

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií



SÍŤOVÉ APLIKACE A SPRÁVA SÍTÍ
2022/2023

Projekt

**Generování NetFlow dat ze zachycené
sít'ové komunikace**

Obsah

Úvod	3
Základní informace	3
Návrh programu	4
Popis implementace	5
Návod na použití.....	7
Testování	8
Zdroje	9

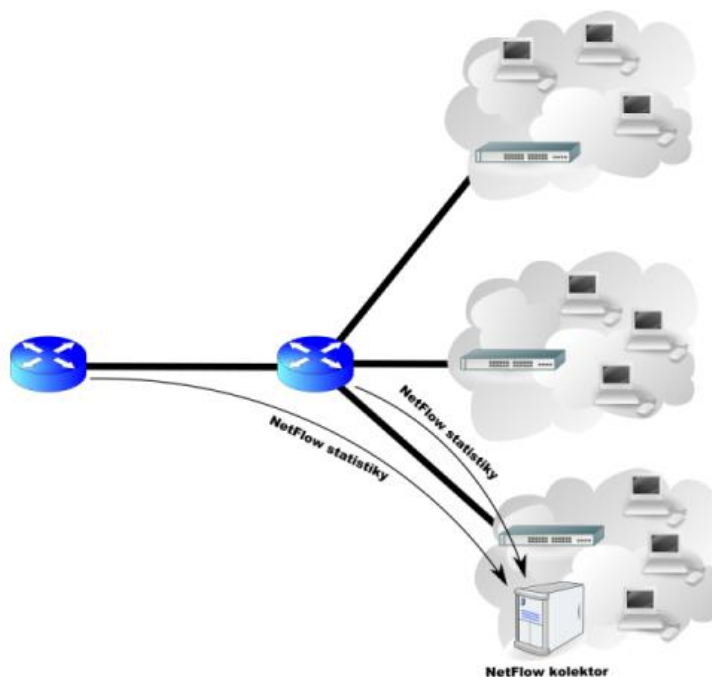
Úvod

Cílem projektu bylo navrhnout a implementovat NetFlow exportér. Jeho úkolem je analyzovat pakety a slučovat je do flows na základě jejich podobnosti. Tyto flows pak na základě zadaných vstupních parametrů odesílány na kolektor.

Základní informace

Netflow je otevřený protokol od společnosti Cisco. Hlavním účelem je monitorování síťového provozu na základě IP toků a poskytovat tak podrobný pohled do provozu na síti. S pomocí NetFlow statistik lze odhalovat vnější i vnitřní incidenty, úzká místa v síti, dominantní zdroje provozu, efektivněji plánovat budoucí rozvoj sítě, sledovat, kdo komunikoval s kým, jak dlouho a s pomocí kterého protokolu.

Architektura NetFlow se skládá z exportéru a kolektoru. Exportér analyzuje příchozí pakety. Na základě IP toků generuje statistiky, které posílá na kolektor. Kolektor sbírá statistiky z exportérů a ukládá je do dlouhodobé databáze. Nad těmito daty pak může běžet nějaká aplikace, která může vizualizovat přehledy nasbíraných statistik uživateli.



