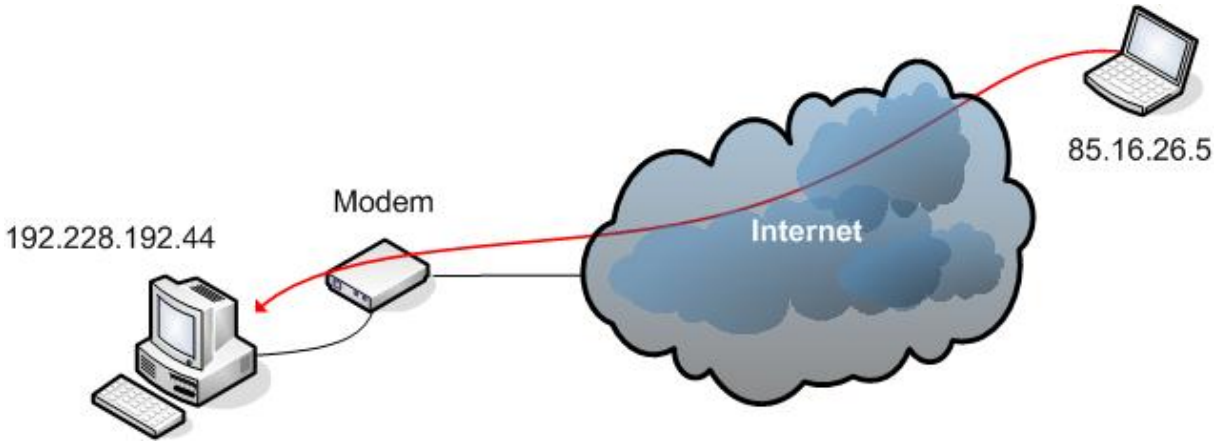
Zabezpečení v síti IP

Problematika zabezpečení je dnes v počítačových sítích jednou z nejdůležitějších oblastí. Uvážíme-li kolik citlivých informací je dnes v počítačích uloženo pak je požadavek na co největší zabezpečení na prvním místě. Dalším důvodem, který klade nároky na zabezpečení sítě a počítačů v ní je množství škodlivého software, který se díky síti internet snadno síří.
V síti IP z pohledu zabezpečení sledujeme 3 hlavní cíle

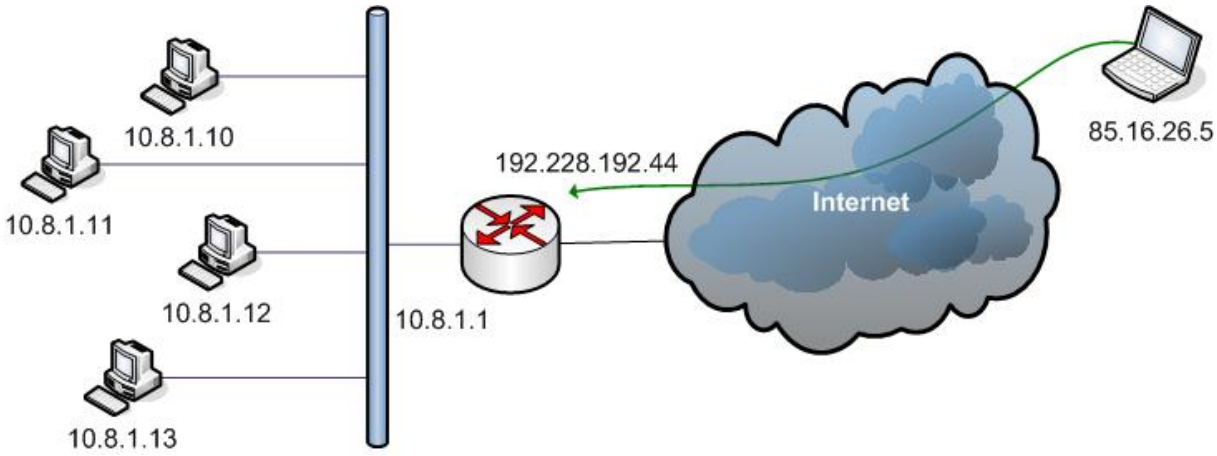
- ochranu před neoprávněným přístupem do sítě
- ochranu před neoprávněným čtením provozu v síti
- zabránit přístupu škodlivého softwaru do sítě



