VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Síťové aplikace
NetFlow v5 exportér

Machala Roman (xmacha86)

Obsah

1 Úvod

NetFlow je síťový protokol vyvinut společností CISCO, který slouží k monitorování a analýze síťového provozu. Umožňuje zachytávat jednotlivé pakety, které následně rozděluje do toků na základě např. zdrojové a cílové IP adresy. Tyto data jsou zachycena kolektorem a následně pomocí protokolu UDP jsou zaslána do centrálního sběrače (kolektoru), kde mohou být analyzována za účelem zjistit vytížení síte, anomálie nebo například i bezpečnostních incidentů[1].

Pro protokol NetFlow existuje mnoho verzí, nicméně tato práce se zabývá pouze verzí v5, což je jedna z nejpoužívanějších verzí vůbec dostupná na drtivé většině routerů různých výrobců.Tato verze byla navržena pro sběr informací síťového provozu pouze na bázi IPv4. Pro podporu IPv6 je nutno vuyžívat vyšších verzí, jako je například NetFlow v9[4].

1.1 IP Tok

Jak již bylo zmíněno výše, protokol NetFlow pracuje s jednotlivými paketami, které rozděluje do **toků**. Každý takový tok je určen unikátní kombinací následujících informací:

- **Zdrojová IP adresa**
- **Cílová IP adresa**
- **Zdrojový PORT**
- **Cílový PORT**
- Typ služby (ToS)
- **Protokol 3 vrstvy**
- Rozhranní

Všechny toky jsou pouze jednosměrné, proto například prohozením adres odesílatele a příjemce nevznikne nový tok, jak je demonstrováno na obrázku 1. V rámci této implementace popsané v této práci jsou ovšem za unikátní identifikátory uvažovány pouze **tučně** vyznačené infromace. Více info o rozdílech a limitacích v sekci 1.3.

Tok 1:

Zdrojová IP:	192.168.1.1
Cílová IP:	10.0.0.1
Zdrojový port:	12345
Cílový port:	80
Typ služby (ToS):	0
Protokol 3 vrstvy:	TCP
Rozhraní:	eth0

Tok 2:

Zdrojová IP:	10.0.0.1
Cílová IP:	192.168.1.1
Zdrojový port:	80
Cílový port:	12345
Typ služby (ToS):	0
Protokol 3 vrstvy:	TCP
Rozhraní:	eth0

Obrázek 1: Příklad 2 různých toků

Z obrázku 1 může být taky patrné, že protokol nebere ohled na obsah jednotlivých paket, co se týče rozdělení paket do toků. V rámci protokolu NetFlow v5 se s obsahem paket nijak nemanipuluje, uchovávají se ovšem další informace, které jsou vhodné pro statistické vyobrazení a monitorování síťového provozu.

1.2 Struktura toků/NetFlow v5 datagram

Kromě klíčových informací sloužících k rozdělení jednotlivých paket do toků se ukládají i jiné informace o každém toku. Výčet těchto informací je vyobrazen jako struktura v jazyce C na obrázku 2. V tomto formátu jsou jednotlivé toky pomocí UDP protokolu odeslány na kolektor.

Jelikož je používán protokol UDP pro export datagramů, je možné, že některé datagramy mohou být ztraceny. Z tohoto důvodu novější verze tohoto protokolu, přesněji verze 5, 7 a 8 obsahuje hlavička, dále popsána na obrázku 3, kontrolní číslo toku (flow control number), které je rovno kontrolnímu číslu předešlého toku + počet toků v předešlém datagramu. Při přijetí nového datagramu tak kolektor může zkontrolovat, zda došlo ke ztrátě toků[2][3].

```
typedef struct NetFlowv5 {
    uint32_t srcaddr;       /* Source IP address */
    uint32_t dstaddr;       /* Destination IP address */
    uint32_t nexthop;       /* IP address of next hop router */
    uint16_t input;         /* SNMP index of input interface */
    uint16_t output;        /* SNMP index of output interface */
    uint32_t dPkts;         /* Packets in the flow */
    uint32_t dOctets;       /* Total number of Layer 3 bytes */
    uint32_t first;         /* SysUptime at start of flow */
    uint32_t last;          /* SysUptime at the time the last packet */
    uint16_t srcport;       /* TCP/UDP source port number */
    uint16_t dstport;       /* TCP/UDP destination port number */
    uint8_t pad1;           /* Unused (zero) bytes */
    uint8_t tcp_flags;      /* Cumulative OR of TCP flags */
    uint8_t prot;           /* IP protocol type (for example, TCP = 6) */
    uint8_t tos;            /* IP type of service (ToS) */
    uint16_t src_as;        /* Autonomous system number of the source */
    uint16_t dst_as;        /* Autonomous system number of the dest */
    uint8_t src_mask;       /* Source address prefix mask bits */
    uint8_t dst_mask;       /* Destination address prefix mask bits */
    uint16_t pad2;          /* Unused (zero) bytes */
} netflowv5;
```