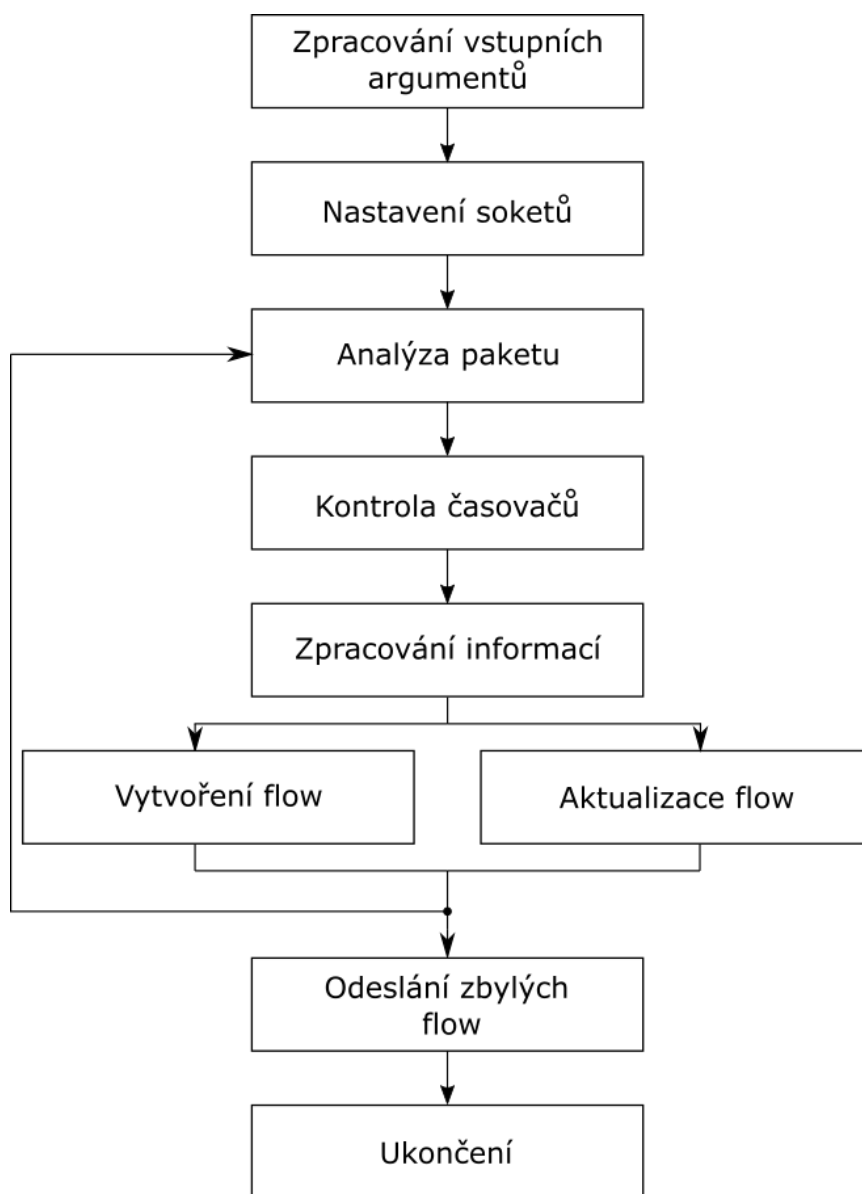
Obrázek 1: Typická architektura NetFlow

IP tok se skládá ze sekvence paketů se shodnou pěticí (sedmicí) údajů: zdrojová/cílová IP adresa, zdrojový/cílový port a typ protokolu. Každý tok o sobě nese informace, jako např. dobu vzniku, dobu trvání a další zobrazené [zde](#).

NetFlow má několik verzí, nejvíce používanou je verze 5, ale v současnosti se začíná ve větším rozsahu využívat verze 9.

Návrh programu

K implementaci byl použit jazyk C a knihovna libpcap. Struktura programu je rozdělena do několika zdrojových kódů a jednoho hlavičkového souboru. Program je navržen tak, aby analyzoval pakety v offline režimu buď z STDIN nebo souboru typu *.pcap. Pakety se stejnými základními parametry slučuje do toků („flows“), které pak exportuje na kolektor. Pro jednoduchost je v jednom paketu exportována jeden tok.



Obrázek 2: Návrh programu

Popis implementace

Program se skládá z dvou hlavních funkcí a několika pomocných. Hlavní funkce jsou **main**, **callback** a **send_flow** popsané níže.

I. main

Funkce main se zabývá obstaráním všech potřebných komponent pro funkci programu. Nejdříve zpracováním vstupních argumentů pomocí funkce **parse_arguments**, která využívá **getopt** a ukládá parametry do implementované struktury **t_Args**. Následně se main postará o založení listu **t_List** pro flows, připravením soketů pomocí funkcí z knihovny **libpcap**, nastavením filtru a následným voláním **callback** funkce pomocí knihovní funkce **pcap_loop**. Po skončení callback se provede export všech zbylých flows v listu, pomocí funkce **send_flow**, kdy čas odeslání je čas posledního příchozího paketu. V poslední části main probíhá patřičné uvolnění všech používaných komponent.

