



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A

KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

FILTROVANIE SIEŤOVEJ PREVÁDZKY

NETWORK TRAFFIC FILTERING

SAMOSTATNÝ PROJEKT

INDIVIDUAL PROJECT

AUTORI PRÁCE

AUTHORS

BRNO 2019

Bc. JOZEF URBANOVSKÝ
Bc. ADRIÁN TOMAŠOV

Obsah

1	Úvod	2
2	Analýza	3
2.1	Firewall a filtrovanie	3
2.2	Implementácia v Linuxovom jadre	3
2.2.1	netfilter	3
2.2.2	iptables	4
2.2.3	nftables	4
2.2.4	bpfilter	4
3	Záver	5
	Literatúra	6

Kapitola 1

Úvod

Táto práca je dokumentáciou k samostatnému projektu z predmetu *Aplikovaná kryptografia*. Samostatný projekt sa zaoberá filtrovaním sieťovej prevádzky v systéme GNU/Linux. Cieľom tohto projektu je programovo realizovať aplikáciu, ktorá má na starosť filtrovať zašifrovanú sieťovú prevádzku. Aplikácia má vytvárať štatistiky o type a množstve šifrovaných dát v sieti a ponúknuť možnosť si ich zobrazit v grafickej forme.

Kapitola 2

Analýza

V tejto kapitole je analyzovaná problematika a spôsob riešenia, ktorý je použitý pri tvorbe tejto programovej aplikácie. Dokumentácia predpokladá, že čitateľ pozná koncepty TCP/IP sieťového modelu a Linuxového jadra.

2.1 Firewall a filtrovanie

Firewall možno označiť ako ľubovoľné sieťové zariadenie, alebo sieťovú aplikáciu, ktorá slúži k riadeniu sieťovej prevádzky medzi logicky oddelenými sieťami. Podstata firewallu je v predefinovaných pravidlách pre jednotlivé pakety a toky na základe informácii z rôznych vrstiev ISO/OSI modelu. Firewally je možné rozdeliť do nasledujúcich kategórii na základe vývoja počítačových sietí.

- Paketový filter
- Aplikačný filter
- Stavový paketový filter
- Stavový paketový filter s kontrolou protokolov ľubovoľných vrstiev ISO/OSI modelu

2.2 Implementácia v Linuxovom jadre

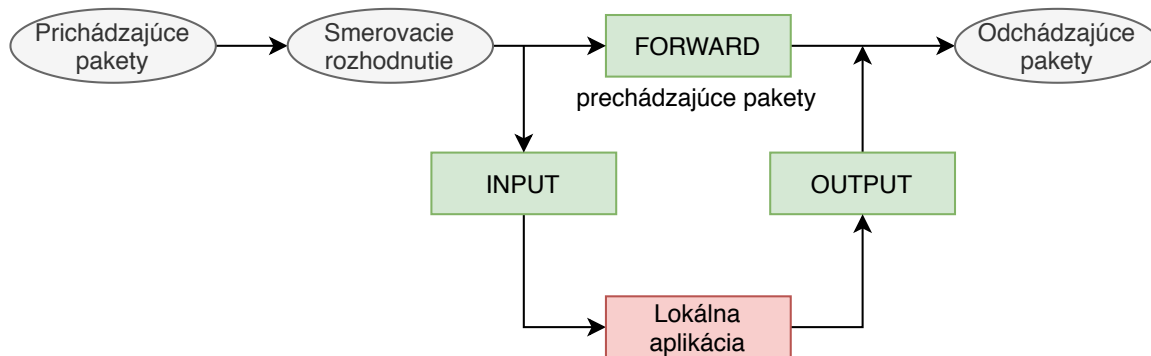
Moderné Linuxové jadro ponúka granulárnu kontrolu rôznych implementácii firewallu pre filtrovanie sieťových paketov. Práca rozoberá staršiu implementáciu filtrovania pomocou *iptables*, nástupcu vo forme *nftables* a aj firewall nasledujúcej generácie známy ako *bpfilter*.

2.2.1 netfilter

netfilter je možné reprezentovať ako framework Linuxového jadra, slúžiacia pre filtrovanie paketov, preklad sieťových adries alebo preklad sieťových portov. Jeho hlavnú úlohu v jadre plnia hooky, ktoré dovoľujú meniť správanie jadra ostatným modulom. Každý paket prechádzajúci kernelom prejde cez sadu hookov, ktoré môže zaregistrovať predurčený modul jadra cez callback a následne zareagovať spustením obslužnej procedúry. Netfilter hooking systém obsahuje moduly jadra ako napríklad *ip_tables*, *ip6_tables*, *arp_tables* a *ebtables*, ktoré možno reprezentovať ako tabuľky pre definíciu pravidiel firewallu.

2.2.2 iptables

Modul jadra `ip_tables` spolu s userspace programom `iptables` slúži na manipuláciu s tabuľkami *Xtables*, ktoré umožňujú združovať sady pravidiel do reťazcov. Reťazce následne definujú jednotlivé pravidlá pre pakety a sú spracovávané sekvenčne. Pravidlá umožňujú ovplyvňovať priebeh sieťovým zásobníkom, kde každý paket musí prejsť aspoň jednou tabuľkou. [1]



Obr. 2.1: Základné reťazce *iptables* obsiahnuté v *netfilteri*

Hlavným problémom *iptables* a dôvodom zlej reputácie, je primárne vysoká duplicita kódu, nakoľko existuje samostatná tabuľka pre každý sieťový protokol, problémy so škálovaním, rýchlosť spracovania a mnohé iné

2.2.3 nftables

Náhrada *iptables* vo forme *nftables* je podsystém v Linuxovom jadre, ktorý mení a nahrádza určité časti samotného *netfilteru*.

2.2.4 bpfILTER

Kapitola 3

Záver

TODO

Literatúra

- [1] Dočekal, M.: Správa linuxového serveru: Linuxový firewall, základy iptables. [Online; navštívené 11.3.2020].
URL <https://www.linuxexpres.cz/praxe/sprava-linuxoveho-serveru-linuxovy-firewall-zaklady-iptables>