Obrázek 2: NetFlow v5 tělo datagramu

```
typedef struct NetFlowHeader {
    uint16_t version;           /* NetFlow export format version num */
    uint16_t count;             /* Number of exported flows */
    uint32_t sysUptime;         /* Current time in ms since start */
    uint32_t unix_secs;         /* Current count of seconds since CUT */
    uint32_t unix_nsecs;        /* Residual nanoseconds since CUT */
    uint32_t flow_sequence;     /* Sequence cnt of total flows seen */
    uint8_t engine_type;        /* Type of flow-switching engine */
    uint8_t engine_id;          /* Slot num of flow-switching engine */
    uint16_t sampling_interval; /* Sampling mode + interval (2b - 14b) */
} NetFlowHeader;
```

Obrázek 3: NetFlow v5 hlavička datagramu

1.3 Rozdíly v implementaci

V této sekci jsou popsány limitace procesu návrhu a implementace exportéru pro protokol NetFlow v5. Tento exportér zpracovává pakety z poskytnutého PCAP souboru. Z tohoto důvodu se s implementací řeší i různé omezení. Následující výčet položek struktury datagramu, popsanou v sekci 1.2, jsou z důvodu načítání paket z PCAP souboru nedostupné:

1. IP adresa routeru dalšího skoku
2. SNMP index vstupního Rozhranní
3. SNMP index výstupního Rozhranní
4. SysUptime od začátku toku - doba od spuštění zařízení na kterém byly zachycenz pakety
5. SysUptime na konci přijetí posledního paketu - doba od spuštění zařízení až po zachycení poslední pakety
6. Číslo autonomního systému zdroje
7. Číslo autonomního systému cíle
8. Prefix masky zdrojové adresy
9. Prefix masky cílové adresy

Kromě tohoto se implementovaný exportér zaměřuje pouze na analýzu TCP paketů. Jednotlivé detaily jsou přiblíženy u samotné implementace.

Jelikož exportér zpracovává pakety ze souboru, tzn. pakety, které byly zachyceny dříve, než byl program spuštěn, jsou pro položky:

- SysUptime od začátku toku
- SysUptime na konci přijetí posledního paketu

uvažovány časy jejich skutečného zachycení, tedy času před spuštěním tohoto programu. Z toho důvodu jsou jednotlivé časové značky **záporné**.

2 Návrh a implementace

Samotná aplikace je rozdělena do několika větších celků, kde každý celek zajišťuje určitou část aplikace. Jednotlivé celky jsou implementovány v samostatných `.c` a `.h` souborech. Jednotlivé celky dohromady potom tvoří výslednou aplikaci pracující jako exportér NetFlow v5 toků.

2.1 Zpracování argumentů

Tento celek se stará o zpracování argumentů příkazové řádky, poskytnuté uživatelem, převodem těchto argumentů do jejich očekávané podoby (pokud je to potřeba), nebo ke kontrole jejich správnosti.

Parametr	Popis	Povinný
`hostname:port`	IP adresa a port kolektoru	Ano
`pcap_soubor`	PCAP soubor obsahující pakety pro analýzu	Ano
`-a | --active`	Aktivní timeout v sekundách	Ne
`-i | --inactive`	Neaktivní timeout v sekundách	Ne
`-d | --debug`	Povolit ladicí výstup	Ne

Tabulka 1: Parametry aplikace

V tabulce 1 je možno vidět, jaké parametry aplikace podporuje. Na jejich pořadí nezáleží, ovšem povinné parametry musejí být vždy přítomny. Pokud nejsou stanoveny parametry **-a** a **-i**, tedy aktivní a neaktivní timeout, pracuje se s defaultní hodnotou 60 sekund.

2.2 Zpracování paket ze souboru PCAP

Pro zpracování jednotlivých paket a jejich manipulace s nimi je prováděna výhradně za pomocí knihovny PCAP[**?**].

3 Testování aplikace

3.1 Návrh testů

3.2 Referenční programy a jejich použití

3.3 Vyhodnocení testování

4 Návod na použití

5 Závěr

Reference

[1] CISCO. *Cisco IOS Flexible NetFlow* https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/flexible-netflow/product_data_sheet0900aecd804b590b.html. 2006. Navštíveno 24.9.2024.

[2] CISCO. *NetFlow Export Datagram Format* https://www.cisco.com/c/en/us/td/docs/net_mgmt/netflow_collection_engine/3-6/user/guide/format.html. 2007. Navštíveno 24.9.2024.

[3] IBM. *NetFlow V5 formats* https://www.ibm.com/docs/en/npi/1.3.1?topic=versions-netflow-v5-formats. 2022. Navštíveno 24.9.2024.

[4] MANAGEENGINE. *What is a NetFlow Collector?* https://www.manageengine.com/products/netflow/what-is-netflow.html?nfa-index-flowtypes. Navštíveno 24.9.2024.