Bezpečnost počítačových sítí - Firewall

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

**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.

Ve velké většině případů je firewall zmiňován právě v souvislostech propojení s Internetem a ve spojitosti s rodinou protokolů TCP/IP. Nicméně, firewally nejsou nutně závislé na Internetu a musejí být schopny pracovat i s jinými protokoly. Internet je sice častý, nicméně ne jediný případ jejich využití. Klasickým příkladem mohou být například vnitropodnikové sítě, kdy jednotlivé pobočky jsou k "hlavnímu stanu" připojeny pomocí privátních kanálů. Tyto kanály (např. WAN sítě) jsou rovněž chráněny firewally, přestože v těchto větvích se nemusí nacházet jediná přípojka do Internetu.

Firewally můžeme rozdělit dle následujících kritérií:

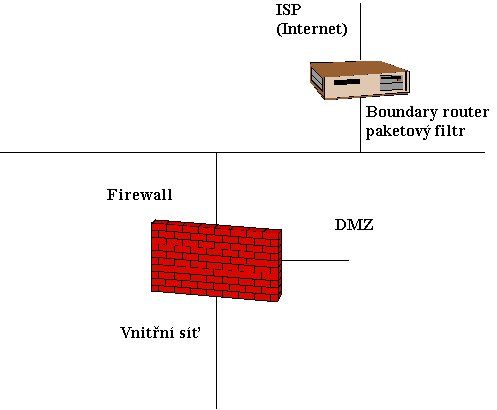
* softwarový
  + integrovaný Windows firewall, Check Point, Kerio Personal Firewall atd.
* hardwarový
  + CISCO ASA, Mikrotik

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. 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.



**Stavový paketový filtr**

Na rozdíl od klasických paketových filtrů si stavové firewall ukládají informace o povolených spojeních. Na základě těchto informací pak rozhodují, zdali 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.

**Použitá literatura:**

VYMAZAL, Michal. *Firewall - základní popis* [online]. 2003 [cit. 2013-02-02]. Dostupné z: <http://www.abclinuxu.cz/clanky/bezpecnost/linuxove-dmz-vi>

*Zabezpečení v síti IP* [online]. [cit. 2013-02-02]. Dostupné z: <http://moodle.vscht.cz/pluginfile.php/2668/mod_resource/content/0/firewall.pdf>

*Zabezpečení sítí, bezpečnostní pravidla* [online]. Trutnov, 2004 [cit. 2013-02-02]. Dostupné z: http://www.spstrutnov.cz/o-skole/projekty/podpora-informacniho-centra/zabezpeceni-siti-bezpecnostni-pravidla.pdf