



**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

<b>1</b>	<b>Úvod</b>	<b>2</b>
<b>2</b>	<b>Analýza</b>	<b>3</b>
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
<b>3</b>	<b>Návrh aplikácie</b>	<b>5</b>
<b>4</b>	<b>Záver</b>	<b>6</b>
	<b>Literatúra</b>	<b>7</b>

# 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 informácií z rôznych vrstiev ISO/OSI modelu. Firewally je možné rozdeliť do nasledujúcich kategórií 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

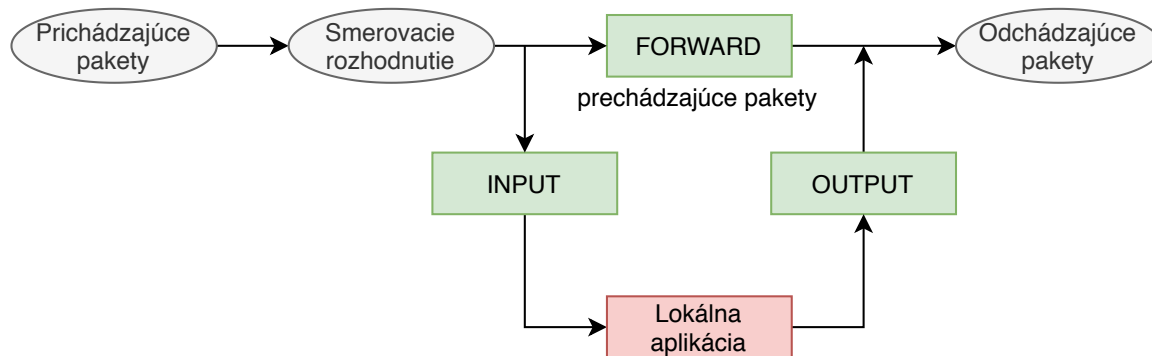
Moderné Linuxové jadro ponúka granulárnu kontrolu rôznych implementácií firewallu pre filtrovanie sieťových paketov. Práca rozoberá staršiu implementáciu filtrovania pomocou *iptables*, nástupcu vo forme *nftables* a aj firewall následujúcej generácie známy ako *bpfilter* [1].

#### 2.2.1 netfilter

*netfilter* je možné reprezentovať ako framework Linuxového jadra, slúžiacia pre filtrovanie paketov, preklad sieťových adres alebo preklad sieťových portov. Jeho hlavnú úlohu v jadre plnia hooky, ktoré dovoľujú 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 umožňujú združovať sady pravidiel do reťazcov. Reťazce následne definujú jednotlivé pravidlá pre pakety a sú spracovávané sekvenčne. Pravidlá umožňujú ovplyvňovať 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 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*. 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 umožňujú 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.

### 2.2.4 bpfilter

## 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>