Firewall – hrozby, napadení, blokové schéma FW, NAT, PAT, proxy, DMZ, tvorba pravidel pro přenosové filtry

Hrozby počítačových sítí

Sítě ohrožuje možnost ilegálních průniků či neoprávněných vstupů osob do účtů, protože rodina protokolů TCP/IP nemá nástroje pro ochranu proti zneužití, je třeba se bránit jinými způsoby.

Veškeré hrozby lze rozdělit na

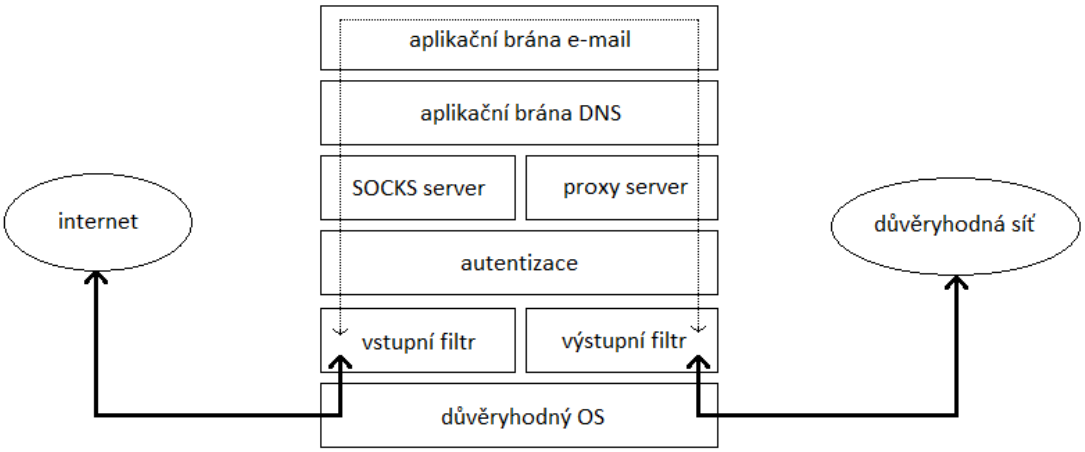
a) **vnější** – bráníme se pomocí firewallů (síťový zátaras); vnější narušitel; přírodní katastrofy; např. proti zneužití důvěrných informací
b) **vnitřní** – řeší je bezpečnostní politika – souhrn pravidel určující chování uživatelů nebo také počítačů v síti; různá pravidla pro připojení, zálohování, připojení kabelů atp.; jsou stanovena přístupová práva a hesla

Vícevrstvý systém ochrany – používáme firewall, bezpečnostní politiku a antivirové programy.

Firewally obecně

Firewall poskytuje ochranu vnitřní sítě před nebezpečím z vnějších sítí. Logicky a fyzicky odděluje bezpečnou a důvěryhodnou síť od nezabezpečené a nedůvěryhodné. Může být řešen hardwarově i softwarově. Pracuje na síťové, transportní a aplikační vrstvě. Soustřeďuje prostředky zabezpečení do jednoho uzlu sítě a povoluje speciálně definovat výjimky v přístupu. Může provádět směrování.

Umisťuje se na hranice sítí – je důležité oddělení vnitřních a vnějších služeb. Firewall blokuje nežádoucí komunikaci jak do sítě, tak i z ní. V chráněné části se nesmí používat modemy ani jiná pevná připojení do internetu.



Funkce firewallů

Hlavní funkcí každého firewallu je **ochrana sítě a monitorování provozu** a dále pak zajištění internetových služeb, zejména zabezpečené e-mailové komunikace – nikdo nesmí odesílat neoprávněně e-maily.

Kromě toho mohou firewally poskytovat další (vedlejší) funkce – regulaci přístupu uživatelů k internetu, funkce NAT, umožňování vzdáleného přístupu či VPN.

Typy firewallů

Paketový filtr

Filtruje pakety na úrovni síťové a transportní vrstvy. Většinou je implementován přímo na routeru, může však být také na serverech nebo na koncových stanicích. Nebezpečím jsou fragmenty – každý fragment obsahuje pouze IP adresy a pokud se nesestaví celá zpráva, nelze provádět kontrolu portů a TCP a UDP hlaviček. Řídí se **sadou pravidel**.