Nezabezpečený přístup k internetu při použití USB modemu

Pokud připojujeme k síti internet počítač např. pomocí USB modemu nebo pomocí modemu s ethernetovým rozhraním, který funguje jako bridge (počítač má veřejnou IP adresu) je nutné jej zabezpečit.
Počítač připojený k síti internet bez firewall v dnešní době vydrží cca. 2 minuty. Poté je nakažen některým s virů. V tomto nejjednodušším případě postačí firewall integrovaný ve Windows XP nebo jiný.

Možností jak zabránit / ztížit přístup k datům v síti pro útočníka je několik. Nejjednodušší ochranu nám poskytuje i služba NAT. Ta je dostupná i v nejlevnějších zařízením pro domácí použití. Typicky ADSL modemy s více ethernetovými porty. Tato zařízení sdružují funkci modemu, routeru a přepínače. Počítačům ve vnitřní přiděluje privátní IP adresy integrovaný DHCP server. Z pohledu ochrany se zde využívá faktu, že privátní IP adresy nejsou v internetu směrovány a tudíž útočník není schopen se připojit přímo k počítači. Z internetu je přístupný pouze router/modem. Na něm ovšem neběží služby typické pro počítač (sdílení souborů apod.). Veškerá komunikace odchází ze sítě LAN s venkovní IP adresou routeru – vnitřní IP adresy jsou tedy pro počítače v internetu neznámé.
Tento způsob ochrany je vhodný a postačující zejména proti nechtěnému softwaru a virům. Tento software při šíření využívá vlastnosti Windows naslouchat na určitých portech provozu na síti.



Základní ochranu poskytuje i NAT. Využívá faktu, že privátní IP adresy nejsou v internetu směrovány

Tento způsob již není vhodný v případě, že potřebujeme zajistit, aby počítače z internetu komunikovaly s některými počítači v síti LAN. Případně naopak zabránit počítačům ze sítě LAN komunikovat s počítači v síti internet. V tomto případě již musíme použít firewall.

Firewall

Firewall je zařízení sloužící k oddělení dvou nebo více sítí. Oddělovanými sítěmi můžeme rozumět např. síť LAN a internet, dvě části sítě LAN s různými požadavky na zabezpečení apod. Jedná se vlastně o jakýsi kontrolní bod, na kterém jsou definována pravidla komunikace – co je povoleno a co je zakázáno. Na firewallu většinou platí pravidlo co není povoleno je zakázáno.

Firewally můžeme rozdělit dle následujících kritérií:

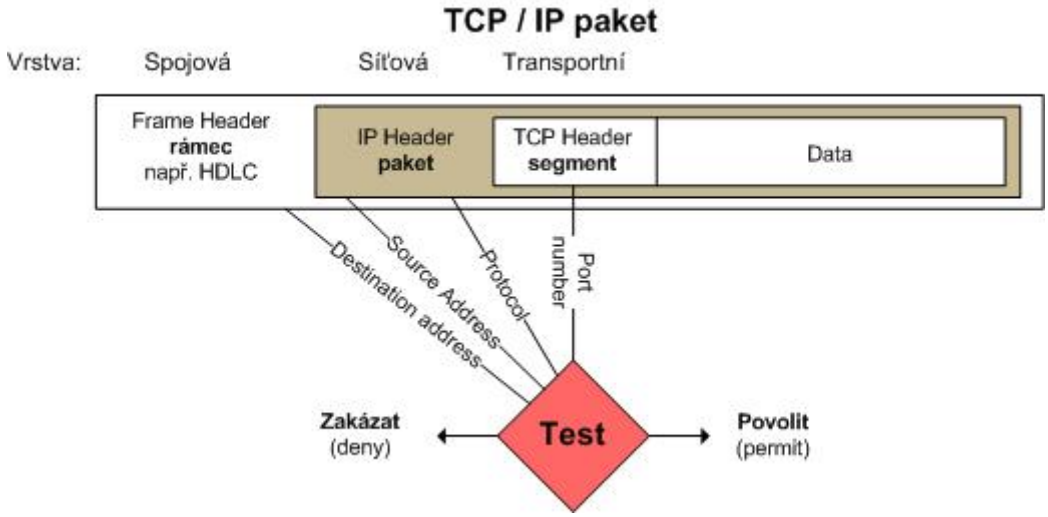
- softwarový
  - integrovaný Windows firewall, Check Point, Kerio Personal Firewall atd.
- hardwarový
  - CISCO ASA, Mikrotik

