

Firewall

Daniel Studený

CESNET z. s. p. o.

daniel.studený@cesnet.cz

Firewall - co to vlastně je?

- Zařízení, které na základě předem definovaných pravidel řídí síťovou komunikaci nějaké sítě se „zbytkem světa“, čímž zvyšuje úroveň bezpečnosti této sítě
- Též se tak přeneseně říká službě operačního systému, která chrání server či stanici tím, že filtruje jejich síťovou komunikaci a neumožňuje aplikacím nestandardní či neschválené chování vůči systémovým prostředkům

Implementace firewallu

- Implementace firewallu
 - server s vhodnou konfigurací vhodného operačního systému – firewall jako služba
 - výhoda: flexibilita, programovatelnost, možnost návaznosti na další služby
 - nevýhoda: zpravidla nižší výkon
 - tzv. hardwarový firewall – síťový prvek sloužící jedinému účelu – firewallingu
 - Výhoda: značná rychlost; má pro svou činnost stavěný hardware, zejména síťová rozhraní
 - Nevýhoda: malá flexibilita, omezené možnosti, závislost na firmware

Činnost firewallů

- Firewall postupně zjišťuje, zda parametry přijatých síťových dat vyhovují pravidlům definovaným správcem sítě (firewallu)
- S daty, která podmínkám daného pravidla vyhovují, provede akci udanou tímto pravidlem (předání, zahození, modifikace, apod.)
- Parametry zahozených (ale někdy i předaných dat) zaprotokoluje za účelem pozdějšího vystopování případného útoku, resp. získání přehledu o přístupech do sítě

Kategorie firewallů

- Jednoduché paketové filtry
 - Pracují na síťové úrovni komunikační abstrakce a mají pravidla utvořená především na základě příchozí a odchozí adresy a typu služby, pro kterou jsou pakety určeny; řízení provozu neovlivňuje obsah předávaných dat
- Stavové firewallly
 - Umožňují přenos síťové komunikace i komplexnějšími protokoly využívajícími několika současně navázaných spojení různého významu

Kategorie firewallů

- Firewally s kontrolou protokolu
 - Rozpoznají zneužití komunikačního protokolu pro jiný než původní účel
 - Provádí základní kontrolu syntaxe dat daného protokolu
- Firewally aplikační (aplikační brány)
 - Sledují i obsah konkrétního komunikačního protokolu; data nepředávají přímo, ale hrají roli prostředníka a znovu je sestavují tak, aby pro chráněnou síť byla bezpečná

Firewallová pravidla

- Statická pravidla
 - Chovají se ke stejnému typu komunikace vždy stejně
- Stavová pravidla
 - Rozhodují na základě některých informací získaných z předchozí komunikace mezi stejnou vnější i chráněnou stanicí
 - urychlují průchod dříve již „schválené“ komunikaci
 - znesnadňují opakované pokusy o útok a průnik do systému chráněné stanice
 - umožňují průchod komunikaci související s jiným, již otevřeným spojením

Firewallová pravidla

- Občasná pravidla
 - Pravidla, která jsou sice v systému firewallu zanesena, ale nejsou aktivní
 - Jejich provozní nasazení je zajištěno:
 - a) ručně, správcem sítě, na základě např. požadavku na zvýšení úrovně zabezpečení, na dočasnou podporu nějakého síťového protokolu či odhalení síťového útoku
 - b) nějakou vnější událostí (např. odhalením útoku serverem IDS)

Obvyklé politiky firewallů

- Statická pravidla
 - zákaz přístupu ke službám, které nejsou chráněnou sítí poskytované
 - zákaz přístupu ke službám, které sice jsou chráněnou sítí poskytované, ale nejsou veřejné
 - omezení přístupu ke službám určeným pouze konkrétním uživatelům (např. vzdálený terminál)
 - zamezení průchodu závadné síťové komunikace do chráněné sítě (vadné pakety, útoky)

Obvyklé politiky firewallů

- Stavová pravidla
 - Zákaz přístupu k dané službě ze stanic, které se v nedávné době pokoušely o větší než malé množství spojení (např. tzv. „probe“ útok)
 - Umožnění přístupu ke službě, která je poskytována jen v případě, že stanice již využívá jinou, nadřizenou službu; též umožnění přístupu ke službě klientům, kteří již byli autorizováni nebo registrováni (např. datové FTP spojení, příchozí VoIP volání, apod.)

Modelový příklad

- Povolit:
 - Komunikaci, která souvisí s již navázanými povolenými spojeními
 - Síťové služby dostupnosti serverů
 - Přístup k veřejným službám (WWW, DNS, mail)
 - Omezený přístup k neveřejným službám (VPN, synchronizace času, vzdálený přístup)

Modelový příklad

- Zakázat
 - Pokusy o útoky (viz. dále)
 - pakety, které jsou zjevně podvržené
 - pakety přicházející s velkou četností
 - vadné pakety
 - pakety s všeobecnou cílovou adresou
 - Zjišťování dostupnosti pracovních stanic
 - Přístup ke službám, které nejsou veřejné
 - Přístup k důvěrným službám bez předchozí autorizace

„obrácený firewall“

- Firewally většinou chrání lokální síť před neoprávněnými přístupy zvenčí
- Někdy je ale zapotřebí naopak ochránit Internet před uživateli lokální sítě (typicky ve vzdělávacích organizacích, v internetových kavárnách, veřejných knihovnách, apod.)
- V takovém případě povolíme našim uživatelům využívat jen část služeb Internetu, v extrémním případě např. jen DNS a WWW