Mají vysokou rychlost, ale poskytují nízké zabezpečení. Obvykle bývá kontrola prováděna na přechodu z 2. do 3. vrstvy. Zkoumá, co obsahují hlavičky paketů – IP adresu odesílatele a příjemce – na základě toho se rozhoduje, zda bude paket propuštěn nebo ne.

Může zakázat tok od určitého vnějšího uzlu nebo tok k určitému vnitřnímu uzlu. Je možné třídit podle čísel portů a je možné tak zakázat určitému uzlu určitou službu přijímat, využívat atp.

Filtry se rozlišují vstupní, výstupní a přenosový. Filtrovat lze podle spousty faktorů – IP adresa rozhraní, typ protokolu, příznaky v TCP segmentu (ACK, SYN, …), množina zdrojových/cílových adres, číslo portu, směrování k jedné stanici, fragmentace, …

Existují všeobecná pravidla, kde se deaktivuje vše kromě povolených věcí, taková pravidla mohou znamenat např. „deaktivovat všechny služby kromě výslovně povolených“, „blokovat směrem ven všechny aktualizace protokolů týkající se vnitřní sítě“ nebo např. „deaktivovat fragmentaci“.

Aplikační brána

Pracuje na aplikační vrstvě. Nekontroluje transportní vrstvu, zabývá se pouze obsahem paketu. Zadrží všechny pakety a u povolených spojení navazuje spojení znovu. Její činnost je bezpečnější, neboť se přístup uskutečňuje na základě autentizace. Její součástí je proxy, NAT a PAT.

Kombinace paketového filtru a aplikační brány

Je dalším typem nastavení činnosti firewallu jakožto celku – jde o zabezpečení sítě řešené právě kombinací jak paketového filtru, tak aplikační brány a jejích součástí.

Proxy

Proxy je ve své podstatě *zástupná služba* pro každou povolenou službu. Provoz proxy zajišťuje proxy server. Účastníka připojí k vzdálenému serveru a dále vystupuje pod jménem účastníka (obdobným způsobem funguje NAT, proxy server je však dokonalejší). Každý aplikační proxy server je vždy určen pro určitý protokol.

Klientům tak umožňuje nepřímé spojení k jinému serveru – proxy server mezi tímto klientem a serverem funguje pak jako prostředník. Důležité je, že proxy server přebírá celou komunikaci – vytváří kompletně nové spojení. Přijatou odpověď předává pak zpět klientovi. Proxy může být zajištěno i jen softwarově.

Nevýhodou je, že jde o jediný ústřední bod, přes který musí vše projít. Jestliže tento bod selže (spadne), spadne celý systém. Z toho pak plyne doporučení, že by proxy server neměl být součástí routeru.

Průběh komunikace přes proxy server

1. klient vyšle požadavek
2. proxy ho celý zkontroluje, přijme ho jako koncový adresát a vytvoří novou komunikaci mezi sebou a skutečným adresátem
3. zprávu může zodpovědět sám (pokud zná řešení) nebo může požadavek zamítnout (např. pokud komunikace není povolená – daná stanice nesmí komunikovat s internetem atp., stanici informace o zamítnutí přijde), pokud komunikace zamítnuta nebyla, komunikace pokračuje
4. po získání odpovědi od skutečného adresáta je obsah odpovědi zkontrolován (část může být vyfiltrována podle nastavených pravidel)
5. odpověď je předána klientovi

NAT – Network Address Translation

Nižší forma proxy – pouze překládá adresy. Mapuje IP adresy na adresy jiné sítě. Pracuje na síťové vrstvě. Může být použit pro propojení sítí, které mají např. neslučitelný adresový prostor. Znemožňuje end-to-end spojení a může snížit rychlost přenosu. Zařízení vystupují pod různými adresami.

Lze jej dělit na dynamický a statický:

a) **dynamický NAT** – tabulka se sestavuje podle potřeby (položky se však mohou vytvářet jen podle provozu zevnitř ven); vytvořené položky jsou dočasné; možnost zpřístupnění nějaké vnější sítě mnoha stanicím přes několik globálních adres
b) **statický NAT** – překladová tabulka je spravována manuálně; každý počítač ve vnitřní síti má stejnou adresu ve vnější síti; počítače nemají plnohodnotné připojení; nefungují některé protokoly jako např. FTP

NAT zvyšuje bezpečnost, protože potenciální útočník nezná opravdovou IP adresu. NAT však nelze srovnávat s firewallem – *schovávání počítače za sebou samotným* je pouze vedlejším efektem primární funkce (překladu IP adres).