II. callback

Funkce callback proběhne pro všechny přijaté pakety ze vstupu, které splňují podmínku filtru, tudíž pouze pakety s protokoly ICMP/TCP/UDP. Má za úkol analyzovat jednotlivé pakety. Vybírá z paketů informace a na základě těchto informací je sdružuje do toků („flows“). Pro uchování těchto informací slouží struktura **t_Flow**. První informace, kterou zpracovává je tzv. „epoch time“, jenž reprezentuje čas v sekundách, který uplynul od 1. 1. 1970 do doby příchodu paketu. Tento čas považujeme jako náš aktuální čas a je využíván k vypočítání intervalů Sysup. Sysup je interval v milisekundách, který uběhl od naboootování, ovšem v našem případě jakožto boot používáme příchod prvního paketu. Jestliže se jedná o první paket, pak je náš aktuální čas zároveň časem naboootování. Dále probíhá kontrola expirace časovačů již vytvořených toků pomocí funkce **check_timers**. Jestliže toku vypršel některý z časovačů je odeslán pomocí **send_flow**. Dále probíhá zjištění pěti informací, pomocí kterých identifikujeme jednotlivé toky. Jsou jimi zdrojová/cílová IP adresa, zdrojový/cílový port a typ protokolu. K těmto informacím zpracováváme ještě další, jako např. tos („type of service“) nebo tcp flags, které je zapotřebí zapisovat a někdy i aktualizovat k jednotlivým tokům. Po zpracování veškerých informací se buď vytváří nový tok anebo se aktualizuje již vytvořený tok s dříve zmíněnou pěticí. Pro vytvoření toku se používá funkce **create_flow** a pro aktualizaci **update_flow**. Při vytváření toku je potřeba kontrolovat zaplnění cache-flow. Jestliže je maximálně zaplněna je před vytvořením nového toku nutno odeslat tok nejstarší, tudíž první tok v listu. U paketů, jež používají protokol TCP je zapotřebí kontrolovat, jestli se stav tcp flags nedostal do FIN/RST. Jestliže ano je tok, do kterého daný paket spadá, exportován.

III. send_flow

Funkce send_flow se stará o odeslání toku na kolektor. V rámci tohoto řešení jeden paket odesílá pouze jeden tok. Funkce si nejdříve připraví proměnnou **packet**, do které bude zapisovat informace o posílaném toku. Jako první se do paketu zapisuje hlavička daného toku, která obsahuje informace ukázané v [obrázku č. 3](#). Hlavička má celkovou velikost 24 B. Následně se zapisují informace o toku ukázané v [obrázku č. 4](#). Jeden tok má velikost 48 B, celý paket má tedy velikost 72 B. Informace, které nejsme schopni z analyzovaných paketů zjistit, ale tok je vyžaduje (nexthop, pad1, ...), mají přiřazenou hodnotu 0. Po zapsání veškerých informací je tok exportován a vymazán z listu.

Table B-3 Version 5 Header Format

Bytes	Contents	Description
0-1	version	NetFlow export format version number
2-3	count	Number of flows exported in this packet (1-30)
4-7	SysUptime	Current time in milliseconds since the export device booted
8-11	unix_secs	Current count of seconds since 0000 UTC 1970
12-15	unix_nsecs	Residual nanoseconds since 0000 UTC 1970
16-19	flow_sequence	Sequence counter of total flows seen
20	engine_type	Type of flow-switching engine
21	engine_id	Slot number of the flow-switching engine
22-23	sampling_interval	First two bits hold the sampling mode; remaining 14 bits hold value of sampling interval

