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 — **Bc. JOZEF URBANOVSKÝ**, **Bc. ADRIÁN TOMAŠOV**

AUTHORS

BRNO 2019

Obsah

Kapitola 1

Úvod

Táto práca je dokumentáciou k samostatnému projektu z predmetu *Aplikovaná kryptografie*. 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 zobraziť 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

[4]

2.2 Implementácia v Linuxovom jadre

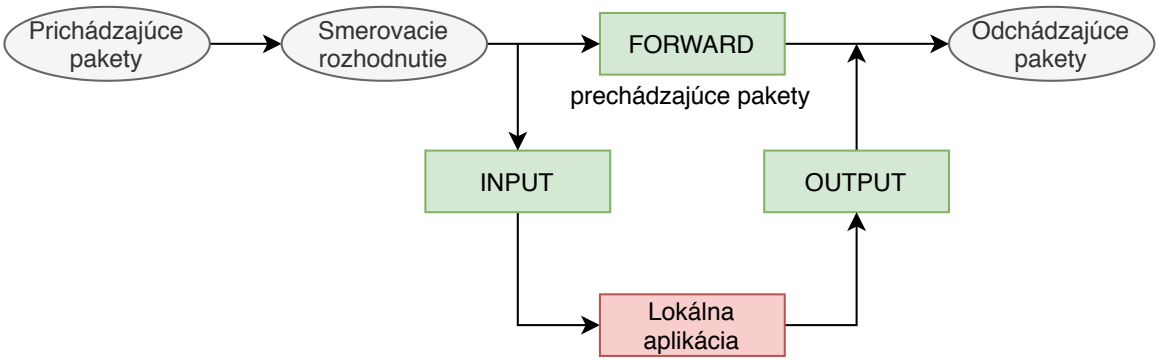
Moderné Linuxové jadro ponúka granulárnu kontrolu rôznych implementácii firewallu pre filtrovanie sieťových paketov. Práca rozoberá staršiu implementáciu filtrovania pomocou *iptables* a nástupcu vo forme *nftables* [1].

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 dovolujú meniť správanie jadra ostatným modulom. Každý paket prechádzajúci kernel 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 [3, 1].

2.2.2 iptables

Modul jadra `ip_tables` spolu s userspace programom `iptables` slúži na manipuláciu s tabuľkami *Xtables*, ktoré umožnujú združovať sady pravidiel do reťazcov. Reťazce následne definujú jednotlivé pravidlá pre pakety a sú spracovávané sekvenčne. Pravidlá umožnujú ovyplvňovať priechod sieťovým zásobníkom, kde každý paket musí prejsť aspoň jednou tabuľkou. [2, 3, 1]



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

iptables ponúka konfiguráciu *netfilteru* ako stavového paketového filtra možného filtrovať sieťovú prevádzku na základe typu protokolu, zdrojovej a cieľovej adresy, zdrojového a cieľového portu, znalostí protokolu a ich stavoch.

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

2.2.3 nftables

Náhrada *iptables* vo forme *nftables* je podsystém v Linuxovom jadre, ktorý mení a nahradzuje určité časti samotného *netfilteru*. Základným blokom tohto podsystému je pridanie virtuálneho stroja do Linuxového jadra, ktorý je schopný spúšťať binárny kód určený na prezeranie sieťových paketov a rozhodovanie podľa pravidiel [1, 3].

nftables neobsaujú žiaden špecifický kód naviazaný na protokol a umožnujú analyzovať aj neznáme pakety, ktorých spracovanie je definované užívateľom cez userspace program *nft*. V prípade nutnosti rozšírenia samotného firewallu je teda nutné len vytvoriť nový binárny kód, ktorý je následne vložený do virtuálneho stroja na vykonávanie a mimo toho nie je potreba meniť žiadnu časť jadra.

Kapitola 3

Návrh aplikácie

Kapitola 4

Záver

TODO

Literatúra

[1] Linux manual pages. [Online; navštívené 11.3.2020].
URL https://www.die.net/

[2] 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

[3] Harald Welte, P. N. A.: The netfilter.org project. [Online; navštívené 11.3.2020].
URL https://netfilter.org

[4] Oppliger, R.: Internet security: firewalls and beyond. *Communications of the ACM*, ročník 40, č. 5, Květen 1997: s. 92–102, doi:10.1145/253769.253802.
URL https://doi.org/10.1145/253769.253802