Výhody nasazení firewallu

- Více možností zabezpečení, než jaké mohou nabídnout lokální paketové filtry
- Možnost zabezpečení zařízení, která sama o sobě zabezpečit nelze
- Ochrana před síťovými útoky
- Centralizace:
 - rychlé uzavření konkrétního datového toku do celé sítě
 - možnost rychlého zabezpečení nového bezpečnostního problému v jediném bodě

Nevýhody nasazení firewallu

- Cenzura, monitorování komunikace
- Zpoždování přenosu, zejména u vysokorychlostních linek
- Neustálý spor správců sítě a jejích uživatelů o tom, co má být povoleno
- Omezení uživatelů ohledně možností využívání služeb Internetu
- Falešné bezpečí – uživatelé mají pocit, že se jim za FW nemůže nic stát a nedbají osobních bezpečnostních zásad
- Každá chyba v konfiguraci firewallu může ovlivnit celou síť

Síťové útoky a obrana proti nim

- Síťové útoky mohou být namířeny proti konkrétním počítačům či celé síti, nebo nemusí mít vůbec žádný konkrétní cíl
- Mohou být pouhou zlomyslností či úmyslným napadením, např. z pomsty
- Jednou z možností, jak proti nim bojovat, je právě zabezpečení lokální sítě pomocí firewallu

Některé typy síťových útoků

- SYN flooding
 - Útočící stroj se snaží na cílovém počítači otevřít co nejvíce spojení, otevření však pouze zahájí, ale nedokončí ho
 - Stavové informace o otevřených spojeních tím pádem brzy vyčerpají systémové prostředky napadeného počítače
 - Stavový firewall může útok odhalit a nepustit do lokální sítě větší než mezní počet požadavků na spojení za časovou jednotku

Některé typy síťových útoků

- Smurfing
 - Využívá službu zjištění dostupnosti počítače, a to s všeobecnou cílovou adresou
 - Některé OS odpovědí nejen útočníkovi, ale též na všeobecnou adresu, tím hrají úlohu „zesilovače“ útoku
 - S podvrženou zdrojovou adresou tak lze přetížit server, kterému byla „ukradena“
 - Pokud je naše síť prostředníkem útoku, stačí zakázat průchod paketů s všeobecnou cílovou adresou; jsme-li obětí, preventivně nelze udělat nic

Některé typy síťových útoků

- DDoS - distribuované zneprovoznění služby
 - Útočník pronikne pomocí červa do většího množství stanic v Internetu
 - Poté začne posílat ze všech těchto stanic velké množství paketů do daného cíle, čímž může zcela ochromit velkou část Internetu
 - Obrana spočívá v nastavení limitů počtu příchozích paketů za časovou jednotku; nadlimitní pakety se zahodí

Některé typy síťových útoků

- Address spoofing – podvržení adresy
 - Používá se spolu s dalšími metodami napadení
 - Zdrojová adresa paketu je zfalšována, útočník
 - není snadno vystopovatelný
 - může získat neautorizovaný přístup k síťovým prostředkům
 - může získat falešnou důvěru uživatele a jeho aplikací
 - částečnou obranou je odfiltrování paketů, které přijdou z jiných rozhraní, než z jakých by měly přijít podle směrovací tabulky, a filtrování paketů které přišly z Internetu se zdrojovou adresou z vyhrazených rozsahů (např. pro NAT)

Některé typy síťových útoků

- DNS cache poisoning
 - Podvržení falešného záznamu nameserveru, který pro danou síť dělá DNS cache
 - Klienti tak navštíví službu falešného serveru, který jim poskytne zkreslené informace, nebo za pomoci dokonalé kopie nějakého portálu (např. Internetového bankovníctví) umožní útočníkovi získat přístupové a jiné důvěrné údaje (tzv. pharming)
 - Obranou proti tomuto útoku je kromě nasazení nejnovějších verzí DNS nameserveru též ochrana lokální sítě NATem či aplikační bránou

Logování firewallu

- Logování firewallu je velmi důležité
 - pro udržení přehledu o přístupu ke službám sítě
 - pro odhalení síťových útoků správcem sítě či IDS
 - pro případné vystopování zdroje útoku pro účely incident handlingu
 - pro detekci špatné konfigurace firewallu (nefunkční aplikace, bezpečnostní díra, apod.)

Logování firewallu

- Do logů se zapisuje
 - zahození paketu nevyhovujícím žádnému pravidlu
 - přijetí paketu na základě povolení některým pravidlem

Logování firewallu

- I logovat se musí s rozumem!
- Typickým příkladem chybné konfigurace firewallu je případ, kdy firewall sice ochrání síť před např. DDoS útokem, ale během něj nedělá nic jiného, než že loguje a tím snižuje svou propustnost, v extrémním případě až na nulu
- Takové logy jsou navíc bezcenné, protože v nich nelze nic nalézt, leckdy jsou i neúplné, protože během útoku dojde disková kapacita firewallu

Logování firewallu

- Co tedy nelogovat?
 - Zejména násobné záznamy, stačí prvních několik událostí za rozumný časový interval
 - Zahození nezajímavých paketů (např. těch, které nejsou útokem, ale komunikací užitečnou pro jiné počítače v síti – DHCP žádosti, pakety s všeobecnou adresou od lokálních stanic, apod.)

???

Dotazy, připomínky?

KONEC

Děkuji Vám za pozornost.