Obrázek 3: Hlavička Flow

Table B-4 Version 5 Flow Record Format

Bytes	Contents	Description
0-3	srcaddr	Source IP address
4-7	dstaddr	Destination IP address
8-11	nexthop	IP address of next hop router
12-13	input	SNMP index of input interface
14-15	output	SNMP index of output interface
16-19	dPkts	Packets in the flow
20-23	dOctets	Total number of Layer 3 bytes in the packets of the flow
24-27	First	SysUptime at start of flow
28-31	Last	SysUptime at the time the last packet of the flow was received
32-33	srcport	TCP/UDP source port number or equivalent
34-35	dstport	TCP/UDP destination port number or equivalent
36	pad1	Unused (zero) bytes
37	tcp_flags	Cumulative OR of TCP flags
38	prot	IP protocol type (for example, TCP = 6; UDP = 17)
39	tos	IP type of service (ToS)
40-41	src_as	Autonomous system number of the source, either origin or peer
42-43	dst_as	Autonomous system number of the destination, either origin or peer
44	src_mask	Source address prefix mask bits
45	dst_mask	Destination address prefix mask bits
46-47	pad2	Unused (zero) bytes

Obrázek 4: Data Flow

Návod na použití

Program byl implementován pro Unixová prostředí. K jeho přeložení je zapotřebí překladač gcc a nástroj GNU Make.

Překlad programu za pomoci Make:

```
$ make
```

Překlad programu bez Make:

```
$ gcc -std=gnu99 -Wall -o flow *.c *.h -lpcap
```

Spuštění programu:

```
$ ./flow [-f <file>] [-c <netflow_collector>[:<port>]] [-a <active_timer>] [-i <inactive_timer>] [-m <count>] [-h]
```

Pokud spuštění předchozím příkladem není možné, je zapotřebí přidělit příkazu rootovská práva pomocí sudo (sudo ./flow ...).

Významy argumentů:

- [-f <file>] – Jméno analyzovaného souboru nebo STDIN.
- [-c <netflow_collector>[:<port>]] – IP adresa, nebo hostname NetFlow kolektoru. Volitelně i UDP port. Implicitně „127.0.0.1:2055“.
- [-a <active_timer>] - Interval v sekundách, po kterém se exportují aktivní záznamy na kolektor. Implicitně 60 s.
- [-i <inactive_timer>] – Interval v sekundách, po kterém se exportují aktivní záznamy na kolektor. Implicitně 10 s.
- [-m <count>] – Udává maximální velikost flow-cache. Při naplnění dojde k exportu nejstarší flow. Implicitně 1024.
- [-h] – Vypíše informace ohledně používání programu.

Testování

K testování projektu byly využity softwary Wireshark, Nfcapd, Nfdump, Softflowd. Wireshark sloužil ke kontrole posílání toků. Dali se v něm zobrazit jednotlivé poslané toky a informace, které nesou.

\$./flow <files/tcp.pcap

cflow						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	CFLOW	114	total: 1 (v5) flow
2	0.000030480	127.0.0.1	127.0.0.1	CFLOW	114	total: 1 (v5) flow
3	0.000033418	127.0.0.1	127.0.0.1	CFLOW	114	total: 1 (v5) flow
4	0.000035265	127.0.0.1	127.0.0.1	CFLOW	114	total: 1 (v5) flow
5	0.000037009	127.0.0.1	127.0.0.1	CFLOW	114	total: 1 (v5) flow
6	0.000038604	127.0.0.1	127.0.0.1	CFLOW	114	total: 1 (v5) flow
7	0.000040327	127.0.0.1	127.0.0.1	CFLOW	114	total: 1 (v5) flow
8	0.000041891	127.0.0.1	127.0.0.1	CFLOW	114	total: 1 (v5) flow
9	0.000043568	127.0.0.1	127.0.0.1	CFLOW	114	total: 1 (v5) flow
10	0.000045461	127.0.0.1	127.0.0.1	CFLOW	114	total: 1 (v5) flow
11	0.000047119	127.0.0.1	127.0.0.1	CFLOW	114	total: 1 (v5) flow
12	0.000048767	127.0.0.1	127.0.0.1	CFLOW	114	total: 1 (v5) flow
13	0.000050374	127.0.0.1	127.0.0.1	CFLOW	114	total: 1 (v5) flow
14	0.000051977	127.0.0.1	127.0.0.1	CFLOW	114	total: 1 (v5) flow
15	0.000054395	127.0.0.1	127.0.0.1	CFLOW	114	total: 1 (v5) flow
16	0.000056484	127.0.0.1	127.0.0.1	CFLOW	114	total: 1 (v5) flow

Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)

Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

User Datagram Protocol, Src Port: 50099, Dst Port: 2055

Cisco NetFlow/IPFIX

Version: 5

Count: 1

SysUptime: 1.57000000 seconds

Timestamp: Sep 28, 2022 00:32:58.617061000 CEST

FlowSequence: 0

EngineType: RP (0)

EngineId: 0

00.. = SamplingMode: No sampling mode configured (0)

.00 0000 0000 0000 = SampleRate: 0

pdu 1/1

SrcAddr: 100.64.208.103

DstAddr: 172.67.75.39

NextHop: 0.0.0.0

InputInt: 0

OutputInt: 0

Packets: 1

Octets: 40

[Duration: 0.000000000 seconds]

SrcPort: 44178

DstPort: 443

Padding: 00

TCP Flags: 0x10

Protocol: TCP (6)

IP ToS: 0x00

SrcAS: 0

DstAS: 0

SrcMask: 0 (prefix: 0.0.0.0/32)

DstMask: 0 (prefix: 0.0.0.0/32)

Padding: 0000

Obrázek 5: Zobrazení odeslaných flows ve Wireshark

Pomocí Nfcapd bylo možné spustit kolektor toků, na který pak bylo možné dané toky posílat. Výstupy generoval do *.nf souborů, které bylo možné zobrazit pomocí Nfdump.

\$./flow -f files/tcp.pcap -c 0.0.0.0:2056

student@student-wi: ~/Desktop/ISA_projekt5 nfdump -r records/2022/11/13/21/nfcapd.202211132111											
Date first seen	Event	XEvent	Proto	Src IP Addr:Port	Dst IP Addr:Port	X-Src IP Addr:Port	X-Dst IP Addr:Port	In Byte	Out Byte		
2022-09-28 00:32:57.047	INVALID	Ignore	TCP	100.64.208.103:44178	-> 172.67.75.39:443	0.0.0.0:0	-> 0.0.0.0:0	40	0		
2022-09-28 00:32:57.047	INVALID	Ignore	TCP	100.64.208.103:41098	-> 2.20.72.139:443	0.0.0.0:0	-> 0.0.0.0:0	52	0		
2022-09-28 00:32:57.047	INVALID	Ignore	TCP	100.64.208.103:41090	-> 2.20.72.139:443	0.0.0.0:0	-> 0.0.0.0:0	52	0		
2022-09-28 00:32:57.047	INVALID	Ignore	TCP	100.64.208.103:41110	-> 2.20.72.139:443	0.0.0.0:0	-> 0.0.0.0:0	52	0		
2022-09-28 00:32:57.047	INVALID	Ignore	TCP	100.64.208.103:41126	-> 2.20.72.139:443	0.0.0.0:0	-> 0.0.0.0:0	52	0		
2022-09-28 00:32:57.047	INVALID	Ignore	TCP	100.64.208.103:41140	-> 2.20.72.139:443	0.0.0.0:0	-> 0.0.0.0:0	52	0		
2022-09-28 00:32:57.052	INVALID	Ignore	TCP	172.67.75.39:443	-> 100.64.208.103:44178	0.0.0.0:0	-> 0.0.0.0:0	40	0		
2022-09-28 00:32:57.061	INVALID	Ignore	TCP	2.20.72.139:443	-> 100.64.208.103:41098	0.0.0.0:0	-> 0.0.0.0:0	52	0		
2022-09-28 00:32:57.067	INVALID	Ignore	TCP	2.20.72.139:443	-> 100.64.208.103:41090	0.0.0.0:0	-> 0.0.0.0:0	52	0		
2022-09-28 00:32:57.067	INVALID	Ignore	TCP	2.20.72.139:443	-> 100.64.208.103:41126	0.0.0.0:0	-> 0.0.0.0:0	52	0		
2022-09-28 00:32:57.067	INVALID	Ignore	TCP	2.20.72.139:443	-> 100.64.208.103:41140	0.0.0.0:0	-> 0.0.0.0:0	52	0		
2022-09-28 00:32:57.067	INVALID	Ignore	TCP	2.20.72.139:443	-> 100.64.208.103:41110	0.0.0.0:0	-> 0.0.0.0:0	52	0		
2022-09-28 00:32:58.308	INVALID	Ignore	TCP	3.68.63.139:443	-> 100.64.208.103:55792	0.0.0.0:0	-> 0.0.0.0:0	1104	0		
2022-09-28 00:32:58.308	INVALID	Ignore	TCP	100.64.208.103:55792	-> 3.68.63.139:443	0.0.0.0:0	-> 0.0.0.0:0	52	0		
2022-09-28 00:32:58.616	INVALID	Ignore	TCP	162.159.130.234:443	-> 100.64.208.103:59164	0.0.0.0:0	-> 0.0.0.0:0	235	0		
2022-09-28 00:32:58.617	INVALID	Ignore	TCP	100.64.208.103:59164	-> 162.159.130.234:443	0.0.0.0:0	-> 0.0.0.0:0	40	0		
Summary: total flows: 16, total bytes: 2031, total packets: 16, avg bps: 10349, avg pps: 10, avg bpp: 126											
Time window: 2022-09-28 00:32:57 - 2022-09-28 00:32:58											
Total flows processed: 16, Blocks skipped: 0, Bytes read: 1408											
Sys: 0.003s flows/second: 4935.2 Wall: 0.000s flows/second: 96969.7											

