Firewally – pokračování, filtrace paketů

Pozor, útok! (9. díl)

V minulém dílu jsme zahájili povídání o firewallech, přinesli jsme vám informace o možnostech jejich využití, o "stavebních kamenech", ze kterých bývají zpravidla budovány, a přiblížili jsme si čtyři základní konfigurace architektur firewallů.
V dnešním, již devátém pokračování seriálu o bezpečnosti si popíšeme, na jakých principech pracuje filtrování paketů, podíváme se, kde je možné získat potřebné informace pro tuto činnost, a co můžeme od filtrování z hlediska bezpečnosti vlastně očekávat.

Úvod

Základním bezpečnostním mechanismem používaným k ochraně privátních sítí připojených k "síti sítí" je tzv. filtrace paketů (packet-filtering). Tento mechanismus určuje na základě námi předem definovaných pravidel pro filtraci paketů (packet-filtering rules), které pakety mohou procházet skrz filtrující směrovač (router) do vnitřní chráněné sítě a které naopak mohou opustit tuto privátní chráněnou síť směrem ven.

Každého čtenáře, který se v této problematice začíná teprve orientovat, pravděpodobně napadne otázka, zda jsou těmito pravidly vybaveny všechny směrovače na internetu . Odpověď je – ne! Efektivní nastavení pravidel filtrace paketů pro tyto směrovače by totiž bylo velmi problematické, ba skoro nemožné a funkce filtrace by zpomalovala tok procházejících paketů. A proto hlavní funkcí těchto směrovačů je "pouze" předávání přijatých paketů k dalšímu směrovači postupně až ke stanovenému cíli.

Těmito zařízeními – směrovači – může být samostatný hardware nebo software, který běží např. na PC nebo unixovém systému a pro komunikaci s dalšími směrovači využívá směrovacích protokolů. Jako příklad si uveďme OSPF (Open Shortest Path First) či RIP (Routing Information Protocol).

Pozn.: K odlišení těchto dvou variant směrovačů se mluví buď o "normálním" směrovači, který se pouze stará o to, jak předat paket dále podle informací obsažených v tomto paketu a ve směrovací tabulce, nebo o filtrujícím (někdy se používá i termín ochranném) směrovači, který podle námi stanovené bezpečnostní politiky a definovaných pravidel rozhoduje, co s daným paketem provede, tj. zda obdržený paket neodporuje daným pravidlům a je možné ho zaslat dále, nebo zda je porušuje a zaslání k cíli skrz tento filtrující směrovač neproběhne.

Jak se filtruje?

A jakému přenosu dat můžeme zabránit pomocí mechanismu filtrace paketů? Můžeme zabránit určitému přenosu podle: 1) adresy, ze které data pocházejí, 2) podle adresy, na kterou směřují, a 3) podle relací, protokolů a aplikací použitých při přenosu těchto dat. Většina systémů pro filtraci paketů ovšem neprovádí žádné akce související s vlastním obsahem dat (samozřejmě existují výjimky), ale naštěstí si můžeme například stanovit pravidlo, na jehož základě budeme přijímat poštu pouze prostřednictvím aplikačního protokolu SMTP.

K tomu, abychom dále porozuměli filtraci paketů a možnostem, co vlastně lze vykonávat, je nutné nejprve pochopit, jak funguje TCP/IP zásobník. Jak jste se mohli dozvědět z informací obsažených již v prvním díle tohoto seriálu (Chip 11/99, str. 128, obr. 2), tento zásobník se skládá ze čtyř vrstev:

z aplikační vrstvy (FTP, Telnet, …), jež je tvořena aplikacemi a procesy využívajícími síť,

z transportní vrstvy (TCP, UDP, ICMP), která poskytuje službu zvanou end to end doručování dat,

z internetové vrstvy (IP), ve které je definován datagram a která obsluhuje směrovaná data,

z vrstvy síťového rozhraní (např. Ethernet, FDDI, ATM), která je tvořena rutinami pro přístup k fyzické síti.