Dále podle funkce:

- Paketový filtr
- Stavový paketový filtr
- Aplikační brána

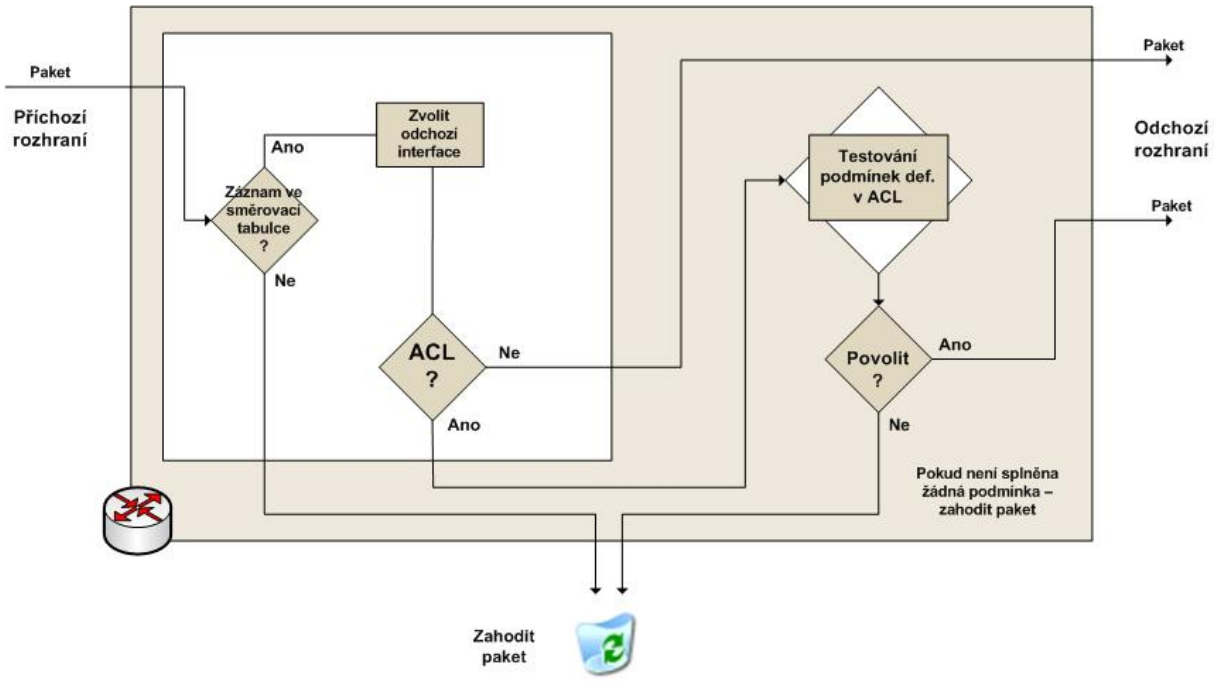
Paketový filtr

Je nejjednodušším typem firewall. Pracuje na třetí nebo čtvrté síťové vrstvě. Jeho princip spočívá v definici tzv. Access Listů. To je seznam pravidel, která přesně uvádějí, která IP adresa smí komunikovat s jinou IP adresou a na jakém portu.



Testování paketů pomocí ACL

Tato funkce je integrovaná ve většině směrovačů. Její výhodou je velká rychlost zpracování a nenáročnost na výkon hardwaru. Na stejném principu fungují i IP-Tables v Linuxu.