PAT – Port Address Translation

Je podmnožinou NAT – umožňuje používat jednu veřejnou IP adresu pro mnoho různých počítačů v LAN. Pracuje na síťové a transportní vrstvě – rozlišuje TCP a UDP komunikaci. Vytváří v sobě tabulku adres podle čísel portů.

Dochází k překladu jak adres, tak i příslušných portů v IP komunikaci. Výhodou je, že za jednou veřejnou IP lze maskovat celá řada služeb, které jsou hostovány na různých serverech. Typickým příkladem jsou FTP a webové servery umístěné v demilitarizované zóně.

PAT zařízení viditelně modifikuje pakety v okamžiku, kdy projdou skrz. Tato modifikace vytváří dojem, že všechny pakety, které jsou odesílány do veřejné sítě od mnoha místních počítačů ve vnitřní síti, pocházejí od jediného počítače – ten je představován právě jednotkou PAT.

Překlad koncového bodu

Když počítač z LAN posílá paket do internetu, PAT zařízení nahrazuje vnitřní IP adresu ve zdrojovém poli hlavičky paketu (zpáteční adresa) s externí IP adresou PAT zařízení (odpověď z internetu tedy přijde na PAT zařízení) a dále přiřadí spojovací číslo portu z množství dostupných portů a toto číslo portu přiloží ke zdrojovému poli portů. Poté je paket odeslán do vnější sítě.

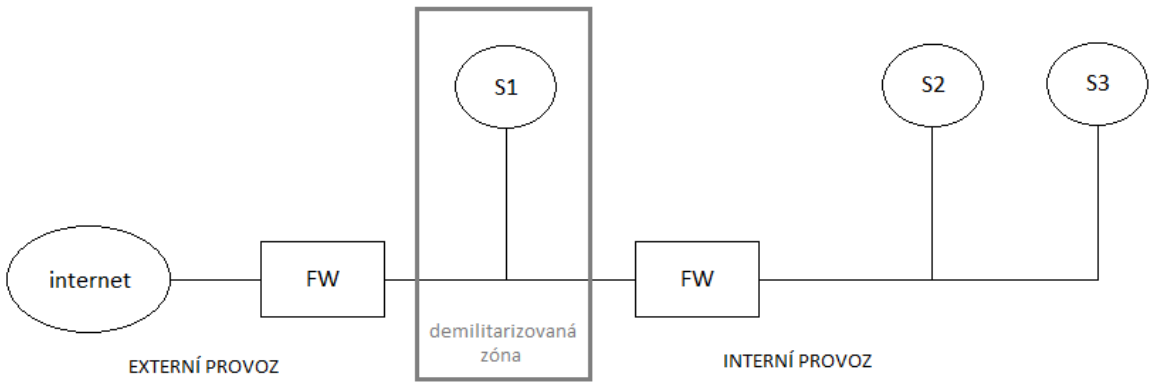
V momentě, kdy přijde odpověď, je podle původně vybraného čísla portu odeslána na příslušný počítač z vnitřní sítě.

Demilitarizovaná zóna (DMZ)

Oblast oddělující internet a vlastní LAN. Zabraňuje průchodu paketů tak, že pakety musejí být adresovány do zóny, která pak zprostředkovává jejich další přenos. Od vstupních částí je oddělena směrovači (pro každý vstup musí být jiný směrovač).

Pro služby, které vyžadují přímý průchod, museí být jednotlivé pakety předem kontrolovány – tuto činnost řeší paketový filtr a aplikační brána SOCKS[1].

Umisťuje se do ní např. web server, e-mail server, koncový bod VPN, aplikační servery či například FTP servery nebo proxy server – tedy veškeré brány, které provoz předávají dále.



Tvorba pravidel pro filtraci

Deaktivují se všechny protokoly a adresy, kromě výslovně povolených služeb; deaktivují se všechny pokusy o připojení k hostiteli sítě; blokují se (směrem ven) všechny aktualizace RIP a OSPF týkající se vnitřní sítě; servery s veřejnými službami jsou zařazeny před paketové filtry.

[1] **SOCKS** (Socket Secure) – protokol umožňující výměnu paketů mezi klientem a serverem přes proxy server; pracuje na relační vrstvě modelu ISO-OSI; SOCKS server přijímá připojení klientů na TCP/1080 portu