Obrázek 6: Zobrazení statistik z kolektoru pomocí nfdump

Softflowd sloužil k poskytnutí referenčních výsledků.

Zdroje

- NetFlow. *Wikipedia* [online]. 13 říjen 2022 [cit. 2022-11-13]. Dostupné z: <https://en.wikipedia.org/wiki/NetFlow>
- NetFlow Export Datagram Format. *Cisco* [online]. 14. září 2007 [cit. 2022-11-13]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/net_mgmt/netflow_collection_engine/3-6/user/guide/format.html#wp1003394
- Writing manual pages. *Cisco* [online]. 6. ledna 2006 [cit. 2022-11-13]. Dostupné z: <https://liw.fi/manpages/>
- Nfcapd. *FreeBSD* [online]. 19. srpna 2005 [cit. 2022-11-13]. Dostupné z: https://www.freebsd.org/cgi/man.cgi?query=nfcapd&apropos=0&sektion=1&man_path=FreeBSD+8.2-RELEASE+and+Ports&format=html
- Send. *Die.net* [online]. [cit. 2022-11-13]. Dostupné z: <https://linux.die.net/man/3/send>
- Send. *Die.net* [online]. [cit. 2022-11-13]. Dostupné z: <https://linux.die.net/man/3/htons>
- Gethostbyname. *Man7.org* [online]. 22. března 2021 [cit. 2022-11-13]. Dostupné z: <https://man7.org/linux/man-pages/man3/gethostbyname.3.html>
- Tcp.h. *Netinet* [online]. [cit. 2022-11-13]. Dostupné z: <https://sites.uclouvain.be/SystInfo/usr/include/netinet/tcp.h.html>
- Udp.h. *Netinet* [online]. [cit. 2022-11-13]. Dostupné z: <https://sites.uclouvain.be/SystInfo/usr/include/netinet/udp.h.html>
- TCP flags. *Pierky's Blog* [online]. [cit. 2022-11-13]. Dostupné z: <https://blog.pierky.com/netflow-weird-tcp-flags-in-flowviewer-and-flow-print/>