Tyto jednotlivé vrstvy si předávají daný paket mezi sebou tak, že níže položená vrstva připojí k danému paketu svoje vlastní záhlaví a celý zbytek považuje za data – tento proces se nazývá zapouzdření (encapsulation).

Pro lepší pochopení tohoto (pro filtrování důležitého) procesu zjednodušeně popíšeme postup, kterým toto zapouzdření probíhá. V aplikační vrstvě je paket tvořen pouze z dat (například z fragmentu nějakého posílaného souboru), v transportní vrstvě pak například protokol TCP připojí k těmto datům své vlastní záhlaví. V internetové vrstvě pak IP protokol považuje celý příchozí paket za data a opět k němu připojí své IP záhlaví a tak dále.

Pozn.: Na straně příjemce tohoto paketu dochází k opačnému postupu, tj. každá vrstva odstraní (zpracuje) své záhlaví předtím, než paket předá výše položené vrstvě. Chceme-li tedy filtrování paketů pochopit a efektivně využívat, je nutné si uvědomit, že nejdůležitější informace jsou obsaženy právě v záhlavích jednotlivých vrstev!

Co se filtruje?

Pro lepší pochopení, co se filtruje a hlavně podle čeho, si uvedeme ilustrativní příklad TCP/IP paketu přenášeného po Ethernetu.

V nejnižší ethernetové vrstvě, jak již víme, je paket složen z ethernetového záhlaví a těla. Předem chci upozornit na skutečnost, že podle informací obsažených v ethernetovém záhlaví nejsme obvykle schopni uskutečnit filtraci. Nejdůležitějšími informacemi, které jsme schopni z tohoto záhlaví získat, jsou informace o druhu paketu, o ethernetové adrese počítače, který vložil paket do daného segmentu, a o cílové ethernetové adrese v daném síťovém segmentu.

Ve výše položené IP vrstvě již můžeme získat velmi cenné informace z IP záhlaví (viz obr. 1). Filtrovat můžeme buď podle čtyřbajtových adres IP zdroje (např. 147.228.42.75) a cíle, nebo podle typu IP protokolu, či podle pole IP možností.

V TCP vrstvě (viz obr. 2) pak dále můžeme z TCP záhlaví získat následující informace vhodné pro stanovení filtrovacích pravidel: dvoubajtové číslo TCP zdrojového a cílového portu a TCP příznakové pole, které obsahuje jeden pro filtraci důležitý ACK bit (tímto bitem je identifikováno, zda daný paket zahajuje TCP spojení).

Vyjmenováním a popsáním informacích vhodných pro filtrování obsažených v jednotlivých vrstvách se dostáváme k možnému seskupení těchto informací do větších celků, rozdělujících filtrování na filtrování podle adres, filtrování podle služeb a filtrování podle čísel portů.

Shrnutí

A o co bychom se měli zajímat či usilovat při návrhu filtrovacích pravidel? Měli bychom vycházet z postoje tzv. implicitního odmítnutí. Tento postoj je mnohem bezpečnější a efektivnější na rozdíl od implicitního povolení, ve kterém se implicitně povoluje vše a zakazují se pouze problematické věci (záporem takovéhoto postoje je logicky skutečnost, že pravděpodobně nikdo nebude nikdy vědět vše o možných problémech a nových nástrahách).

Čtenáři, kteří by chtěli vyzkoušet filtrování paketů hned po dočtení tohoto článku, mají na výběr ze tří možností: první variantou je nákup komerčního řešení, druhou je stažení volně šiřitelného softwaru (viz infotipy). Třetí řešení je určeno dovednějším čtenářům, kteří disponují potřebnými zkušenostmi a znalostmi, a mohou si tedy filtrování paketů sami naprogramovat.

Příště

V příštím díle dokončíme naše poznávání firewallových systémů bližším seznámením s tzv. proxy systémy.

[Milan Pinte I pinte@atlas.cz]