Postup testování paketů pomocí ACL

Stavový paketový filtr

Na rozdíl od klasických paketových filtrů si stavové firewall ukládají informace o povolených spojeních. Na základě těchto informací pak rozhodují zda-li komunikace spadá do již povoleného spojení. Tím dochází k urychlení rozhodovacího procesu a umožňuje to zahrnout do povoleného spojení i související komunikaci. Vhodné např. pro FTP řídící komunikace probíhá na portu 21 a datová komunikace na portu 20.

Aplikační brána

Aplikační brány jsou jakési Proxy firewall. Veškerá komunikace přes aplikační bránu probíhá formou dvou spojení – klient (iniciátor spojení) se připojí na aplikační bránu (proxy), ta příchozí spojení zpracuje a na základě požadavku klienta otevře nové spojení k serveru, kde klientem je aplikační brána. Data, která aplikační brána dostane od serveru pak zase v původním spojení předá klientovi. Kontrola se provádí na sedmé (aplikační) vrstvě síťového modelu OSI (proto se těmto firewallům říká aplikační brány).

Vedlejším efektem použití aplikační brány je, že server nevidí zdrojovou adresu klienta, který je původcem požadavku, ale jako zdroj požadavku je uvedena vnější adresa aplikační brány. Aplikační brány díky tomu automaticky působí jako nástroje pro překlad adres (NAT), nicméně tuto funkcionalitu má i většina paketových filtrů.

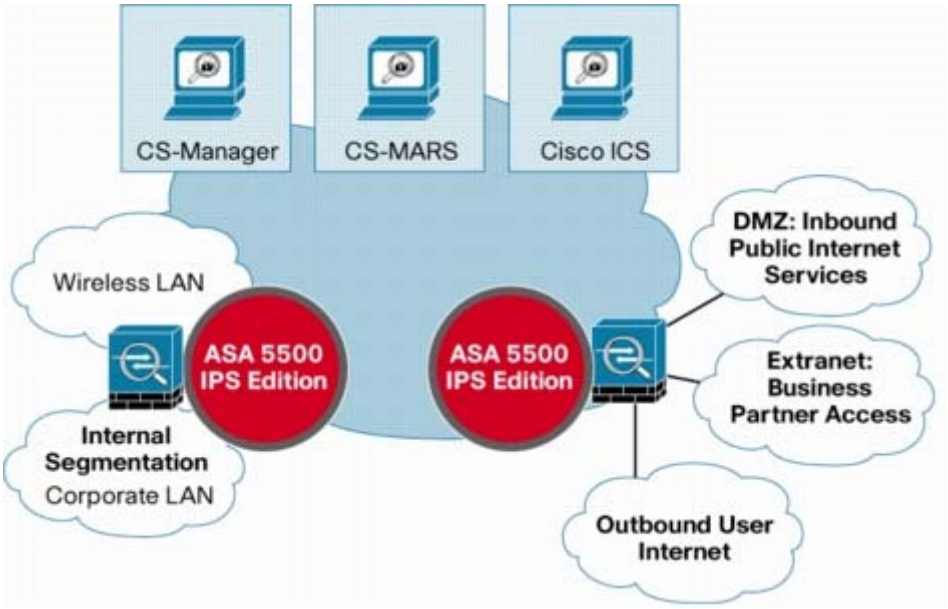
Pokročilé metody zabezpečení sítí IP

Dalším způsobem jak se chránit např. proti virům a dalšímu nechtěnému softwaru je použití některého detekčního mechanismu na vstupu do sítě LAN.

Zejména se jedná o:

- IDS – Intrusion Detection System
- IPS – Intrusion Prevention System

Obě tyto technologie fungují podobně jako antiviry. Na základě inspekce paketů jsou schopny rozeznat zda-li paket neobsahuje virus nebo jinou nepovolenou komunikaci. IPS obsahuje do jisté míry inteligentní algoritmus, který je schopen sám rozhodovat co povolit. Nevýhodou těchto systémů je určité zpomalení oproti paketovým filtrům. Další nevýhodou je samozřejmě cena zařízení a zejména cena aktualizací signatur virů atd. Logicky vyplývá, že toto zařízení bez automatických aktualizací signatur bude během velice krátké doby bezcenné. Zejména systém IDS přináší nutnou administrativní činnost – je zapotřebí definovat co povolit.
Poslední problematickou oblastí zde může být použití šifrované komunikace. Pokud tento druh komunikace prochází přes zařízení typu IPS může se stát, že část zašifrované komunikace bude odpovídat známému viru a systém ji nepustí do sítě – spojení se pak rozpadne. K tom u samozřejmě nedochází příliš často, nicméně při obrovském množství paketů, které si systémy mezi sebou vyměňují k tomu občas dojde.

