Vysoké učení technické v Brně

Fakulta informačních technologií

Síťové aplikace a správa sítí

2020/2021

Generování NetFlow dat ze zachycené sítové komunikace

Matúš Vráblik (xvrabl05) Brno, 12. Listopad 2021

Obsah

Úvod do problematiky

NetFlow

NetFlow je protokol, ktorý sa používa na monitorovanie sieťovej prevádzky na základe IP tokov. Skladá sa z 3 častí: Exportér, Kolektor a Analyzátor. V rámci tohoto projektu sa implementuje exportér.

Exportér

Exportér zlučuje zachytené pakety do tokov a exportuje záznamy o týchto tokoch do kolektora. Keďže robíme offline resp. exportér zo zachytených záznamov tak časy tokov nie sú v prítomnom čase a preto sa ich export líši. Ako časové značky sa používajú časy jednotlivých paketov. Toky sa exportujú v prípade že sa naplní niektorá z nižšie uvedených podmienok pre expiráciu tokov a naplní sa pole expirovaných tokov 30-timi tokmi alebo sa prečítajú všetky pakety a odošlú sa na kolektor všetky aktívne aj expirované toky rovnakým spôsobom, teda všetky aktívne sa expirujú a následne exportujú.

Návrh aplikácie

Aplikácia načítava pakety zo zadaného vstupu. Každý paket sa priradí do toku spolu s informáciami o pakete potrebnými pre V5 formát hlavičky a záznamu. Toky sa pripravia na export a následne sa exportujú ak je pripravených 30 tokov na export alebo sa dočítali všetky pakety zo vstupu. Exportuje sa na predvolený localhost server a port 2055 ak nie je argumentami programu nastavené inak.

Popis implementácie

Argumenty

Z argumentov aplikácie sa upravia hodnoty pre server, port, active, inactive, vstupný súbor a veľkosť cache pre toky.

main()

Otvorí sa vstupný súbor (predvolený STDIN) pomocou pcap_fopen_offline(), zistí sa dĺžka ethernetovej hlavičky pomocou pcap_datalink() a spracujú sa postupne všetky pakety funkciou pcap_loop(), ktorá volá got_packet() funkciu s predvolenými parametrami. Po spracovaní všetkých paketov sa exportujú všetky toky ktoré zostali v cache-i tokov funkciou exportFlowAll().

got_packet()

Skontroluje či je packet typu ETHERTYPE_IP, ak nie tak ho preskočí. Vytvorí identifikátor paketu, ktorý obsahuje navyše čas paketu, príznaky TCP a dĺžku paketu v byte-och. Naplní identifikátor zdrojovou a cieľovou IP adresou aj portom a ToS. Prevedie paket na štruktúru ip z ktorej vyčíta veľkosť hlavičky ip a zistí s akým protokolom bol paket odoslaný. Podľa protokolu prevedie paket znova na štruktúru podľa typu (TCP, UDP, ICMP) a do identifikátora vloží zdrojový a cieľový port, v prípade ICMP paketu type a code respektíve. Pri TCP pakete vkladá do indetifikátora ešte TCP príznaky. Následne sa volá funkcia updateFlow() s identifikátorom ako parametrom.

updateFlow()

Pokúsi sa nájsť aktívny tok podľa identifikátora. Nastaví aktuálny čas aplikácie na čas z identifikátora pomocou setLatest().

Ak sa nenašiel tok tak sa nastaví čas začiatku aplikácie pomocou setFirst(). Prevedie sa kontrola na veľkosť pola tokov, ak obsahuje počet prvkov rovný hodnote cache tokov tak sa najstarší presunie z pola tokov do pola expirovaných tokov. Pokračuje sa vytvorením nového toku a vložením to pola tokov.

Ak sa našiel tok, tak sa prevedú kontroly na prítomnosť TCP príznakov FIN a RST, kontrola doby toku a kontrola na neaktívnosť toku. Ak sa splní niektorá z týchto podmienok, tak sa tok presunie do pola expirovaných tokov a volá sa táto funkcia odznova, aktuálne volanie funkcie sa ukončuje. Ak sa nesplní žiadna z podmienok, aktualizujú sa nasledujúce hodnoty tohto toku z identifikátora: TCP príznaky, byte-i, pakety v toku a čas posledného paketu v toku. Expirovanie toku sa vykonáva funkciou exportFlow().

exportFlow()

Porovná počet tokov v poli expirovaných a ak je menší ako 30 (limit V5 formátu) tak vloží tok z parametru funkcie do pola expirovaných tokov. V opačnom prípade sa exportujú všetky prvky pola expirovaných tokov funkciou exportExpired(). Tok z parametru funkcie sa vloží do prázdneho pola expirovaných tokov.

exportExpired()

Naplní premennú header o veľkosti 24B byte po byte podla NetFlow V5 formátu hlavičky. Naplní premennú record o veľkosti 48B znova byte po byte podľa NetFlow V5 formátu záznamu a vloží sa do premennej data o veľkosti 24B + 48B*(veľkosť pola expirovaných tokov) pre každý prvok v poli expirovaných tokov. Uloží výsledok do súboru datafile a spustí sa udp klient, ktorý vytvoril Petr Matoušek, s adresou a portom zadaným pri volaní exportéru ako argumenty a súborom datafile ako stdin.

exportFlowAll()

Najprv sa expirujú všetky toky z pola aktívnych tokov a potom sa zavolá funkcia exportExpired().

setLatest()

Funkcia na nastavenie najaktuálnejšieho času.

setFirst()

Funkcia nastaví počiatočný čas aplikácie ak ešte nebol nastavený.

Základné informácie o programe

Dokáže spracovať TCP, UDP a ICMP pakety, iné ignoruje.

Podporuje pakety zachytené s linkovým tipom ppp, linux ssl, slip, BSD loopback encapsulation a Ethernet.

Toky rozdeľuje podal 6-tice: zdrojová IP, cieľová IP, zdrojový port, cieľový port, protocol, ToS.

TCP toky ukončuje pri príznakoch FIN a RST.

ICMP – do zdrojového portu a cieľového portu uloží hodnoty z ICMP type a code respektíve.

Návod na použitie

./flow [options]

-c <netflow_collector:port> IP adresa alebo hostname NetFlow kolektoru, UDP port je volitelný (localhost:2055, pokiaľ nie je špecifikované)

-f <file> meno analyzovaného súboru (STDIN ak nie je špecifikované)

-a <active_timer> interval v sekundách, ktorý keď uplynie tak sa daný aktívny tok považuje za expirovaný (Predvolená hodnota 60 sekúnd)

-i <inactive_timer> interval v sekundách, ktorý keď uplynie tak sa daný neaktívny tok považuje za expirovaný (Predvolená hodnota 10 sekúnd)

-m <count> veľkosť cache tokov. Pri dosiahnutí max. veľkosti sa expiruje najstarší záznam v cachi (1024 pokiaľ nie je špecifikované)