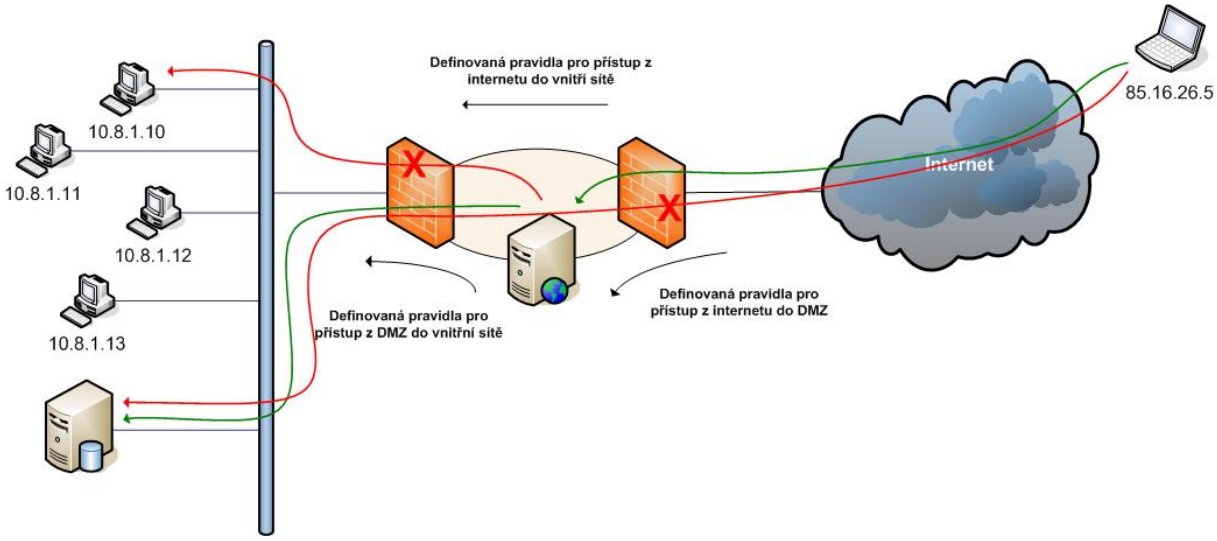


Systém IPS

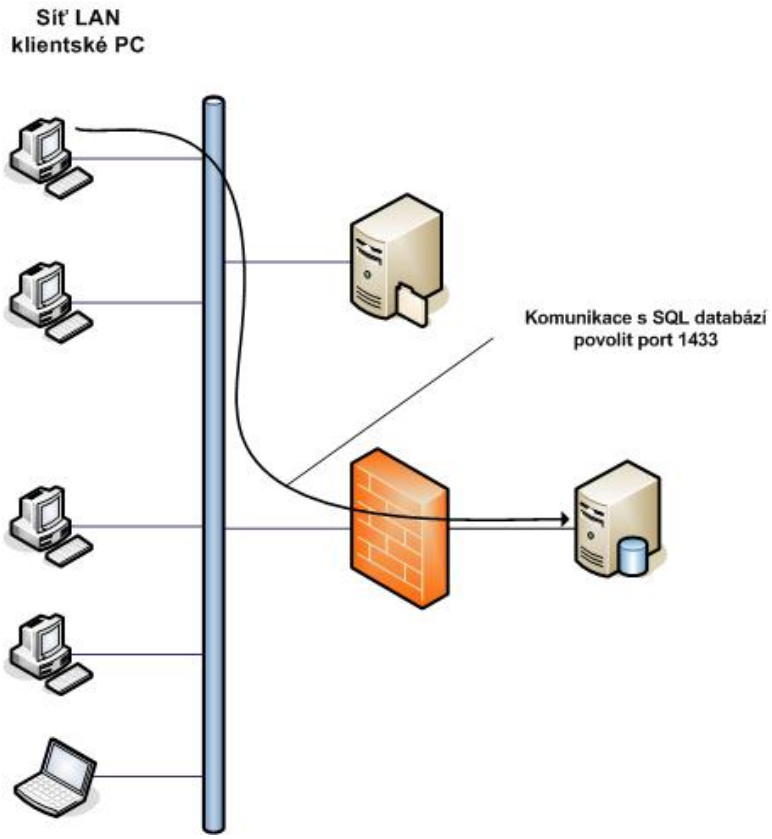
Použití firewallu

- **DMZ** – demilitarizovaná zóna

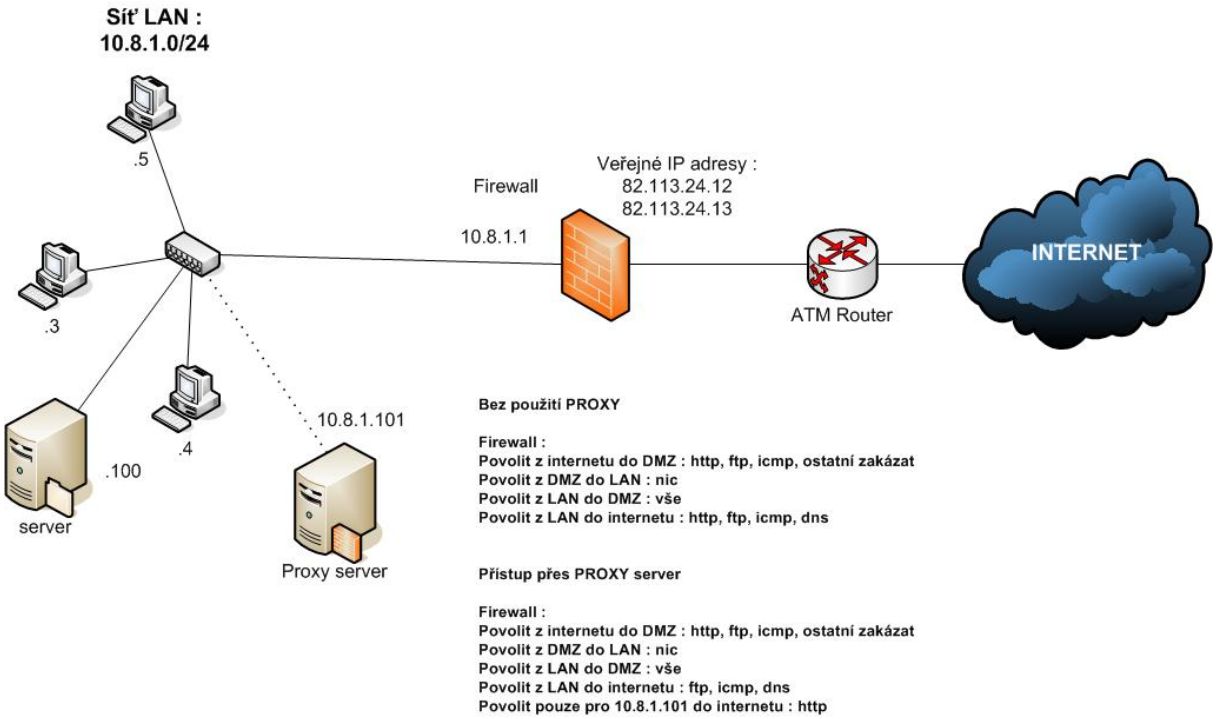
Slouží k umístění serverů, které mají být přístupné i z intranetu. Definujeme zde pravidla s kterými počítači ve vnitřní síti smí komunikovat počítače umístěné v DMZ a na jakých portech. Dále definujeme pravidla, které porty jsou otevřeny z internetu do DMZ apod.



Použití DMZ pro přístup k webovému serveru



Firewall můžeme použít i pro rozdělení vnitřní sítě na segmenty



Vynucení použití Proxy - serveru počítači v síti LAN